ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αλγεβρικοί αλγόριθμοι και εφαρμογές στη γεωμετρία

ΗΛΙΑΣ Π. ΤΣΙΓΑΡΙΔΑΣ

ΑΘΗΝΑ
ΑΥΓΟΥΣΤΟΣ 2006

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αλγεβρικοί αλγόριθμοι και εφαρμογές στη γεωμετρία

Ηλίας Π. Τσιγαρίδας

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: **Ιωάννης Εμίρης**, Αναπληρωτής Καθηγητής ΕΚΠΑ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:

Ιωάννης Εμίρης, Αναπληρωτής Καθηγητής ΕΚΠΑ
Θεοχάρης Θεοχάρης, Αναπληρωτής Καθηγητής ΕΚΠΑ
Νικόλαος Μισυρλής, Καθηγητής ΕΚΠΑ

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Ιωάννης Εμίρης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Σέργιος Θεοδωρίδης,
Καθηγητής ΕΚΠΑ

Θεοχάρης Θεοχάρης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Νικόλαος Καλουπτσίδης,
Καθηγητής ΕΚΠΑ

Ηλίας Κουτσουπιάς,
Καθηγητής ΕΚΠΑ

Νικόλαος Μισυρλής,
Καθηγητής ΕΚΠΑ

Ευάγγελος Ράπτης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Ημερομηνία Εξέτασης: 29 Αυγούστου 2006

Περίληψη

Πραγματικοί αλγεβρικοί αριθμοί είναι οι πραγματικοί αριθμοί που προκύπτουν ως ρίζες πολυωνύμων σε μία μεταβλητή, με ακέραιους συντελεστές. Στόχος της παρούσας διατριβής είναι η ανάπτυξη, ανάλυση και αποτελεσματική υλοποίηση αλγορίθμων ακριβείας (exact algorithms), που βασίζονται σε αριθμητική ακεραίων απεριόριστης ακρίβειας και αφορούν υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς, καθώς και εφαρμογές αυτών σε προβλήματα και αλγορίθμους της μη γραμμικής υπολογιστικής γεωμετρίας.

Προκειμένου να κατασκευαστούν οι πραγματικοί αλγεβρικοί αριθμοί πρέπει να επιλυθεί, στους πραγματικούς, ένα πολυώνυμο με ακέραιους συντελεστές.

Ενοποιούμε και απλοποιούμε την θεωρία που αφορά τους αλγορίθμους επίλυσης, οι οποίοι βασίζονται στην υποδιαίρεση, και βελτιώνουμε την πολυπλοκότητα του αλγορίθμου που βασίζεται στα συνεχή κλάσματα. Επιτυγχάνεται, με νέο τρόπο, το καλύτερο γνωστό φράγμα πολυπλοκότητας. Επιπρόσθετα, αποδεικνύεται ότι το φράγμα αυτό ισχύει και για πολυώνυμα με τετράγωνα, ενώ με την ίδια πολυπλοκότητα υπολογίζουμε και την πολλαπλότητα των ριζών. Αποδεικνύουμε ένα νέο φράγμα για την αναμενόμενη πολυπλοκότητα της μεθόδου των συνεχών κλασμάτων. Οι αλγόριθμοι επίλυσης γενικεύονται και σε πολυωνυμικά συστήματα δύο μεταβλητών. Τα πειραματικά μας αποτελέσματα επιβεβαιώνουν την ταχύτητα των μεθόδων.

Οι αλγόριθμοι για τους πραγματικούς αλγεβρικούς αριθμούς αφορούν την κατασκευή, την σύγκριση και τον υπολογισμό του προσήμου ενός πολυωνύμου πάνω σε έναν και δύο πραγματικούς αλγεβρικούς αριθμούς, καθώς και το πρόβλημα της απαλοιφής ποσοδεικτών. Αν ο βαθμός του πολυωνύμου είναι μικρός (μέχρι 4 για μία μεταβλητή, μέχρι 2 για δύο μεταβλητές), προτείνουμε αλγορίθμους ειδικού σκοπού οι οποίοι έχουν σταθερή αριθμητική πολυπλοκότητα. Για όλους τους παραπάνω αλγορίθμους παρουσιάζεται υλοποίηση σε C++ και πειραματική μελέτη.

Στην υπολογιστική γεωμετρία μελετούνται τα κατηγορήματα που απαιτούνται στους αλγορίθμους υπολογισμού της διάταξης ελλειπτικών τόξων στο επίπεδο και στον υπολογισμό του διαγράμματος Voronoi ελλείψεων. Τέλος, δοθέντος ενός κυρτού πολυγώνου με ακέραιες κορυφές εξετάζουμε αλγορίθμους που μας επιτρέπουν να το διασπάσουμε σε δύο άλλα κυρτά πολύγωνα τέτοια ώστε το άθροισμά τους κατά Minkowski να ισούται με το αρχικό πολύγωνο.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Αλγεβρικοί αλγόριθμοι, Υπολογιστική γεωμετρία
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ : πραγματικοί αλγεβρικοί αριθμοί, πραγματική επίλυση, επιλύουσα, διατάξεις, διάγραμμα Voronoi

Abstract

Real algebraic numbers are the real numbers that are real roots of univariate polynomials with integer coefficients. We study exact algorithms, from a theoretical and an implementation point of view, based on integer arithmetic of arbitrary precision, for computations with real algebraic numbers and applications of these algorithms on problems and algorithms in non linear computational geometry.

In order to construct a real algebraic number we must compute the real roots of a univariate polynomial with integer coefficients.

We unify and simplify the theory behind the subdivision based algorithms for real root isolation and we improve the complexity of the algorithm that is based on the continued fraction expansion of the real numbers. The best known complexity bound up today is achieved using new techniques. Moreover, we prove that the bound holds for non square-free polynomials and that in the same complexity bound we can compute the multiplicities of the real roots. We prove a new bound for the expected complexity of the algorithm based on continued fractions. We generalize the real root isolation algorithms to bivariate polynomial systems. Our experimental analysis proves the effectiveness of our methods.

The algorithms that we consider for computations with real algebraic numbers are construction, comparison, sign evaluation and quantifier elimination. If the degree of the polynomial is small, i.e. ≤ 4 in the univariate case and ≤ 2 in the bivariate case, we propose special purpose algorithms that have constant arithmetic complexity. For all the algorithms we present a C++ implementation and an experimental analysis.

In computational geometry we study the predicates needed by the algorithms for the arrangement of elliptic arcs in the plane and the computation of the Voronoi diagram of ellipses, also in the plane. Finally, given a convex lattice polygon we study algorithms for decomposing it to two other convex lattice polygons, such that their Minkowski sum is the original polygon.

SUBJECT AREA: Algebraic algorithms, Computational geometry
KEYWORDS: real algebraic numbers, real solving
resultant, arrangements, Voronoi diagram

Στο μπαμπά, στη μαμά και στην Άννα

Ευχαριστίες

Η εκπόνηση μιας διδακτορικής διατριβής είναι μια δύσκολη προσπάθεια. Είναι σίγουρο ότι δεν θα είχα καταφέρει να ολοκληρώσω τη διατριβή μου αν οι καθηγητές μου, οι φίλοι μου και η οικογένεια μου δεν με είχαν βοηθήσει. Τα λίγα λόγια που τους αφιερώνω εδώ είναι το ελάχιστο που μπορώ να κάνω. Άλλωστε η ευγνωμοσύνη δεν περιγράφεται.

Καταρχάς, θα ήθελα να ευχαριστήσω τον καθηγητή μου Γιάννη Εμίρη για την εμπιστοσύνη που μου έδειξε και για την ευκαιρία που μου έδωσε να ασχοληθώ με επιστημονικά ζητήματα που με ενδιέφεραν. Δεν θα ξεχάσω ποτέ ότι η πόρτα του γραφείου του ήταν πάντοτε ανοιχτή και ότι επέλεξε συνειδητά όχι να με 'χειριστεί', αλλά να με στηρίξει και με ενθαρρύνει. Ελπίζω να ανταποκρίθηκα στις προσδοκίες του και ο σεβασμός και η ευγνωμοσύνη μου να ανταποδίδουν σε κάποιο βαθμό τις προσπάθειές του.

Είμαι πολύ τυχερός που οι καθηγητές Σέργιος Θεοδωρίδης, Θεοχάρης Θεοχάρης, Νικόλαος Καλουπτσίδης, Ηλίας Κουτσουπιάς, Νικόλαος Μισυρλής και Ευάγγελος Ράπτης μου έκαναν την εξαιρετική τιμή να συμμετάσχουν στην επταμελή μου επιτροπή. Τους ευχαριστώ θερμά.

Θα ήθελα επίσης να ευχαριστήσω τον Bernard Mourrain, την Monique Teillaud και τον David Daney, από το INRIA Sophia-Antipolis, και τον Μενέλαο Καραβέλα, από το Πανεπιστήμιο της Κρήτης, για τη συνεργασία μας και την εμπιστοσύνη τους. Ιδιαίτερα ο Bernard λειτούργησε ως συνεπιβλέποντάς μου και με βοήθησε όσο περισσότερο μπορούσε. Τον ευχαριστώ για όλα.

Όταν ξεκινήσα την εκπόνηση της διδακτορικής μου διατριβής πίστευα ότι οι επιστημονικές προκλήσεις θα ήταν τα μόνα εμπόδια που συναντούσα. Κάτι τέτοιο όμως δεν ανταποκρίνεται στην πραγματικότητα, ή τουλάχιστον δεν ανταποκρίνεται στην πραγματικότητα που βιώσα εγώ. Η εκπόνηση μιας διατριβής απαιτεί να ξεπεράσεις και πολλά άλλα εμπόδια και είναι μια ψυχοφθόρα διαδικασία. Μια διαδικασία την οποία δεν θα είχα καταφέρει να φέρω εις πέρας χωρίς τη βοήθεια των φίλων μου και της οικογένειάς μου.

Στη Χρυσηίδα λέω απλά ευχαριστώ. Άλλωστε με καταλαβαίνει καλύτερα από τον καθένα και ό,τι και να γράψω θα ήταν πλεονασμός.

Ο Γιώργος Κ είναι ένας πολύ σημαντικός φίλος για μένα. Τον ευχαριστώ για την φιλία του και για τις ατελείωτες βόλτες που κάναμε προσπαθώντας να λύσουμε το γόρδιο δεσμό ενός ακόμα $f(x)$. Ίσως και με το Νίκο Π να καταφέρουμε να λύσουμε κάποιον.

Στους φίλους μου στο DI, ή πέριξ αυτού, Βασίλη, Κυριάκο, Γιώργο, Θανάση, Στρατή, Αντώνη, Μάριο, Γεράσιμο, Ευριπίδη, Δημήτρη και Χρήστο οφείλω, τουλάχιστον, ένα μεγάλο ευχαριστώ.

Τα τελευταία 3 χρόνια τις περισσότερες ώρες της ημέρας (μερικές φορές και της νύχτας) τις πέρασα με τους φίλους μου στα διπλανά 'γραφεία' (sic). Τη Μαρία, τον Ορέστη και το Γιώργο. Με

ανέχτηκαν και τους ανέχτηκα και μοιραστήκαμε τα κουτσομπολιά μας, τις χαρές και τις λύπες μας. Τους ευχαριστώ θερμά και θα τους είμαι ευγνώμων για πάντα.

Η απομόνωση κατά διαστήματα που απαιτεί μια διδακτορική διατριβή με έκανε να παραμελήσω πολλούς από τους φίλους μου εκτός του Πανεπιστημίου. Ο Παντελής Κ, ο Κώστας Π, η Σεβαστή Ν και οι κουμπάροι μου Νίκος και Βούλα πρέπει να έχουν τα μεγαλύτερα παράπονα. Τους ευχαριστώ για την κατανόησή τους και τους ζητώ να με συγχωρήσουν. Θα επανορθώσω στην πρώτη ευκαιρία.

Στο Βασίλη, στον Κώστα και στο Χρήστο θα τους εξηγήσω σε κάποιο άλλο αγώνα Champions League τι ερευνώ ακριβώς. Τους ευχαριστώ που με στήριξαν και ας μην καταλαβαίνουν γιατί μπήκα σε όλη αυτή τη διαδικασία.

Ο θείος μου ο Δημήτρης μου στάθηκε όσο περισσότερο μπορούσε και λίγο παραπάνω. Τον ευχαριστώ πολύ.

Η μητέρα μου και η αδελφή μου έκαναν ότι μπορούσαν για να με βοηθήσουν στην προσπάθειά μου. Αν ήξεραν και λίγα μαθηματικά παραπάνω ίσως να μου έλυναν και κάποια εξίσωση. Σε κάθε περίπτωση τους χρωστώ τα πάντα και τους αφιερώνω τη διατριβή μου ως το ελάχιστο που θα μπορώ να κάνω.

Ελπίζω να μην έχω ξεχάσει να αναφέρω κάποιον. Αν το έχω κάνει του ζητώ να με συγχωρήσει.

Ηλίας Π. Τσιγαρίδας
Αθήνα
Αύγουστος, 2006

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Αν θες να μάθεις για τη διαδρομή,
ρώτησε αυτούς που επιστρέφουν.

Κινέζικο γνωμικό

Πραγματικοί αλγεβρικοί αριθμοί είναι οι πραγματικοί αριθμοί που προκύπτουν ως ρίζες πολυωνύμων σε μία μεταβλητή, με ακέραιους συντελεστές. Σκοπός της παρούσας διατριβής είναι η ανάπτυξη, ανάλυση και αποτελεσματική υλοποίηση αλγορίθμων που βασίζονται σε αριθμητική ακριβείας[1] και αφορούν την επίλυση στους πραγματικούς πολυωνυμικών εξισώσεων, υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς καθώς και εφαρμογές αυτών σε προβλήματα και αλγορίθμους της μη γραμμικής υπολογιστικής γεωμετρίας.

Ας θεωρήσουμε το παρακάτω τμήμα ενός προγράμματος σε C++ το οποίο ορίζει δύο ακεραίους και τους συγκρίνει:

```
int a = 3;
int b = 5;

if ( a > b )  { execute algorithm A; }
if ( a < b )  { execute algorithm B; }
if ( a == b ) { execute algorithm C; }
```

Στόχος μας είναι να μελετήσουμε αλγορίθμους που να μας επιτρέπουν να γράψουμε αντίστοιχα προγράμματα όπου οι μεταβλητές είναι, αντί για ακέραιοι, πραγματικοί αλγεβρικοί αριθμοί και να μελετήσουμε την πολυπλοκότητα των αλγορίθμων αυτών. Για παράδειγμα, θα θέλαμε να έχουμε τη δυνατότητα να γράφουμε προγράμματα όπως:

[1] Σε όλη τη διατριβή, η λέξη *ακριβής* χρησιμοποιείται για την απόδοση του αγγλικού όρου *exact*. Όταν αναφερόμαστε σε *ακριβείς αλγορίθμους* (exact algorithms) ή σε *αριθμητική ακριβείας* (exact arithmetic) ή σε *ακριβείς υπολογισμούς* (exact computations) θα εννοούμε αλγορίθμους ή υπολογισμούς που βασίζονται σε αριθμητική ακεραίων ή ρητών αριθμών απεριόριστης ακρίβειας.

```
root_of a = solve( "x^3-2")[2];
root_of b = solve( "x^5-3")[2];

if ( a > b )  { execute algorithm A; }
if ( a < b )  { execute algorithm B; }
if ( a == b ) { execute algorithm C; }
```

Ο τύπος **root_of** είναι ο τύπος για τους πραγματικούς αλγεβρικούς αριθμούς και έχει αντικαταστήσει τον τύπο για τους ακεραίους (**int**) του προηγούμενου προγράμματος. Αντίστοιχη λειτουργικότητα με την αρχικοποίηση των ακεραίων έχει η συνάρτηση **solve**. Η συνάρτηση δέχεται ως είσοδο ένα πολυώνυμο και επιστρέφει μια λίστα (ή διάνυσμα) από πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του πολυωνύμου. Στο προηγούμενο πρόγραμμα επιλέξαμε (και στις δύο περιπτώσεις) τη δεύτερη μικρότερη ρίζα του αντίστοιχου πολυωνύμου. Οι τρεις τελευταίες γραμμές των προγραμμάτων είναι ακριβώς οι ίδιες. Και στις δύο περιπτώσεις, ανάλογα με τη διάταξη των αριθμών, εκτελείται κάποιος αλγόριθμος.

Ο ορισμός (ή αρχικοποίηση ή κατασκευή) πραγματικών αλγεβρικών αριθμών, που αντιστοιχεί στην επιλύση στους πραγματικούς ενός πολυωνύμου σε μία μεταβλητή με ακέραιους συντελεστές (ακέραιο πολυώνυμο) και η σύγκρισή τους είναι από τους πιο σημαντικούς υπολογισμούς, όπως επίσης και ο υπολογισμός του προσήμου ενός πολυωνύμου όταν αποτιμηθεί πάνω σε έναν αλγεβρικό αριθμό, η επίλυση συστημάτων πολυωνυμικών ανισώσεων σε μία μεταβλητή και οι αριθμητικές πράξεις με ρητούς και έναν πραγματικό αλγεβρικό αριθμό. Επίσης, οι πραγματικοί αλγεβρικοί αριθμοί μπορούν να κατασκευαστούν και κατά ζεύγη, όταν επιλύουμε στους πραγματικούς ένα πολυωνυμικό σύστημα σε δύο μεταβλητές. Έτσι προκύπτει η ανάγκη για υπολογισμούς όπου εμπλέκονται δύο πραγματικοί αλγεβρικοί αριθμοί.

Μια σημαντική παρατήρηση αφορά την πολυπλοκότητα των υπολογισμών. Οι πραγματικοί αλγεβρικοί αριθμοί προκύπτουν ως ρίζες ακέραιων πολυωνύμων, συνεπώς η πολυπλοκότητα των υπολογισμών εξαρτάται από κάποιο μέτρο της πολυπλοκότητας της αναπαράστασης των πολυωνύμων· το βαθμό τους και το μήκος της αναπαράστασης των συντελεστών τους.

Σε ποιούς αλγορίθμους εμφανίζονται οι πραγματικοί αλγεβρικοί αριθμοί; Εμφανίζονται όταν υπάρχουν μη γραμμικοί υπολογισμοί, πολυωνυμικής μορφής, όπως για παράδειγμα στη γεωμετρική σχεδίαση και μοντελοποίηση, στη ρομποτική, στην απαλοιφή ποσοδεικτών σε λογική πρώτης τάξης στο χώρο των πραγματικών αριθμών, στην (πραγματική) επίλυση πολυωνυμικών συστημάτων, καθώς αυτή ανάγεται στην επίλυση ενός πολυωνύμου σε μία μεταβλητή, σε αναδρομικές ακολουθίες πολυωνυμικών υπολογισμών (cascaded computations). Στη μη γραμμική υπολογιστική γεωμετρία, όπου ασχολούμαστε με πολυωνυμικές (αλγεβρικές) καμπύλες και επιφάνειες, οι υπολογισμοί με πραγματικούς αλγεβρικούς αριθμούς έχουν κεντρικό ρόλο. Πρέπει να τονίσουμε ότι οι μη γραμμικότητες δεν προκύπτουν μόνο από μη γραμμικά (γεωμετρικά) αντικείμενα όπως οι αλγεβρικές καμπύλες και επιφάνειες· μπορούν να προκύψουν και από γραμμικά αντικείμενα, όπως οι ευθείες και τα ευθύγραμμα τμήματα. Παραδείγματα τέτοιων προβλημάτων είναι ο υπολογισμός του διαγράμματος Voronoi ευθυγράμμων τμημάτων στο επίπεδο ή ευθειών στο χώρο. Ενθαρρύνουμε τον ενδιαφερόμενο αναγνώστη να ανατρέξει στην προσκεκλημένη ομιλία[2] του 22ου Ευρωπαϊκού Συνεδρίου Υπολογιστικής Γεωμετρίας, που αναφέρεται στη στενή

[2] www-sop.inria.fr/geometrica/team/Monique.Teillaud/talks/EWCG.pdf

σχέση της σύγχρονης υπολογιστικής γεωμετρίας, κυρίως μη γραμμικής, και της γεωμετρικής σχεδίασης με την επίλυση πολυωνύμων και πολυωνυμικών συστημάτων και υπολογισμών με πραγματικούς αλγεβρικούς αριθμούς. Επιπρόσθετα, όλοι οι παραπάνω υπολογισμοί πρέπει να πραγματοποιούνται με ακρίβεια προκειμένου αφενός μεν να αναγνωρίζουμε και να χειριζόμαστε εκφυλισμένες καταστάσεις (degeneracies), όπως για παράδειγμα την ισότητα πραγματικών αλγεβρικών αριθμών, την ύπαρξη πολλαπλών ριζών, την εφαπτομενική τομή καμπυλών και επιφανειών, αφετέρου δε να πιστοποιείται ότι υπολογίζουμε το σωστό αποτέλεσμα.

Οι πραγματικοί αλγεβρικοί αριθμοί μας επιτρέπουν να κάνουμε περισσότερους υπολογισμούς από ό,τι αν δουλεύαμε μόνο με τους ρητούς ή διαφορετικά μας επιτρέπουν να περιγράψουμε περισσότερα προβλήματα. Η σύνδεση των πραγματικών αλγεβρικών αριθμών με τη γεωμετρία έχει τις ρίζες της πολύ βαθιά στο χρόνο. Η μεγάλη μαθηματική και φιλοσοφική σχολή (αν ο διαχωρισμός μεταξύ μαθηματικών και φιλοσοφίας υφίσταται) του Πυθαγόρα του Σάμιου (περίπου 560–480 πΧ) πίστευε ότι, οι ολόκληροι αριθμοί (ακέραιοι) και οι λόγοι τους (ρητοί) μπορούσαν να περιγράψουν οποιαδήποτε γεωμετρική κατασκευή και άρα δεν υπήρχε ανάγκη για άλλους αριθμούς. Ο πυρήνας της φιλοσοφικής τους σκέψης ήταν η θεώρηση ότι οι ολόκληροι αριθμοί κυβερνούν τον κόσμο. Η μεγαλύτερη ανακάλυψη της σχολής ήταν, ίσως το πιο γνωστό μαθηματικό θεώρημα, το πυθαγόρειο θεώρημα. Αυτή ακριβώς η ανακάλυψη οδήγησε στη διάλυση της σχολής. Ο αριθμός που διέλυσε τον πυρήνα της πυθαγόρειας φιλοσοφικής σκέψης ήταν ο $\sqrt{2}$, ο οποίος ονομάζεται *σταθερά του Πυθαγόρα* και μπορεί να κατασκευαστεί (γεωμετρικά) ως η υποτείνουσα ενός ισοσκελούς ορθογωνίου τριγώνου με κάθετες πλευρές μήκους 1. Ο Πυθαγόρας απέδειξε ότι ο $\sqrt{2}$ δεν μπορεί να γραφτεί ως λόγος δύο ολόκληρων (ακεραίων) αριθμών. Συνεπώς, απέδειξε ότι υπάρχουν και άλλοι αριθμοί εκτός από τους ρητούς, γεγονός που ερχόταν σε ευθεία σύγκρουση με τη φιλοσοφική θεώρηση που πρέσβευε. Η απόδειξη αυτή, εκτός από τον Πυθαγόρα, είναι στενά συνδεδεμένη και με έναν άλλο φιλόσοφο που συμμετείχε στη σχολή του, τον Ίππασο τον Μεταπόντιο, ο οποίος γεννήθηκε, μάλλον, γύρω στο 500 πΧ στη Μεγάλη Ελλάδα. Κατά μία εκδοχή ήταν ο Ίππασος που βρήκε την απόδειξη για τον $\sqrt{2}$ κατά τη διάρκεια ενός θαλάσσιου ταξιδιού και τον σκότωσαν φανατικοί πυθαγόριοι πετώντας τον στη θάλασσα. Κατά μια άλλη εκδοχή ο Ίππασος διέδωσε την ύπαρξη του $\sqrt{2}$ εκτός του πυθαγόρειου κοινοβίου, γεγονός το οποίο οδήγησε στη θανάτωσή του, καθώς οι πυθαγόριοι έδιναν όρκο σιωπής κατά την είσοδό τους στη σχολή. Σε κάθε περίπτωση, ο Ίππασος πλήρωσε με τη ζωή του την ύπαρξη και άλλων αριθμών πέρα από τους ρητούς.

Σήμερα, τους αριθμούς που δεν μπορούν να γραφτούν ως ρητοί, δηλαδή ως κλάσμα δύο ακεραίων, τους ονομάζουμε άρρητους (irrational). Υπενθυμίζουμε ότι η ακολουθία των δεκαδικών ψηφίων των άρρητων αριθμών δεν τερματίζει και δεν γίνεται περιοδική. Δεν είναι εύκολο να αποδείξουμε ότι κάποιος αριθμός είναι άρρητος. Για παράδειγμα είναι ακόμα ανοιχτό πρόβλημα το αν ο αριθμός $\pi^{\sqrt{2}}$ είναι άρρητος. Η παρούσα διατριβή δεν ασχολείται με τους άρρητους αριθμούς, αλλά με ένα υποσύνολό τους, τους πραγματικούς αλγεβρικούς αριθμούς[3]. Ωστόσο, προκειμένου να βοηθήσουμε τον Πυθαγόρα στο *δίλημμά* του αφενός θεωρούμε ότι το θεμελιακό αριθμητικό αντικείμενο είναι οι ρητοί αριθμοί και κάνουμε υπολογισμούς μόνο με αυτούς, αφετέρου συνδέουμε τους πραγματικούς αλγεβρικούς αριθμούς με γεωμετρικά προβλήματα. Εφόσον

[3]Το σύνολο των πραγματικών αλγεβρικών αριθμών είναι υποσύνολο του συνόλου των άρρητων αριθμών μόνο αν του αφαιρέσουμε το σύνολο ρητών. Ελπίζουμε ο αναγνώστης να συγχωρέσει αυτή την παράλειψη.

ο $\sqrt{2}$ είναι πραγματικός αλγεβρικός αριθμός μπορούμε και αυτόν να τον χειριστούμε κάνοντας υπολογισμούς μόνο με ρητούς. *Ίσως*, αν ο Πυθαγόρας ήταν γνώστης αυτών των μαθηματικών, η δολοφονία του Ίππασου να είχε αποτραπεί.

Ποιό είναι το σύνολο των πραγματικών αλγεβρικών αριθμών; Θα συμβολίζουμε με $\mathbb{N}$ το σύνολο των φυσικών αριθμών, με $\mathbb{Z}$ το σύνολο των ακεραίων, με $\mathbb{Q}$ το σύνολο των ρητών, με $\mathbb{R}$ το σύνολο των πραγματικών και με $\mathbb{C}$ το σύνολο των μιγαδικών αριθμών. Μπορούμε να διατάξουμε τα σύνολα αυτά, ως εξής:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}_{alg} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Στην προηγούμενη σχέση έχουμε εισάγει ένα ακόμα σύνολο, το $\mathbb{R}_{alg}$, το οποίο είναι το σύνολο των πραγματικών αλγεβρικών αριθμών. Παρατηρούμε ότι δεν είναι όλοι οι πραγματικοί αριθμοί στοιχεία του $\mathbb{R}_{alg}$, καθώς δεν μπορούν όλοι οι πραγματικοί να εκφραστούν ως ρίζα κάποιου πολυωνύμου με ακέραιους συντελεστές. Για παράδειγμα ένας τέτοιος αριθμός είναι ο π. Αυτοί οι αριθμοί ονομάζονται *υπερβατικοί*. Τέτοιοι αριθμοί δεν θα μας απασχολήσουν στην παρούσα διατριβή. Στόχος είναι η ανάλυση και υλοποίηση υπολογισμών με στοιχεία του $\mathbb{R}_{alg}$ και εφαρμογές των υπολογισμών στην υπολογιστική γεωμετρία.

Αντί περιεχομένων

Αλγεβρικοί αλγόριθμοι ονομάζονται οι αλγόριθμοι για αλγεβρικά προβλήματα. Ή διαφορετικά, με τον όρο αλγεβρικοί αλγόριθμοι αναφερόμαστε στην αλγοριθμική προσέγγιση της άλγεβρας [5, 14, 38, 64, 66, 71, 112, 160, 187, 263, 275]. Οι εφαρμογές των αλγεβρικών αλγορίθμων περιλαμβάνουν τη συμβολική επεξεργασία, την αυτοματοποιημένη απόδειξη θεωρημάτων, την κρυπτογραφία, τη ρομποτική, την υπολογιστική γεωμετρία, την υπολογιστική βιολογία, τη σχεδίαση με υπολογιστή, τη γεωμετρική μοντελοποίηση και πολλές άλλες επιστημονικές περιοχές. Μερικά μόνο από τα προβλήματα που απασχολούν την επιστημονική περιοχή των αλγεβρικών αλγορίθμων είναι η αριθμητική με ακέραιους και ρητούς απεριόριστης ακρίβειας, οι υπολογισμοί σε χώρους πηλίκα (modulo ένα στοιχείο του χώρου), οι υπολογισμοί με πίνακες, οι υπολογισμοί με πολυώνυμα μίας και πολλών μεταβλητών, η επίλυση πολυωνύμων και πολυωνυμικών συστημάτων στους πραγματικούς ή/και στους μιγαδικούς, η παραγοντοποίηση ακεραίων και πολυωνύμων, η απαλοιφή ποσοδεικτών σε λογική πρώτης τάξης στους πραγματικούς αριθμούς· και φυσικά αλγόριθμοι και δομές δεδομένων για την αποθήκευση και τον χειρισμό των βασικών αντικειμένων, όπως τα πολυώνυμα, οι πίνακες, τα ιδεώδη και οι πραγματικοί αλγεβρικοί αριθμοί.

Τα σημαντικότερα ανοιχτά προβλήματα στην περιοχή των αλγεβρικών αλγορίθμων, που βασίζονται στην αριθμητική ακριβείας, αφορούν στην κατανόηση της θεωρητικής και πρακτικής πολυπλοκότητάς τους και τη σύγκρισή τους με τους αλγορίθμους της αριθμητικής ανάλυσης. Στόχος της περιοχής είναι να 'ανταγωνιστεί' τους αλγορίθμους που βασίζονται σε αριθμητική κινητής υποδιαστολής και να συμβάλλει σε μια υβρική προσέγγιση που θα στηρίζεται και στις δύο προσεγγίσεις (symbolic-numeric approach). Η παρούσα διδακτορική διατριβή εντάσσεται στο παραπάνω πλαίσιο και το περιεχόμενο και η συνεισφορά της συνοψίζονται ως εξής:

Στο Κεφ. 2 παρουσιάζουμε το απαραίτητο αλγεβρικό υπόβαθρο για την κατανόηση της διατριβής. Παρουσιάζουμε τις πολυπλοκότητες των βασικών υπολογισμών με ακέραια πολυώνυμα μιας μεταβλητής, την έννοια της επιλύουσας (resultant), τις πολυωνυμικές ακολουθίες υπολοίπων και

διάφορους αλγορίθμους για τον υπολογισμό τους. Τέλος, αναφερόμαστε συνοπτικά στην αναπαράσταση πολυωνύμων στη βάση Bernstein. Με την εξαίρεση της Πρότ. 2.36 τα αποτελέσματα του κεφαλαίου δεν είναι πρωτότυπα.

Στο Κεφ. 3 μελετάμε φράγματα στις πραγματικές ρίζες πολυωνύμων και αλγορίθμους για την απομόνωση των πραγματικών ριζών ακέραιων πολυωνύμων σε μία μεταβλητή. Τα πρωτότυπα αποτελέσματα αφορούν τη μελέτη της ποιότητας των φραγμάτων για τις θετικές πραγματικές ρίζες, ένα θεώρημα για τα σύνθετα φράγματα διαχωρισμού, την ενοποίηση και απλοποίηση της θεωρίας για τους αλγορίθμους επίλυσης πολυωνύμου, που βασίζονται στην υποδιαίρεση και τη βελτίωση της πολυπλοκότητας κατά δύο παράγοντες του αλγορίθμου των συνεχών φραγμάτων. Επιπρόσθετα, αποδεικνύουμε ότι το φράγμα πολυπλοκότητας ισχύει και για πολυώνυμα με τετράγωνα και ότι με την ίδια πολυπλοκότητα υπολογίζουμε και την πολλαπλότητα των ριζών.

Στο Κεφ. 4 μελετάμε αλγορίθμους για υπολογισμούς με έναν και δύο πραγματικούς αλγεβρικούς αριθμούς. Όσον αφορά στους υπολογισμούς με έναν αλγεβρικό αριθμό, αν και οι περισσότεροι αλγόριθμοι είναι γνωστοί, η πολυπλοκότητά τους δεν έχει μελετηθεί. Παρουσιάζουμε σε ενιαίο πλαίσιο τους αλγορίθμους για υπολογισμούς με έναν αλγεβρικό αριθμό και την πολυπλκοκότητά τους. Σε κάθε περίπτωση βελτιώνουμε τα φράγματα πολυπλοκότητας κατά δύο ή τρεις παράγοντες. Στη συνέχεια παρουσιάζουμε τις πολυπλοκότητες για τον υπολογισμό πολυωνυμικών ακολουθιών υπολοίπων, πολυωνύμων σε δύο μεταβλητές, δύο αλγόριθμους για την πραγματική επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές και αλγορίθμους για υπολογισμούς με δύο αλγεβρικούς αριθμούς. Όλοι οι αλγόριθμοι είναι καινούργιοι και τα προκύπτοντα φράγματα βελτιώνουν σε κάθε περίπτωση τα ήδη γνωστά.

Στο Κεφ. 5 παρουσιάζουμε αλγορίθμους για την επίλυση πολυωνυμικών εξισώσεων βαθμού ≤ 4 και πολυωνυμικών συστημάτων σε δύο μεταβλητές, όπου τα πολυώνυμα είναι βαθμού ≤ 2 καθώς επίσης και υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς βαθμού ≤ 4. Αποδεικνύουμε ότι όλοι οι παραπάνω υπολογισμοί έχουν πολυπλοκότητα $\mathcal{O}(1)$. Ας σημειωθεί ότι αφενός μεν δεν αναπαριστούμε τις ρίζες των πολυωνύμων με ριζικά αφετέρου δε οι υπολογισμοί εμπεριέχουν μόνο αριθμητική ακεραίων. Το σύνολο των αποτελεσμάτων είναι πρωτότυπο.

Στο Κεφ. 6 παρουσιάζουμε την υλοποίηση των αλγεβρικών αλγορίθμων που παρουσιάστηκαν στα κεφάλαια 3, 4 και 5 και αφορούν την πραγματική επίλυση ακέραιων πολυωνύμων και πολυωνυμικών συστημάτων και τη σύγκριση πραγματικών αλγεβρικών αριθμών. Η υλοποίησή μας είναι σε C++ και αποτελεί μέρος της αλγεβρικής βιβλιοθήκης SYNAPS [4]. Παρουσιάζουμε πειραματικά αποτελέσματα για πολυώνυμα βαθμού ≤ 4 αλλά και για πολυώνυμα βαθμού 1000 και δυαδικού μήκους συντελεστών 8000 bits.

Στο Κεφ. 7 παρουσιάζουμε δύο εφαρμογές των αλγεβρικών μεθόδων σε κατηγορήματα που απαιτούνται από τους αλγορίθμους υπολογισμού της διάταξης ελλειπτικών τόξων στο επίπεδο και στον υπολογισμό του διαγράμματος Voronoi ελλείψεων στο επίπεδο. Η υλοποίηση των αλγορίθμων είναι σε C++ και βασίζεται στην γεωμετρική βιβλιοθήκη CGAL [5]. Όλα τα αποτελέσματα είναι πρωτότυπα.

Στο Κεφ. 8 δοθέντος ενός κυρτού πολυγώνου με ακέραιες κορυφές στο επίπεδο (ακέραιο πολύγωνο), εξετάζουμε αλγορίθμους που μας επιτρέπουν να το διασπάσουμε σε δύο άλλα κυρτά

[4] www-sop.inria.fr/galaad/logiciels/synaps/
[5] www.cgal.org

πολύγωνα τέτοια ώστε το άθροισμά τους κατά Minkowski να είναι το αρχικό πολύγωνο. Κάθε πολυώνυμο σε δύο μεταβλητές αντιστοιχίζεται σε ένα ακέραιο πολύγωνο, το πολύγωνο (πολύτοπο) του Newton. Η διάσπαση του πολυτόπου του Newton είναι αναγκαία συνθήκη προκειμένου το αντίστοιχο πολυώνυμο να παραγοντοποιείται. Βελτιώνουμε τη μέχρι σήμερα γνωστή πολυπλοκότητα και παρουσιάζουμε βέλτιστους αλγορίθμους για την περίπτωση που ένας προσθετέος έχει σταθερό πλήθος ακμών.

ΚΕΦΑΛΑΙΟ 2

Αλγεβρικό υπόβαθρο

Τα μαθηματικά είναι η μουσική της αιτίας.

James Joseph Sylvester

Στα μαθηματικά δεν καταλαβαίνεις πράγματα. Απλά τα συνηθίζεις.

John von Neumann

Περίληψη

Παρουσιάζουμε συνοπτικά τη βασική θεωρία και τους αλγορίθμους που απαιτούνται για την κατανόηση των υπολοίπων κεφαλαίων της διατριβής. Καταρχάς παρουσιάζουμε την δυαδική πολυπλοκότητα των βασικών πράξεων μεταξύ πολυωνύμων. Ορίζουμε την έννοια του μέγιστου κοινού διαιρέτη και της επιλύσουσας δύο πολυωνύμων. Επίσης παρουσιάζουμε τις πολυωνυμικές ακολουθίες υπολοίπων, τη βασική θεωρία και ιδιότητες που τις διέπουν, διάφορους τρόπους κατασκευής τους και τη δυαδική πολυπλοκότητα των βασικών αλγορίθμων που τις εμπεριέχουν. Τέλος, αναφερόμαστε συνοπτικά στην αναπαράσταση πολυωνύμων στη βάση Bernstein.

Με την εξαίρεση της Πρότ. 2.36, η οποία παρουσιάστηκε στην εργασία [97] τα αποτελέσματα του κεφαλαίου δεν είναι πρωτότυπα.

Η πολυπλοκότητα ενός προβλήματος είναι συνάρτηση κάποιου μέτρου των δεδομένων της εισόδου και της εξόδου του. Τα προβλήματα τα οποία θα μας απασχολήσουν έχουν ως είσοδο ακέραιους ή ρητούς αριθμούς ή/και ακέραια ή ρητά πολυώνυμα. Στο μοντέλο υπολογισμού των αλγορίθμων που θα παρουσιάσουμε μπορούμε να αναπαραστήσουμε και να κάνουμε υπολογισμούς με ακεραίους απεριόριστης ακρίβειας, γι' αυτό και οι αλγόριθμοι ονομάζονται ακριβείς αλγόριθμοι (exact algorithms). Λόγω του γεγονότος ότι τα αντικείμενά μας δεν

έχουν καθορισμένη διάσταση, οι βασικές πράξεις με αυτά, όπως για παράδειγμα η πρόσθεση και ο πολλαπλασιασμός, δεν έχουν σταθερή πολυπλοκότητα αλλά εξαρτώμενη από το μήκος της αναπαράστασής τους.

Θα παρουσιάσουμε την πολυπλοκότητα των βασικών πράξεων ακεραίων αριθμών. Ακολούθως θα παρουσιάσουμε τη βασική θεωρία των πολυωνύμων και αλγορίθμους πάνω σε πολυώνυμα που θα μας χρειαστούν στα επόμενα κεφάλαια.

Χρησιμοποιούμε το συμβολισμό $\mathcal{O}$ για την αριθμητική και τον συμβολισμό $\mathcal{O}_B$ για την δυαδική (Boolean) πολυπλοκότητα. Ο συμβολισμός $\tilde{\mathcal{O}}$ και $\tilde{\mathcal{O}}_B$ αγνοεί τους λογαριθμικούς παράγοντες. Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία [57, 122].

2.1 Περί των αριθμών

Το βασικό αντικείμενο σε όλους τους αλγορίθμους είναι οι ακέραιοι αριθμοί, για τους οποίους υποθέτουμε ότι δίδονται σε δυαδική αναπαράσταση, δηλαδή αναπαρίστανται ως μία λίστα από 0 και 1. Ένας ρητός αριθμός αναπαρίσταται με δύο συνεχόμενες λίστες που αντιστοιχούν στον αριθμητή και στον παρανομαστή του, οι οποίες χωρίζονται από μία κενή θέση. Για έναν ακέραιο $a \in \mathbb{Z}$ ορίζουμε ως μήκος της δυαδικής αναπαράστασής του ή *δυαδικό μήκος* (bit size) την ποσότητα $\mathcal{L}(a) = 1 + \lceil \lg(|a|) + 1 \rceil$, όπου το $+1$ χρειάζεται για την αναπαράσταση του προσήμου. Αν $a = \frac{b}{c} \in \mathbb{Q}$ τότε $\mathcal{L}(a) = \max\{\mathcal{L}(b), \mathcal{L}(c)\}$. Με $|a|$ συμβολίζουμε το μέτρο του a, και αν $a \in \mathbb{Z}$ ή $a \in \mathbb{Q}$, τότε μέτρο είναι η απόλυτη τιμή του.

Θεώρημα 2.1

Έστω $a, b \in \mathbb{Z}$ τέτοιοι ώστε $\mathcal{L}(a) = \mathcal{L}(b) = \tau$. Η πολυπλοκότητα των πράξεων της πρόσθεσης και της αφαίρεσης ($a + b, a - b$) είναι $\Theta(\tau)$.

Αν $a, b \in \mathbb{Z}$ τότε θα συμβολίζουμε με $\mathsf{quo}(a, b)$ και $\mathsf{rem}(a, b)$ το πηλίκο και το υπόλοιπο, αντίστοιχα, της ακέραιας διαίρεσης των a και b.

Θεώρημα 2.2

Έστω $a, b \in \mathbb{Z}$ τέτοιοι ώστε $\mathcal{L}(a) = \mathcal{L}(b) = \tau$. Η πολυπλοκότητα των πράξεων του πολλαπλασιασμού, $a \cdot b$, της διαίρεσης με υπόλοιπο, $\mathsf{quo}(a, b) \wedge \mathsf{rem}(a, b)$, του τετραγωνισμού, a^2, και του αντιστρόφου, a^{-1}, είναι $\tilde{\mathcal{O}}_B(\mathsf{M}(\tau))$.

Σε ό,τι θα ακολουθήσει υποθέτουμε ότι γρήγοροι αλγόριθμοι πολλαπλασιασμού είναι διαθέσιμοι, για παράδειγμα αλγόριθμοι που βασίζονται στο Γρήγορο Μετασχηματισμό Fourier (Fast Fourier Transform, FFT). Συνεπώς, η πολυπλοκότητα του πολλαπλασιασμού και της διαίρεσης ακεραίων αριθμών είναι $\mathsf{M}(\tau) = \mathcal{O}_B(\tau \lg^c \tau) = \tilde{\mathcal{O}}_B(\tau)$. Για περισσότερες πληροφορίες καθώς και για τις αποδείξεις των θεωρημάτων ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία, δείτε για παράδειγμα [160, 263, 275].

2.2 Περί των πολυωνύμων

Σε ό,τι θα ακολουθήσει θα συμβολίζουμε με $\mathcal{K}$ ένα αλγεβρικά κλειστό σώμα, δηλαδή κάποια αλγεβρική δομή τέτοια ώστε όλα τα πολυώνυμα σε μία μεταβλητή με συντελεστές από το $\mathcal{K}$ να έχουν λύσεις στο $\mathcal{K}$. Με $\mathcal{R}$ θα συμβολίζουμε έναν υποδακτύλιο με μονάδα του $\mathcal{K}$ και με $\mathcal{F}$ το σώμα πηλίκων του $\mathcal{R}$. Ένα παράδειγμα μιας τέτοιας ιεραρχίας αλγεβρικών δομών είναι $\mathcal{R} = \mathbb{Z}$, $\mathcal{F} = \mathbb{Q}$ και $\mathcal{K} = \mathbb{C}$ [108, 258].

Αν $\mathcal{S}$ είναι κάποια αλγεβρική δομή τότε θα συμβολίζουμε με $\mathcal{S}[X_1, \ldots, X_k]$ το χώρο των πολυωνύμων με k μεταβλητές με συντελεστές από το $\mathcal{S}$. Το χώρο των πολυωνύμων πολλών μεταβλητών τα οποία θέλουμε να τα δούμε ως μιας μεταβλητής με συντελεστές πολυώνυμα σε πολλές (τις υπόλοιπες) μεταβλητές τον συμβολίζουμε ως $(\mathcal{S}[X_1, \ldots, X_{k-1}])[X_k]$.

Έστω ένα πολυώνυμο μιας μεταβλητής $f \in \mathcal{S}[X]$:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \tag{2.1}$$

αν $a_n \neq 0$ τότε ο βαθμός του πολυωνύμου είναι n, $\deg(f) = n$, και ο μεγιστοβάθμιος όρος του είναι $\mathrm{lead}(f) = a_n$. Όταν $\mathrm{lead}(f) = 1$ το πολυώνυμο ονομάζεται *μονικό* (monic). Ορίζουμε ως $f = 0$ το μηδενικό πολυώνυμο και εξ ορισμού $\deg(0) = -\infty$ και $\mathrm{lead}(0) = 1$.

Αν $f \in \mathcal{S}[X_1, \ldots, X_k]$ τότε με $\deg(f)$ δηλώνουμε το συνολικό βαθμό (total degree), ενώ με $\deg_{X_k}(f)$ συμβολίζουμε το βαθμό του f αν θεωρήσουμε ότι $f \in (\mathcal{S}[X_1, \ldots, X_{k-1}])[X_k]$.

Υποθέτουμε ότι $f \in \mathbb{C}[X]$ και ορίζουμε τις ακόλουθες μετρικές

$$\|f\|_\infty = \max\{|a_n|, \ldots, |a_1|, |a_0|\} \tag{2.2}$$

$$\|f\|_2 = \sqrt{|a_n|^2 + \cdots + |a_1|^2 + |a_0|^2} \tag{2.3}$$

για τις οποίες ισχύει η ανισότητα

$$\|f\|_\infty < \|f\|_2 < \sqrt{n+1}\,\|f\|_\infty \tag{2.4}$$

Για μια πληρέστερη και πιο εκτενή εισαγωγή στη θεωρία των πολυωνύμων ο αναγνώστης μπορεί να ανατρέξει, για παράδειγμα στους Cox et al. [59], Fraleigh [108], Prasolov [218], van der Waerden [258], Zippel [276].

Βασικές πράξεις

Θα μας απασχολήσουν κυρίως πολυώνυμα στο $\mathbb{Z}[X]$. Προκειμένου να αναπαραστήσουμε τα πολυώνυμα χρησιμοποιούμε την πυκνή αναπαράσταση, δηλαδή υποθέτουμε ένα διάνυσμα που περιέχει (σε δυαδική αναπαράσταση) τους συντελεστές του πολυωνύμου και ότι η πρόσβαση σε κάποιο συντελεστή έχει πολυπλοκότητα $\mathcal{O}(1)$. Όταν $f \in \mathbb{Z}[X]$ θα συμβολίζουμε με $\mathcal{L}(f)$ το μέγιστο δυαδικό μήκος των συντελεστών του f, δηλαδή $\mathcal{L}(f) = \lg(\|f\|_\infty)$. Επίσης, με τον όρο δυαδικό μήκος ενός πολυωνύμου θα υπονοούμε το μέγιστο δυαδικό μήκος των συντελεστών του.

Θεωρούμε $f, g \in \mathbb{Z}[X]$

$$\begin{aligned} f &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \\ g &= b_m X^m + b_{n-1} X^{m-1} + \cdots + b_1 X + b_0 \end{aligned} \tag{2.5}$$

τέτοια ώστε $\deg(f) = n \geq m = \deg(g)$, $\mathcal{L}(f) \leq \tau$, $\mathcal{L}(g) \leq \tau$ και έστω $c \in \mathbb{Z}$, $\mathcal{L}(c) = \sigma$.

Θα παρουσιάσουμε συνοπτικά την πολυπλοκότητα μερικών βασικών πράξεων. Ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία για περισσότερες λεπτομέρειες [25, 160, 212, 263, 275, 276].

Πρόσθεση και αφαίρεση

Το $h \in \mathbb{Z}[X]$, όπου $h = f \pm g$, υπολογίζεται με πολυπλοκότητα $\mathcal{O}_B(n\tau)$. Ισχύει $\deg(h) \leq n$ (ισότητα στην περίπτωση της πρόσθεσης) και $\mathcal{L}(h) \leq \tau + 1$.

Πολλαπλασιασμός

Το $h \in \mathbb{Z}[X]$, όπου $h = f \cdot g$, υπολογίζεται με πολυπλοκότητα $\mathcal{O}_B(\mathsf{M}(n, \tau))$. Ισχύει $\deg(h) = mn$ και $\mathcal{L}(h) \leq 2\tau + \lg n$. Όπως και στην περίπτωση του πολλαπλασιασμού ακεραίων θα υποθέσουμε γρήγορους αλγορίθμους πολλαπλασιασμού πολυωνύμων βασισμένους στο γρήγορο μετασχηματισμό Fourier, οπότε $\mathcal{O}_B(\mathsf{M}(n, \tau)) = \widetilde{\mathcal{O}}_B(n\tau)$ [212, 240].

Απεικονίσεις-μετασχηματισμοί

- Αντιστροφή: $h = \mathcal{R}(f)(X) := X^n f(\frac{1}{X})$

  Η πολυπλοκότητα του μετασχηματισμού είναι $\mathcal{O}(n)$ ή $\mathcal{O}_B(n\tau)$. Ωστόσο, με κατάλληλη αναπαράσταση του πολυωνύμου μπορούμε να επιτύχουμε πολυπλοκότητα $\mathcal{O}(1)$. Επιπρόσθετα $\deg(h) = n$ και $\mathcal{L}(h) = \tau$. Θεωρούμε ότι $a_0 \neq 0$.

- Μετατόπιση: $h = \mathcal{T}_c(f)(X) := f(X + c)$

  Η πολυπλοκότητα του μετασχηματισμού είναι $\mathcal{O}_B(\mathsf{M}\left(n^2 \lg n + n\tau + n^2\sigma\right))$ ή παραλείποντας τους (πολυ-) λογαριθμικούς παράγοντες $\widetilde{\mathcal{O}}_B(n^2 \lg n + n\tau + n^2\sigma)$ [262]. Επιπρόσθετα $\deg(h) = n$ και $\mathcal{L}(h) = \mathcal{O}(\tau + n\sigma)$.

  Η μετατόπιση είναι από τους πιο σημαντικούς μετασχηματισμούς. Οι γρήγοροι αλγόριθμοι για αυτή την πράξη στην βιβλιογραφία αναφέρονται και με τον όρο *fast Taylor shifts*.

- Ομοθεσία: $h = \mathcal{H}_c(f)(X) := f(cX)$ και $h = \mathcal{H}'_c(f)(X) := c^n f(\frac{X}{c}) = \mathcal{R}(\mathcal{H}_c(\mathcal{R}(f)))(X)$

  Η πολυπλοκότητα του μετασχηματισμού είναι $\mathcal{O}_B(n\,\mathsf{M}(\max\{\tau, n\sigma\}))$ ή $\widetilde{\mathcal{O}}_B(n\,\max\{\tau, n\sigma\})$. Επιπρόσθετα $\deg(h) = n$ και $\mathcal{L}(h) = \mathcal{O}(\tau + n\sigma)$.

- Παράγωγος: Συμβολίζουμε με $f^{(k)}$ την k παράγωγο του f. Η αποτίμηση όλων των παραγώγων πάνω σε κάποιο αριθμό c έχει την ίδια πολυπλοκότητα με τη μετατόπιση. Πολλές φορές μας ενδιαφέρει η αποτίμηση των κανονικοποιημένων παραγώνων, $f^{(k)}(X)/k!$ (normalized derivatives), πράξη η οποία είναι (σχεδόν) ισοδύναμη με την μετατόπιση, καθώς εμφανίζονται στην ανάπτυξη κατά Taylor του $f(x + c)$ [25, 212, 243, 262].

Αποτίμηση

Ο ομομορφισμός εκτίμησης $\phi_c : \mathbb{Z}[X] \to \mathbb{Z}$, όπου $f \mapsto f(c)$, για κάθε $f \in \mathbb{Z}[X]$, θα ονομάζεται *αποτίμηση* (του f) πάνω στο c. Ο υπολογισμός της αποτίμησης $f(c)$, με τη βοήθεια του σχήματος Horner έχει πολυπλοκότητα $\mathcal{O}_B(n\,\mathsf{M}(\max\{\tau, n\sigma\}))$ και $\mathcal{L}(f(c)) \leq \tau + n\sigma + \lg n$. Ο υπολογισμός της αποτίμησης του f πάνω σε ένα σύνολο από n διαφορετικούς ακεραίους, $c_1, \ldots, c_n$, όπου $\mathcal{L}(c_i) \leq \sigma$, έχει πολυπλοκότητα $\mathcal{O}_B(n\,\lg^2 n\,\mathsf{M}(\max\{\tau, n\sigma\}))$ ή $\widetilde{\mathcal{O}}_B(n \max\{\tau, n\sigma\})$ [25, 263, 275] και βασίζεται στην τεχνική 'διαίρει και βασίλευε'. Επίσης, την ίδια πολυπλοκότητα έχει ο υπολογισμός της αποτίμησης όλων των παραγώγων του f πάνω στο c, δηλαδή $\widetilde{\mathcal{O}}_B(n \max\{\tau, n\sigma\})$ [25, 212, 243, 262].

Διαίρεση

Αν οι συντελεστές των πολυωνύμων ανήκουν σε κάποιο σώμα τότε μπορούμε να ορίσουμε και τη διαίρεση των πολυωνύμων:

Θεώρημα 2.3 (Διαίρεση πολυωνύμων)
Έστω $f, g \in \mathcal{F}[X]$ και $g \neq 0$. Υπάρχουν μοναδικά πολυώνυμα $Q, R \in \mathcal{F}[X]$ τέτοια ώστε

$$f = gQ + R$$

και $\deg(R) < \deg(g)$. Το Q, αντίστοιχα R, ονομάζεται πηλίκο, αντίστοιχα υπόλοιπο και συμβολίζεται με $\mathsf{quo}(f, g)$, αντίστοιχα $\mathsf{rem}(f, g)$.

Ωστόσο, αν οι συντελεστές δεν ανήκουν σε σώμα, π.χ $f, g \in \mathbb{Z}[X]$, τότε η διαίρεση δεν μπορεί να οριστεί. Προκειμένου να οριστεί η διαίρεση για κάθε αντιμεταθετικό δακτύλιο ο Jacobi [138] εισήγαγε την έννοια της ψευδο-διαίρεσης.

Θεώρημα 2.4 (Ψευδο-διαίρεση πολυωνύμων)
Έστω $f, g \in \mathcal{R}[X]$. Υπάρχουν μοναδικά πολυώνυμα $Q, R \in \mathcal{R}[X]$ τέτοια ώστε

$$\mathsf{lead}(g)^{\delta-1} f = gQ + R$$

και $\deg(R) < \deg(g)$, όπου $\delta = \max\{1, \deg(f) - \deg(g)\}$. Το Q, αντίστοιχα R, ονομάζεται ψευδο-πηλίκο, αντίστοιχα ψευδο-υπόλοιπο, και συμβολίζεται με $\mathsf{pquo}(f, g)$, αντίστοιχα $\mathsf{prem}(f, g)$.

Η πολυπλοκότητα της ψευδο-διαίρεσης είναι $\mathcal{O}_B(m\,\mathsf{M}(n\tau))$ ή $\widetilde{\mathcal{O}}_B(m\,n\,\tau)$ και $\mathcal{L}(\mathsf{prem}(f, g)) = \mathcal{O}(n\,\tau)$, $\mathcal{L}(\mathsf{pquo}(f, g)) = \mathcal{O}(n\,\tau)$ [25, 263, 275].

Θα λέμε ότι το $g \in \mathcal{R}[X]$ διαιρεί ακριβώς το $f \in \mathcal{R}[X]$ αν $\mathsf{rem}(f, g) = 0$ ή $\mathsf{prem}(f, g) = 0$. Για το δυαδικό μήκος των διαιρετών ενός πολυωνύμου ισχύει το φράγμα του Mignotte [188, 189]. Πιο συγκεκριμένα, αν $f = g \cdot Q$ και $f, g, Q \in \mathbb{Z}[X]$ τότε $\mathcal{L}(Q) = \mathcal{O}(n\,\mathcal{L}(f))$ και το ίδιο ισχύει για το g.

Μέγιστος κοινός διαιρέτης

Η αμέσως επόμενη πράξη, η οποία είναι πολύ μεγάλης σημασίας, είναι ο υπολογισμός του μέγιστου κοινού διαιρέτη (ΜΚΔ) δύο πολυωνύμων. Ο ΜΚΔ δύο πολυωνύμων είναι το πολυώνυμο που διαιρεί ακριβώς τόσο τα δύο πολυώνυμα όσο και κάθε άλλο πολυώνυμο που τα διαιρεί ακριβώς. Αν $\mathcal{R}$ είναι μια περιοχή μοναδικής ανάλυσης (UFD, Unique Factorization Domain), για παράδειγμα αν $\mathcal{R} = \mathbb{Z}$ ή $\mathcal{R} = \mathbb{Z}[Y]$, τότε το $\mathcal{R}[X]$ είναι επίσης UFD [108, 258]. Κατά συνέπεια, μπορούμε να ορίσουμε τον μέγιστο κοινό διαιρέτη (ΜΚΔ) δύο πολυωνύμων $f, g \in \mathcal{R}[X]$, τον οποίο συμβολίζουμε ως $\gcd(f, g)$.

Ο ΜΚΔ είναι εξέχουσας σημασίας καθώς επιτρέπει, πέρα των άλλων, να δώσουμε απαντήσεις σε προβλήματα όπως αυτό της εύρεσης των διαφορετικών ριζών ενός πολυωνύμου ή όπως του υπολογισμού των κοινών ριζών δύο πολυωνύμων. Πιο συγκεκριμένα ισχύουν τα ακόλουθα:

- Ο αριθμός των κοινών ριζών των $f, g \in \mathcal{R}[X]$ είναι $\deg(\gcd(f, g))$.
- Ο αριθμός των διαφορετικών ριζών του $f \in \mathcal{R}[X]$ είναι $\deg(f) - \deg(\gcd(f, f'))$.

Ο υπολογισμός του μέγιστου κοινού διαιρέτη έχει πολυπλοκότητα σχεδόν όσο και η ψευδοδιαίρεση, δηλαδή $\widetilde{\mathcal{O}}_B(n\,m\,\tau)$ και $\mathcal{L}(\gcd(f, g)) = \mathcal{O}(n\,\tau)$. Λόγω της πολύ μεγάλης σημασίας αυτού του υπολογισμού θα επανέλθουμε σε επόμενες παραγράφους.

Επιλύουσα δύο πολυωνύμων

Ένα από τα πιο βασικά εργαλεία στους αλγεβρικούς αλγορίθμους, και όχι μόνο, είναι η επιλύουσα (resultant). Η επιλύουσα είναι στενά συνδεδεμένη τόσο με τη θεωρία της απαλοιφής (elimination), γι' αυτό ονομάζεται και *απαλοίφουσα* (eliminant), όσο και με τον υπολογισμό του ΜΚΔ και την εύρεση μιγαδικών ριζών. Για περισσότερες λεπτομέρειες σχετικά με την απαλοίφουσα και για τις αποδείξεις των θεωρημάτων που παραλείπουμε ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [5, 14, 38, 59, 66, 114, 160, 178, 187, 190, 251, 263, 275, 276].

Μπορούμε να διατυπώσουμε το ακόλουθο θεώρημα [114, 249, 251]:

Θεώρημα 2.5 (Επιλύουσα)

Θεωρούμε δύο πολυώνυμα $f, g \in \mathcal{K}[X]$ όπως στην Εξ. (2.5) τέτοια ώστε $a_n\, b_m \neq 0$. Υπάρχει ένα μοναδικό, εκτός από το πρόσημο, ανάγωγο πολυώνυμο $\mathtt{res}(f, g) \in \mathbb{Z}[a_n, \ldots, a_1, a_0, b_m, \ldots, b_1, b_0]$ το οποίο είναι μηδέν όταν τα $f(X)$ και $g(X)$ έχουν κάποιου κοινό παράγοντα. Επιπρόσθετα, το $\mathtt{res}(f, g)$ είναι ομογενές και $\deg(\mathtt{res}(f, g)) = \deg(f) + \deg(g) = m + n$.

Το πολυώνυμο αυτό ονομάζεται επιλύουσα (resultant).

Ο ορισμός και η ύπαρξη της επιλύουσας μπορεί να επεκταθεί και σε συστήματα πολυωνύμων πολλών μεταβλητών, δείτε για παράδειγμα [60, 114, 251]. Στη γενική περίπτωση η επιλύουσα είναι η 'ελάχιστη' συνθήκη επιλυσιμότητας (minimum condition of solvability) πάνω στους συντελεστές. Δηλαδή είναι η *ελάχιστη*, ικανή και αναγκαία, συνθήκη, πάνω στους συντελεστές, για την ύπαρξη μιγαδικών λύσεων ενός συστήματος $\ell + 1$ πολυωνυμικών εξισώσεων σε ℓ μεταβλητές. Στην παρούσα διατριβή δεν θα μας απασχολήσουν προβλήματα όπου $\ell > 1$, εκτός από την Εν. 7.3 όπου θα χρησιμοποιήσουμε την επιλύουσα προκειμένου να απαλείψουμε κάποιες μεταβλητές.

Στην περίπτωση πολυωνύμων σε μία μεταβλητή μπορούμε να εκφράσουμε την επιλύουσα δύο πολυωνύμων ως την ορίζουσα ενός πίνακα, του πίνακα Sylvester. Αν τα πολυώνυμα είναι πολλών μεταβλητών τότε δεν γνωρίζουμε έναν τέτοιο πίνακα στη γενική περίπτωση, αν και υπάρχουν αποτελέσματα για την περίπτωση τριών εξισώσεων και δύο μεταβλητών [154] και άλλων ειδικών περιπτώσεων [72, 73].

Ορισμός 2.6 (Πίνακας Sylvester). *Έστω* $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{m} b_i X^i \in \mathcal{K}[X]$. *Ο πίνακας Sylvester των* f *και* g, $\mathtt{Syl}(f,g)$, *είναι ο παρακάτω πίνακας διαστάσεων* $(m+n)\times(m+n)$

$$\mathtt{Syl}(f,g) := \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_m & b_{m-1} & \dots & b_0 \end{pmatrix} \begin{matrix} X^{m-1}f \\ X^{m-2}f \\ \vdots \\ X^0 f \\ X^{n-1}g \\ X^{n-2}g \\ \vdots \\ X^0 g \end{matrix}$$

όπου υπάρχουν m *γραμμές με τους συντελεστές* a_i *του* f, n *γραμμές με τους συντελεστές* b_i *του* g *και οι άδειες θέσεις περιέχουν μηδενικά.*

Θεώρημα 2.7 (Επιλύουσα δύο πολυωνύμων)

Αν θεωρήσουμε τους συντελεστές των f *και* g *ως παραμέτρους, με την προϋπόθεση ότι* $a_n b_m \neq 0$, *τότε, για οποιαδήποτε τιμή των παραμέτρων, η επιλύουσα των* f *και* g *ως προς* X *ισούται με την ορίζουσα του πίνακα Sylvester,*

$$\mathtt{res}(f,g) = \det(\mathtt{Syl}(f,g))$$

Η επιλύουσα συμβολίζεται ως $\mathtt{res}_X(f,g)$ όταν τα f και g είναι πολυώνυμα πολλών μεταβλητών, π.χ $f, g \in \mathcal{K}[Y_1, \dots, Y_k, X]$, και θέλουμε να δηλώσουμε ότι αναφερόμαστε στην επιλύουσά τους θεωρώντας τα πολυώνυμα μιας μεταβλητής ως προς X, δηλαδή $f, g \in (\mathcal{K}[Y_1, \dots, Y_k])[X]$.

Μπορούμε επίσης να διατυπώσουμε το επόμενο θεώρημα:

Θεώρημα 2.8

Έστω $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{m} b_i X^i$, $f, g \in \mathcal{K}[X]$. *Τα επόμενα είναι ισοδύναμα:*

1. *Τα* f *και* g *έχουν κάποια κοινή ρίζα στο* $\mathcal{K}$.
2. $\deg(\gcd(f,g)) = k > 0$.
3. *Υπάρχουν* $A, B \in \mathcal{K}[X]$, *τέτοια ώστε* $\deg(A) < m-k$ *και* $\deg(B) < n-k$, *από τη σχέση Bézout, τέτοια ώστε να μην είναι και τα δύο μηδέν και* $A\,f + B\,g = 0$.
4. $\mathtt{res}(f,g) = \det(\mathtt{Syl}(f,g)) = 0$

Παράδειγμα 2.9. *Έστω*

$$\begin{aligned} f &= a_2X^2 + a_1X + a_0 \\ g &= b_2X^2 + b_1X + b_0 \end{aligned}$$

Ο πίνακας Sylvester των f και g είναι

$$\mathtt{Syl}(f,g) = \begin{bmatrix} a_2 & a_1 & a_0 & 0 \\ 0 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 \\ 0 & b_2 & b_1 & b_0 \end{bmatrix}$$

και η επιλύουσα είναι

$$\mathtt{res}(f,g) = a_2^2b_0^2 + a_2b_1^2a_0 - a_2b_1a_1b_0 - 2\,a_2b_2b_0a_0 + b_2a_1^2b_0 - b_2a_1b_1a_0 + b_2^2a_0^2$$

Παρατηρούμε ότι $\deg(\mathtt{res}(f,g)) = \deg(f) + \deg(g) = 2 + 2 = 4$. *Η επιλύουσα είναι η βέλτιστη συνθήκη για την επιλυσιμότητα και συνεπώς ο συνολικός βαθμός του* $\mathtt{res}(f,g) \in \mathbb{Z}[a_2, a_1, a_0, b_2, b_1, b_0]$, *ο οποίος είναι 4, είναι βέλτιστος. Ή διαφορετικά, στη γενική περίπτωση, εκτός από την επιλύσουσα δεν υπάρχει άλλο πολυώνυμο ως προς τους συντελεστές των f και g, με συνολικό βαθμό ≤ 4, ο μηδενισμός του οποίου να μας εξασφαλίζει την ύπαρξη κοινών λύσεων των f και g.*

Επίσης, παρατηρούμε ότι η επιλύσουσα είναι ένα εκέραιο πολυώνυμο ως προς τους συντελεστές των f και g και δεν περιέχει την μεταβλητή X. Δηλαδή η επιλύουσα (απαλοίφουσα) έχει απαλείψει από το σύστημα $f = g = 0$ την μεταβλητή X.

Παρουσιάζουμε μερικές ιδιότητες της επιλύουσας.

Λήμμα 2.10. *Έστω $f, g, h \in \mathcal{K}[X]$ τέτοια ώστε $\deg(f) = n$, $\deg(g) = m$ και $\alpha, \beta \in \mathcal{K}$.*

1. $\mathtt{res}(\alpha, f) = \alpha^n$.
2. $\mathtt{res}(X - \alpha, f) = f(\alpha)$.
3. $\mathtt{res}(f,g) = (-1)^{mn}\, res(g,f)$.
4. $\mathtt{res}(\alpha f, g) = \alpha^n\, \mathtt{res}(f,g)$.
5. $\mathtt{res}(f \cdot h, g) = \mathtt{res}(f,g) \cdot \mathtt{res}(h,g)$.
6. *Αν $f = gQ + R$ και $\deg(R) = r$, $m \geq n > r$, τότε*

$$\mathtt{res}(f,g) = (-1)^{n(m-r)}\, a_n^{m-r}\, \mathtt{res}(R,g) = (-1)^{mn}\, a_n^{m-r}\, \mathtt{res}(g,R)$$

Το προηγούμενο λήμμα οδηγεί στον ακόλουθο χαρακτηρισμό της επιλύουσας:

Θεώρημα 2.11

Έστω $f, g \in \mathcal{R}[x]$, όπως στην Εξ. (2.5), με ρίζες $\alpha_1, \ldots, \alpha_n$ και $\beta_1 \ldots, \beta_m \in \mathcal{K}$. Ισχύουν τα ακόλουθα:

$$\mathtt{res}(f,g) \;=\; a_n^m\, b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn}\, b_m^n \prod_{i=1}^{m} f(\beta_i)$$

Ο πίνακας Bézout

Στην περίπτωση δύο πολυωνύμων σε μία μεταβλητή υπάρχει και άλλος τρόπος να υπολογίσουμε την επιλύουσα ως ορίζουσα κάποιου πίνακα. Η κατασκευή βασίζεται στον πίνακα Bézout των f και g και οφείλεται στους Bézout και Cayley.

Δοθέντων δύο πολυωνύμων f και g, όπως στην (2.5), ο πίνακας Bézout [14, 187, 190, 276] των f και g είναι ο συμμετρικός πίνακας

$$\mathtt{Bz}(f,g) = \begin{pmatrix} c_{0,0} & \ldots & c_{0,n-1} \\ \vdots & & \vdots \\ c_{n-1,0} & \ldots & c_{n-1,n-1} \end{pmatrix} \tag{2.6}$$

όπου τα $c_{i,j}$ ορίζονται από την έκφραση Cayley

$$\frac{f(X)\,g(Y) - f(Y)\,g(X)}{X - Y} = \sum_{i,j=0}^{n-1} c_{i,j}\, X^i\, Y^j.$$

Ο πίνακας Bézout είναι στενά συνδεδεμένος με τον πίνακα Sylvester. Η ορίζουσα του πίνακα Bézout είναι η επιλύουσα των f και g. Δηλαδή

$$\mathtt{res}(f,g) = \det(\mathtt{Bz}(f,g)).$$

Η διάσταση του πίνακα Bézout είναι $n \times n$ όπου $n = \max\{\deg(f), \deg(g)\}$ και είναι μικρότερη από αυτή του πίνακα Sylvester. Επίσης, μπορούμε να υπολογίσουμε τον πίνακα Bézout και στην περίπτωση που έχουμε $\ell + 1$ πολυώνυμα σε ℓ μεταβλητές. Σε αυτή την περίπτωση, η ορίζουσα του πίνακα μας δίνει κάποιο πολλαπλάσιο της επιλύουσας του συστήματος. Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [20, 21, 86].

Διακρίνουσα

Στενά συνδεδεμένη με την έννοια της επιλύουσας είναι η έννοια της διακρίνουσας.

Ορισμός 2.12 (Διακρίνουσα). *Έστω $f = \sum_{i=0}^{n} a_i X^i \in \mathcal{R}[X]$, $n \geq 2$ και $\gamma_1, \ldots, \gamma_n \in \mathcal{K}$ οι ρίζες του. Ορίζουμε ως διακρίνουσα (discriminant) του A την πόσοτητα*

$$\mathsf{disc}(f) := a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\gamma_i - \gamma_j)^2$$

Παράδειγμα 2.13. *Αν* $f = a\,x^2 + b\,x + c$ *τότε* $\mathsf{disc}(f) = b^2 - 4\,a\,c$.

Ο ορισμός της διακρίνουσας δεν παρέχει κάποιον τρόπο υπολογισμού της, κάτι που επιτυγχάνεται με το ακόλουθο θεώρημα από το οποίο επίσης προκύπτει ότι $\mathsf{disc}(f) \in \mathcal{R}[a_n, \ldots, a_1, a_0]$.

Θεώρημα 2.14
Έστω $f = \sum_{i=0}^{n} a_i X^i \in \mathcal{R}[X]$, *τότε*

$$\mathtt{res}(f, f') = \pm\, a_n\, \mathsf{disc}(f) = (-1)^{\frac{n(n-1)}{2}}\, a_n\, \mathsf{disc}(f)$$

Παρατηρούμε ότι ο ο ορισμός της διακρίνουσας δεν απαιτεί την ύπαρξη (μόνο) διαφορετικών ριζών. Κατά συνέπεια $\mathsf{disc}(f) = 0$ αν και μόνο αν το f έχει πολλαπλές ρίζες ή ισοδύναμα $\mathtt{res}(f, f') = 0$ αν και μόνο αν το f έχει πολλαπλές ρίζες. Αν $f \in \mathbb{Z}[X]$ και δεν έχει πολλαπλές ρίζες τότε $\mathsf{disc}(f) \geq 1$. Ένα άνω φράγμα στη διακρίνουσα μας παρέχει το επόμενο θεώρημα, όπου $\mathcal{M}(f)$ είναι το μέτρο Mahler του f (Ορ. 3.2), το οποίο θα ορίσουμε στο επόμενο κεφάλαιο.

Θεώρημα 2.15
Αν $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ *με* $\deg(f) = n$ *τότε*

$$|\mathsf{disc}(f)| \leq n^n\, \mathcal{M}(f)^{2(n-1)} \leq n^n\, \|f\|_2^{2(n-1)}$$

2.3 Πολυωνυμικές ακολουθίες υπολοίπων

Ας υποθέσουμε ότι $\mathcal{R}$ είναι μια περιοχή μοναδικής ανάλυσης, π.χ $\mathcal{R} = \mathbb{Z}$ ή $\mathcal{R} = \mathbb{Z}[Y]$. Έστω $A, B \in \mathcal{R}[X]$ τέτοια ώστε

$$\begin{array}{rcl} A(X) & = & a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0 \\ B(X) & = & b_q X^q + b_{q-1} X^{q-1} + \cdots + b_1 X + b_0 \end{array} \tag{2.7}$$

όπου $\deg(A) = p \geq q = \deg(B) > 0$. Αν $\mathcal{R} = \mathbb{Z}$ τότε θεωρούμε ότι $\mathcal{L}(A), \mathcal{L}(B) \leq \tau$.

Επιστρέφουμε στο πρόβλημα του υπολογισμού του ΜΚΔ δύο πολυωνύμων. Προκειμένου να υπολογίσουμε το $\gcd(A, B)$ μπορούμε να θεωρήσουμε ότι $A, B \in \mathcal{F}[X]$ και να εφαρμόσουμε τον αλγόριθμο του Ευκλείδη, δείτε για παράδειγμα [160, 263, 275]. Πιο συγκεκριμένα, θεωρούμε $P_{q+1} = A$, $P_q = B$, $Q_i = \mathsf{quo}(P_{i+1}, P_i)$ και $P_{i-1} = \mathsf{rem}(P_{i+1}, P_i)$, οπότε

$$\begin{array}{rcll} P_{q+1} & = & Q_q P_q + P_{q-1} & \deg(P_{q-1}) < \deg(P_q) \\ P_q & = & Q_{q-1} P_{q-1} + P_{q-1} & \deg(P_{q-2}) < \deg(P_{q-1}) \\ & \vdots & & \\ P_{h+2} & = & Q_{h+1} P_{h+1} + P_h & \deg(P_h) < \deg(P_{h+1}) \\ P_{h+1} & = & Q_h P_h + 0 & \end{array} \tag{2.8}$$

όπου $\gcd(A, B) = P_h$. Ο αλγόριθμος τερματίζει καθώς ο βαθμός μειώνεται σε κάθε βήμα.

Ωστόσο, όταν $\mathcal{R} = \mathbb{Z}$ και $\mathcal{F} = \mathbb{Q}$ η προσέγγιση που ακολουθήσαμε για τον υπολογισμό του ΜΚΔ εισάγει ρητούς αριθμούς τους οποίους θέλουμε να αποφύγουμε γιατί οι πράξεις με ρητούς έχουν (πολύ) μεγάλη πολυπλοκότητα. Χαρακτηριστικά αναφέρουμε ότι η πρόσθεση δύο ακεραίων αυξάνει το δυαδικό μήκος του αποτελέσματος κατά 1, ενώ η πρόσθεση δύο ρητών διπλασιάζει το δυαδικό μήκος του αποτελέσματος. Συνεπώς, επιθυμούμε όχι μόνο γρήγορους αλγορίθμους για τον υπολογισμό του ΜΚΔ αλλά και αλγορίθμους που απαιτούν πράξεις μόνο στο $\mathcal{R}$ και στο $\mathcal{R}[X]$. Προκειμένου να επιτύχουμε τους στόχους μας θα ορίσουμε πιο αυστηρά την ακολουθία πολυωνύμων $(P_{q+1}, P_q, \ldots, P_h)$ και θα αναδείξουμε την άμεση συσχέτιση των συντελεστών των P_i με συγκεκριμένες υποορίζουσες του πίνακα Sylvester των A και B.

Η παρουσίασή μας βασίζεται στους von zur Gathen and Lücking [264] και Yap [275] αλλά είναι πιο απλοποιημένη. Θα χρειαστούμε τους ακόλουθους ορισμούς:

Το *περιεχόμενο* (*content*) του A είναι ο ΜΚΔ των συντελεστών του και το συμβολίζουμε ως $\mathsf{content}(A)$. Το *πρωταρχικό μέρος* (*primitive part*) του A προκύπτει αν διαιρέσουμε το A με το $\mathsf{content}(A)$ και το συμβολίζουμε με $\mathsf{pp}(A)$. Αν στο $\mathcal{R}$ δεν ορίζεται ο ΜΚΔ τότε $\mathsf{content}(A) = 1$. Δύο πολυώνυμα A, B είναι όμοια όταν $\mathsf{pp}(A) = \mathsf{pp}(B)$ και συμβολίζουμε $A \sim B$.

Ορισμός 2.16 (Πολυωνυμική ακολουθία υπολοίπων). *Έστω A, B όπως στην Εξ. (2.7). Ορίζουμε ως πολυωνυμική ακολουθία υπολοίπων (polynomial remainder sequence) των A και B την ακολουθία $\mathbf{PRS}(A, B) = (R_{q+1} = A, R_q = B, R_{q-1}, \ldots, R_h)$, για την οποία ισχύει*

$$\mathfrak{a}_i R_{i+1} = Q_i R_i + \mathfrak{b}_i R_{i-1} \tag{2.9}$$

όπου $\deg(R_{i-1}) < \deg(R_i)$, $q \geq i \geq h+1$. Απαιτούμε $\mathfrak{a}_i, \mathfrak{b}_i \in \mathcal{R}$ και $R_i \in \mathcal{R}[X]$. Επίσης ορίζουμε και την αντίστοιχη ακολουθία πηλίκων $\mathbf{PQS}(A, B) = (Q_q, Q_{q-1}, \ldots, Q_h, R_h)$.

Το μήκος της ακολουθίας είναι $q - h + 2$.

Αν ισχύει $p < q$, τότε η ακολουθία είναι $\mathbf{PRS}(A, B) = (R_{p+2} = A, R_{p+1} = B, R_p = A, \ldots, R_h)$. Υποθέτουμε $p \geq q$ προκειμένου να διευκολυνθούμε στην αριθμητική των δεικτών.

Η $\mathbf{PRS}$ είναι *πλήρης* (complete) αν η (2.9) ικανοποιείται για $i = h$ και ισχύει $R_{h-1} = 0$. Όλες οι ακολουθίες που θα θεωρήσουμε θα είναι πλήρεις, εκτός αν ρητά αναφέρεται το αντίθετο. Η $\mathbf{PRS}$ ονομάζεται κανονική (normal ή regular) αν $\deg(R_i) - \deg(R_{i+1}) = 1$, διαφορετικά ονομάζεται ελαττωματική (defective). Όταν η $\mathbf{PRS}$ είναι πλήρης και κανονική τότε $h = 0$, το μήκος της ακολουθίας είναι $q + 2$ και ο δείκτης σε κάθε πολυώνυμο R_i δηλώνει το βαθμό του.

Αξίζει να παρατηρήσουμε ότι μπορούμε να ορίσουμε μια ακολουθία υπολοίπων με μοναδικό τρόπο αν υποθέσουμε κάποια ακολουθία ζευγών $(\mathfrak{a}_i, \mathfrak{b}_i)$ ή κάποιο τρόπο υπολογισμού τους. Στην περίπτωση αυτή τα R_{i-1} και Q_i ορίζονται μοναδικά επιλύοντας ένα γραμμικό συστήμα. Ωστόσο, προκειμένου να διευκολύνουμε τον αναγνώστη, σε όλους τους κανόνες υπολογισμού πολυωνυμικών ακολουθιών υπολοίπων που θα παρουσιάσουμε, θα δίνουμε και τον τρόπο υπολογισμού των R_{i-1} και Q_i.

Ευκλείδια ακολουθία

Στην περίπτωση που ισχύει $\mathcal{R} = \mathcal{F}$ και $(\mathfrak{a}_i, \mathfrak{b}_i) = (1, 1)$ τότε η ακολουθία υπολοίπων είναι ακριβώς η ακολουθία υπολοίπων που εμφανίζεται κατά τη διάρκεια του αλγορίθμου του Ευκλείδη για τον

υπολογισμό του $\gcd(A, B)$, Εξ. (2.8), με τη μόνη διαφορά είναι ότι η αρίθμηση των δεικτών είναι στην περίπτωση της **PRS** φθίνουσα. Συνεπώς, το τελευταίο πολυώνυμο της ακολουθίας είναι ο ΜΚΔ των A και B. Την ακολουθία αυτή θα τη συμβολίσουμε με $\mathbf{Euclid-PRS}(A, B)$ και οι (αναδρομικοί) κανόνες ορισμού της είναι:

$$\mathbf{Euclid-PRS}(A, B) \quad \left\{ \begin{array}{rcl} (\mathfrak{a}_i, \mathfrak{b}_i) & = & (1, 1) \\ R_{i-1} & = & \mathsf{rem}\,(R_{i+1}, R_i) \\ Q_i & = & \mathsf{quo}\,(R_{i+1}, R_i) \end{array} \right\} \tag{2.10}$$

Οι κανόνες της (2.10) είναι στην ουσία ένας αλγόριθμος υπολογισμού της **Euclid – PRS**. Το ίδιο ισχύει και για τους επόμενους κανόνες που θα παρουσιάσουμε.

Στη χειρότερη περίπτωση υπάρχουν $\Omega(q)$ πολυώνυμα στην ακολουθία, τα οποία έχουν βαθμούς $\Omega(p)$. Κατά συνέπεια ο συνολικός αριθμός των συντελεστών όλων των πολυωνύμων στην ακολουθία είναι $\Omega(pq)$ και άρα ένα κάτω φράγμα για την αριθμητική πολυπλοκότητα υπολογισμού της ακολουθίας είναι $\Omega(pq)$. Αν $\mathcal{R} = \mathbb{Z}$ και $\mathcal{L}(A), \mathcal{L}(B) \leq \tau$ τότε το δυαδικό μήκος των πολυωνύμων στην ακολουθία φράσσεται από $\mathcal{O}(p^2\tau)$ [175]. Σε αυτό το σημείο αξίζει να επισημάνουμε ότι το άθροισμα των βαθμών των Q_i είναι $\mathcal{O}(q)$ και άρα το πλήθος των συντελεστών των πολυωνύμων που ανήκουν στην ακολουθία των πηλίκων είναι $\mathcal{O}(q)$.

Ακολουθίες κατά Sturm

Εξέχουσας σημασίας είναι η πολυωνυμική ακολουθία υπολοίπων κατά Sturm [248], η οποία διαφέρει κατά ένα πρόσημο από την Ευκλείδια ακολουθία. Οι κανόνες ορισμού της είναι:

$$\mathbf{Sturm}(A, B) \quad \left\{ \begin{array}{rcl} (\mathfrak{a}_i, \mathfrak{b}_i) & = & (1, -1) \\ R_{i-1} & = & \mathsf{rem}\,(R_{i+1}, R_i) \\ Q_i & = & \mathsf{quo}\,(R_{i+1}, R_i) \end{array} \right\} \tag{2.11}$$

Ο Sturm [248] χρησιμοποίησε την ακολουθία $\mathbf{Sturm}(A, A')$ για να απομονώσει τις πραγματικές ρίζες του A, η οποία και ονομάζεται *ακολουθία Sturm*.

Οι ακολουθίες κατά Sturm ορίζονται με πιο γενικό τρόπο ως ακολούθως:

Ορισμός 2.17. *Μια ακολουθία πραγματικών πολυωνύμων $(p_k, p_{k-1}, \ldots, p_1, p_0)$ είναι ακολουθία κατά Sturm στο διάστημα (a, b), όπου τα a και b μπορούν να είναι και $\pm\infty$, αν $\forall\, c \in (a, b)$, ισχύουν*

(i) $p_k(a)\, p_k(b) \neq 0$

(ii) *Αν* $p_k(c) = 0$ *τότε* $\exists\, \epsilon \in \mathbb{R}$ *τέτοιο ώστε* $\forall u \in (c - \epsilon, c)$, *αντίστοιχα* $\forall u \in (c, c + \epsilon)$, *να ισχύει* $p_k(u)\, p_{k-1}(u) < 0$, *αντίστοιχα* $p_k(u)\, p_{k-1}(u) > 0$.

(iii) *Αν* $p_i(c) = 0$, $0 \leq i \leq k - 1$, *τότε* $p_{i-1}(c)\, p_{i+1}(c) < 0$.

(iv) $p_0(c) \neq 0$.

Ένας από τους τρόπους υπολογισμού (υπάρχουν άπειροι) μιας ακολουθίας κατά Sturm παρουσιάζεται στην (2.11). Σε επόμενες παραγράφους θα γενικεύσουμε τον ορισμό της ακολουθίας κατά Sturm.

Ψευδο-Ευκλείδια ακολουθία

Όταν $\mathcal{R} \neq \mathcal{F}$ τότε δεν ορίζεται πάντοτε η διαίρεση και γι' αυτό το λόγο έχει εισαχθεί η ψευδο-διαίρεση (Θεωρ. 2.4). Η ακολουθία πολυωνυμικών υπολοίπων που ορίζεται με τη βοήθεια της ψευδο-διαίρεσης ονομάζεται *ψευδο-Ευκλείδια* (pseudo-Euclidean) και συμβολίζεται με $\mathbf{EPRS}(A, B)$. Θα χρησιμοποιήσουμε τον συμβολισμό $\mathfrak{r}_i = \mathsf{lead}(R_i)$ και $\delta_i = \max\{1, \deg(R_{i+1}) - \deg(R_i)\}$. Οι κανόνες της $\mathbf{EPRS}$ είναι:

$$\mathbf{EPRS}(A, B) \quad \left\{ \begin{array}{l} (\mathfrak{a}_i, \mathfrak{b}_i) = \left(\mathfrak{r}_i^{\delta_i+1}, 1\right) \\ R_{i-1} = \mathsf{rem}(\mathfrak{a}_i R_{i+1}, R_i) \\ Q_i = \mathsf{quo}(\mathfrak{a}_i R_{i+1}, R_i) \end{array} \right\} \tag{2.12}$$

όπου ο υπολογισμός των R_{i-1} και Q_i εμπεριέχει μόνο ακριβείς (χωρίς υπόλοιπο) διαιρέσεις με τους συντελεστές. Την αντίστοιχη ακολουθία πηλίκων τη συμβολίζουμε με $\mathbf{EPQS}(A, B)$. Παρατηρούμε ότι $R_{i-1} = \mathsf{rem}(\mathfrak{a}_i R_{i+1}, R_i) = \mathsf{prem}(R_{i-1}, R_i)$ και $Q_i = \mathsf{quo}(\mathfrak{a}_i R_{i+1}, R_i) = \mathsf{pquo}(R_{i-1}, R_i)$.

Η ψευδο-Ευκλείδια ακολουθία είναι ο πιο εύκολος και προφανής τρόπος υπολογισμού μιας πολυωνυμικής ακολουθίας υπολοίπων και κατά συνέπεια του ΜΚΔ δύο πολυωνύμων. Η αριθμητική πολυπλοκότητα του υπολογισμού της είναι $\mathcal{O}(pq)$ και άρα βέλτιστη. Επιπρόσθετα, μπορεί να δειχτεί ότι οποιαδήποτε άλλη ακολουθία που ικανοποιεί τις απαιτήσεις της (2.9) παράγει πολυώνυμα τα οποία είναι όμοια με αυτά της $\mathbf{EPRS}$.

Ωστόσο, το δυαδικό μήκος των πολυωνύμων στην $\mathbf{EPRS}(A, B)$ αυξάνεται εκθετικά σε σχέση το μήκος της ακολουθίας. Μπορεί να δειχτεί [160, 178, 263, 264, 275] ότι το R_i μπορεί να έχει δυαδικό μήκος μεγαλύτερο κατά ένα παράγοντα $(1+\sqrt{2})^i$ σε σχέση με το δυαδικό μήκος των A και B. Συνεπώς η $\mathbf{EPRS}$ απαιτεί εκθετικό αριθμό δυαδικών πράξεων και άρα δεν έχει μεγάλη πρακτική σημασία.

Πρωταρχική ακολουθία

Προκειμένου να αντιμετωπίσουμε την εκθετική συμπεριφορά της $\mathbf{EPRS}$ η πιο προφανής λύσης είναι να αντικαταστήσουμε κάθε R_{i-1} στην $\mathbf{EPRS}$ με το πρωταρχικό του μέρος. Δηλαδή να θέσουμε $\mathfrak{b}_i = \mathsf{content}(R_{i-1})$. Η ακολουθία που σχηματίζεται με αυτόν το τρόπο ονομάζεται *πρωταρχική ακολουθία πολυωνυμικών υπολοίπων* (primitive polynomial remainder sequence) και θα τη συμβολίζουμε με $\mathbf{PPRS}$. Οι κανόνες της είναι:

$$\mathbf{PPRS}(A, B) \quad \left\{ \begin{array}{l} (\mathfrak{a}_i, \mathfrak{b}_i) = \left(\mathfrak{r}_i^{\delta_i+1}, \mathsf{content}(\mathsf{prem}(R_{i-1}, R_i))\right) \\ R_{i-1} = \mathsf{rem}(\mathfrak{a}_i R_{i+1}, R_i) / \mathfrak{b}_i \\ Q_i = \mathsf{quo}(\mathfrak{a}_i R_{i+1}, R_i) \end{array} \right\} \tag{2.13}$$

όπου ο υπολογισμός των R_{i-1} και Q_i εμπεριέχει μόνο ακριβείς διαιρέσεις με τους συντελεστές. Η αντίστοιχη ακολουθία πηλίκων συμβολίζεται με $\mathbf{PPQS}(A, B)$.

Η ακολουθία $\mathbf{PPRS}(A, B)$ είναι ό,τι καλύτερο μπορούμε να περιμένουμε σχετικά με το δυαδικό μήκος των πολυωνύμων της ακολουθίας. Ωστόσο, ο υπολογισμός της απαιτεί σε κάθε βήμα τον υπολογισμό του περιεχομένου ενός πολυωνύμου, πράξη η οποία είναι αρκετά χρονοβόρα. Είναι πολύ δύσκολο να υπολογίσουμε θεωρητικά τη δυαδική πολυπλοκότητα του υπολογισμού της

πρωταρχικής ακολουθίας, καθώς δεν μπορούμε να προβλέψουμε τον συσχετισμό των συντελεστών των πολυωνύμων που εμφανίζονται στην ακολουθία, αν και μπορεί να δειχτεί ότι αν η ακολουθία υπολογιστεί συμβολικά οι συντελεστές των πολυωνύμων της ακολουθίας (που είναι πολυώνυμα ως προς τους συντελεστές των αρχικών πολυωνύμων) είναι ανάγωγα πολυώνυμα και μεταξύ τους πρώτα [83]. Για τον υπολογισμό όλης της ακολουθίας απαιτούνται $\mathcal{O}(p\,q)$ πράξεις, καθώς τόσο είναι το πλήθος των συντελεστών. Υπάρχουν $\mathcal{O}(q)$ πολυώνυμα στην ακολουθία. Αν κάνουμε την ασθενή υπόθεση ότι απαιτείται ένας υπολογισμός ΜΚΔ για κάθε πολυώνυμο της ακολουθίας, τότε απαιτούνται τουλάχιστον $\mathcal{O}(p\,q^2)$ αριθμητικές πράξεις. Όπως θα παρουσιάσουμε στην επόμενη παράγραφο που θα αναφερθούμε στις υπο-επιλύουσες, το δυαδικό μήκος των συντελεστών της ακολουθίας είναι τουλάχιστον $\mathcal{O}(p\,\tau)$. Άρα, η δυαδική πολυπλοκότητα υπολογισμού της **PPRS** είναι τουλάχιστον $\widetilde{\mathcal{O}}_B(p\,q^2\,\mathsf{M}\,(p\,\tau))$. Οι αλγόριθμοι που θα παρουσιάσουμε στη συνέχεια έχουν καλύτερη πολυπλοκότητα, αν και η σπουδαιότητα της πρωταρχικής ακολουθίας δεν πρέπει να υποτιμάται τουλάχιστον σε υπολογισμούς με πολυώνυμα σχετικά μικρού βαθμού.

Σε κάθε περίπτωση γεννάται το ερώτημα σχετικά με το πως θα μπορούσαμε να υπολογίσουμε το περιεχόμενο ενός πολυωνύμου της **EPRS**, ή έστω κάποιου αρκετά μεγάλου διαιρέτη του, χωρίς να καταφύγουμε στους χρονοβόρους υπολογισμούς του μέγιστου κοινού διαιρέτη πολλών αριθμών. Επιπρόσθετα, θα επιθυμούσαμε το δυαδικό μήκος των συντελεστών να πλησιάζει όσο το δυνατόν περισσότερο αυτό της πρωταρχικής ακολουθίας, δηλαδή στη χειρότερη περίπτωση να αυξάνεται γραμμικά.

Πιο συγκεκριμένα αν $\mathbf{EPRS}(A, B) = (R_{q+1}, R_q, \ldots, R_h)$ σκοπός μας είναι να υπολογίσουμε μια άλλη ακολουθία $(P_{q+1}, P_q, \ldots, P_h)$, τέτοια ώστε $R_i \sim P_i$ και $P_i = R_i/\beta_i$, όπου $\beta_i \in \mathcal{R}$ και η διαίρεση είναι χωρίς υπόλοιπο.

Υπο-επιλύουσες (subresultants)

Προκειμένου να αντιμετωπιστεί το πρόβλημα της εκθετική αύξησης του δυαδικού μήκους των συντελεστών στην ψευδο-Ευκλείδια ακολουθία και ταυτόχρονα να αποφευχθεί ο υπολογισμός της πρωταρχικής ακολουθίας που εμπεριέχει πολλούς υπολογισμούς αρχικά ο Collins [54] και στη συνέχεια οι Brown and Traub [35] (ξανα-)ανακάλυψαν τις πολυωνυμικές υπο-επιλύουσες (ή υπο-απαλοίφουσες) (polynomials subresultants) οι οποίες ορίζονται ως ορίζουσες κάποιας παραλλαγής του πίνακα Sylvester, δείτε επίσης [34, 36, 37, 178]. Ο Habicht [125] ήδη από το 1948 είχε εισαγάγει αυτή την προσέγγιση. Ο αναγνώστης μπορεί να ανατρέξει στην εργασία των Ho and Yap [133] για την μοντέρνα εκδοχή της προσέγγισης του Habicht.

Ο αναγνώστης μπορεί να ανατρέξει στους von zur Gathen and Lücking [264] οι οποίοι παρουσιάζουν με ενοποιημένο τρόπο τις διάφορες παραλλαγές σχετικά με τις υπο-επιλύουσες ή στον El Kahoui [83] όπου η έννοια της υπο-επιλύσουσας γενικεύεται για κάθε αβελιανό δακτύλιο. Για πιο σύγχρονες εκδοχές των υπο-επιλυουσών ο αναγνώστης μπορεί να ανατρέξει στους Basu et al. [14], González-Vega et al. [118, 119], Lickteig and Roy [174, 175], Lombardi et al. [176], von zur Gathen and Gerhard [263], Yap [275] όπου επίσης περιέχονται και οι αποδείξεις των θεωρημάτων που παρουσιάζουμε.

Έστω k πολυώνυμα $A_i = \sum_{j=0}^{n_i} a_{ij} X^j \in \mathcal{R}[X]$, $1 \leq i \leq k$ και $\ell = 1 + \max_{1 \leq i \leq k} n_i$. Θεωρούμε

τον πίνακα

$$mat(A_1, \ldots, A_k) = [a_{i,\ell-j}]$$

του οποίου η i γραμμή περιέχει τους συντελεστές του A_i και $a_{ij} = 0$ αν $j > n_j = \deg(A_i)$. Ο πίνακας έχει διαστάσεις $k \times \ell$.

Ορισμός 2.18. *Έστω $M \in \mathcal{R}^{k\times\ell}$, $\ell \leq k$. Το πολυώνυμο ορίζουσας (determinant polynomial) του M είναι:*

$$detpol(M) := \det(M^{(k)})X^{\ell-k} + \cdots + \det(M^{(\ell)})$$

όπου $M^{(i)}$ είναι ένας τετραγωνικός υποπίνακας του M, ο οποίος αποτελείται από τις πρώτες $k-1$ στήλες και την i στήλη ($\ell \leq i \leq k$).

Ορισμός 2.19 (subresultants). *Έστω $A, B \in \mathcal{R}[X]$, όπως στην Εξ. (2.7).*

- *Η k (πολυωνυμική) υπο-επιλύουσα (k^{th} subresultant) των A και B είναι το πολυώνυμο*

  $$\mathbf{SR}_k(A, B) = detpol(M_k)$$

  όπου $M_k = mat(X^{q-k-1}A, \ldots, A, X^{p-k-1}B, \ldots, B)$.

- *Η ακολουθία υπο-επιλυουσών (subresultant chain) των A και B είναι:*

  $$\mathbf{SR}(A, B) = (\mathbf{SR}_{q+1} = A, \mathbf{SR}_q = B, \mathbf{SR}_{q-1}, \ldots, \mathbf{SR}_0)$$

- *Ο $k-$οστός πρωτεύων συντελεστής της υπο-επιλύσουσας (k^{th} principal subresultant coefficient) των A και B είναι*

  $$\mathbf{psc}_k(A, B) = \det(M_k^{(k)}), \quad 0 \leq k \leq q$$

  όπου $\mathbf{psc}_{q+1} = 1$.

Αν δεν υπάρχει ο κίνδυνος σύγχυσης τότε θα συμβολίζουμε $\mathbf{SR}_i(A, B) = \mathbf{SR}_i$ και $\mathbf{psc}_i(A, B) = \mathbf{psc}_i = \mathbf{sr}_i$.

Οι υπο-επιλύουσες δεν είναι τίποτα άλλο από κάποια υλοποίηση πολυωνυμικών ακολουθιών υπολοίπων με τις επιπλέον ιδιότητες ότι τα πολυώνυμα της ακολουθίας είναι στο $\mathcal{R}[X]$, ότι συμπεριφέρονται καλά κάτω από ομομορφισμούς εκτίμησης και ότι αν $\mathcal{R} = \mathbb{Z}$ η αύξηση στο δυαδικό μήκος των πολυωνύμων είναι το πολύ γραμμική.

Παρατηρούμε ότι ο πίνακας $M_0 = mat(X^{q-1}A, \ldots, A, X^{p-}B, \ldots, B)$ είναι ο πίνακας Sylvester των A και B, δηλαδή ισχύει $\mathtt{Syl}(A, B) = M_0$. Πιο συγκεκριμένα ισχύει το ακόλουθο θεώρημα:

Θεώρημα 2.20

Το πολυώνυμο $\mathbf{SR}_0(A, B)$ είναι (εκτός ίσως από το πρόσημό του) η επιλύουσα των A και B, δηλαδή $\mathbf{SR}_0(A, B) = \pm\mathtt{res}(A, B)$.

Από την ακολουθία $\mathbf{SR}(A, B)$ μπορούμε να υπολογίσουμε τον ΜΚΔ των A και B. Πιο συγκεκριμένα ισχύει ότι:

$$\mathbf{SR}_k(A, B) = \gcd(A, B) \Leftrightarrow \begin{cases} \mathbf{psc}_0(A, B) = \cdots = \mathbf{psc}_{k-1}(A, B) = 0 \\ \mathbf{psc}_k(A, B) \neq 0 \end{cases}$$

και $\deg(\gcd(A, B)) = k$.

Από τον ορισμό του πρωτεύοντος συντελεστή της υπο-επιλύουσας προκύπτει ότι μπορεί να είναι και μηδέν! Δηλαδή ο πρωτεύων συντελεστής δεν είναι απαραίτητα και ο μεγιστοβάθμιος όρος της υπο-επιλύουσας. Στη γενική περίπτωση ισχύει $\mathsf{lead}\left(\mathbf{SR}_i\right) \neq \mathbf{psc}_i$ και $\deg(\mathbf{SR}_i) \leq i$. Όταν $\forall i$ ισχύει $\mathbf{psc}_i \neq 0$, δηλαδή $\deg(\mathbf{SR}_i) = i$, τότε η ακολουθία είναι κανονική (normal ή regular) αλλιώς είναι ελαττωματική (defective). Οι ορισμοί είναι ακριβώς οι ίδιοι με αυτούς των πολυωνυμικών ακολουθιών υπολοίπων. Επίσης, αν $\deg(\mathbf{SR}_j) = k < j$, τότε $\mathbf{SR}_i = 0$ για $j + 1 \geq i > k$ και $\deg(\mathbf{SR}_k) = k$ και $\mathbf{SR}_j \sim \mathbf{SR}_k$. Αυτό είναι και το κλασικό θεώρημα δομής για τις υπο-επιλύουσες (gap structure theorem of subresultants) [54, 178].

Πρέπει να προσθέσουμε ότι θα μπορούσαμε να είχαμε χρησιμοποιήσει τον πίνακα Bézout προκειμένου να ορίσουμε την ακολουθία υπο-επιλυουσών [20, 21, 136].

Προκειμένου οι ακολουθίες υπο-επιλυουσών να υπακούουν τον Ορ. (2.9) θεωρούμε ότι έχουμε απομακρύνει τα μηδενικά πολυώνυμα που βρίσκονται στις ενδιάμεσες θέσεις της $\mathbf{SR}(A, B)$ και επεκτείνουμε τον ορισμό έτσι ώστε να επιτρέπουμε να υπάρχουν δύο, συνεχόμενα, ίδιου βαθμού πολυώνυμα στην ακολουθία.

Τόσο οι υπο-επιλύουσες όσο και οι συντελεστές τους προκύπτουν ως ορίζουσες κάποιων υποπινάκων του πίνακα Sylvester και γι' αυτό έχουν πολύ καλή συμπεριφορά κάτω από ομομορφισμούς εκτίμησης, δείτε για παράδειγμα [118, 119, 120, 178]. Δηλαδή, μπορούμε να θεωρήσουμε τους συντελεστές των πολυωνύμων ως παραμέτρους, να υπολογίζουμε τις υπο-επιλύουσες συμβολικά και στη συνέχεια να αποδώσουμε τιμές στους παραμέτρους έχοντας την εγγύηση ότι θα υπολογίσουμε το ίδιο αποτέλεσμα με το αν είχαμε αντικαταστήσει τις παραμέτρους στην αρχή και στη συνέχεια υπολογίζαμε την ακολουθία των υπο-επιλυουσών.

Επίσης, το γεγονός ότι ορίζονται από ορίζουσες μας επιτρέπει να φράξουμε το δυαδικό μήκος των πολυωνύμων της ακολουθίας χρησιμοποιώντας την ανισότητα του Hadamard, δείτε για παράδειγμα [275, 276], και πιο συγκεκριμένα αν $\mathcal{R} = \mathbb{Z}$ τότε ισχύει ότι $\mathcal{L}\left(\mathbf{SR}_i\right) = \mathcal{O}(p\tau)$.

Ωστόσο, προκειμένου να υπολογίσουμε τις υπο-επιλύουσες δεν υπολογίζουμε ορίζουσες. Ο λόγος είναι ότι η πολυπλόκοτητα του υπολογισμού της ορίζουσας είναι $\mathcal{O}(p^3)$ και καθώς έχουμε $\mathcal{O}(q)$ πολυώνυμα στην ακολουθία θα καταλήγαμε σε έναν αλγόριθμο με πολυπλοκότητα $\mathcal{O}(p^3 q)$ που απέχει πολύ από το βέλτιστο που είναι $\mathcal{O}(pq)$. Οι αλγόριθμοι που υπολογίζουν υπο-επιλύουσες εκμεταλλεύονται την ειδική μορφή του πίνακα Sylvester και συνάγουν διάφορα θεωρήματα που αφορούν διαιρέτες του περιεχομένου των πολυωνύμων της ακολουθίας των υπο-επιλυουσών και χρησιμοποιούν ψευδο-διαιρέσεις. Το πιο γνωστό θεώρημα είναι το εξής:

Θεώρημα 2.21

Για $0 < k < q$, $k < q - 1$, το ψευδο-υπόλοιπο των $\mathbf{SR}_{k+1}$ και $\mathbf{SR}_k$ είναι πολλαπλάσιο του $\mathbf{SR}_{k-1}$, δηλαδή

$$\mathbf{SR}_{k-1} = \mathsf{prem}\left(\mathbf{SR}_{k+1}, \mathbf{SR}_k\right) / \mathsf{lead}\left(\mathbf{SR}_{k+1}\right)$$

Το προηγούμενο θεώρημα μας παρέχει ένα αλγόριθμο υπολογισμού της ακολουθίας ο οποίος είναι πολυπλοκότητας $\mathcal{O}(p\,q)$ ή $\mathcal{O}_B(p\,q\,\mathsf{M}\left(p\,\tau\right))$, όταν $\mathcal{R} = \mathbb{Z}$.

Η παρουσίαση και άλλων θεωρημάτων είναι πέρα πό τις επιδιώξεις της παρούσας διατριβής. Ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία [54, 175, 176, 263, 264] για περισότε-

ρες λεπτομέρειες. Για λόγους πληρότητας θα παρουσιάσουμε χωρίς απόδειξη μερικούς ακόμα κανόνες υπολογισμού ακολουθιών πολυωνυμικών υπολοίπων ή ακολουθιών υπο-επιλυουσών:

$$[54]\quad \mathbf{reduced-PRS}(A,B)\quad \left\{\begin{array}{rcl} \mathfrak{a}_{q+1} &=& 1\\ (\mathfrak{a}_i,\mathfrak{b}_i) &=& \left(\mathfrak{r}_i^{\delta_i+1},\mathfrak{a}_{i+1}\right)\\ R_{i-1} &=& \mathsf{rem}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)/\mathfrak{b}_i\\ Q_i &=& \mathsf{quo}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)\end{array}\right\} \tag{2.14}$$

$$[34,\,54]\quad \mathbf{Subresultant-PRS}(A,B)\quad \left\{\begin{array}{rcll} \mathfrak{r}_{q+1} &=& 1 & \\ (\mathfrak{a}_i,\mathfrak{b}_i) &=& \left(\mathfrak{r}_i^{\delta_i+1},-\mathfrak{r}_{i+1}\,\psi_i^{\delta_i+1}\right) & \\ \psi_i &=& \left\{\begin{array}{ll} -1 & i=q\\ (-\mathfrak{r}_{i+1})^{\delta_{i+1}}\,\psi_{i+1}^{1-\delta_{i+1}} & \text{αλλιώς}\end{array}\right. & \\ R_{i-1} &=& \mathsf{rem}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)/\mathfrak{b}_i & \\ Q_i &=& \mathsf{quo}\left(\mathfrak{a}_i\,R_{i+1},R_i\right) & \end{array}\right\} \tag{2.15}$$

$$[36,\,37]\quad \mathbf{improved-PRS}(A,B)\quad \left\{\begin{array}{rcll} \mathfrak{r}_{q+1} &=& 1 & \\ (\mathfrak{a}_i,\mathfrak{b}_i) &=& \left(\mathfrak{r}_i^{\delta_i+1},-\mathfrak{r}_{i+1}\,\psi_i^{\delta_i+1}\,\mu_{i+1}^{-\delta_i-1}\right)\mu_i & \\ \psi_i &=& \left\{\begin{array}{ll} -1 & i=q\\ (-\mu_{i+2}\,\mathfrak{r}_{i+1})^{\delta_{i+1}}\,\psi_{i+1}^{1-\delta_{i+1}} & \text{αλλιώς}\end{array}\right. & \\ R_{i-1} &=& \mathsf{rem}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)/\mathfrak{b}_i & \\ Q_i &=& \mathsf{quo}\left(\mathfrak{a}_i\,R_{i+1},R_i\right) & \end{array}\right\} \tag{2.16}$$

όπου τα μ_i είναι τέτοια ώστε να ικανοποιείται η Εξ. (2.9). Ο Brown [36, 37] προτείνει $\mu_i = \mathsf{gcd}\left(\mathsf{lead}\left(A\right),\mathsf{lead}\left(B\right)\right)$.

Ακολουθίες Sturm-Habicht

Υπάρχουν επίσης και οι ακολουθίες Sylvester-Habicht, οι οποίες συμβολίζονται με $\mathbf{StHa}(A,B)$ και οι οποίες αν $B=A'$ ονομάζονται ακολουθίες Sturm-Habicht [14, 118, 119, 175, 176]. Οι ακολουθίες αυτές είναι εξ ορισμού προσημασμένες (δείτε τον Ορ. 2.3) και όταν η ακολουθία είναι κανονική είναι, εκτός από κάποιο πρόσημο, οι ίδιες με την $\mathbf{SR}(A,B)$. Όταν όμως η ακολουθία είναι ελαττωματική τότε τα πολυώνυμα που την αποτελούν έχουν μικρότερους συντελεστές.

Όσον αφορά του κανόνες υπολογισμού της, υποθέτουμε ότι έχουμε δύο συνεχόμενα πολυώνυμα R_j και R_{j-1} της ακολουθίας και θέλουμε να υπολογίσουμε τα δύο επόμενα, δηλαδή τα R_k και R_{k-1}. Οι κανόνες είναι

1. $h_k\,R_{j-1} = \mathfrak{r}_{j-1}\,R_k$, όπου $h_k = (-1)^{(j-k)(j-k+1)/2}\,\dfrac{\mathfrak{r}_{j-1}^{j-k}}{\mathfrak{r}_j^{j-k-1}}$.
2. $R_\ell = 0$, για $k<\ell<j$.

3. $\mathfrak{r}_j^2\, R_{k-1} = -\,\mathsf{rem}\,(\mathfrak{r}_{j-1}\, h_k\, R_j, R_{j-1})$.

όπου ο υπολογισμός του υπολοίπου στην τελευταία σχέση εμπεριέχει μόνο ακριβείς διαιρέσεις με τους συντελεστές του διαιρέτη και του διαιρετέου. Αν $\deg(R_{j-1}) = j-1$ τότε $k = j-1$ και η ακολουθία είναι κανονική. Την ακολουθία αυτή έχουμε χρησιμοποιήσει στις υλοποιήσεις μας.

Γενικευμένες ακολουθίες Sturm

Οι γενικευμένες ακολουθίες Sturm [275] αποτελούν γενίκευση των ακολουθιών κατά Sturm, Εξ. (2.11).

Ορισμός 2.22 (Γενικευμένες ακολουθίες Sturm). *Έστω $A, B \in \mathbb{R}[X]$ όπως στην Εξ. (2.7). Ορίζουμε ως γενικευμένη ακολουθία Sturm (generalized Sturm sequence) ή προσημασμένη πολυωνυμική ακολουθία υπολοίπων (signed polynomial remainder sequence) ή προσημασμένη ακολουθία υπο-επιλυουσών (signed subresultant chain) των A και B την ακολουθία $\mathbf{St}(A,B) = (R_{q+1} = A, R_q = B, R_{q-1}, \ldots, R_h)$, για την οποία ισχύει*

$$\mathfrak{a}_i\, R_{i+1} = Q_i\, R_i + \mathfrak{b}_i\, R_{i-1} \qquad a_i b_i < 0 \tag{2.17}$$

όπου $\mathfrak{a}_i \mathfrak{b}_i < 0$, $q \geq i \geq h+1$ και το μήκος της ακολουθίας της ακολουθίας είναι $q-h+2$. Απαιτούμε $\mathfrak{a}_i, \mathfrak{b}_i \in \mathcal{R}$ και $R_i \in \mathcal{R}[X]$. Επίσης θεωρούμε και την ακολουθία πηλίκων $\mathbf{StQ}(A,B) = (Q_q, Q_{q-1}, \ldots, Q_h, A_h)$.

Οι ακολουθίες υπο-επιλυουσών που παρουσιάσαμε σε προηγούμενες παραγράφους μπορούν να γίνουν προσημασμένες είτε προσαρμόζοντας κατάλληλα τους κανόνες υπολογισμού τους είτε μετά τον υπολογισμό τους να χρησιμοποιήσουμε το αλγόριθμο του Yap [275], ο οποίος είναι γραμμικός, ώστε να τις καταστήσουμε προσημασμένες. Επίσης, όλα τα θεωρήματα που ισχύουν για τις υπο-επιλύουσες ισχύουν και αν είναι προσημασμένες.

Σημείωση 2.23. *Σε ό,τι θα ακολουθήσει θα θεωρήσουμε μόνο προσημασμένες ακολουθίες υπο-επιλυουσών και όταν αναφερόμαστε σε υπο-επιλύουσες θα εννοούμε προσημασμένες υπο-επιλύουσες.*

Προκειμένου να μην επιβαρύνουμε περαιτέρω τον συμβολισμό θα θεωρήσουμε $\mathbf{SR} = \mathbf{St}$ και $\mathbf{SRQ} = \mathbf{StQ}$.

Αν $\mathbf{SR}(A,B)$ είναι μια (προσημασμένη) ακολουθία υπο-επιλυουσών τότε συμβολίζουμε με $\mathbf{SR}(A, B\,;\, \mathsf{a})$ την ακολουθία που προκύπτει αν αποτίμησουμε όλα τα πολυώνυμα της ακολουθίας στο a, δηλαδή

$$\mathbf{SR}(A, B\,;\, \mathsf{a}) = (\mathbf{SR}_{q+1}(\mathsf{a}), \mathbf{SR}_q(\mathsf{a}), \ldots, \mathbf{SR}_1(\mathsf{a}), \mathbf{SR}_0(\mathsf{a}))$$

Ορισμός 2.24. *Έστω η ακολουθία $\mathtt{a} = (a_0, a_1, \ldots, a_k) \in \mathbb{R}^k$. Ορίζουμε το πλήθος των εναλλαγών προσήμων στην ακολουθία $\mathtt{a}$, το οποίο συμβολίζουμε $\mathtt{VAR}(\mathtt{a})$, αναγωγικά στο k ως:*

$$\begin{aligned} \mathtt{VAR}(a_1) &= 0 \\ \mathtt{VAR}(a_1, \ldots, a_k) &= \begin{cases} \mathtt{VAR}(a_1, \ldots, a_{k-1}) + 1 & \text{αν } \mathrm{sign}(a_{k-1} a_k) = -1 \\ \mathtt{VAR}(a_1, \ldots, a_{k-1}) & \text{αλλιώς} \end{cases} \end{aligned}$$

Σημείωση 2.25. *Αν* $f = \sum_{i=0}^{n} a_i X^i$ *τότε* $\mathtt{VAR}(f) = \mathtt{VAR}(a_n, \ldots, a_1, a_0)$.

Τα παρακάτω θεωρήματα αναδεικνύουν τη μεγάλη σημασία των προσημασμένων ακολουθιών:

Θεώρημα 2.26

Έστω $A, B \in \mathbb{R}[X]$ *σχετικά πρώτα μεταξύ τους. Αν* $\mathsf{a} < \mathsf{b}$, $\mathsf{a}, \mathsf{b} \in \mathbb{R} \cup \{\pm\infty\}$ *δεν είναι ρίζες του* A *τότε*

$$\begin{aligned} \mathtt{VAR}\left(\mathbf{SR}(A, B\,;\,[\mathsf{a},\mathsf{b}])\right) &:= \mathtt{VAR}\left(\mathbf{SR}(A, B\,;\,\mathsf{a})\right) - \mathtt{VAR}\left(\mathbf{SR}(A, B\,;\,\mathsf{b})\right) \\ &= \sum_{\substack{\gamma \mid A(\gamma)=0 \\ \mathsf{a}<\gamma<\mathsf{b}}} \mathrm{sign}\left(A'(\gamma)B(\gamma)\right) \end{aligned}$$

Η αποτίμηση στο $\pm\infty$ πραγματοποιείται θεωρώντας το όριο στο $\pm\infty$. Αν στο προηγούμενο θεώρημα αντικαταστήσουμε το $B = A'$ τότε η ποσότητα $\mathtt{VAR}\left(\mathbf{SR}(A, A'\,;\,[\mathsf{a},\mathsf{b}])\right)$ μας δίνει το πλήθος των πραγματικών ριζών του A στο διάστημα (a, b). Το επόμενο πόρισμα οφείλεται στον Sturm [248].

Πόρισμα 2.27. *Έστω* $A \in \mathbb{R}[X]$. *Αν* $\mathsf{a} < \mathsf{b}$, $\mathsf{a}, \mathsf{b} \in \mathbb{R} \cup \{\pm\infty\}$ *δεν είναι ρίζες του* A *τότε*

$$\mathtt{VAR}\left(\mathbf{SR}(A, A'\,;\,\mathsf{a})\right) - \mathtt{VAR}\left(\mathbf{SR}(A, A'\,;\,\mathsf{b})\right) = \#\{\gamma \mid A(\gamma) = 0 \wedge \mathsf{a} < \gamma < \mathsf{b}\}$$

Το προηγούμενο πόρισμα μπορεί να προκύψει θεωρώντας $B = 1$ στο παρακάτω θεώρημα:

Θεώρημα 2.28

Έστω $A, B \in \mathbb{R}[X]$ *σχετικά πρώτα μεταξύ τους. Αν* $\mathsf{a} < \mathsf{b}$, $\mathsf{a}, \mathsf{b} \in \mathbb{R}$ *δεν είναι ρίζες του* A *τότε*

$$\mathtt{VAR}\left(\mathbf{SR}(A, A'B\,;\,\mathsf{a})\right) - \mathtt{VAR}\left(\mathbf{SR}(A, A'B\,;\,\mathsf{b})\right) = \sum_{\substack{\gamma \mid A(\gamma)=0 \\ \mathsf{a}<\gamma<\mathsf{b}}} \mathrm{sign}\left(B(\gamma)\right)$$

Σημείωση 2.29. *Αν χρησιμοποιούσαμε τις ακολουθίες Sylvester-Habicht ή Sturm-Habicht τότε ο ορισμός του* $\mathtt{VAR}\left(\mathbf{StHa}(A, B\,;\,\mathsf{a})\right)$ *θα πρέπει να τροποποιηθεί ελαφρά. Πιο συγκεκριμένα, αφού διαγράψουμε τα μηδενικά πολυώνυμα, αποτιμούμε την ακολουθία πάνω στο* a *και προκειμένου να μετρήσουμε τις εναλλαγές προσήμων, μετράμε 1 εναλλαγή για κάθε ομάδα προσήμων* $[+, 0, 0, -]$ *και* $[-, 0, 0, +]$ *και 2 εναλλαγές για κάθε ομάδα* $[+, 0, 0, +]$ *και* $[-, 0, 0-]$.

Σε ό,τι θα ακολουθήσει θα συμβολίζουμε με $\mathbf{SR}(A)$ την ακολουθία $\mathbf{SR}(A, A')$.

Πολυπλοκότητα υπολογισμών με υπο-επιλύουσες

Θεωρούμε ότι $\mathcal{R} = \mathbb{Z}$ και $A, B, \in \mathbb{Z}[X]$ για A και B όπως στην Εξ. (2.7).

Υπάρχουν πολλοί αλγόριθμοι [14, 77, 176, 263, 275] για τον υπολογισμό προσημασμένων ακολουθιών υπο-επιλυουσών οι οποίοι βασίζονται, ως επί το πλείστον, στους κανόνες που έχουμε αναφέρει. Με την εξαίρεση του αλγορίθμου του Ducos [77], οι αλγόριθμοι προσπαθούν να είναι όσο το δυνατόν κοντύτερα στην ψευδο-Ευκλείδια ακολουθία και να υπολογίσουν διαιρέτες του περιεχομένου των πολυωνύμων της ακολουθίας.

Μπορούμε να διατυπώσουμε το ακόλουθο θεώρημα [14, 77, 176, 222]:

Θεώρημα 2.30

Έστω $A, B \in \mathbb{Z}[X]$ τέτοια ώστε $\deg(A) = p \geq q = \deg(B)$ και $\mathcal{L}(A) = \mathcal{L}(B) = \tau$. Η πολυπλοκότητα υπολογισμού της ακολουθίας $\mathbf{SR}(A, B)$ είναι $\mathcal{O}_B(pq\,\mathsf{M}(p\tau))$, ή $\widetilde{\mathcal{O}}_B(p^2q\tau)$. Επιπρόσθετα $\mathcal{L}(\mathbf{SR}_j(A, B)) = \mathcal{O}(p\tau)$.

Η παραπάνω πολυπλοκότητα είναι σχεδόν βέλτιστη, με την εξαίρεση κάποιων σταθερών και λογαριθμικών παραγόντων, καθώς: Υπάρχουν $\Omega(q)$ πολυώνυμα στην ακολουθία, τα οποία έχουν βαθμούς $\Omega(p)$, κατά συνέπεια ο συνολικός αριθμός των συντελεστών που εμφανίζονται στην ακολουθία είναι $\Omega(pq)$. Αυτή η παρατήρηση μας επιτρέπει να επιχειρηματολογήσουμε ότι η αριθμητική πολυπλοκότητα $O(pq)$ που επιτυγχάνεται από τους αλγορίθμους είναι βέλτιστη. Εφόσον το μέγιστο δυαδικό μήκος των συντελεστών είναι $\Omega(p\tau)$ με παρόμοιο τρόπο συνάγουμε και ότι η δυαδική πολυπλοκότητα είναι βέλτιστη.

Ωστόσο, το φράγμα πολυπλοκότητας αφορά το σύνολο της ακολουθίας $\mathbf{SR}(A, B)$. Όταν για παράδειγμα δεν ενδιαφερόμαστε για όλη την ακολουθία (π.χ μας ενδιαφέρει κάποιο συγκεκριμένο πολυώνυμο της ακολουθίας) ή όταν ο τελικός στόχος είναι η αποτίμηση της ακολουθίας πάνω σε έναν αριθμό τότε υπάρχουν και πιο γρήγοροι αλγόριθμοι. Η βασική τους ιδέα είναι να αναπαραστήσουν την $\mathbf{SR}(A, B)$ εμμέσως με τη χρήση της αντίστοιχης πολυωνυμικής ακολουθίας πηλίκων, $\mathbf{SRQ}(A, B)$.

Οι αλγόριθμοι είναι *διαίρει-και-βασίλευε* και βασίζονται πάνω στην δομή του αλγορίθμου HALF-GCD [247, 275]. Στην σύγχρονη μορφή τους οι αλγόριθμοι παρουσιάστηκαν από τον Reischert [222] και τους Lickteig and Roy [175], δείτε επίσης [263].

Αν $\mathbf{SRQ}(A, B) = (Q_0, Q_1, \ldots, Q_{k-1}, \mathbf{SR}_k)$ είναι η ακολουθία πηλίκων που αντιστοιχεί στην $\mathbf{SR}(A, B)$ όπου $\mathbf{SR}_k \neq 0$, τότε μπορούμε να διατυπώσουμε το ακόλουθο θεώρημα [14, 175, 222, 263]:

Θεώρημα 2.31

Έστω $A, B \in \mathbb{Z}[X]$ τέτοια ώστε $\deg(A) = p \geq q = \deg(B))$ και $\mathcal{L}(A) = \mathcal{L}(B) = \tau$. Ο υπολογισμός της ακολουθίας $\mathbf{SRQ}(A, B)$, της επιλύουσας, $\mathtt{res}(A, B)$, και του ΜΚΔ, $\gcd(A, B)$, έχει πολυπλοκότητα $\mathcal{O}_B(q \lg q \mathsf{M}(p\tau))$ ή $\widetilde{\mathcal{O}}_B(p\,q\,\tau)$. Επιπρόσθετα, $\mathcal{L}(\mathtt{res}(A, B)) = \mathcal{L}(\gcd(A, B)) = \mathcal{O}(p\,\tau)$.

Παρατηρούμε ότι το πλήθος των συντελεστών της $\mathbf{SRQ}(A, B)$ είναι $\mathcal{O}(q)$ και ότι έχουν μέγιστο δυαδικό μήκος $\mathcal{O}(p\tau)$ [14, 222]. Όσον αφορά στον υπολογισμό κάποιου πολυωνύμου της ακολουθίας $\mathbf{SR}(A, B)$ και στον υπολογισμό του $\gcd(A, B)$, η πολυπλοκότητα του Θεωρ. 2.31 είναι

βέλτιστη, με την εξαίρεση κάποιων σταθερών και πολυλογαριθμικών παραγόντων. Αυτό προκύπτει από το γεγονός ότι στη γενική περίπτωση ο βαθμός των πολυωνύμων στην ακολουθία είναι $\mathcal{O}(q)$ και οι συντελεστές τους έχουν δυαδικό μήκος $\mathcal{O}(p\tau)$. Δεν συμβαίνει το ίδιο και με τον υπολογισμό του $\mathtt{res}(A, B)$. Στη γενική περίπτωση το δυαδικό μήκος όλων των συντελεστών του $\mathtt{res}(A, B)$ είναι $\mathcal{O}(p\tau)$, για παράδειγμα αν $\mathtt{res}(A, B) \in \mathbb{Z}$.

Μπορούμε να χρησιμοποιήσουμε την ακολουθία πηλίκων προκειμένου να υπολογίσουμε την αποτίμηση της $\mathbf{SR}(A, B)$ πάνω σε κάποιο αριθμό [65, 241, 247]. Η αποτίμηση πρέπει να αρχίσει από το τελευταίο στοιχείο της ακολουθίας υπολοίπων. Το επόμενο θεώρημα [175, 222] μας παρέχει την πολυπλοκότητα αυτού του υπολογισμού.

Θεώρημα 2.32

Ο υπολογισμός της αποτίμησης της $\mathbf{SR}(A, B)$ πάνω σε ένα αριθμό $\mathsf{a} \in \mathbb{Q} \cup \{\pm\infty\}$, $\mathcal{L}(\mathsf{a}) = \sigma$, $\mathbf{SR}(A, B\,;\, \mathsf{a})$, έχει πολυπλοκότητα $\mathcal{O}_B(q\ \lg(q)\,\mathsf{M}(\max(p\tau, q\sigma)))$ ή $\mathcal{O}_B(q\,\mathsf{M}(\max(p\tau, q\sigma)))$ εάν η $\mathbf{SRQ}(A, B)$ δεν είναι ήδη υπολογισμένη.

Και στις δύο περιπτώσεις η πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(q \max\{p\tau, q\sigma\})$.

Σημείωση 2.33. *Σε πολλές περιπτώσεις (π.χ απομόνωση πραγματικών ριζών, σύγκριση πραγματικών αλγεβρικών αριθμών) χρειάζεται να υπολογίσουμε την αποτίμηση $\mathbf{SR}(A, B\,;\, \mathsf{a})$, όπου $\mathcal{L}(\mathsf{a}) = \mathcal{O}(p\tau)$. Εάν υπολογίσουμε την αποτίμηση εφαρμόζοντας διαδοχικά τον κανόνα του Horner τότε αφού υπάρχουν $\Omega(q^2)$ συντελεστές στην ακολουθία και πρέπει να πολλαπλασιάσουμε αριθμούς δυαδικού μήκους $\mathcal{O}(p\tau)$ και $\mathcal{O}(p^2\tau)$, η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(p^2q^2\tau)$.*

Ωστόσο, ακόμα και όταν υπάρχει η ανάγκη υπολογισμού της ακολουθίας $\mathbf{SR}(A, B)$ η ακολουθία $\mathbf{SRQ}(A, B)$ μπορεί να υπολογιστεί με την ίδια πολυπλοκότητα [14, 222]. Οπότε μπορούμε πάντοτε να χρησιμοποιήσουμε την ακολουθία πηλίκων για αποτιμήσεις.

Το $A \in \mathcal{R}[X]$ λέμε ότι είναι χωρίς τετράγωνα αν $\deg(\gcd(A, A')) = 0$. Ή διαφορετικά, το A δεν έχει ρίζες πολλαπλότητας > 1 στο $\mathcal{K}$. Ορίζουμε το χωρίς τετράγωνα μέρος του A ως

$$A_{red} = \frac{A}{\gcd(A, A')}$$

Παρατηρούμε ότι η διαίρεση είναι καλώς ορισμένη στο $\mathcal{R}[X]$, δηλαδή είναι μια τέλεια διαίρεση χωρίς υπόλοιπο. Για τον υπολογισμό του χωρίς τετράγωνα μέρους του A, ισχύει το ακόλουθο θεώρημα [14, Algorithm 10.17, p. 326]:

Θεώρημα 2.34

Αν $A \in \mathbb{Z}[X]$ τέτοιο ώστε $\deg(A) = p$ και $\mathcal{L}(A) = \tau$, τότε το χωρίς τετράγωνα μέρος του A, A_{red}, μπορεί να υπολογιστεί από την ακολουθία $\mathbf{SR}(A, A')$, με πολυπλοκότητα $\mathcal{O}_B(p \lg p \mathsf{M}(p\tau))$ ή $\widetilde{\mathcal{O}}_B(p^2\tau)$. Επιπρόσθετα, $\mathcal{L}(A_{red}) = \mathcal{O}(p + \tau)$.

Σημείωση 2.35. *Υπάρχει ένα βήμα κανονικοποίησης [14] στον υπολογισμό του τελευταίου στοιχείου της ακολουθίας* $\mathbf{SR}(A, A^{'})$ *και γι' αυτό επιτυγχάνουμε* $\mathcal{L}\left(A_{red}\right) = \mathcal{O}(p + \tau)$. *Εάν χρησιμοποιούσαμε το γενικό φράγμα για τις ακολουθίες υπο-επιλυουσών ή το φράγμα του Mignotte [187] σχετικά με το δυαδικό μήκος των συντελεστών των διαιρετών ενός πολυωνύμου τότε θα συν άγαμε ότι* $\mathcal{L}\left(A_{red}\right) = \mathcal{O}(p\tau)$.

2.4 Πολυώνυμα στη βάση Bernstein

Όλα τα πολυώνυμα βαθμού $\leq d$ στο $\mathbb{R}[X]$ αποτελούν ένα διανυσματικό χώρο διάστασης d πάνω στο $\mathbb{R}$. Η συνήθης αναπαράσταση των πολυωνύμων, Εξ. (2.1), είναι κάποιος γραμμικός συνδυασμός των στοιχειωδών πολυωνύμων $\{1, X, \ldots, X^d\}$. Αυτά τα στοιχειώδη πολυώνυμα αποτελούν και (μία) βάση του διανυσματικού χώρου η οποία ονομάζεται *βάση δυνάμεων* (power basis).

Ωστόσο, μπορούμε να αναπαραστήσουμε τα πολυώνυμα χρησιμοποιώντας άλλες βάσεις. Στην παρούσα παράγραφο παρουσιάσουμε συνοπτικά τη βάση Bernstein για την αναπαράσταση των πολυωνύμων. Η αναπαράσταση σε βάση Bernstein είναι αριθμητικά ευσταθής σε αντίθεση με τη βάση δυνάμεων που είναι αριθμητικά ασταθής. Αυτός είναι και ο λόγος που έχει πολύ μεγάλη πρακτική σημασία. Θα πρέπει ωστόσο να τονίσουμε ότι η διαδικασία μετατροπής από τη βάση των δυνάμεων στη βάση Bernstein και το αντίστροφο είναι διαδικασίες αριθμητικά ασταθείς. Για περισσότερες λεπτομέρειες και για μια πιο εκτενή περιγραφή της βάσης Bernstein και των ιδιοτήτων της ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία, π.χ [102, 103, 104].

Έστω $\mathbb{R}[X]_d$ το σύνολο των πραγματικών πολυωνύμων βαθμού $\leq d$. Έστω $a < b \in \mathbb{R}$, συμβολίζουμε με

$$\mathfrak{B}_d^i(X; a, b) = \binom{d}{i} \frac{(X-a)^i (b-X)^{d-1}}{(b-a)^d} \quad i = 0, \ldots, d$$

τη βάση Bernstein των $\mathbb{R}[X]_d$ στο διάστημα $[a, b]$.

Για κάθε πολυώνυμο $f \in \mathbb{R}[X]_d = \sum_{i=0}^{d} b_i \mathfrak{B}_d^i(X; a, b)$, το οποίο αναπαρίσταται στη βάση Bernstein, οι συντελεστές $\mathbf{b} = (b_i)_{i=0,\ldots,d}$ ονομάζονται *συντελεστές ελέγχου* (*control coefficients*) του f. Συμβολίζουμε με $\mathtt{VAR}(f) \equiv \mathtt{VAR}(\mathbf{b})$, το πλήθος των εναλλαγών προσήμου. στην ακολουθία $\mathbf{b}$ των συντελεστών (αφού αφαιρέσουμε τα μηδενικά).

Δοθέντος πολυωνύμου f με αναπαράσταση στη βάση Bernstein στο διάστημα $\mathcal{I} = [a, b]$, ο αλγόριθμος του de Casteljau, δείτε για παράδειγμα [14, 205], μας επιτρέπει να υπολογίσουμε την αναπαράσταση του f σε δύο υποδιαστήματα του $\mathcal{I}$, $\mathcal{I}_L = [a, (1-t)a + tb]$ και $\mathcal{I}_R = [(1-t)a + tb, b]$, όπου $0 \leq t \leq 1$. Πιο συγκεκριμένα, $\mathbf{b}_L = (b_0^i)_{i=0,\ldots,d}$ (αντίστοιχα $\mathbf{b}_R = (b_i^{d-i})_{i=0,\ldots,d}$) είναι οι συντελεστές ελέγχου του f στο I_L (αντίστοιχα I_R), όπου $b_i^0 = b_i, i = 0, \ldots, d$, και

$$b_i^r = (1-t)\, b_i^{r-1} + t\, b_{i+1}^{r-1}(t), \quad 0 \leq i \leq d-r,\ 0 \leq r \leq d. \tag{2.18}$$

Προκειμένου να αναλύσουμε την πολυπλοκότητα του αλγορίθμου του de Casteljau αναφέρουμε μερικούς πολυωνυμικούς μετασχηματισμούς που σχετίζονται με αναπαράσταση στη βάση

Bernstein. Ο αναγνώστης μπορεί να ανατρέξει στους Mourrain et al. [205] για περισσότερες λεπτομέρειες.

Έστω $\mathbb{R}[X,Y]_{[d]}$ το σύνολο όλων των ομογενών πολυωνύμων βαθμού d με μεταβλητές (X,Y). Για κάθε $f \in \mathbb{R}[X]_d$, συμβολίζουμε με $\overline{f}$ την ομογενοποίηση του f στο βαθμό d. Για $\lambda \neq 0, \mu \in \mathbb{R}$ θεωρούμε τις ακόλουθες απεικονίσεις $\mathbb{R}^2 \to \mathbb{R}^2$:

- $\mathcal{R} : (X,Y) \mapsto (Y,X)$,
- $\mathcal{H}_\lambda : (X,Y) \mapsto (\lambda X, Y)$,
- $\mathcal{H}'_\lambda : (X,Y) \mapsto (X, \lambda Y)$,
- $\mathcal{T}_\mu : (X,Y) \mapsto (X - \mu Y, Y)$,
- $\mathcal{T}'_\mu : (X,Y) \mapsto (X, Y - \mu X)$.

Η σύνθεση των παραπάνω απεικονίσεων με το $\overline{f}$ παράγει αντιστρέψιμες απεικονίσεις πάνω στο σύνολο των πολυωνύμων βαθμού d και οι αντίστοιχες απεικονίσεις στα μη ομογενή πολυώνυμα τις οποίες και θα συμβολίσουμε με τα ίδια σύμβολα είναι, $\forall f \in \mathbb{R}[X]_d$:

- $\mathcal{R}(f) = X^d f(1/X)$,
- $\mathcal{H}_\lambda(f) = f(\lambda X)$,
- $\mathcal{H}'_\lambda(f) = f(\lambda^{-1} X)$,
- $\mathcal{T}_\mu(f) = f(X - \mu)$,
- $\mathcal{T}'_\mu(f) = (1 - \mu\, X)^d f(\frac{X}{1-\mu\, X})$.

Για κάθε πολυώνυμο $f(X) = \sum_{i=0}^d b_i \mathfrak{B}_d^i(X;a,b)$, έχουμε

$$\mathcal{R} \circ \mathcal{T}_1 \circ \mathcal{R} \circ \mathcal{H}_{b-a} \circ \mathcal{T}_{-a}(f) = \sum_{i=0}^{d} \binom{d}{i} b_i X^i.$$

Ας θεωρήσουμε ένα διάστημα $[c,d]$. Η αναπαράσταση του f στη βάση Bernstein στο $[c,d]$ είναι $f(X) = \sum_{i=0}^d b'_i \mathfrak{B}_d^i(X;c,d)$. Η απεικόνιση η οποία μετασχηματίζει το f από τη βάση Bernstein στο διάστημα $[a,b]$ στη βάση Bernstein στο διάστημα $[c,d]$, δηλαδή από το $\sum_{i=0}^d \binom{d}{i} b_i X^i$ στο $\sum_{i=0}^d \binom{d}{i} b'_i X^i$ είναι

$$\mathcal{R} \circ \mathcal{T}_1 \circ \mathcal{R} \circ \mathcal{H}_{d-c} \circ \mathcal{T}_{-c} \circ \mathcal{T}_a \circ \mathcal{H}_{\frac{1}{b-a}} \circ \mathcal{R} \circ \mathcal{T}_{-1} \circ \mathcal{R} = \mathcal{T}'_1 \circ \mathcal{H}_{d-c} \circ \mathcal{T}_{a-c} \circ \mathcal{H}_{\frac{1}{b-a}} \circ \mathcal{T}'_{-1} \tag{2.19}$$

Αν θεωρήσουμε $[a,b] = [0,1]$ και $[c,d] = [0,\frac{1}{2}]$ τότε η απεικόνιση (2.19) γίνεται: $\mathcal{R} \circ \mathcal{T}_{-1} \circ \mathcal{R} \circ \mathcal{H}_{\frac{1}{2}} \circ \mathcal{R} \circ \mathcal{T}_1 \circ \mathcal{R}$. Μετά από απλοποιήσεις, έχουμε

$$\mathcal{S}_L : \overline{f} \mapsto \overline{f}\left(X + \frac{Y}{2}, \frac{Y}{2}\right) = \overline{f} \circ \mathcal{T}_{-1} \circ \mathcal{H}'_{\frac{1}{2}}. \tag{2.20}$$

Αν θεωρήσουμε τη συμμετρική περίπτωση, δηλαδή $[a,b] = [0,1]$ και $[c,d] = [\frac{1}{2},1]$ τότε η απεικόνιση (2.19) γίνεται: $\mathcal{R}\circ\mathcal{T}_{-1}\circ\mathcal{R}\circ\mathcal{H}_{\frac{1}{2}}\circ\mathcal{T}_{-\frac{1}{2}}\circ\mathcal{R}\circ\mathcal{T}_1\circ\mathcal{R}$. Η οποία αντιστοιχεί στην ακόλουθη απεικόνιση στα ομογενή πολυώνυμα:

$$\mathcal{S}_R : \overline{f} \mapsto \overline{f}\left(\frac{X}{2}, \frac{X}{2}+Y\right) = \overline{f}\circ\mathcal{T}'_{-1}\circ\mathcal{H}_{\frac{1}{2}}. \tag{2.21}$$

Και στις δύο περιπτώσεις, αν πολλαπλασιάσουμε με 2^d παράγουμε την απεικόνιση $\overline{\mathcal{S}}_R : \overline{p} \mapsto \overline{p}(X, X+2Y)$, (αντίστοιχα $\overline{\mathcal{S}}_L : \overline{p} \mapsto \overline{p}(2X+Y, Y)$), η οποία ενεργεί σε πολυώνυμα με ακέραιους συντελεστές.

Η επόμενη πρόταση μας επιτρέπεινα υλοποιήσουμε τη διάσπαση ενός πολυωνύμου σε δύο υποδιαστήματα με την εφαρμογή μετασχηματισμών μετατόπισης.

Πρόταση 2.36. *Έστω $(b_i)_{i=0,\ldots,d} \in \mathbb{Z}^{d+1}$ οι συντελεστές ενός πολυωνύμου f στη βάση Bernstein στο διάστημα $[a,b]$, και έστω ν ένα φράγμα στο δυαδικό μήκος των συντελεστών. Η πολυπλοκότητα του υπολογισμού των συντελεστών στη βάση Bernstein του f πάνω στα δύο υποδιαστήματα $[a, \frac{a+b}{2}]$ και $[\frac{a+b}{2}, b]$ φράσσεται από $\widetilde{\mathcal{O}}_B(d(d+\nu))$ και το δυαδικό μήκος των συντελεστών από $d+\nu$.*

Απόδειξη: Χρησιμοποιώντας το σχήμα του de Casteljau, Εξ. (2.18) με $t = \frac{1}{2}$, αποδεικνύουμε με επαγωγή ότι οι συντελεστές $b_i^r = \frac{(b_i^{r-1} + b_{i+1}^{r-1})}{2}$ είναι της μορφής $\frac{\overline{b}_i^r}{2^i}$, όπου $\overline{b}_i^r \in \mathbb{Z}$ είναι δυαδικού μήκους $\leq \nu + r$. Θέτοντας τον ίδιο παρανομαστή 2^d προκύπτουν ακέραιοι συντελεστές μήκους $\leq \nu + d$.

Συμβολίζουμε με ν' το μήκος των συντελεστών $\left(\binom{d}{i} b_i\right)_{i=0,\ldots,d}$ όπου $(b_i)_{i=0,\ldots,d}$ είναι οι συντελεστές του f στη βάση Bernstein $(\mathfrak{B}_d^i(X;a,b))_{i=0,\ldots,d}$. Παρατηρούμε ότι $\nu' \leq \nu + d$.

Για τον υπολογισμό των συντελεστών του f στα διαστήματα $[a, \frac{a+b}{2}]$ και $[\frac{a+b}{2}, b]$, εφαρμόζουμε τις ίδιες απεικονίσεις όπως όταν υπολογίζαμε τους συντελεστές ενός πολυωνύμου στη βάση Bernstein στα διαστήματα $[0, \frac{1}{2}]$ και $[\frac{1}{2}, 1]$, δοθέντος της αναπαράστασης σε βάση Bernstein στο διάστημα $[0,1]$.

Σύμφωνα με την Εξ. (2.20), η εκτέλεση του αλγόριθμου de Casteljau αντιστοιχεί αρχικά στον πολλαπλασιασμό με τους διωνυμικούς συντελεστές, στη συνέχεια σε μια μετατόπιση $Y \to X+Y$, σε μια κλιμάκωση της μιας μεταβλητής του ομογενούς πολυωνύμου $\overline{f}$ κατά $\frac{1}{2}$ και τέλος σε μια διαίρεση με τους διωνυμικούς συντελεστές[1].

Εφόσον το δυαδικό μήκος των δυωνυμικών συντελεστών φράσσεται από d (το άθροισμά τους είναι 2^d), πολλαπλασιάζοντας τους με b_i κοστίζει το πολύ $\widetilde{\mathcal{O}}_B(d(\nu+d))$. Η μετατόπιση κατά 1 ενός πολυωνύμου βαθμού d με συντελεστές δυαδικού μήκους $\leq \nu + d$ απαιτεί $\widetilde{\mathcal{O}}_B(d(d+\nu))$ [262] και παράγει ένα πολυώνυμο με συντελεστές μήκους $\mathcal{O}(\nu+d)$. Συνεπώς η μετατόπιση του πολυωνύμου κατά $\frac{1}{2}$ και ο υπολογισμός του πηλίκου με τους διωνυμικούς συντελεστές απαιτεί $\widetilde{\mathcal{O}}_B(d(\nu+d))$ δυαδικές πράξεις..

Κατά συνέπεια, η πολυπλοκότητα του υπολογισμού των συντελεστών Bernstein του f στο υποδιάστημα $[a, \frac{a+b}{2}]$ φράσσεται από $\widetilde{\mathcal{O}}_B(d(\nu+d))$. Εκ συμμετρίας, αντιστρέφοντας τους συντελεστές του f, προκύπτει το ίδιο φράγμα για τους συντελεστές του f στο $[\frac{a+b}{2}, b]$.

Έτσι ολοκληρώνεται η απόδειξη. ΟΕΔ

2.5 Σύνοψη – Μελλοντικές επεκτάσεις

Το κεφάλαιο περιέχει τις βασικές αλγεβρικές και αλγοριθμικές έννοιες που απαιτούνται για την κατανόηση της διατριβής. Παρουσιάμε την πολυπλοκότητα των βασικών πράξεων με ακέραιους αριθμούς και πολυώνυμα σε μία μεταβλητή, την έννοια της επιλύουσας και της διακρίνουσας και τις ακολουθίες πολυωνυμικών υπολοίπων. Τέλος, παρουσιάσαμε συνοπτικά την αναπαράσταση των πολυωνύμων στη βάση Bernstein και αποδείξαμε ότι δοθέντος ενός πολυωνύμου στη βάση Bernstein σε κάποιο διάστημα, ο υπολογισμός των συντελεστών του σε δύο υποδιαστήματα του αρχικού διαστήματος ανάγεται σε δύο μετατοπίσεις κατά 1 και άρα η πολυπλοκότητά του είναι αυτή της μετατόπισης.

Όπως γίνεται εύκολα κατανοητό από τον αναγνώστη η περιοχή των (προσημασμένων) πολυωνυμικών ακολουθιών υπολοίπων είναι τεράστια με πολλούς, μερικές φορές αντικρουόμενους, ορισμούς και δεκάδες θεωρήματα. Θεωρούμε ως μεγάλη επιστημονική πρόκληση τη πρόταση μιας θεωρίας που να ενοποιεί και να απλοποιεί τις παρούσες προσεγγίσεις. Επίσης μια ενδελεχής πειραματική μελέτη των διαφόρων αλγορίθμων υπολογισμού των ακολουθιών υπολοίπων πρέπει να είναι από τις πρώτες προτεραιότητες.

Το μεγαλύτερο ανοιχτό πρόβλημα αφορά τον υπολογισμό της επιλύουσας δύο πολυωνύμων. Δοθέντων δύο πολυωνύμων βαθμού d και δυαδικού μήκους τ, οι καλύτεροι μέχρι σήμερα αλγόριθμοι υπολογίζουν την επιλύουσα με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2\tau)$ [175, 222]. Ωστόσο, η επιλύουσα έχει δυαδικό μήκος $\mathcal{O}(d\tau)$ στη χειρότερη περίπτωση. Υπάρχει αλγόριθμος, έστω και πιθανοτικός, που να υπολογίζει την επιλύουσα δύο πολυωνύμων με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d\tau)$;

ΚΕΦΑΛΑΙΟ 3

Πραγματική επίλυση πολυωνύμων σε μία μεταβλητή

> Ομαδοποίησε τους υπολογισμούς. Ταξινόμησέ τους ανάλογα με την πολυπλοκότητά τους και όχι σύμφωνα με τη μορφή τους. Αυτή νομίζω είναι η αποστολή των μελλοντικών μαθηματικών.
>
> Evariste Galois

Περίληψη

Δοθέντος ενός ακέραιου πολυωνύμου, όχι απαραίτητα χωρίς τετράγωνα, σε μία μεταβλητή παρουσιάζουμε αλγορίθμους για τον υπολογισμό διαστημάτων με ρητά άκρα που απομονώνουν τις πραγματικές ρίζες του και υπολογίζουν τις πολλαπλότητές τους.

Τα πρωτότυπα αποτελέσματα του κεφαλαίου αφορούν τη μελέτη της ποιότητας των φραγμάτων για τις θετικές πραγματικές ρίζες, ένα θεώρημα για τα σύνθετα φράγματα διαχωρισμού, την ενοποίηση και απλοποίηση της θεωρίας για τους αλγορίθμους επίλυσης πολυωνύμου που βασίζονται στην υποδιαίρεση και τη βελτίωση της πολυπλοκότητας κατά δύο παράγοντες του αλγορίθμου των συνεχών φραγμάτων. Επιπρόσθετα, για όλους τους αλγορόιθμους επίλυσης, αποδεικνύουμε ότι το φράγμα πολυπλοκότητας ισχύει και για πολυώνυμα με τετράγωνα και ότι με την ίδια πολυπλοκότητα υπολογίζουμε και την πολλαπλότητα των ριζών. Μέρος των αποτελεσμάτων παρουσιάστηκε στις εργασίες [97, 252, 253].

Η επίλυση πολυωνυμικών εξισώσεων είναι ένα από τα παλαιότερα και πιο γνωστά προβλήματα στα μαθηματικά. Οι προσπάθειες επίλυσης της πολυωνυμικής εξίσωσης αποτέλεσαν τη γεννησιουργό αιτία για πολλές από τις πιο σημαντικές μαθηματικές έννοιες. Ενδεικτικά αναφέρουμε τους άρρητους και τους μιγαδικούς αριθμούς, τη θεωρία ομάδων, την έννοια του σώματος και του ιδεώδους, τη θεωρία των συμμετρικών συναρτήσεων και την επιλύουσα.

Στη σύγχρονη ιστορία των μαθηματικών η επίλυση της πολυωνυμικής εξίσωσης δεν κατέχει τον κεντρικό ρόλο που κατείχε στους περασμένους αιώνες, αν και εξακολουθεί να αποτελεί το κεντρικό πρόβλημα για τους ερευνητές στις περιοχές της αριθμητικής ανάλυσης και της υπολογιστικής άλγεβρας, τουλάχιστον. Ο αναγνώστης που ενδιαφέρεται για την ιστορική εξέλιξη της επίλυσης της πολυωνυμικής εξίσωσης, κυρίως από τη σκοπιά της αριθμητικής ανάλυσης, μπορεί να ανατρέξει στις εργασίες του Pan [210, 211]. Επίσης σχεδόν όλες οι εργασίες σχετικά με την επίλυση πολυωνυμικών εξισώσεων περιέχονται στην ιστοσελίδα του John Michael McNamee[1], δείτε επίσης [183, 184, 185].

Τα τελευταία 20 με 30 χρόνια η επίλυση, ή πιο σωστά, οι αλγόριθμοι επίλυσης της πολυωνυμικής εξίσωσης βρίσκονται ξανά στο επίκεντρο καθώς πολλές επιστημονικές περιοχές, όπως η μη γραμμική υπολογιστική γεωμετρία, η σχεδίαση με υπολογιστή, η γεωμετρική μοντελοποίηση, τα συστήματα γεωγραφικών πληροφοριών και η ρομποτική έχουν επικεντρωθεί σε προβλήματα με καμπύλα αντικείμενα ή/και σε προβλήματα που περιέχουν μη γραμμικότητες πολυωνυμικής μορφής. Σε τέτοια προβλήματα η επίλυση της πολυωνυμικής εξίσωσης παίζει πολύ σημαντικό ρόλο τόσο από θεωρητική όσο από πρακτική άποψη.

Πώς ορίζεται όμως η πολυωνυμική εξίσωση και τί εννούμε με τον όρο επίλυση;

Σε ό,τι θα ακολουθήσει θα θεωρήσουμε το πολυώνυμο $A \in \mathcal{R}[X]$, όπου $\mathcal{R}$ κάποιος υποδακτύλιος του $\mathbb{C}$, και

$$A(X) = a_d\, X^d + a_{d-1}\, X^{d-1} + \cdots + a_1\, X + a_0 \tag{3.1}$$

Προκειμένου να αποφύγουμε εκφυλισμένες περιπτώσεις θεωρούμε $a_d\, a_0 \neq 0$. Αν $A \in \mathbb{Z}[X]$ τότε $\mathcal{L}(A) = \tau$. Η πολυωνυμική εξίσωση είναι η εξίσωση

$$A(X) = 0$$

Με τον όρο επίλυση εννοούμε τον υπολογισμό αριθμών γ, τέτοιων ώστε να ισχύει $A(\gamma) = 0$. Αυτοί οι αριθμοί ονομάζονται ρίζες (roots) της πολυωνυμικής εξίσωσης. Το θεμελιώδες θεώρημα της άλγεβρας (Fundamental theorem of algebra), το οποίο διατυπώθηκε αρχικά από τον Descartes και του οποίου η πρώτη (ημιτελής) απόδειξη παρουσιάστηκε στη διδακτορική διατριβή του Gauss, μας εξασφαλίζει ότι το πολυώνυμο έχει ακριβώς τόσες (μιγαδικές) ρίζες όσες και ο βαθμός του, αν μετρήσουμε και τις πολλαπλότητές τους. Δηλαδή υπάρχουν μιγαδικοί αριθμοί $\gamma_1, \ldots, \gamma_d \in \mathbb{C}$ τέτοιοι ώστε η (3.1) να γράφεται ως

$$A(X) = a_d \prod_{i=1}^{d} (X - \gamma_i)$$

Αν ενδιαφερόμαστε για τον υπολογισμό μόνο των πραγματικών ριζών τότε χρησιμοποιούμε τον όρο πραγματική επίλυση. Σχετικά με το θεμελιώδες θεώρημα της άλγεβρας ο αναγνώστης μπορεί να ανατρέξει για παράδειγμα στους van der Waerden [258] και Uspensky [255].

Στην παρούσα διατριβή θα ασχοληθούμε με την πραγματική επίλυση ακέραιων πολυωνύμων, δηλαδή $A \in \mathbb{Z}[X]$. Οι αριθμοί που προκύπτουν ως λύσεις ακεραίων πολυωνύμων ονομάζονται αλγεβρικοί αριθμοί και αν είναι πραγματικοί τότε ονομάζονται πραγματικοί αλγεβρικοί αριθμοί. Πιο συγκεκριμένα

[1] `www1.elsevier.com/homepage/sac/cam/mcnamee/`

Ορισμός 3.1. *Ένας πραγματικός αριθμός ονομάζεται πραγματικός αλγεβρικός αριθμός αν είναι ρίζα κάποιου πολυωνύμου με ακέραιους συντελεστές.*

Το σύνολο των πραγματικών αλγεβρικών αριθμών είναι σώμα και το συμβολίζουμε με $\mathbb{R}_{alg}$. Το $\mathbb{R}_{alg}$ είναι αριθμήσιμο και ισχύει

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}_{alg} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Αν $\gamma \in \mathbb{R}_{alg}$ τότε από όλα τα πολυώνυμα $A \in \mathbb{Z}[X]$ για τα οποία ισχύει $A(\gamma) = 0$, εκείνα με τον ελάχιστο βαθμό ονομάζονται ελαχιστικά (minimal) πολυώνυμα του γ. Αν επιπλέον απαιτήσουμε το πολυώνυμο να είναι πρωταρχικό (primitive) τότε ονομάζεται ελάχιστο (minimum) πολυώνυμο του γ. Ο βαθμός του γ, $\deg(\gamma)$, είναι ο βαθμός του ελάχιστου πολυωνύμου του και αν $\gamma = 0$ τότε εξ ορισμού το ελάχιστο πολυώνυμο είναι το $A = 0$ και $\deg(\gamma) = -\infty$. Αν το A έχει και άλλες (μιγαδικές) ρίζες εκτός από το γ τότε αυτοί οι αριθμοί ονομάζονται συζυγείς (conjugate) του γ.

Κατά συνέπεια το πρόβλημα της επίλυσης της πολυωνυμικής εξίσωσης είναι (σχεδόν) ισοδύναμο με το πρόβλημα της κατασκευής των στοιχείων του $\mathbb{R}_{alg}$. Οπότε τίθεται το ερώτημα: Πώς αναπαριστούμε τα στοιχεία του $\mathbb{R}_{alg}$ ή ισοδύναμα ποιά είναι η έξοδος των αλγορίθμων πραγματικής επίλυσης πολυωνυμικών εξισώσεων;

Για να απαντήσει στα παραπάνω ερωτήματα, η αλγεβρική προσέγγιση υπολογίζει τις λύσεις μιας πολυωνυμικής εξίσωσης με τη βοήθεια των βασικών πράξεων και ριζικών. Η προσέγγιση αυτή στη γενική περίπτωση, όπως απέδειξαν οι εργασίες των Abel και Galois δεν μπορεί να επιλύσει πολυώνυμα βαθμού μεγαλύτερου από 4.

Η αριθμητική προσέγγιση υπολογίζει κάποια προσέγγιση στις ρίζες μέχρι κάποια ακρίβεια, η οποία είτε είναι είσοδος στον αλγόριθμο είτε είναι το φράγμα διαχωρισμού (Εν. 3.2) και βασίζεται σε αριθμούς κινητής υποδιαστολής. Χαρακτηριστικά παραδείγματα αυτής της προσέγγισης είναι οι εργασίες των Pan [210, 213, 214], Renegar [223], Schönhage [239]. Ο αναγνώστης μπορεί επίσης να ανατρέξει στους Henrici [131], Marden [181], Obreschkoff [207], Ostrowski [209], Ralston and Rabinowitz [221], Stetter [246] για περισσότερα αποτελέσματα σχετικά με μεθόδους και αλγορίθμους αριθμητικής επίλυσης.

Οι αλγόριθμοι πραγματικής επίλυσης ακέραιων πολυωνύμων σε μία μεταβλητή, που θα μας απασχολήσουν, έχουν ως έξοδο διαστήματα με άκρα ρητούς αριθμούς που θα περιέχουν μία και μόνο μία ρίζα του $A(X)$ και εμπεριέχουν πράξεις μόνο με ακεραίους απεριόριστης ακρίβειας. Τα διαστήματα αυτά ονομάζονται *διαστήματα απομόνωσης* και οι αλγόριθμοι ονομάζονται *αλγόριθμοι απομόνωσης*. Ο διαχωρισμός του προβλήματος της προσέγγισης από το πρόβλημα της απομόνωσης των (πραγματικών) ριζών ενός πολυωνύμου, πιθανόν οφείλεται στον Lagrange [167], χωρίς ωστόσο να παραγνωρίσουμε τη συμβολή των Fourier [107], Sturm [248], Vincent [261]. Στη σύγχρονη εκδοχή τους οι αλγόριθμοι απομόνωσης παρουσιάστηκαν από τους Uspensky [255], Collins and Loos [55] και Collins and Akritas [52]. Θα επανέλθουμε στις σχετικές εργασίες για αλγορίθμους απομόνωσης στη συνέχεια του κεφαλαίου. Επιπρόσθετα, οι αλγόριθμοι που θα παρουσιάσουμε υπολογίζουν και τις πολλαπλότητές των πραγματικών ριζών εκτός από τα διαστήματα απομόνωσης τους. Όσον αφορά στην αναπαράσταση των στοιχείων του $\mathbb{R}_{alg}$ θα την παρουσιάσουμε αναλυτικά στο επόμενο κεφάλαιο.

Συνοψίζοντας και υιοθετώντας την ορολογία του Yap [275], το παρόν κεφάλαιο ασχολείται με το *θεμελιώδες υπολογιστικό πρόβλημα της άλγεβρας*.

Τι θα ακολουθήσει

Αρχικά παρουσιάζουμε το μέτρο Mahler για πολυώνυμα και πραγματικούς αλγεβρικούς αριθμούς και διαφόρων ειδών φράγματα στις πραγματικές και μιγαδικές ρίζες ενός πολυωνύμου. Στη συνέχεια παρουσιάζουμε ένα αλγόριθμο για τον υπολογισμό των πολλαπλοτήτων των πραγματικών ριζών ενός πολυωνύμου. Τέλος, παρουσιάζουμε αλγορίθμους για την απομόνωση των πραγματικών ριζών. Πιο συγκεκριμένα παρουσιάζουμε τον αλγόριθμο του Kronecker, τους αλγορίθμους υποδιαίρεσης STURM, DESCARTES και BERNSTEIN και τον αλγόριθμο των συνεχών κλασμάτων CF.

3.1 Μέτρο Mahler

Θα παρουσιάσουμε το μέτρο Mahler [180] πολυωνύμων και αλγεβρικών αριθμών. Για τις αποδείξεις των θεωρημάτων που παραλείπουμε ο αναγνώστης μπορεί να ανατρέξει στους Mignotte [187] και Mignotte and Stefanescu [190].

Ορισμός 3.2 (μέτρο Mahler). *[180] Έστω $A \in \mathbb{C}[X] \setminus \mathbb{C}$, τέτοιο ώστε*

$$A = \sum_{i=0}^{d} a_i X^i = a_d (X - \gamma_1) \cdots (X - \gamma_d)$$

όπου $a_d \neq 0$. Το μέτρο Mahler του A, το οποίο συμβολίζουμε ως $\mathcal{M}(A)$, ορίζεται ως

$$\mathcal{M}(A) = |a_d| \prod_{j=1}^{d} \max\{1, |\gamma_j|\}$$

Για το μέτρο Mahler ισχύουν οι ακόλουθες ιδιότητες:

Λήμμα 3.3. *Έστω $A, B \in \mathbb{C}[X] \setminus \mathbb{C}$, τέτοια ώστε το μέτρο Mahler να ορίζεται, $\deg(A) = d$ και $k \in \mathbb{N}^*$, τότε*

1. $\mathcal{M}\left(X^d A(\frac{1}{X})\right) = \mathcal{M}(A(X))$
2. $\mathcal{M}(A \cdot B) = \mathcal{M}(A) \cdot \mathcal{M}(B)$
3. $\mathcal{M}\left(A(X^k)\right) = \mathcal{M}(A(X))$

Απόδειξη: Θεωρούμε, χωρίς βλάβη της γενικότητας, ότι τα A και B δεν έχουν ούτε το 0 ως ρίζα, ούτε κάποια ρίζα μέτρου 1. Έστω $A = \sum_{i=0}^{d} a_i X^i$ και $B = \sum_{i=0}^{p} b_i X^i$ των οποίων οι (μιγαδικές) ρίζες είναι:

$$\begin{array}{ccccccccccc} |\alpha_1| & \leq & \ldots & \leq & |\alpha_k| & < & 1 & < & |\alpha_{k+1}| & \leq & \ldots & \leq & |\alpha_d| \\ |\beta_1| & \leq & \ldots & \leq & |\beta_l| & < & 1 & < & |\beta_{l+1}| & \leq & \ldots & \leq & |\beta_p| \end{array}$$

Προκειμένου να αποδείξουμε την πρώτη ανισότητα, υπενθυμίζουμε ότι οι συντελεστές του πολυωνύμου είναι συμμετρικές πολυωνυμικές συναρτήσεις των ριζών [187, 190, 275] και ως εκ τούτου ο σταθερός όρος είναι το γινόμενο των (μιγαδικών) ριζών, αν το πολυώνυμο είναι μονικό.

Συνεπώς για το A ισχύει ότι $\prod_{i=1}^{d} |\alpha_i| = \left|\frac{a_0}{a_d}\right|$. Επίσης, το $X^d A(\frac{1}{X}) = a_0\, X^d + \cdots + a_{d-1}X + a_d$ έχει (μιγαδικές) ρίζες

$$\frac{1}{|\alpha_d|} \leq \cdots \leq \frac{1}{|\alpha_{k+1}|} < 1 < \frac{1}{|\alpha_k|} \leq \cdots \leq \frac{1}{|\alpha_1|}$$

Άρα

$$\begin{aligned} \mathcal{M}(A) &= |a_d| \cdot |\alpha_{k+1}| \cdots |\alpha_d| \\ &= |a_d| \left|\frac{a_0}{a_d}\right| \left|\frac{1}{\alpha_1}\right| \cdots \left|\frac{1}{\alpha_k}\right| \quad = |a_0| \left|\frac{1}{\alpha_1}\right| \cdots \left|\frac{1}{\alpha_k}\right| \\ &= \mathcal{M}\left(X^d A\left(\frac{1}{X}\right)\right) \end{aligned}$$

Όσον αφορά τη δεύτερη ανισότητα, οι μιγαδικές ρίζες του $A \cdot B$ είναι $\{\alpha_i\}_{1\leq i\leq d} \cup \{\beta_j\}_{1\leq j\leq p}$. Επίσης ισχύει ότι $\mathsf{lead}(A \cdot B) = a_d \cdot b_p$. Συνεπώς

$$\mathcal{M}(A \cdot B) = a_d b_p \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \prod_{j=1}^{p} \max\{1, |\beta_j|\} = \mathcal{M}(A) \cdot \mathcal{M}(B)$$

Η τελευταία ανισότητα είναι τετριμμένη. ΟΕΔ

Η δεύτερη ιδιότητα του Λημ. 3.4 αναδεικνύει και την σπουδαιότητα του μέτρου Mahler καθώς, σε αντίθεση με άλλες μετρικές, είναι συμβατό με τον πολλαπλασιασμό πολυωνύμων. Επίσης, το ακόλουθο λήμμα φράσσει το μέτρο Mahler και είναι εξαιρετικής σημασίας:

Λήμμα 3.4 (Landau). *Αν $A \in \mathbb{C}[X]$ δεν είναι μονώνυμο τότε $\mathcal{M}(A) \leq \|A\|_2$. Αν $A \in \mathbb{Z}[X]$ και $\mathcal{L}(A) = \tau$ τότε*

$$\mathcal{M}(A) \leq \|A\|_2 \leq 2^{\tau}\sqrt{d+1} \tag{3.2}$$

Ορισμός 3.5 (Μέτρο Mahler αλγεβρικού αριθμού). *Το μέτρο Mahler ενός αλγεβρικού αριθμού γ, το οποίο θα συμβολίζουμε ως $\mathcal{M}(\gamma)$, είναι το μέτρο $\mathcal{M}(A)$ οποιουδήποτε ελάχιστου πολυωνύμου $A \in \mathbb{Z}[X]$ του γ.*

Το ελάχιστο πολυώνυμο, που ανήκει στο $\mathbb{Z}[X]$, ενός αλγεβρικού αριθμού είναι μοναδικό, με την εξαίρεση του πολλαπλασιασμού με -1. Κατά συνέπεια αν υποθέσουμε ότι θεωρούμε τον μεγιστοβάθμιο όρο ενός πολυωνύμου πάντα θετικό τότε το $\mathcal{M}(\gamma)$ είναι καλώς (μοναδικά) ορισμένο. Επίσης ισχύουν οι παρακάτω ανισότητες, η απόδειξη των οποίων βασίζεται στον ορισμό 3.2.

Πρόταση 3.6. *Έστω α και β δύο αλγεβρικοί αριθμοί τέτοιοι ώστε $\deg(\alpha) = m$ και $\deg(\beta) = n$.*

Τότε ισχύουν οι παρακάτω σχέσεις:

$$\begin{aligned}
\frac{1}{\mathcal{M}(\alpha)} &\leq |\alpha| \leq \mathcal{M}(\alpha) \\
\mathcal{M}(\alpha \cdot \beta) &\leq \mathcal{M}(\alpha)^n \cdot \mathcal{M}(\beta)^m \\
\mathcal{M}(\alpha + \beta) &\leq 2^{m\,n} \mathcal{M}(\alpha)^n \cdot \mathcal{M}(\beta)^m \\
\mathcal{M}\left(\alpha^{\frac{1}{k}}\right) &\leq \mathcal{M}(\alpha) \qquad\qquad \forall\, k \in \mathbb{N}^* \\
\mathcal{M}\left(\alpha^{-1}\right) &= \mathcal{M}(\alpha) \\
\mathcal{M}\left(\alpha^{k}\right) &\leq \mathcal{M}(\alpha)^k \qquad\qquad \forall\, k \in \mathbb{N}^*
\end{aligned}$$

3.2 Φράγματα στις ρίζες

Απόλυτα φράγματα

Αν $A \in \mathbb{C}[X]$ σκοπός μας είναι να υπολογίσουμε ένα δίσκο $D \subset \mathbb{C}$, ως συνάρτηση των συντελεστών, ο οποίος περιέχει όλες τις ρίζες του A. Αν θεωρήσουμε ότι το D έχει κέντρο το μηδέν τότε αρκεί να υπολογίσουμε μια ακτίνα η οποία να έχει μέτρο μεγαλύτερο από το μέτρο της μεγαλύτερης (κατά μέτρο) ρίζας του A. Τέτοιου είδους φράγματα ονομάζονται *απόλυτα φράγματα* ή *φράγματα εγκλεισμού*.

Για τις αποδείξεις των θεωρημάτων που παραλείπουμε ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [131, 187, 190, 192, 233, 233, 238, 245, 257, 275].

Θεώρημα 3.7 (Cauchy 1829)

Έστω $A \in \mathbb{C}[X]$ και έστω $r[A]$ η μοναδική θετική ρίζα του

$$\mathcal{C}_A(X) = |a_d|\, X^d - |a_{d-1}|\, X^{d-1} - \cdots - |a_1|\, X - |a_0| \ \in \mathbb{C}[X]$$

Όλες οι (μιγαδικές) ρίζες του A περιέχονται στο δίσκο $|X| \leq r[A]$. Το $\mathcal{C}_A[X]$ ονομάζεται πολυώνυμο Cauchy του A.

Τα περισσότερα απόλυτα φράγματα προσπαθούν να προσεγγίσουν όσο το δυνατόν καλύτερα το $r[A]$, δηλαδή υπολογίζουν κάποιο ξ τέτοιο ώστε $r[A] \leq \xi$. Οι καλύτερες προσεγγίσεις επιτυγχάνονται με το παρακάτω θεώρημα:

Θεώρημα 3.8 (M. Fujiwara, 1926)

Έστω $A \in \mathbb{C}[X]$ και $\lambda_0, \ldots, \lambda_{d-1} \in (0, \infty)$ τέτοια ώστε $\frac{1}{\lambda_0} + \cdots + \frac{1}{\lambda_{d-1}} \leq 1$, τότε όλες οι (μιγαδικές) ρίζες του A περιέχονται στο δίσκο $|X| \leq F_\lambda(A)$, όπου

$$F_\lambda(A) = \max_{0 \leq k \leq d-1} \left\{ \left(\lambda_k \left| \frac{a_k}{a_d} \right| \right)^{\frac{1}{d-k}} \right\}$$

Το επόμενο φράγμα, το οποίο οφείλεται στο Kuniyeda, δίνει συνήθως χειρότερα αποτελέσματα από το αυτό του Fujiwara, αλλά το παρουσιάζουμε για λόγους πληρότητας.

Θεώρημα 3.9 (M. Kuniyeda, 1916)
Έστω $A \in \mathbb{C}[X]$ και $p, q > 0$ τέτοια ώστε $\frac{1}{p} + \frac{1}{q} = 1$ τότε όλες οι (μιγαδικές ρίζες του A περιέχονται στο δίσκο $|X| \leq \xi$, όπου

$$\xi = \left(1 + \left(\sum_{j=0}^{d-1} \left| \frac{a_j}{a_d} \right|^p \right)^{\frac{q}{p}} \right)^{\frac{1}{q}}$$

Τα παρακάτω φράγματα προκύπτουν από το Θεωρ. 3.8 με κατάλληλη επιλογή των λ_i.

Πόρισμα 3.10. *Αν γ είναι η μεγαλύτερη κατά μέτρο ρίζα του $A \in \mathbb{C}[X]$ τότε*

$$\textit{(Cauchy)} \qquad |\gamma| \leq 1 + \frac{\max\{|a_0|, \ldots, |a_{d-1}|\}}{|a_d|}$$

$$|\gamma| \leq \frac{1}{\sqrt[d]{2} - 1} \max\left\{ \frac{|a_{d-1}|}{\binom{d}{1}|a_d|}, \sqrt{\frac{|a_{d-2}|}{\binom{d}{2}|a_d|}}, \sqrt[3]{\frac{|a_{d-3}|}{\binom{d}{3}|a_d|}}, \ldots, \sqrt[d]{\frac{|a_0|}{\binom{d}{d}|a_d|}} \right\}$$

$$\textit{(Cauchy)} \qquad |\gamma| \leq \max\left\{ \frac{d|a_{d-1}|}{|a_d|}, \sqrt{\frac{d|a_{d-2}|}{|a_d|}}, \sqrt[3]{\frac{d|a_{d-3}|}{|a_d|}}, \ldots, \sqrt[d]{\frac{d|a_0|}{|a_d|}} \right\}$$

Αν $A \in \mathbb{Z}[X]$ και χρησιμοποιώντας την ανισότητα (2.4) τότε το πρώτο φράγμα του Πορ. 3.10 γίνεται

$$|\gamma| \leq 1 + \frac{\|A\|_\infty}{|a_d|} \leq 1 + \frac{\|A\|_2}{|a_d|}$$

όπου η δεύτερη ανισότητα ονομάζεται φράγμα Landau [275], δείτε επίσης το Λημ. 3.4. Τα φράγματα του Πορ. 3.10 είναι βέλτιστα, δηλαδή υπάρχουν πολυώνυμα των οποίων η μεγαλύτερη ρίζα είναι κάποιο από τα φράγματα, συνεπώς είναι μεταξύ τους (θεωρητικά) ισοδύναμα. Επιπρόσθετα, η μέγιστη τιμή τους είναι 2^τ και η ελάχιστη $2^{-\tau}$, αν $A \in \mathbb{Z}[X]$.

Σημείωση 3.11. *Θεωρούμε ένα αλγόριθμο* absoluteRootBound *ο οποίος υλοποιεί κάποιο από τα παραπάνω απόλυτα φράγματα. Η πολυπλοκότητα του υπολογισμού όλων των φραγμάτων αν $A \in \mathbb{Z}[X]$, $\deg(A) = d$ και $\mathcal{L}(A) = \tau$ είναι $\widetilde{\mathcal{O}}_B(d\tau)$.*

Προκειμένου να υπολογίσουμε ένα κάτω απόλυτο φράγμα στις ρίζες του A θεωρούμε το πολυώνυμο $\mathcal{R}(A)(X)$, του οποίου οι ρίζες είναι $\frac{1}{\gamma}$. Υπολογίζουμε κάποιο απόλυτο φράγμα στις ρίζες του $\mathcal{R}(A)(X)$, οπότε έχουμε ότι $\frac{1}{|\gamma|} \leq$ absoluteRootBound$(\mathcal{R}(A))$ ή $|\gamma| \geq 1/$absoluteRootBound$(\mathcal{R}(A))$.

Δηλαδή θεωρούμε τον αλγόριθμο lowerAbsoluteRootBound*, για τον οποίο ισχύει ότι*

$$\text{lowerAbsoluteRootBound}(A) = 1/\text{absoluteRootBound}(\mathcal{R}(A))$$

και ο οποίος έχει την ίδια πολυπλοκότητα με τον absoluteRootBound.

Θετικά φράγματα

Τα απόλυτα φράγματα υπολογίζουν έναν δίσκο στο μιγαδικό επίπεδο που περιέχει όλες τις ρίζες. Ωστόσο, σε πολλές περιπτώσεις, όπως για παράδειγμα στην απομόνωση των πραγματικών ριζών με τον αλγόριθμο των συνεχών κλασμάτων, χρειαζόμαστε φράγματα που αφορούν μόνο τις θετικές πραγματικές ρίζες. Τέτοιου είδους φράγματα θα τα ονομάσουμε *θετικά φράγματα*. Αν και μπορούμε να χρησιμοποιήσουμε τα απόλυτα φράγματα, η ελπίδα είναι ότι μπορούμε να υπολογίσουμε πιο σφιχτά φράγματα γιατί ενδιαφερόμαστε για μια ειδική περίπτωση. Δεν υπάρχει μεγάλη βιβλιογραφία για τα θετικά φράγματα. Οι πιο σημαντικές εργασίες οφείλονται στους Kioustelidis [157] και Stefanescu [244].

Θεώρημα 3.12

[157] Έστω $A \in \mathbb{R}[X]$ και U_A το σύνολο των δεικτών των αρνητικών συντελεστών του A, δηλαδή $U_A := \{k \mid k \leq d \wedge a_k < 0\}$. Έστω το πολυώνυμο

$$\mathcal{C}_A^+(X) := a_d X^d + \sum_{k \in U_A} a_k X^k$$

Το $\mathcal{C}_A^+$ έχει μία μοναδική θετική ρίζα, που συμβολίζουμε με $r^+[A]$ και οποία και αποτελεί ένα άνω φράγμα στις θετικές πραγματικές ρίζες του A (αν υπάρχουν).

Απόδειξη: Αν το $\mathcal{C}_A^+$ έχει το μηδέν ως σταθερό όρο τότε το διαιρούμε με την κατάλληλη δύναμη του X έτσι ώστε ο σταθερός όρος να είναι διάφορος του μηδενός. Υποθέτουμε ότι ο σταθερός όρος δεν είναι μηδέν. Παρατηρούμε ότι $\mathtt{VAR}(\mathcal{C}_A^+) = 1$, άρα το $\mathcal{C}_A^+$ έχει μία μοναδική θετική ρίζα, σύμφωνα με τον κανόνα προσήμων του Descartes (Θεωρ. 3.28).

Αν το A δεν έχει θετικές πραγματικές ρίζες τότε το θεώρημα ισχύει. Έστω $\gamma > 0$ η μεγαλύτερη θετική ρίζα του A. Τότε ισχύει ότι

$$\begin{aligned} a_d \gamma^d = -\sum_{i=0}^{d-1} a_i \gamma^i \leq -\sum_{k \in U_A} a_k \gamma^k \;\Leftrightarrow \\ a_d \gamma^d + \sum_{k \in U_A} a_k \gamma^k \leq 0 \\ \mathcal{C}_A^+(\gamma) \leq 0 \end{aligned}$$

Παρατηρούμε ότι $\mathcal{C}_A^+(0) < 0$ και $\mathcal{C}_A^+(+\infty) > 0$, οπότε το γ είναι μικρότερο ή ίσο από $r^+[A]$. ΟΕΔ

Αν και το $\mathcal{C}_A^+$ εξαρτάται από κάποιο υποσύνολο του συνόλου των συντελεστών του A, το επαγόμενο φράγμα είναι χειρότερο από αυτό που προκύπτει από τη θετική ρίζα του πολυωνύμου Cauchy (Θεωρ. 3.7), όπως δείχνει το επόμενο λήμμα. Η χρησιμότητά του θα φανεί στη συνέχεια όταν παρουσιάσουμε το Λημ. 3.17.

Λήμμα 3.13. *Ισχύει $r[A] \leq r^+[A]$.*

Απόδειξη: Παρατηρούμε ότι $\mathcal{C}_A(0) < 0$ και $\mathcal{C}_A(+\infty) > 0$ και ότι

$$\begin{aligned}\mathcal{C}_A(r^+[A]) &= a_d(r^+[A])^d + \sum_{k\in U_A} a_k\,(r^+[A])^k + \sum_{k\notin U_A} a_k\,(r^+[A])^k \\ &= 0 + \sum_{k\notin U_A} a_k\,(r^+[A])^k \geq 0\end{aligned}$$

ΟΕΔ

Μπορούμε τώρα να ορίσουμε ένα φράγμα ανάλογο με αυτό το Fujiwara για την περίπτωση των θετικών πραγματικών ριζών. Το επόμενο θεώρημα οφείλεται στον Kioustelidis [157].

Θεώρημα 3.14

Έστω $A = \sum_{i=0}^{d} a_i X^d \in \mathbb{R}[X]$ και έστω ένα σύνολο μη αρνητικών αριθμών $\mu = \{\mu_k\}_{k\in U_A}$, τέτοιο ώστε $\sum_{k\in U_A} \frac{1}{\mu_k} \leq 1$. τότε

(1) η ποσότητα

$$N_\mu(A) := \max_{k\in U_A}\left\{\left(\mu_k\left|\frac{a_k}{a_d}\right|\right)^{\frac{1}{d-k}}\right\}$$

είναι ένα άνω φράγμα στις θετικές πραγματικές ρίζες του A.

(2) Η ελάχιστη τιμή του $N_\mu(A)$, αν θεωρεί ως συνάρτηση των μ_k, είναι η μοναδική θετική ρίζα του $\mathcal{C}_A^+$, δηλαδή $r^+[A] = \min_\mu N_\mu(A)$.

Απόδειξη: Αρκεί να δειχτεί ότι $r^+[A] \leq N_\mu(A)$. Θα το δείξουμε με αναγωγή σε άτοπο. Έστω $r^+[A] > N_\mu(A)$. Τότε $\forall\, k \in U_A$ ισχύει

$$r^+[A] > \left(\mu_k\left|\frac{a_k}{a_d}\right|\right)^{\frac{1}{d-k}} \Rightarrow \frac{1}{\mu_k} a_d\,(r^+[A])^d > |a_k|\,(r^+[A])^k$$

και αθροίζοντας πάνω σε όλα τα $k \in U_A$ έχουμε

$$\begin{aligned} a_d\,(r^+[A])^d \sum_{k\in U_A}\frac{1}{\mu_k} &> \sum_{k\in U_A}|a_k|(r^+[A])^k \\ a_d\,(r^+[A])^d \sum_{k\in U_A}\frac{1}{\mu_k} &> a_d(r^+[A])^d \\ \sum_{k\in U_A}\frac{1}{\mu_k} &> 1 \qquad\qquad \text{ΑΤΟΠΟ!}\end{aligned}$$

Για την απόδειξη του δεύτερης ιδιότητας αρκεί να θεωρήσουμε

$$\mu_k = \frac{a_d}{a_k}\,\left(r^+[A]\right)^{d-k}$$

όπου $k \in U_A$.

ΟΕΔ

Αν και αποδείξαμε (Λημ. 3.13) ότι $r[A] \leq r^+[A]$ τα φράγματα που λαμβάνουμε για το θετικό πολυώνυμο Cauchy είναι καλύτερα από αυτά που λαμβάνουμε από το θεώρημα του Fujiwara. Δηλαδή ισχύει $N_\mu(A) \leq F_\lambda(A)$.

Λήμμα 3.15. *Αν $F_\lambda(A)$ κάποιο άνω φράγμα στις θετικές ρίζες του A, τότε μπορούμε πάντοτε να επιλέξουμε μια ακολουθία $\mu \subset \lambda$, τέτοια ώστε $N_\mu(A) \leq F_\lambda(A)$.*

Απόδειξη: Έστω ένα φράγμα $F_\lambda(A)$. Από το Θεωρ. 3.8 έχουμε ότι $\sum_{j=0}^{d-1} \frac{1}{\lambda_j} \leq 1$ και $\lambda_j > 0$. Συνεπώς οποιοδήποτε υποσύνολο των αντιστρόφων έχει άθροισμα ≤ 1. Επιλέγουμε ακολουθία μ τέτοια ώστε $\mu_k = \lambda_j$ και $k \in U_A$. Τότε ισχύει

$$\left\{ \left(\mu_k \left| \frac{a_k}{a_d} \right| \right)^{\frac{1}{d-k}} \right\}_{k \in U_A} \subseteq \left\{ \left(\lambda_j \left| \frac{a_j}{a_d} \right| \right)^{\frac{1}{d-j}} \right\}_{0 \leq j \leq d-1}$$

οπότε συνάγουμε ότι $N_\mu(A) \leq F_\lambda(A)$. ΟΕΔ

Λήμμα 3.16. *Έστω $A = \sum_{i=0}^{d} a_i X^d \in \mathbb{R}[X]$. Το συναρτησοειδές*

$$N_2(A) := 2 \max_{k \in U_A} \left\{ \left| \frac{a_k}{a_d} \right|^{\frac{1}{d-k}} \right\} \tag{3.3}$$

αποτελεί ένα άνω φράγμα στις θετικές ρίζες του A και ισχύει $r^+[A] \leq N_2(A) \leq 2\, r^+[A]$.

Απόδειξη: Σύμφωνα με το Θεωρ. 3.14, επιλέγοντας $\mu_k = 2^{d-k}$, έχουμε $r^+[A] \leq N_2(A)$. Εφόσον $r^+(A)$ είναι ρίζα του $\mathcal{C}_A^+$ ισχύει

$$\mathcal{C}_A^+ \left(r^+[A] \right) = a_d \left(r^+[A] \right)^d + \sum_{k \in U_A} a_k \left(r^+[A] \right)^k = 0 \quad \Leftrightarrow$$

$$1 = \sum_{k \in U_A} \left| \frac{a_k}{a_d} \right| \left(r^+[A] \right)^{k-d}$$

Παρατηρούμε ότι στην τελεταία ισότητα, όλες οι ποσότητες του αθροίσματος είναι θετικές, συνεπώς κάθε μια από αυτές πρέπει να είναι ≤ 1. Δηλαδή ισχύει

$$\left| \frac{a_k}{a_d} \right| \left(r^+[A] \right)^{k-d} \leq 1 \quad \Leftrightarrow \quad \left| \frac{a_k}{a_d} \right| \leq \left(r^+[A] \right)^{d-k}$$

Συνδυάζοντας την τελευταία ανισότητα με την (3.3) συμπεραίνουμε ότι $N_2(A) \leq 2\, r^+[A]$. ΟΕΔ

Το παρακάτω λήμμα μας δίνει μια ένδειξη για την ποιότητα του φράγματος $N_2(A)$, στη χειρότερη περίπτωση.

Λήμμα 3.17. *Αν $A \in \mathbb{C}[X]$ και γ μια θετική του ρίζα τότε $\gamma \leq N_2(A) \leq 2\, d \cdot \gamma$.*

Απόδειξη: Η αριστερή ανισότητα είναι προφανής. Από την εργασία του van der Sluis [257] ξέρουμε ότι $F_2(A) \leq 2\,d \cdot \gamma$ και από το προηγούμενο λήμμα ότι $N_2(A) \leq F_2(A)$. ΟΕΔ

Στηριζόμενοι στο Θεωρ. 3.14 μπορούμε να συνάγουμε καινούργια φράγματα για τις θετικές ρίζες ενός (πραγματικού) πολυωνύμου, παρόμοια με αυτά του Πορ. 3.10.

Πόρισμα 3.18. *Αν γ είναι η μεγαλύτερη πραγματική θετική ρίζα του $A \in \mathbb{R}[X]$ και $\ell \geq 1$, τότε*

1. $|\gamma| \leq \max_{k \in U_A} \left\{ \sqrt[d-k]{\ell \left| \frac{a_k}{a_d} \right|} \right\}$
2. *Αν ρ η (μοναδική) θετική ρίζα του $X^d - \sum_{k \in U_A} X^k$ τότε* $|\gamma| \leq \max_{k \in U_A} \left\{ \rho \sqrt[d-k]{\left| \frac{a_k}{a_d} \right|} \right\}$
3. $|\gamma| \leq \frac{1}{\sqrt[d]{2}-1} \max_{k \in U_A} \left\{ \sqrt[d-k]{\frac{|a_k|}{\binom{d}{k}|a_d|}} \right\}$

Απόδειξη: Η απόδειξη στηρίζεται στο Θεωρ. 3.14 με κατάλληλη επιλογή των μ_k.

1. Επιλέγουμε $\mu_k = \ell$ για $k \in U_A$. Αν $\ell = |U_A|$, τότε το φράγμα είναι γνωστό ως κανόνας του Cauchy. Θα μπορούσαμε επίσης να επιλέξουμε $\ell = d = \deg(A)$.
2. Παρατηρούμε ότι $\rho > 1$ και επιλέγουμε $\mu_k = \rho^k$ για $k \in U_A$.
3. Επιλέγουμε $\mu_k^{-1} = \binom{d}{k}(2^{1/d} - 1)^k$ για $k \in U_A$.

ΟΕΔ

Το ακόλουθο φράγμα δεν προκύπτει από το Θεωρ. 3.14. Οφείλεται στον Stefanescu [244] και αν μπορεί να εφαρμοστεί δίνει σχεδόν πάντα καλύτερα φράγματα. Το θεώρημα που παρουσιάζουμε έχει πιο ασθενείς υποθέσεις από αυτό που παρουσίασε ο Stefanescu. Η απόδειξη είναι ακριβώς η ίδια και γι' αυτό την παραλείπουμε.

Θεώρημα 3.19

[244] Έστω $A \in \mathbb{R}[X]$ τέτοιο ώστε να μπορεί να γραφτεί ως

$$A(X) = c_1 X^{d_1} - b_1 X^{m_1} + c_2 X^{d_2} - b_2 X^{m_2} + \cdots + c_k X^{d_k} - b_k X^{m_k} + g(X)$$

όπου $g(X) \in \mathbb{R}_+[X]$, $c_i > 0$, $b_i > 0$, $d_i > m_i$ για $1 \leq i \leq k$. Τότε ο αριθμός

$$\max\left\{ \left(\frac{b_1}{c_1}\right)^{1/(d_1-m_1)}, \ldots, \left(\frac{b_k}{c_k}\right)^{1/(d_k-m_k)} \right\}$$

είναι ένα άνω φράγμα στις θετικές ρίζες του A.

Σημείωση 3.20. *Θεωρούμε έναν αλγόριθμο* positiveRootBound *ο οποίος υλοποιεί κάποιο από τα παραπάνω φράγματα. Η πολυπλοκότητα του υπολογισμού όλων των φραγμάτων αν $A \in \mathbb{Z}[X]$, $\deg(A) = d$ και $\mathcal{L}(A) = \tau$ είναι $\widetilde{\mathcal{O}}_B(d\tau)$.*

Αντίστοιχα με την περίπτωση των απολύτων φραγμάτων (Σημ. 3.11) θεωρούμε τον αλγόριθμο positiveLowerBound *ο οποίος υπολογίζει ένα κάτω φράγμα στις θετικές ρίζες του A και ο οποίος έχει την ίδια πολυπλοκότητα με του* positiveRootBound.

Σύνθετα φράγματα και φράγματα διαχωρισμού

Ορισμός 3.21. *Έστω $A \in \mathbb{C}[X]$ και $\gamma_1, \ldots, \gamma_d$ οι (μιγαδικές) ρίζες του, ορίζουμε ως φράγμα διαχωρισμού (separation bound) των ριζών του A την ποσότητα*

$$\Delta(A) := \min_{i \neq j} |\gamma_i - \gamma_j|$$

Πρόταση 3.22. *Έστω $A = \sum_{i=0}^{d} a_i X^i \in \mathbb{C}[X]$ χωρίς τετράγωνα, τότε*

$$\Delta(A) > \sqrt{\frac{3|\mathsf{disc}(A)|}{d^{d+2}}} \|A\|_2^{1-d} \geq \sqrt{\frac{3|\mathsf{disc}(A)|}{d^{d+2}}} \mathcal{M}(A)^{1-d}$$

Αν ενδιαφερόμαστε για το φράγμα διαχωρισμού μεταξύ πραγματικών ριζών τότε υπάρχει το φράγμα του Rump [276], το οποίο είναι λίγο καλύτερο από τα προηγούμενα φράγματα

Πρόταση 3.23. *Έστω $A \in \mathbb{C}[X]$ χωρίς τετράγωνα τότε*

$$\Delta_{real}(A) > \sqrt{\frac{8}{d^{d+2}}} \frac{1}{1 + \|A\|_\infty^d}$$

Σημείωση 3.24. *Τα φράγματα διαχωρισμού είναι βέλτιστα, με την εξαίρεση κάποιων σταθερών. Τα πολυώνυμα Mignotte [187, 189, 190]*

$$f = X^d - 2(aX - 1)^2$$

όπου $d \geq 3$, $a \in \mathbb{Q}$ και $a \geq 3$, τα οποία είναι ανάγωγα στο $\mathbb{Q}[X]$, έχουν δύο πραγματικές ρίζες πολύ κοντά στο $1/a$ και ισχύει ότι $\Delta(f) < 2\,a^{-(d+2)/2}$. Συνεπώς το δυαδικό μήκος ενός (ρητού) αριθμού που βρίσκεται ανάμεσα σε δύο πραγματικές ρίζες ενός πολυωνύμου είναι στη γενική περίπτωση $\mathcal{O}(d\tau)$.

Ωστόσο, στη γενική περίπτωση τα φράγματα διαχωρισμού είναι πολύ άσχημα. Για παράδειγμα το θεωρητικό φράγμα διαχωρισμού για το πολυώνυμο Wilkinson $\sum_{i=0}^{20}(X - i)$ είναι περίπου 10^{-344} ενώ στην πραγματικότητα είναι 1!

Σημείωση 3.25. *Αν και η εκτίμηση του φράγματος διαχωρισμού με τη χρήση της νόρμας $\|\cdot\|_2$ είναι πιο ακριβής καθώς εξαρτάται από το πολυώνυμο το οποίο εξετάζουμε, όταν μελετούμε την ασυμπτωτική πολυπλοκότητα το δυαδικό μηκός όλων των φραγμάτων είναι το ίδιο, δηλαδή $\Delta(A) = 2^{-\mathcal{O}(d\tau)}$.*

Θα αποδείξουμε ένα θεώρημα το οποίο αφορά το γινόμενο διαφορών (μιγαδικών) ριζών ενός πολυωνύμου. Ένα παρόμοιο θεώρημα πρωτοπαρουσιάστηκε από τον Davenport [65] αλλά αφορούσε μόνο τις πραγματικές ρίζες και απαιτούσε πιο ισχυρές προϋποθέσεις. Μια άλλη παραλλαγή του θεωρήματος παρουσιάστηκε από τον Johnson [139], δείτε επίσης [163], η οποία αφορούσε και τις μιγαδικές ρίζες και χαλάρωνε τις υποθέσεις αρκετά. Στην πιο γενική του μορφή το θεώρημα παρουσιάστηκε από τον Mignotte [191] και επίσης από τους Du et al. [76].

Θεώρημα 3.26 (Davenport-Mahler bound)

Έστω $\{\alpha_1, \ldots, \alpha_k\}$ και $\{\beta_1, \ldots, \beta_k\}$ υποσύνολα διαφορετικών (μιγαδικών) ριζών του f (όχι απαραίτητα χωρίς τετράγωνα) τέτοια ώστε $\beta_i \notin \{\alpha_1, \ldots, \alpha_i\}$ και $|\beta_i| \leq |\alpha_i|$, για όλα τα $i \in \{1, \ldots, k\}$. Τότε

$$\prod_{i=1}^{k} |\alpha_i - \beta_i| \geq \mathcal{M}(f)^{-d+1} d^{-\frac{d}{2}} \left(\frac{\sqrt{3}}{d}\right)^k$$

Το φράγμα ισχύει και όταν $\alpha_1 > \beta_1 = \alpha_2 > \beta_2 = \ldots \alpha_k > \beta_k := \alpha_{k+1}$, είναι διαφορετικές πραγματικές ρίζες του f.

Η παραλλαγή, που αποδεικνύουμε στη συνέχεια, βασίζεται σε ένα θεώρημα του Mignotte [187], δείτε επίσης [190], αλλά η απόδειξη είναι πιο απλή και οι ανισότητες εμπεριέχουν το μέτρο Mahler. Αν και αντικαθιστούμε το παράγοντα d^d με τον παράγοντα 2^{d^2}, όταν $d = \mathcal{O}(\tau)$ τότε τα φράγματα είναι ισοδύναμα. Επιπρόσθετα, χαλαρώνουμε στο ελάχιστο τις υποθέσεις του θεωρήματος και άρα διευρύνουμε τη χρήση του, όπως θα γίνει σαφές και στην ανάλυση των αλγορίθμων απομόνωσης. Τέλος, αποδεικνύουμε και ένα άνω φράγμα [252].

Θεώρημα 3.27 (Davenport-Mahler-Mignotte revisited)

Έστω $A \in \mathbb{Z}[X]$ τέτοιο ώστε $\deg(A) = d$ και $\mathcal{L}(A) = \tau$. Έστω Ω ένα σύνολο από k ζεύγη (i, j) τέτοια ώστε $1 \leq i < j \leq d$. Θεωρούμε τις μη μηδενικές (μιγαδικές) ρίζες του A σε αύξουσα διάταξη κάτα μέτρο, δηλαδή $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_d|$. Τότε

$$2^k \mathcal{M}(A)^k \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{k - \frac{d(d-1)}{2}} \mathcal{M}(A)^{1-d-k} \sqrt{\mathsf{disc}(A)}$$

Απόδειξη: Έστω $\overline{\Omega}$ το πολυσύνολο $\overline{\Omega} = \{j \mid (i, j) \in \Omega\}$ και $|\overline{\Omega}| = k$.

Θα χρησιμοποιήσουμε την ανισότητα

$$|a - b| \leq 2 \max\{|a|, |b|\} \quad a, b \in \mathbb{C} \tag{3.4}$$

και το γεγονός ότι για κάθε ρίζα του A ισχύει $\frac{1}{\mathcal{M}(A)} \leq |\gamma_i| \leq \mathcal{M}(A)$ (Πρότ. 3.6).

Προκειμένου να δείξουμε την αριστερή ανισότητα του θεωρήματος

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \leq 2^k \prod_{j\in\overline{\Omega}} |\gamma_j| \leq 2^k \max_{j\in\overline{\Omega}} |\gamma_j|^k \leq 2^k \mathcal{M}(A)^k.$$

Η διακρίνουσα του A (Ορ. 2.12) είναι $\mathsf{disc}(A) = \mathsf{lead}\,(A)^{2d-2} \prod_{i<j} (\gamma_i - \gamma_j)^2$. Προκειμένου να δείξουμε τη δεξιά ανισότητα του θεωρήματος θεωρούμε την απόλυτη τιμή της διακρίνουσας του A:

$$\begin{aligned} |\mathsf{disc}(A)| &= |\,\mathsf{lead}\,(A)\,|^{2d-2} \prod_{i<j} |\gamma_i - \gamma_j|^2 \\ &= |\,\mathsf{lead}\,(A)\,|^{2d-2} \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j|^2 \prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j|^2 \qquad \Leftrightarrow \\ \sqrt{|\mathsf{disc}(A)|} &= |\,\mathsf{lead}\,(A)\,|^{d-1} \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j| \end{aligned}$$

Θεωρούμε το γινόμενο $\prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j|$ και εφαρμόζουμε $\frac{d(d-1)}{2} - k$ φορές την ανισότητα (3.4). Τότε

$$\begin{aligned} \prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j| &\leq 2^{\frac{d(d-1)}{2}-k} |\gamma_1|^0 |\gamma_2|^1 \cdots |\gamma_d|^{d-1} \Big(\prod_{j\in\overline{\Omega}} |\gamma_j|\Big)^{-1} \\ &\leq 2^{\frac{d(d-1)}{2}-k} \mathcal{M}(A)^{d-1} |\,\mathsf{lead}\,(A)\,|^{1-d} \mathcal{M}(A)^k \end{aligned}$$

όπου επίσης χρησιμοποιήσαμε την ανισότητα $|\gamma_1|^0 |\gamma_2|^1 \cdots |\gamma_d|^{d-1} \leq |\mathcal{M}(A)/\,\mathsf{lead}\,(A)\,|^{d-1}$, και το γεγονός ότι αφού $\forall i$, $|\gamma_i| \geq \mathcal{M}(A)^{-1}$, από Πρότ. 3.6, τότε $\prod_{j\in\overline{\Omega}} |\gamma_j| \geq |\gamma_1|^k \geq \mathcal{M}(A)^{-k}$. Και η απόδειξη ολοκληρώθηκε. ΟΕΔ

Φράγματα στο πλήθος των πραγματικών ριζών

Τα θεωρήματα τα οποία θα παρουσιάσουμε φράσσουν το πλήθος των πραγματικών ριζών ενός πολυωνύμου A. Συνήθως μας προσφέρουν μια υπερεκτίμηση και δεν είναι ακριβή όπως για παράδειγμα το Πορ. 2.27.

Θεώρημα 3.28 (Descartes' rule of sign)

Ο αριθμός των πραγματικών ριζών, έστω R, ενός πολυωνύμου $A \in \mathbb{R}[X]$ στο $(0,\infty)$ φράσσεται από $\mathtt{VAR}(A)$ και πιο συγκεκριμένα $R \equiv \mathtt{VAR}(A) \mod 2$.

Σημείωση 3.29. *Στη γενική περίπτωση ο κανόνας προσήμων του Descartes παρέχει μια υπερεκτίμηση στο πλήθος των πραγματικών ριζών. Ωστόσο, εάν ξέρουμε ότι το πολυώνυμο είναι υπερβολικό, δηλαδή έχει μόνο πραγματικές ρίζες, ή εάν οι εναλλαγές προσήμων είναι 0 ή 1, τότε μας δίνει το ακριβές πλήθος των πραγματικών ριζών.*

Ο κανόνας προσήμων του Descartes είναι ανεξάρτητος από τη βάση στην οποία αναπαρίστανται τα πολυώνυμα. Κατά συνέπεια ισχύει και όταν τα πολυώνυμα είναι στη βάση Bernstein (Εν. 2.4), δηλαδή ισχύει το ακόλουθο θεώρημα [14]:

Πρόταση 3.30. *Έστω πραγματικό πολυώνυμο A στην αναπαράσταση στη βάση Bernstein στο διάστημα $[a, b]$. Ο αριθμός R των πραγματικών ριζών του A στο $[a, b]$ φράσσεται από $\mathtt{VAR}(A)$. Επιπλέον $R \equiv \mathtt{VAR}(A) \mod 2$.*

Ο κανόνας προσήμων του Descartes μπορεί να προκύψει από το επόμενο θεώρημα το οποίο οφείλεται στον Budan. Για την απόδειξη ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία, π.χ [5, 187].

Θεώρημα 3.31 (Budan)

Έστω $A \in \mathbb{R}[X]$, τέτοιο ώστε $\deg(A) = d$ και έστω $a < b$, με $a, b \in \mathbb{R}$. Έστω A_a, αντίστοιχα A_b, το πολυώνυμο που παράγεται αφού εφαρμόσουμε στο A του μετασχηματισμό $X \mapsto X + a$, αντίστοιχα $X \mapsto X + b$. Τότε ισχύουν τα ακόλουθα:

1. $\mathtt{VAR}(A_a) \geq \mathtt{VAR}(A_b)$.
2. $\#\{\gamma \in (a, b) | A(\gamma) = 0\} \leq \mathtt{VAR}(A_a) - \mathtt{VAR}(A_b)$.
3. $\#\{\gamma \in (a, b) | A(\gamma) = 0\} \equiv \mathtt{VAR}(A_a) - \mathtt{VAR}(A_b) \mod 2$.

Τα ακόλουθα θεωρήματα είναι το αντίστροφο του κανόνα των προσήμων του Descartes και είναι εξαιρετικά χρήσιμα για την απόδειξη τερματισμού των αλγορίθμων απομόνωσης των πραγματικών ριζών ενός πολυωνύμου, που θα παρουσιάσουμε στη συνέχεια. Πιο συγκεκριμένα εξασφαλίζουν προϋποθέσεις, κάτω από τις οποίες, το πλήθος των εναλλαγών προσήμων να μας δίνει ακριβώς το πλήθος των πραγματικών ριζών. Για τις αποδείξεις των παραπάνω θεωρημάτων ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [14, 53, 162, 163].

Θεώρημα 3.32 (Το θεώρημα του ενός κύκλου)

Έστω $f \in \mathbb{R}[X]$, $\mathcal{I} = [a, b] \in \mathbb{R}^2$. Εάν ο δίσκος $D = (\frac{a+b}{2}, \frac{|\mathcal{I}|}{2})$ δεν περιέχει καμία ρίζα του f τότε $\mathtt{VAR}(f) = 0$.

Θεώρημα 3.33 (Το θεώρημα των δύο κύκλων)

Έστω $f \in \mathbb{R}[X]$, $\mathcal{I} = [a, b] \in \mathbb{R}^2$. Εάν η ένωση των δίσκων $D_1 = \left(i\frac{\sqrt{3}}{6}|\mathcal{I}|, \frac{|\mathcal{I}|}{2}\right)$ και $D_2 = \left(-i\frac{\sqrt{3}}{6}|\mathcal{I}|, \frac{|\mathcal{I}|}{2}\right)$ περιέχει μία και μόνο ρίζα του f (η οποία είναι κατά συνέπεια πραγματικός αριθμός) τότε $\mathtt{VAR}(f) = 1$.

3.3 Εύρεση πραγματικών ριζών πολυωνύμου

Οι βιβλιογραφικές αναφορές που παρουσιάζουμε για το πρόβλημα είναι μόνο η κορυφή του παγόβουνου και γι' αυτό ενθαρρύνουμε τον αναγνώστη να ανατρέξει στη βιβλιογραφία για περισσότερες πληροφορίες.

Καταρχάς πρέπει να υπενθυμίσουμε ότι ενδιαφερόμαστε μόνο για τις πραγματικές ρίζες ενός ακέραιου πολυωνύμου και ότι με τον όρο επίλυση εννοούμε τον υπολογισμό διαστημάτων απομόνωσης των πραγματικών ριζών. Επίσης, μας ενδιαφέρουν *μόνο* ακριβείς αλγόριθμοι, δηλαδή αλγόριθμοι που χρησιμοποιούν (μόνο) αριθμητική ακεραίων απεριόριστης ακρίβειας. Αν d είναι ο βαθμός του πολυωνύμου και τ το δυαδικό του μήκος, σε ό,τι θα ακολουθήσει θα θεωρήσουμε $N = \max\{d, \tau\}$.

Οι πιο γνωστοί και πιο συχνά χρησιμοποιούμενοι στην πράξη αλγόριθμοι για την απομόνωση των πραγματικών ριζών είναι οι αλγόριθμοι υποδιαίρεσης. Αυτοί οι οι αλγόριθμοι μιμούνται τη φιλοσοφία του αλγόριθμου της δυαδικής αναζήτησης. Πιο συγκεκριμένα ελέγχουν σε ένα αρχικό διάστημα το πλήθος των ριζών που περιέχει, στη συνέχεια το διαιρούν σε δύο ίσα υποδιαστήματα και ο αλγόριθμος επαναλαμβάνεται μέχρι να υπάρξει κάποια πιστοποίηση ότι το διάστημα το οποίο ελέγχουν περιέχει μία ή καμία ρίζα.

Οι πιο γνωστοί αλγόριθμοι και τους οποίους θα εξετάσουμε κάτω από ένα ενιαίο πρίσμα είναι οι αλγόριθμοι DESCARTES, BERNSTEIN και STURM.

Ο αλγόριθμος DESCARTES, ο οποίος βασίζεται στον κανόνα προσήμων του Descartes, παρουσιάστηκε στην σύγχρονη εκδοχή του από τους Collins and Akritas [52] και των οποίων η ανάλυση πέτυχε πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^6\tau^2)$. Στην συνέχεια ο Johnson [139] βελτίωσε την πολυπλοκότητα σε $\widetilde{\mathcal{O}}_B(d^5\tau^2)$ χωρίς να χρησιμοποιήσει γρήγορους αλγορίθμους για την μετατόπιση πολυωνύμου. Ωστόσο, η απόδειξη του Johnson [139] περιείχε κάποια κενά τα οποία διόρθωσε ο Krandick [162] ο οποίος επιπλέον παρουσίασε έναν διαφορετικό τρόπο διάσχισης του δένδρου αναζήτησης του αλγορίθμου. Οι Rouillier and Zimmermann [230] παρουσίασαν ένα ενοποιημένο πλαίσιο για όλες τις παραλλαγές του αλγορίθμου Descartes με βέλτιστη διαχείριση μνήμης και επιπλέον παρουσίασαν μια πολύ γρήγορη υλοποίηση. Η ορθότητα και ο τερματισμός του αλγορίθμου στηρίζονται στο θεώρημα του Vincent (Θεωρ. 3.43) ή/και στα θεωρήματα του ενός και των δύο κύκλων τα οποία παρουσιάστηκαν από τους Collins and Johnson [53] και στη συνέχεια έγιναν πιο σφιχτά από τους Krandick and Mehlhorn [163] χωρίς ωστόσο να επηρεάσουν την ασυμπτωτική πολυπλοκότητα.

Ο αλγόριθμος BERNSTEIN βασίζεται επίσης στον κανόνα προσήμων του Descartes αλλά και στις ιδιότητες της αναπαράστασης των πολυωνύμων στη βάση Bernstein. Ο αλγόριθμος παρουσιάστηκε από τους Lane and Riesenfeld [169] αλλά η ανάλυσή του πρωτοπαρουσιάστηκε από τους Mourrain et al. [203]. Ο αναγνώστης μπορεί να ανατρέξει και στους Mourrain et al. [205] για μια παραλλαγή με βέλτιστη διαχείριση μνήμης και για τη σύνδεση με τον αλγόριθμο DESCARTES. Στο ίδιο πλαίσιο οι Eigenwillig et al. [80] παρουσίασαν έναν πιθανοτικό αλγόριθμο για πολυώνυμα χωρίς τετράγωνα με συντελεστές που δεν είναι γνωστοί ακριβώς (bit stream coefficients). Η πολυπλοκότητα όλων των προσεγγίσεων είναι $\widetilde{\mathcal{O}}_B(d^6\tau^2)$.

Σχετικά πρόσφατα η πολυπλοκότητα τόσο για τον αλγόριθμο DESCARTES όσο και για τον BERNSTEIN βελτιώθηκε σε $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ από τους Eigenwillig et al. [81], δείτε επίσης [97] για μια πιο απλή προσέγγιση όπου επιπρόσθετα το πολυώνυμο δεν είναι απαραίτητα χωρίς τετράγωνα.

Ο αλγόριθμος STURM εισήχθη από τον Sturm [248] αλλά η ανάλυσή του και η γενίκευσή του έτσι ώστε να εμπεριέχει μόνο πράξεις με ακέραιους αριθμούς πρωτοπαρουσιάστηκε από τον Heindel [129], δείτε επίσης [55], και η πολυπλοκότητα του αλγορίθμου ήταν $\widetilde{\mathcal{O}}_B(d^7\tau^3)$. Ο Davenport [65] παρουσιάζει μια πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$, αλλά αν και αποδεικνύει ότι το πλήθος των βημάτων του αλγορίθμου είναι $\mathcal{O}(d\tau)$ δεν παρουσίασε το κόστος του κάθε βήματος, προφα-

νώς γιατί οι γρήγοροι αλγόριθμοι αποτίμησης προσημασμένων ακολουθιών υπο-επιλυουσών δεν ήταν γνωστοί εκείνη την εποχή. Γι' αυτό άλλωστε στο βιβλίο των Davenport, Siret, and Tournier [66] που ακολούθησε αναφέρεται ότι η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^6\tau^3)$. Οι Du et al. [76] δίνοντας ένα επιχείρημα απόσβεσης (amortized argument) πέτυχαν μια πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ για πολυώνυμα χωρίς τετράγωνα. Τέλος οι Emiris and Tsigaridas [91], δείτε επίσης [97], απλοποίησαν και συμπλήρωσαν τα κενά στην προσέγγιση του Davenport [65].

Ένας διαφορετικός ακριβής αλγόριθμος για την απομόνωση των πραγματικών ριζών ενός πολυωνύμου είναι ο αλγόριθμος των συνεχών κλασμάτων (continued fractions), τον οποίο θα συμβολίζουμε με CF. Διαφέρει από τους αλγορίθμους υποδιαίρεσης στο ότι αντί να υποδιαιρεί ένα αρχικό διάστημα που περιέχει όλες τις πραγματικές ρίζες του πολυωνύμου, υπολογίζει την ανάπτυξη σε συνεχές κλάσμα των ριζών.

Η πρώτη διατύπωση του αλγορίθμου οφείλεται στον Vincent [261]. ο αναγνώστης μπορεί επίσης να ανατρέξει στον Akritas [1, 5] για ιστορικές αναφορές. Ο αλγόριθμος του Vincent βασιζόταν σε ένα θεώρημα που διατύπωσε ο ίδιος (είναι το Θεωρ. 3.43 χωρίς τις συνθήκες τερματισμού) το οποίο εξασφαλίζει ότι επαναλαμβανόμενοι μετασχηματισμοί ενός πολυωνύμου τελικά δίνουν ένα πολυώνυμο με μία ή καμία εναλλαγή προσήμων στη λίστα των συντελεστών του. Κατά συνέπεια, από τον κανόνα προσήμων του Descartes προκύπτει ότι το μετασχηματισμένο πολυώνυμο έχει μία, αντίστοιχα καμία, πραγματική ρίζα στο $(0, \infty)$. Εάν καταλήξουμε με μία εναλλαγή προσήμων τότε οι αντίστροφοι μετασχηματισμοί μπορούν να εφαρμοστούν προκειμένου να υπολογίσουμε το διάστημα το οποίο απομονώνει την πραγματική ρίζα του αρχικού πολυωνύμου. Επιπρόσθετα, τα $c_i \in \mathbb{Z}$ που χρησιμοποιούνται ως μετατοπίσεις στους διάφορους μετασχηματισμούς αντιστοιχούν στα μερικά πηλίκα της ανάπτυξης σε συνεχή κλάσματα της πραγματικής ρίζας που απομονώσαμε.

Ωστόσο, ο αλγόριθμος του Vincent έχει εκθετική πολυπλοκότητα [52]. Αυτό συμβαίνει γιατί ο υπολογισμός των c_i στους μετασχηματισμούς του Θεωρ. 3.43 πραγματοποιείται με επαναλαμβανόμενες μετατοπίσεις της μορφής $X \mapsto X + 1$. Συνεπώς αν ένα από τα c_i (ή το το άθροισμά τους) είναι μέτρου, έστω, 2^τ τότε απαιτείται εκθετικό πλήθος βημάτων για τον υπολογισμό τους. Ο Uspensky [255] επέκτεινε το θεώρημα του Vincent υπολογίζοντας ένα άνω φράγμα στο πλήθος των μετασχηματισμών που απαιτούνται προκειμένου να απομονωθούν οι πραγματικές ρίζες, αλλά δεν κατάφερε να αντιμετωπίσει τον εκθετικό χαρακτήρα του αλγορίθμου. Ο αναγνώστης μπορεί επίσης να ανατρέξει στους Cantor et al. [47], Rosen and Shallit [228] όπου επιπρόσθετα εξετάζεται το πρόβλημα της προσέγγισης των πραγματικών αλγεβρικών αριθμών. Χρησιμοποιώντας το θεώρημα του Vincent οι Collins and Akritas [52] πρότειναν τον αλγόριθμο DESCARTES.

Ο Akritas [2, 5] αντιμετώπισε την εκθετική συμπεριφορά του αλγορίθμου, υπολογίζοντας τα c_i που εμφανίζονται στους μετασχηματισμούς ως θετικά κάτω φράγματα των πραγματικών ριζών. Ο Akritas πέτυχε μια πολυπλοκότητα της τάξης του $\widetilde{\mathcal{O}}_B(d^5\tau^3)$ ή $\widetilde{\mathcal{O}}_B(N^8)$, χωρίς να χρησιμοποιήσει γρήγορους αλγορίθμους μετατόπισης (Εν. 2.2). Ωστόσο, δεν είναι σαφές το πως και αν η προσέγγισή του λαμβάνει υπόψιν το γεγονός ότι το δυαδικό μήκος των συντελεστών ενός πολυώνυμου αυξάνει αν του εφαρμόσουμε έναν μετασχηματισμό μετατόπισης $X \mapsto b + X$. Ένα άλλο σημαντικό σημείο είναι το μέτρο των c_i. Η Εξ. (3.9) υποδηλώνει ότι το μέτρο των μερικών πηλίκων είναι μη φραγμένο. Ο αλγόριθμος CF είναι ο αλγόριθμος που χρησιμοποιείται από το MATHEMATICA [4] για την απομόνωση των πραγματικών ριζών. Ο αναγνώστης μπορεί να ανατρέξει στους Akritas and Strzebonski [3] για μια πειραματική μελέτη των διαφόρων αλγορίθμων απομόνωσης

με υλοποιήσεις βασισμένες στο MATHEMATICA.

Μια άλλη κατηγορία αλγορίθμων, τους οποίους δεν θα μελετήσουμε, είναι οι αριθμητικοί (numerical) αλγόριθμοι, όπου ο όρος *αριθμητικός* χρησιμοποιείται με την έννοια της αριθμητικής ανάλυσης [210, 214, 239]. Οι αλγόριθμοι αυτοί απαιτούν υπολογισμούς με αριθμούς κινητής υποδιαστολής απεριόριστης ακρίβειας (multiprecision floats) και υπολογίζουν προσεγγίσεις σε όλες τις ρίζες, πραγματικές και μιγαδικές, του πολυωνύμου προς επίλυση μέχρι κάποια ακρίβεια ϵ. Προκειμένου να αναγνωριστούν και να απομονωθούν οι πραγματικές ρίζες θα πρέπει να θέσουμε το ϵ ίσο με το φράγμα διαχωρισμού.

Οι βέλτιστοι αλγόριθμοι χρησιμοποιούν την τεχνική 'διαίρει και βασίλευε' και σε γενικές γραμμές η βασική ιδέα είναι η εξής: Δοθέντος ενός πολυωνύμου υπολογίζονται δύο δίσκοι (splitting circles) στο μιγαδικό επίπεδο που περιέχουν περίπου ίσο αριθμό (μιγαδικών) ριζών. Το πολυώνυμο παραγοντοποιείται προσεγγιστικά σε δύο πολυώνυμα οι ρίζες των οποίων είναι (προσεγγιστικά, μέχρι ακρίβεια ϵ) ίσες με τις ρίζες που περιέχονται στους κύκλους. Ο αλγόριθμος επαναλαμβάνεται για καθένα από τα δύο πολυώνυμα και σταματά όταν γίνουν γραμμικά. Η πολυπλοκότητα των αριθμητικών αλγορίθμων είναι σχεδόν βέλτιστη και πιο συγκεκριμένα $\widetilde{\mathcal{O}}_B(d^3\tau)$ ή $\widetilde{\mathcal{O}}_B(N^4)$ [214, 239] αλλά αποτελεσματικές υλοποιήσεις αυτών είναι ακόμα ζητούμενο. Αξίζει επίσης να αναφέρουμε και τον αριθμητικό αλγόριθμο ABERTH [22, 23] για τον οποίο υπάρχει μια πολύ αποτελεσματική υλοποίηση και ο οποίος έχει πολύ καλά πρακτικά αποτελέσματα αλλά για τον οποίο η δυαδική πολυπλοκότητα δεν είναι γνωστή. Στο ίδιο πλαίσιο εντάσσεται και ο αλγόριθμος του Sebastiano e Silva του οποίου η ανάλυση παρουσιάστηκε από τον Cardinal [49].

Όλοι οι παραπάνω αλγόριθμοι υποθέτουν πολυώνυμα χωρίς τετράγωνα.

Στις επόμενες παραγράφους θα παρουσιάσουμε ένα γενικό αλγόριθμο που δέχεται ως είσοδο πολυώνυμα όχι απαραίτητα χωρίς τετράγωνα και υπολογίζει τα διαστήματα απομόνωσης και τις πολλαπλότητες των πραγματικών ριζών. Θα παρουσιάσουμε ένα ενιαίο πλαίσιο για όλους τους αλγορίθμους υποδιαίρεσης, το οποίο απλοποιεί την ανάλυση των αλγορίθμων DESCARTES, BERNSTEIN και STURM. Στο πλαίσιο αυτό μπορούν να ενταχθούν όλοι οι αλγόριθμοι οι οποίοι βασίζονται στην υποδιαίρεση ενός αρχικού διαστήματος, όπως για παράδειγμα ο αλγόριθμος αποκλεισμού των Dedieu and Yakoubsohn [68]. Επίσης, θα βελτιώσουμε την πολυπλοκότητα του αλγορίθμου CF κατά ένα παράγοντα $d\,\tau$ ή N^2. Τέλος, για όλους τους αλγορίθμους απομόνωσης, θα δείξουμε ότι το φράγμα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ ισχύει και για πολυώνυμα τα οποία δεν είναι χωρίς τετράγωνα και στην ίδια πολυπλοκότητα θα υπολογίσουμε και τις πολλαπλότητες των πραγματικών ριζών.

Ο γενικός αλγόριθμος

Παρουσιάζουμε έναν γενικό αλγόριθμο απομόνωσης των πραγματικών ριζών και υπολογισμού των πολλαπλοτήτων τους, ενός πολυωνύμου $A \in \mathbb{Z}[X]$. Ο ψευδο-κώδικας, REALROOTSOLVER, παρουσιάζεται στον Αλγ. 1.

Η είσοδος του αλγορίθμου είναι ένα πολυώνυμο $A \in \mathbb{Z}[X]$ με $\deg(A) = d$ και $\mathcal{L}(A) = \tau$. Η έξοδος του αλγορίθμου είναι μία λίστα (ή διάνυσμα) που περιέχει διαστήματα απομόνωσης των πραγματικών ριζών $L = [[a_1, b_1], \ldots, [a_k, b_k]]$, όπου $a_i, b_i \in \mathbb{Q}$, και μία λίστα με τις πολλαπλότητές τους $M = [m_1, \ldots, m_k]$, όπου $m_i \in \mathbb{N}$, k είναι το πλήθος των πραγματικών ριζών του A_{red} και $\sum_{i=1}^{k} m_i = d$.

Algorithm 1: realRootSolver (A)

Input: $A \in \mathbb{Z}[X]$

Output: Μια λίστα με τα διαστήματα απομόνωσης και μία με τις πολλαπλότητες των ριζών

1 $A_{red} \leftarrow$ squareFreePart(A)
2 $B \leftarrow$ absoluteRootBound(A_{red})
3 $\mathbb{J}_0 = [-B, B]$
4 $L \leftarrow$ realRootIsolator$(A_{red}, \mathbb{J}_0)$
5 $M \leftarrow$ computeMultiplicities(A_{red}, L)
6 return L, M

Αρχικά ο αλγόριθμος υπολογίζει το χωρίς τετράγωνα μέρος του A, καλώντας τη συνάρτηση squareFreePart. Στη συνέχεια υπολογίζει ένα διάστημα που περιέχει όλες τις πραγματικές ρίζες του A_{red}, καλώντας τον αλγόριθμο absoluteRootBound. Τέλος, καλεί κάποιον αλγόριθμο υπολογισμού των διαστημάτων απομόνωσης των πραγματικών ριζών, realRootIsolator, και υπολογίζει τις πολλαπλότητες καλώντας την συνάρτηση computeMultiplicities.

Στη συνέχεια περιγράφουμε και αναλύουμε την πολυπλοκότητα των διαφόρων συναρτήσεων (αλγορίθμων) που χρησιμοποιεί ο αλγόριθμος realRootSolver.

- squareFreePart
  Έστω A_{red} το χωρίς τετράγωνα μέρος του A. Παρατηρούμε ότι $\deg(A_{red}) = \mathcal{O}(d)$ και $\mathcal{L}(A_{red}) = \mathcal{O}(d + \tau)$. Η πολυπλοκότητα αυτού του υπολογισμού είναι $\widetilde{\mathcal{O}}_B(d^2\tau)$ αν χρησιμοποιήσουμε τους γρήγορους αλγορίθμους για τον υπολογισμό ακολουθιών πολυωνυμικών υπολοίπων. Δείτε Θεωρ. 2.34.

- absoluteRootBound
  Μπορούμε να χρησιμοποιήσουμε ένα από τα απόλυτα φράγματα που παρουσιάστηκαν στην Εν. 3.2, δείτε και Σημ. 3.11. Όλα τα φράγματα έχουν, ασυμπτωτικά, το ίδιο δυαδικό μήκος, συνεπώς μπορούμε να υποθέσουμε ότι $B = 2^\tau$ και $\mathbb{J}_0 = [\mathsf{a}, \mathsf{b}] = [-2^\tau, 2^\tau]$.

  Η πολυπλοκότητα του βήματος αυτού είναι $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B(d(d + \tau)) = \widetilde{\mathcal{O}}_B(d^2 + d\tau)$.

- computeMultiplicites
  Προκειμένου να υπολογίσουμε τις πολλαπλότητες των πραγματικών ριζών του A πρέπει καταρχάς να υπολογίσουμε την *ελεύθερη τετραγώνων παραγοντοποίηση* του. Αυτή η παραγοντοποίηση συνίσταται από πολυώνυμα $(g_1, g_2, \ldots, g_m)$ τέτοια ώστε $A = g_1 g_2^2 \cdots g_m^m$, $g_m \neq 1$, τα g_i είναι πρώτα μεταξύ τους και χωρίς τετράγωνα. Για τον υπολογισμό της παραγοντοποίησης χρησιμοποιούμε τον αλγόριθμο του Yun [263] ο οποίος έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2\tau)$. Μάλιστα προκειμένου να είμαστε πιο ακριβής μπορούμε να πούμε ότι το κόστος της παραγοντοποίησης είναι δύο φορές το κόστος υπολογισμού του $\mathbf{SR}(A, A')$ [112]. Επιπλέον, ισχύει $\deg(g_j) = \delta_j \leq d$ και $\mathcal{L}(g_j) = O(d\tau)$, όπως προκύπτει από το φράγμα του Mignotte [187, 188, 189], όπου $1 \leq j \leq m$.

Κάθε διάστημα απομόνωσης περιέχει μία και μόνο μία πραγματική ρίζα του A_{red} και άρα το A_{red} αλλάζει πρόσημο αν αποτιμηθεί στα άκρα του κάθε διαστήματος, δηλαδή ισχύει $A_{red}(\mathsf{a}_i)A_{red}(\mathsf{b}_i) < 0$, $1 \leq i \leq k$, σύμφωνα με το θεώρημα του Bolzano.

Παρατηρούμε ότι ένα και μόνο ένα από τα πολυώνυμα g_j πρέπει να αλλάζει πρόσημο σε κάθε διάστημα απομόνωσης καθώς είναι χωρίς τετράγωνα και πρώτα μεταξύ τους. Αν κάποιο g_j αλλάζει πρόσημο σε κάποιο από τα διαστήματα απομόνωσης τότε η πολλαπλότητα της πραγματικής ρίζας που περιέχεται στο διάστημα αυτό είναι j. Κάθε g_j μπορεί να αποτιμηθεί σε κάποιο άκρο ενός διαστήματος απομόνωσης με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(\delta_i^2\, d\, \tau)$, αν χρησιμοποιήσουμε τον κανόνα του Horner. Μπορούμε ωστόσο να το αποτιμήσουμε πάνω σε όλα τα άκρα (το πλήθος τους είναι το πολύ $d+1$) σε χρόνο $\widetilde{\mathcal{O}}_B(\delta_i\, d^2\, \tau)$ [263, 275] (δείτε Εν. 2.2).

Εφόσον $\sum_{i=1}^{m} \delta_i \leq d$ η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$.

Αν το πλήθος των διαστημάτων που περιέχει η λίστα L είναι k τότε κατασκευάζουμε μία λίστα M, μεγέθους k, τέτοια ώστε αν $M[j] = m_j \in \mathbb{N}$, τότε η πραγματική ρίζα του A που περιέχεται στο j-οστό διάστημα απομόνωσης της L έχει πολλαπλότητα m_j.

Από τα παραπάνω προκύπτει ότι η συνολική πολυπλοκότητα του αλγορίθμου realRootSolver είναι το μέγιστο ανάμεσα στο $\widetilde{\mathcal{O}}_B(d^3\tau)$ και στην πολυπλοκότητα του αλγορίθμου realRootIsolator.

3.4 Ο αλγόριθμος του Kronecker

Ο Kronecker [166], δείτε επίσης [55], παρουσίασε έναν αλγόριθμο για την απομόνωση των πραγματικών ριζών ενός πολυωνύμου χωρίς τετράγωνα. Ο αλγόριθμος βασίζεται στον θεώρημα του Bolzano, δηλαδή ότι αν σε ένα διάστημα περιέχεται μία και μόνο πραγματική ρίζα ενός πολυωνύμου τότε το πολυώνυμο έχει διαφορετικό πρόσημο στα άκρα του διαστήματος. Ο αλγόριθμος είναι απλός αλλά όχι πολυωνυμικός. Τον παρουσιάζουμε προκειμένου να εισάγουμε τον αναγνώστη στους ακριβείς αλγορίθμους απομόνωσης των πραγματικών ριζών αλλά και για να απαντήσουμε σε ένα ερώτημα των Collins and Loos [55] σχετικά με το αναμενόμενο πλήθος των διαστημάτων που εξετάζει ο αλγόριθμος.

Ο ψευδο-κώδικας του αλγορίθμου kronecker παρουσιάζεται στον Αλγ. 2. Η είσοδος του αλγορίθμου είναι ένα πολυώνυμο A_{red} χωρίς τετράγωνα και η έξοδός του είναι μία λίστα L με τα διαστήματα απομόνωσης των πραγματικών ριζών.

Καταρχάς, ο αλγόριθμος υπολογίζει ένα απόλυτο φράγμα στις ρίζες (Εν. 3.2). Όλα τα φράγματα έχουν, ασυμπτωτικά, το ίδιο δυαδικό μήκος, συνεπώς μπορούμε να υποθέσουμε ότι $B = 2^\tau$. Το βήμα αυτό μπορεί να μην εκτελεστεί αν υποθέσουμε ότι έχει προηγηθεί ο αλγόριθμος realRootIsolator. Στη συνέχεια υπολογίζει το φράγμα διαχωρισμού, έστω Δ (Εν. 3.2).

Ακολούθως χωρίζει το διάστημα $[-B, B]$ σε διαστήματα μήκους Δ και ελέγχει, με το θεώρημα του Bolzano, αν κάποιο από αυτά περιέχει κάποια πραγματική ρίζα του A_{red}. Η συνάρτηση add$(L, [\mathsf{a}, \mathsf{b}])$, εισάγει το διάστημα $[\mathsf{a}, \mathsf{b}]$ στη λίστα L των διαστημάτων απομόνωσης.

Η ανάλυση της πολυπλοκότητας του αλγορίθμου βασίζεται στο πόσες φορές εκτελείται ο βρόγχος **while** (Γραμμή 6), δηλαδή εξαρτάται από το πόσα διαστήματα εξετάζει. Εφόσον το

Algorithm 2: KRONECKER (A_{red})

Input: $A_{red} \in \mathbb{Z}[X]$
Output: Μια λίστα από διαστήματα απομόνωσης

```
1  L ← ∅
2  B ← AbsoluteRootBound(A_red)
3  Δ ← separationBound(A_red)
4  a ← −B
5  s_L ← sign(A_red(a))
6  while a < B do
7      b ← a + Δ
8      s_R ← sign(A_red(b))
9      if s_R = 0 then L ← add(L, [b, b])
10     if s_L · s_R < 0 then L ← add(L, [a, b])
11     a ← b
12     s_L ← s_R
13 return L
```

αρχικό διάστημα είναι $[-2^\tau, 2^\tau]$ έχει μήκος $2^{\tau+1}$. Επίσης $\Delta = 2^{-\mathcal{O}(d\tau)}$, δείτε Εν. 3.2. Επομένως, ο αλγόριθμος εξετάζει $2^{\mathcal{O}(d\tau)}$ διαστήματα.

Σε κάθε βήμα υπολογίζει την αποτίμηση του A_{red} πάνω σε ένα ρητό αριθμό δυαδικού μήκους το πολύ $\mathcal{O}(d\tau)$. Η πολυπλοκότητα της αποτίμησης είναι $\tilde{\mathcal{O}}_B(d^3\tau)$ (Εν. 2.2).

Συνεπώς μπορούμε να διατυπώσουμε το παρακάτω θεώρημα:

Θεώρημα 3.34 (KRONECKER)
Έστω πολυώνυμο $A_{red} \in \mathbb{Z}[X]$ χωρίς τετράγωνα, τέτοιο ώστε $\deg(A_{red}) = d$ και $\mathcal{L}(A_{red}) = \tau$. Ο αλγόριθμος KRONECKER *απομονώνει τις πραγματικές ρίζες του A_{red} σε χρόνο $\tilde{\mathcal{O}}_B(2^{d\tau}d^3\tau)$.*

Υπάρχει μια προφανής βελτίωση του αλγορίθμου KRONECKER. Αντί να υπολογίζουμε κάθε φορά τα πρόσημα στα άκρα ενός διαστήματος θα μπορούσαμε να υπολογίζουμε το πρόσημο στα άκρα d διαστημάτων, ταυτόχρονα, με την ίδια πολυπλοκότητα (Εν. 2.2). Δυστυχώς αυτή η παραλλαγή δεν βελτιώνει την εκθετική πολυπλοκότητα του αλγορίθμου καθώς τα διαστήματα που πρέπει να εξεταστούν είναι $2^{\mathcal{O}(d\tau)}/d = 2^{\mathcal{O}(d\tau)}$.

Αν χρησιμοποιήσουμε τον αλγόριθμο KRONECKER ως REALROOTISOLATOR στον Αλγ. 1 τότε η πολυπλοκότητα είναι $\tilde{\mathcal{O}}_B(2^{d\tau}d^3\tau + d^3\tau)$ ή $\tilde{\mathcal{O}}_B(2^{d\tau}d^3\tau)$ για τον υπολογισμό και των πολλαπλοτήτων των πραγματικών ριζών.

Οι Collins and Loos [55] έθεσαν το ερώτημα σχετικά με το πόσα διαστήματα κατά μέσο όρο εξετάζει ο αλγόριθμος KRONECKER. Θα προσπαθήσουμε να απαντήσουμε σε αυτό το ερώτημα κάνοντας την υπόθεση ότι κάθε διάστημα έχει την ίδια πιθανότητα να περιέχει μία πραγματική ρίζα του A_{red}.

Αν υποθέσουμε ότι το πλήθος των πραγματικών ριζών, έστω R, δεν είναι γνωστό και ότι $R < d$, τότε ο αλγόριθμος, πάντοτε, εξετάζει όλα τα διαστήματα, καθώς δεν μπορεί να γνωρίζει πότε πρέπει να σταματήσει.

Ας υποθέσουμε λοιπόν ότι γνωρίζουμε το ακριβές πλήθος των πραγματικών ριζών, $R \leq d$. Έστω K όλα τα διαστήματα προς εξέταση. Όλες οι δυνατές θέσεις των ριζών είναι $\binom{K}{R}$. Το πόσα διαστήματα θα εξεταστούν εξαρτάται από τη θέση της μεγαλύτερης ρίζας, η οποία μπορεί να βρίσκεται από τη θέση R έως και τη θέση K. Αν βρίσκεται στην ℓ θέση, όπου $R \leq \ell \leq K$, τότε εξετάζονται ℓ διαστήματα και υπάρχουν $\binom{\ell-1}{R}$ τέτοιες περιπτώσεις. Συνεπώς η μέση τιμή του πλήθους των εξεταζόμενων διαστημάτων είναι

$$\frac{\sum_{\ell=R}^{K} \binom{\ell-1}{R-1} \ell}{\binom{K}{R}} = \frac{R\,(K+1)}{R+1}$$

Αν $R = 1$, τότε προφανώς δεν χρειάζεται να εκτελεστεί ο αλγόριθμος KRONECKER καθώς έχουμε, από κατασκευής, ένα διάστημα απομόνωσης, το $[-B, B]$. Αν παρ' όλα αυτά ο αλγόριθμος εκτελεστεί, για παράδειγμα αν θέλουμε να υπολογίσουμε ένα, μικρού μήκους, διάστημα που να περιέχει την πραγματική ρίζα, τότε το αναμενόμενο πλήθος των εξεταζόμενων διαστημάτων είναι $\frac{K+1}{2}$. Το οποίο προφανώς συμπίπτει με τον αναμενόμενο πλήθος πλήθος συγκρίσεων κατά τη σειριακή αναζήτηση ενός στοιχείου σε ένα πίνακα [161].

3.5 Αλγόριθμοι υποδιαίρεσης

Στην παρούσα παράγραφο θα εξειδικεύσουμε τον αλγόριθμο REALROOTISOLATOR με αλγορίθμους υποδιαίρεσης, τους οποίους θα συμβολίσουμε με $\text{SUBDIVISIONSOLVER}_{\text{SM}}$. Θα θεωρήσουμε ότι το πολυώνυμο, A_{red} που εξετάζουμε είναι χωρίς τετράγωνα και ότι $\deg(A_{red}) = d$ και $\mathcal{L}(A_{red}) = \tau$. Υπενθυμίζουμε ότι οι αλγόριθμοι υποδιαίρεσης για την απομόνωση των πραγματικών ριζών είναι παρόμοιοι με αυτόν της δυαδικής αναζήτησης.

Ο ψευδοκώδικας του γενικού αλγορίθμου υποδιαίρεσης παρουσιάζεται στον Αλγ. 3. Η είσοδος είναι το πολυώνυμο $A_{red} \in \mathbb{Z}[X]$ χωρίς τετράγωνα και ένα διάστημα $\mathcal{I}_0$ στο οποίο θέλουμε να απομονώσουμε τις πραγματικές ρίζες του A_{red}. Συνήθως το $\mathcal{I}_0$ περιέχει όλες τις πραγματικές ρίζες του A_{red}. Ο αλγόριθμος χρησιμοποιεί μια στοίβα Q η οποία περιέχει ζεύγη της μορφής $\{f, \mathcal{I}\}$. Η σημασιολογία του ζεύγους είναι ότι απαιτείται να απομονώσουμε τις πραγματικές ρίζες του f στο διάστημα $\mathcal{I}$.

Στον Αλγ. 3 εμφανίζονται κλήσεις σε μερικές βοηθητικές, εξωτερικές, συναρτήσεις (αλγορίθμους). Καταρχάς εμφανίζονται δύο συναρτήσεις που αφορούν τη στοίβα Q. Η συνάρτηση $\text{PUSH}(Q, \{f, \mathcal{I}\})$, η οποία εισάγει το ζεύγος $\{f, \mathcal{I}\}$ στην κορυφή της στοίβας και η συνάρτηση $\text{POP}(Q)$ η οποία επιστρέφει το ζεύγος που βρίσκεται στην κορυφή της στοίβας Q και ταυτόχρονα το διαγράφει από αυτήν. Επίσης η συνάρτηση $\text{ADD}(L, \mathcal{I})$, εισάγει το διάστημα $\mathcal{I}$ στη λίστα L των διαστημάτων απομόνωσης.

Τέλος, υπάρχουν τρεις εξωτερικές συναρτήσεις με δείκτη SM οι οποίες επιδέχονται διαφορετικής υλοποίησης ανάλογα με τον αλγόριθμο υποδιαίρεσης που χρησιμοποιείται. Καταρχάς, η συνάρτηση $\text{INITIALIZATION}_{\text{SM}}$ εκτελεί κάποιες διαδικασίες αρχικοποίησης ανάλογα με τον αλγόριθμο υποδιαίρεσης. Η συνάρτηση $\text{COUNT}_{\text{SM}}(f, \mathcal{I})$ επιστρέφει το πλήθος (ή ένα άνω φράγμα στο

Algorithm 3: SUBDIVISIONSOLVER$_{\text{SM}}(A_{red}, \mathcal{I}_0)$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I}_0 = [\mathsf{a}, \mathsf{b}]$
Output: Μια λίστα από διαστήματα απομόνωσης

```
1  INITIALIZATION_SM(A_red, I_0)
2  L ← ∅
3  Q ← ∅
4  Q ← PUSH(Q, {A, I_0})
5  while Q ≠ ∅ do
6      {f, I} ← POP(Q)
7      V ← COUNT_SM(f, I)
8      switch V do
9          case V = 0 continue
10         case V = 1 L ← ADD(L, I)
11         case V > 1
12             {f_L, I_L}, {f_R, I_R} ← SPLIT_SM(f, I)
13             Q ← PUSH(Q, {f_L, I_L})
14             Q ← PUSH(Q, {f_R, I_R})
15 RETURN L
```

πλήθος) των πραγματικών ριζών του f στο $\mathcal{I}$. Τέλος η συνάρτηση $\text{SPLIT}_{\text{SM}}(f, \mathcal{I})$ υποδιαιρεί το διάστημα $\mathcal{I}$ σε δύο ίσα υποδιαστήματα και ανάλογα με τον αλγόριθμο ενδεχομένως υποδιαιρεί και το f.

Παρατηρούμε ότι η πολυπλοκότητα του αλγορίθμου υποδιαίρεσης εξαρτάται από το πόσες φορές εκτελείται ο βρόγχος while (Γραμμή 5 στον Αλγ. 3) και από το κόστος των συναρτήσεων $\text{COUNT}_{\text{SM}}(f, \mathcal{I})$ και $\text{SPLIT}_{\text{SM}}(f, \mathcal{I})$. Επίσης, σε κάθε βήμα του αλγορίθμου, αφού το προς εξέταση διάστημα χωρίζεται σε δύο ίσα υποδιαστήματα, μπορούμε να υποθέσουμε ότι το δυαδικό μήκος των άκρων του διαστήματος αυξάνεται κατά ένα. Πιο συγκεκριμένα αν υποθέσουμε ότι τα άκρα του αρχικού διαστήματος $\mathcal{I}_0$, έχουν μήκος τ, τότε στο h βήμα του αλγορίθμου το δυαδικό μήκος των άκρων του προς εξέταση διαστήματος $\mathcal{I} \subseteq \mathcal{J}_0$ είναι $\tau + h$.

Οι διάφοροι αλγόριθμοι υποδιαίρεσης χαρακτηρίζονται ανάλογα με το πως υλοποιούν τις τρεις αυτές συναρτήσεις. Θα εξετάσουμε τρεις τέτοιους αλγορίθμους:

- τον αλγόριθμο STURM ή $\text{SUBDIVISIONSOLVER}_{\text{STURM}}$,
- τον αλγόριθμο DESCARTES ή $\text{SUBDIVISIONSOLVER}_{\text{DESCARTES}}$, και
- τον αλγόριθμο BERNSTEIN ή $\text{SUBDIVISIONSOLVER}_{\text{BERNSTEIN}}$.

Σημείωση 3.35. *Στον Αλγ. 3 θα πρέπει να προστεθεί ένας έλεγχος σχετικά με το αν το μέσο κάποιου προς εξέταση διαστήματος $\mathcal{I}$ αποτελεί ρίζα του f. Ο έλεγχος αυτός δεν επηρεάζει την πολυπλοκότητα του αλγορίθμου και γι' αυτό τον παραλείπουμε για λόγους απλότητας.*

Επιπρόσθετα, ο Αλγ. 3 μπορεί εύκολα να τροποποιηθεί έτσι ώστε να απομονώσει τις πραγματικές ρίζες του A_{red} σε κάποιο διάστημα $\mathcal{J} \subseteq \mathcal{I}_0$.

Ο αλγόριθμος STURM

Ο αλγόριθμος STURM μοιάζει περισσότερο από όλους τους αλγορίθμους υποδιαίρεσης με αυτόν της δυαδικής αναζήτησης. Χρησιμοποιεί αποτιμήσεις της προσημασμένης ακολουθίας υποεπιλθουσών $\mathbf{SR}(A_{red})$ προκειμένου να μετρήσει το πλήθος των πραγματικών ριζών του A_{red} που περιέχονται σε ένα διάστημα $\mathcal{I}$ (Θεωρ. 2.27).

Παρατηρούμε ότι το Θεωρ. 2.27 μας επιτρέπει να μετρήσουμε τις ρίζες ενός πολυωνύμου σε ένα διάστημα ακόμα και αν αυτό δεν είναι χωρίς τετράγωνα. Δηλαδή, θα μπορούσαμε να χρησιμοποιήσουμε την ακολουθία $\mathbf{SR}(A)$ αντί της $\mathbf{SR}(A_{red})$. Ωστόσο, προκειμένου να επιτύχουμε ομοιόμορφη παρουσίαση για όλους τους αλγορίθμους υποδιαίρεσης θα υποθέσουμε ότι η είσοδος είναι ένα πολυώνυμο χωρίς τετράγωνα, καθώς αυτή η υπόθεση (τελικά) δεν επηρεάζει σημαντικά τον υπολογισμό της πολυπλοκότητας.

Το ότι ο αλγόριθμος τερματίζει, εξασφαλίζεται από το ότι το $\mathbb{Q}$ είναι Αρχιμήδειο σώμα [14]. Ένα σώμα είναι Αρχιμήδειο αν μπορεί να οριστεί σε αυτό διάταξη, και άρα απόλυτη τιμή, και αν για κάθε στοιχείο του, έστω x, υπάρχει ένας φυσικός αριθμός n τέτοιος ώστε $|x| < n$. Κατά συνέπεια, οι συνεχείς υποδιαιρέσεις μικραίνουν τα διαστήματα, τα οποία τελικά γίνονται τόσο μικρά όσο το φράγμα διαχωρισμού. Προφανώς, σε διαστήματα με μήκος τόσο μικρό όσο το φράγμα διαχωρισμού περιέχεται μία ή καμία πραγματική ρίζα.

Algorithm 4: INITIALIZATION$_{\text{STURM}}(A_{red}, \mathcal{I})$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: $\mathbf{StHa}(A)$

1 COMPUTE $\mathbf{SR}(A_{red})$

Algorithm 5: COUNT$_{\text{STURM}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Το πλήθος των (διαφορετικών) πραγματικών ριζών του f στο $[\mathsf{a}, \mathsf{b}]$

1 RETURN VAR$(\mathbf{SR}(A\,;\,\mathsf{a}) - \text{VAR}(\mathbf{SR}(A\,;\,\mathsf{b}))$

Algorithm 6: SPLIT$_{\text{STURM}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Διαμέριση του διαστήματος $\mathcal{I}$ και του f

1 $\mathsf{m} \leftarrow \frac{\mathsf{a}+\mathsf{b}}{2}$
2 $\mathcal{I}_L \leftarrow [\mathsf{a}, \mathsf{m}]$
3 $\mathcal{I}_R \leftarrow [\mathsf{m}, \mathsf{b}]$
4 RETURN $\{f, \mathcal{I}_L\}, \{f, \mathcal{I}_R\}$

Παρουσιάζουμε τώρα την ανάλυση πολυπλοκότητας των διαφόρων συναρτήσεων που εμπλέκονται στην εκτέλεση του αλγορίθμου.

- INITIALIZATION$_{\text{STURM}}$ (Αλγ. 4)
  Η αρχικοποίηση του αλγορίθμου συνίσταται στο να υπολογίσουμε την ακολουθία $\mathbf{SR}(A_{red})$. Η πολυπλοκότητα της συνάρτησης είναι $\widetilde{\mathcal{O}}_B(d^2\tau)$ (Θεωρ. 2.31).

- SPLIT$_{\text{STURM}}$ (Αλγ. 6)
  Η συνάρτηση αυτή υπολογίζει το μέσον του $\mathcal{I}$ και επιστρέφει δύο υποδιαστήματα. Η πολυπλοκότητα της συνάρτησης είναι $\mathcal{O}_B(\tau + h)$.

- COUNT$_{\text{STURM}}$ (Αλγ. 5)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση διάστημα είναι το $\mathcal{I}$. Τα άκρα του $\mathcal{I}$ έχουν δυαδικό μήκος φραγμένο από $\tau + h$.

  Το κόστος της συνάρτησης εξαρτάται από το κόστος αποτίμησης της ακολουθίας $\mathbf{SR}(A_{red})$ πάνω στα άκρα του $\mathcal{I}$, το οποίο είναι $\widetilde{\mathcal{O}}_B\left(d^2(\tau + h)\right)$ (Θεωρ. 2.32).

  Υπενθυμίζουμε ότι η συνάρτηση COUNT$_{\text{STURM}}(f, \mathcal{I})$ μετρά *ακριβώς* το πλήθος των πραγματικών ριζών του f στο $\mathcal{I}$.

Σημείωση 3.36. *Παρατηρούμε ότι δεν χρειάζεται να περνάμε ως παράμετρο κάποιο πολυώνυμο f στις συναρτήσεις* SPLIT$_{\text{STURM}}$ *και* COUNT$_{\text{STURM}}$. *Παρ'όλα αυτά το κάνουμε προκειμένου ο ψευδοκώδικας να είναι ο ίδιος σε όλους τους αλγορίθμους υποδιαίρεσης. Επίσης, σε όλη τη διάρκεια του αλγορίθμου $f \equiv A_{red}$.*

Ο αλγόριθμος DESCARTES

Algorithm 7: INITIALIZATION$_{\text{DESCARTES}}(A_{red}, \mathcal{I}_0)$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I}_0 = [\mathsf{a}, \mathsf{b}]$
Output: Το A_{red} μετασχηματίζεται έτσι ώστε όλες οι ρίζες του στο $\mathcal{I}_0$ να είναι στο $(0, 1)$

1 $A_{red} \leftarrow A_{red}\left((\mathsf{b} - \mathsf{a})X + \mathsf{a}\right)$

Algorithm 8: COUNT$_{\text{DESCARTES}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$
Output: Ένα άνω φράγμα στις πραγματικές ρίζες του f στο $(0, 1)$

1 $g \leftarrow \mathcal{T}_{-1}(\mathcal{R}(f))(X)$
2 RETURN VAR(g)

Algorithm 9: SPLIT$_{\text{DESCARTES}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$
Output: Διαμέριση του διαστήματος $\mathcal{I}$ και του f

1 $\mathsf{m} \leftarrow \frac{\mathsf{a}+\mathsf{b}}{2}$
2 $\mathcal{I}_L \leftarrow [\mathsf{a}, \mathsf{m}]$
3 $\mathcal{I}_R \leftarrow [\mathsf{m}, \mathsf{b}]$
4 $f_L \leftarrow \mathcal{H}_2'(f)(X)$
5 $f_R \leftarrow \mathcal{T}_{-1}(\mathcal{H}_2'(f))(X)$
6 RETURN $\{f_L, \mathcal{I}_L\}, \{f_R, \mathcal{I}_R\}$

Ο αλγόριθμος DESCARTES, όπως ήδη έχουμε αναφέρει, βασίζεται στον κανόνα προσήμων του Descartes (Θεωρ. 3.28).

Αρχικά το A_{red} μετασχηματίζεται έτσι ώστε όλες οι ρίζες του στο $\mathcal{I}_0$ να περιέχονται πλέον στο $(0,1)$. Στο βήμα h του αλγορίθμου πρέπει να εξεταστεί το ζεύγος $\{f, \mathcal{I}\}$. Οι ρίζες του προς εξέταση πολυωνύμου f στο $(0,1)$ αντιστοιχούν στις ρίζες του A_{red} στο $\mathcal{I}$. Αν το f έχει περισσότερες από μία ρίζες τότε υπολογίζονται δύο υποδιαστήματα του $\mathcal{I}$, τα $\mathcal{I}_L$ και $\mathcal{I}_R$, όπως επίσης και δύο πολυώνυμα, f_L και f_R, τέτοια ώστε οι ρίζες του f_L, αντίστοιχα f_R, στο $(0,1)$ να αντιστοιχούν στις ρίζες του A_{red} στο $\mathcal{I}_L$, αντίστοιχα $\mathcal{I}_R$, και ο αλγόριθμος επαναλαμβάνεται.

Παρατηρούμε ότι ο κανόνας προσήμων του Descartes δίνει στη γενική περίπτωση μια υπερεκτίμηση για το πλήθος των θετικών πραγματικών ριζών. Κατά συνέπεια οι υποδιαιρέσεις συνεχίζονται μέχρι τα προς εξέταση διαστήματα να έχουν μήκος τόσο όσο υποδηλώνουν τα θεωρήματα του ενός και των δύο κύκλων (Θεωρ. 3.32 και Θεωρ. 3.33) προκειμένου να εξασφαλίσουμε ότι θα έχουμε μία ή καμία εναλλαγή προσήμων και άρα ο κανόνας των προσήμων θα υπολογίσει ακριβώς το πλήθος των θετικών πραγματικών ριζών. Το γεγονός ότι το $\mathbb{Q}$ είναι Αρχιμήδειο σώμα εξασφαλίζει ότι από τις υποδιαιρέσεις τελικώς θα προκύψουν τέτοια (μικρά) διαστήματα και άρα ο αλγόριθμος θα τερματίσει.

Παρουσιάζουμε τώρα την ανάλυση πολυπλοκότητας των διαφόρων συναρτήσεων που εμπλέκονται στην εκτέλεση του αλγορίθμου.

- $\text{INITIALIZATION}_{\text{DESCARTES}}$ (Αλγ. 7)
  Η αρχικοποίηση του αλγορίθμου συνίσταται στο να μετασχηματίσουμε το A_{red} σε ένα πολυώνυμο $\overline{A}_{red}$ τέτοιο ώστε οι ρίζες του A_{red} στο $\mathcal{I}_0$ να αντιστοιχούν στις ρίζες του $\overline{A}_{red}$ στο $(0,1)$. Αυτό επιτυγχάνεται με τον μετασχηματισμό $\phi(X) = (\mathsf{b}-\mathsf{a})X + \mathsf{a}$. Θεωρούμε ότι $\mathcal{L}(\mathsf{a}) = \mathcal{L}(\mathsf{b}) = \tau$ και άρα η πολυπλοκότητα της αρχικοποίησης είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Εν. 2.2). Παρατηρούμε ότι για το $\overline{A}_{red}$ ισχύει $\deg(\overline{A}_{red}) = d$ και $\mathcal{L}\left(\overline{A}_{red}\right) = \mathcal{O}(d\tau)$.

  Προκειμένου να μην επιβαρύνουμε τον συμβολισμό θα συμβολίσουμε το $\overline{A}_{red}$ πάλι με A_{red}.

- $\text{COUNT}_{\text{DESCARTES}}$ (Αλγ. 8)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Οι ρίζες του f στο $(0,1)$ αντιστοιχούν στις ρίζες του αρχικού πολυωνύμου στο $\mathcal{I}$. Παρατηρούμε ότι τα άκρα του $\mathcal{I}$ έχουν δυαδικό μήκος φραγμένο από $\tau + h$. Επίσης το προς εξέταση πολυώνυμο έχει δυαδικό μήκος $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$, όπως προκύπτει από την συνάρτηση SPLIT.

  Προκειμένου να μετρήσουμε τις ρίζες του f στο $(0,1)$ υπολογίζουμε το πολυώνυμο $g = \mathcal{T}_{-1} \circ \mathcal{R} \circ f$. Οι ρίζες του g στο $(0,\infty)$ αντιστοιχούν στις ρίζες του f στο $(0,1)$.

  Προκειμένου να μετρήσουμε τις ρίζες χρησιμοποιούμε τον κανόνα προσήμων του Descartes (Θεωρ. 3.28), άρα αρκεί να υπολογίσουμε τις αλλαγές προσήμων στους συντελεστές του g.

  Ο μετασχηματισμός αντιστροφής, $\mathcal{R}$, δεν αλλάζει το μέγιστο δυαδικό μήκος των συντελεστών και απαιτεί $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B\left(d(d\tau + dh)\right)$ (Εν. 2.2).

  Ο μετασχηματισμός $\mathcal{T}_{-1} \circ \mathcal{R} \circ f$ έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2 \lg d + d(d\tau + dh) + d^2)$ και $\mathcal{L}(g) = \mathcal{O}(d\tau + (d+1)h)$ (Εν. 2.2).

  Η συνάρτηση $\texttt{VAR}(g)$ απαιτεί $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B\left(d(d\tau + (d+1)h)\right)$.

Συνεπώς το συνολικό κόστος της συνάρτησης είναι $\widetilde{\mathcal{O}}_B(d^2 \lg d + d^2\tau + d^2 h)$.

- SPLIT$_{\text{DESCARTES}}$ (Αλγ. 9)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Παρατηρούμε ότι τα άκρα του $\mathcal{I}$ έχουν δυαδικό μήκος φραγμένο από $\tau + h$. Επίσης το προς εξέταση πολυώνυμο έχει δυαδικό μήκος $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$.

  Υπολογίζουμε το μέσον του διαστήματος $\mathcal{I}$ με πολυπλοκότητα $\mathcal{O}_B(\tau + h)$.

  Εφόσον $f_L = \mathcal{H}_2^{'}(f)(X)$ ο υπολογισμός του απαιτεί $\mathcal{O}(d)$ πράξεις ολίσθησης και $\mathcal{L}(f_L) = \mathcal{O}(d\tau + dh + d)$ (Εν. 2.2).

  Παρατηρούμε ότι $f_R = \mathcal{T}_{-1}(\mathcal{H}_2^{'}(f) = \mathcal{T}_{-1}(f_L)(X)$. Συνεπώς ο υπολογισμός του έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2 \lg d + d(d\tau + (d+1)h + d) + d^2)$ και $\mathcal{L}(f_R) = \mathcal{O}(d\tau + dh + 2d)$ (Εν. 2.2).

  Συμπεραίνουμε ότι η συνολική πολυπλοκότητα της συνάρτησης είναι $\widetilde{\mathcal{O}}_B(d^2 \lg d + d^2\tau + d^2 h)$ και ότι $\mathcal{L}(f_L) = \mathcal{L}(f_R) = \mathcal{O}(d\tau + dh)$.

  Μια σημαντική παρατήρηση αφορά το μέγιστο δυαδικό μήκος των συντελεστών των f_L και f_R. Αρχικά $\mathcal{L}(A_{red}) = d\tau$. Σε κάθε βήμα του αλγορίθμου υπόκειται (το πολύ) σε μια ομοθεσία και σε μία μετατόπιση και άρα οι συντελεστές του αυξάνουν (το πολύ) κατά έναν προσθετικό παράγοντα d. Γι' αυτό υποθέτουμε ότι στο h βήμα του αλγορίθμου $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$.

Ο αλγόριθμος BERNSTEIN

Algorithm 10: INITIALIZATION$_{\text{BERNSTEIN}}(A_{red}, \mathcal{I}_0)$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I}_0 = [\mathsf{a}, \mathsf{b}]$
Output: Το A_{red} μετασχηματίζεται στη βάση Bernstein στο διάστημα $\mathcal{I}_0$

1 $A_{red} \leftarrow \sum_{i=0}^{d} b_i \mathfrak{B}_d^i(X; \mathsf{a}, \mathsf{b})$

Algorithm 11: COUNT$_{\text{BERNSTEIN}}(f, \mathcal{I})$

Input: $f = \sum_{i=0}^{d} b_i \mathfrak{B}_i^d(X)$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Ένα άνω φράγμα στις πραγματικές ρίζες του f στο $\mathcal{I}$

1 RETURN VAR$(b_0, \ldots, b_d)$

Algorithm 12: SPLIT$_{\text{BERNSTEIN}}(f, \mathcal{I})$

Input: $f = \sum_{i=0}^{d} b_i \mathfrak{B}_i^d(X)$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Διαμέριση του διαστήματος $\mathcal{I}$ και του f

1 $\mathsf{m} \leftarrow \frac{\mathsf{a}+\mathsf{b}}{2}$
2 $\mathcal{I}_L \leftarrow [\mathsf{a}, \mathsf{m}]$
3 $\mathcal{I}_R \leftarrow [\mathsf{m}, \mathsf{b}]$
4 $f_L \leftarrow \overline{\mathcal{S}}_L(f)(X)$
5 $f_R \leftarrow \overline{\mathcal{S}}_R(f)(X)$
6 RETURN $\{f_L, \mathcal{I}_L\}, \{f_R, \mathcal{I}_R\}$

Μια απλή παρατήρηση που μπορεί να γίνει στον αλγόριθμο του DESCARTES είναι ότι είναι ανεξάρτητος από το βάση στην οποία αναπαρίσταται το πολυώνυμο. Στον αλγόριθμο DESCARTES που παρουσιάσαμε υποθέσαμε ότι τα πολυώνυμα είναι στη βάση των δυνάμεων. Ο αλγόριθμος BERNSTEIN υποθέτει πολυώνυμα στη βάση Bernstein (Εν. 2.4). Ο λόγος χρησιμοποίησης αυτής της αναπαράστασης είναι ότι η αριθμητική ευστάθεια των πολυωνύμων στη βάση αυτή είναι πολύ καλή και έτσι τα αποτελέσματα του αλγορίθμου αν υλοποιηθεί με αριθμούς κινητής υποδιαστολής ή και με αριθμητική διαστημάτων είναι αριθμητικά ευσταθή. Επιπρόσθετα, οι βρόγχοι των διαφόρων υπολογισμών που εμπλέκονται στην υλοποίηση του αλγορίθμου είναι πιο σφιχτοί από ότι στον αλγόριθμο DESCARTES και συνεπώς πιο γρήγοροι στην πράξη. Τέλος, ο έλεγχος για το πλήθος των ριζών είναι πολύ πιο απλοποιημένος από αυτόν του DESCARTES.

Κατά τα λοιπά ο αλγόριθμος ομοιάζει με τον DESCARTES. Αρχικά το πολυώνυμο αναπαρίσταται στη βάση Bernstein στο διάστημα $\mathcal{I}_0$. Στο βήμα h του αλγορίθμου πρέπει να εξεταστεί το ζεύγος $\{f, \mathcal{I}\}$. Οι ρίζες του προς εξέταση πολυωνύμου f στο $\mathcal{I}$ αντιστοιχούν στις ρίζες του A_{red} στο $\mathcal{I}$. Αν το f έχει περισσότερες από μία ρίζες τότε υπολογίζονται δύο υποδιαστήματα του $\mathcal{I}$, τα $\mathcal{I}_L$ και $\mathcal{I}_R$ και η αναπαράσταση του f στη βάση Bernstein στα δύο αυτά υποδιαστήματα χρησιμοποιώντας τις απεικονίσεις (2.20) και (2.21) και ο αλγόριθμος επαναλαμβάνεται.

Το ότι ο αλγόριθμος τερματίζει εξασφαλίζεται, όπως και στην περίπτωση του DESCARTES, από τα θεωρήματα του ενός και των δύο κύκλων (Θεωρ. 3.32 και Θεωρ. 3.33) και από το ότι το $\mathbb{Q}$ είναι Αρχιμήδειο.

- INITIALIZATION$_{\text{BERNSTEIN}}$ (Αλγ. 10)
  Η αρχικοποίηση του αλγορίθμου συνίσταται στο να αναπαραστήσουμε το A_{red} στη βάση Bernstein στο διάστημα $\mathcal{I}$. Η μετατροπή απαιτεί $\mathcal{O}(d^2)$ αριθμητικές πράξεις και οι συντελεστές του νέου πολυωνύμου έχουν δυαδικό μήκος $\mathcal{O}(d\tau)$, δείτε Εν. 2.4 και [203, 205].

  Άρα το κόστος της αρχικοποίησης είναι φραγμένο από $\widetilde{\mathcal{O}}_B(d^3\tau)$. Το νέο πολυώνυμο στη βάση Bernstein θα το συμβολίσουμε ξανά με A_{red} προκειμένου να μην επιβαρύνουμε τον συμβολισμό.

- COUNT$_{\text{BERNSTEIN}}$ (Αλγ. 11)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Για το f ισχύει ότι $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$.

  Η συνάρτηση $\mathtt{VAR}(f) = \mathtt{VAR}(b_0, \ldots, b_d)$ απαιτεί $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B\left(d(d\tau + dh)\right)$.

- SPLIT$_{\text{BERNSTEIN}}$ (Αλγ. 12)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Για το f ισχύει ότι $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$, όπως ακριβώς και στον αλγόριθμο DESCARTES.

  Υπολογίζουμε τις αναπαραστάσεις του f στη βάση Bernstein για τα διαστήματα $\mathcal{I}_L$ και $\mathcal{I}_R$, f_L και f_R, χρησιμοποιώντας τις απεικονίσεις (2.20) και (2.21), με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d(d + d\tau + d\,h)) = \widetilde{\mathcal{O}}_B(d^3 + d^2\tau + d^2h)$ (Πρότ. 2.36).

Το δένδρο διαμέρισης

Προκειμένου να ολοκληρώσουμε την ανάλυση πολυπλοκότητας των αλγορίθμων υποδιαίρεσης πρέπει να υπολογίσουμε το πλήθος των βημάτων που εκτελούν. Υπενθυμίζουμε ότι αλγόριθμοι υποδιαίρεσης ακολουθούν τη φιλοσοφία του αλγορίθμου της δυαδικής αναζήτησης. Κατά συνέπεια, μπορούμε να υποθέσουμε ένα δυαδικό δένδρο, έστω T, ανάλογο με αυτό της δυαδικής αναζήτησης, το οποίο στη ρίζα του έχει το αρχικό διάστημα, $\mathcal{I}_0$ που περιέχει όλες τις πραγματικές ρίζες του A_{red} και το οποίο υποδιαιρείται κατά την εκτέλεση των αλγορίθμων. Το δένδρο αυτό το ονομάζουμε *δένδρο διαμέρισης*. Ο αριθμός των βημάτων που εκτελούν οι αλγόριθμοι υποδιαίρεσης ισούται με το πλήθος των κόμβων του δένδρου διαμέρισης, το οποίο συμβολίζουμε με $\#(T)$. Σε κάθε κόμβο του T αντιστοιχούμε ένα υποδιάστημα του $\mathcal{I}_0$. Παρατηρούμε ότι τα διαστήματα που αντιστοιχούν σε κόμβους στο ίδιο βάθος του δένδρου έχουν για άκρα ρητούς αριθμούς με το ίδιο δυαδικό μήκος καθώς έχουν προκύψει μετά από ίσο αριθμό υποδιαιρέσεων. Επίσης, τα φύλλα του δένδρου περιέχουν διαστήματα που περιέχουν είτε μία είτε καμία πραγματική ρίζα του f και το μήκος τους (των διαστημάτων) δεν είναι μικρότερο από το διάστημα απομόνωσης. Στόχος μας είναι να φράξουμε το $\#(T)$.

Έστω $\mathfrak{I}$ το σύνολο των διαστημάτων τα οποία έχουν δύο παιδιά φύλλα στο δένδρο διαμέρισης. Εκ κατασκευής, αν $\mathcal{I} \in \mathfrak{I}$ τότε $\text{COUNT}_{\text{SM}}(f, \mathcal{I}) \geq 2$, γιατί αλλιώς δεν υπήρχε λόγος να το υποδιαιρέσουμε περαιτέρω. Ωστόσο, για τα δύο παιδιά του $\mathcal{I}$, έστω $\mathcal{I}_L$ και $\mathcal{I}_R$, ισχύει $\text{COUNT}_{\text{SM}}(f_L, \mathcal{I}_L) \in \{0, 1\}$, αντίστοιχα $\text{COUNT}_{\text{SM}}(f_R, \mathcal{I}_R) \in \{0, 1\}$, επειδή είναι φύλλα στο δένδρο διαμέρισης. Αν ενδιαφερόμαστε μόνο για τον αλγόριθμο STURM τότε ισχύουν οι πιο αυστηρές σχέσεις $\text{COUNT}_{\text{STURM}}(f, \mathcal{I}) = 2$ και $\text{COUNT}_{\text{STURM}}(f_L, \mathcal{I}_L) = \text{COUNT}_{\text{STURM}}(f_R, \mathcal{I}_R) = 1$, επειδή ο αλγόριθμος αυτός μετρά ακριβώς το πλήθος των ριζών σε κάποιο διάστημα.

Παρατηρούμε ότι $|\mathfrak{I}|$ είναι μικρότερο ή ίσο από $\text{COUNT}_{\text{SM}}(A_{red}, \mathcal{I}_0)$, καθώς σε κάθε διαμέριση το άθροισμα των εναλλαγών προσήμων του f δεν αυξάνεται και για τους τρεις αλγορίθμους. Ειδικά για τον αλγόριθμο BERNSTEIN, δείτε [14, 203, 205]. Πιο συγκεκριμένα ισχύει $|\mathfrak{I}| \leq \text{COUNT}_{\text{SM}}(A_{red}, \mathcal{I}_0) \leq d$.

Αν για κάποια (μιγαδική) ρίζα του f, έστω α, το πραγματικό της μέρος ανήκει σε ένα διάστημα $\mathcal{I}$, $\Re(\alpha) \in \mathcal{I}$, τότε θα τη συμβολίζουμε με $\alpha_{\mathcal{I}}$. Μπορούμε να αποδείξουμε την ακόλουθη πρόταση, η οποία είναι σημαντική από μόνη της και θα μας βοηθήσει στο να φράξουμε το πλήθος των διαμερίσεων.

Πρόταση 3.37. *Έστω $\mathcal{I} \in \mathfrak{I}$. Υπάρχουν δύο διαφορετικές (μιγαδικές) ρίζες $\alpha_{\mathcal{I}} \neq \beta_{\mathcal{I}}$ του f τέτοιες ώστε $|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| < 2\,|\mathcal{I}|$.*

Απόδειξη: Θεωρούμε ένα διάστημα $\mathcal{I} \in \mathfrak{I}$, τα δύο παιδιά του $\mathcal{I}_L$ και $\mathcal{I}_R$ στο δένδρο διαμέρισης και τα πολυώνυμα f_L και f_R που αντιστοιχούν σε αυτά. Υπάρχουν οι ακόλουθες περιπτώσεις σχετικά με τις εναλλαγές προσήμων των f_L και f_R στα δύο υποδιαστήματα $\mathcal{I}_L$ και $\mathcal{I}_R$:

- $(1, 1)$: για όλους τους αλγορίθμους, υπάρχουν δύο, διαφορετικές μεταξύ τους, πραγματικές ρίζες $\alpha \in \mathcal{I}_L$ και $\beta \in \mathcal{I}_R$ στο διάστημα $\mathcal{I}$. Συνεπώς $|\alpha - \beta| \leq |\mathcal{I}|$. Αυτή είναι και η μοναδική περίπτωση για τον αλγόριθμο STURM.

- $(0, 0)$: αυτή η περίπτωση μπορεί να παρουσιαστεί μόνο στους αλγορίθμους DESCARTES και BERNSTEIN. Εφόσον ισχύει $\text{COUNT}_{\text{SM}}(f, \mathcal{I}) \geq 2$, από το θεώρημα του ενός κύκλου

(Θεωρ. 3.32) συνεπάγεται ότι υπάρχουν δύο συζυγείς μιγαδικές ρίζες $\beta, \overline{\beta}$ στον δίσκο $D(m(\mathcal{I}), \frac{|\mathcal{I}|}{2})$. Συνεπώς $|\beta - \overline{\beta}| \leq |\mathcal{I}|$.

- $(1,0)$ ή $(0,1)$: αυτή η περίπτωση μπορεί να παρουσιαστεί μόνο στους αλγορίθμους DESCARTES και BERNSTEIN. Υπάρχει μία πραγματική ρίζα α στο $\mathcal{I}$. Εφόσον $\text{COUNT}_{\text{SM}}(f, \mathcal{I}) \geq 2$, από το θεώρημα των δύο κύκλων (Θεωρ. 3.33) υπάρχουν δύο συζυγείς μιγαδικές ρίζες $\beta, \overline{\beta}$ στην ένωση των δίσκων $D(m(\mathcal{I}) \pm \frac{1}{2\sqrt{3}}\mathbf{i}|\mathcal{I}|, \frac{1}{\sqrt{3}}|\mathcal{I}|)$. Η ένωση περιέχεται στο δίσκο με διάμετρο $2\,|\mathcal{I}|$. Συνεπώς $|\beta - \alpha| < 2|\mathcal{I}|$.

Και η πρόταση αποδείχτηκε. ΟΕΔ

Πρόταση 3.38. *Οι αλγόριθμοι διαμέρισης εκτελούν $\mathcal{O}(d^2 + d\,\tau)$ βήματα.*

Απόδειξη: Ο αριθμός των βημάτων που εκτελούν οι αλγόριθμοι διαμέρισης ισούται με το πλήθος των κόμβων του δένδρου διαμέρισης, τον οποίο θα συμβολίσουμε με $\#(T)$.

Παρατηρούμε ότι το $\#(T)$ είναι μικρότερο ή ίσο από δύο φορές το άθροισμα των κόμβων που περιέχονται στο μονοπάτι από κάθε $\mathcal{I} \in \mathfrak{I}$ στη ρίζα του δένδρου. Επιπρόσθετα το πλήθος των κόμβων στο μονοπάτι από $\mathcal{I} \in \mathfrak{I}$ στη ρίζα του δένδρου διαμέρισης είναι $\lg \frac{|\mathcal{I}_0|}{|\mathcal{I}|}$. Συνεπώς

$$\begin{aligned}
\#(T) &\leq 2 \sum_{\mathcal{I} \in \mathfrak{I}} \lg \frac{|\mathcal{I}_0|}{|\mathcal{I}|} \\
&\leq 2\,|\mathfrak{I}|\ \lg |\mathcal{I}_0| - 2 \sum_{\mathcal{I} \in \mathfrak{I}} \lg |\mathcal{I}| \\
&\leq 2\,|\mathfrak{I}|\ \lg |\mathcal{I}_0| + |\mathfrak{I}| - \sum_{\mathcal{I} \in \mathfrak{I}} \lg |\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| \\
&\leq 2\,|\mathfrak{I}|\ \lg |\mathcal{I}_0| + |\mathfrak{I}| - \lg \prod_{\mathcal{I} \in \mathfrak{I}} |\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}|
\end{aligned} \tag{3.5}$$

όπου στην προτελευταία ανισότητα χρησιμοποιήσαμε το γεγονός ότι από την Εν. 3.37 ισχύει

$$|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| \leq 2\,|\mathcal{I}| \Rightarrow 1 - \lg |\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| \geq -\lg |\mathcal{I}|$$

Για το αρχικό διάστημα $\mathcal{I}_0$, χρησιμοποιώντας ένα από τα απόλυτα φράγματα εγκλεισμού όλων των (πραγματικών) ριζών (Εν. 3.2), ισχύει

$$\mathcal{I}_0 = [-2^\tau, 2^\tau] \Rightarrow \lg |\mathcal{I}_0| = \tau + 1 \tag{3.6}$$

Επίσης, καθώς σε κάθε επίπεδο του δένδρου διαμέρισης δεν μπορούμε να έχουμε περισσότερα από d διαστήματα προς εξέταση, ισχύει

$$|\mathfrak{I}| \leq d \tag{3.7}$$

Προκειμένου να εφαρμόσουμε το Θεωρ. 3.27 στην (3.5), πρέπει να αναδιατάξουμε την ποσότητα $\prod_{\mathcal{I} \in \mathfrak{I}} |\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}|$ έτσι ώστε οι απαιτήσεις για τους δείκτες των ριζών να ικανοποιούνται. Οι προϋποθέσεις του θεωρήματος δεν ικανοποιούνται αν εμφανίζονται συμμετρικά γινόμενα.

Θεωρούμε τη χειρότερη περίπτωση, να εμφανίζονται *μόνο* συμμετρικά γινόμενα, δηλαδή η ποσότητά μας είναι της μορφής $\prod|(\alpha_{\mathcal{I}}-\beta_{\mathcal{I}})(\beta_{\mathcal{I}}-\alpha_{\mathcal{I}})|$. Κατά συνέπεια, θεωρούμε το τετράγωνο της ανισότητας του Θεωρ. 3.27 αντικαθιστώντας την ποσότητα k με $\frac{|\mathfrak{I}|}{2}$ και λαμβάνοντας υπ' όψιν ότι $\mathsf{disc}(A_{red})\geq 1$ (αφού το A_{red} είναι χωρίς τετράγωνα), έχουμε

$$\begin{aligned}\prod_{\mathcal{I}\in\mathfrak{I}}|\alpha_{\mathcal{I}}-\beta_{\mathcal{I}}| \;&\geq\; \left(2^{\frac{|\mathfrak{I}|}{2}-\frac{d(d-1)}{2}}\,\mathcal{M}(f)^{1-d-\frac{|\mathfrak{I}|}{2}}\right)^2\\ -\lg\prod_{I\in\mathfrak{I}}|\alpha_{\mathcal{I}}-\beta_{\mathcal{I}}| \;&\leq\; d^2-d+|\mathfrak{I}|+(2d+|\mathfrak{I}|-2)\lg\mathcal{M}(f)\end{aligned}\tag{3.8}$$

Λαμβάνοντας υπόψιν ότι $\lg\mathcal{M}(f)\leq\tau+\frac{1}{2}\lg(d+1)$ (Λημ. 3.4) και συνδυάζοντας τις εξισώσεις (3.6), (3.7) και (3.8) με την εξίσωση (3.5) έχουμε ότι

$$\#(T)\leq 2\,d\,(\tau+1)+d+d^2+(3d-1)(\tau+\frac{1}{2}\lg(d+1))$$

Και τελικά $\#(T)=\mathcal{O}(d^2+d\tau+d\lg d)$. ΟΕΔ

Σημείωση 3.39. *Μπορεί να αποδειχτεί ότι $\#(T)=\mathcal{O}(d\tau+d\lg d)$, χρησιμοποιώντας το Θεωρ. 3.26 και έτσι να γλυτώσουμε έναν παράγοντα d^2 [65, 76, 81, 91, 97]. Ωστόσο η απόδειξη είναι πολύ πιο δύσκολη σε αυτή την περίπτωση καθώς απαιτείται να αποδείξουμε ότι πάντοτε μπορούμε να αναδιατάξουμε τα γινόμενα των ριζών στην* (3.8) *με τέτοιο τρόπο ώστε οι απαιτήσεις του Θεωρ. 3.26 να ικανοποιούνται. Επιπρόσθετα, ο παράγοντας d^2 δεν παίζει κανένα ρόλο όταν $d=\mathcal{O}(\tau)$ ή όταν το πολυώνυμο που επιλύουμε δεν είναι χωρίς τετράγωνα.*

Πολυπλοκότητα των αλγορίθμων υποδιαίρεσης

Θα αποδείξουμε ότι η πολυπλοκότητα των αλγορίθμων υποδιαίρεσης είναι $\widetilde{\mathcal{O}}_B(d^4\tau^2)$. Υποθέτουμε (καταρχάς) $d=\mathcal{O}(\tau)$ για να απλοποιήσουμε τον συμβολισμό.

Θεώρημα 3.40 (SUBDIVISIONSOLVER**)**

Έστω $A_{red}\in\mathbb{Z}[x]$ χωρίς τετράγωνα, τέτοιο ώστε $\deg(A_{red})=d$ και $\mathcal{L}(A_{red})=\tau$. Οι αλγόριθμοι υποδιαίρεσης STURM, DESCARTES *και* BERNSTEIN *για την απομόνωση των πραγματικών ριζών του A_{red} έχουν πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\,\tau^2)$.*

Επιπρόσθετα το δυαδικό μήκος των ρητών αριθμών που είναι άκρα των διαστημάτων απομόνωσης φράσσεται από $\mathcal{O}(d\,\tau)$.

Απόδειξη: Τα άκρα των διαστημάτων απομόνωσης έχουν δυαδικό μήκος το πολύ $\mathcal{O}(d\tau)$, όπως προκύπτει από το φράγμα διαχωρισμού (Σημ. 3.24). Υπενθυμίζουμε ότι το πλήθος των βημάτων και για τους τρεις αλγορίθμους είναι $\mathcal{O}(d^2+d\tau)$. Εξετάζουμε κάθε αλγόριθμο ξεχωριστά.

- STURM

  Στη χειρότερη περίπτωση πρέπει να αποτιμήσουμε την $\mathbf{SR}(A_{red})$ πάνω σε κάποιο ρη-

τό αριθμό δυαδικού μήκους $\mathcal{O}(d\tau)$. Η πολυπλοκότητα της αποτίμησης είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Θεωρ. 2.32). Εφόσον χρειάζεται να εκτελέσουμε το πολύ $\mathcal{O}(d^2+d\tau)$ τέτοιες αποτιμήσεις (Πρότ. 3.38), το συνολικό κόστος του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^5\tau+d^4\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

- DESCARTES
  Το κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^2\lg d+d^2\tau+d^2h)$ για την συνάρτηση COUNT και $\widetilde{\mathcal{O}}_B(d^2\lg d+d^2\tau+d^2h)$ για τη συνάρτηση SPLIT (Εν. 3.5). Το συνολικό κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^2\lg d+d^2\tau+d^2h)$.

  Αθροίζοντας πάνω σε όλα τα βήματα του αλγορίθμου που είναι $\sum h = \widetilde{\mathcal{O}}_B(d^2+d\tau)$ (Πρότ. 3.38), συμπεραίνουμε ότι η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^6+d^5\tau+d^4\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

- BERNSTEIN
  Το κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^2\tau+d^2h)$ για τη συνάρτηση COUNT και $\widetilde{\mathcal{O}}_B(d^3+d^2\tau+d^2h)$ για τη συνάρτηση SPLIT (Εν. 3.5). Το συνολικό κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^3+d^2\tau+d^2h)$.

  Αθροίζοντας πάνω σε όλα τα βήματα του αλγορίθμου που είναι $\sum h = \widetilde{\mathcal{O}}_B(d^2+d\tau)$ (Πρότ. 3.38), συμπεραίνουμε ότι η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^6+d^5\tau+d^4\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

Και το θεώρημα αποδείχτηκε. ΟΕΔ

Όταν πρέπει να απομονώσουμε τις πραγματικές ρίζες ενός πολυωνύμου A, το οποίο δεν είναι χωρίς τετράγωνα και/ή θέλουμε να υπολογίσουμε τις πολλαπλότητες των πραγματικών ριζών τότε μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο REALROOTSOLVER (Αλγ. 1) αντικαθιστώντας τη συνάρτηση REALROOTISOLATOR με κάποιον από τους αλγορίθμους STURM, DESCARTES ή BERNSTEIN. Η πολυπλοκότητα του REALROOTSOLVER είναι το μέγιστο ανάμεσα στην πολυπλοκότητα του REALROOTISOLATOR και του $\widetilde{\mathcal{O}}_B(d^3\tau)$. Επιπρόσθετα θα πρέπει να λάβουμε υπόψιν μας ότι το δυαδικό μήκος του A_{red} είναι $\mathcal{O}(d+\tau)$ (Θεωρ. 2.34) καθώς αντιπροσωπεύει το μέγιστο δυαδικό μήκος των συντελεστών του χωρίς τετράγωνα μέρους του πολυωνύμου A.

Μπορούμε να διατυπώσουμε το ακόλουθο πιο γενικό θεώρημα.

Θεώρημα 3.41 (REALROOTSOLVER)

Έστω $A\in\mathbb{Z}[X]$ τέτοιο ώστε $\deg(A)=d$ και $\mathcal{L}(A)=\tau$, όχι απαραίτητα χωρίς τετράγωνα. Η πολυπλοκότητα του αλγορίθμου REALROOTSOLVER *για την απομόνωση και τον υπολογισμό των πολλαπλοτήτων των πραγματικών ριζών του A, χρησιμοποιώντας ως* REALROOTISOLATOR *οποιουδήποτε από τους αλγορίθμους* STURM, DESCARTES *και* BERNSTEIN *είναι $\widetilde{\mathcal{O}}_B(d^6+d^5\,\tau+d^4\,\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ αν $d=\mathcal{O}(\tau)$.*

Επιπρόσθετα, το δυαδικό μήκος των ρητών αριθμών που είναι άκρα των διαστημάτων απομόνωσης φράσσεται από $\mathcal{O}(d\,\tau)$.

Σημείωση 3.42. *Αν θεωρήσουμε ότι* $N = \max\{d, \tau\}$*, τότε η πολυπλοκότητα των παραπάνω αλγορίθμων είναι* $\widetilde{\mathcal{O}}_B(N^6)$*. Υπενθυμίζουμε ότι η πολυπλοκότητα των αριθμητικών (προσεγγιστικών) αλγορίθμων είναι* $\widetilde{\mathcal{O}}_B(d^3\tau) = \widetilde{\mathcal{O}}_B(N^4)$*.*

Όσον αφορά τους αλγορίθμους DESCARTES και BERNSTEIN θα μπορούσαμε να μην υπολογίσουμε το χωρίς τετράγωνα μέρος του A_{red}. Σε αυτή την περίπτωση θα βασιζόμασταν σε μια γενίκευση του θεωρήματος του Vincent (Θεωρ. 3.43), η οποία οφείλεται στο Wang [6]. Χρησιμοποιώντας αυτό το θεώρημα μπορούμε να συνεχίσουμε τις υποδιαιρέσεις μέχρι να φτάσουμε το φράγμα διαχωρισμού. Τότε ο αριθμός των εναλλαγών προσήμων θα υποδήλωνε την πολλαπλότητα της πραγματικής ρίζας που θα είχαμε απομονώσει.

Η προσέγγιση αυτή αν και σημαντική γιατί καταρρίπτει την μέχρι σήμερα γνωστή υπόθεση ότι οι οι αλγόριθμοι που στηρίζονται στον κανόνα προσήμων του Descartes πρέπει να απαιτούν πολυώνυμο χωρίς τετράγωνα, δεν συνίσταται για πρακτικές εφαρμογές καθώς είναι πολύ δαπανηρό υπολογιστικά να απαιτήσουμε να υποδιαιρέσεις μέχρι το θεωρητικό φράγμα διαχωρισμού, δείτε Σημ. 3.24.

3.6 Ο αλγόριθμος των συνεχών κλασμάτων

Εισαγωγή στα συνεχή κλάσματα

Παρουσιάζουμε μια γρήγορη επισκόπηση των συνεχών κλασμάτων η οποία αν και απέχει παρασάγκας από το να χαρακτηριστεί πλήρης ικανοποιεί τις ανάγκες μας. Η παρουσίασή μας ακολουθεί τον van der Poorten [256]. Για μια πιο λεπτομερή παρουσίαση ο αναγνώστης μπορεί να ανατρέξει για παράδειγμα στους Akritas [5], Bombieri and van der Poorten [31], Khintchine [155], van der Poorten [256], Yap [275].

Ένα *απλό συνεχές κλάσμα* (*simple or regular continued fraction*) είναι μια (πιθανά άπειρη) έκφραση της μορφής

$$c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \dots}} = [c_0, c_1, c_2, \dots]$$

όπου οι αριθμοί c_i ονομάζονται *μερικά πηλίκα* (*partial quotients*), $c_i \in \mathbb{Z}$ και $c_i \geq 1$ για $i > 0$. Παρατηρούμε ότι το c_0 μπορεί να είναι είτε θετικός είτε αρνητικός αριθμός, ωστόσο για τον αλγόριθμο που θα παρουσιάσουμε μπορούμε να υποθέσουμε ότι $c_0 \geq 0$. Θεωρώντας τις αναδρομικές σχέσεις

$$\begin{aligned} P_{-1} &= 1, \quad P_0 = c_0, \quad P_{n+1} = c_{n+1}\,P_n + P_{n-1} \\ Q_{-1} &= 0, \quad Q_0 = 1, \quad Q_{n+1} = c_{n+1}\,Q_n + Q_{n-1} \end{aligned}$$

μπορεί να δειχτεί με επαγωγή ότι $R_n = \frac{P_n}{Q_n} = [c_0, c_1, \dots, c_n]$, για $n = 0, 1, 2, \dots$ και επίσης ότι

$$\begin{aligned} P_n\,Q_{n+1} - P_{n+1}\,Q_n &= (-1)^{n+1} \\ P_n\,Q_{n+2} - P_{n+2}\,Q_n &= (-1)^{n+1} c_{n+2} \end{aligned}$$

Αν $\gamma = [c_0, c_1, \dots]$ τότε

$$\gamma = c_0 + \frac{1}{Q_0 Q_1} - \frac{1}{Q_1 Q_2} + \cdots = c_0 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{Q_{n-1} Q_n}$$

και καθώς η προηγούμενη σχέση είναι μια σειρά από αριθμούς που συνεχώς μειώνονται και έχουν εναλλασσόμενα πρόσημα, συμπεραίνουμε ότι συγκλίνει σε έναν πραγματικό αριθμό γ. Ένα πεπερασμένο τμήμα $R_n = \frac{P_n}{Q_n} = [c_0, c_1, \dots, c_n]$ ονομάζεται $n-$οστό *αναγώγημα* (*convergent* ή *approximant*) του γ και η ουρά $\gamma_{n+1} = [c_{n+1}, c_{n+2}, \dots]$ είναι γνωστή ως *ολικό πηλίκο* (*complete quotients*). Δηλαδή ισχύει $\gamma = [c_0, c_1, \dots, c_n, \gamma_{n+1}]$ για $n = 0, 1, 2, \dots$. Υπάρχει μία '1-1' αντιστοιχία μεταξύ των πραγματικών αριθμών και συνεχών κλασμάτων, όπου τα πεπερασμένα συνεχή κλάσματα αντιστοιχούν σε ρητούς αριθμούς.

Είναι γνωστό ότι $Q_n \geq F_{n+1}$ και ότι $F_{n+1} < \phi^n < F_{n+2}$, όπου F_n είναι ο $n-$οστός όρος Fibonacci και $\phi = \frac{1+\sqrt{5}}{2}$ ο *χρυσός λόγος* (*golden ratio*). Τα συνεχή κλάσματα είναι η καλύτερη (για δεδομένο μέτρο παρανομαστή) προσέγγιση, δηλαδή

$$\frac{1}{Q_n(Q_{n+1} + Q_n)} \leq \left| \gamma - \frac{P_n}{Q_n} \right| \leq \frac{1}{Q_n Q_{n+1}} \leq \frac{1}{Q_n^2} < \phi^{-2n}$$

Ισχύει επίσης και η λιγότερο ακριβής σχέση:

$$\left| \gamma - \frac{P_n}{Q_n} \right| < \frac{1}{c_{n+1} Q_n^2}$$

Έστω $\gamma = [c_0, c_1, \dots]$ η ανάπτυξη σε συνεχές κλάσμα ενός πραγματικού αριθμού. Η κατανομή Gauss-Kuzmin [31, 224] δηλώνει ότι για σχεδόν όλους τους πραγματικούς αριθμούς γ (το σύνολο των εξαιρέσεων έχει Lebesque μέτρο μηδέν) η πιθανότητα ένας θετικός ακέραιος δ να εμφανίζεται στην ανάπτυξη σε συνεχές κλάσμα του γ είναι

$$\mathbf{Prob}[c_i = \delta] = \lg \frac{(\delta+1)^2}{\delta(\delta+2)}, \quad i > 0 \tag{3.9}$$

Η κατανομή Gauss-Kuzmin δεν μας επιτρέπει να φράξουμε τη μέση τιμή των μερικών πηλίκων ή με άλλα λόγια η αναμενόμενη τιμή (μέσος όρος) των μερικών πηλίκων αποκλίνει, δηλαδή

$$\mathbf{E}[c_i] = \sum_{\delta=1}^{\infty} \delta \, \mathbf{Prob}[c_i = \delta] = \infty,$$

για κάθε $i > 0$. Παρ' όλα αυτά ο γεωμετρικός αλλά και ο αρμονικός μέσος όχι μόνο φράσσονται ασυμπτωτικά αλλά φράσσονται και από μία σταθερά. Για την περίπτωση του γεωμετρικού μέσου αυτή η σταθερά είναι η περίφημη σταθερά Khintchine [155], όπου

$$\lim_{n \to \infty} \sqrt[n]{\prod_{i=1}^{n} c_i} = \mathcal{K} = 2.685452001...$$

και για την οποία σταθερά δεν είναι γνωστό αν είναι άρρητος ή υπερβατικός αριθμός. Ο αναγνώστης μπορεί να ανατρέξει στην εργασία των Bailey et al. [12] όπου υπάρχει μια εμπεριστατωμένη

μελέτη των λεγόμενων *Khintchine's means*. Η αναμενόμενη τιμή του δυαδικού μήκους των μερικών πηλίκων είναι σταθερή για σχεδόν όλους τους αλγεβρικούς αριθμούς, όταν $n \to \infty$ ή n αρκετά μεγάλο [155, 224]. Ακολουθώντας προσεκτικά τους Richtmyer et al. [224], έχουμε:

$$\mathbf{E}[\ln c_i] = \frac{1}{n}\sum_{i=1}^{n} \ln c_i = \ln K = 0.98785...,$$

καθώς $n \to \infty$, $\forall i > 0$. Αν $\mathcal{L}(c_i) \triangleq b_i$, τότε

$$\mathbf{E}[b_i] = \mathcal{O}(1) \tag{3.10}$$

Ένας πραγματικός αριθμός έχει (τελικά) περιοδική ανάπτυξη σε συνεχές κλάσμα αν και μόνο αν είναι πραγματική ρίζα ενός πολυωνύμου δευτέρου βαθμού. Το σύνολο των πραγματικών αλγεβρικών αριθμών είναι Lebesque μέτρου 0 και ενδεχομένως τόσο η κατανομή Gauss–Kuzmin όσο και ο νόμος του Khintchine να μην ισχύει στο $\mathbb{R}_{alg}$. Όπως τονίζουν οι Brent, van der Poorten, and Riele [33]: "There is no reason to believe that the continued fraction expansions of non-quadratic algebraic irrationals generally do anything other than faithfully follow Khintchine's law"[2]. Επιπρόσθετα, ένα πλήθος πειραματικών αποτελεσμάτων [31, 224, 228] επιβεβαιώνει τον ισχυρισμό, ότι τόσο η κατανομή Gauss-Kuzmin όσο και ο νόμος του Khintchine είναι εν ισχύ στην ανάπτυξη σε συνεχές κλάσμα των πραγματικών αλγεβρικών αριθμών, βαθμού > 2. Αποτελεί τεράστια μαθηματική πρόκληση η θεωρητική κατάρριψη ή απόδειξη του ισχυρισμού. Σχετικά με το μεγαλύτερο αριθμό που μπορεί να εμφανιστεί στην ανάπτυξη σε συνεχές κλάσμα ενός ρητού αριθμού ο αναγνώστης μπορεί να ανατρέξει στην εργασία του Hensley [132].

Αξίζει να τονίσουμε ότι αν και στηριζόμαστε στην εικασία ότι τα μερικά πηλίκα των πραγματικών αλγεβρικών αριθμών είναι μη φραγμένου μέτρου, αυτή είναι η χειρότερη δυνατή περίπτωση. Αν αποδειχτεί ότι φράσσονται τότε αυτό μπορεί να οδηγήσει μόνο σε βελτίωση της πολυπλοκότητας του αλγορίθμου CF που εξετάζουμε.

Περιγραφή του αλγορίθμου CF

Ο αλγόριθμος CF εξαρτάται από το ακόλουθο θεώρημα, το οποίο παρουσιάστηκε από τον Vincent το 1836 [261]. Το αντίστροφο του Θεωρ. 3.43 εξασφαλίζει τον τερματισμό του CF και ο αναγνώστης μπορεί να ανατρέξει στους Akritas [5], Collins and Loos [55], Mignotte [187]. Ένα πολύ ενδιαφέρον ερώτημα είναι εάν τα θεωρήματα του ενός και των δύο κύκλων (Θεωρ. 3.32 και Θεωρ. 3.33) που χρησιμοποιούνται για την ανάλυση του τερματισμού των αλγορίθμων υποδιαίρεσης μπορούν να χρησιμοποιηθούν και ίσως να βελτιώσουν την πολυπλοκότητα του CF. Η απόδειξη του Θεωρ. 3.43 υπάρχει στις εργασίες των Akritas [5], Alesina and Galuzzi [6], Uspensky [255]. Για μια πιο σύγχρονη και κομψή εκδοχή του θεωρήματος του Vincent, ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στους Alesina and Galuzzi [6].

Θεώρημα 3.43

Έστω $A_{red} \in \mathbb{Z}[X]$, χωρίς τετράγωνα, τέτοιο ώστε $\deg(A_{red}) = d$ *και έστω* $\Delta > 0$ *το φράγμα*

[2] Ελεύθερη μετάφραση: Δεν συντρέχει κανένας λόγος που να μας κάνει να πιστεύουμε ότι οι μη τετραγωνικοί αλγεβρικοί αριθμοί δεν ακολουθούν πιστά τον νόμο του Khintchine.

Algorithm 13: CF (A, M, L)

Input: $A \in \mathbb{Z}[X]$, $M(X) = \frac{kX+l}{mX+n}$, $k, l, m, n \in \mathbb{Z}$
Output: A list of isolating intervals

if $A(0) = 0$ **then**
  $L \leftarrow \text{ADD}(L, [M(0), M(0)])$;
  $A \leftarrow A(X)/X$;
  CF(A, M, L);
$V \leftarrow \text{VAR}(A)$;
if $V = 0$ **then** RETURN ;
if $V = 1$ **then**
  $L \leftarrow \text{ADD}(L, [M(0), M(\infty)])$;
  RETURN ;
$b \leftarrow \text{PLB}(A)$ // PLB $\equiv$ POSITIVELOWERBOUND ;
if $b > 1$ **then** $A \leftarrow A(b + X), M \leftarrow M(b + X)$;
$A_1 \leftarrow A(1 + X)$, $M_1 \leftarrow M(1 + X)$;
CF(A_1, M_1, L) // Looking for real roots in $(1, +\infty)$;
$A_2 \leftarrow A(\frac{1}{1+X})$, $M_2 \leftarrow M(\frac{1}{1+X})$;
CF(A_2, M_2, L) // Looking for real roots in $(0, 1)$;
RETURN ;

διαχωρισμού του. Έστω n ο μεγαλύτερος δείκτης, τέτοιος ώστε

$$F_{n-1}\Delta > 2 \quad \textit{και} \quad F_{n-1}F_n\Delta > 1 + \frac{1}{\epsilon_d}$$

όπου F_n είναι ο n-οστός όρος της ακολουθίας Fibonnaci και $\epsilon_d = \left(1 + \frac{1}{d}\right)^{\frac{1}{d-1}} - 1$. Η απεικόνιση $X \mapsto [c_0, c_1, \ldots, c_n, X]$, όπου $c_0, c_1, \ldots, c_n$ είναι μια αυθαίρετη ακολουθία θετικών ακεραίων μετασχηματίζει το $A_{red}(X)$ στο $A_n(X)$, το οποίο δεν έχει παραπάνω από μία εναλλαγή προσήμων.

Σημείωση 3.44. *Καθώς ισχύει ότι $\frac{3}{4d^2} < \epsilon_d < \frac{4}{d^2}$ [55] συνάγουμε ότι $\frac{1}{\epsilon_d} + 1 < 2d^2$ για $d \geq 2$. Κατά συνέπεια, εάν $d \geq 2$ μπορούμε να αντικαταστήσουμε τις δύο συνθήκες του Θεωρ. 3.43 από την $F_{n-1}\Delta \geq 2d^2$, καθώς $F_n \geq F_{n-1} \geq 1$ και $F_{n-1}F_n\Delta \geq F_{n-1}\Delta \geq 2d^2 > 2$.*

Το Θεώρ. 3.43 μπορεί να χρησιμοποιηθεί προκειμένου να απομονώσουμε τις θετικές πραγματικές ρίζες ενός πολυωνύμου A_{red}, χωρίς τετράγωνα. Προκειμένου να απομονώσουμε τις αρνητικές πραγματικές ρίζες εφαρμόζουμε τον μετασχηματισμό $X \mapsto -X$ στο πολυώνυμο και επαναλαμβάνουμε τον αλγόριθμο. Συνεπώς σε ό,τι ακολουθεί θα υποθέσουμε ότι αναφερόμαστε μόνο στις θετικές πραγματικές ρίζες του A_{red}.

Η παραλλαγή του Vincent για τον αλγόριθμο CF είναι η ακόλουθη: Ένα πολυώνυμο A μετασχηματίζεται σε A_1 με την απεικόνιση $X \mapsto 1 + X$ και αν $\mathtt{VAR}(A_1) = 0$ ή $\mathtt{VAR}(A_1) = 1$ τότε το A έχει 0, αντίστοιχα 1, πραγματική ρίζα μεγαλύτερη από 1 (Θεώρ. 3.28 και Σημ. 3.29). Αν $\mathtt{VAR}(A_1) < \mathtt{VAR}(A)$ τότε (πιθανώς) υπάρχουν πραγματικές ρίζες του A στο $(0, 1)$, όπως προκύπτει από το Θεώρημα του Budan (Θεωρ. 3.31). Το A_2 παράγεται εφαρμόζοντας την απεικόνιση $X \mapsto 1/(1+X)$ στο A, αν $\mathtt{VAR}(A_2) = 0$ ή $\mathtt{VAR}(A_2) = 1$ τότε το A έχει 0, αντίστοιχα 1, πραγματική ρίζα μεγαλύτερη από 1 (Θεώρ. 3.28 και Σημ. 3.29).

Η παραλλαγή του Uspensky [255] για τον αλγόριθμο CF, δείτε επίσης [228], σε κάθε βήμα παράγει και τα δύο πολυώνυμα A_1 και A_2, πιθανώς όπως αναφέρει ο Akritas [1], επειδή δεν γνώριζε το Θεώρημα του Budan (Θεώρ. 3.31). Και στις δύο παραλλαγές, αν το μετασχηματισμένο πολυώνυμο έχει παραπάνω από μία ενναλλαγή προσήμων τότε επαναλαμβάνουμε τη διδαδικασία.

Ας θεωρήσουμε την όλη διαδικασία του CF αλγορίθμου ως ένα άπειρο δυαδικό δένδρο του οποίου η ρίζα αντιστοιχεί στο αρχικό πολυώνυμο A_{red}. Μια διακλάδωση από ένα κόμβο σε ένα δεξί παιδί αντιστοιχεί στον μετασχηματισμό $X \mapsto X + 1$, ενώ προς σε ένα αριστερό παιδί στον μετασχηματισμό $X \mapsto \frac{1}{1+X}$. Παρατηρούμε ότι μια ακολουθία από c μετασχηματισμούς $X \mapsto 1 + X$ ακολουθούμενη από έναν του τύπου $X \mapsto 1/(1 + X)$ είναι ισοδύναμη με δύο μετασχηματισμούς: έναν του τύπου $X \mapsto c + 1/X$ ακολουθούμενο από $X \mapsto 1 + X$. Κατά συνέπεια ο αλγόριθμος του Vincent (και του Uspensky) είναι μια ακολουθία από μετασχηματισμούς όπως αυτοί του Θεώρ. 3.43 και άρα το δένδρο είναι πεπερασμένο. Στα φύλλα, του δυαδικού δένδρου που έχουμε υποθέσει, αντιστοιχούν (μετασχηματισμένα) πολυώνυμα τα οποία έχουν το πολύ μία εναλλαγή προσήμων, αν το Θεώρ. 3.43 ισχύει. Ο Akritas [2], δείτε επίσης [5], αντικατέστησε μια σειρά από μετασχηματισμούς $X \mapsto X + 1$ με έναν μετασχηματισμό του τύπου $X \mapsto X + b$, όπου το b είναι ένα θετικό κάτω φράγμα (PLB) στις θετικές πραγματικές ρίζες του πολυωνύμου που εξετάζουμε. Το φράγμα αυτό υπολογίζεται με κάποιον από τους τύπους της Εν. 3.2. Με αυτό τον τρόπο, ο αριθμός των βημάτων του CF αλγόριθμου είναι πολυωνυμικός και η πολυπλοκότητά του είναι $\widetilde{\mathcal{O}}_B(d^5\tau^3)$. Ωστόσο, δεν είναι προφανές εάν και πώς η ανάλυση της πολυπλοκότητας λαμβάνει υπόψιν της ότι οι συντελεστές του πολυωνύμου μεγαλώνουν μετά από ένα μετασχηματισμό μετατόπισης. Ένα ακόμα σημαντικό ζήτημα είναι το μέτρο και το δυαδικό μήκος των c_i (μερικών πηλίκων) που εμφανίζονται κατά τη διάρκεια του αλγορίθμου και χρησιμοποιούνται ως παράμετροι μετατόπισης.

Για εκείνα τα πολυώνυμα που έχουν μόνο μία εναλλαγή προσήμου χρειάζεται να υπολογίσουμε το διάστημα όπου κείται η πραγματική ρίζα του αρχικού πολυωνύμου A_{red}. Ας θεωρήσουμε ένα πολυώνυμο A_n το οποίο αντιστοιχεί σε ένα φύλλο του δυαδικού δένδρου του αλγορίθμου και το οποίο έχει μία εναλλαγή προσήμου. Παρατηρούμε ότι το A_n έχει παραχθεί από μετασχηματισμούς σαν και αυτούς του Θεώρ. 3.43, με τη βοήθεια μιας ακολουθίας θετικών ακεραίων $c_0, c_1, \ldots, c_n$. Αυτοί οι μετασχηματισμοί μπορούν να γραφτούν σε πιο συμπαγή μορφή με τη χρήση αναγωγημάτων:

$$M : X \mapsto \frac{P_n X + P_{n-1}}{Q_n X + Q_{n-1}} \tag{3.11}$$

όπου $\frac{P_{n-1}}{Q_{n-1}}$ και $\frac{P_n}{Q_n}$ είναι συνεχόμενα αναγωγήματα του συνεχούς κλάσματος $[c_0, c_1, \ldots, c_n]$. Παρατηρούμε ότι η (3.11) είναι ένας μετασχηματισμός Möbius, για περισσότερες λεπτομέρειες δείτε [5, 275]. Εφόσον το A_n έχει μία εναλλαγή προσήμου. συνεπάγεται ότι έχει μία πραγματική ρίζα στο $(0, \infty)$, συνεπώς προκειμένου να υπολογίσουμε το διάστημα απομόνωσης που αντιστοιχεί στο

αρχικό πολυώνυμο A_{red} αποτιμούμε το δεξί μέλος της (3.11) στο 0 και στο ∞. Τα άκρα (πιθανώς μη διατεταγμένα) του διαστήματος απομόνωσης είναι $\frac{P_{n-1}}{Q_{n-1}}$ και $\frac{P_n}{Q_n}$.

Ο ψευδο-κώδικας του αλγορίθμου CF παρουσιάζεται στον Αλγ. 13.

Η αρχική είσοδος του αλγορίθμου είναι ένα πολυώνυμο $A_{red}(X)$ χωρίς τετράγωνα, ο τετριμμένος μετασχηματισμός $M(X) = X$ και μια κενή λίστα L όπου θα τοποθετηθούν τα διαστήματα απομόνωσης. Χρειαζόμαστε το συναρτησοειδές M προκειμένου να κρατάμε τους μετασχηματισμούς που λαμβάνουν χώρα κατά την εκτέλεση του αλγορίθμου και έτσι να παράγουμε τα διαστήματα απομόνωσης. Η συνάρτηση PLB(A) υπολογίζει ένα θετικό κάτω φράγμα στις θετικές πραγματικές ρίζες του A. Παρατηρούμε ότι οι Γραμμές 14 και 15 στον αλγόριθμο θα έπρεπε να εκτελούνται μόνο όταν $\texttt{VAR}(A_1) < \texttt{VAR}(A_2)$, σύμφωνα με το θεώρημα του Budan (Θεωρ. 3.31), αλλά προκειμένου να απλοποιήσουμε την παρουσίαση το παραλείπουμε, καθώς απλά διπλασιάζουν την πολυπλοκότητα.

Σημείωση 3.45. *Υπάρχουν δύο πολύ απλές αλλά πολύ σημαντικές παρατηρήσεις που αφορούν το Θεωρ. 3.43. Όταν το μετασχηματισμένο πολυώνυμο έχει μία εναλλαγή προσήμου, τότε το διάστημα με άκρα $\frac{P_{n-1}}{Q_{n-1}} = [c_0, c_1, \ldots, c_{n-1}]$ και $\frac{P_n}{Q_n} = [c_0, c_1, \ldots, c_n]$ (πιθανώς όχι σε διάταξη) απομονώνουν μια πραγματική ρίζα του A_{red}, έστω γ_i. Τότε, προκειμένου το Θεωρ. 3.43 να ισχύει μπορούμε να θεωρήσουμε αντί του ελάχιστου φράγματος διαχωρισμού Δ, την ποσότητα $|\gamma_i - \gamma_{c_i}|$, όπου γ_{c_i} είναι η (μιγαδική) ρίζα του A_{red} που βρίσκεται πιο κοντά στην ρίζα γ_i.*

Ομοίως, όταν το μετασχηματισμένο πολυώνυμο δεν έχει καμία εναλλαγή προσήμου και τα $\frac{P_{n-1}}{Q_{n-1}}$ και $\frac{P_n}{Q_n}$ απομονώνουν το θετικό πραγματικό μέρος μιας μιγαδικής ρίζας γ_i, τότε επίσης μπορούμε να αντικαταστήσουμε το Δ με $|\gamma_i - \gamma_{c_i}|$.

Θεώρημα 3.46

Ο αλγόριθμος CF *εκτελεί το πολύ $\mathcal{O}(d^2 + d\tau)$ βήματα.*

Απόδειξη: Έστω $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_k|$, $k \leq d$ οι (μιγαδικές) ρίζες του A_{red} με θετικό πραγματικό μέρος και έστω γ_{c_i} η ρίζα του A_{red} που είναι η πλησιέστερη στην γ_i.

Θεωρούμε το δυαδικό δένδρο T που παράγεται από την εκτέλεση του αλγορίθμου CF. Ο αριθμός των βημάτων του αλγορίθμου αντιστοιχεί στο πλήθος των κόμβων του T, και το οποίο πλήθος συμβολίζουμε με $\#(T)$. Θα χρησιμοποιήσουμε μερικά επιχειρήματα και το συμβολισμό από τους Eigenwillig et al. [81] προκειμένου να κλαδέψουμε το δένδρο.

Σε κάθε κόμβο v του T αντιστοιχούμε ένα μετασχηματισμό Möbius, $M_v : X \mapsto \frac{kX+l}{mX+n}$, ένα πολυώνυμο A_v και εμμέσως ένα διάστημα $\mathcal{I}_v$ με πιθανώς μη διατεγμένα άκρα, τα οποία και υπολογίζονται αν αποτιμήσουμε το M_v στο 0 και στο ∞.

Υπενθυμίζουμε ότι το A_v παράγεται εφαρμόζοντας τον μετασχηματισμό M_v στο A_{red}. Στη ρίζα του (δένδρου) T αντιστοιχούμε τα A_{red}, $M(X) = X$ (όπου $k = n = 1, l = m = 0$) και εμμέσως το διάστημα $(0, \infty)$.

Θεωρούμε ότι ένα φύλλο u του T είναι **type-i** αν το (αντίστοιχο) διάστημα $\mathcal{I}_u$ περιέχει $i \geq 0$ πραγματικές ρίζες. Εφόσον ο αλγόριθμος τερματίζει τα φύλλα του δένδρου είναι είτε type-0 είτε type-1. Θα κλαδέψουμε κάποια φύλλα του T προκειμένου να προκύψει ένα συγκεκριμένο

υποδένδρο, έστω T', όπου θα είναι εύκολο να μετρήσουμε τον αριθμό των κόμβων του. Καταρχάς απομακρύνουμε κάθε φύλλο του οποίου ο αδελφός κόμβος δεν είναι φύλλο. Στη συνέχεια θεωρούμε όλα τα φύλλα τα οποία έχουν αδελφούς κόμβους που είναι φύλλα. Εάν και τα δύο (αδελφά) φύλλα είναι type-1 τότε απομακρύνουμε τυχαία ένα από αυτά. Εάν το ένα από αυτά είναι τύπου type-1, τότε απομακρύνουμε το άλλο. Εάν είναι και τα δύο type-0, τότε αυτό σημαίνει ότι στον πατέρα τους αντιστοιχεί ένα πολυώνυμο με τουλάχιστον δύο εναλλαγές προσήμου και ότι προσπαθούμε να απομονώσουμε το θετικό πραγματικό μέρος μιας μιγαδικής ρίζας. Κρατάμε το φύλλο το οποίο περιέχει το θετικό πραγματικό μέρος της μιγαδικής ρίζας. Κατά συνέπεια $\#(T) < 2\,\#(T')$.

Στη συνέχεια θεωρούμε τα φύλλα του T'. Όλα είναι type-0 ή type-1. Και στις δύο περιπτώσεις στο αντίστοιχο διάστημα $\mathcal{I}_v$, περιέχεται το θετικό πραγματικό μέρος μιας ρίζας του A_{red} και ισχύει $|\mathcal{I}_v| \geq |\gamma_i - \gamma_{c_i}|$ (Σημ. 3.45). Επίσης, ο αριθμός των κόμβων από ένα φύλλο μέχρι τη ρίζα του δένδρου είναι n_i, ο οποίος είναι τέτοιος ώστε να ικανοποιείται η συνθήκη της Σημ. 3.44. Καθώς το n_i είναι ο μικρότερος δείκτης τέτοιος ώστε η συνθήκη της Σημ. 3.44 να ικανοποιείται, εάν μειώσουμε το n_i κατά ένα τότε η ανισότητα δεν ισχύει πλέον. Συνεπώς

$$F_{n_i-2}|\gamma_i - \gamma_{c_i}| \leq 2d^2 \Rightarrow \phi^{n_i-3}|\gamma_i - \gamma_{c_i}| < 2d^2 \Rightarrow n_i < 4 + 2\lg d - \lg|\gamma_i - \gamma_{c_i}|$$

Αθροίζουμε πάνω σε όλα τα n_i προκειμένου να φράξουμε το πλήθος των κόμβων του T', οπότε

$$\#(T') \leq \sum_{i=1}^{k} n_i \leq 2k(2 + \lg d) - \sum_{i=1}^{k} \log|\gamma_i - \gamma_{c_i}| \leq 2k(2 + \lg d) - \log\prod_{i=1}^{k}|\gamma_i - \gamma_{c_i}| \qquad (3.12)$$

Προκειμένου να εφαρμόσουμε το Θεωρ. 3.27 πρέπει να αναδιατάξουμε την ποσότητα $\prod_{\mathcal{I}\in\mathcal{J}}|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}|$ έτσι ώστε οι απαιτήσεις για τους δείκτες των ριζών να ικανοποιούνται. Οι προϋποθέσεις του θεωρήματος δεν ικανοποιούνται αν εμφανίζονται συμμετρικά γινόμενα. Θεωρούμε τη χειρότερη περίπτωση, να εμφανίζονται *μόνο* συμμετρικά γινόμενα, δηλαδή η ποσότητά μας είναι της μορφής $\prod|(\alpha_{\mathcal{I}} - \beta_{\mathcal{I}})(\beta_{\mathcal{I}} - \alpha_{\mathcal{I}})|$. Κατά συνέπεια θεωρούμε το τετράγωνο της ανισότητας του Θεωρ. 3.27 αντικαθιστώντας την ποσότητα $\frac{k}{2}$ με k και λαμβάνοντας υπ' όψιν ότι $\mathrm{disc}(A_{red}) \geq 1$, αφού το A_{red} είναι χωρίς τετράγωνα. Συνεπώς

$$\begin{aligned} \prod_{i=1}^{k}|\gamma_i - \gamma_{c_i}| \;&\geq\; \left(2^{\frac{k}{2} - \frac{d(d-1)}{2}}\,\mathcal{M}(A)^{1-d-\frac{k}{2}}\right)^2 \\ -\log\prod_{i=1}^{d}|\gamma_i - \gamma_{c_i}| \;&\leq\; d^2 - d - k + (2d + k - 2)\lg\mathcal{M}(A) \end{aligned} \qquad (3.13)$$

Η (3.12) γίνεται $\#(T') \leq 2k(2 + \lg d) + d^2 - d - k + (2d + k - 2)\lg\mathcal{M}(A)$. Ωστόσο, για το μέτρο Mahler είναι γνωστό ότι $\mathcal{M}(A) \leq 2^\tau\sqrt{d+1} \Rightarrow \lg\mathcal{M}(A) \leq \tau + \lg d$, για $d \geq 2$ (Λημ. 3.4), και έτσι $\#(T') \leq 2k(2 + \lg d) + d^2 - d - k + (2d + k - 2)(\tau + \lg d)$. Εφόσον $\#(T) < 2\,\#(T')$ και $k \leq d$, συμπεραίνουμε ότι $\#(T) = \mathcal{O}(d^2 + d\,\tau + d\lg d)$. ΟΕΔ

Η πολυπλοκότητα του CF

Προκειμένου να ολοκληρώσουμε την ανάλυση του CF αλγορίθμου πρέπει να υπολογίσουμε το κόστος κάθε βήματος. Στην χειρότερη περίπτωση κάθε βήμα απαιτεί τον υπολογισμό του θετικού κάτω φράγματος, b, στις θετικές πραγματικές ρίζες (Γραμμή 10) και τρεις μετασχηματισμούς, $X \mapsto b + X$, $X \mapsto 1 + X$ και $X \mapsto \frac{1}{1+X}$ (Γραμμές 11, 12 και 14 στον Αλγ. 13). Η αντιστροφή έχει πολυπλοκότητα $\mathcal{O}(d)$. Συνεπώς η πολυπλοκότητα του αλγορίθμου εξαρτάται από το κόστος των μετατοπίσεων (Γραμμή 11 στον Αλγ. 13) με την προϋπόθεση ότι απαιτείται ένας μικρός αριθμός από κλήσεις της PLB προκειμένου να υπολογιστεί ένα μερικό πηλίκο. Προς το παρόν δεχόμαστε αυτή την υπόθεση και θα την τεκμηριώσουμε στη συνέχεια.

Προκειμένου να υπολογίσουμε την συνολική πολυπλοκότητα πρέπει να φράξουμε το μέγεθος των $\mathcal{L}(c_k) \triangleq b_k, 0 \leq k \leq n_i$, δείτε επίσης την (3.10).

Αρχικά το A_{red} έχει βαθμό d και δυαδικό μήκος τ. Προφανώς ένας μετασχηματισμός μετατόπισης δεν αλλάζει το βαθμό του. Μια μετατόπιση με έναν ακέραιο, δυαδικού μήκος b_h, αυξάνει το δυαδικό μήκος του πολυωνύμου κατά ένα προσθετικό παράγοντα $d\, b_h$, στη χειρότερη περίπτωση (Εν. 2.2). Στο h βήμα του αλγορίθμου το πολυώνυμο έχει δυαδικό μήκος $\mathcal{O}(\tau + d\sum_{i=1}^{h} b_i)$ και εκτελούμε μια μετατόπιση με έναν ακέραιο μήκους b_{h+1}. Τα αποτελέσματα της Εν. 2.2 (Fast Taylor Shifts) μας υποδεικνύουν ότι αυτή η μετατόπιση μπορεί να γίνει με πολυπλοκότητα $\mathcal{O}_B\left(\mathsf{M}\left(d^2 \lg d + d^2 b_{h+1} + d(\tau + d\sum_{i=1}^{h} b_i)\right)\right)$ ή $\mathcal{O}_B\left(\mathsf{M}\left(d^2 \lg d + d\tau + d^2 \sum_{i=1}^{h+1} b_i\right)\right)$.

Απομένει να φράξουμε την ποσότητα $\sum_{i=1}^{h+1} b_i$. Γι' αυτό το σκοπό χρησιμοποιούμε την (3.10), η οποία φράσσει το $\mathbf{E}[b_i]$. Χρησιμοποιώντας την γραμμικότητα της αναμενόμενης τιμής προκύπτει ότι $\mathbf{E}[\sum_{i=1}^{h+1} b_i] = \mathcal{O}(h)$. Εφόσον $h \leq \#(T) = \mathcal{O}(d^2 + d\tau)$ (Θεωρ. 3.46), το αναμενόμενο κόστος, στη χειρότερη περίπτωση, στο βήμα h είναι $\mathcal{O}_B(\mathsf{M}\left(d^2 \lg d + d\tau + d^2(d^2 + d\tau)\right))$ ή $\widetilde{\mathcal{O}}_B(d^2(d^2 + d\tau))$.

Τέλος, πολλαπλασιάζοντας με τον αριθμό των βημάτων, $\#(T)$, συμπεραίνουμε ότι η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(d^6 + d^5\tau + d^4\tau^2)$, ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ εάν $d = \mathcal{O}(\tau)$, ή $\widetilde{\mathcal{O}}_B(N^6)$, όπου $N = \max\{d, \tau\}$.

Προκειμένου να απομονώσουμε τις αρνητικές πραγματικές ρίζες εφαρμόζουμε στο A_{red} τον μετασχηματισμό $X \mapsto -X$ και επαναλαμβάνουμε τον αλγόριθμο.

Όταν πρέπει να απομονώσουμε τις πραγματικές ρίζες ενός πολυωνύμου A, το οποίο δεν είναι ελεύθερο τετραγώνων και/ή θέλουμε να υπολογίσουμε τις πολλαπλότητες των πραγματικών ριζών τότε, όπως και στην περίπτωση των αλγορίθμων υποδιαίρεσης, μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο REALROOTSOLVER (Αλγ. 1) αντικαθιστώντας τη συνάρτηση REALROOTISOLATOR με τον αλγόριθμο CF.

Η προηγούμενη συζήτηση μας επιτρέπει να διατυπώσουμε το ακόλουθο θεώρημα:

Θεώρημα 3.47

Έστω $A \in \mathbb{Z}[X]$, όχι απαραίτητα χωρίς τετράγωνα, τέτοιο ώστε $\deg(A) = d > 2$ και $\mathcal{L}(A) = \tau$. Η αναμενόμενη πολυπλοκότητα του αλγορίθμου REALROOTSOLVER *για την απομόνωση και τον υπολογισμό των πολλαπλοτήτων των πραγματικών ριζών του A, χρησιμοποιώντας ως* REALROOTISOLATOR *του αλγόριθμο* CF*, είναι $\widetilde{\mathcal{O}}_B(d^6 + d^5\,\tau + d^4\,\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ αν $d = \mathcal{O}(\tau)$.*

Επιπρόσθετα το δυαδικό μήκος των ρητών αριθμών που είναι άκρα των διαστημάτων απομόνωσης φράσσεται από $\mathcal{O}(d\,\tau)$.

Σημείωση 3.48. *Η υπόθεση $d > 2$ δύναται να αντικατασταθεί από $d > 4$, καθώς μπορούμε να επιλύσουμε στους πραγματικούς πολυώνυμα βαθμού μέχρι 4 σε χρόνο $\mathcal{O}(1)$ ή $\widetilde{\mathcal{O}}_B(\tau)$ [92].*

Σημείωση 3.49. *Μπορούμε να δείξουμε ότι και η πολυπλοκότητα στη χειρότερη περίπτωση του* CF *είναι $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ διαφοροποιώντας ελάχιστα τον αλγόριθμο. Σε κάθε βήμα του αλγορίθμου διαμερίζουμε το A_1 σε δύο άλλα πολυώνυμα $A_{1,1}$ και $A_{1,2}$ χρησιμοποιώντας την συνάρτηση* $\text{SPLIT}_{\text{DESCARTES}}$*. Με αυτή την μικρή τροποποίηση ο* CF *είναι σχεδόν ο ίδιος με του αλγόριθμο* DESCARTES *και άρα έχει στην χειρότερη περίπτωση την ίδια πολυπλοκότητα.*

Εναλλακτικά μπορούμε επίσης να να χρησιμοποιήσουμε το γεγονός ότι στη χειρότερη περίπτωση πρέπει να κάνουμε κάποια μετατόπιση με έναν αριθμό δυαδικού μήκους το πολύ $\mathcal{O}(d\tau)$ όπως προκύπτει από το φράγμα διαχωρισμού και να συνάγουμε την πολυπλοκότητα στη χειρότερη περίπτωση.

Ρητοί αριθμοί και η υλοποίηση του PLB

Υπάρχουν δύο σημεία στον αλγόριθμο CF τα οποία χρήζουν μεγαλύτερης ανάλυσης και τα οποία η βιβλιογραφία έχει παραβλέψει.

Το πρώτο αφορά τους ρητούς αριθμούς. Αν το προς επίλυση πολυώνυμο A έχει κάποιους ρητούς αριθμούς για ρίζες τότε η ανάπτυξη σε συνεχή κλάσματα αυτών των ριζών δεν ακολουθεί ούτε την κατανομή Gauss-Kuzmin ούτε το νόμο του Khintchine. Ωστόσο, αν ένας ρητός αριθμός, $\frac{p}{q}$ είναι ρίζα του A τότε ο p διαιρεί τον a_0 και ο q διαιρεί τον a_d. Συνεπώς στη χειρότερη περίπτωση $\mathcal{L}(p/q) = \mathcal{O}(\tau)$ και άρα οι ρητοί αριθμοί απομονώνονται πολύ νωρίς στην εκτέλεση του αλγορίθμου. Το γεγονός ότι τους μεταχειριζόμαστε όπως τους αλγεβρικούς αριθμούς βαθμού μεγαλύτερου από δύο είναι μια υπερεκτίμηση.

Το δεύτερο σημείο αφορά τον αριθμό των κλήσεων της συνάρτησης PLB που απαιτούνται προκειμένου να υπολογιστεί ένα μερικό πηλίκο. Στην Εν. 3.6 κάναμε την παραδοχή ότι ο αριθμός αυτός είναι μικρός. Στην πράξη είναι σχεδόν πάντοτε έτσι εκτός από μία πολύ ειδική περίπτωση, όταν το πολυώνυμο έχει μόνο ρητούς αριθμούς για ρίζες οι οποίες είναι $\gg 1$. Η μη καλή συμπεριφορά του αλγορίθμου CF οφείλεται στο γεγονός ότι η συνάρτηση PLB πρέπει να κληθεί αρκετές φορές. Οι Richtmyer et al. [224] προκειμένου να αντιμετωπίσουν τέτοια προβλήματα πραγματοποιούν ένα μικρό αριθμό από επαναλήψεις Newton για να υπολογίσουν μια καλή προσέγγιση του μερικού πηλίκου. Οι Akritas [2], Akritas and Strzebonski [3], Akritas et al. [4] επιλύουν (πρακτικώς) το πρόβλημα εφαρμόζοντας την ομοθεσία $X \mapsto bX$, όπου b είναι το υπολογισμένο φράγμα, όταν $b \geq 16$.

Η παρατήρηση ότι ο αριθμός των κλήσεων της PLB είναι μικρός ενισχύεται από την (3.9), από την οποία προκύπτει ότι η πιθανότητα ένα μερικό πηλίκο να είναι μέτρου ≤ 10 είναι ~ 0.87. Γι' αυτό στην πράξη τα μερικά πηλίκα είναι πολύ μικρού δυαδικού μήκους. Επιπρόσθετα, η σχέση

$$\left|\gamma - \frac{P_n}{Q_n}\right| < \frac{1}{c_{n+1}\, Q_n^2}$$

μας λέει ότι η εμφάνιση ενός μερικού πηλίκου ασυνήθιστα μεγάλου μέτρου σημαίνει ότι η *προηγούμενη* προσέγγιση του αλγεβρικού αριθμού ήταν πάρα πολύ καλή.

Προκειμένου να θεμελιώσουμε θεωρητικά τη συμπεριφορά του CF θα χρησιμοποιήσουμε τα αποτελέσματα για την ποιότητα των φραγμάτων στις θετικές πραγματικές ρίζες που παρουσιάσαμε στην Εν. 3.2.

Το φράγμα που χρησιμοποιούμε για την υλοποίηση του PLB είναι το N_2, δείτε Εξ. (3.3). Αν b είναι το υπολογισθέν φράγμα και γ η κοντινότερη σε αυτό ρίζα, την οποία προσπαθούμε να απομονώσουμε, τότε από το Λημ. 3.17 ισχύει ότι $b \leq \gamma \leq d\,b$. Υπενθυμίζουμε ότι το κάτω φράγμα υπολογίζεται αρχικά ως άνω φράγμα στο αντίστροφο πολυώνυμο, το οποίο στη συνέχεια αντιστρέφεται, δείτε Σημ. 3.20.

Συνεπώς, κάποιος από τους ακεραίους στο διάστημα $[b, d\,b]$ αντιστοιχεί στο μερικό πηλίκο του γ που προσπαθούμε να υπολογίσουμε. Μπορούμε να χρησιμοποιήσουμε δυαδική αναζήτηση σε συνδυασμό με το θεώρημα του Budan (Θεωρ. 3.31) προκειμένου να βρούμε ένα διάστημα $[c, c+1] \subseteq [b, d\,b]$ στο οποίο περιέχεται το γ και όπου το $c \in \mathbb{Z}$ είναι μερικό πηλίκο που αναζητούμε. Το θεώρημα του Budan υλοποιείται με 2 μετατοπίσεις, οπότε η δυαδική αναζήτηση απαιτεί, για τον υπολογισμό του μερικού πηλίκου c, το πολύ $\mathcal{O}(\lg d + \lg b)$ μετατοπίσεις.

Όμως $b \leq c \Rightarrow \mathcal{L}(b) \leq \mathcal{L}(c) = \mathcal{O}(1)$, καθώς το c είναι μερικό πηλίκο στην ανάπτυξη του γ σε συνεχές κλάσμα, και άρα το δυαδικό του μήκος υπακούει το νόμο του Khintchine, Εξ. (3.10). Συνεπώς, σε κάθε βήμα του αλγορίθμου πρέπει να εκτελεστούν το πολύ $\mathcal{O}(\lg d)$ μετατοπίσεις, αντί για 2 που είχαμε υποθέσει. Δηλαδή, η πολυπλοκότητα του αλγορίθμου πρέπει να πολλαπλασιαστεί με ένα παράγοντα $\lg d$, ο οποίος δεν αλλάζει το φράγμα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

Στην πράξη η ποιότητα των φραγμάτων είναι πάρα πολύ καλή και ποτέ δεν κάνουμε δυαδική αναζήτηση προκειμένου να υπολογίσουμε το μερικό πηλίκο!

3.7 Σύνοψη – Μελλοντικές επεκτάσεις

Το παρόν κεφάλαιο επικεντρώνεται ρίζες των ακέραιων πολυωνύμων. Αρχικά παρουσιάσαμε απόλυτα, θετικά, σύνθετα φράγματα και φραγματα διαχωρισμού για τις πραγματικές και μιγαδικές ρίζες. Όσον αφορά τα θετικά φράγματα ενοποιήσαμε τα ήδη γνωστά φράγματα, προτείναμε κάποια καινούργια και αποδείξαμε κάποια αποτελέσματα για την ποιότητά τους.

Η ενασχόλησή μας με τα θετικά φράγματα και τα φράγματα διαχωρισμού συνεχίζεται. Θεωρούμε ότι είναι εξαιρετικά ενδιαφέρουσα μια συνολική θεωρία για τα θετικά φράγματα, όπως αυτή του van der Sluis [257] για τα απόλυτα φράγματα. Επίσης ενδιαφέρουσα είναι η απόδειξη κάποιου αποτελέσματος για την ποιότητα του φράγματος του Stefanescu (Θεωρ. 3.19).

Το σημείο αναφοράς του κεφαλαίου είναι απομόνωση των πραγματικών ριζών ενός ακέραιου πολυωνύμου, βαθμού d και δυαδικού μήκους τ, και ο υπολογισμός των πολλαπλοτήτων τους. Ενοποιήσαμε τους αλγορίθμους υποδιαίρεσης και βελτιώσαμε την πολυπλοκότητα του αλγορίθμου των συνεχών κλασμάτων κατά δύο παράγοντες, όπου επιπρόσθετα οριστικοποιήσαμε την θεωρητική του θεμελίωση. Η πολυπλοκότητα όλων των αλγορίθμων είναι $\widetilde{\mathcal{O}}_B(d^4\,\tau^2)$. Αποδείξαμε ότι το φράγμα της πολυπλοκότητας ισχύει και για πολυώνυμα με τετράγωνα και ότι στην ίδια πολυπλοκότητα μπορούμε να υπολογίσουμε τις πολλαπλότητες ριζών.

Υπενθυμίζουμε στον αναγνώστη ότι η πολυπλοκότητα των αριθμητικών (προσεγγιστικών) αλγορίθμων [213, 214, 239] είναι $\widetilde{\mathcal{O}}_B(d^3\,\tau)$ ή $\widetilde{\mathcal{O}}_B(N^4)$, όπου $N = \max\{d, \tau\}$. Ένα από τα μεγαλύτερα ανοιχτά ερωτήματα είναι αν οι ακριβείς αλγόριθμοι μπορούν να επιτύχουν αυτό το φράγμα πολυπλοκότητας. Επίσης, ποιό είναι το κάτω φράγμα των αλγορίθμων απομόνωσης; Παρατηρούμε ότι η έξοδος των αλγορίθμων είναι $\mathcal{O}(d)$ διαστήματα απομόνωσης με άκρα δυαδικού μήκους $\mathcal{O}_B(d\,\tau)$, οπότε ένα κάτω φράγμα είναι το $\mathcal{O}_B(d^2\tau)$. Είναι το φράγμα βέλτιστο; Από την άλλη αν μας δοθεί ένα πολυώνυμο και $\mathcal{O}(d)$ διαστήματα απομόνωσης των πραγματικών ριζών του, με άκρα δυαδικού μήκους $\mathcal{O}_B(d\,\tau)$, μπορούμε να υπολογίσουμε τις πολλαπλότητες των ριζών με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\,\tau)$, η οποία είναι βέλτιστη. Μήπως αυτό είναι το βέλτιστο κάτω φράγμα;

Όσον αφορά τους αλγορίθμους υποδιαίρεσης δεν υπάρχει ελπίδα για πολυπλοκότητα $\widetilde{\mathcal{O}}_B(N^4)$, καθώς τόσο ο αριθμός των βημάτων που εκτελούν όσο και το κόστος του κάθε βήματος είναι βέλτιστο. Το αμέσως επόμενο βήμα θα πρέπει να είναι η ένταξη στους αλγορίθμους υποδιαίρεσης του αλγορίθμου αποκλεισμού (exclusion algorithm) των Dedieu and Yakoubsohn [68] και η βελτίωση της πολυπλοκότητάς του. Για τον αλγόριθμο των συνεχών κλασμάτων πιστεύουμε ότι, με κάποιες μικρές τροποποιήσεις, μπορούμε να επιτύχουμε (αναμενόμενη) πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\tau)$. Αν αλλάξουμε την αναπαράσταση των πραγματικών ριζών και αντί για διαστήματα απομόνωσης υιοθετήσουμε την κωδικοποίηση Thom [58], τότε χρησιμοποιώντας τον αλγόριθμο του Canny [44] μπορούμε να προτείνουμε έναν αλγόριθμο με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(N^5)$.

Τέλος, οι ακριβείς αλγόριθμοι στην πράξη είναι πολύ γρήγοροι και σπάνια επιτυγχάνουν το φράγμα πολυπλοκότητας της χειρότερης περίπτωσης. Ποιά είναι η αναμενόμενη πολυπλοκότητα των αλγορίθμων;

Στα παραπάνω προβλήματα ευελπιστούμε ότι θα μπορέσουμε να παρουσιάσουμε αποτελέσματα στο άμεσο μέλλον.

ΚΕΦΑΛΑΙΟ 4

Υπολογισμοί με πραγματικούς αλγεβρικούς αριθμούς

Ο Θεός έφτιαξε τους ακέραιους,
όλοι οι υπόλοιποι αριθμοί είναι
δημιουργήματα του ανθρώπου.

Leopold Kronecker

Περίληψη

Το παρόν κεφάλαιο ασχολείται με αλγορίθμους που αφορούν υπολογισμούς με ένα και δύο πραγματικούς αλγεβρικούς αριθμούς. Πιο συγκεκριμένα παρουσιάζονται αλγόριθμοι για την αναπαράσταση πραγματικών αλγεβρικών αριθμών, για τον υπολογισμό του προσήμου της αποτίμησης ενός πολυωνύμου πάνω σε έναν και δύο αλγεβρικούς αριθμούς και για το πρόβλημα των ταυτόχρονων ανισώσεων. Τέλος, παρουσιάζουμε δύο αλγορίθμους για την πραγματική επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές. Όλοι αλγόριθμοι βασίζονται στις προσημασμένες ακολουθίες πολυωνυμικών υπολοίπων.

Όσον αφορά στους υπολογισμούς με έναν αλγεβρικό αριθμό, αν και οι περισσότεροι αλγόριθμοι είναι γνωστοί, η πολυπλοκότητά τους δεν έχει μελετηθεί. Παρουσιάζουμε σε ενιαίο πλαίσιο τους αλγορίθμους για υπολογισμούς με έναν αλγεβρικό αριθμό και την πολυπλκοκότητά τους. Σε κάθε περίπτωση βελτιώνουμε τα φράγματα πολυπλοκότητας κατά δύο ή τρεις παράγοντες. Στη συνέχεια παρουσιάζουμε τις πολυπλοκότητες για τον υπολογισμό πολυωνυμικών ακολουθιών υπολοίπων, πολυωνύμων σε δύο μεταβλητές, δύο αλγόριθμους για την πραγματική επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές και αλγορίθμους για υπολογισμούς με δύο αλγεβρικούς αριθμούς. Τα προκύπτοντα φράγματα πολυπλοκότητας βελτιώνουν σε κάθε περίπτωση τα ήδη γνωστά. Μέρος των αποτελεσμάτων έχει παρουσιαστεί στις εργασίες [87, 91, 97].

Το σύνολο των πραγματικών αλγεβρικών αριθμών, το οποίο είναι σώμα, το συμβολίζουμε με $\mathbb{R}_{alg}$. Προκειμένου να περιγράψουμε και να αναλύσουμε αλγορίθμους που αφορούν υπολογισμούς με αλγεβρικούς αριθμούς πρέπει να επιλέξουμε μια αναπαράστασή τους. Επιλέγουμε την αναπαράσταση διαστήματος απομόνωσης (isolating interval representation).

Ορισμός 4.1. *Η αναπαράσταση με διάστημα απομόνωσης ενός πραγματικού αλγεβρικού αριθμού,* $\gamma \in \mathbb{R}_{alg}$*, συμβολίζεται με* $\gamma \cong (A(X), \mathcal{I})$*, όπου* $A \in \mathbb{Z}[X]$ *είναι χωρίς τετράγωνα,* $A(\gamma) = 0$*,* $\gamma \in \mathcal{I}$*,* $\mathcal{I} = [a, b]$*,* $a, b, \in \mathbb{Q}$ *και το* A *δεν έχει άλλη πραγματική ρίζα στο* $\mathcal{I}$*.*

Η αναπαράσταση με διάστημα απομόνωσης δεν είναι μοναδική. Καταρχάς δεν απαιτούμε το A να είναι το ελάχιστο πολυώνυμο του γ. Αν και υπάρχουν αλγόριθμοι που υπολογίζουν το ελάχιστο πολυώνυμο, θέλουμε να τους αποφύγουμε λόγω της μεγάλης θεωρητικής και πρακτικής πολυπλοκότητάς τους. Ακόμη και στην περίπτωση που το ελάχιστο πολυώνυμο είναι γνωστό, το διάστημα απομόνωσης δεν μπορεί να οριστεί μοναδικά.

Παράδειγμα 4.2. *Αν* $\gamma = \sqrt{2}$ *τότε οι αναπαραστάσεις* $\gamma \cong (X^2 - 2, [0, 3])$*,* $\gamma \cong (X^2 - 2, [1, 2])$ *και* $\gamma \cong ((X^2 - 2)(X - 10), [0, 9])$ *είναι ισοδύναμες αναπαραστάσεις του* γ*.*

Εκτός από την αναπαράσταση με διάστημα απομόνωσης, υπάρχουν και άλλες αναπαραστάσεις για τους πραγματικούς αλγεβρικούς αριθμούς. Ο αναγνώστης μπορεί να ανατρέξει για παράδειγμα, στους Cohen [51], Mishra [193], Yap [275] για περισσότερες λεπτομέρειες. Αξίζει ωστόσο να αναφέρουμε την αναπαράσταση με κωδικοποίηση κατά Thom την οποία εισήγαγαν οι Coste and Roy [58], όπου οι πραγματικές ρίζες ενός ακέραιου πολυωνύμου χαρακτηρίζονται (μοναδικά) από το πρόσημο όλων των παραγώγων του πολυωνύμου πάνω σε αυτές. Η προσέγγιση αυτή είναι καθαρά συμβολική, δεν εξαρτάται από τα φράγματα διαχωρισμού και είναι νόμιμη όχι μόνο για ακέραια πολυώνυμα αλλά και για πολυώνυμα σε σε οποιοδήποτε κλειστό αλγεβρικό σώμα. Για την πολυπλοκότητα των υπολογισμών αυτών ο αναγνώστης μπορεί να ανατρέξει στους Coste and Roy [58], Roy and Szpirglas [231] αλλά και στους Cucker et al. [63], Mishra and Pedersen [194], όπου παρουσιάζονται αποτελέσματα πολυπλοκότητας στην κλάση NC. Δεν θα ασχοληθούμε με αυτή την προσέγγιση.

Το υπόλοιπο του κεφαλαίου χωρίζεται σε δύο ενότητες. Η πρώτη αφορά υπολογισμούς με έναν πραγματικό αλγεβρικό αριθμό και η δεύτερη με δύο.

4.1 Υπολογισμοί με έναν αλγεβρικό αριθμό

Σε ό,τι θα ακολουθήσει θα παρουσιάσουμε έναν αλγόριθμο που κατασκευάζει πραγματικούς αλγεβρικούς αριθμούς. Επίσης, αλγορίθμους που συγκρίνουν πραγματικούς αλγεβρικούς αριθμούς, που υπολογίζουν το πρόσημο ενός πολυωνύμου αν αποτιμηθεί πάνω σε έναν πραγματικό αλγεβρικό αριθμό, έναν αλγόριθμο για τον υπολογισμό ενδιάμεσων σημείων σε μία διατεταγμένη λίστα από πραγματικούς αλγεβρικούς αριθμούς και τέλος έναν αλγόριθμο για το πρόβλημα των ταυτόχρονων ανισώσεων.

Ο Canny [46] αλλά και ο Rump [232] προτείνουν, αφενός μεν οι πραγματικοί αλγεβρικοί αριθμοί να αναπαρίστανται με διάστημα απομόνωσης, αφετέρου δε οι υπολογισμοί με αυτούς να γίνονται με συνεχείς εκλεπτύνσεις των διαστημάτων απομόνωσης, βασιζόμενοι στις ιδιότητες της αριθμητικής διαστημάτων και στα φράγματα διαχωρισμού πολυωνυμικών συστημάτων [46, 275]. Με άλλα λόγια οι υπολογισμοί πραγματοποιούνται με προσεγγίσεις των πραγματικών αλγεβρικών αριθμών οι οποίες βελτιώνονται αν δεν είναι ικανοποιητικές. Για παράδειγμα, προκειμένου

να υπολογιστεί το πρόσημο μιας (πολυωνυμικής) έκφρασης που περιέχει πραγματικούς αλγεβρικούς αριθμούς, αντικαθιστούμε τους πραγματικούς αλγεβρικούς αριθμούς με τα διαστήματα απομόνωσής τους και εκτελούμε τις πράξεις χρησιμοποιώντας αριθμητική διαστημάτων. Αν το αποτέλεσμα, το οποίο είναι ένα διάστημα, δεν περιέχει το 0, τότε μπορούμε να αποφασίσουμε το πρόσημό του. Αν περιέχει το 0 τότε εκλεπτύνουμε τα διαστήματα απομόνωσης, χρησιμοποιώντας τα πολυώνυμα που ορίζουν τους αλγεβρικούς αριθμούς, μέχρι το διάστημα του αποτελέσματος να μην περιέχει το 0 ή μέχρι να ξεπεράσουμε το φράγμα διαχωρισμού της έκφρασης, οπότε και το αποτέλεσμα είναι 0. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι μπορεί να υλοποιηθεί, σχετικά εύκολα, με αριθμούς κινητής υποδιαστολής, είτε στην ακρίβεια της μηχανής είτε απεριόριστης ακρίβειας και επίσης όταν η έκφρασή δεν είναι μηδέν τότε είναι πάρα πολύ αποτελεσματική. Από την άλλη μεριά αν το αποτέλεσμα της έκφρασης είναι 0 ή πολύ κοντά στο 0, τότε προκειμένου να αποφασίσουμε το πρόσημο της έκφρασης πρέπει το διάστημα του αποτελέσματος να είναι μικρότερο από το φράγμα διαχωρισμού. Τα φράγματα διαχωρισμού αντικατοπτρίζουν τη χειρότερη δυνατή περίπτωση και όπως έχουμε αναφέρει και στην περίπτωση της μιας μεταβλητής είναι στη γενική περίπτωση πολύ κακής ποιότητας, δείτε Εν. 3.2. Στο ίδιο πλαίσιο κινείται η προσέγγιση του Johnson [140], οι αλγόριθμοι που παρουσιάζουν οι Basu et al. [14] και η ακόμα πιο γενική προσέγγιση των Burnikel et al. [40, 42], Li and Yap [172], Pion and Yap [216] οι οποίοι παρουσιάζουν το γενικό θεωρητικό υπόβαθρο αυτής της πρόσεγγισης και για τις τέσσερις βασικές πράξεις. Δείτε επίσης τις εργασίες των Li et al. [173], Yap [274].

Οι αλγόριθμοι που παρουσιάζουμε χρησιμοποιούν την αναπαράσταση με διάστημα απομόνωσης αλλά επιπρόσθετα βασίζονται στις προσημασμένες πολυωνυμικές ακολουθίες υπολοίπων προκειμένου να αποφύγουμε την εκλέπτυση των διαστημάτων.

Μια τέτοια προσέγγιση προτείνουν οι Schwartz and Sharir [241] και επίσης χρησιμοποιεί ο Rioboo [225, 226, 227]. Μάλιστα η υλοποίηση του Rioboo [225, 226] στο μαθηματικό λογισμικό AXIOM είναι η μοναδική μέχρι σήμερα, που επιτρέπει όλες τις πράξεις μεταξύ πραγματικών αλγεβρικών αριθμών, χωρίς να χρησιμοποιεί προσεγγίσεις τους. Αλγόριθμοι που αφορούν όλες τις βασικές πράξεις παρουσιάζονται από τον Loos [177], δείτε επίσης [193, 218, 275]. Η αλγοριθμική προσέγγιση που ομοιάζει περισσότερο στη δική μας είναι αυτή του Sakkalis [234]. Όσον αφορά τους υπολογισμούς με έναν πραγματικό αλγεβρικό αριθμό, οι περισσότεροι από τους αλγορίθμους που παρουσιάζουμε δεν είναι κανούργιοι. Ωστόσο, περιέργως πως, η πολυπλοκότητά τους δεν παρουσιάζεται στην βιβλιογραφία. Σε κάθε περίπτωση βελτιώνουμε την πολυπλοκότητα κατά 2 ή 3 παράγοντες.

Αν και γενικώς πιστεύεται ότι η πρώτη προσέγγιση είναι η καλύτερη στην πράξη, αυτό δεν είναι πάντοτε αληθές. Μια προσεκτική υλοποίηση των αλγορίθμων που παρουσιάζουμε μπορεί να οδηγήσει σε λογισμικό που μπορεί να επιλύσει πολύ γρήγορα πολλά από τα προβλήματα που παρουσιάζονται στις εφαρμογές. Επιπρόσθετα, το μεγάλο πλεονέκτημα της προσέγγισής μας είναι η θεωρήτική της πληρότητα, η οποία μας επιτρέπει να μελετήσουμε θεωρητικά τους αλγορίθμους υπολογισμού και να συνάγουμε φράγματα πολυπλοκότητας τα οποία είναι πολύ καλύτερα από οποιαδήποτε άλλη προσέγγιση. Ίσως το πιο σημαντικό πλεονέκτημα της προσέγγισή μας είναι το γεγονός ότι αν ο βαθμός των πραγματικών αλγεβρικών αριθμών είναι σταθερός, τότε η αριθμητική πολυπλοκότητα όλων των αλγορίθμων που παρουσιάζουμε, με την εξαίρεση του αλγορίθμου κατασκευής, είναι $\mathcal{O}(1)$, καθώς δεν εξαρτώμαστε από το φράγμα διαχωρισμού.

Κατασκευή

Δοθέντος ενός πολυωνύμου $A \in \mathbb{Z}[X]$,τέτοιου ώστε $\deg(A) = d$ και $\mathcal{L}(A) = \tau$, ο αλγόριθμος που υπολογίζει τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του A παρουσιάζεται στον Αλγ. 14. Για να απομονώσουμε τις ρίζες χρησιμοποιούμε τον αλγόριθμο readRootSolver (Αλγ. 1) με κάποιον από τους αλγορίθμους sturm, descartes, bernstein ή cf. Το κόστος επίλυσης είναι $\widetilde{\mathcal{O}}_B(d^6 + d^4\tau^2)$. Το πολυώνυμο που ορίζει τους αλγεβρικούς αριθμούς είναι το χωρίς τετράγωνα μέρος του A, το οποίο έχει δυαδικό μήκος $\mathcal{O}(d+\tau)$. Το δυαδικό μήκος των άκρων των διαστημάτων απομόνωσης είναι $\mathcal{O}(d\tau)$. Παρατηρούμε ότι πρέπει να ταξινομήσουμε τα διαστήματα απομόνωσης πριν κατασκευάσουμε τους αλγεβρικούς αριθμούς. Το κόστος της ταξινόμησης είναι $\mathcal{O}(d^2 \lg d)$ ή $\widetilde{\mathcal{O}}_B(d^3\,\tau)$, χρησιμοποιώντας για παράδειγμα τον αλγόριθμο quick-sort [57].

Η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(d^6 + d^4\tau^2)$.

Algorithm 14: construct (A)

Input: $A \in \mathbb{Z}[X]$
Output: Μια λίστα με τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του A και τις πολλαπλότητές τους.

```
1 R ← ∅
2 L, M ← realRootSolver(A)
3 sort([L, M])
4 foreach 𝓘 ∈ L do
5 |  R ← (A_red, 𝓘)
6 return R, M
```

Σημείωση 4.3. *Αν $\gamma \equiv (A, \mathcal{I} = [\mathsf{a}, \mathsf{b}])$, το $\mathcal{I}$ περιέχει μόνο μία πραγματική ρίζα του A και συνεπώς το A αλλάζει πρόσημο στα άκρα του $\mathcal{I}$, εκτός από την περίπτωση που $\mathsf{a} = \mathsf{b}$ οπότε και ισχύει $A(\mathsf{a}) = A(\mathsf{b}) = 0$. Μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι $0 \notin (\mathsf{a}, \mathsf{b})$, εκτός αν $\gamma = \mathsf{a} = \mathsf{b} = 0$.*

Παρατηρούμε επίσης ότι το πρόσημο του γ μπορεί να εξαχθεί εύκολα από το πρόσημο των a *και* b.

Στη συνέχεια θα παρουσιάσουμε αλγορίθμους (και την πολυπλοκότητά τους) για μερικές πολύ βασικές πράξεις με πραγματικούς αλγεβρικούς αριθμούς. Οι αλγεβρικοί αριθμοί θα έχουν την αναπαράσταση $\gamma \cong (A, \mathcal{I}) = [\mathsf{a}, \mathsf{b}]$, όπου το A είναι χωρίς τετράγωνα και $\deg(A) = d$, $\mathcal{L}(A) = \tau$ και $\mathcal{L}(\mathsf{a}) = \mathcal{L}(\mathsf{b}) = \mathcal{O}(d\tau)$, εκτός αν ρητά αναφέρεται το αντίθετο.

Υπολογισμός προσήμου

Ο αλγόριθμος υπολογισμού προσήμου, sign_at(f, γ) (Αλγ. 15), υπολογίζει το πρόσημο της αποτίμησης ενός πολυωνύμου f πάνω στον πραγματικό αλγεβρικό αριθμό γ. Θεωρούμε ότι $\deg(f) \leq d$ και $\mathcal{L}(f) = \sigma$.

Για να υπολογίσουμε το πρόσημο χρησιμοποιούμε το Θεωρ. 2.26 και έτσι έχουμε

$$\mathtt{VAR}(\mathbf{SR}(A, f\ ;\ [\mathsf{a}, \mathsf{b}])) = \mathrm{sign}\left(f(\gamma) \cdot A'(\gamma)\right)$$

Όμως $\mathrm{sign}(A'(\gamma)) = \mathrm{sign}(A(\mathsf{b}) - A(\mathsf{a}))$, οπότε συμπεραίνουμε ότι

$$\mathrm{sign}(f(\gamma)) = \mathtt{VAR}(\mathbf{SR}(A, f\ ;\ [\mathsf{a}, \mathsf{b}])) \cdot \mathrm{sign}(A(\mathsf{b}) - A(\mathsf{a}))$$

Το κόστος του υπολογισμού $\mathtt{VAR}(\mathbf{SR}(A, f\ ;\ [\mathsf{a}, \mathsf{b}]))$ είναι δύο φορές το κόστος υπολογισμού του $\mathbf{SR}(A, f\ ;\ \mathsf{a})$, το οποίο είναι $\widetilde{\mathcal{O}}_B(d^2 \max\{\sigma, d\tau\})$ (Θεωρ. 2.32). Το κόστος των αποτιμήσεων $A(\mathsf{a})$ και $A(\mathsf{b})$ είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$ (2.2), αν και μπορεί να θεωρηθεί ότι το πρόσημό τους είναι ήδη γνωστό.

Algorithm 15: SIGN_AT (f, γ)

Input: $f \in \mathbb{Z}[X], \gamma \cong (A, \mathcal{I} = [\mathsf{a}, \mathsf{b}])$
Output: $\mathrm{sign}(f(\gamma))$

1 RETURN $\mathrm{sign}\left(\mathtt{VAR}(\mathbf{SR}(A, f\ ;\ [\mathsf{a}, \mathsf{b}])) \cdot \mathrm{sign}(A'(\gamma))\right)$

Πόρισμα 4.4. *Έστω $f(X) \in \mathbb{Z}[X]$, όπου $\deg(f) \leq d$ και $\mathcal{L}(f) = \sigma$, και έστω ένας πραγματικός αλγεβρικός αριθμός $\gamma \cong (A, [\mathsf{a}, \mathsf{b}])$, όπου $\deg(A) = d$, $\mathcal{L}(A) = \tau$ και $\mathcal{L}(\mathsf{a}) = \mathcal{L}(\mathsf{b}) = \mathcal{O}(d\tau)$. Η πολυπλοκότητα του* SIGN_AT(f, γ) *είναι $\widetilde{\mathcal{O}}_B(d^2 \max\{\sigma, d\tau\})$.*

Η υπόθεση $\deg(f) \leq d$ είναι χωρίς βλάβη της γενικότητας καθώς αν $\deg(f) > d$, τότε μπορούμε να υπολογίσουμε το SIGN_AT$(A, \mathrm{prem}(f, A))$ καθώς

$$\left|\mathrm{lead}(A)^{\deg(f)-\deg(A)+1}\right| f = A \cdot \mathrm{pquo}(f, A) + \mathrm{prem}(f, A) \Rightarrow f(\gamma) = \mathrm{prem}(f, A)(\gamma)$$

Σύγκριση

Ο αλγόριθμος σύγκρισης, COMPARE(γ_1, γ_2), δύο πραγματικών αλγεβρικών αριθμών $\gamma_1 \cong (A_1, \mathcal{I}_1 = [\mathsf{a}_1, \mathsf{b}_1])$ και $\gamma_2 \cong (A_2, \mathcal{I}_2 = [\mathsf{a}_2, \mathsf{b}_2])$ παρουσιάζεται στον Αλγ. 16. Αν τα διαστήματα $\mathcal{I}_1$ και $\mathcal{I}_2$ είναι ξένα μεταξύ τους ή αν μόνο ένας από τους γ_1 και γ_2 ανήκει στο $\mathcal{I}_1 \cap \mathcal{I}_2$ τότε μπορούμε εύκολα να τους συγκρίνουμε. Αν και οι δύο ανήκουν στο $\mathcal{J} = \mathcal{I}_1 \cup \mathcal{I}_2$ τότε

$$\gamma_1 \geq \gamma_2 \Leftrightarrow A_2(\gamma_1) \cdot A_2'(\gamma_2) \geq 0$$

Το πρόσημο της αποτίμησης $A_2(\gamma_1)$ μπορούμε να το υπολογίσουμε με τον αλγόριθμο SIGN_AT(A_2, γ_1) και το κόστος της, το οποίο είναι και το κόστος του αλγορίθμου COMPARE, είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$.

Πόρισμα 4.5. *Έστω πραγματικοί αλγεβρικοί αριθμοί $\gamma_1 \cong (A_1, \mathcal{I}_1 = [\mathsf{a}_1, \mathsf{b}_1])$ και $\gamma_2 \cong (A_2, \mathcal{I}_2 = [\mathsf{a}_2, \mathsf{b}_2])$ όπου $\deg(A_{1,2}) = d$, $\mathcal{L}(A_{1,2}) = \tau$ και $\mathcal{L}(\mathsf{a}_{1,2}) = \mathcal{L}(\mathsf{b}_{1,2}) = \mathcal{O}(d\tau)$. Η σύγκρισή τους με τον αλγόριθμο* COMPARE *έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\tau)$.*

Algorithm 16: COMPARE (γ_1, γ_2)

Input: $\gamma_1 \cong (A_1, \mathcal{I}_2 = [\mathsf{a}_1, \mathsf{b}_1]), \gamma_2 \cong (A_2, \mathcal{I}_2 = [\mathsf{a}_2, \mathsf{b}_2])$
Output: Σύγκριση των γ_1 και γ_2

```
1  J ← I1 ∩ I2 = [c, d]
2  if J = ∅ then
3  |   if I1 < I2 then RETURN −1
4  |   else RETURN 1
5  if γ1 ∉ J then
6  |   if I1 < J then RETURN −1
7  |   else RETURN 1
8  if γ2 ∉ J then
9  |   if I2 < J then RETURN 1
10 |   else RETURN −1
11 RETURN SIGN_AT(A2, γ1) · sign(A2'(γ2))
```

Ενδιάμεσα σημεία

Σε πολλές περιπτώσεις, δοθέντων πραγματικών αλγεβρικών αριθμών (σε διάταξη) που είναι ρίζες ενός πολυωνύμου A χρειάζεται να υπολογίσουμε ρητά σημεία ανάμεσα στους αριθμούς. Αυτό μπορεί να γίνει διατρέχοντας τη λίστα L που επιστρέφει ο αλγόριθμος CONSTRUCT(A) και για κάθε ζεύγος διαστημάτων να θεωρήσουμε το μέσο του πάνω άκρου του πρώτου διαστήματος και του κάτω άκρου του δεύτερου διαστήματος. Το πρώτο (τελευταίο), ενδιάμεσο σημείο το υπολογίζουμε αφαιρώντας (προσθέτοντας) 1 στο κάτω (άνω) άκρο του πρώτου (τελευταίου) διαστήματος απομόνωσης. Τον αλγόριθμο αυτό θα τον συμβολίσουμε με INTERMEDIATE_POINTS και η πολυπλοκότητα του είναι $\widetilde{\mathcal{O}}_B(d^2\,\tau)$ ή $\widetilde{\mathcal{O}}_B(R\,d\,\tau)$, όπου R είναι το πλήθος των πραγματικών ριζών του A.

Το πρόβλημα των ταυτόχρονων ανισώσεων

Έστω $f, A_1, \ldots, A_{n_1}, B_1, \ldots, B_{n_2}, C_1, \ldots, C_{n_3} \in \mathbb{Z}[X]$, όπου συνολικός τους βαθμός φράσσεται από d και το δυαδικό τους μήκος από τ. Θέλουμε να υπολογίσουμε το πλήθος αλλά και τις πραγματικές ρίζες, γ, του f για τις οποίες ισχύει $A_i(\gamma) > 0$, $B_j(\gamma) < 0$ και $C_k(\gamma) = 0$ και $1 \le i \le n_1, 1 \le j \le n_2, 1 \le k \le n_3$. Έστω $n = n_1 + n_2 + n_3$.

Το παραπάνω πρόβλημα ονομάζεται *πρόβλημα των ταυτόχρονων ανισώσεων* (simultaneous inequalities) ή SI για συντομία.

Οι Ben-Or, Kozen, and Reif [15] παρουσίασαν τον αλγόριθμο BKR για την επίλυση του προβλήματος στην πιο γενική του μορφή, όπου τα πολυώνυμα είναι πολλών μεταβλητών. Ωστόσο, στις πολλές μεταβλητές ο BKR είχε εκθετική συμπεριφορά. Στη συνέχεια ο Canny [45] παρουσίασε μια παραλλαγή του BKR η οποία έχει ψευδο-πολυωνυμική πολυπλοκότητα στις πολλές μεταβλητές και η οποία έχει καλύτερη πολυπλοκότητα στην περίπτωση της μιας μεταβλητής. Πιο συγκεκριμένα, η αριθμητική πολυπλοκότητα του SI στην περίπτωση της μιας μεταβλητής είναι

$\mathcal{O}(n(R\,d\,\lg(R)\,\lg^2(d)+R^{2.376}))$, όπου R είναι το πλήθος των πραγματικών ριζών του A.

Οι Coste and Roy [58] εισήγαγαν την κωδικοποίηση των πραγματικών ριζών ενός πολυωνύμου κατά Thom, όπου οι ρίζες χαρακτηρίζονται και αναπαρίστανται από το πρόσημο (όλων) των παραγώγων του f πάνω σε αυτές. Βασιζόμενοι σε αυτή την αναπαράσταση παρουσίασαν ένα αλγόριθμο, βασισμένο στον BKR, για το πρόβλημα SI. Η προσέγγισή τους, όπως και οι προσεγγίσεις των Ben-Or et al. [15] και Canny [45], είναι συμβολική και ο αλγόριθμος τους είναι νόμιμος για πολυώνυμα ορισμένα σε οποιοδήποτε πραγματικό κλειστό σώμα. Η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(N^8)$, όπου $N=\max\{d,n,\tau,R\}$, αλλά δεν χρησιμοποιούν τους γρήγορους αλγορίθμους για τον υπολογισμό ακολουθιών υπο-επιλυουσών.

Τέλος, οι Basu et al. [14], δείτε επίσης [231], παρουσιάζουν έναν αλγόριθμο για το SI, όπου γίνεται η παραδοχή ότι οι πραγματικοί αλγεβρικοί αριθμοί είναι σε αναπαράσταση με διάστημα απομόνωσης, ο οποίος έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(nd^6\tau^2)$ ή $\widetilde{\mathcal{O}}_B(N^9)$. Χρησιμοποιούν συνεχείς εκλεπτύνσεις των διαστημάτων απομόνωσης και δεν υποθέτουν γρήγορους αλγορίθμους για τον πολλαπλασιασμό.

Ο αλγόριθμός που παρουσίαζουμε βελτιώνει την πολυπλοκότητα του προβλήματος κατά δύο ή τρεις παράγοντες και είναι πολύ πιο απλός από όλες τις μέχρι τώρα προσεγγίσεις.

Πόρισμα 4.6. *Υπάρχει αλγόριθμος για το πρόβλημα των ταυτόχρονων ανισώσεων (SI) με πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(d^4\tau\max\{n,\tau\})$.

Απόδειξη: Αρχικά υπολογίζουμε τις πραγματικές ρίζες του f σε αναπαράσταση με διάστημα απομόνωσης με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (Θεωρ. 3.41). Υπάρχουν το πολύ d πραγματικές ρίζες. Για κάθε πραγματική ρίζα γ του f και για κάθε πολυώνυμο A_i, B_j και C_k, υπολογίζουμε το πρόσημο $\mathrm{sign}\,(A_i(\gamma))$, $\mathrm{sign}\,(B_j(\gamma))$ και $\mathrm{sign}\,(C_k(\gamma))$. Ο υπολογισμός του προσήμου έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Πορ. 4.4) και στη χειρότερη περίπτωση πρέπει να επαναλάβουμε αυτή τη διαδικασία n φορές. Συνεπώς, η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(\max\{nd^4\tau, d^4\tau^2\})$. ΟΕΔ

Υπολογισμοί σε σώμα επέκτασης

Έστω $\gamma\cong(A,\mathbb{J})$. Ας υποθέσουμε προς τη στιγμή ότι το A είναι το ελάχιστο πολυώνυμο του γ. Αν στο $\mathbb{Q}$ επισυνάψουμε το γ τότε το καινούργιο σύνολο το συμβολίζουμε με $\mathbb{Q}(\gamma)$ και το ονομάζουμε σώμα επέκτασης. Η αλγεβρική δομή $\mathbb{Q}(\gamma)$ είναι ένας διανυσματικός χώρος πάνω στο $\mathbb{Q}$ και μία βάση του είναι η $\{1,\gamma,\ldots,\gamma^{d-1}\}$. Κατά συνέπεια τα στοιχεία $\beta\in\mathbb{Q}(\alpha)$ είναι πολυώνυμα ως προς γ βαθμού το πολύ $d-1$ με ακέραιους συντελεστές. Παρατηρούμε ότι πάντοτε μπορούμε να απαλείψουμε τους παρανομαστές με το ΕΚΠ.

Οι πράξεις της πρόσθεσης, της αφαίρεσης και του πολλαπλασιασμού υλοποιούνται όπως ακριβώς και στα πολυώνυμα μιας μεταβλητής (Παρ. 2.2). Η πιο βασική πράξη είναι ο υπολογισμός τους προσήμου, $\mathrm{sign}(\beta)$, $\beta\in\mathbb{Q}(\gamma)$. Ωστόσο, ο β είναι αναπαρίσταται με ένα πολυώνυμο μιας μεταβλητής ως προς γ, έστω f, συνεπώς $\mathrm{sign}(\beta)=\textsc{sign\_at}(A,f)$. Προκειμένου να συγκρίνουμε $\beta_1,\beta_2\in\mathbb{Q}(a)$, αρκεί να υπολογίσουμε το $\mathrm{sign}(\beta_1-\beta_2)$.

Το γεγονός ότι όλες οι πράξεις υλοποιούνται είτε ως πράξεις πολυωνύμων είτε με τη χρήση των ακολουθιών υπο-επιλυουσών μας επιτρέπει να μην απαιτήσουμε το ελάχιστο πολυώνυμο

του γ, αλλά ένα οποιοδήποτε πολυώνυμο το οποίο έχει το γ ως ρίζα. Ωστόσο, χρειάζεται ειδική προσοχή στη διαίρεση β_1/β_2 [195]. Μια άλλη προσέγγιση [49] χρησιμοποιεί τη βάση Horner για να αναπαραστήσει τα πολυώνυμα που ορίζουν το $\beta \in \mathbb{Q}(\gamma)$.

4.2 Υπολογισμοί με δύο αλγεβρικούς αριθμούς

Θα παρουσιάσουμε αλγορίθμους που αφορούν υπολογισμούς με δύο αλγεβρικούς αριθμούς και την επίλυση πολυωνυμικών συστημάτων με δύο μεταβλητές. Όλοι οι αλγόριθμοι που θα παρουσιάσουμε βασίζονται στις προσημασμένες ακολουθίες υπο-επιλυουσών.

Αρχικά θα επεκτείνουμε τα αποτελέσματα της Εν. 2.3, που αφορούν υπολογισμούς με υπο-επιλύουσες με πολυνώνυμα σε μία μεταβλητή, σε πολυώνυμα με πολλές μεταβλητές. Στη συνέχεια θα παρουσιάσουμε έναν αλγόριθμο για τον υπολογισμό του προσήμου της αποτίμησης ενός πολυωνύμου (σε δύο μεταβλητές) πάνω σε δύο πραγματικούς αλγεβρικούς αριθμούς. Τέλος, θα παρουσιάσουμε δύο αλγορίθμους για την επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές και έναν αλγόριθμο για το πρόβλημα των ταυτόχρονων ανισώσεων.

Υπο-επιλύουσες πολυωνύμων σε δύο μεταβλητές

Στους αλγορίθμους που θα παρουσιάσουμε θα χρησιμοποιήσουμε συστηματικά την τεχνική της *δυαδικής τμηματοποίησης* (binary segmentation) [24, 25, 159, 222, 263], η πρώτη παραλλαγή της οποίας πιθανώς οφείλεται στον Kronecker. Η ιδέα της δυαδικής τμηματοποίησης είναι η εξής: Εφαρμόζουμε έναν κατάλληλο ομομορφισμό εκτίμησης σε ένα ακέραιο πολυώνυμο, δηλαδή το αποτιμούμε πάνω σε έναν κατάλληλο ακέραιο αριθμό και προφανώς το αποτέλεσμα είναι ένας ακέραιος αριθμός. Στη συνέχεια, εφαρμόζουμε τον αλγόριθμο που μας ενδιαφέρει στον ακέραιο που είναι το απολέσμα της αποτίμησης και τέλος στο αποτέλεσμα (που είναι επίσης αριθμός) εφαρμόζουμε τον αντίστροφο ομομορφισμό εκτίμησης έτσι ώστε να πάρουμε το αποτέλεσμα. Ιδιαίτερη προσοχή απαιτείται έτσι ώστε ο αριθμός πάνω στον οποίο, αρχικά, θα αποτιμήσουμε το πολυώνυμό μας να είναι αρκετά μεγάλος έτσι ώστε στο τελικό αποτέλεσμα να είναι δυνατόν να εφαρμοστεί ο αντίστροφος ομομορφισμός. Οι διάφορες παραλλαγές αυτής της τεχνικής χαρακτηρίζονται ανάλογα με τον αλγόριθμο κωδικοποίησης, δηλαδή ανάλογα με το πως επιλέγουν τους ακεραίους που χρησιμοποιούν για τις αποτιμήσεις. Για το λόγο αυτό, το ακόλουθο λήμμα, που οφείλεται στον Klose [159] είναι πολύ σημαντικό, καθώς μέσω ενός ομομορφισμού εκτίμησης απεικονίζει πολυώνυμα σε ακεραιίους αριθμούς και εξασφαλίζει την ύπαρξη της αντίστροφης απεικόνισης.

Λήμμα 4.7. *Έστω $n, \lambda \in \mathbb{N}$. Αν $n \geq 2$ τότε $D \in \mathbb{N}$ αλλιώς $D = \infty$. Έστω $\nu = (\nu_1, \nu_2, \ldots, \nu_n)$ με $\nu_i = (\lambda+1)(D^{i-1} + D^{i-2} + \cdots + D + 1)$, $1 \leq i \leq n$. Ο ομομορφισμός εκτίμησης*

$$\begin{aligned} \phi_\nu : P_{\lambda,D} &\to \mathbb{Z} \\ f &\mapsto f(2^{\nu_1}, \ldots, 2^{\nu_n}) \end{aligned}$$

όπου $P_{\lambda,D} = \{f \in \mathbb{Z}[X_1, \ldots, X_n] \,|\, \mathcal{L}(f) \leq \lambda \wedge \deg(f) \leq D\}$, είναι $1-1$ και υπάρχει η αντίστροφη απεικόνιση, $\phi_\nu^{-1} : \phi_\nu(\mathbb{Z}) \to \mathbb{Z}[X_1, \ldots, X_n]$.

Επιπρόσθετα αν $f \in P_{\lambda,D}$ και $\deg(f) = p \leq D$ και $\mathcal{L}(f) = \sigma \leq \lambda$, τότε $\mathcal{L}(\phi_\nu(f)) \leq \nu_n p + \sigma + 1$.

Με απλά λόγια το Λημ. 4.7 μας εξασφαλίζει ότι αν επιλέξουμε ακεραίους σύμφωνα με τους κανόνες του τότε οι αποτιμήσεις διαφορετικών πολυωνύμων του $P_{\tau,D}$ δίνουν διαφορετικό αποτέλεσμα. Το επόμενο παράδειγμα αναδεικνύει τη χρήση του Λημ. 4.7.

Παράδειγμα 4.8. *Έστω το πολυώνυμο* $f = X^2 + 3X + 1 \in \mathbb{Z}[X]$. *Αντικαθιστώντας όπου* X *το* $2^2 = 4$ *έχουμε ότι* $\phi_1(f) = 4^2 + 3\cdot 4 + 1 = 29$. *Από το* 29 *προκύπτει το* f *ως εξής. Παρατηρούμε ότι* $\left(\mathsf{rem}\left(29, 4^2\right), \mathsf{quo}\left(29, 4^2\right)\right) = (13, 1)$ *οπότε ο μεγιστοβάθμιος συντελεστής είναι* 1. *Στη συνέχεια* $\left(\mathsf{rem}\left(13, 4^1\right), \mathsf{quo}\left(13, 4^1\right)\right) = (1, 3)$ *οπότε ο συντελεστής του γραμμικού όρου είναι* 3 *και τέλος αφού* $\left(\mathsf{rem}\left(1, 4^0\right), \mathsf{quo}\left(1, 4^0\right)\right) = (0, 1)$, *ο σταθερός όρος είναι* 1.

Επίσης παρατηρήστε ότι $(29)_{10} = (01\,11\,01)_2$. *Τα δύο πρώτα ψηφία της δυαδικής αναπαράστασης είναι ο συντελεστής του* X^2, *τα δύο επόμενα του* X *και τα δύο τελευταία του σταθερού όρου.*

Το επόμενο θεώρημα είναι η επέκταση του Θεωρ. 2.30 για πολυώνυμα σε πολλές μεταβλητές.

Θεώρημα 4.9

Έστω $f, g \in (\mathbb{Z}[Y_1, \ldots, Y_n])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ *και* $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. *Επιπρόσθετα, έστω* $\deg_{Y_i}(f) \leq d$ *και* $\deg_{Y_i}(g) \leq d$, *όπου* $1 \leq i \leq n$. *Ο υπολογισμός της ακολουθίας* $\mathbf{SR}(f, g)$ *ως προς* X, *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(2^{n-1}\, p^{n+2}\, q\, d^n\, \tau)$.

Απόδειξη: Θα χρησιμοποιήσουμε το Λημ. 4.7. Θεωρούμε τον ομομορφισμό εκτίμησης $\phi = \phi_n$, όπου $\nu_i = (\lambda+1)(D^{i-1}+\cdots+D+1)$, $\lambda = \max\{\mathcal{L}(\mathbf{SR}_j(f, g))\}$, και $D \geq \max\{\deg(\mathbf{SR}_j(f, g))\}$, όπου $1 \leq i \leq n$ και $0 \leq j \leq q$.

Τα πολυώνυμα $\phi(f)$ και $\phi(g)$ είναι μιας μεταβλητής, δηλαδή $\phi(f), \phi(g) \in \mathbb{Z}[X]$. Επίσης, $\deg(\phi(f)) = p \leq q = \deg(\phi(g))$ και τα $\mathcal{L}(\phi(f)) = \mathcal{L}(\phi(g))$ φράσσονται από

$$\mathcal{O}(d \cdot \lambda \cdot \sum_{i=1}^{n} \nu_i + \tau) = \mathcal{O}(d \cdot \lambda \cdot D^{n-1})$$

Από το Θεωρ. 2.30 η ακολουθία $\mathbf{SR}(\phi(f), \phi(g))$ υπολογίζεται σε $\mathcal{O}\left(p\, q\, \mathsf{M}\left(p \cdot d \cdot \lambda \cdot D^{n-1}\right)\right)$.

Απομένει να επιλέξουμε τα D και λ τα οποία εξαρτώνται από το βαθμό και το δυαδικό μήκος των πολυωνύμων $\mathbf{SR}_j \in \mathbb{Z}[X]$. Προκειμένου να φράξουμε το βαθμό των $\mathbf{SR}_j$ χρησιμοποιούμε τον ορισμό τους ως πολυώνυμα οριζουσών (Ορ. 2.19) και την ανισότητα του Hadamard [14] και συμπεραίνουμε ότι $\deg(\mathbf{SR}_j(f, g)) \leq d(p + q - 2j)$. Οπότε επιλέγουμε $D = 2dp$. Με την ίδια τεχνική φράσσουμε και το δυαδικό τους μήκος. Πιο συγκεκριμένα

$$\mathcal{L}(\mathbf{SR}_j(f, g)) \leq (\tau + \mathcal{L}(p + q))(p + q - 2j) + n\,\mathcal{L}((p + q)d + 1)$$

οπότε επιλέγουμε $\lambda = \mathcal{O}(p\tau + (p + n)\lg(pd))$ ή $\lambda = \widetilde{\mathcal{O}}(p\tau)$. Κατά συνέπεια ο υπολογισμός της ακολουθίας $\mathbf{SR}(\phi(f), \phi(g))$ έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(2^{n-1}\, p^{n+2}\, q\, d^n\, \tau)$.

Προκειμένου να υπολογίσουμε την ακολουθία $\mathbf{SR}(f, g)$ ως προς X, αρκεί να εφαρμόσουμε τον μετασχηματισμό ϕ^{-1} στα πολυώνυμα της ακολουθίας $\mathbf{SR}(\phi(f), \phi(g))$. ΟΕΔ

Ο Reischert [222] για την απόδειξη του Θεωρ. 4.9 χρησιμοποιεί επαναληπτική δυαδική τμηματοποίηση κατά Kronecker, δείτε επίσης [263]. Ωστόσο, ο μετασχηματισμός του Λημ. 4.7 έχει πιο εύκολο αλγόριθμο κωδικοποίησης και αποκωδικοποίησης [159]. Η δε αριθμητική πολυπλοκότητά του είναι γραμμική ως προς την έξοδο και απαιτεί μόνο προσθέσεις και ολισθήσεις [159] και σε καμία περίπτωση δεν επηρεάζει την πολυπλοκότητα όλων των αλγορίθμων που παρουσιάζουμε. Η πολυπλοκότητα υπολογισμού της ακολουθίας **SR**, Θεωρ. 4.9, που παρουσιάσαμε είναι ίδια με αυτή που παρουσίασε ο Reischert [222] και είναι καλύτερη κατά ένα παράγοντα 2 (και κάποιους πολυ-λογαριθμικούς παράγοντες) από αυτή που παρουσίασε ο Klose [159].

Το επόμενο θεώρημα επεκτείνει το Θεωρ. 2.31 και αφορά τον υπολογισμό της ακολουθίας **SRQ** σε πολυώνυμα πολλών μεταβλητών. Το φράγμα πολυπλοκλότητας που επιτυγχάνεται είναι το ίδιο με αυτό του Reischert [222].

Θεώρημα 4.10

Έστω $f, g \in (\mathbb{Z}[Y_1, \ldots, Y_n])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ *και* $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. *Επιπρόσθετα, έστω* $\deg_{Y_i}(f) \leq d$ *και* $\deg_{Y_i}(g) \leq d$, *όπου* $1 \leq i \leq n$.

Ο υπολογισμός της ακολουθίας $\mathbf{SRQ}(f, g)$, *οποιουδήποτε πολυωνύμου της ακολουθίας* $\mathbf{SR}(f, g)$, *του* $\mathtt{res}(f, g)$ *και του* $\gcd(f, g)$ *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(2^{n-1}\, p^{n+1}\, q\, d^n\, \tau)$.

Απόδειξη: Χρησιμοποιούμε τον ίδιο μετασχηματισμό, όπως και στην απόδειξη του Θεωρ. 4.9. Έτσι έχουμε $\phi(f), \phi(g) \in \mathbb{Z}[X]$ όπου $\deg(f) = p \geq q = \deg(g)$ και $\mathcal{L}(f) = \mathcal{L}(q) = \mathcal{O}(d \cdot \lambda \cdot D^{n-1})$. Ο υπολογισμός $\mathbf{SRQ}(\phi(f), \phi(g))$ έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(p\, q\, d\, \lambda\, D^{n-1})$ (Θεωρ. 2.31). Αντικαθιστώντας $\lambda = \widetilde{\mathcal{O}}(p\tau)$ και $D = 2\, d\, p$ προκύπτει η ζητούμενη πολυπλοκότητα.

Καθώς τα $\mathtt{res}(f, g)$ και $\gcd(f, g)$ είναι στοιχεία της ακολουθίας **SRQ**, το θεώρημα αποδείχτηκε. ΟΕΔ

Με την εξαίρεση του υπολογισμού της επιλύουσας, η πολυπλοκότητα του προηγούμενου θεωρήματος είναι βέλτιστη. Αυτό δεν ισχύει μόνο για την περίπτωση της επιλύουσας.

Για πολυώνυμα σε δύο μεταβλητές τα δύο προηγούμενα θεωρήματα μας οδηγούν στα ακόλουθα πορίσματα:

Πόρισμα 4.11. *Έστω* $f, g \in (\mathbb{Z}[Y])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$, $\deg_Y(f) \leq d$, $\deg_Y(g) \leq d$ *και* $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. *Ο υπολογισμός της ακολουθίας* $\mathbf{SR}(f, g)$ *ως προς* X *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(p^3\, q\, d\, \tau)$.

Επιπρόσθετα $\mathcal{L}(\mathbf{SR}_j(f, g)) = \mathcal{O}(p\tau)$ *και* $\deg_Y(\mathbf{SR}_j(f, g)) \leq 2\, d\, p$.

Πόρισμα 4.12. *Έστω* $f, g \in (\mathbb{Z}[Y])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ $\deg_Y(f) \leq d$, $\deg_Y(g) \leq d$ *και* $\mathcal{L}(F) \leq \mathcal{L}(G) \leq \tau$. *Ο υπολογισμός της ακολουθίας* $\mathbf{SRQ}(f, g)$, *ως προς* X, *οποιουδήποτε πολυωνύμου στην ακολουθία* $\mathbf{SR}(f, g)$, *του* $\mathtt{res}(f, g)$ *και του* $\gcd(f, g)$ *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(p^2\, q\, d\, \tau)$.

Επιπρόσθετα $\deg_Y(\mathtt{res}(f, g)) \leq 2\, d\, p$.

Το επόμενο πόρισμα, περιέργως πως, δεν παρουσιάζεται στην βιβλιογραφία.

Πόρισμα 4.13. *Έστω* $f, g \in (\mathbb{Z}[Y])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ $\deg_Y(f) \leq d$, $\deg_Y(g) \leq d$ *και* $\mathcal{L}(F), \mathcal{L}(G) \leq \tau$. *Ο υπολογισμός της αποτίμησης* $\mathbf{SR}(f, g\,;\, \mathsf{a})$, *ως προς* X, *όπου* $\mathcal{L}(\mathsf{a}) = \sigma$, *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(q\ \max\{p^2\, d\, \tau, q\, \sigma\})$.

Επιπρόσθετα $\mathbf{SR}_j(\mathsf{a}) \in \mathbb{Z}[Y]$, $\deg_Y(\mathbf{SR}_j(\mathsf{a})), \deg(\mathbf{SR}_j(\mathsf{a})) \leq 2\, d\, p$ *και* $\mathcal{L}(\mathbf{SR}_j(\mathsf{a})) = \mathcal{O}(\max\{p\, \tau, d\, \sigma\})$.

Απόδειξη: Θα χρησιμοποιήσουμε το Λημ. 4.7. Θεωρούμε τον ομομορφισμό εκτίμησης $\phi = \phi_1$, όπου $\nu_1 = \nu = (L+1)$, $L = \max\{\mathcal{L}(\mathbf{SR}_j(f, g))\} = \mathcal{O}(p\, \tau)$, $0 \leq j \leq d$. Για τα πολυώνυμα $\phi(f), \phi(g) \in \mathbb{Z}[X]$ ισχύει $\mathcal{L}(\phi(f)) = \mathcal{L}(\phi(g)) = \mathcal{O}(d\, L + \tau) = \mathcal{O}(d\, L)$.

Υπολογίζουμε την αποτίμηση $\mathbf{SR}(\phi(f), \phi(g)\,;\, \mathsf{a})$ με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(q\ \max\{p\, d\, L, q\, \sigma\})$ ή $\widetilde{\mathcal{O}}_B(q\ \max\{p^2\, d\, \tau, q\, \sigma\})$ (Θεωρ. 2.32). Για κάθε ένα $\mathbf{SR}_j(\phi(f), \phi(g)\,;\, \mathsf{a}) \in \mathbb{Z}$, $0 \leq j \leq q$, εφαρμόζουμε τον μετασχηματισμό ϕ^{-1} προκειμένου να πάρουμε το $\mathbf{SR}_j(f, g\,;\, \mathsf{a}) \in \mathbb{Z}[X]$.

Προκειμένου να φράξουμε το βαθμό των $\mathbf{SR}_j$ ως προς Y χρησιμοποιούμε τον ορισμό τους ως πολυώνυμα οριζουσών (Ορ. 2.19) και την ανισότητα του Hadamard [14] και συμπεραίνουμε ότι $\deg_Y(\mathbf{SR}_j(\mathsf{a})) = \deg(\mathbf{SR}_j(\mathsf{a})) \leq 2\, d\, p$. Και με την ίδια τεχνική, εφόσον $\mathcal{L}(\mathbf{SR}_j(f, g)) = \mathcal{O}(p\, \tau)$ συνάγουμε ότι $\mathcal{L}(\mathbf{SR}_j(f, g\,;\, \mathsf{a})) = \mathcal{O}(\max\{p\, \tau, d\, \sigma\})$ (Εν. 2.2). ΟΕΔ

Το γεγονός ότι οι (προσημασμένες) ακολουθίες υπο-επιλυουσών (signed subresultant sequences) έχουν καλή συμπεριφορά ακόμα κι όταν οι συντελεστές των πολυωνύμων είναι παράμετροι, δείτε [118, 119] και Εν. 2.3, βρίσκει εφαρμογή όταν απαιτούνται υπολογισμοί με πολυώνυμα πολλών μεταβλητών (στην περίπτωσή μας με δύο μεταβλητές). Αν f και g είναι δύο πολυώνυμα με παραμετρικούς συντελεστές, τέτοια ώστε ο βαθμός τους να μην μεταβάλλεται για οποιαδήποτε τιμή των παραμέτρων, ο υπολογισμός της ακολουθίας $\mathbf{SR}(f, g)$ μας εγγυάται ότι για οποιαδήποτε τιμή των παραμέτρων η ακολουθία είναι ορθή. Θα χρησιμοποιήσουμε αυτή την ιδιότητα, στην περίπτωση που τα f και g είναι πολυώνυμα σε δύο μεταβλητές, προκειμένου να υπολογίσουμε την $\mathbf{SR}(f, g)$ ως προς Y (ή ως προς X) θεωρώντας ότι τα πολυώνυμα ανήκουν στο $(\mathbb{Z}[X])[Y]$ (ή στο $(\mathbb{Z}[Y])[X]$).

Η επόμενη υπόθεση είναι πολύ χρήσιμη για τη συνέχεια.

Ορισμός 4.14 (Υπόθεση της γενικής θέσης). *Δύο πολυώνυμα* $f, g \in \mathcal{R}[X, Y]$ *είναι σε γενική θέση αν* $\mathsf{lead}_Y(f) \neq 0$, $\mathsf{lead}_Y(g) \neq 0$ *και για κάθε* $(\alpha_1, \beta), (\alpha_2, \beta) \in \mathcal{K}^2$ *τέτοια ώστε* $f(\alpha_1, \beta) = g(\alpha_1, \beta) = 0$ *και* $f(\alpha_2, \beta) = g(\alpha_2, \beta) = 0$ *να ισχύει* $\alpha_1 \neq \alpha_2$.

Με άλλα λόγια, η υπόθεση της γενικής θέσης απαιτεί οι λύσεις του συστήματος $f = g = 0$ με κοινή τεταγμένη να έχουν διαφορετική τετμημένη και οι μεγιστοβάθμιοι όροι ως προς Y να μην μηδενίζονται. Το ακόλουθο θεώρημα, το οποίο βασίζεται στην υπόθεση της γενικής θέσης, είναι εξέχουσας σημασίας:

Θεώρημα 4.15

[14, 116, 117] Έστω $f, g \in \mathcal{R}[X, Y]$ *τα οποία είναι σχετικά πρώτα αν τα θεωρήσουμε πολυώνυμα ως προς* Y *και ικανοποιούν την υπόθεση της γενικής θέσης. Έστω*

$$\mathbf{SR}_j(f, g) = \mathbf{sr}_j(X) Y^j + \mathbf{sr}_{j,i-1}(X) Y^{j-1} + \cdots + \mathbf{sr}_{j,0}(X) \quad \in (\mathcal{R}[X])[Y]$$

τα πολυώνυμα της ακολουθίας $\mathbf{SR}(f, g)$ *ως προς* Y, *όπου* $\mathbf{sr}_j = \mathbf{psc}_j$. *Αν* $(\alpha, \beta) \in \mathcal{K}^2$, *τέτοιο ώστε* $f(\alpha, \beta) = g(\alpha, \beta) = 0$ *τότε υπάρχει δείκτης* k *τέτοιος ώστε*

$$\mathbf{sr}_0(\alpha) = \cdots = \mathbf{sr}_{k-1}(\alpha) = 0, \quad \mathbf{sr}_k(\alpha) \neq 0, \quad \beta = -\frac{1}{k} \frac{\mathbf{sr}_{k,k-1}(\alpha)}{\mathbf{sr}_k(\alpha)}$$

Απόδειξη: Έστω ότι για κάποια ρίζα $\alpha \in \mathcal{K}$ του $\mathbf{sr}_0 = \mathbf{SR}_0 \in \mathcal{R}[X]$ ισχύει $\mathbf{sr}_0(\alpha) = \mathbf{sr}_1(\alpha) = 0, \ldots, \mathbf{sr}_{k-1}(\alpha) = 0$ και $\mathbf{sr}_k(\alpha) \neq 0$. Στην ακολουθία $\mathbf{SR}(f, g)$, η οποία είναι ως προς Y, κάνουμε την αντικατάσταση $X = \alpha$. Την προκύπτουσα ακολουθία, η οποία έχει πολυώνυμα στον χώρο $(\mathbb{Z}[\alpha])[Y]$, τη συμβολίσουμε $\widetilde{\mathbf{SR}}$. Λόγω των καλών ιδιοτήτων των ακολουθιών υποεπιλυουσών, είμαστε βέβαιοι ότι η ακολουθία είναι η ίδια με αυτή που θα είχαμε υπολογίσει αν είχαμε κάνει την αντικατάσταση $X = \alpha$ μόνο στα f και g και ακολούθως είχαμε υπολογίσει την ακολουθία.

Εφόσον ο πρώτος μη μηδενικός πρωταρχικός συντελεστής της $\widetilde{\mathbf{SR}}$ έχει δείκτη k, ο ΜΚΔ των $\widetilde{f}, \widetilde{g} \in (\mathbb{Z}[\alpha])[Y]$ είναι το πολυώνυμο $\widetilde{\mathbf{SR}}_k$, το οποίο έχει βαθμό k, και άρα τα $\widetilde{f}, \widetilde{g}$ έχουν k κοινές ρίζες (Θεωρ. 2.20). Με άλλα λόγια οι Y συντεταγμένες των λύσεων του συστήματος $f = g = 0$, που έχουν για X συντεταγμένη το α, είναι οι ρίζες του $\widetilde{\mathbf{SR}}_k$. Ωστόσο, τα f και g είναι σε γενική θέση, συνεπώς κάθε λύση του συστήματος έχει διαφορετική X συντεταγμένη. Κατά συνέπεια το $\widetilde{\mathbf{SR}}_k$ πρέπει να έχει μία και μόνο μία ρίζα και επειδή είναι βαθμού k, έχει μία πραγματική ρίζα πολλαπλότητας k.

Άρα $\widetilde{\mathbf{SR}}_k = (k \cdot \mathbf{sr}_k(\alpha)\, Y + \mathbf{sr}_{k,k-1}(\alpha))^k$ και συνεπώς η ρίζα του είναι $-\frac{1}{k}\frac{\mathbf{sr}_{k,k-1}(\alpha)}{\mathbf{sr}_k(\alpha)}$. ΟΕΔ

Υπολογισμός προσήμου

Algorithm 17: SIGN_AT(F, α, β)

Input: $F \in \mathbb{Z}[X, Y], \alpha \cong (A, \mathbb{J}_1 = [\mathsf{a}_1, \mathsf{b}_1]), \beta \cong (B, \mathbb{J}_2 = [\mathsf{a}_2, \mathsf{b}_2])$
Output: $\mathrm{sign}(F(\alpha, \beta))$

1 $Q_1 \leftarrow \emptyset$
2 $L_1 \leftarrow \mathbf{SR}_X(A, F\,;\, \mathsf{a}_1)$
3 **foreach** $f \in L_1$ **do** $Q_1 \leftarrow$ ADD$(Q_1,$ SIGN_AT$(f, \beta))$
4 $Q_2 \leftarrow \emptyset$
5 $L_2 \leftarrow SR_X(A, F\,;\, \mathsf{b}_1)$
6 **foreach** $f \in L_2$ **do** $Q_2 \leftarrow$ ADD$(Q_2,$ SIGN_AT$(f, \beta))$
7 RETURN $(\mathrm{VAR}(Q_1) - \mathrm{VAR}(Q_2)) \cdot \mathrm{sign}(A'(\alpha))$

Όπως και στην περίπτωση των υπολογισμών με έναν πραγματικό αλγεβρικό αριθμό, ο πιο σημαντικός υπολογισμός είναι το πρόσημο της αποτίμησης. Πιο συγκεκριμένα, θεωρούμε $F \in \mathbb{Z}[X, Y]$, $\alpha \cong (A(x), \mathbb{J}_1)$ και $\beta \cong (B(X), \mathbb{J}_2)$ όπου $\mathbb{J}_1 = [a_1, b_1]$, $\mathbb{J}_2 = [a_2, b_2]$. Θέλουμε να υπολογίσουμε το πρόσημο της αποτίμησης $F(\alpha, \beta)$. Τον υπολογισμό αυτό θα τον συμβολίσουμε με SIGN_AT(F, α, β). Ο ψευδο-κώδικας του αλγορίθμου παρουσιάζεται στον Αλγ. 17.

Θεώρημα 4.16

Έστω $F \in \mathbb{Z}[X, Y]$ τέτοιο ώστε $\deg_X(F) = \deg_Y(F) = n_1$ και $\mathcal{L}(F) = \sigma$ και δύο πραγματικοί

αλγεβρικοί αριθμοί $\alpha \cong (A, \mathcal{I}_\alpha) = [\mathsf{a}_1, \mathsf{b}_1]$, $\beta \cong (B, \mathcal{I}_\beta) = [\mathsf{a}_2, \mathsf{b}_2]$ *όπου* $A, B \in \mathbb{Z}[X]$, $\deg(A) = \deg(B) = n_2$, $\mathcal{L}(A) = \mathcal{L}(B) = \sigma$ *και* $\mathcal{I}_\alpha, \mathcal{I}_\beta \in \mathbb{Q}^2$ *και το δυαδικό μήκος των άκρων τους φράσσεται από* $\mathcal{O}(n_2\,\sigma)$.

Μπορούμε να υπολογίσουμε το πρόσημο της αποτίμησης του F *πάνω στους* α *και* β, *δηλαδή* SIGN_AT(F, α, β), *χρησιμοποιώντας τον Αλγ. 17 με πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(n_1^3\, n_2^3\, \sigma)$, *υποθέτουτας ότι* $n_1 \leq n_2$.

Απόδειξη: Αρχικά θεωρούμε το F ως πολυώνυμο ως προς X με συντελεστές πολυώνυμα ως προς Y, δηλαδή $F \in (\mathbb{Z}[Y])[X]$ και προσπαθούμε να υπολογίσουμε το πρόσημό του αν το αποτιμήσουμε πάνω στο α, όπως ακριβώς κάναμε και στην περίπτωση της μίας μεταβλητής (Αλγ. 15).

Υπολογίζουμε την αποτίμηση της ακολουθίας $\mathbf{SR}(A, F)$ ως προς X, πάνω στο a_1, δηλαδή την ακολουθία $\mathbf{SR}(A, F\,;\, \mathsf{a}_1)$ (Γραμμή 2 στον Αλγ. 17). Ο υπολογισμός αυτός κοστίζει $\widetilde{\mathcal{O}}_B(n_1^2\, n_2^2\, \sigma)$ (Πορ. 4.13). Η ακολουθία $\mathbf{SR}(A, F\,;\, \mathsf{a}_1)$ (L_1 στον Αλγ. 17) περιέχει $\mathcal{O}(n_1)$ πολυώνυμα στο $\mathbb{Z}[Y]$ με βαθμούς $\mathcal{O}(n_1\, n_2)$ και δυαδικό μήκος $\mathcal{O}(n_1\, n_2\, \sigma)$.

Για κάθε ένα πολυώνυμο στην $\mathbf{SR}(A, F\,;\, \mathsf{a}_1)$, υπολογίζουμε το SIGN_AT$(\mathbf{SR}_j(A, F\,;\, \mathsf{a}_1), \beta)$ (Γραμμή 3 στον Αλγ. 17) και μετράμε τις εναλλαγές προσήμων. Ο υπολογισμός SIGN_AT$(\mathbf{SR}_j(A, F\,;\, \mathsf{a}_1), \beta)$ κοστίζει $\widetilde{\mathcal{O}}_B(n_1^2\, n_2^3\, \sigma)$ (Θεωρ. 2.32) και καθώς χρειαζόμαστε $\mathcal{O}(n_1)$ τέτοιους υπολογισμούς, το συνολικός κόστος είναι $\widetilde{\mathcal{O}}_B(n_1^3\, n_2^3\, \sigma)$.

Κάνουμε το ίδιο για το δεξί άκρο του $\mathcal{I}_\alpha$ το b_1 και αφαιρούμε τις εναλλαγές προσήμων. Ο υπολογισμός του $\mathrm{sign}(A'(\alpha))$ γίνεται όπως στον Αλγ. 15 και κοστίζει $\widetilde{\mathcal{O}}_B(n_2^3\, \sigma)$.

Συμπεραίνουμε ότι η συνολική πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(n_1^3\, n_2^3\, \sigma)$. ΟΕΔ

Από όσο είμαστε σε θέση να γνωρίζουμε η πολυπλοκότητα του προηγούμενου θεωρήματος δεν ήταν γνωστή μέχρι σήμερα. Μπορούμε να γενικεύσουμε το Θεώρημα στον υπολογισμό προσήμου της αποτίμησης ενός πολυωνύμου με k μεταβλητές πάνω σε k πραγματικούς αλγεβρικούς αριθμούς, ακολουθώντας την προσέγγιση του Sakkalis [234]. Ωστόσο, το γεγονός ότι χρησιμοποιούμε ακολουθίες υπο-επιλυουσών, αντί για προσημασμένες Ευκλείδιες ακολουθίες, βελτιώνει τόσο τη θεωρητική [14] όσο και την πρακτική πολυπλοκότητα [66, 87, 275].

Δύο αλγόριθμοι για την επίλυση συστημάτων

Θεωρούμε το σύστημα

$$\begin{cases} F = \displaystyle\sum_{1 \leq i \leq d} \sum_{1 \leq j \leq d} a_{i,j} X^i Y^j = 0 \\ G = \displaystyle\sum_{1 \leq i \leq d} \sum_{1 \leq j \leq d} d_{i,j} X^i Y^j = 0 \end{cases} \tag{4.1}$$

Υποθέτουμε ότι τα πολυώνυμα του συστήματος $F, G \in \mathbb{Z}[X, Y]$ είναι σχετικά πρώτα και ότι $\deg(F) = \deg(G) = n$ και $\mathcal{L}(F) = \mathcal{L}(G) = \sigma$. Θα παρουσιάσουμε δύο αλγορίθμους και την ανάλυσή τους που αφορούν την πραγματική επίλυση του παραπάνω συστήματος. Οι ιδέα και των δύο αλγορίθμων είναι να προβάλλουμε το σύστημα στον X και στον Y άξονα, να υπολογίσουμε

τις συντεταγμένες των λύσεων και στη συνέχεια με κάποιο τρόπο να τις ταιριάξουμε. Η διαφορά των αλγορίθμων έγκειται στον τρόπο ταιριάσματος. Οι προβολές του συστήματος στους άξονες επιτυγχάνονται με την βοήθεια της επιλύουσας. Υπενθυμίζουμε, δείτε Εν. 2.2, ότι η επιλύουσα δύο πολυωνύμων σε δύο μεταβλητές *απαλείφει* τη μία μεταβλητή. Η έξοδος των αλγορίθμων είναι μια λίστα με ζεύγη πραγματικών αλγεβρικών αριθμών, που είναι λύσεις του συστήματος και αν είναι δυνατόν μια λίστα με τις πολλαπλότητες.

Αν και το πρόβλημα της επίλυσης συστημάτων είναι μια από τις πιο ενεργές επιστημονικές περιοχές στην κοινότητα των αλγεβρικών αλγορίθμων, ο κύριος όγκος των εργασιών επικεντρώνεται σε πολυωνυμικά συστήματα με k μεταβλητές, δείτε για παράδειγμα[1] [46, 84, 95, 168, 197, 198, 199, 200]. Αυτός είναι ο λόγος που αποτελέσματα σε πολυωνυμικά συστήματα 2 μεταβλητών είναι αρκετά περιορισμένα.

Ο απλός αλγόριθμος (NAIVE_SOLVE)

Algorithm 18: NAIVE_SOLVE(F, G)

Input: $F, G \in \mathbb{Z}[X, Y]$

Output: Οι πραγματικές λύσεις του συστήματος $F = G = 0$

```
1  R_x ← res_y(F, G)
2  L_x, M_x ← CONSTRUCT(R_x)
3  R_y ← res_x(F, G)
4  L_y, M_y ← CONSTRUCT(R_y)
5  Q ← ∅
6  foreach α ∈ L_x do
7      foreach β ∈ L_y do
8          if SIGN_AT(F, α, β) = 0 ∧ SIGN_AT(G, α, β) = 0 then
9              Q ← ADD(Q, {α, β})
10 RETURN Q
```

Ο αλγόριθμος NAIVE_SOLVE, ο ψευδο-κώδικας του οποίου παρουσιάζεται στον Αλγ. 18, είναι ο πλέον προφανής. Υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις X και Y συντεταγμένες των πραγματικών λύσεων του συστήματος ως λύσεις των προβολών $\mathtt{res}_Y(F, G)$ και $\mathtt{res}_Y(F, G)$ και στη συνέχεια τις ταιριάζουμε χρησιμοποιώντας τον αλγόριθμο SIGN_AT (Αλγ. 17).

Η είσοδος του αλγορίθμου είναι τα δύο πολυώνυμα $F, G \in \mathbb{Z}[X, Y]$ και η έξοδος του είναι μία λίστα από ζεύγη πραγματικών αλγεβρικών αριθμών σε αναπαράσταση με διάστημα απομόνωσης, η οποία συμβολίζεται με Q στον Αλγ. 18.

Η ορθότητα του αλγορίθμου προκύπτει από το γεγονός ότι αφενός μεν όλες οι πραγματικές λύσεις του συστήματος προκύπτουν από ως πραγματικές λύσεις των $\mathtt{res}_x(F, G)$ και $\mathtt{res}_y(F, G)$

[1] Η βιβλιογραφία για τα πολυωνυμικά συστήματα πολλών μεταβλητών που παρουσιάζουμε είναι ενδεικτική.

και αφετέρου δε από το γεγονός ότι ένα ζεύγος $(\alpha, \beta) \in \mathbb{R}^2_{alg}$ είναι λύση του συστήματος αν και μόνο αν $F(\alpha, \beta) = G(\alpha, \beta) = 0$.

Το επόμενο θεώρημα περιγράφει αναλυτικά τα βήματα του αλγορίθμου και αναλύει την πολυπλοκότητά τους.

Θεώρημα 4.17 (NAIVE_SOLVE)

Έστω $F, G \in \mathbb{Z}[X, Y]$ σχετικά πρώτα, με συνολικό βαθμό που φράσσεται από n και μέγιστο δυαδικό μήκος συντελεστών που φράσσεται από σ. Η πραγματική επίλυση του συστήματος $F = G = 0$ με τον αλγόριθμο NAIVE_SOLVE *έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^{14}\,\sigma)$, με την υπόθεση ότι $\sigma = \mathcal{O}(n^4)$.*

Απόδειξη: Καταρχάς υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις X συντεταγμένες των πραγματικών λύσεων του συστήματος, υπολογίζοντας την επιλύουσα των F και G ως προς Y, R_x, (Γραμμή 1 στον Αλγ. 18). Η πολυπλοκότητα του βήματος είναι $\widetilde{\mathcal{O}}_B(n^4\sigma)$ (Πορ. 4.12). Παρατηρούμε ότι $\deg(R_x) = \mathcal{O}(n^2)$ και $\mathcal{L}(R_X) = \mathcal{O}(n\,\sigma)$. Υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του R_x, με αναπαράσταση διαστήματος απομόνωσης (Γραμμή 2 στον Αλγ. 18) με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^{10}\sigma^2)$ (Θεωρ. 3.41) και τους τοποθετούμε στη λίστα L_x.

Ομοίως και με την ίδια πολυπλοκότητα, υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις Y συντεταγμένες των λύσεων του συστήματος (Γραμμές 3 και 4 στον Αλγ. 18) και τους τοποθετούμε στη λίστα L_y.

Η αναπαράσταση των πραγματικών αλγεβρικών αριθμών που έχουμε υπολογίσει, περιέχει το χωρίς τετράγωνα μέρος του R_x ή του R_y. Και στις δύο περιπτώσεις το δυαδικό μήκος του πολυωνύμου είναι $\mathcal{O}(n + n\,\sigma) = \mathcal{O}(n\,\sigma)$ (Θεωρ. 2.34). Τα διαστήματα απομόνωσης έχουν άκρα ρητούς αριθμούς με δυαδικό μήκος $\mathcal{O}(n^3\,\sigma)$ (Σημ. 3.24). Τέλος, τόσο το μέγεθος της L_x όσο και της L_y είναι $\mathcal{O}(n^2)$.

Σχηματίζουμε όλα τα δυνατά ζεύγη πραγματικών αλγεβρικών αριθμών και ελέγχουμε αν μηδενίζουν τόσο το F όσο και το G (Γραμμή 8 στον Αλγ. 18). Αυτό επιτυγχάνεται με τον αλγόριθμο SIGN_AT (Αλγ. 17). Πρέπει να πραγματοποιήσουμε το πολύ $\mathcal{O}(n^4)$ τέτοιους υπολογισμούς και κάθε ένας από αυτούς κοστίζει $\widetilde{\mathcal{O}}_B(n^{10}\sigma)$ (Θεωρ. 4.16).

Συνεπώς, η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(n^{14}\sigma)$. ΟΕΔ

Ο αλγόριθμος που παρουσιάσαμε, αν και προφανής, δεν έχει αναλυθεί μέχρι σήμερα. Το μειονέκτημα του αλγορίθμου NAIVE, εκτός από τη μεγάλη θεωρητική του πολυπλοκότητα είναι ότι δεν υπολογίζει τις πολλαπλότητες των λύσεων. Επίσης, η πολυπλοκότητα στην πράξη του αλγορίθμου SIGN_AT (Αλγ. 17) είναι πολύ μεγάλη. Από την άλλη η απλότητά του το κάνει πολύ εύκολα υλοποιήσιμο και ιδιαίτερα ελκυστικό. Μια παραλλαγή του αλγορίθμου NAIVE_SOLVE, όπου ο έλεγχος για το αν ένα ζεύγος είναι λύση του συστήματος πραγματοποιείται με συνεχώς βελτιούμενες προσεγγίσεις των πραγματικών αλγεβρικών αριθμών, χρησιμοποιείται πολύ συχνά στην πράξη.

Algorithm 19: MRUR_SOLVE (F, G)

Input: $F, G \in \mathbb{Z}[X, Y]$ τέτοια ώστε να ικανοποιούν την υπόθεση της γενικής θέσης
Output: Οι πραγματικές λύσεις του συστήματος $F = G = 0$

$\mathbf{SR} \leftarrow \mathbf{SR}_y(F, G)$
/* Προβολή στον X άξονα */
$R_x \leftarrow \mathtt{res}_y(F, G)$
$P_x, M_x \leftarrow$ CONSTRUCT(R_x)
/* Προβολή στον Y άξονα */
$R_y \leftarrow \mathtt{res}_x(F, G)$
$P_y, M_y \leftarrow$ CONSTRUCT(R_y)
$I \leftarrow$ INTERMEDIATE_POINTS(P_y)
/* Παραγοντοποίηση του R_x σύμφωνα με τους πρωτεύοντες συντελεστές της ακολουθίας **SR** και υπολογισμός των ριζών του R_x που τους μηδενίζουν */
$K \leftarrow$ COMPUTE_K$(\mathbf{SR}, P_x)$
$Q \leftarrow \emptyset$
/* Ταίριασμα των λύσεων */
foreach $\alpha \in P_x$ **do**
  $\beta \leftarrow$ FIND(α, K, P_y, I)
  $Q \leftarrow$ ADD$(Q, \{\alpha, \beta\})$
RETURN Q

Ο αλγόριθμος modified RUR (MRUR_SOLVE)

Ο επόμενος αλγόριθμος που θα παρουσιάσουμε, ονομάζεται modified RUR ή MRUR_SOLVE και έχει καλύτερη (θεωρητική και πρακτική) πολυπλοκότητα από τον NAIVE_SOLVE.

Η είσοδος του αλγορίθμου είναι τα δύο πολυώνυμα του συστήματος (4.1). Ωστόσο, ο MRUR_SOLVE υποθέτει ότι τα πολυώνυμα ικανοποιούν την υπόθεση της γενικής θέσης (Ορ. 4.14). Η υπόθεση αυτή χρειάζεται γιατί ο αλγόριθμος χρησιμοποιεί το Θεωρ. 4.15. Η υπόθεση της γενικής θέσης είναι χωρίς βλάβη της γενικότητας καθώς μπορούμε να επιβάλλουμε στα πολυώνυμα του συστήματος ένα μετασχηματισμό της μορφής $(X, Y) \mapsto (X + aY, Y)$, όπου το a είναι είτε ένας τυχαίος αριθμός ή κάποιος αριθμός ντετερμινιστικά υπολογισμένος τέτοιος ώστε να ικανοποιείται η υπόθεση της γενικής θέσης [116, 235] πριν από την εκτέλεση του αλγορίθμου πραγματικής επίλυσης.

Τα αρκτικόλεξο RUR στην ονομασία του αλγορίθμου σημαίνει Rational Univariate Representation (ρητή αναπαράσταση σε μία μεταβλητή). Το Θεωρ.4.15 αναπαριστά τη μία συντεταγμένη ως ρητή πολυωνυμική αναπαράσταση ως προς την άλλη συντεταγμένη. Έτσι προέκυψε το RUR στην ονομασία.

Η τεχνική του RUR γενικεύεται σε συστήματα πολλών μεταβλητών. Πιο συγκεκριμένα, μπορούμε να υπολογίσουμε κάποιον πραγματικό αλγεβρικό αριθμό και να εκφράσουμε τις λύσεις

του συστήματος ως ρητές πολυωνυμικές συναρτήσεις ως προς αυτόν τον αριθμό. Επίσης, η ιδέα του RUR δεν είναι καινούργια, δείτε για παράδειγμα [14, 44, 46, 74, 223, 229], καθώς αποτελεί γενίκευση του υπολογισμού του πρωτεύοντος στοιχείου (primitive element) που παρουσιάστηκε από τον van der Waerden [258], ενώ οι πρώτες βάσεις τέθηκαν από τον Kronecker.

Ο αλγόριθμος που παρουσιάζουμε μοιάζει αρκετά με τον αλγόριθμο των González-Vega and El Kahoui [116], Gonzalez-Vega and Necula [117] που αφορά το στενά συνδεδεμένο πρόβλημα του υπολογισμού της τοπολογίας μιας επίπεδης πραγματικής αλγεβρικής καμπύλης. Βασικό βήμα σε αυτό τον αλγόριθμο, και αποφασιστικό για την πολυπλοκότητά του, είναι η επίλυση ενός πολυωνυμικού συστήματος σε δύο μεταβλητές. Ωστόσο, ο αλγόριθμος των González-Vega and El Kahoui [116], Gonzalez-Vega and Necula [117] σταματά όταν υπολογίζει μια ρητή πολυωνυμική αναπαράσταση των λύσεων του συστήματος (RUR), χρησιμοποιώντας το Θεωρ. 4.15. Αυτό δεν είναι (πάντοτε) ικανοποιητικό καθώς η αναπαράσταση των Y συντεταγμένων είναι έμμεση Αν για παράδεγμα χρειάζεται να κάνουμε πράξεις με αυτούς τους αριθμούς ή να τους συγκρίνουμε κ.ο.κ, τότε πρέπει να επεξεργαστούμε περαιτέρω την αναπαράσταση των λύσων του συστήματος. Φυσικά θα μπορούσαμε να υπολογίσουμε το ελάχιστο πολυώνυμο που εκφράζει τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις Y συντεταγμένες αλλά αυτός ο υπολογισμός είναι μεγάλης θεωρητικής αλλά και πρακτικής πολυπλοκότητας.

Επιλέγουμε μια διαφορετική προσέγγιση, έτσι ώστε η έξοδος του αλγορίθμου να είναι μια λίστα από ζεύγη πραγματικών αλγεβρικών αριθμών σε αναπαράσταση με διάστημα απομόνωσης και επειδή τροποποιούμε τον αλγόριθμο των González-Vega and El Kahoui [116], Gonzalez-Vega and Necula [117], γιαυτό ονομάζουμε τον αλγόριθμο modified RUR (τροποποιημένη ρητή αναπαράσταση σε μία μεταβλητή).

Επίσης η πιο σημαντική διαφορά του MRUR_SOLVE με τον αλγόριθμο των González-Vega and El Kahoui [116], Gonzalez-Vega and Necula [117] είναι επιλέγουν να απαραστήσουν τους πραγματικούς αλγεβρικούς αριθμούς με την κωδικοποίηση κατά Thom [58], ενώ εμείς επιλέγουμε την αναπαράσταση με διάστημα απομόνωσης. Η πολυπλοκότητα του αλγορίθμου τους είναι $\widetilde{\mathcal{O}}_B(N^{16})$, όπου $N = \max\{n, \sigma\}$. Ακόμα και η ανάλυση του αλγορίθμου των González-Vega and El Kahoui [116], Gonzalez-Vega and Necula [117] όταν οι αριθμοί αναπαρίστανται με διάστημα απομόνωσης, δεν έχει παρουσιαστεί μέχρι σήμερα. Ο αλγόριθμος που θα παρουσιάσουμε έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(N^{12})$.

Η ανάλυση του MRUR_SOLVE

Ο ψευδο-κώδικας του αλγορίθμου MRUR_SOLVE παρουσιάζεται στον Αλγ. 19. Θα εξετάσουμε βήμα προς βήμα την ανάλυση της πολυπλοκότητάς του.

Περιγραφικά, ο αλγόριθμος είναι ο εξής: Προβάλουμε το σύστημα στον X (Γραμμές 2 και 3) και στον Y άξονα (Γραμμές 4 και 5). Στη συνέχεια για κάθε X συντεταγμένη λύσης (Γραμμή 9) υπολογίσουμε την αντίστοιχη Y συντεταγμένη (Γραμμή 10) χρησιμοποιώντας το Θεωρ. 4.15.

Η είσοδος του αλγορίθμου είναι δύο πολυώνυμα $F, G \in \mathbb{Z}[X, Y]$, τέτοια ώστε να ικανοποιούν την υπόθεση της γενικής θέσης. Υποθέτουμε ότι $\deg(F) = \deg(G) = n$ και $\mathcal{L}(F) = \mathcal{L}(G) = \sigma$.

Καταρχάς υπολογίζουμε την ακολουθία $\mathbf{SR}(F, G)$ ως προς Y (Γραμμή 1 στον Αλγ. 19) με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^5\,\sigma)$ (Πορ. 4.11).

Η προβολή στο X άξονα (Γραμμές 2 και 3 στον Αλγ. 19)
Προκειμένου να υπολογίσουμε την προβολή του συστήματος (4.1) στον X άξονα πρέπει να απαλείψουμε από το σύστημα την μεταβλητή Y. Γιαυτό υπολογίζουμε την επιλύουσα, R_x, των F και G ως προς Y (Γραμμή 2 στον Αλγ. 19). Ο υπολογισμός του R_x (Γραμμή 2 στον Αλγ. 19) έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^4\,\sigma)$ (Θεωρ. 4.12). Εναλλακτικά, θα μπορούσαμε να υπολογίσουμε το R_x ως το πρώτο από το τέλος μη μηδενικό πολυώνυμο της ακολουθίας $\mathbf{SR}(F,G)$, αλλά η πολυπλοκότητα αυτού του βήματος δεν είναι σημαντική για τον αλγόριθμο.

Οι πραγματικές λύσεις του R_x είναι οι X συντεταγμένες των λύσεων του συστήματος. Παρατηρούμε ότι $R_x \in \mathbb{Z}[X]$, εφόσον τα F και G είναι σχετικά πρώτα, και ότι $\deg(R_x) = \mathcal{O}(n^2)$ και $\mathcal{L}(R_x) = \mathcal{O}(n\,\sigma)$. Στη συνέχεια υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του R_x, σε αναπαράσταση με διάστημα απομόνωσης (Γραμμή 3 στον Αλγ. 19) χρησιμοποιώντας τον αλγόριθμο CONSTRUCT (Αλγ. 14) με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^{10}\,\sigma^2)$ (Θεωρ. 3.41). Παρατηρούμε ότι αναπαράσταση των πραγματικών αλγεβρικών αριθμών που έχουμε υπολογίσει περιέχει το ελεύθερο τετραγώνων μέρος του R_x, το οποίο έχει δυαδικό μήκος $\mathcal{O}(n+n\,\sigma) = \mathcal{O}(n\,\sigma)$ (Θεωρ. 2.34) και ότι τα διαστήματα απομόνωσης έχουν άκρα ρητούς αριθμούς με δυαδικό μήκος $\mathcal{O}(n^3\,\sigma)$ (Σημ. 3.24). Έστω ότι οι πραγματικοί αλγεβρικοί αριθμοί που υπολογίσαμε είναι

$$\alpha_1 < \alpha_2 < \cdots < \alpha_{m-1} < \alpha_m \tag{4.2}$$

όπου $m \leq 2\,n^2$ είναι το πλήθος των διακριτών πραγματικών ριζών του R_x. Ο αλγόριθμος CONSTRUCT επιστρέφει ένα διάνυσμα, P_x, που περιέχει τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του R_x και ένα διάνυσμα, M_x, που περιέχει τις πολλαπλότητές τους.

Τέλος, αν α είναι κάποια πραγματική ρίζα του R_x, τότε η πολλαπλότητά του ως ρίζα του R_x είναι και η πολλαπλότητα του (α,β) ως λύση του συστήματος, όπου β η αντίστοιχη Y συντεταγμένη του. Το γεγονός αυτό απορρέει από την υπόθεση της γενικής θέσης.

Η προβολή στον Y άξονα (Γραμμές 4, 5 και 6 στον Αλγ. 19)
Προκειμένου να προβάλουμε το σύστημα στον Y άξονα πρέπει να απαλείψουμε από αυτό την μεταβλητή X. Η διαδικασία είναι ακριβώς η ίδια με την προβολή στον X άξονα, αλλά με αντεστραμμένους τους ρόλους των X και Y. Κατά συνέπεια ο υπολογισμός των πραγματικών αλγεβρικών αριθμών που αντιστοιχούν στις Y συντεταγμένες των λύσεων του συστήματος έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^{10}\,\sigma^2)$. Οι ρίζες του R_y περιέχονται στον διάνυσμα P_y και οι πολλαπλότητές τους στο διάνυσμα M_y.

Επιπρόσθετα εκτελούμε τον αλγόριθμο INTERMEDIATE_POINTS (Παρ. 4.1), Γραμμή 6 στον Αλγ. 19, προκειμένου να υπολογίσουμε ρητά σημεία ανάμεσα στις πραγματικές ρίζες του R_y. Η πολυπλοκότητα του INTERMEDIATE_POINTS είναι $\widetilde{\mathcal{O}}_B(n^5\sigma)$ (Παρ. 4.1) και επίσης το δυαδικό μήκος των ρητών αριθμών που υπολογίζει είναι $\mathcal{O}(n^3\,\sigma)$. Η χρησιμότητα των σημείων αυτών θα φανεί στη συνέχεια. Έστω ότι οι ρίζες του R_y και τα ενδιάμεσα σημεία q_j είναι

$$q_0 < \beta_1 < q_1 < \beta_2 < \cdots < \beta_{\ell-1} < q_{\ell-1} < \beta_\ell < q_\ell \tag{4.3}$$

όπου $\ell \leq m \leq 2\,n^2$ είναι το πλήθος των διαφορετικών πραγματικών ριζών του R_y. Εφόσον το σύστημα βρίσκεται σε γενική θέση, κάθε πραγματική ρίζα του R_x πρέπει να αντιστοιχεί σε ακριβώς μία πραγματική ρίζα του R_y. Γιαυτό το λόγο ισχύει $\ell \leq m \leq 2\,n^2$. Τα ενδιάμεσα σημεία περιέχονται στο διάνυσμα I.

Ο αλγόριθμος COMPUTE_K (Γραμμή 7 στον Αλγ. 19)
Προκειμένου να εφαρμόσουμε το Θεωρ. 4.15 θα πρέπει για κάθε πραγματική ρίζα του R_x να υπολογίσουμε εκείνο το δείκτη k για τον οποίο ικανοποιούνται οι υποθέσεις του θεωρήματος. Αυτό ακριβώς κάνει ο αλγόριθμος COMPUTE_K. Πιο συγκεκριμένα, για κάποιο πραγματικό αλγεβρικό αριθμό α που είναι ρίζα του R_x, υπολογίζει εκείνο τον δείκτη k για τον οποίο ισχύουν οι υποθέσεις του Θεωρ. 4.15 και αποθηκεύει το αποτέλεσμα στο διάνυσμα K. Η υπόθεση της γενικής θέσης μας εξασφαλίζει ότι θα υπάρχει πάντοτε ένας και μοναδικός δείκτης k για κάθε α.

Προκειμένου ο αλγόριθμος COMPUTE_K να μας επιστρέψει τον κατάλληλο δείκτη k για κάθε πραγματική ρίζα του R_x που περιέχεται στο διάνυσμα P_x, ορίζουμε αναδρομικά μια οικογένεια πολυωνύμων $\Gamma_j(x)$:

$$\begin{aligned}
\Phi_0(X) &= \frac{\mathbf{sr}_0(X)}{\gcd(\mathbf{sr}_0(X), \mathbf{sr}_0'(X))} \\
\Phi_1(X) &= \gcd(\Phi_0(X), \mathbf{sr}_1(X)) \qquad & \Gamma_1 &= \frac{\Phi_0(X)}{\Phi_1(X)} \\
\Phi_2(X) &= \gcd(\Phi_1(X), \mathbf{sr}_2(X)) \qquad & \Gamma_2 &= \frac{\Phi_1(X)}{\Phi_2(X)} \\
&\vdots \\
\Phi_{n-1}(X) &= \gcd(\Phi_{n-2}(X), \mathbf{sr}_{n-1}(X)) \quad & \Gamma_{n-1} &= \frac{\Phi_{n-2}(X)}{\Phi_{n-1}(X)}
\end{aligned}$$

Υπενθυμίζουμε ότι $\mathbf{sr}_i = \mathbf{psc}_i \in \mathbb{Z}[X]$ είναι ο μεγιστοβάθμιος όρος του πολυωνύμου $\mathbf{SR}_j \in (\mathbb{Z}[X])[Y]$ ή διαφορετικά, ο πρωτεύων συντελεστής του του πολυωνύμου $\mathbf{SR}_j$ (Ορ. 2.19). Το $\Phi_0(x)$ είναι το ελεύθερο τετραγώνων μέρος του $R_x = \mathbf{sr}_0 = \mathbf{psc}_0 \in \mathbb{Z}[X]$, το οποίο έχει ήδη υπολογίσει ο αλγόριθμος CONSTRUCT(R_x) (Γραμμή 3 στον Αλγ. 19).

Έστω α κάποιος από τους πραγματικούς αλγεβρικούς αριθμούς που περιέχει το διάνυσμα P_x, ή διαφορικά κάποια από τις πραγματικές ρίζες του R_x ή ισοδύναμα του Φ_0. Εκ κατασκευής ισχύει $\Phi_0(X) = \prod_j \Gamma_j(X)$ και $\gcd(\Gamma_j, \Gamma_i) = 1$ αν $j \neq i$. Το α είναι ρίζα του Φ_0 και άρα ρίζα το πολύ ενός Γ_j, για κάποιο δείκτη j. Για εκείνο τον δείκτη j που ισχύει $\Gamma_j(\alpha) = 0$, ισχύει επίσης $\mathbf{sr}_0(\alpha) = \mathbf{sr}_1(\alpha) = 0, \ldots, \mathbf{sr}_j(\alpha) = 0$ και $\mathbf{sr}_{j+1}(\alpha) \neq 0$. Συνεπώς ο ζητούμενος δείκτης k για το α είναι $k = j + 1$. Ωστόσο το α είναι σε αναπαράσταση με διάστημα απομόνωσης, κατά συνέπεια εκείνο το Γ_j το οποίο το έχει ως πραγματική ρίζα θα πρέπει στα άκρα του διαστήματος απομόνωσης να αλλάζει πρόσημο, σύμφωνα με το Θεώρημα του Bolzano.

Συνοψίζοντας, τα βήματα του αλγορίθμου COMPUTE_K είναι τα εξής: Υπολογίζει την παραγοντοποίηση $\Phi_0 = \prod_j \Gamma_j$ του χωρίς τετράγωνα μέρους του R_x. Στη συνέχεια για κάθε πραγματική ρίζα του R_x υπολογίζει εκείνο το Γ_j το οποίο αλλάζει πρόσημο στα άκρα του διαστήματος απομόνωσης του α. Ο δείκτης k που αντιστοιχεί στο α είναι ο $k = j + 1$.

Ας μελετήσουμε τώρα την πολυπλοκότητα του αλγορίθμου. Εφόσον το Φ_0 είναι το χωρίς τετράγωνα μέρος του R_x ισχύει $\deg(\Phi_0) = \mathcal{O}(n^2)$ και $\mathcal{L}(\Phi_0) = \mathcal{O}(n + n\sigma) = \mathcal{O}(n\sigma)$ (Θεωρ. 2.34). Τα Γ_j είναι διαιρέτες του Φ_0, οπότε $\sum_j \deg(\Gamma_j) = \mathcal{O}(n^2)$ και από το φράγμα του Mignotte [187, 190] $\mathcal{L}(\Gamma_j) = \mathcal{O}(n^3\sigma)$. Για τον υπολογισμό της παραγοντοποίησης $\Phi_0(X) = \prod_j \Gamma_j(X)$ χρειαζόμαστε $\mathcal{O}(n)$ υπολογισμούς μέγιστων κοινών διαιρετών με πολυώνυμα βαθμού $\mathcal{O}(n^2)$ και

δυαδικού μήκους $\mathcal{O}(n^3\sigma)$. Ο υπολογισμός του ΜΚΔ κοστίζει $\widetilde{\mathcal{O}}_B(n^7\,\sigma)$ (Θεωρ. 2.31) και άρα το συνολικό κόστος είναι $\widetilde{\mathcal{O}}_B(n^8\,\sigma)$.

Προκειμένου να αντιστοιχήσουμε κάθε α σε κάποιο Γ_j πρέπει να υπολογίσουμε το πρόσημο της αποτίμησης κάθε Γ_j πάνω στα άκρα του διαστήματος απομόνωσης. Το πλήθος των α είναι το πολύ $\mathcal{O}(n^2)$ συνεπώς τόσο είναι και το πλήθος των άκρων των διαστημάτων απομόνωσης. Επιπρόσθετα το άκρα έχουν δυαδικό μήκος $\mathcal{O}(n^3\,\sigma)$. Αν $\deg(\Gamma_j) = \delta_j$, τότε μπορούμε να αποτιμήσουμε το Γ_j ταυτόχρονα πάνω σε όλα τα άκρα (των διαστημάτων απομόνωσης) με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(\delta_j\,n^5\,\sigma)$ (Παρ. 2.2). Εφόσον $\sum \delta_j = \mathcal{O}(n^2)$ όλες οι αποτιμήσεις επιτυγχάνονται με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^7\,\sigma)$.

Συνεπώς η συνολική πολυπλοκότητα του αλγορίθμου COMPUTE_K είναι $\widetilde{\mathcal{O}}_B(n^8\,\sigma)$.

Υπολογισμός των λύσεων και ο αλγόριθμος FIND (Γραμμές 9–11 στον Αλγ. 19)
Έχοντας υπολογίσει τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις X και στις Y συντεταγμένες των λύσεων του συστήματος (4.1), αυτό που απομένει είναι να ταιριάξουμε κατάλληλα. Αυτός ακριβώς είναι ο σκοπός του αλγορίθμου FIND. Δέχεται ως είσοδο κάποια πραγματική ρίζα του R_x, η οποία είναι η X συντεταγμένη κάποιας πραγματικής λύσης του συστήματος (4.1) και υπολογίζει την αντίστοιχη Y συντεταγμένη την οποία συμβολίζουμε με β.

Θα περιγράψουμε αναλυτικά τα βήματα του αλγορίθμου FIND και την ανάλυση της πολυπλοκότητάς του.

Για κάποια ρίζα α του R_x έχουμε ήδη υπολογίσει τον δείκτη k για τον οποίο ικανοποιούνται οι υποθέσεις του Θεωρ. 4.15. Συνεπώς μπορούμε να υπολογίσουμε την αντίστοιχη Y συντεταγμένη ως ρητή πολυωνυμική παράσταση ως προς α. Αυτή είναι

$$A(\alpha) = -\frac{1}{k}\frac{\mathbf{sr}_{k,k-1}(\alpha)}{\mathbf{sr}_k(\alpha)} = \frac{A_1(\alpha)}{A_2(\alpha)}$$

Η υπόθεση της γενικής θέσης μας εξασφαλίζει ότι υπάρχει ένα μοναδικό β_j, που περιέχεται στο διάνυσμα P_y, για το οποίο ισχύει ότι $\beta_j = A(\alpha)$, όπου $1 \le j \le \ell$. Προκειμένου να υπολογίσουμε τον κατάλληλο δείκτη j θα χρησιμοποιήσουμε τα ενδιάμεσα σημεία, τα οποία περιέχονται στο διάνυσμα I. Δείτε επίσης την Εξ. (4.3).

Για τον μοναδικό δείκτη j για τον οποίο ισχύει $\beta_j = A(\alpha)$ θα ισχύει

$$q_j < A(\alpha) = \frac{A_1(\alpha)}{A_2(\alpha)} < q_{j+1}$$

συνεπώς ο ζητούμενος δείκτης j είναι η θέση του αριθμού $A(\alpha)$ ανάμεσα στους διατεταγμένους αριθμούς $q_0 < \cdots < q_\ell$. Αυτός ο υπολογισμός επιτυγχάνεται, χρησιμοποιώντας δυαδική αναζήτηση, με το πολύ $\mathcal{O}(\lg \ell) = \mathcal{O}(\lg n)$ συγκρίσεις του αριθμού $A(\alpha)$ με τους ρητούς αριθμού q_j. Το τελευταίο όμως είναι ισοδύναμο με τον υπολογισμό του προσήμου της αποτίμησης του πολυωνύμου $B_j(X) = A_1(X) - q_j\,A_2(X)$ πάνω στον αλγεβρικό αριθμό α. Δηλαδή αρκεί να εκτελέσουμε τον αλγόριθμο SIGN_AT(B_j, α) (Αλγ. 15), το πολύ $\mathcal{O}(\lg n)$ φορές.

Όσον αφορά την πολυπλοκότητα του SIGN_AT(B_j, α), υπενθυμίζουμε ότι το α ορίζεται από ένα πολυώνυμο με βαθμό $\mathcal{O}(n^2)$, δυαδικό μήκος $\mathcal{O}(n\,\sigma)$ και ότι το δυαδικό μήκος των άκρων του διαστήματος απομόνωσης είναι $\mathcal{O}(n^3\,\sigma)$. Επίσης $\mathcal{L}(q_j) = \mathcal{O}(n^3\sigma)$ και $\deg(A_1) = \deg(\mathbf{sr}_{k,k-1}) =$

$\mathcal{O}(n^2)$, $\deg(A_2) = \deg(\mathrm{sr}_k) = \mathcal{O}(n^2)$, $\mathcal{L}(A_1) = \mathcal{O}(n\sigma)$, $\mathcal{L}(A_2) = \mathcal{O}(n\sigma)$. Άρα $\deg(P_j) = \mathcal{O}(n^2)$ και $\mathcal{L}(P_j) = \mathcal{O}(n^3\sigma)$.

Συμπεραίνουμε ότι ο αλγόριθμος SIGN_AT(P_j, α) και ο FIND έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^7\sigma)$.

Όσον αφορά την συνολική πολυπλοκότητα του βρόγχου (Γραμμές 9-11) παρατηρούμε ότι το πλήθος των α είναι το πολύ $\mathcal{O}(n^2)$. Συνεπώς η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(n^9\sigma)$.

Συνολική πολυπλοκότητα του αλγορίθμου

Συνοψίζουμε τις πολυπλοκότητες των διαφόρων βημάτων του αλγορίθμου.

Οι προβολές στον X και Y άξονα επιτυγχάνονται με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^{10}\sigma^2)$. Η παραγοντοποίηση, του χωρίς τετράγωνα μέρους του R_x και ο υπολογισμός των δεικτών k πραγματοποιείται χρησιμοποιώντας το Θεωρ. 4.15 και έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^7\sigma)$. Ο βρόγχος (Γραμμή 9 στον Αλγ. 19) έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^9\sigma)$, καθώς εκτελείται το πολύ $\mathcal{O}(n^2)$ φορές και κάθε βήμα έχει πολυπλοκότητα το πολύ $\widetilde{\mathcal{O}}_B(n^7\sigma)$.

Κατά συνέπεια μπορούμε να διατυπώσουμε το παρακάτω θεώρημα:

Θεώρημα 4.18 (MRUR_SOLVE**)**

Έστω $F, G \in \mathbb{Z}[X, Y]$ τέτοια ώστε να ικανοποιούν την υπόθεση της γενικής θέσης, να είναι σχετικά πρώτα, ο συνολικός βαθμός τους να φράσσεται από n και μέγιστο δυαδικό μήκος τους από σ. Η πραγματική επίλυση του συστήματος $F = G = 0$ με τον αλγόριθμο MRUR_SOLVE *έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(n^{10}\sigma^2)$.*

Ταυτόχρονες ανισώσεις με δύο μεταβλητές

Έστω $P, Q, A_1, \ldots, A_{\ell_1}, B_1, \ldots, B_{\ell_2}, C_1, \ldots, C_{\ell_3} \in \mathbb{Z}[X, Y]$, τα οποία έχουν συνολικό βαθμό που φράσσεται από n και δυαδικό μήκος που φράσσεται από σ. Θέλουμε να υπολογίσουμε το πλήθος αλλά και τις πραγματικές ρίζες, (α, β), του συστήματος $P(X, Y) = Q(X, Y) = 0$ για τις οποίες ισχύουν $A_i(\alpha, \beta) > 0$, $B_j(\alpha, \beta) < 0$ και $C_k(\alpha, \beta) = 0$ και $1 \le i \le \ell_1, 1 \le j \le \ell_2, 1 \le k \le \ell_3$. Θεωρούμε $\ell = \ell_1 + \ell_2 + \ell_3$.

Πόρισμα 4.19. *Υπάρχει αλγόριθμος ο οποίος επιλύει το πρόβλημα των ταυτόχρονων ανισώσεων με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(\max\{\ell\, n^{12}\sigma,\, n^{14}\sigma\}) = \widetilde{\mathcal{O}}_B(n^{12}\sigma\, \max\{\ell, n^2\})$.*

Απόδειξη: Αρχικά υπολογίζουμε την αναπαράσταση διαστήματος απομόνωσης όλων των πραγματικών αλγεβρικών αριθμών που αποτελούν λύση του συστήματος $P = Q = 0$ σε $\widetilde{\mathcal{O}}_B(n^{14}\sigma)$ (Θεωρ. 4.17). Υπάρχουν το πολύ n^2 πραγματικές ρίζες του συστήματος. Για κάθε λύση (α, β) και για κάθε πολυώνυμο A_i, B_j, C_k υπολογίζουμε τα πρόσημα $\mathrm{sign}(A_i(\alpha, \beta))$, $\mathrm{sign}(B_i(\alpha, \beta))$ και $\mathrm{sign}(C_i(\alpha, \beta))$.

Ο υπολογισμός των προσήμων πραγματοποιείται σε $\widetilde{\mathcal{O}}_B(n^{10}\sigma)$ (Θεωρ. 4.16) και στην χειρότερη περίπτωση πραγματοποιούμε n^2 τέτοιους υπολογισμούς. Συνεπώς το συνολικό κόστος είναι $\widetilde{\mathcal{O}}_B(\max\{\ell\, n^{12}\sigma,\, n^{14}\sigma\})$. ΟΕΔ

4.3 Σύνοψη – Μελλοντικές επεκτάσεις

Στο παρόν κεφάλαιο παρουσιάσαμε αλγορίθμους για υπολογισμούς με έναν και δύο πραγματικούς αλγεβρικούς αριθμούς, για τον υπολογισμό πολυωνυμικών ακολουθιών υπολοίπων για πολυώνυμα πολλών μεταβλητών και δύο αλγορίθμους για την πραγματική επίλυση πολυωνυμικών συστημάτων με δύο μεταβλητές.

Η άμεση επέκταση των αλγορίθμων που παρουσιάζουμε είναι οι αλγόριθμοι για τις 4 βασικές πράξεις μεταξύ δύο πραγματικών αλγεβρικών αριθμών. Το πολυώνυμο που ορίζει ένα πραγματικό αλγεβρικό αριθμό που είναι το άθροισμα, η διαφορά, το γινόμενο ή το κλάσμα δύο άλλων, μπορεί να υπολογιστεί με την βοήθεια της επιλύουσας. Ποιά είναι η πολυπλοκότητα των τεσσάρων βασικών πράξεων;

Όσον αφορά την επίλυση πολυωνυμικών συστημάτων, θα πρέπει πρέπει να μελετηθούν οι τεχνικές λεπτομέρειες της τυχαίας μετατόπισης που απαιτείται για να εφαρμοστεί ο αλγόριθμος MRUR_SOLVE και να επεκταθεί ο αλγόριθμος σε πολυωνυμικά συστήματα τριών μεταβλητών.

Τέλος, θεωρούμε εξαιρετικά ενδιαφέρον να μελετηθεί η πολυπλοκότητα όλων των αλγορίθμων που παρουσιάσαμε στον παρόν κεφάλαιο, όταν η αναπαράσταση των πραγματικών αλγεβρικών αριθμών είναι με κωδικοποίηση Thom [58] και χρησιμοποιηθούν ως βάση οι αλγόριθμοι του Canny [44].

ΚΕΦΑΛΑΙΟ 5

Αλγεβρικοί αριθμοί μικρού βαθμού

> Οι τέλειοι αριθμοί, όπως και οι τέλειοι άνθρωποι, είναι πολύ σπάνιοι.
>
> René Descartes

Περίληψη

Παρουσιάζουμε (βέλτιστους) αλγορίθμους για την απομόνωση και τον υπολογισμό των πολλαπλοτήτων των πραγματικών ριζών πολυωνύμων και την κατασκευή, σύγκριση και υπολογισμό προσήμων πραγματικών αλγεβρικών αριθμών όταν ο βαθμός είναι ≤ 4. Επίσης επιλύουμε πολυωνυμικά συστημάτα δύο μεταβλητών συνολικού βαθμού ≤ 2. Η πολυπλοκότητα όλων των αλγορίθμων είναι $\mathcal{O}(1)$ ή $\tilde{\mathcal{O}}_B(\tau)$.

Το σύνολο των αποτελεσμάτων του παρόντος κεφαλαίου είναι πρωτότυπο και μέρη του έχουν παρουσιαστεί στις εργασίες [88, 92, 93, 206].

Πραγματικοί αλγεβρικοί αριθμοί μικρού βαθμού παρουσιάζονται στη σχεδίαση με υπολογιστή, στη γεωμετρική μοντελοποίηση, στη μη γραμμική υπολογιστική γεωμετρία. Η ανάπτυξη αποδοτικών θεωρητικά και πρακτικά αλγορίθμων για υπολογισμούς με αλγεβρικούς αριθμούς μικρού βαθμού είναι εξέχουσας σημασίας καθώς τέτοιοι υπολογισμοί εμπλέκονται στα βασικά βήματα υπολογισμού της διάταξης επίπεδων αλγεβρικών καμπυλών, στα Voronoi διαγράμματα κυρτών αντικειμένων [79, 82, 98, 99, 130, 149, 171] και στις κινητικές δομές δεδομένων [123]. Είναι επίσης πολύ σημαντικοί σε βιβλιοθήκες λογισμικού όπως η CORE [146], η EXACUS [18], η ESOLID [152] και ο επερχόμενος καμπύλος πυρήνας της CGAL [96].

Οι πολυωνυμικές εξισώσεις βαθμού ≤ 4 μπορούν να λυθούν με ριζικά, η με άλλα λόγια επιδέχονται αναλυτικής λύσης. Για αυτή την προσέγγιση ο αναγνώστης μπορεί να ανατρέξει για παράδειγμα στον van der Waerden [258]. Οι Kaplan and White [144] παρουσιάζουν μια ενοποιημένη θεωρία επίλυσης των πολυωνύμων βαθμού ≤ 4, η οποία βασίζεται στους κυκλικούς

πίνακες. Ωστόσο, θέλουμε να αποφύγουμε την αναλυτική προσέγγιση για πολλούς λόγους. Καταρχάς, ο υπολογισμός των ριζικών είναι πολύ ακριβός υπολογιστικά και δεν μπορεί να γίνει μόνο με τη χρήση ρητών αριθμών. Ακόμα κι αν χρησιμοποιήσουμε αριθμούς κινητής υποδιαστολής οι τύποι των ριζικών είναι πολύ ασταθείς αριθμητικά, ιδιαίτερα στην περίπτωση πολλαπλών ριζών. Δεύτερον στην περίπτωση του τρίτου και του τετάρτου βαθμού, όταν το πολυώνυμο έχει πραγματικές ρίζες τότε απαιτούνται (πάντοτε) πράξεις με μιγαδικούς αριθμούς προκειμένου να τις υπολογίσουμε. Τέλος, ακόμα και αν χρειαζόμαστε μόνο κάποια (κάποιες) από τις ρίζες του πολυωνύμου δεν μπορούμε να συνάγουμε τη διάταξη από τους τύπους με τα ριζικά και πρέπει να υπολογίσουμε όλες τις ρίζες.

Προκειμένου να αντιμετωπίσουμε όλα τα προηγούμενα προβλήματα, χρειαζόμαστε αλγορίθμους που να είναι συμβολικοί, που να εμπλέκουν, αν είναι δυνατόν, μόνο τις βασικές πράξεις και να υπολογίζουν και τις πολλαπλότητες των ριζών. Για να αποφύγουμε προβλήματα αριθμητικής αστάθειας και υπολογισμούς με αριθμούς κινητής υποδιαστολής, απορρίπτουμε την αναλυτική επίλυση και αναπαριστούμε τις (πραγματικές) ρίζες χρησιμοποιώντας την αναπαράσταση με διάστημα απομόνωσης (Ορ. 4.1). Η άμεση προσέγγιση θα ήταν να χρησιμοποιήσουμε τους γενικούς αλγορίθμους που παρουσιάζονται στο Κεφ. 4. Σε αυτή την περίπτωση η δυαδική πολυπλοκότητα της απομόνωσης των πραγματικών ριζών, θα ήταν $\tilde{\mathcal{O}}_B(\tau^2)$ και η αριθμητική $\mathcal{O}(\tau)$, καθώς ο αριθμός των βημάτων των αλγορίθμων εξαρτάται από το δυαδικό μήκος των συντελεστών. Στόχος μας είναι να παρουσιάσουμε αλγορίθμους με πολυπλοκότητα $\mathcal{O}(1)$ ή $\tilde{\mathcal{O}}_B(\tau)$. Όπως απέδειξε και ο Lazard [170], στην εργασία του για τις αναγκαίες συνθήκες στους συντελεστές ενός τεταρτοβάθμιου πολυωνύμου προκειμένου αυτό να είναι πάντοτε θετικό, οι γενικού σκοπού αλγόριθμοι δεν επάγουν πάντοτε βέλτιστες λύσεις ή αλγορίθμους για συγκεκριμένα (και πιο περιορισμένα) προβλήματα.

Προκειμένου να υπολογίσουμε συμβολικά το πλήθος των πραγματικών ριζών και τις πολλαπλότητές τους, μιας πολυωνυμικής εξίσωσης βαθμού ≤ 4 θεωρούμε τους συντελεστές του πολυωνύμου ως παραμέτρους και επεκτείνουμε το σύστημα διακρινουσών (discrimination system), $\mathcal{DS}$, το οποίο εισήγαγε ο Yang [273], δείτε επίσης [14, 88, 92, 93, 170, 179, 267, 270], στο σύστημα διακρινουσών και απομόνωσης (isolation and discrimination system), το οποίο συμβολίζουμε ως $\mathcal{IDS}$. Το $\mathcal{IDS}$ είναι ένα σύνολο από πολυωνυμικές εκφράσεις και ανισότητες στους συντελεστές του πολυωνύμου, οι οποίες αρκούν για να περιγράψουν το πλήθος, τις πολλαπλότητες και την αναπαράσταση με διάστημα απομόνωσης των πραγματικών ριζών. Για παράδειγμα, στο γνωστό σε όλους τριώνυμο η διακρίνουσά του αρκεί για να χαρακτηρίσει (και να απομονώσει) το πλήθος των πραγματικών ριζών. Υπενθυμίζουμε ότι ο μηδενισμός της διακρίνουσας ενός πολυωνύμου είναι η ικανή και αναγκαία συνθήκη έτσι ώστε το πολυώνυμο να έχει (μιγαδικές) ρίζες με πολλαπλότητες, δείτε Εν. 2.2. Για πολυώνυμα μεγαλύτερου βαθμού χρειάζονται επιπλέον ποσότητες, όχι για να βεβαιώσουν την ύπαρξη ριζών με πολλαπλότητα αλλά για να υπολογίσουν το πλήθος και την πολλαπλότητα των ριζών· αυτές είναι το σύστημα διακρινουσών.

Η προσέγγισή που θα ακολουθήσουμε υπολογίζει το σύστημα διακρινουσών χρησιμοποιώντας τις προσημασμένες ακολουθίες υπο-επιλυουσών. Τις διάφορες ποσότητες που εμφανίζονται, τις εκφράζουμε ως συνάρτηση των αναλλοίωτων (invariant) του πολυωνύμου και ως στοιχεία του πίνακα Bézout του πολυωνύμου και της παραγώγου του (Εν. 2.2), προκειμένου να ελαχιστοποιήσουμε το υπολογιστικό κόστος. Για την αναπαράσταση με διαστήματα απομόνωσης υπολογίζουμε ρητούς αριθμούς (*σημεία διαχωρισμού*) που διαχωρίζουν τις πραγματικές ρίζες, τους οποίους εκ-

φράζουμε ως ρητές πολυωνυμικές συναρτήσεις των συντελεστών του πολυωνύμου. Τα σημεία διαχωρισμού είναι πολύ σημαντικά καθώς μπορούν να αποτελέσουν αρχικές προσεγγίσεις σε επαναληπτικές μεθόδους προσέγγισης των ριζών και αποτελούν πρόβλημα αυτόνομου ενδιαφέροντος.

Η κατασκευή αλγεβρικών αριθμών βαθμού ≤ 4 σε σταθερό χρόνο μας επιτρέπει να παρουσιάσουμε αλγορίθμους, επίσης σταθερού χρόνου, για την σύγκριση, για τον υπολογισμό του προσήμου αποτίμησης και για την επίλυση πολυωνυμικών συστημάτων δύο μεταβλητών συνολικού βαθμού ≤ 2. Οι παρουσιαζόμενοι αλγόριθμοι είναι βέλτιστοι ή σχεδόν βέλτιστοι ως προς τον αλγεβρικό βαθμό (algebraic degree) των εξεταζόμενων ποσοτήτων, όπου αλγεβρικός βαθμός είναι ο συνολικός βαθμός των εξεταζόμενων (πολυωνυμικών) ποσοτήτων ως προς τους συντελεστές του πολυωνύμου.

Το γεγονός ότι μπορούμε να απομονώσουμε τις πραγματικές ρίζες πολυωνύμων βαθμού μικρότερου ή ίσου του 4 έχοντας υπολογίζει συμβολικά όλες τις απαιτούμενες ποσότητες και το $\mathcal{IDS}$, μας επιτρέπει να προτείνουμε ειδικούς αλγορίθμους για την απαλοιφή ενός ποσοδείκτη $\exists x$ από κάποια φόρμουλα $\exists x(P)$, όπου η P αποτελείται από διαζεύξεις και συζεύξεις πολυωνυμικών εξισώσεων βαθμού ≤ 4 και ανισώσεων οποιουδήποτε βαθμού, βασιζόμενοι στην προσέγγιση της εικονικής αντικατάστασης (virtual substitution) [134, 170, 179, 267, 268, 269, 270]

Σε ό,τι θα ακολουθήσει θα θεωρήσουμε ότι η είσοδος είναι οι συντελεστές ενός πολυωνύμου f, όπου $\deg(f) \leq 4$, και όλοι οι αλγόριθμοι που θα παρουσιάσουμε εξετάζουν το πρόσημο κάποιων πολυωνυμικών ποσοτήτων στους συντελεστές. Από την άποψη της πολυπλοκότητας σκοπός μας είναι να ελαχιστοποιήσουμε όσο το δυνατόν το συνολικό βαθμό των εξεταζόμενων ποσοτήτων και ή το δυνατόν τις απαιτούμενες πράξεις.

Ιστορική αναδρομή

Η αλγεβρική λύση μιας εξίσωσης βαθμού ≤ 4 συνίσταται στον υπολογισμό κάποιων τύπων για τις ρίζες, οι οποίοι περιέχουν πεπερασμένο αριθμό βασικών πράξεων και ριζικών.

Οι πρώτοι που ασχολήθηκαν με την εύρεση των ριζών της πολυωνυμικής εξίσωσης δευτέρου βαθμού ήταν οι Αιγύπτιοι, οι Βαβυλώνιοι και οι Κινέζοι μηχανικοί. Ίσως η πρώτη γνωστή λύση της εξίσωσης να είναι ένα Αιγυπτιακός πάπυρος από την εποχή του Μέσου Βασιλείου, περίπου 2160-1700 π.Χ. Επίσης, σε πινακίδια από πηλό τα οποία χρονολογούνται ανάμεσα στο 1800 π.Χ και 1600 π.Χ οι αρχαίοι Βαβυλώνιοι παρουσιάζουν πολυωνυμικές εξισώσεις δευτέρου βαθμού και μερικούς απλούς τρόπους επίλυσής τους. Ο Ινδός μαθηματικός Baudhayana, ο οποίος έγραψε το *Sulba Sutr* στην αρχαία Ινδία περίπου τον 8^o αιώνα π.Χ, χρησιμοποίησε πρώτος εξισώσεις της μορφής $ax^2 = c$ και $ax^2 + bx = c$ και παρουσίασε τρόπους επίλυσής τους.

Βαβυλώνιοι μαθηματικοί γύρω στο 400 π.Χ και Κινέζοι μαθηματικοί γύρω στο 200 π.Χ χρησιμοποίησαν μεθόδους συμπληρώματος του τετραγώνου προκειμένου να επιλύσουν πολυωνυμικές εξισώσεις δευτέρου βαθμού με θετικές ρίζες αλλά δεν παρουσίασαν ένα γενικό τύπο επίλυσης. Ο Ευκλείδης παρουσίασε μία γενική γεωμετρική μέθοδο γύρω στο 300 π.Χ και ο Διόφαντος στα *Αριθμητικά* υπολόγιζε τη μία λύση μιας δευτεροβάθμιας εξίσωσης. Στο βιβλίο *Bakshali Manuscript* το οποίο γράφτηκε στην Ινδία μεταξύ του 200 π.Χ και του 400 μ.Χ παρουσιάστηκε ένας γενικός αλγεβρικός τύπος για την επίλυση δευτέρου βαθμού εξισώσεων. Ο πρώτος μαθηματικός που υπολόγιζε αρνητικές λύσεις της εξίσωσης ήταν ο Brahmagupta (Ινδία, $7^{ος}$ αιώνας). Ο

Muhammad ibn Musa al-Kwarizmi (Περσία, $9^{ος}$ αιώνας) ανέπτυξε ένα σύνολο από τύπους οι οποίοι δίνουν τις θετικές ρίζες. Ο Abraham bar Hiyya Ha-Nasi, γνωστός επίσης και με το λατινικό του όνομα Savasorda, εισήγαγε στην Ευρώπη την πλήρη λύση της εξίσωσης με το βιβλίο του *Liber embadorum* τον $12^{ο}$ αιώνα.

Ο Shridhara (Ινδία, $9^{ος}$ αιώνας) ήταν από τους πρώτους μαθηματικούς που έδωσαν ένα γενικό κανόνα επίλυσης της πολυωνυμικής εξίσωσης δευτέρου βαθμού, αλλά τα γραπτά του δεν διεσώθηκαν. Επίσης ο Viéta ήταν ανάμεσα στους πρώτους που αντικατέστησαν τις γεωμετρικές μεθόδους με αλγεβρικές αν και είναι αμφίβολο αν είχε συλλάβει τον γενικό τύπο επίλυσης της εξίσωσης,

Οι προσπάθειες επίλυσης της κυβικής εξίσωσης ξεκινούν από τα τέλη του $15^{ου}$ αιώνα. Το 1494 ο Ιταλός μαθηματικός Luca Pacioli μελετούσε την εξίσωση και εξέφρασε την πεποίθηση ότι είναι αδύνατον να επιλυθεί. Αυτή η παρατήρηση λειτούργησε ως πρόκληση και αποτέλεσε το άγιο δισκοπότηρο για την Ιταλική μαθηματική κοινότητα του $16^{ου}$ αιώνα.

Ο πρώτος που αντιμετώπισε την πρόκληση ήταν ο Scipione dal Ferro (1465-1526), καθηγητής μαθηματικών στον Πανεπιστήμιο της Bologna. Περίπου το 1500 ο dal Ferro ανακάλυψε την λύση της συμπιεσμένης (depressed) κυβικής εξίσωσης, δηλαδή της κυβικής εξίσωσης χωρίς τον όρο δευτέρου βαθμού. Ένας απλός γραμμικός μετασχηματισμός φέρνει πάντα τη γενική εξίσωση τρίτου βαθμού σε αυτή τη μορφή. Ο del Ferro δεν δημοσίευσε τα αποτελέσματά του, πιθανώς γιατί είχε αμφιβολίες για την ορθότητά τους. Αν η λύση του ήταν λανθασμένη τότε θα έθετε σε σοβαρό κίνδυνο την πανεπιστημιακή του θέση. Ωστόσο, την κοινοποίησε στον ανιψιό και μαθητή του Antonio Maria Fior.

Ο Fior δεν ήταν καλός στο να κρατάει μυστικά και έτσι διάφορες φήμες κυκλοφορούσαν στην Bologna, οι οποίες συνέκλιναν στο ότι η κυβική εξίσωση είχε επιλυθεί. Ορμώμενος από τις φήμες ο Nicolo of Brescia, γνωστός ως Tartaglia (αυτός που τραυλίζει) έλυσε μια ειδική περίπτωση της κυβικής εξίσωσης, την $x^3 + mx^2 = n$ και δεν το κράτησε κρυφό! Ο Fior προκάλεσε τον Tartaglia σε ένα δημόσιο διαγωνισμό. Ο καθένας θα έδινε στον άλλο 30 προβλήματα και θα είχαν στη διάθεσή τους 40 ή 50 μέρες να τα λύσουν. Νικητής θα ήταν αυτός που έλυνε τα περισσότερα προβλήματα και υπήρχαν και μικρά βραβεία για κάθε πρόβλημα ξεχωριστά. Φυσικά ο Fior έθεσε ως ένα από τα προβλήματα την συμπιεσμένη κυβική εξίσωση. Ο Tartaglia έλυσε σε λιγότερο από μία μέρα όλα τα προβλήματα εκτός από την κυβική εξίσωση. Λίγο πριν εκπνεύσει η προθεσμία έλυσε και το τελευταίο πρόβλημα.

Τα νέα της νίκης του Tartaglia έφτασαν στον Gerolamo Cardano από το Μιλάνο, ο οποίος εντυπωσιάστηκε από τη λύση της εξίσωσης. Έγραψε δε πολλές φορές στον Tartaglia και τελικά τον έπεισε να τον επισκεφτεί το 1539. Στη συνάντησή τους κατάφερε να πείσει τον Tartaglia να του αποκαλύψει τη λύση της κυβικής εξίσωσης, ορκίστηκε όμως να μην αποκαλύψει πριν ο Tartaglia τη δημοσιεύσει. Το 1543 ο Cardano με τον μαθητή του Ludovico Ferrari κοιτάζοντας τα χαρτιά του del Ferro ανακάλυψε ότι η λύση του Tartaglia ήταν η ίδια με αυτή του del Ferro και θεώρησε ότι μπορούσε να σπάσει τον όρκο του. Τελικά, δημοσίευσε τη λύση του πολυωνύμου τρίτου (και τετάρτου) βαθμού στην εργασία του *Ars Magna* (Μεγάλη Τέχνη) το 1545, που είναι η πρώτη εργασία άλγεβρας στα λατινικά, δίνοντας τα εύσημα μόνο στον del Ferro και στον εαυτό του.

Μετά την αποκάλυψη από τον Tartaglia στον Cardano της λύσης της κυβικής εξίσωσης ο τελευταίος παρότρυνε τον μαθητή του Lodovico Ferrari να ασχοληθεί με την επίλυση της εξίσωσης

τετάρτου βαθμού. Ο Ferrari τα κατάφερε και έδωσε ίσως την πιο κομψή από όλες τις γνωστές λύσεις. Ωστόσο, ο Cardano έκλεψε τη λύση και τη δημοσίευσε στο *Ars Magna*, λέγοντας ότι Ferrari ανακάλυψε τη λύση μετά από αίτημά του ('[Ferrari] invented it at my request').

Αργότερα αποδείχτηκε από τον Niels Henrik Abel και τον Evariste Galois ότι η τετάρτου βάθμου εξίσωση είναι το σύνορο. Δηλαδή ότι δεν μπορούμε να εκφράσουμε τις ρίζες οποιονδήποτε πολυωνύμων βαθμού μεγαλύτερου από 4 με τύπους που περιέχουν πεπερασμένο αριθμό βασικών πράξεων και ριζικά.

Περισσότερα ιστορικά στοιχεία παρουσιάζονται στην ιστοσελίδα του BBC[1], στην ιστοσελίδα mathworld[2] του Eric W. Weisstein και στις εργασίες των Dunham [78] και Boyer [32]. Αυτές οι αναφορές αποτέλεσαν και τις πηγές της σύντομης ιστορικής ανασκόπησης που παρουσιάσαμε.

5.1 Πολυώνυμα απομόνωσης και πραγματικές ρίζες

Από το θεώρημα του Rolle μπορούμε εύκολα να συνάγουμε ότι ανάμεσα σε δύο πραγματικές ρίζες ενός πολυωνύμου παρεμβάλεται τουλάχιστον μία ρίζα της παραγώγου, δείτε για παράδειγμα [187, 190, 275]. Ωστόσο, μπορούμε να υπολογίσουμε και άλλα πολυώνυμα με αυτή την ιδιότητα. Η παρακάτω πρόταση, η οποία οφείλεται στους Sederberg and Chang [242], και η οποία γενικεύει ένα θεώρημα του de Gua [187, 190] μας παρέχει μια τέτοια δυνατότητα.

Πρόταση 5.1. *Έστω $f(X) \in \mathbb{R}[X]$, δύο συνεχόμενες πραγματικές ρίζες του γ_1, γ_2 και δύο άλλα (οποιαδήποτε) πολυώνυμα $B(X), C(X) \in \mathbb{R}[X]$. Θεωρούμε το πολυώνυμο*

$$A(X) := B(X)f'(X) + C(X)f(X) \tag{5.1}$$

όπου $A \in \mathbb{R}[X]$ και f' η παράγωγος του f. Τουλάχιστον ένα από τα $A(X)$ και $B(X)$ έχει τουλάχιστον μία πραγματική ρίζα στο κλειστό διάστημα $[\gamma_1, \gamma_2]$. Επιπρόσθετα είναι πάντοτε δυνατόν να έχουμε $\deg(A) + \deg(B) \leq \deg(f) - 1$.

Τα $A(X)$ και $B(X)$ ονομάζονται πολυώνυμα απομόνωσης (isolating polynomials).

Απόδειξη: Αν $A(\gamma_1) = 0$ ή $A(\gamma_2) = 0$ ή $B(\gamma_1) = 0$ ή $B(\gamma_2) = 0$ η πρόταση ισχύει. Ας υποθέσουμε ότι οι γ_1 και γ_2 δεν είναι ρίζες ούτε του $A(X)$ ούτε του $B(X)$.

Εφόσον $f(\gamma_1) = 0$, η (5.1) γίνεται

$$A(\gamma_1) = B(\gamma_1)f'(\gamma_1) \Rightarrow \operatorname{sign}(f'(\gamma_1)) = \operatorname{sign}(A(\gamma_1)B(\gamma_1)) \tag{5.2}$$

Εφόσον $f(\gamma_2) = 0$, η (5.1) γίνεται

$$A(\gamma_2) = B(\gamma_2)f'(\gamma_2) \Rightarrow \operatorname{sign}(f'(\gamma_2)) = \operatorname{sign}(A(\gamma_2)B(\gamma_2)) \tag{5.3}$$

Από το θεώρημα του Rolle ανάμεσα σε δύο πραγματικές ρίζες του f υπάρχει τουλάχιστον μία ρίζα του f' και από το θεώρημα του Bolzano έχουμε ότι $\operatorname{sign}(f'(\gamma_1))\operatorname{sign}(f'(\gamma_2)) < 0$ Συνεπώς, συνδυάζοντας τις (5.2) και (5.3) έχουμε ότι

$$\operatorname{sign}(A(\gamma_1)B(\gamma_1)) \cdot \operatorname{sign}(A(\gamma_2)B(\gamma_2)) < 0$$

[1] `http://www.bbc.co.uk/dna/h2g2/A2982567`
[2] `http://mathworld.wolfram.com/`

Από το θεώρημα του Bolzano η συνάρτηση $A(X)B(X)$ έχει τουλάχιστον μία πραγματική ρίζα στο (γ_1, γ_2) και η πρόταση αποδείχτηκε. ΟΕΔ

Η Πρότ. 5.1 αν και απλή είναι πολύ ισχυρή. Παρατηρήστε ότι στην (5.1) μπορούμε να θεωρήσουμε ότι τα $B(X)$ και $C(X)$ είναι οι συντελεστές B'ezout στην ακολουθία πολυωνύμων που παράγεται από τον Ευκλείδιο αλγόριθμο των f και f'. Βασιζόμενοι (και) σε αυτή την ιδιότητα οι Ben-Or et al. [16] απέδειξαν ότι αν ένα πολυώνυμο έχει μόνο πραγματικές ρίζες τότε αφενός οι πραγματικές ρίζες της ακολουθίας πηλίκων, του πολυωνύμου και της παραγώγου του, τις απομονώνουν και αφετέρου μία από αυτές τις χωρίζει σε δύο σχεδόν ισομεγέθη σύνολα.

Επίσης, όταν το πολυώνυμο έχει μόνο πραγματικές ρίζες τότε ισχύει το ακόλουθο θεώρημα το οποίο οφείλεται στον Netwon [275].

Θεώρημα 5.2

Αν το πολυώνυμο $f = a_n X^n + \binom{n}{1} a_{n-1} X^{n-1} + \cdots + \binom{n}{n-1} a_1 X + a_0$ *έχει* n *πραγματικές ρίζες τότε* $a_i^2 \geq a_{i-1} a_{i+1}$, $1 \leq i \leq n-1$.

5.2 Πραγματική επίλυση

Μπορούμε τώρα να εξετάσουμε τα πολυώνυμα βαθμού ≤ 4. Στόχος μας είναι να χαρακτηρίσουμε, με συμβολικό τρόπο, τις πραγματικές τους ρίζες (πλήθος και πολλαπλότητες), να τις απομονώσουμε και τελικά να υπολογίσουμε το σύστημα διακρινουσών και απομόνωσης.

Το δευτεροβάθμιο πολυώνυμο

Θεωρούμε το δευτεροβάθμιο πολυώνυμο (quadratic), ή τριώνυμο, $f \in \mathbb{Z}[X]$, με $a_2 > 0$

$$f(X) = a_2 X^2 + a_1 X + a_0 \tag{5.4}$$

Οι (μιγαδικές) λύσεις του (5.4) είναι

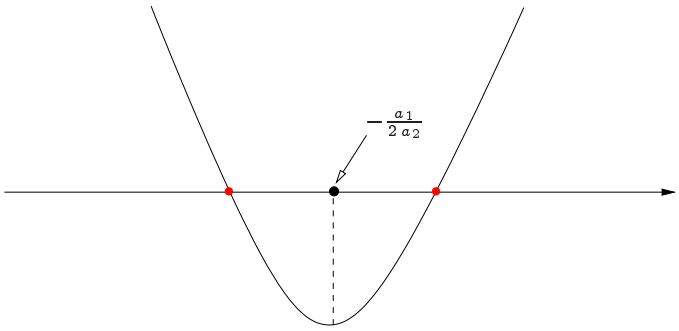
$$\frac{-a_1 \pm \sqrt{\Delta}}{2a_2}$$

όπου $\Delta = \mathsf{disc}(f) = a_1^2 - 4a_2 a_0$ είναι διακρίνουσα του f. Το πρόσημο της διακρίνουσας παρέχει όλες τις πληροφορίες που χρειαζόμαστε προκειμένου να χαρακτηρίσουμε και να απομονώσουμε τις πραγματικές ρίζες του f, όπως δείχνει και το ακόλουθο λήμμα:

Λήμμα 5.3. *Έστω* $f(X) = a_2 X^2 + a_1 X + a_0 \in \mathbb{R}[X]$. *Αν* $\Delta = 0$ *τότε το* f *έχει μία διπλή ρίζα, την* $-\frac{a_1}{2a_2}$. *Αν* $\Delta > 0$ *τότε ο αριθμός* $-\frac{a_1}{2a_2}$ *διαχωρίζει τις δύο πραγματικές ρίζες του* f.

Απόδειξη: Αν $\Delta = 0$ η απόδειξη είναι προφανής και βασίζεται στην τεχνική της συμπλήρωσης του τετραγώνου.

Αν $\Delta > 0$ τότε το f έχει δύο διαφορετικές πραγματικές ρίζες. Παρατηρούμε ότι η παράγωγος $f' = 2a_2 X + a_1$ έχει ρίζα το $-\frac{a_1}{2a_2}$, και σύμφωνα με το θεώρημα του Rolle είναι ανάμεσα στις ρίζες του f. Η περίπτωση αυτή παρουσιάζεται στο Σχ. 5.1. ΟΕΔ



Σχήμα 5.1: Απομόνωση των ριζών του δευτεροβάθμιου πολυωνύμου

Η τετμημένη του ακρότατου απομονώνει τις πραγματικές ρίζες ενός πολυωνύμου $f = a_2X^2 + a_1X + a_0$ για οποίο ισχύει $\Delta > 0$.

Συνεπώς μπορούμε να διατυπώσουμε την ακόλουθη πρόταση

Πρόταση 5.4. *Το $\mathcal{IDS}$ του δευτεροβάθμιου πολυωνύμου* (5.4) *είναι*

(1)	$\Delta < 0$	$\{\}$	
(2)	$\Delta = 0$	$\{2\}$	$\gamma_1 = -\frac{a_1}{2a_2}$
(3)	$\Delta > 0$	$\{1,1\}$	$\gamma_1 \cong [f, (-\infty, -\frac{a_1}{2a_2})]$ $\gamma_2 \cong [f, (-\frac{a_1}{2a_2}, +\infty)]$

Σημείωση 5.5 (Πως διαβάζουμε το $\mathcal{IDS}$). *Η πρώτη στήλη περιέχει την απαρίθμηση των περιπτώσεων. Η δεύτερη στήλη περιέχει τις πολυωνυμικές ανισότητες που ισχύουν. Η τρίτη στήλη περιέχει τις πολλαπλότητες και το πλήθος των πραγματικών ριζών και η τελευταία στήλη την αναπαράσταση με διάστημα απομόνωσης. Ο συμβολισμός $\{2\}$ σημαίνει ότι έχουμε μία διπλή ρίζα και ο $\{1,1\}$ ότι έχουμε δύο διαφορετικές πραγματικές ρίζες πολλαπλότητας 1.*

Για παράδειγμα αν ένα (δευτεροβάθμιο) πολυώνυμο, όπως στην (5.4)*, είναι τύπου* (2) *τότε ισχύει $\Delta = 0$, έχει μία διπλή ρίζα, η οποία είναι ο αριθμός $-\frac{a_1}{2a_2}$.*

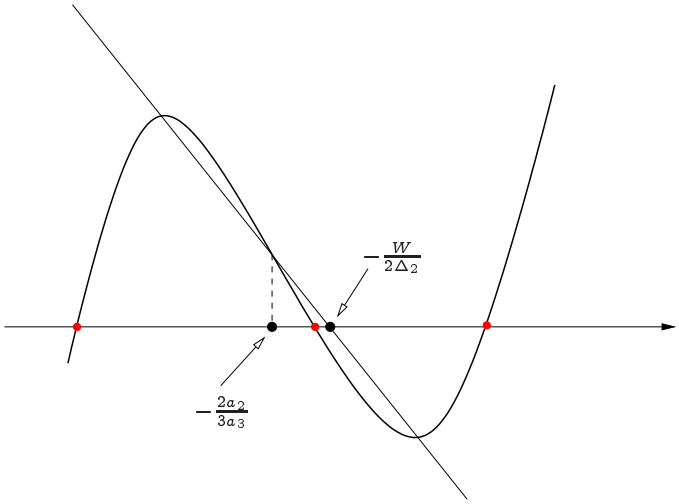
Το τριτοβάθμιο πολυώνυμο

Θεωρούμε το κυβικό πολυώνυμο (cubic) $f \in \mathbb{Z}[X]$, όπου $a_3 > 0$,

$$f = a_3\,X^3 + a_2\,X^2 + a_1\,X + a_0 \tag{5.5}$$

του οποίου οι μιγαδικές λύσεις είναι

$$\begin{aligned}
\gamma_1 &= -\frac{a_2}{3a_3} + (S+T) \\
\gamma_2 &= -\frac{a_2}{3a_3} - \frac{1}{2}(S+T) + \frac{1}{2}\,\mathrm{i}\sqrt{3}(S-T) \\
\gamma_3 &= -\frac{a_2}{3a_3} - \frac{1}{2}(S+T) - \frac{1}{2}\,\mathrm{i}\sqrt{3}(S-T)
\end{aligned} \tag{5.6}$$



Σχήμα 5.2: Απομόνωση των ριζών του τριτοβάθμιου πολυωνύμου

Η ευθεία η οποία ενώνει τα δύο ακρότατα ενός κυβικού πολυωνύμου $f = a_3X^3 + a_2X^2 + a_1X + a_0$ και για οποίο ισχύει $\Delta_1 > 0 \wedge P > 0$.

όπου

$$S = \sqrt[3]{R + \sqrt{R^2 + Q^3}}, \quad T = \sqrt[3]{R - \sqrt{R^2 + Q^3}}, \quad Q = \frac{\Delta_2}{a_3^2}, \quad R = -\frac{\Delta_1}{2a_3^3}$$

Χρειαζόμαστε να ορίσουμε τις ακόλουθες ποσότητες

$$\begin{array}{lcllcl} \Delta_2 & = & a_2^2 - 3\,a_3\,a_1 & \Delta_3 & = & a_1^2 - 3\,a_2\,a_0 \\ W & = & a_2\,a_1 - 9\,a_3\,a_0 & P & = & 2\,a_2\Delta_2 - 3\,c_3\,W \end{array} \tag{5.7}$$

οι οποίες είναι είτε αναλλοίωτες του κυβικού πολυωνύμου [62] είτε στοιχεία του πίνακα Bézout του f και του f'. Η διακρίνουσα του κυβικού πολυωνύμου είναι:

$$\Delta_1 = \mathsf{disc}(f) = W^2 - 4\,\Delta_2\,\Delta_3 \tag{5.8}$$

Από τις σχέσεις (5.6) είναι εμφανές ότι απαιτούνται πράξεις με μιγαδικούς αριθμούς προκειμένου να υπολογίζουμε με ριζικά τις (πραγματικές) ρίζες της (5.5).

Προκειμένου να υπολογίσουμε το σύστημα διακρινουσών του πολυωνύμου τρίτου βαθμού θεωρούμε την (προσημασμένη) ακολουθία υπο-επιλυουσών του f και του f', $\mathbf{SR}(f, f')$ (Εν. 2.3). Υπολογίζουμε την ακολουθία συμβολικά και είμαστε βέβαιοι ότι για οποιαδήποτε ανάθεση τιμών στις παραμέτρους, με τον περιορισμό $a_3 \neq 0$, η ακολουθία θα είναι νόμιμη. Η ακολουθία $\mathbf{SR}(f, f')$ είναι

$$\mathbf{SR}(f, f') = \begin{cases} \mathbf{SR}_3(X) & = & f(X) \\ \mathbf{SR}_2(X) & = & f^{'}(X) \\ \mathbf{SR}_1(X) & = & 2\Delta_2 X + W \\ \mathbf{SR}_0(X) & = & -3\Delta_1 \end{cases} \tag{5.9}$$

όπου οι συντελεστές των πολυωνύμων της ακολουθίας παρουσιάζονται με τη βοήθεια των ποσοτήτων των (5.7) και (5.8).

Αν θεωρήσουμε τη γραφική παράσταση ενός κυβικού πολυωνύμου f, με τρεις πραγματικές ρίζες, τότε ισχύει το παρακάτω (γεωμετρικό) λήμμα:

Λήμμα 5.6. *Έστω κυβικό πολυώνυμο f όπως στην* (5.5)*, με τρεις πραγματικές ρίζες. Το μέγιστο, το ελάχιστο και το σημείο καμπής της γραφικής παράστασης του f είναι συνευθειακά. Η ευθεία που ενώνει τα τρία αυτά σημεία ονομάζεται ευθεία απομόνωσης του κυβικού πολυωνύμου (isolating line).*

Απόδειξη: Οι τετμημένες των ακρότατων του f υπολογίζονται αν επιλύσουμε την εξίσωση $f'(X) = 0$. Συνεπώς τα ακρότατα του f είναι τα σημεία $\mathbf{p}_1 = (w_1, f(w_1))$ και $\mathbf{p}_2 = (w_2, f(w_2))$ όπου

$$w_{1,2} = \frac{-a_2 \pm \sqrt{\Delta_2}}{3\,a_3}$$

Θεωρούμε την ευθεία που διέρχεται από τα $\mathbf{p}_1$ και $\mathbf{p}_2$, η εξίσωση της οποίας είναι

$$Y = kX + l, \text{ όπου } k = -\frac{2\Delta_2}{a_3} \text{ και } l = -\frac{W}{a_3} \tag{5.10}$$

Η τετμημένη του σημείου καμπής της f προκύπτει από τη λύση της $f''(X) = 3a_3X + a_2 = 0$ και άρα το σημείο καμπής είναι το $\left(-\frac{2a_2}{3a_3}, f(-\frac{2a_2}{3a_3})\right)$. Με αντικατάσταση αποδεικνύουμε ότι η ευθεία απομόνωσης διέρχεται από το σημείο καμπής και η απόδειξη του λήμματος ολοκληρώνεται. ΟΕΔ

Στο Σχ. 5.2 παρουσιάζεται η ευθεία απομόνωσης ενός κυβικού πολυωνύμου με τρεις πραγματικές ρίζες. Μπορούμε τώρα να παρουσιάσουμε το συστήμα διακρινουσών και απομόνωσης.

Πρόταση 5.7. *Το $\mathcal{IDS}$ του κυβικού πολυωνύμου* (5.5) *είναι*

(1)	$\Delta_1 < 0 \wedge P = 0$	$\{1,1,1\}$	$\gamma_1 \cong \left(h, (-\infty, -\frac{2a_2}{3a_3})\right)$ $\gamma_2 = -\frac{2a_2}{3a_3}$ $\gamma_3 \cong \left(h, (-\frac{2a_2}{3a_3}, +\infty)\right)$
(2)	$\Delta_1 < 0 \wedge P < 0$	$\{1,1,1\}$	$\gamma_1 \cong \left(f, (-\infty, -\frac{W}{2\Delta_2})\right)$ $\gamma_2 \cong \left(f, (-\frac{W}{2\Delta_2}, -\frac{a_2}{3a_3})\right)$ $\gamma_3 \cong \left(f, (-\frac{2a_2}{3a_3}, +\infty)\right)$
(3)	$\Delta_1 < 0 \wedge P > 0$	$\{1,1,1\}$	$\gamma_1 \cong \left(f, (-\infty, -\frac{a_2}{3a_3})\right)$ $\gamma_2 \cong \left(f, (-\frac{a_2}{3a_3}, -\frac{W}{2\Delta_2})\right)$ $\gamma_3 \cong \left(f, (-\frac{W}{2\Delta_2}, +\infty)\right)$
(4)	$\Delta_1 > 0 \wedge a_0 = 0$	$\{1\}$	$\gamma_1 = 0$
(5)	$\Delta_1 > 0 \wedge a_0 < 0$	$\{1\}$	$\gamma_1 \cong (f, (0, +\infty))$
(6)	$\Delta_1 > 0 \wedge a_0 > 0$	$\{1\}$	$\gamma_1 \cong (f, (-\infty, 0))$
(7)	$\Delta_1 = 0 \wedge \Delta_2 \neq 0$	$\{1,2\}$	$\gamma_1 = \min\left\{\frac{-W}{2\Delta_2}, \frac{-a_2\Delta_2 + a_3 W}{a_3\Delta_2}\right\}$ $\gamma_2 = \max\left\{\frac{-W}{2\Delta_2}, \frac{-a_2\Delta_2 + a_3 W}{a_3\Delta_2}\right\}$
(8)	$\Delta_1 = 0 \wedge \Delta_2 = 0$	$\{3\}$	$\gamma_1 = -\frac{2a_2}{3a_3}$

όπου $h = 9a_3^2X^2 + 12a_2a_3X + 4a_2^2 + 9a_3a_1$.

Απόδειξη: Θα εξετάσουμε τι συμβαίνει σε κάθε περίπτωση του $\mathcal{IDS}$.

Η ποσότητα $\mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) - \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty))$ σύμφωνα με το Πορ. 2.27 μας δίνει το πλήθος των πραγματικών ριζών της f. Επίσης το πρόσημο της αποτίμησης του $\mathbf{SR}_j$ στο $\pm\infty$ υπολογίζεται ως $\mathtt{sign}(\lim_{X\to\pm\infty} \mathbf{SR}_j(X))$.

Διακρίνουμε τις παρακάτω περιπτώσεις:

- Το f είναι τύπου (1) ή (2) ή (3). Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(-,+,-,+) = 3$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,+,+) = 0$$

  και συνεπώς $V_- - V_+ = 3 - 0 = 4$, οπότε το f έχει 3 πραγματικές ρίζες (Πορ. 2.27) που είναι ο μέγιστος αριθμός ριζών που μπορεί να έχει και άρα είναι απλές, δηλαδή $\{1,1,1\}$.

  Παρατηρούμε ότι για την τετμημένη του σημείου καμπής ισχύει ότι

$$\mathtt{sign}\left(f(-\frac{2a_2}{3a_3})\right) = \mathtt{sign}(2a_2\Delta_2 - 3a_3W) = \mathtt{sign}(P)$$

  Αν το f είναι τύπου (1) τότε $\mathtt{sign}\left(f(-\frac{2a_2}{3a_3})\right) = \mathtt{sign}(P) = 0$ και γνωρίζουμε τη μία ρίζα ακριβώς· συνεπώς $f = (X + \frac{2a_2}{3a_3})\,h$. Αναπαριστούμε τις άλλες δύο ρίζες χρησιμοποιώντας το δευτεροβάθμιο πολυώνυμο h και το $-\frac{2a_2}{3a_3}$ ως σημείο διαχωρισμού τους.

Αν το f είναι τύπου (2) ή (3) τότε θεωρούμε την ευθεία απομόνωσης (Λημ. 5.6). Αντικαθιστώντας στην (5.10) $Y = 0$, παρατηρούμε ότι η ευθεία απομόνωσης τέμνει τον X άξονα στο σημείο $\left(-\frac{W}{2\Delta_2}, 0\right)$. Επειδή το f έχει μόνο πραγματικές ρίζες ισχύει $\Delta_2 > 0$ [3] (Θεωρ. 5.2). Η τετμημένη του σημείου καμπής, $-\frac{2c_2}{3c_3}$, βρίσκεται ανάμεσα στις ρίζες καθώς αποτελεί τον αριθμητικό τους μέσο. Υποθέτουμε ότι $\text{sign}\left(f(-\frac{2c_2}{3c_3})\right) = P > 0$. Τότε υπάρχει μία ρίζα του f αριστερά του $-\frac{2c_2}{3c_3}$ και δύο δεξιά (Σχ. 5.2). Παρατηρούμε ότι

$$-\frac{a_2}{3a_3} < -\frac{W}{2\Delta_2} \Longleftrightarrow P > 0$$

Λόγω του γεγονότος ότι η f είναι κυρτή δεξιά από το σημείο καμπής, η ευθεία απομόνωσης κόβει τον X άξονα μετά τη δεύτερη ρίζα και πριν την τρίτη. Κατά συνέπεια οι $-\frac{2c_2}{3c_3}$ και $-\frac{W}{2\Delta_2}$ διαχωρίζουν τις ρίζες του f. Η περίπτωση $P < 0$ είναι όμοια και ισχύει $-\frac{a_2}{3a_3} > -\frac{W}{2\Delta_2}$.

Παρατηρούμε ότι το $-\frac{W}{2\Delta_2}$ δεν μπορεί να είναι ρίζα της f καθώς ισχύει

$$\text{sign}\left(f(-\frac{W}{2\Delta_2]})\right) = \text{sign}(P \cdot \Delta_1) \neq 0$$

- Η f είναι τύπου (4) ή (5) ή (6). Ισχύει ότι

$$V_- = \texttt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \texttt{VAR}(-,+,\pm \vee 0,-) = 2$$
$$V_+ = \texttt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \texttt{VAR}(+,+,\mp \vee 0,-) = 1$$

και συνεπώς $V_- - V_+ = 2 - 1 = 0$, οπότε το f έχει 1 πραγματική ρίζα (Πορ. 2.27). Εφόσον δεν μηδενίζεται κάποιο $\mathbf{psc}_i$, $i \in \{0, 1\}$ η ρίζα έχει πολλαπλότητα 1 (Θεωρ. 2.20). Η ρίζα είναι αρνητική, θετική ή μηδέν ανάλογα με το πρόσημο του a_0.

- Η f είναι τύπου (7). Ισχύει ότι

$$V_- = \texttt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \texttt{VAR}(-,+,-,0) = 2$$
$$V_+ = \texttt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \texttt{VAR}(+,+,+,0) = 0$$

και συνεπώς $V_- - V_+ = 2 - 0 = 2$, οπότε το f έχει 2 πραγματικές ρίζες (Πορ. 2.27). Παρατηρούμε ότι από το Θεωρ. 5.2 συνάγουμε ότι $\Delta_2 \geq 0$.

Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_1$. Οπότε η μία ρίζα, αυτή με πολλαπλότητα 2, είναι η λύση της εξίσωσης $\mathbf{SR}_1 = 0$, δηλαδή η $-\frac{W}{2\Delta_2}$. Η απλή ρίζα είναι η $\frac{-a_2\Delta_2 + a_3 W}{a_3\Delta_2}$.

- Η f είναι τύπου (8). Ισχύει ότι

$$V_- = \texttt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \texttt{VAR}(-,+,0,0) = 1$$
$$V_+ = \texttt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \texttt{VAR}(+,+,0,0) = 0$$

και συνεπώς $V_- - V_+ = 1 - 0 = 1$, οπότε το f έχει 1 πραγματική ρίζα (Πορ. 2.27).

Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = \mathbf{psc}_1 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_2$. Η ρίζα έχει πολλαπλότητα 3 και υπολογίζεται ως η διπλή ρίζα του $\mathbf{SR}_2 = f'$.

Εφόσον έχουμε θεωρήσει όλους τους δυνατούς συνδυασμούς προσήμων των **psc**, η πρόταση αποδείχτηκε. ΟΕΔ

Το τεταρτοβάθμιο πολυώνυμο

Θεωρούμε το τεταρτοβάθμιο πολυώνυμο (quartic) $f \in \mathbb{Z}[X]$, όπου $a > 0$.

$$f(X) = a\,X^4 - 4\,b\,X^3 + 6\,c\,X^2 - 4\,d\,X + e \tag{5.11}$$

Προκειμένου να υπολογίζουμε τις ρίζες του f με τη χρήση ριζικών εφαρμόζουμε τον μετασχηματισμό $X \mapsto X + \frac{b}{a}$ και στη συνέχεια διαιρούμε με τον μεγιστοβάθμιο όρο, οπότε προκύπτει ένα πολυώνυμο της μορφής $g = x^4 + px^2 + qx + r$ του οποίου οι λύσεις δίνονται από τους τύπους

$$\begin{array}{ll} \frac{1}{2}\left(\sqrt{\alpha} + \sqrt{\beta} + \sqrt{\gamma}\right) & \frac{1}{2}\left(-\sqrt{\alpha} + \sqrt{\beta} - \sqrt{\gamma}\right) \\ \frac{1}{2}\left(\sqrt{\alpha} - \sqrt{\beta} - \sqrt{\gamma}\right) & \frac{1}{2}\left(-\sqrt{\alpha} - \sqrt{\beta} + \sqrt{\gamma}\right) \end{array}$$

όπου τα α, β και γ είναι οι τρεις ρίζες της κυβικής εξίσωσης

$$y^3 + 2py^2 + (p^2 - 3r)y - d^2$$

η οποία ονομάζεται *διαλυτική* (resolvent cubic).

Καταρχάς θα παρουσιάσουμε κάποιες από τις αναλλοίωτες (invariants) του πολυωνύμου τετάρτου βαθμού. Για περισσότερες λεπτομέρειες σχετικά με τις αναλλοίωτες ο αναγνώστης μπορεί να ανατρέξει στους Sturmfels [250] και Salmon [236] και ειδικά για το πολυώνυμο τετάρτου βαθμού στις εργασίες του Cremona [61, 62]. Θεωρούμε τις ρητές αναλλοίωτες του f, δηλαδή τις αναλλοίωτες κάτω από πίνακες μετασχηματισμών που ανήκουν στον χώρο $GL(2, \mathbb{Q})$. Αυτές οι αναλλοίωτες σχηματίζουν ένα βαθμωτό δακτύλιο (graded ring) [62], του οποίου οι γεννήτορες, βαθμών 2 και 3 αντίστοιχα, είναι

$$\begin{aligned} H &= W_3 + 3\,\Delta_3 = ae - 4bd + 3c^2 \\ G &= -d\,W_1 - e\,\Delta_2 - c\,\Delta_3 = ace + 2bcd - ad^2 - eb^2 - c^3 \end{aligned} \tag{5.12}$$

Τα H και G είναι αλγεβρικά (πολυωνυμικά) ανεξάρτητα. Κάθε άλλη αναλλοίωτη είναι ένα ισοβαρές πολυώνυμο στα H και G, δηλαδή είναι ομογενές στους συντελεστές του f. Η πιο σημαντική και γνωστή αναλλοίωτη είναι

$$\Delta_1 = \mathrm{disc}(f) = H^3 - 27\,G^2 \tag{5.13}$$

η οποία είναι η *διακρίνουσα* (*discriminant*) του f. Οι ημι-αναλλοίωτες (seminvariants) του f είναι τα H, G και

$$\begin{aligned} \Delta_2 &= b^2 - a\,c \\ R &= a\,W_1 + 2\,b\,\Delta_2 = 2b^3 + a^2 d + -3abc \\ Q &= 12\,\Delta_2^2 - a^2\,H = 9a^2c^2 - 24acb^2 + 12b^4 - ea^3 + 4a^2db \end{aligned} \tag{5.14}$$

Επίσης χρειαζόμαστε και τις ακόλουθες ποσότητες οι οποίες δεν είναι αναλλοίωτες αλλά στοιχεία του πίνακα Bézout του f και του f'.

$$\begin{array}{lcllcllcl} \Delta_3 &=& c^2 - b\,d & W_1 &=& a\,d - b\,c & T_1 &=& -9\,W_1^2 + 27\,\Delta_2\,\Delta_3 - 3\,W_3\,\Delta_2 \\ \Delta_4 &=& d^2 - c\,e & W_2 &=& b\,e - c\,d & T_2 &=& 3\,H\,W_1 - 9\,b\,G \\ & & & W_3 &=& a\,e - b\,d & & & \end{array} \tag{5.15}$$

Ισχύει η ακόλουθη πρόταση [92, 273]

Πρόταση 5.8. *Έστω $f(X)$ όπως στην (5.11). Το σύστημα διακρινουσών είναι:*

$$\begin{array}{lll} (1) & \Delta_1 > 0 \wedge T_1 > 0 \wedge \Delta_2 > 0 & \{1,1,1,1\} \\ (2) & \Delta_1 > 0 \wedge (T_1 \leq 0 \vee \Delta_2 \leq 0) & \{\} \\ (3) & \Delta_1 < 0 & \{1,1\} \\ (4) & \Delta_1 = 0 \wedge T_1 > 0 & \{2,1,1\} \\ (5) & \Delta_1 = 0 \wedge T_1 < 0 & \{2\} \\ (6) & \Delta_1 = 0 \wedge T_1 = 0 \wedge \Delta_2 > 0 \wedge R = 0 & \{2,2\} \\ (7) & \Delta_1 = 0 \wedge T_1 = 0 \wedge \Delta_2 > 0 \wedge R \neq 0 & \{3,1\} \\ (8) & \Delta_1 = 0 \wedge T_1 = 0 \wedge \Delta_2 < 0 & \{\} \\ (9) & \Delta_1 = 0 \wedge T_1 = 0 \wedge \Delta_2 = 0 & \{4\} \end{array}$$

Σημείωση 5.9. *Ο Yang [273] έχει ένα μικρό τυπογραφικό λάθος στον ορισμό του T_1. Επίσης το σύστημα διακρινουσών είναι νόμιμο για $f \in \mathbb{R}[X]$.*

Προκειμένου να υπολογίσουμε το σύστημα διακρινουσών του πολυωνύμου τετάρτου βαθμού θεωρούμε την (προσημασμένη) ακολουθία υπο-επιλυουσών του f και του f', $\mathbf{SR}(f, f')$ (Παρ. 2.3). Μπορούμε να υπολογίσουμε την ακολουθία συμβολικά και είμαστε βέβαιοι ότι για οποιαδήποτε ανάθεση τιμών στις παραμέτρους, με τον περιορισμό $a \neq 0$, η ακολουθία θα είναι νόμιμη. Η ακολουθία $\mathbf{SR}(f, f')$ είναι

$$\mathbf{SR}(f, f') = \begin{cases} \mathbf{SR}_4(X) &=& f(X) \\ \mathbf{SR}_3(X) &=& f'(X) \\ \mathbf{SR}_2(X) &=& 3\,\Delta_2 X^2 + 3\,W_1 X - W_3 \\ \mathbf{SR}_1(X) &=& T_1\,X + T_2 \\ \mathbf{SR}_0(X) &=& \Delta_1 \end{cases} \tag{5.16}$$

όπου τους συντελεστές των πολυωνύμων της ακολουθίας παρουσιάζονται με τη βοήθεια των ποσοτήτων των (5.13), (5.14) και (5.15). Προκειμένου να υπολογίσουμε το πλήθος και τις πολλαπλότητες των πραγματικών ριζών του f αποτιμούμε την $\mathbf{SR}(f, f')$ στο $\pm\infty$ και χρησιμοποιούμε το Πορ. 2.27. Ιδιαίτερη προσοχή χρειάζεται στην περίπτωση ύπαρξης πολλαπλών ριζών. Γι' αυτή την περίπτωση θα χρησιμοποιήσουμε το Θεωρ. 2.20.

Αν και το σύστημα διακρινουσών του τετάρτου βαθμού πολυωνύμου είναι γνωστό, αριθμοί που απομονώνουν τις πραγματικές του ρίζες δεν είναι και τόσο εύκολο να υπολογιστούν. Ας δούμε αναλυτικά τι συμβαίνει σε όλες τις περιπτώσεις της Πρότ. 5.8, όμοια με την απόδειξη του $\mathcal{IDS}$ του κυβικού πολυωνύμου.

(1) $\{1,1,1,1\}$. Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,+,-,+) = 4$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,+,+,+) = 0$$

και συνεπώς $V_- - V_+ = 4 - 0 = 4$, οπότε το f έχει 4 πραγματικές ρίζες (Πορ. 2.27).

Τα σημεία διαχωρισμού θα τα εξετάσουμε στη συνέχεια.

(2) $\{\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,-\vee 0,+\vee 0,+) = 2$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,-\vee 0,-\vee 0,+) = 2$$

και συνεπώς $V_- - V_+ = 2 - 2 = 0$, οπότε το f δεν έχει πραγματικές ρίζες (Πορ. 2.27).

(3) $\{1,1\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,\pm\vee 0,\pm\vee 0,-) = 3$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,\pm\vee 0,\pm\vee 0,-) = 1$$

και συνεπώς $V_- - V_+ = 3 - 1 = 2$, οπότε το f έχει πραγματικές ρίζες (Πορ. 2.27). Παρατηρούμε ότι η περίπτωση

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,-,-,-) = 1$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,-,+,-) = 3$$

δεν μπορεί να συμβεί καθώς δίνει αποτέλεσμα $V_- - V_+ = 1 - 3 = -2$!

Τα σημεία διαχωρισμού καλύπτονται από την περίπτωση (1).

(4) $\{2,1,1\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,+,-,0) = 3$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,+,+,0) = 0$$

και συνεπώς $V_- - V_+ = 3 - 0 = 3$, οπότε το f έχει 3 πραγματικές ρίζες (Πορ. 2.27).

Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = -\Delta_1 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_1$. Οπότε η ρίζα του $\mathbf{SR}_1$ είναι ρίζα του f (πολλαπλότητας 2) και του f' (πολλαπλότητας 1) και έχει τιμή $-\frac{T_2}{T_1}$. Μπορούμε να διαιρέσουμε το f με $(SR_1)^2$ και το πηλίκο της διαίρεσης είναι ένα δευτεροβάθμιο πολυώνυμο το οποίο ορίζει τις άλλες δύο ρίζες.

(5) $\{2\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,\pm,+,0) = 2$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,\mp,-,0) = 1$$

και συνεπώς $V_- - V_+ = 2 - 1 = 1$, οπότε το f έχει 1 πραγματική ρίζα (Πορ. 2.27).

Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = -\Delta_1 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_1$. Συνεπώς η διπλή ρίζα έχει τιμή $-\frac{T_2}{T_1}$, όπως και στην προηγούμενη περίπτωση.

(6) $\{2,2\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,+,0,0) = 2$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,+,0,0) = 0$$

και συνεπώς $V_- - V_+ = 2 - 0 = 2$, οπότε το f έχει 2 πραγματικές ρίζες (Πορ. 2.27).

Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = \mathbf{psc}_1 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_2$. Η συνθήκη $R = 0$ μας εξασφαλίζει ότι το $\mathbf{SR}_2$ έχει δύο διαφορετικές ρίζες. Εκφράζουμε τις ρίζες ως τις πραγματικές ρίζες του τριωνύμου $\mathbf{SR}_2 = 3\Delta_2 X^2 + 3W_1 X - W_3$.

Μια σημαντική παρατήρηση αφορά τη συνθήκη $R = 0$. Ισοδύναμα θα μπορούσαμε να θεωρήσουμε τη συνθήκη $\mathsf{disc}(\mathbf{SR}_2) = 3W_1^2 - 4\Delta_2 W_3 \neq 0$, η οποία όμως είναι πιο πολύπλοκη. Η συνθήκη για το R προκύπτει αν θεωρήσουμε τους συντελεστές ως συμμετρικές συναρτήσεις των ριζών και προσπαθήσουμε να διαχωρίσουμε την παρούσα από την επόμενη περίπτωση. Παρατηρούμε ότι είναι πολύ δύσκολο, αν όχι ανέφικτο, να παρουσιαστούν αλγόριθμοι που να λειτουργούν ως μαύρα κουτιά και να υπολογίζουν τις *βέλτιστες* κατά κάποια έννοια συνθήκες! Τέτοιου είδους αρνητικά αποτελέσματα παρουσιάζονται από τον Lazard [170], όπως επίσης και οι βέλτιστες συνθήκες στους συντελεστές προκειμένου ένα τεταρτοβάθμιο πολυώνυμο να είναι πάντοτε θετικό.

(7) $\{3,1\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,+,0,0) = 2$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,+,0,0) = 0$$

και συνεπώς $V_- - V_+ = 2 - 0 = 2$, οπότε το f έχει 2 πραγματικές ρίζες (Πορ. 2.27).

Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = \mathbf{psc}_1 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_2$. Η συνθήκη $R = 0$ μας εξασφαλίζει ότι το $\mathbf{SR}_2$ έχει μία διπλή ρίζα (και άρα ως ρίζα του f έχει πολλαπλότητα 3) η οποία είναι $-\frac{W_1}{2\Delta_2}$. Η απλή ρίζα είναι $\frac{3\,aW_1 + 8\,b\Delta_2}{2\,a\Delta_2}$.

Ισχύει η ίδια παρατήρηση για το R όπως για την προηγούμενη περίπτωση. Ισοδύναμα, θα μπορούσαμε να θεωρήσουμε τη συνθήκη $\mathsf{disc}(\mathbf{SR}_2) = 3W_1^2 - 4\Delta_2 W_3 = 0$.

(8) $\{\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,-,0,0) = 2$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,-,0,0) = 2$$

και συνεπώς $V_- - V_+ = 1 - 1 = 0$, οπότε το f δεν έχει πραγματικές ρίζες (Πορ. 2.27).

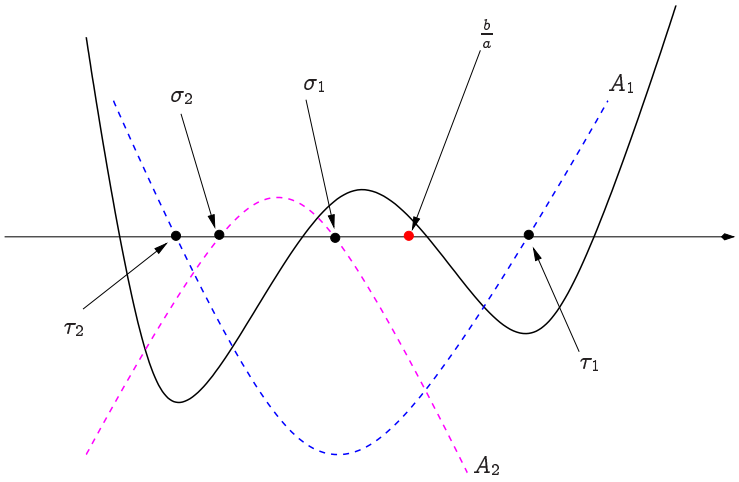
Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = \mathbf{psc}_1 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_2$ και άρα οι μιγαδικές ρίζες είναι πολλαπλότητας 2.

(9) $\{4\}$ Ισχύει ότι

$$V_- = \mathtt{VAR}(\mathbf{SR}(f\,;\,-\infty)) = \mathtt{VAR}(+,-,0,0,0) = 1$$
$$V_+ = \mathtt{VAR}(\mathbf{SR}(f\,;\,+\infty)) = \mathtt{VAR}(+,+,0,0,0) = 0$$

και συνεπώς $V_- - V_+ = 1 - 0 = 1$, οπότε το f έχει μία πραγματική ρίζα (Πορ. 2.27).

Από τις ιδιότητες των υπο-επιλυουσών (Θεωρ. 2.20) εφόσον $\mathbf{SR}_0 = \mathbf{psc}_0 = \mathbf{psc}_1 = \mathbf{psc}_2 = 0$ τότε $\gcd(f, f') = \mathbf{SR}_3$. Η μοναδική πραγματική ρίζα είναι η $\frac{b}{a}$, η οποία έχει πολλαπλότητα 3 ως ρίζα του $\mathbf{SR}_3 = f'$.



Σχήμα 5.3: Απομόνωση των ριζών του τεταρτοβάθμιου πολυωνύμου

Η γραφική παράσταση της f, (5.11), και τα δύο πολυώνυμα διαχωρισμού, A_1 και A_2 και οι ρίζες τους. Το $\frac{b}{a}$ είναι ο αριθμητικός μέσος των ριζών και σημείο διαχωρισμού.

Υπολογισμός σημείων διαχωρισμού

Απομένει να υπολογίσουμε σημεία διαχωρισμού για την περίπτωση που το πολυώνυμο έχει τέσσερις, διαφορετικές μεταξύ τους, πραγματικές ρίζες. Προκειμένου να το επιτύχουμε θα χρησιμοποιήσουμε την Πρότ. 5.1 και βοηθητικά πολυώνυμα απομόνωσης. Σε ότι θα ακολουθήσει θα θεωρήσουμε ότι το f είναι τύπου (1).

Το πρώτο πολυώνυμο απομόνωσης

Έστω $B_1(X) = ax - b$ και $C_1(X) = -4a$ τότε από την (5.1) προκύπτει το πολυώνυμο

$$A_1(X) = 3\,\Delta_2\,X^2 + 3\,W_1\,X - W_3. \tag{5.17}$$

Καθώς ο αριθμός $\frac{b}{a}$ είναι ο αριθμητικός μέσος των (μιγαδικών) ριζών του f τότε αν το f έχει 4 πραγματικές ρίζες τότε σίγουρα βρίσκεται κάπου ανάμεσά τους.

Προκειμένου να υπολογίσουμε δύο ακόμα τέτοιους αριθμούς επιλύσουμε την (5.17), και έστω $\sigma_{1,2}$ οι ρίζες της

$$\sigma_{1,2} = \frac{-3W_1 \pm \sqrt{9W_1^2 + 12\Delta_2 W_3}}{6\Delta_2} \tag{5.18}$$

Εύκολα δείχνουμε ότι $\text{sign}\left(f(\frac{b}{a})\right) = \text{sign}\left(a^2 H - 3\Delta_2^2\right)$, συνεπώς

$$\begin{cases} \sigma_1 < \frac{b}{a} < \sigma_2, & \text{αν } f(\frac{b}{a}) > 0 \\ \sigma_1 < \sigma_2 < \frac{b}{a}, & \text{αν } f(\frac{b}{a}) < 0 \ \wedge \ R > 0 \\ \frac{b}{a} < \sigma_1 < \sigma_2, & \text{αν } f(\frac{b}{a}) < 0 \ \wedge \ R < 0 \end{cases} \tag{5.19}$$

όπου R είναι υποαναλλοίωτη και την έχουμε ορίσει προηγουμένως. Αν $f(\frac{b}{a}) = 0$ τότε ξέρουμε ακριβώς μια ρίζα και συνεπώς το πρόβλημα είναι ευκολότερο καθώς οι άλλες τρεις ρίζες είναι λύσεις κάποιου κυβικού πολυωνύμου. Στο Σχ. 5.3 παρουσιάζεται η περίπτωση $f(\frac{b}{a}) > 0$.

Επισημαίνουμε ότι η διακρίνουσα του A_1 είναι αναλλοίωτη του f ως προς την μετατόπιση.

Το δεύτερο πολυώνυμο απομόνωσης

Προκειμένου να υπολογίσουμε ένα ακόμα πολυώνυμο απομόνωσης θεωρούμε τα $B_2(X) = dx - e$ και $C_2(X) = -4d$ και από την (5.1) προκύπτει το πολυώνυμό

$$A_2(X) = W_3\, X^3 - 3\, W_2\, X^2 - 3\, \Delta_4\, F \tag{5.20}$$

του οποίου οι ρίζες είναι

$$0, \tau_{1,2} = \frac{3W_2 \pm \sqrt{9W_2^2 + 12\Delta_4 W_3}}{6W_3} \tag{5.21}$$

Από την Πρότ. 5.1 τουλάχιστον δύο από τους $\{0, \tau_1, \tau_2\}$ διαχωρίζουν τις πραγματικές ρίζες του f (Σχ. 5.3), όπου $\tau_{1,2}$ είναι οι μη μηδενικές ρίζες του $A(X)$. Αν υποθέσουμε ότι οι ρίζες της (5.11) είναι > 0, έτσι ώστε το 0 να μην είναι σημείο διαχωρισμού, η διάταξη των τ_1, τ_2 και $\frac{e}{d}$ καθορίζεται ανάλογα με την (5.19).

Επιπλέον πολυώνυμα απομόνωσης

Ας θεωρήσουμε το $f(X) = \sum_{i=1}^{4} = a_i X^i$. Έστω $B(X) = a_i X - k a_j$ και $C(X) = \ell$ όπου a_i και a_j είναι συντελεστές του f (αλλά μπορούν να είναι οποιοσδήποτε ρητός αριθμός) και k και ℓ παράμετροι. Κάνοντας πράξεις κατασκευάζουμε το πολυώνυμο $A(X) := B(X)f'(X) + C(X)f(X)$ το οποίο είναι της μορφής

$$A(X) = b_4 X^4 + b_3 X^3 + b_2 X^2 + b_1 X + b_0$$

όπου οι συντελεστές του b_i είναι γραμμικές συναρτήσεις των παραμέτρων k και ℓ. Μπορούμε να επιλέξουμε δύο από τους συντελεστές b_i και να τους θέσουμε ίσους με μηδέν, δηλαδή να κατασκευάσουμε ένα 2×2 γραμμικό σύστημα με αγνώστους τους παραμέτρους k και ℓ.

Εάν επιλέξουμε τους b_4 και b_3 τότε έχουμε το πρώτο πολυώνυμο απομόνωσης. Εάν επιλέξουμε τους b_3 και b_1 τότε έχουμε το διτετράγωνο πολυώνυμο

$$3\, aW_1 X^4 + 6(3b\Delta_3 - d\Delta_2)X^2 - eW_1 - 8b\Delta_3 \tag{5.22}$$

το οποίο είναι χαρακτηριστικό της f, αποτελεί κάποια αναλλοίωτη καμπύλη του f (covariant) και του οποίου είτε η μεγαλύτερη ρίζα διαχωρίζει τις δύο μεγαλύτερες ρίζες της f είτε η μικρότερη διαχωρίζει τις δύο μικρότερες.

Ρητά σημεία διαχωρισμού

Ας επιστρέψουμε στο πρόβλημα του υπολογισμού ρητών σημείων διαχωρισμού. Υποθέτουμε ότι το 0 δεν είναι ρίζα του f (γιατί αλλιώς θα είχαμε ένα κυβικό πολυώνυμο), συνεπώς $e \neq 0$. Προκειμένου να απλοποιήσουμε τον συμβολισμό και να μειώσουμε το πλήθος των παραμέτρων

ας υποθέσουμε επιπλέον ότι $b = 0$ (ο γραμμικός μετασχηματισμός $X \mapsto X + \frac{b}{a}$ το πετυχαίνει πάντοτε αυτό).

Θέτοντας $b = 0$ στο A_1, Εξ. (5.17), οι λύσεις του είναι

$$\sigma_{1,2} = \frac{3\,d \pm \sqrt{9\Delta_4 - 3\,ce}}{6c} \tag{5.23}$$

Θέτοντας $b = 0$ στο A_2, Εξ. (5.20), οι λύσεις του είναι

$$\tau_{1,2,3} = \frac{-3\,dc \pm \sqrt{9\,d^2c^2 + 12\,ae\Delta_4}}{2ae}, 0 \tag{5.24}$$

Οι αριθμοί $\{\frac{b}{a}, \sigma_1, \sigma_2\}$, με κάποια διάταξη διαχωρίζουν τις ρίζες του f. Το ίδιο και οι $\{0, \frac{e}{d}, \tau_1, \tau_2\}$. Η δύσκολη περίπτωση είναι όταν τ_i και σ_j, $i, j \in \{1, 2\}$, διαχωρίζουν το ίδιο ζευγάρι συνεχόμενων πραγματικών ριζών του f. Μια τέτοια περίπτωση εμφανίζεται στο Σχ. 5.3, όπου τα σ_2 και τ_2 διαχωρίζουν τις δύο μικρότερες πραγματικές ρίζες του πολυωνύμου.

Ας υποθέσουμε ότι αυτό συμβαίνει για το ζευγάρι σ_1 και τ_1, δηλαδή ισχύει $\gamma_i < \tau_1 < \sigma_1 < \gamma_{i+1}$ για $1 \le i \le 3$. Θα χρειαστούμε το επόμενο λήμμα.

Λήμμα 5.10. *Για κάθε $m, n, m', n' \in \mathbb{N}^*$, $0 < \frac{m}{n} < \frac{m'}{n'} \Rightarrow \frac{m}{n} < \frac{m+m'}{n+n'} < \frac{m'}{n'}$.*

Απόδειξη: Η απόδειξη είναι εύκολη αν παρατηρήσουμε ότι ισχύει $m\,n' < m'\,n$. ΟΕΔ

Θέτουμε

$$M := 9\Delta_4 - 3\,ce, \quad N := 12\,ae\Delta_4 + 9\,d^2c^2 \tag{5.25}$$

Παρατηρούμε ότι τα M και N είναι οι διακρίνουσες των A_1 και A_2. Χρησιμοποιώντας το Λημ. 5.10 συμπεραίνουμε ότι

$$\tau_1 < \frac{3d - 3dc + \sqrt{M} + \sqrt{N}}{6c + 2ae} < \sigma_1$$

Αν μπορέσουμε να υπολογίσουμε έναν ακέραιο $K \in [\sqrt{M}, \sqrt{N}]$, τότε αρκεί να αντικαταστήσουμε την ποσότητα $\sqrt{M} + \sqrt{N}$ με $2K$. Συμβολίζουμε το υπολογισθέν σημείο διαχωρισμού με $\sigma_1 \oplus \tau_1$, και παρατηρούμε ότι έχει αλγεβρικό βαθμό 2 στους συντελεστές του πολυωνύμου. Θα δείξουμε ότι μπορούμε να επιλέξουμε $K = \lfloor\sqrt{M}\rfloor + 1$, δηλαδή ότι ισχύει $\sqrt{M} \le \lfloor\sqrt{M}\rfloor + 1 \le \sqrt{N}$.

Θεώρημα 5.11

Για κάθε πολυώνυμο τετάρτου βαθμού $f \in \mathbb{Z}[X]$ με 4 διαφορετικές πραγματικές ρίζες και $b = 0$, ισχύει $\sqrt{N} - \sqrt{M} \ge 1$ ή

$$\sqrt{9\Delta_4 - 3\,ce} \le \lfloor\sqrt{9\Delta_4 - 3\,ce}\rfloor + 1 \le \sqrt{9\,d^2c^2 + 12\,ae\Delta_4}$$

ή εναλλακτικά $|\sqrt{9\Delta_4 - 3\,ce} - \sqrt{9\,d^2c^2 + 12\,ae\Delta_4}| \ge 1$.

Απόδειξη: Υπενθυμίζουμε ότι $M = 9d^2 - 12ce$ και $N = 12aed^2 - 12ace^2 + 9d^2c^2$. Αρκεί να δείξουμε ότι:

$$\begin{aligned}
\sqrt{N} &\geq 1 + \sqrt{M} && \Leftrightarrow \\
\sqrt{\frac{N}{M}} &\geq 1 + \frac{1}{\sqrt{M}} && \Leftarrow \\
\sqrt{\frac{N}{M}} &\geq 2 && \Leftrightarrow \\
\frac{N}{M} &\geq 4 && \Leftrightarrow \\
\frac{N}{M} = \frac{4aed^2 - 4ace^2 + 3d^2c^2}{3d^2 - 4ce} &\geq 4 && \Leftrightarrow \\
4aed^2 - 4ace^2 + 3d^2c^2 &\geq 12d^2 - 16ce && \Leftrightarrow \\
4aed^2 - 4ace^2 + 3d^2c^2 - 12d^2 + 16ce &\geq 0.
\end{aligned} \tag{5.26}$$

Εφόσον το f είναι τύπου (1) από την Πρότ. 5.8 προκύπτει ότι $\Delta_2 > 0 \Rightarrow c < 0$. Από τον κανόνα προσήμων του Descartes (Θεωρ. 3.28) προκύπτει ότι αν $e > 0$ τότε υπάρχουν το 2 θετικές και 2 αρνητικές ρίζες ενώ αν $e < 0$ τότε υπάρχουν 3 θετικές και 1 αρνητική αν $d < 0$ ή το αντίστροφο αν $d > 0$. Καταρχάς θεωρούμε $e > 0$.

Θεωρούμε την (πολυωνυμική) συνάρτηση $g(a, c, d, e) = 4aed^2 - 4ace^2 + 3d^2c^2 - 12d^2 + 16ce$, Το πρόβλημα τώρα είναι να υπολογίσουμε την ελάχιστη τιμή της g (στους ακεραίους) κάτω από τους περιορισμούς $a \geq 1$, $c \leq -5$, $d \geq 0$ και $e \geq 5$. Τις περιπτώσεις $-5 < c \leq 0$ και $0 < e < 5$ θα τις εξετάσουμε ξεχωριστά. Εισάγουμε τις μεταβλητές y_1, y_2 και y_2 και θα χρησιμοποιήσουμε τους πολλαπλασιαστές Lagrange για την εύρεση του ελαχίστου. Κατά συνέπεια θέλουμε να λύσουμε το πρόβλημα

$$\begin{aligned}
\min\ L(a, c, d, e, y_1, y_2, \lambda_1, \lambda_2) \;=\; & g(a, c, d, e) + \\
& \lambda_1(c + y_1^2 + 5) + \\
& \lambda_2(-e + y_2^2 + 5) \\
& \lambda_3(-a + y_3^2 + 1)
\end{aligned} \tag{5.27}$$

Υπολογίζουμε τις μερικές παραγώγους του L και τελικά προκύπτει ότι πρέπει να λύσουμε το σύστημα

$$\left\{\begin{array}{rcll}
\frac{\partial}{\partial a}L &=& 12\,e\left(d^2 - ce\right) - \lambda_3 &= 0 \\
\frac{\partial}{\partial c}L &=& -12\,ae^2 + 18\,d^2c + 48\,e + \lambda_1 &= 0 \\
\frac{\partial}{\partial d}L &=& 24\,aed + 18\,dc^2 - 72\,d &= 0 \\
\frac{\partial}{\partial e}L &=& 12\,a\left(d^2 - ce\right) - 12\,aec + 48\,c - \lambda_2 &= 0 \\
\frac{\partial}{\partial y_1}L &=& 2\,\lambda_1 y_1 &= 0 \\
\frac{\partial}{\partial y_2}L &=& 2\,\lambda_2 y_2 &= 0 \\
\frac{\partial}{\partial y_3}L &=& 2\,\lambda_3 y_3 &= 0 \\
\frac{\partial}{\partial \lambda_1}L &=& c + 5 + {y_1}^2 &= 0 \\
\frac{\partial}{\partial \lambda_2}L &=& -e + 5 + {y_2}^2 &= 0 \\
\frac{\partial}{\partial \lambda_3}L &=& -a + 1 + {y_3}^2 &= 0
\end{array}\right\} \tag{5.28}$$

Η λύση του συστήματος (5.28) είναι η $(a, c, d, e) = (1, -5, 0, 5)$ και αντίστοιχη τιμή της συνάρτησης είναι $g(1, -5, 0, 5) = 300 > 0$ η οποία είναι τοπικό ελάχιστο. Για την επίλυση του

συστήματος χρησιμοποιήσαμε το MAPLE 9.5. Αν $-5 < c < 0$ και $0 < e < 5$ τότε αντικαθιστούμε όλους τους δυνατούς συνδυασμούς στα M και N και διαπιστώνουμε ότι η ανισότητα $\sqrt{N} - \sqrt{M} \geq 1$ ισχύει. Αν $c = 0$ τότε $\sqrt{A} = 3|d|$, οπότε έχουμε ένα ρητό σημείο διαχωρισμού.

Αν $e < 0$ τότε επιλύουμε ένα σύστημα όμοιο με το (5.28) όπου ο περιορισμός για το e έχει αντικατασταθεί από τον $e + 1 - y_2^2$. ΟΕΔ

Συνεπώς μπορούμε να διατυπώσουμε την ακόλουθη πρόταση

Πρόταση 5.12. *Εστω πολυώνυμο τετάρτου βαθμού $f \in \mathbb{Z}[X]$ με τέσσερις διαφορετικές πραγματικές ρίζες. Τουλάχιστον τρεις από τους ρητούς αριθμούς $\{0, \frac{b}{a}, \frac{e}{d}, \sigma_i \oplus \tau_j\}$, $i, j \in \{1, 2\}$ είναι σημεία διαχωρισμού των ριζών του f.*

Σημείωση 5.13. *Έχουμε παρατηρήσει ότι στην πράξη αρκεί να θεωρήσουμε ως σημεία διαχωρισμού τα*

$$\sigma_{1,2} = \frac{3\,d \pm \lceil \sqrt{9\Delta_4 - 3\,ce}\,\rceil}{6c}$$

και συνεπώς δεν χρειάζεται ο υπολογισμός του δεύτερου πολυωνύμου απομόνωσης. Ωστόσο δεν έχουμε καταφέρει να αποδείξουμε θεωρητικά τον παραπάνω ισχυρισμό.

Το επόμενο θεώρημα συνοψίζει όλο το μέχρι τώρα κεφάλαιο

Θεώρημα 5.14

Για όλα τα ακέραια πολυώνυμα βαθμού ≤ 4 μπορούμε να υπολογίζουμε ρητά σημεία διαχωρισμού με τη χρήση σταθερού αριθμού βασικών πράξεων $\pm, *$ και $\lfloor \cdot \rfloor$.

Πόρισμα 5.15. *Έστω αριθμοί $\omega_1 < \cdots < \omega_n$ όπου $2 \leq n \leq 3$. Τότε υπάρχουν αριθμοί $\ell_1, \ldots \ell_{n-1}$ οι οποίοι τους διαχωρίζουν και οι οποίοι προκύπτουν ως συμμετρικές ρητές πολυωνυμικές συναρτήσεις των ω_i.*

Απόδειξη: Θεωρούμε το πολυώνυμο το οποίο έχει για ρίζες τα ω_i. Οι συντελεστές τους είναι συμμετρικές συναρτήσεις των ω_i. Τα σημεία διαχωρισμού είναι ρητές πολυωνυμικές συναρτήσεις των συντελεστών, άρα και συμμετρικές ρητές πολυωνυμικές συναρτήσεις των ω_i. ΟΕΔ

Αν επιτρέψουμε και την πράξη $\lfloor \cdot \rfloor$, το προηγούμενο πόρισμα ισχύει και για $n = 4$.

5.3 Σύγκριση αλγεβρικών αριθμών

Προκειμένου να συγκρίνουμε δύο αλγεβρικούς αριθμούς βαθμού ≤ 4 θα χρησιμοποιήσουμε τον αλγόριθμο COMPARE (Αλγ. 16). Ωστόσο, θα υπολογίσουμε συμβολικά τις ακολουθίες υποεπιλυουσών, θεωρώντας τους συντελεστές των πολυωνύμων ως παραμέτρους, προκειμένου αφενός για να αποδείξουμε ότι η σύγκριση απαιτεί σταθερό πλήθος αριθμητικών πράξεων και αφετέρου για να επιταχύνουμε τον υπολογισμό στην πράξη.

Ο βαθμός 2

Έστω $\alpha \cong (f_1 = a_2X^2 - 2a_1X + a_0, \mathbb{I}_1)$ και $\beta \cong (f_2 = b_2X^2 - 2b_1 + b_0, \mathbb{I}_2)$ Υπολογίζουμε την ακολουθία $\mathbf{SR}(f_1, f_2)$ η οποία είναι

$$\begin{aligned}\mathbf{SR}_3 &= f_1\\ \mathbf{SR}_2 &= f_2\\ \mathbf{SR}_1 &= 2\,J\,X - G\\ \mathbf{SR}_0 &= -a_2\,(G^2 - 4\,J\,J_1)\end{aligned}$$

όπου $J = a_2b_1 - b_2a_1$, $J_1 = a_1b_0 - b_1a_0$ και $G = a_2b_0 - b_2a_0$. Ανάλογα με τον τύπο των α και β η ακολουθία πρέπει να αποτιμηθεί σε δύο από τους αριθμούς $\{\pm\infty, -\frac{a_1}{a_2}, -\frac{b_1}{b_2}\}$ και στη συνέχεια να μετρήσουμε τις εναλλαγές προσήμων. Η προσέγγιση που παρουσιάζουμε ομοιάζει με αυτή των Emiris and Karavelas [85, 149], αλλά χρησιμοποιούμε μόνο μία ακολουθία υπολοίπων ενώ η προσέγγιση των Emiris and Karavelas [85, 149] χρησιμοποιεί πολλές αλλά δεν υποθέτει ότι οι αλγεβρικοί αριθμοί είναι σε αναπαράσταση με διαστήαμτα απομόνωσης. Επίσης οι Devillers et al. [69, 70] αναδεικνύουν τη γεωμετρική πληροφορία πίσω από τη σύγκριση αλγεβρικών αριθμών βαθμού 2 και παρουσιάζουν έναν (βέλτιστο) αλγόριθμο για τη σύγκριση των δύο μικρότερων ριζών.

Στην εικόνα παρουσιάζουμε τις διάφορες ποσότητες που πρέπει να αποτιμηθούν προκειμένου να συγκρίνουμε τις δύο μεγαλύτερες ρίζες δύο δευτεροβάθμιων εξισώσεων.

Ο μέγιστος αλγεβρικός βαθμός που απαιτείται για την σύγκριση δύο πραγματικών αλγεβρικών αριθμών βαθμού 2 παρουσιάζεται και το υπολογισμό της επιλύσουσας, $\mathbf{SR}_0$ και είναι 4. Καθώς η επιλύουσα είναι η βέλτιστη συνθήκη για την ύπαρξη κοινών ριζών και ο αλγεβρικός βαθμός της είναι βέλτιστος, συνάγουμε ότι, όσο αφορά τον αλγεβρικό βαθμό, ο αλγόριθμος σύγκρισης είναι επίσης βέλτιστος.

Ο βαθμός 3 και 4

Έστω $\alpha \cong (f_1, \mathbb{I}_1)$ και $\beta \cong (f_2, \mathbb{I}_2)$ όπου $\deg(f1) \leq 4$ και $\deg(f_2) \leq 4$. Προκειμένου να συγκρίνουμε τους α και β, σύμφωνα με τον Αλγ. 16, πρέπει να υπολογίσουμε ένα κοινό διάστημα, να υπολογίσουμε την $\mathbf{SR}(f_1, f_2)$ και να την αποτιμήσουμε στα άκρα του διαστήματος.

Στο Σχ. 5.4 παρουσιάζουμε τις διάφορες ποσότητες που πρέπει να ελένξουμε προκειμένου να συγκρίνουμε τις δύο μεγαλύτερες ρίζες δύο κυβικών πολυώνυμων.

Παρουσιάζουμε αναλυτικά την ακολουθία υπο-επιλυουσών όταν και τα δύο πολυώνυμα είναι τετάρτου βαθμού.

Έστω δύο τεταρτοβάθμιο πολυώνυμα

$$f_i(X) = a_iX^4 - 4b_iX^3 + 6c_iX^2 - 4d_iX + e_i.$$

όπου $i = 1, 2$. Η ακολουθία υπο-επιλυουσών $\mathbf{SR}(f_1, f_2)$ είναι

$$\begin{aligned}
\mathbf{SR}_5(X) &= f_1(X) \\
\mathbf{SR}_4(X) &= f_2(X) \\
\mathbf{SR}_3(X) &= -4J\,X^3 + 6G\,X^2 - 4M\,X + M_3 \\
\mathbf{SR}_2(X) &= S_{22}\,X^2 + S_{21}\,X + S_{20} \\
\mathbf{SR}_1(X) &= S_{11}\,X + S_{10} \\
\mathbf{SR}_0(X) &= -8M_5(S_{11} - M_3S_{21}) \\
&\quad +32M_4(M_5S_{22} - M_4S_{20}) \\
&\quad -12M_6(S_{10} - 2M_3S_{20}) \\
&\quad +M_3^2(M_3^2 - 16MM_4 - 16JM_5 + 36GM_6)
\end{aligned}$$

όπου

$$\begin{aligned}
S_{22} &= 2\left[4J(M + 6J_1) - 9G^2\right] \\
S_{21} &= 2\left[6GM - J(16M_1 + M_3)\right] \\
S_{20} &= 8JM_4 - 3GM_3 \\
S_{11} &= -4S_{22}(6M_2 + M_4) - 16M_1S_{21} + 8MS_{20} \\
&\quad +2[-JM_3(16M_1 - M_3) \\
&\quad +16M(M^2 - 6JM_2) - 32J^2M_5] \\
S_{10} &= 6M_6S_{22} - (16M_1 + M_3)S_{20} \\
&\quad -8M(MM_3 - 6JM_6)
\end{aligned}$$

και

$$\begin{aligned}
J &= a_1b_2 - a_2b_1 & K &= a_1c_2 + a_2c_1 - 2b_1b_2 \\
J_1 &= b_1c_2 - b_2c_1 & G &= a_1c_2 - a_2c_1 \\
M &= a_1d_2 - a_2d_1 & M_1 &= b_1d_2 - b_2d_1 \\
M_2 &= c_1d_2 - c_2d_1 & M_3 &= a_1e_2 - a_2e_1 \\
M_4 &= b_1e_2 - b_2e_1 & M_5 &= d_1e_2 - d_2e_1 \\
M_6 &= c_1e_2 - c_2e_1
\end{aligned}$$

Έχουμε θεωρήσει όλα τα δυνατά σημεία διαχωρισμού των α και β και όλες τις δυνατές αποτιμήσεις της ακολουθίας $\mathbf{SR}(f_1, f_2)$ πάνω σε αυτά. Θεωρούμε όλες τις δυνατές αποτιμήσεις της ακολουθίας ως ένα (τριαδικό) δένδρο, το οποίο έχει ως κόμβους τις αποτιμήσεις ενός πολυωνύμου της ακολουθίας πάνω σε ένα από τα άκρα και το οποίο διακλαδώνεται ανάλογα με το πρόσημο της αποτίμησης. Μπορούμε να προϋπολογίσουμε όλα τα δυνατά αποτελέσματα και σε αρκετές περιπτώσεις να αποφασίσουμε για το αποτέλεσμα πριν φτάσουμε στα φύλλα του δένδρου. Στο σημείο αυτό πρέπει να τονίσουμε ότι οι αλγόριθμοι που προτείνουμε παράγονται αυτόματα με κώδικα που έχουμε γράψει στο MAPLE.

Ο μέγιστος αλγεβρικός βαθμός των συντελεστών των πολυωνύμων της ακολουθίας $\mathbf{SR}(f_1, f_2)$ είναι 8. Προκειμένου να υπολογίσουμε το τον μέγιστο αλγεβρικό βαθμό που απαιτείται για την σύγκριση πρέπει να θεωρήσουμε την αποτίμηση της ακολουθίας πάνω σε σημεία διαχωρισμού.

Θεώρημα 5.16

Υπάρχει αλγόριθμος που συγκρίνει δύο αλγεβρικούς αριθμούς βαθμού 4 και ο μέγιστος αλγεβρικός βαθμός των ποσοτήτων που εμφανίζονται είναι 14.

Απόδειξη: Προκειμένου να συγκρίνουμε δύο ρίζες δύο τεταρτοβάθμιων πολυωνύμων, χρησιμοποιώντας τον αλγόριθμο COMPARE αποτιμούμε την ακολουθία υπο-επιλυουσών πάνω σε δύο σημεία διαχωρισμού.

Τα σημεία διαχωρισμού δεν είναι ρητοί αριθμοί αλλά περιέχουν τετραγωνικές ρίζες και τα πολυώνυμα που τους ορίζουν έχουν συντελεστές με αλγεβρικό βαθμό 2, ως προς τους συντελεστές του αρχικού πολυωνύμου, δείτε Εξ. (5.18). Συνεπώς, πρέπει να αποτιμήσουμε την ακολουθία υπο-επιλυουσών, πάνω σε αλγεβρικούς αριθμούς. Αυτό που χρειαζόμαστε δεν είναι η αποτίμηση αλλά το πρόσημο της αποτίμησης, το οποίο μπορούμε να το υπολογίσουμε με τους αλγορίθμους της Εν. 5.4. Κατά συνέπεια, υπάρχει αλγόριθμος.

Όσον αφορά το μέγιστο αλγεβρικό βαθμό που εμφανίζεται, εργαζόμαστε ως εξής. Η χειρότερη περίπτωση είναι όταν θέλουμε το πρόσημο των πολυωνύμων της $\mathbf{SR}$ όταν αποτιμηθεί πάνω στους σ_1 ή σ_2. Έστω ότι μας ενδιαφέρει ο σ_1. Ο μέγιστος αλγεβρικός βαθμός εμφανίζεται κατά τον υπολογισμό της αποτίμησης του $\mathbf{SR}_1$. Ο αλγεβρικός βαθμός των συντελεστών του $\mathbf{SR}_1(X)$ είναι 6. Ισχύει $\mathtt{deg}(\mathbf{SR}_1) = 1$, οπότε ο υπολογισμός του $\mathtt{sign}(\mathbf{SR}_1(\sigma_1))$ είναι ισοδύναμος με τον υπολογισμό του προσήμου του A_1, που ορίζει τον σ_1, όταν αποτιμηθεί πάνω στη ρίζα του $\mathbf{SR}_1$. Αυτή η αποτίμηση έχει αλγεβρικό βαθμό 14, ο οποίος είναι και ένα άνω φράγμα για τον αλγόριθμό μας. ΟΕΔ

Παρατηρείστε ότι $\mathtt{deg}(\mathtt{res}(f_1, f_2)) = \mathtt{deg}(\mathbf{SR}_0) = 8$.

Όπως αναφέρθηκε στην Εν. 2.2, η επιλύουσα είναι η ικανή και αναγκαία συνθήκη που εξασφαλίζει ότι δύο πολυώνυμα έχουν κοινή ρίζα. Μάλιστα όσον αφορά τον αλγεβρικό βαθμό είναι η ελάχιστη συνθήκη, ή διαφορετικά είναι η ελάχιστη συνθήκη για επιλυσιμότητα. Ωστόσο, δεν είναι γνωστό αν είναι και η ελάχιστη συνθήκη για την σύγκριση δύο πραγματικών ριζών δύο πολυωνύμων. Διατυπώνουμε το ακόλουθο ισχυρισμό.

Ισχυρισμός 5.17 (Ελάχιστη συνθήκη για σύγκριση). *Προκειμένου να συγκρίνουμε δύο ρίζες δύο πολυωνυμικών εξισώσεων, το φράγμα στον αλγεβρικό βαθμό των εξεταζόμενων ποσοτήτων που προκύπτει από την επιλύουσα των δύο πολυωνύμων δεν είναι πάντοτε σφιχτό.*

Ή διαφορετικά, η επιλύουσα είναι η ελάχιστη συνθήκη για την επιλυσιμότητα αλλά όχι η ελάχιστη συνθήκη για την σύγκριση πραγματικών αλγεβρικών αριθμών.

5.4 Ο υπολογισμός προσήμου

Με τον όρο υπολογισμό προσήμου αναφερόμαστε στον υπολογισμό του προσήμου της αποτίμησης ενός πολυωνύμου πάνω σε ένα αλγεβρικό αριθμό. Στο παρόν κεφάλαιο ο αλγεβρικός αριθμός είναι βαθμού ≤ 4. Για τον υπολογισμό χρησιμοποιούμε τον αλγόριθμο SIGN_AT (Αλγ. 16), ο οποίος, όπως και ο αλγόριθμος COMPARE της προηγούμενης παραγράφου, χρειάζεται την αποτίμηση μιας ακολουθίας υποαπαλοιφουσών πάνω σε δύο ρητά σημεία.

Ωστόσο το $\mathcal{IDS}$ μας επιτρέπει, εκτός από τον υπολογισμό του προσήμου, να αντιμετωπίσουμε ένα ακόμα πιο γενικό πρόβλημα, το πρόβλημα της απαλοιφής ποσοδεικτών (quantifier elimination). Στα προβλήματα απαλοιφής ποσοδεικτών η είσοδος είναι φόρμουλες του τύπου $\exists x(P)$,

όπου το P είναι ένας συνδυασμός από πολυωνυμικές εξισώσεις και ανισώσεις στο x και άλλες ελεύθερες (free variables) μεταβλητές $y_1, \ldots, y_n$. Για κάποιες καθορισμένες πραγματικές τιμές των $y_1, \ldots, y_n$ το σύνολο S των πραγματικών τιμών του x που ικανοποιούν την P είναι η ένωση ξένων μεταξύ τους διαστημάτων. Τα άκρα των αυτών των διαστημάτων είναι οι πραγματικές ρίζες κάποιων πολυωνύμων του P και των $\pm\infty$. Συνεπώς προκειμένου να ελέγξουμε εάν το S είναι κενό ή όχι αρκεί να ελέγξουμε αν μία από αυτές τις ρίζες, ή το $\pm\infty$ ανήκει στο S. Αυτοί οι υπολογισμοί μπορούν να εκφραστούν ως πεπερασμένες συζεύξεις και διαζεύξεις από φόρμουλες $P[\alpha/x]$ όπου οι εκφράσεις α, που εξαρτώνται από τα $y_1, \ldots, y_n$ έχουν αντικαταστήσει το x στο P. Η μέθοδος αυτή είναι γνωστή ως *εικονική αντικατάσταση* (virtual substitution) [179, 267, 268, 269, 270].

Χρησιμοποιώντας τις φόρμουλες χωρίς ποσοδείκτες μπορούμε να παράγουμε αλγορίθμους για την αποτίμηση προσήμου οι οποίοι δεν περιέχουν βρόγχους (straight-line programs). Καθώς το πρόβλημα της απαλοιφής ποσοδεικτών είναι πιο γενικό, είναι αυτό το οποίο θα παρουσιάσουμε.

Ο βαθμός 2

Αποδεικνύεται ότι για την επίλυση του προβλήματος

$$(\exists x \in \mathbb{R})[f(x) := a_2\, x^2 + a_1\, x + a_0 \wedge (g(x)\, \rho\, 0)]$$

όπου $a_2 > 0$ και $\rho \in \{>, =, <\}$ αρκεί να επιλύσουμε όλα τα προβλήματα απαλοιφής ποσοδεικτών όπου $\deg(g) \leq 1$. Συνεπώς η είσοδος είναι ένα πολυώνυμο f βαθμού 2 και ένα πολυώνυμο g και τα δύο με συντελεστές παραμέτρους.

Έστω $g = b_1 X + b_0 \in \mathbb{R}[X]$, $\deg(g) \geq 1$ και $b_1 \geq 0$. Ο στόχος μας είναι να υπολογίσουμε τύπους χωρίς ποσοδείκτες της μορφής $\phi_{n,i,j,s}$, όπου n είναι ο βαθμός του g (στην περίπτωσή μας είναι $n \leq 1$), i είναι ο τύπος της f (από την Πρότ. 5.4), j είναι η πραγματική ρίζα του f που μας ενδιαφέρει (η μικρότερη πραγματική ρίζα έχει δείκτη 1) και $s \in \{-1, 0, +1\}$ περιγράφει το πρόσημο του g πάνω στη ρίζα j.

Αν $n = \deg(g) = 0$, δηλαδή $g = b_0$ τότε

$$\begin{aligned} \psi_{0,?,?,-1} &:= b_0 < 0 \\ \psi_{0,?,?,0} &:= b_0 = 0 \\ \psi_{0,?,?,+1} &:= b_0 > 0 \end{aligned}$$

όπου το ? σημαίνει ότι η φόρμουλα ισχύει για οποιοδήποτε τύπο και ρίζα του f.

Έστω $n = 1$. Θεωρούμε $p = -\frac{a_1}{2a_2}$ και $\beta = -\frac{b_0}{b_1}$. Σύμφωνα με την Πρότ. 5.4 διακρίνουμε τις ακόλουθες περιπτώσεις για τον τύπο του f:

(1) Δεν έχουμε πραγματικές ρίζες.

(2) Το f έχει μια διπλή πραγματική ρίζα, την $\alpha = p$. Συνεπώς $\mathrm{sign}(g(\gamma)) = \mathrm{sign}(g(p)) = \mathrm{sign}(g(-\frac{a_1}{2a_2})) = \mathrm{sign}(J)$, όπου $J = -b_1 a_1 + 2\, b_0 a_2$. Οι τύποι χωρίς ποσοδείκτες είναι

$$\begin{aligned} \psi_{1,2,1,-1} &:= g[p/x] > 0 \\ \psi_{1,2,1,0} &:= g[p/x] = 0 \\ \psi_{1,2,1,+1} &:= g[p/x] > 0 \end{aligned}$$

(3) Διακρίνουμε δύο περιπτώσεις ανάλογα με το ποια πραγματική ρίζα, έστω α, του f ενδιαφερόμαστε. Πιο συγκεκριμένα

i. Έστω $\alpha \cong (f, (-\infty, -\frac{a_1}{2a_2}))$
Αν $-\frac{b_0}{b_1} \geq -\frac{a_1}{2a_2}$ τότε $\mathrm{sign}(g(\alpha)) = -1$. αλλιώς $\mathrm{sign}(g(\gamma)) = -\mathrm{sign}(f(-\frac{b_0}{b_1}))$. Δηλαδή ελέγχουμε αρχικά αν $p \leq \beta$ και αν όχι υπολογίζουμε το πρόσημο του $f(p)$. Οι τύποι χωρίς ποσοδείκτες είναι

$$\begin{aligned}
\psi_{1,3,1,-1} &:= g[p/x] \leq 0 \vee f[\beta/x] < 0 \\
\psi_{1,3,1,0} &:= g[p/x] < 0 \vee f[\beta/x] = 0 \\
\psi_{1,3,1,+1} &:= g[p/x] > 0 \vee f[\beta/x] > 0
\end{aligned}$$

ii. Έστω $\alpha \cong [f, (-\frac{a_1}{2a_2}, \infty)]$ Αν $-\frac{b_0}{b_1} \leq -\frac{a_1}{2a_2}$ τότε $\mathrm{sign}(g(\alpha)) = 1$. αλλιώς $\mathrm{sign}(g(\gamma)) = -\mathrm{sign}(f(-\frac{b_0}{b_1}))$. Οι φόρμουλες χωρίς ποσοδείκτες είναι

$$\begin{aligned}
\psi_{1,3,2,-1} &:= g[p/x] \leq 0 \vee f[\beta/x] < 0 \\
\psi_{1,3,2,0} &:= g[p/x] < 0 \vee f[\beta/x] = 0 \\
\psi_{1,3,2,+1} &:= g[p/x] > 0 \vee f[\beta/x] > 0
\end{aligned}$$

Στη συνέχεια θα καταρρίψουμε την υπόθεση ότι το g είναι βαθμού ≤ 1 και ότι ο μεγιστοβάθμιος όρος είναι θετικός.

Έστω $n > 0$, και $b^* = \mathrm{lead}\,(g)$, $g^* = g - b^* x^n$ και $g^{**} = \mathrm{rem}\,(a^m g, f)$, όπου m είναι ο ο μικρότερος άρτιος μεγαλύτερος από $n-2$. Έστω $\sigma^*_{n-1,i,j,s}(\sigma^{**}_{2,i,j,s})$ η φόρμουλα $\sigma_{n-1,i,j,s}(\sigma_{2,i,j,s})$ κατασκευασμένη ως προς το πολυώνυμο g^* (ως προς το πολυώνυμο g^{**}) αντί για το πολυώνυμο g.

Για $n = 1$ έστω $\psi^-_{n,i,j,s}$ είναι η φόρμουλα $\psi_{n,i,j,s}$ ως προς το πολυώνυμο $-g$ αντί του g. Τότε

$$\sigma_{n,i,j,s} := (a^* = 0 \wedge \sigma^*_{n-1,i,j,s}) \vee (a^* > 0 \wedge \psi_{n,i,j,s}) \vee (a^* < 0 \wedge \psi^-_{n,i,j,s})$$

Για $n \geq 2$ θέτουμε $\sigma_{n,i,j,s} := \sigma^{**}_{2,i,j,s}$.

Προκειμένου να υλοποιήσουμε τον παραπάνω αλγόριθμο, έχουμε υπολογίσει συμβολικά όλες τους τύπους χωρίς ποσοδείκτες και όταν μας ζητείται να αποφασίσουμε για κάποιο συγκεκριμένο πρόβλημα, αντικαθιστούμε τις τιμές των παραμέτρων και αποφασίζουμε ανάλογα το πρόσημο των διαφόρων ποσοτήτων.

Το πρώτο ερώτημα που γεννάται αφορά την ποιότητα των παρουσιαζόμενων αλγορίθμων. Αν θεωρήσουμε ως μέτρο το μέγιστο αλγεβρικό βαθμό που εμφανίζεται τότε παρατηρούμε ότι αυτός είναι 3, στην χειρότερη περίπτωση. Για παράδειγμα κατά τον υπολογισμό $f[\beta/x]$. Ο αλγεβρικός βαθμός της επιλύουσας των f και g (αν $\deg(g) \leq 1$), η οποία είναι $b_1^2\, a_0 - b_0\, b_1\, a_1 + b_0^2\, a_2$, είναι επίσης 3. Καθώς η επιλύουσα είναι η απαραίτητη (και βέλτιστη) συνθήκη επίλυσης συμπεραίνουμε ότι ο αλγόριθμος που παρουσιάσαμε είναι βέλτιστος ως προς τον αλγεβρικό βαθμό.

Επίσης βέλτιστοι, κατά την ίδια έννοια είναι και οι αλγόριθμοι για τους βαθμούς 3 και 4.

Ο βαθμός 3 και 4

Από την προηγούμενη παράγραφο είναι σαφές ότι ο βασικός υπολογισμός είναι ο υπολογισμός του προσήμου της αποτίμησης ενός πολυωνύμου πάνω σε ένα αλγεβρικό αριθμό. Οι φόρμουλες για τον βαθμό 3 και 4 είναι πολύ μακροσκελείς και δεν θα τις παρουσιάσουμε αναλυτικά. Θα παρουσιάσουμε όμως αναλυτικά τον τρόπο με τον οποίο κατασκευάζονται. Πιο συγκεκριμένα θα παρουσιάσουμε πως μπορούμε να υπολογίσουμε συμβολικά όλες τις ποσότητες που χρειάζονται για να υπολογίσουμε το πρόσημο ενός πολυωνύμου πάνω σε έναν αλγεβρικό αριθμό βαθμού 3. Η επέκταση σε βαθμό 4 είναι άμεση.

Έστω $\gamma \cong (f, (\mathsf{a}, \mathsf{b}))$, όπου $f = a_3X^3 + a_2X^2 + a_1X + a_0$, $g = b_2X^2 + b_1X + b_0$ και $a_3b_2 \neq 0$. Θέλουμε να υπολογίσουμε το $sign[g(\gamma)]$.

Υπολογίζουμε την προσημασμένη ακολουθία υποεπιλυουσών των f και g, η οποία είναι

$$\begin{array}{lcl} \mathbf{SR}_3 & = & f \\ \mathbf{SR}_2 & = & \mathbf{sr}_{22}X^2 + \mathbf{sr}_{21}X + \mathbf{sr}_{20} \\ \mathbf{SR}_1 & = & \mathbf{sr}_{11}X + \mathbf{sr}_{10} \\ \mathbf{SR}_0 & = & \mathbf{sr}_0 \end{array} \tag{5.29}$$

όπου

$$\begin{array}{lcl} \mathbf{sr}_{22} & = & K_1 \\ \mathbf{sr}_{21} & = & K_2 \\ \mathbf{sr}_{20} & = & K_3 \\ \mathbf{sr}_{11} & = & -K_1K_7 + K_2K_6 \\ \mathbf{sr}_{10} & = & -K_1K_4 + K_3K_6 \\ \mathbf{sr}_0 & = & -K_1K_7K_5 + K_1K_4K_8 - K_6K_3K_8 + K_6K_2K_5 - K_7K_2K_4 + K_3{K_7}^2 \end{array} \tag{5.30}$$

όπου $K_i, 1 \leq i \leq 8$ είναι τα στοιχεία του πίνακα Bézout των f και g, δηλαδή

$$\begin{pmatrix} K_1 & K_2 & K_3 \\ K_6 & K_7 & K_4 \\ K_7 & K_8 & K_5 \end{pmatrix} = \begin{pmatrix} b_2 & b_1 & b_0 \\ a_3b_1 - b_2a_2 & b_0a_3 - b_2a_1 & -b_2a_0 \\ b_0a_3 - b_2a_1 & b_0a_2 - b_2a_0 - a_1b_1 & -a_0b_1 \end{pmatrix} \tag{5.31}$$

Ας θεωρήσουμε τον υπολογισμό

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathbf{sr}_{22} & \mathbf{sr}_{21} & \mathbf{sr}_{20} \\ 0 & 0 & \mathbf{sr}_{11} & \mathbf{sr}_{10} \\ 0 & 0 & 0 & \mathbf{sr}_0 \end{pmatrix} \begin{pmatrix} a^3 & b^3 \\ a^2 & b^2 \\ a & b \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{SR}_3(a) & \mathbf{SR}_3(b) \\ \mathbf{SR}_2(a) & \mathbf{SR}_2(b) \\ \mathbf{SR}_1(a) & \mathbf{SR}_1(b) \\ \mathbf{SR}_0 & \mathbf{SR}_0 \end{pmatrix} = (M_1 \quad M_2) = M \tag{5.32}$$

ο οποίος περιγράφει την αποτίμηση της ακολουθίας $\mathbf{SR}(f, g)$ πάνω στα a και b. Η πρώτη στήλη του M περιέχει την $\mathbf{SR}(f, g\,;\, \mathsf{a})$ και η δεύτερη την $\mathbf{SR}(f, g\,;\, \mathsf{b})$. Αν μετρήσουμε τις εναλλαγές προσήμων στην πρώτη στήλη ($\mathtt{VAR}(M_1)$) και στη δεύτερη ($\mathtt{VAR}(M_2)$) τότε $sign(g(\gamma)) = \mathtt{VAR}(M_1) - \mathtt{VAR}(M_2)$ σύμφωνα με τον Αλγ. 16. Όλοι οι δυνατοί συνδυασμοί προσήμων είναι $\leq 2 \times 3^5 = 486$, αν και δεν είναι όλοι εφικτοί.

Με την ίδια διαδικασία υπολογίζουμε συμβολικά τις απαιτούμενες ποσότητες για τον βαθμό 4.

5.5 Αποτίμηση προσήμου σε δύο μεταβλητές

Θέλουμε να υπολογίσουμε το πρόσημο του πολυωνύμου $f(X)$

$$f(X,Y) = r\,X^2 + s\,Y^2 + t\,X\,Y + u\,X + v\,Y + w. \tag{5.33}$$

όταν το αποτιμήσουμε πάνω σε δύο αλγεβρικούς αριθμούς $\gamma_x \cong (P_x, \mathcal{I}_x)$ και $\gamma_y \cong (P_y, \mathcal{I}_y)$ οι οποίοι είναι βαθμού ≤ 4.

Για τον υπολογισμό του προσήμου θα χρησιμοποιήσουμε τον Αλγ. 17. Επειδή ο βαθμός των εμπλεκομένων ποσοτήτων είναι μικρός ≤ 2, μπορούμε να υπολογίσουμε συμβολικά όλες τις ποσότητες που χρειαζόμαστε.

Ας θεωρήσουμε το ακόλουθο παράδειγμα

$$\begin{array}{l} \gamma_x \cong [P_x, \mathcal{I}_x] \\ \gamma_y \cong [P_y, \mathcal{I}_y] \\ P_x(X) = a_2\,X^2 + a_1\,X + a_0 \\ P_y(Y) = b_4\,Y^4 + b_3\,Y^3 + b_2\,Y^2 + b_1\,Y + b_0 \end{array} \tag{5.34}$$

Η προσημασμένη ακολουθία $\mathbf{SR}(P_x, f)$ είναι

$$\begin{array}{lcl} \mathbf{SR}_3(X) & = & P_x \\ \mathbf{SR}_2(X) & = & f \\ \mathbf{SR}_1(X) & = & S_{21}\,X + S_{20} \\ \mathbf{SR}_0(X) & = & -r(S_{34}\,\gamma_y^4 + S_{33}\,\gamma_y^3 + S_{32}\,\gamma_y^2 + S_{31}\,\gamma_y + S_{30}) \end{array} \tag{5.35}$$

όπου

$$\begin{array}{lcl} S_{21} & = & r(a_2\,t\,\gamma_y + a_2\,u - r\,a_1) \\ S_{20} & = & r(a_2\,s\,\gamma_y^2 - r\,a_0 + a_2\,v\,\gamma_y + a_2\,w) \\ S_{34} & = & {a_2}^2\,s^2 \\ S_{33} & = & -a_1\,a_2\,t\,s + 2\,a_2^2\,s\,v \\ S_{32} & = & a_0 a_2 t^2 - a_1 a_2 t v - a_1 a_2 u s + r {a_1}^2 s + {a_2}^2 v^2 - 2\,a_2 s r a_0 + 2\,{a_2}^2 s w \\ S_{31} & = & -2\,a_2 r a_0 v - a_1 t r a_0 - a_1 a_2 t w - a_1 a_2 u v + r {a_1}^2 v + 2\,a_0 a_2 t u + 2\,{a_2}^2 v w \\ S_{30} & = & -2\,a_2 r a_0 w - a_1 a_2 u w + r {a_1}^2 w - a_1 u r a_0 + {a_2}^2 w^2 + r^2 {a_0}^2 + a_0 a_2 u^2 \end{array} \tag{5.36}$$

Αποτιμούμε την $\mathbf{SR}(P_x, f)$ πάνω στο αριστερό (δεξί) άκρο του $\mathcal{I}_x$ και προκύπτουν πολυώνυμα σε μία μεταβλητή ως προς y. Προκειμένου να υπολογίσουμε το πρόσημό τους εφαρμόζουμε τους αλγορίθμους υπολογισμού προσήμου σε μία μεταβλητή από την Παρ.5.4.

Σύστημα δύο μεταβλητών βαθμού 2

$$\begin{array}{l} f_1(X,Y) = r_1\,X^2 + s_1\,Y^2 + t_1\,X\,Y + u_1\,X + v_1\,Y + w_1 \\ f_2(X,Y) = r_2\,X^2 + s_2\,Y^2 + t_2\,X\,Y + u_2\,X + v_2\,Y + w_2 \end{array} \tag{5.37}$$

Θεωρούμε το σύστημα $f_1 = f_2 = 0$, όπου $f_{1,2} \in \mathbb{Z}[X,Y]$ είναι συνολικού βαθμού το πολύ 2. Θα υποθέσουμε ότι σύστημα έχει πεπερασμένο αριθμό (μιγαδικών) λύσεων. Αυτό μπορούμε

εύκολα να το διαπιστώσουμε καθώς οι απαλοίφουσες που υπολογίζουμε παρακάτω δεν θα είναι πολυώνυμα μιας μεταβλητής.

Οι πραγματικές λύσεις του συστήματος είναι σημεία στον $\mathbb{R}^2$.

Προκειμένου να υπολογίσουμε το σύστημα υπολογίζουμε $R_x = \mathtt{res}_x(f_1, f_2) \in \mathbb{Z}[X]$ και $R_y = \mathtt{res}_y(f_1, f_2) \in \mathbb{Z}[Y]$ απαλείφοντας τα Y και X αντίστοιχα. Παρατηρούμε ότι $\deg(R_x) \leq 4$ και $\deg(R_y) \leq 4$.

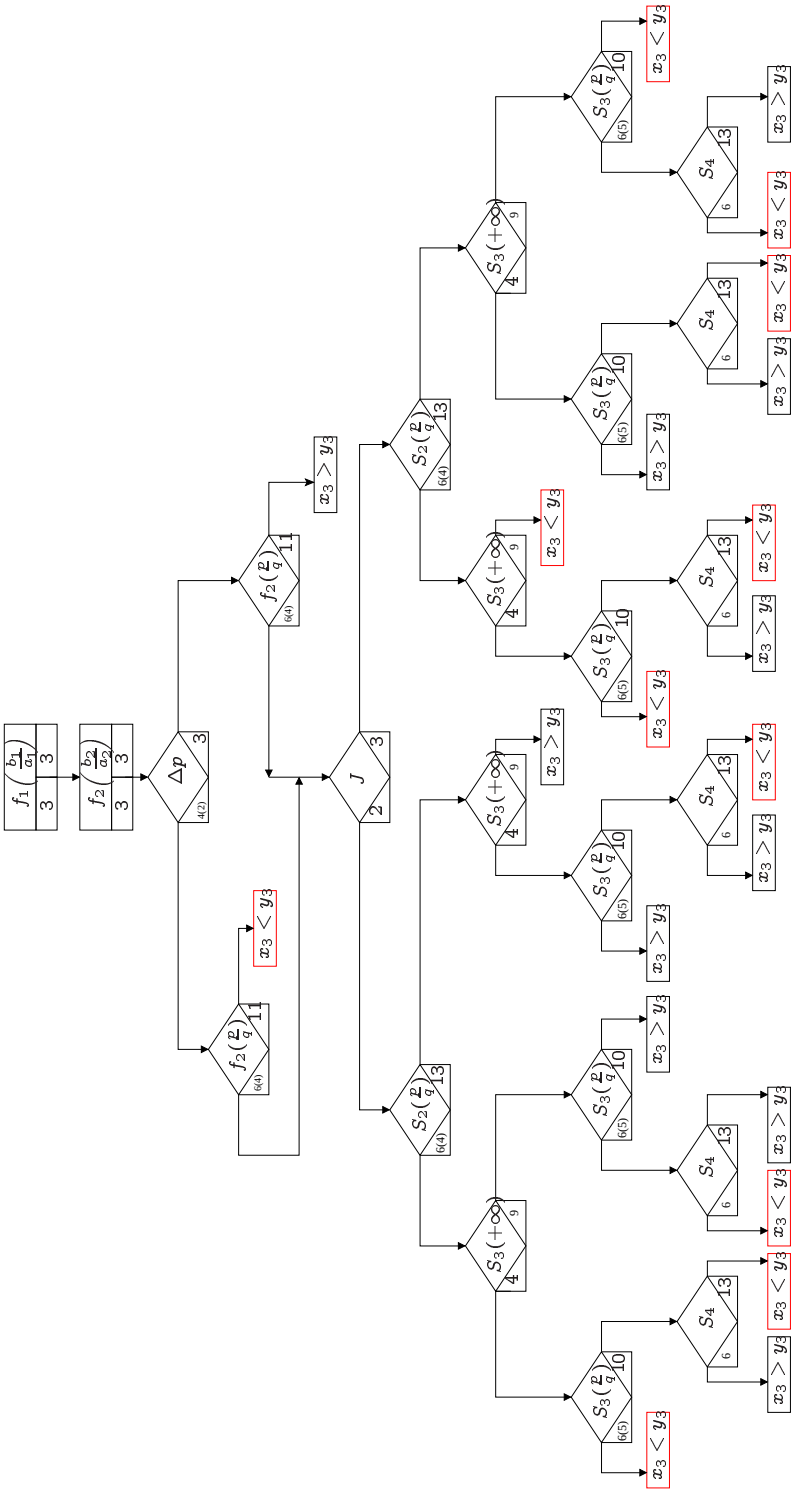
Αν απομονώσουμε τις πραγματικές ρίζες των R_x και R_y τότε τα σημεία σημεία διαχωρισμού των πραγματικών τους ριζών ορίζουν ένα πλέγμα στο πραγματικό επίπεδο, στα κελλιά του οποίου περιέχονται οι πραγματικές λύσεις του συστήματος. Το πλέγμα έχει από 1 έως 4 στήλες και αντίστοιχα από 1 έως 4 γραμμές. Αν το R_x δεν έχουν πολλαπλές ρίζες τότε μπορούμε πολύ εύκολα να υπολογίσουμε το ταίριασμα των αλγεβρικών αριθμών, καθώτι το σύστημα είναι σε γενική θέση. Η δύσκολη περίπτωση για τον γενικό αλγόριθμο είναι όταν υπάρχουν πολλαπλές ρίζες. Ωστόσο από το $\mathcal{IDS}$ συμπεραίνουμε ότι σε αυτή την περίπτωση οι λύσεις είναι ρητοί αριθμοί και άρα μπορούμε πιο εύκολα να υπολογίσουμε το ταίριασμα.

Η μόνη δύσκολη περίπτωση είναι όταν και το R_x και R_y είναι βαθμού 4 και τύπου (6). Σε αυτή την περίπτωση το σύστημα μπορεί να έχει είτε 4 απλές λύσεις είτε δύο λύσεις με πολλαπλότητα 2. Μόνο σε αυτή την περίπτωση χρησιμοποιούμε την συνάρτηση SIGN_AT.

5.6 Σύνοψη – Μελλοντικές επεκτάσεις

Παρουσιάσαμε αλγορίθμους για την απομόνωση πραγματικών ριζών ακέραιων πολυωνύμων βαθμού ≤ 4 και αλγορίθμους για την σύγκριση και την αποτίμηση προσήμου πραγματικών αλγεβρικών αριθμών, βαθμού ≤ 4. Τέλος, επιλύσαμε πολυωνυμικά συστήματα σε δύο μεταβλητές βαθμού ≤ 2.

Υπάρχουν ρητά σημεία διαχωρισμού των πραγματικών ριζών πολυωνύμων βαθμού ≤ 9 τα οποία να υπολογίζονται σε σταθερό χρόνο;



Σχήμα 5.4: Σύγκριση των μεγαλύτερων ριζών δύο κυβικών πολυωνύμων

Ο αλγόριθμος υπολογισμού $x_3 \diamond y_3$ όπου $\diamond \in \{<, >\}$ και x_3 και y_3 είναι οι δύο μεγαλύτερες ρίζες δύο κυβικών πολυωνύμων. Στους ρόμβους παρουσιάζονται οι ποσότητες των οποίων το πρόσημο πρέπει να υπολογιστεί. Κάτω αριστερά είναι ο αλγεβρικός βαθμός και κάτω δεξιά ο αριθμός των πράξεων που απαιτούνται.

ΚΕΦΑΛΑΙΟ 6

Περί της υλοποίησης

Η διαφορά της θεωρίας από την πράξη είναι πολύ μικρή στη θεωρία αλλά πολύ μεγάλη στην πράξη.

Yoggi Bara

The asymptotically best algorithms frequently turn out to be worst on all problems for which they are used.

D. G. Cantor and
H. Zassenhauss [48]

Περίληψη

Παρουσιάζουμε την υλοποίηση και πειραματικά αποτελέσματα σχετικά με την επίλυση ακέραιων πολυωνύμων και πολυωνυμικών συστημάτων σε δύο μεταβλητές.

Το σύνολο σχεδόν των υλοποιήσεων έχει πραγματοποιηθεί σε C++ και αποτελεί μέρος της βιβλιοθήκης SYNAPS. Ο σχεδιασμός του λογισμικού έχει παρουσιαστεί στην εργασία [204] και μέρος των πειραματικών αποτελεσμάτων στις εργασίες [88, 92, 97].

Υπάρχει διάχυτη η ψευδαίσθηση ότι η υλοποίηση αλγορίθμων είναι μια εύκολη, ή στην καλύτερη περίπτωση, μια όχι και τόσο επιστημονική διαδικασία. Μάλιστα, αυτό πιστεύεται ότι ισχύει για οποιαδήποτε γλώσσα προγραμματισμού.

Ωστόσο, τουλάχιστον για τους επιστημονικούς υπολογισμούς, οι λεπτομέρειες της υλοποίησης και του σχεδιασμού είναι εξίσου σημαντικές με την θεωρητική ανάλυση των προβλημάτων. Για παράδειγμα εγείρονται ερωτήματα, όπως: Ποιά είναι η βέλτιστη δομή δεδομένων για την

υλοποίηση των πολυωνύμων; Πίνακας, στοίβα, σωρός, κατακερματισμένος πίνακας; Ποιός είναι ο βέλτιστος (στην πράξη) αλγόριθμος για πολλαπλαπλασιασμό πολυωνύμων; Ποιός είναι ο βέλτιστος αλγόριθμος για τον υπολογισμό πολυωνυμικών ακολουθιών υπολοίπων; Η αριθμητική στους αλγεβρικούς αλγορίθμους πρέπει να βασίζεται σε αριθμούς κινητής υποδιαστολής απεριόριστης ακρίβειας ή σε ακεραίους απεριόριστης ακρίβειας; Προφανώς ο κατάλογος των ερωτημάτων είναι πολύ μακρύς και απάντησή τους απαιτεί ενδελεχή θεωρητική και πειραματική μελέτη.

Αναφέρουμε απλά ότι ένα από τα σημαντικότερα ανοιχτά προβλήματα, στην επιστημονική περιοχή των αλγεβρικών αλγορίθμων, όπως αναφέρει ο Kaltofen [143], είναι το αν είναι εφικτές υλοποιήσεις των βέλτιστων θεωρητικά αλγορίθμων τέτοιες ώστε να τους καθιστούν και βέλτιστους στην πράξη. Το πιο γνωστό πρόβλημα που εμπίπτει σε αυτή την κατηγορία είναι ο πολλαπλασιασμός πινάκων.

Στόχος του κεφαλαίου είναι να δείξει ότι οι σύγχρονες τεχνικές προγραμματισμού, καθιστούν τους αλγορίθμους πραγματικής επίλυσης και υπολογισμών με πραγματικούς αλγεβρικούς αριθμούς, όχι μόνο ικανοποιητικούς στην πράξη αλλά και ανταγωνιστικούς, και μερικές φορές υπέρτερους, των προσεγγιστικών αλγορίθμων της αριθμητικής ανάλυσης.

Λίγα λόγια για τον πηγαίο κώδικα

Θα παρουσιάσουμε τα βασικά σημεία της υλοποίησης σε C++ των αλγορίθμων για επίλυση στους πραγματικούς και υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς, δηλαδή των αλγορίθμων των Κεφαλαίων 3 και 4. Υποθέτουμε ότι αναγνώστης έχει γνώσεις του συνταντικού και ιδιωμάτων της C++. Το σύνολο των υλοποιήσεων που θα παρουσιάσουμε είναι μέρος της βιβλιοθήκης SYNAPS [1] [75, 204], η οποία είναι μια βιβλιοθήκη, ανοιχτού λογισμικού, σε C++ για αλγεβρικούς και αριθμητικούς υπολογισμούς. Ο πυρήνας της βιβλιοθήκης παρέχει δομές δεδομένων και κλάσεις για τα βασικά αντικείμενα αλγεβρικών υπολογισμών, όπως για παράδειγμα διανύσματα, πίνακες (πυκνούς, αραιούς, δομημένους), πολυώνυμα σε μία και πολλές μεταβλητές, λίστες. Επίσης, υπάρχουν υλοποιημένοι πολλοί αλγόριθμοι για την επίλυση πολυωνύμων σε μία μεταβλητή και πολυωνυμικών συστημάτων με οποιοδήποτε αριθμό μεταβλητών και για υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς και σύνδεση με την βιβλιοθήκη LAPACK για υπολογισμούς της γραμμικής άλγεβρας.

Τόσο η υλοποίησή μας, όσο και το σύνολο των υλοποιήσεων της SYNAPS, ακολουθούν το παράδειγμα του γενικευμένου προγραμματισμού και υιοθετούν σύγχρονες προγραμματιστικές της C++ για τους επιστημονικούς υπολογισμούς. Όπως για παράδειγμα τον στατικό πολυμορφισμό (static polymorphism), τα πρότυπα εκφράσεων (expression templates) και τα πρότυπα μεταπρογραμμάτων (template metaprograms). Ο αναγνώστης που ενδιαφέρεται για αυτές τις τεχνικές και για τη θεωρία που τις ακολουθεί μπορεί να ανατρέξει στις εργασίες του Veldhuizen [259, 260], όπως και στις τεχνικές αναφορές στην ιστοσελίδα του[2].

Θα σκιαγραφήσουμε τα βασικά χαρακτηριστικά της υλοποίησης.

[1] www-sop.inria.fr/galaad/software/synaps/

[2] http://osl.iu.edu/ tveldhui/papers/techniques/

Η σημαντικότερη κλάση που έχουμε αναπτύξει αναφέρεται στην πραγματική επίλυση πολυωνύμων και πολυωνυμικών συστημάτων. Η βασική αφηρημένη (abstract) κλάση είναι η **SOLVER**. Μέρος της υλοποίησή της είναι:

```
template < class T >
struct SOLVER {
  typedef NumberTraits<T>::RT     RT;       // the Integer type
  typedef NumberTraits<T>::FT     FT;       // the Rational type
  typedef NumberTraits<T>::FIT    FIT;      // the interval type

  typedef UPolDse<T>              Poly;     // univariate polynomial type
  typedef UPolDse< UPolDse<T> >   Poly_2;   // bivariate polynomial type
  typedef root_of<T, Poly>        RO_t;     // algebraic number type
  ...
};
```

Η **SOLVER** παρέχει όλες τις απαραίτητες πληροφορίες που χρειαζόμαστε σχετικά με τους αριθμητικούς τύπους, τα πολυώνυμα και τους πραγματικούς αλγεβρικούς αριθμούς. Η βασική ιδέα είναι ότι ο χρήστης ή οι αλγόριθμοι συνάγουν όλους τους τύπους που χρειάζονται από την κλάση **SOLVER**. Η κλάση παραμετροποιείται, **T** στον κώδικα, με κάποιο τύπο που αντιστοιχεί στους ακεραίους αριθμούς. Στη συνέχεια με από την κλάση **NumberTraits** συνάγουμε όλους τους υπόλοιπους τύπους που ενδιαφέρουν, όπως τον τύπο για τους ρητούς αριθμούς, για τα διαστήματα με ρητά άκρα, για τα πολυώνυμα κ.ο.κ.

Προκειμένου να διαχωρίσουμε τους διάφορους αλγορίθμους επίλυσης, η κλάση που αντιστοιχεί σε κάθε έναν από αυτούς, κληρονομεί από τη SOLVER. Για παράδειγμα[3] έχουμε τις παρακάτω κλάσεις:

```
// Real solving using the algrorithm STURM
template < class T >
struct Sturm : public SOLVER<T>           {  };

// Real solving using the algrorithm CF
template < class T >
struct ContFrac : public SOLVER<T>        {  };

// Real solving using the algrorithm BERNSTEIN
template < class T >
struct Bernstein : public SOLVER<T>       {  };

template < class T >
struct IslBzBdgSturm : public SOLVER<T>   {  };

struct SlvBzStd : public SOLVER< double>  {  };

struct SlvBzBdg : public SOLVER<QQ>       {  };
```

[3] Η πραγματική υλοποίηση είναι λίγο πιο περίπλοκη, αλλά για λόγους παρουσίασης μπορούμε να τη θεωρήσουμε όπως παρουσιάζεται. Ο αναγνώστης μπορεί να ανατρέξει στο εγχειρίδειο της SYNAPS για μια πιο ακριβή περιγραφή.

Το πρότυπο της συνάρτησης για την επίλυση πολυωνύμων σε μία μεταβλητή είναι

```
template < class SLV >
Seq< typename SLV::RO_t >
Solve( typename SLV::Poly& f, SLV);
```

η οποία έχει ως είσοδο ένα πολυώνυμο f και μία κλάση επίλυσης και επιστρέφει μια λίστα με πραγματικούς αλγεβρικούς αριθμούς. Κάθε κλάση επίλυσης πρέπει να εξιδικεύσει (specialize) τη συνάρτηση **Solve**. Ένα παράδειγμα κώδικα για την επίλυση ενός πολυωνύμου με τη χρήση της κλάσης επίλυσης **Sturm** είναι:

```
#include <synaps/init.H>
#include <synaps/solve/Sturm.H>

typedef SYNAPS::ZZ            NT;
typedef SYNAPS::Sturm<NT>     SLV;

typedef SLV::RT             RT;
typedef SLV::FT             FT;
typedef SLV::Poly           Poly;
typedef SLV::RO_t           RO_t;

int main() {
  Poly f("3*x^7-4*x^3-2*x");
  SYNAPS::Seq<sol_t> sol = sol = SYNAPS::Solve( f, SLV());
%   std::cout << "Solutions: " << sol.size() << std::endl;
%   for (int j =0; j < sol.size(); ++j)
%     std::cout << j << ": " << sol[j] << std::endl;
}
```

και η έξοδος του προγράμματος είναι:

```
Solutions:
0: root_of( 1*x, 0 ) in [ 0,0 ], approx = 0
1: root_of( 3*x^6-4*x^2-2, 1 ) in [ -7/3,0 ], approx = -1.162548
2: root_of( 3*x^6-4*x^2-2, 2 ) in [ 0,7/3 ], approx = 1.16254858
```

Αντί για την κλάση **Sturm** θα μπορούσαμε να είχαμε χρησιμοποιήσει μια οποιαδήποτε άλλη κλάση επίλυσης από αυτές που παρουσιάσαμε προηγουμένως. Με όμοιο τρόπο ορίζεται και η συνάρτηση για την επίλυση ενός πολυωνυμικού συστήματος σε δύο μεταβλητές:

```
template < class SLV >
Seq< std::pair< typename SLV::RO_t, typename SLV::RO_t > >
Solve( typename SLV::Poly_2& f, typename SLV::Poly_2& g, SLV);
```

Όσον αφορά τους πραγματικούς αλγεβρικούς αριθμούς, κατασκευάζονται όταν επιλύουμε ένα πολυώνυμο με την συνάρτηση **Solve** και υποστηρίζονται και οι παρακάτω συναρτήσεις:

```
// comparison
template < class T, class Poly >
bool compare( const root_of<T, Poly>& a, const root_of<T, Poly>& b);
```

```
// sign evaluation in one variable
template < class T, class Poly >
int sign_at( const Poly& f, const root_of<T, Poly>& a);

// sign evaluation in two variables
template < class Poly_2, class T, class Poly >
int sign_at( const Poly_2& f, const root_of<T, Poly>& a,
                              const root_of<T, Poly>& b);
```

6.1 Πειραματικά αποτελέσματα

Στην παρούσα ενότητα θα παρουσιάσουμε πειραματικά αποτελέσματα σχετικά με την απομόνωση των πραγματικών ριζών ακέραιων πολυωνύμων και πολυωνυμικών συστημάτων με δύο μεταβλητές. Για την περίπτωση της μιας μεταβλητής τα πειράματα αφορούν πολυώνυμα βαθμού ≤ 4, προκειμένου να αναδείξουμε την (βέλτιστη) πρακτική συμπεριφορά των αλγορίθμων του Κεφ. 5 και πολυώνυμα αυθαίρετα μεγάλου βαθμού.

Συγκρίνουμε με διάφορες άλλες (γνωστές) υλοποιήσεις. Τη πρώτη φορά που αναφερόμαστε σε κάποιο λογισμικό δίνουμε και πληροφορίες για τους αλγορίθμους στους οποίους στηρίζεται και για τις ιδιαιτερότητές του.

Σε πολλά σημεία αναφέρουμε συμβολικές-αριθμητικές τεχνικές ή φίλτρα. Αυτές οι υλοποιήσεις προσπαθούν να εκτελέσουν τους υπολογισμούς αρχικά με αριθμητική βασισμένη σε **double** ή/και αριθμητική διαστημάτων, όπου **double** είναι ο τύπος δεδομένων που προσφέρεται για αριθμητική κινητής υποδιαστολής βασισμένη στην υπολογιστική μηχανή. Αν το αποτέλεσμα ή κάποιος ενδιάμεσος υπολογισμός δεν μπορεί να αναπαρασταθεί με **double** τότε ολόκληρος ο υπολογισμός επαναλαμβάνεται με αριθμητική ακεραίων ή/και ρητών απεριόριστης ακρίβειας. Αυτού του είδους οι τεχνικές ονομάζονται φίλτρα γιατί φιλτάρουν εκείνους τους υπολογισμούς που μπορούν να εκτελεστούν με αριθμητική της μηχανής. Υπάρχουν πολλών ειδών φίλτρα και συμβολικές αριθμητικές τεχνικές, για παράδειγμα στατικά και δυναμικά φίλτρα. Οι υλοποιήσεις μας, στην παρόντα χρόνο, δεν χρησιμοποιούν φίλτρα γι' αυτό και δεν θα επεκταθούμε περισσότερο σε αυτές τις τεχνικές.

Τα πειράματα πραγματοποιήθηκαν σε ένα Pentium (2.6 GHz), με τον μεταγλωτιστή g++ 3.4.4 σε λειτουργικό περιβάλλον linux.

Πολυώνυμα σε μία μεταβλητή

Πολυώνυμα βαθμού ≤ 4

Θα παρουσιάσουμε πειραματικά αποτελέσματα σχετικά με την πραγματική επίλυση πολυωνυμικών εξισώσεων βαθμού ≤ 4 και με τη σύγκριση πραγματικών αλγεβρικών αριθμών βαθμού ≤ 4.

Η υλοποίηση των αλγορίθμων για βαθμό ≤ 4 είναι αδιαφανής στον χρήστη. Ο χρήστης χρησιμοποιεί τις συναρτήσεις που παρουσιάσαμε στην προηγούμενη ενότητα και αν το πολυώνυμο (ή

msec	A	B	Γ	Δ
f-S^3	0.142	0.153	0.150	0.177
S^3	0.291	0.320	0.142	0.112
RS	5.240	6.320	4.930	5.180
BERNSTEIN	1.058	1.011	0.717	1.850
CORE	3.050	3.520	2.240	1.470
GKR	2.287	2.973	2.212	1.595
NIX	0.358	0.362	0.215	0.377

Πίνακας 6.1: Επίλυση και σύγκριση πραγματικών ριζών ακέραιων πολυωνύμων βαθμού ≤ 4

οι αλγεβρικοί αριθμοί) είναι βαθμού ≤ 4, τότε εφαρμόζονται οι αλγόριθμοι που παρουσιάστηκαν στο Κεφ. 5.

Η πρώτη ομάδα πειραμάτων αφορά την κατασκευή και την σύγκριση πραγματικών αλγεβρικών αριθμών βαθμού ≤ 4. και χωρίζονται σε 4 κατηγορίες. Η κατηγορία A περιέχει πολυώνυμα με 4 ρητές ρίζες στο διάστημα $[-1, 1]$ των οποίων το δυαδικό μήκος είναι 40 bits. Η B τυχαία περιέχει πολυώνυμα τα οποία κατασκευάστηκαν με παρεμβολή στο χωρίο $[-1, 1] \times [-1, 1]$ και των οποίων το δυαδικό μήκος είναι 90 bits. Η Γ περιέχει πολυώνυμα Mignotte, της μορφής $a(x^4 - 2(Lx - 1)^2)$, όπου το δυαδικό μήκος των a και L είναι 40 bits. Τέλος η κατηγορία Δ αφορά πολυώυμα που έχουν ρίζες με πολλαπλότητες. Οι ρίζες είναι τυχαίοι ρητοί αριθμοί στο $[-1, 1]$ και το δυαδικό μήκος των πολυωνύμων είναι 30. Για κάθε κατηγορία επιλέγουμε τυχαία δύο πολυώνυμα, απομονώνουμε τις πραγματικές τους ρίζες, υπολογίζουμε τις πολλαπλότητες, κατασκευάζουμε τους αντίστοιχους πραγματικούς αλγεβρικούς αριθμούς και στις στη συνέχεια διαλέγουμε τυχαία δύο από αυτούς και τους συγκρίνουμε. Τα αποτελέσματα παρουσιάζονται στον Πίνακα 6.1, όπου οι χρόνοι είναι σε msec και είναι ο μέσος όρος από 10000 τρεξίματα.

Συγκρίναμε τις υλοποιήσεις GKR, BERNSTEIN, NIX, CORE και RS.

Το GKR είναι μια βιβλιοθήκη σε C++ με αλγορίθμους για πολυώνυμα η οποία χρησιμοποιείται σε κινητικές δομές δεδομένων και οφείλεται στους Guibas et al. [123]. Το BERNSTEIN είναι η υλοποίηση του αλγορίθμου BERNSTEIN (Εν. 3.5) που υπάρχει στη SYNAPS και βασίζεται στην εργασία των Mourrain et al. [203]. Το NIX είναι βιβλιοθήκη σε C++ που αφορά αλγορίθμους για πολυώνυμα και πραγματικούς αλγεβρικούς αριθμούς. Είναι μέρος του EXACUS [18] και βασίζεται στη βιβλιοθήκη LEDA [186]. Πιο συγκεκριμενα η αριθμητική του βασίζεται στον τύπο Leda real [39] της LEDA. Η CORE [145, 146] είναι μια βιβλιοθήκη για ακριβείς υπολογισμούς. Χρησιμοποιεί τη βιβλιοθήκη GMP για αριθμητική με ακέραιους και ρητούς απεριόριστης ακρίβειας και για την επίλυση πολυωνύμων παρέχει μια υλοποίηση του αλγορίθμου STURM (Εν. 3.5). Τόσο το NIX όσο και η CORE προκειμένου να συγκρίνουν πραγματικούς αλγεβρικούς αριθμούς εκλεπτύνουν τα διαστήματα απομόνωσης που τους περιέχουν μέχρι είτε αυτά να γίνουν ξένα μεταξύ τους είτε να είναι τόσο μικρά, μικρότερα από το φράγμα διαχωρισμού, οπότε μπορούν να συμπεράνουν ότι οι αριθμοί είναι ίσοι.

Το RS είναι το λογισμικό που βασίζεται στους αλγορίθμους των Rouillier and Zimmermann [230], και παρέχει μια υλοποίηση του αλγορίθμου DESCARTES (Εν. 3.5). Η αριθμητική που χρησιμοποιεί βασίζεται τόσο στη βιβλιοθήκη GMP όσο και στην MPFR. Το RS απομονώνει τις ρίζες ενός

πολυωνύμου και δεν υπολογίζει τις πολλαπλότητες ούτε χειρίζεται πραγματικούς αλγεβρικούς αριθμούς. Η υλοποίηση είναι συμβολική-αριθμητική (symbolic-numeric) με την έννοια ότι αρχικά επιχειρείται να απομονωθούν οι ρίζες με αριθμητική βασισμένη σε doubles, στη συνέχεια με αριθμητική διαστημάτων σε αριθμούς κινητής υποδιαστολής, μέχρι κάποια ακρίβεια και τέλος αν τα προηγούμενα έχουν αποτύχει οι ρίζες απομονώνονται με ακέραια αριθμητική απεριόριστης ακρίβειας. Συνεπώς το RS χρησιμοποιεί με πολύ αποτελεσματικό τρόπο φίλτρα και είναι από τις γρήγορες διαθέσιμες βιβλιοθήκες για την επίλυση πολυωνύμων. Δυστυχώς ο πηγαίος κώδικας δεν διατίθεται ελεύθερα και το εκτελέσιμο είναι προσβάσιμο διαμέσου μιας διεπαφής στο MAPLE, οπότε κάποια χρονική επιβάρυνση προστίθεται στους χρόνους του.

Συμβολίζουμε την υλοποίηση των αλγορίθμων του Κεφ. 5 με s^3, και αντιστοιχεί Static Sturm Sequences ή Salmon-Sturm-Sylvester. Χρησιμοποιούμε την αριθμητική ακεραίων της βιβλιοθήκης GMP. Το fs^3 είναι η υλοποίησή μας τροποποιημένη έτσι ώστε η αριθμητική να βασίζεται στον αριθμητικό τύπο **Lazy_exact_nt** της CGAL. Ο τύπος αυτός υλοποιεί κάποια φίλτρα. Πιο συγκεκριμένα, μια ακολουθία υπολογισμών αποθηκεύεται σε ένα δένδρο. Οι υπολογισμοί εκτελούνται με **double** και αν το αποτέλεσμα δεν είναι δυνατόν να αναπαρασταθεί με **double** τότε ο υπολογισμός ξαναγίνεται με αριθμητική GMP. Εκτός από το s^3 κανένα άλλο λογισμικό δεν έχει τη συνατότητα να απομονώσει κάποια συγκεκριμένη πραγματική ρίζα, αλλά πρέπει να τις απομονώσει όλες προκειμένου να επιλέξει κάποια συγκεκριμένη.

Τα αποτελέσματα της πρώτης κατηγορίας πειραμάτων στον Πίνακα 6.1 δείχνουν ότι η υλοποίηση s^3 είναι καθαρά γρηγορότερη από τα CORE, SYNAPS και GKR για πολυώνυμα και αλγεβρικούς αριθμούς μικρού βαθμού, ακόμα και στην περίπτωση που δεν χρησιμοποιούμε αριθμητική με φίλτρα. Το s^3 είναι γρηγορότερο ακόμα και από το NIX το οποίο έχει ενγενώς αριθμητική με φίλτρα. Ειδική προσοχή πρέπει να δοθεί στην κατηγορία πειραμάτων Δ, όπου το s^3 είναι κατά πολύ γρηγορότερο από οποιαδήποτε άλλη προσέγγιση. Αυτό εξηγείται από το γεγονός ότι όταν υπάρχουν ρίζες με πολλαπλότητα οι αλγόριθμοι του Κεφ. 5 χρειάζονται λιγότερες πράξεις για να τις υπολογίσουν.

Πρέπει να σημειώσουμε ότι οι χρόνοι του RS έχουν κάποια επιβάρυνση η οποία οφείλεται στο γεγονός ότι το χρησιμοποιούμε διαμέσου του MAPLE, αλλά θεωρούμε ότι η σύγκριση είναι εφικτή καθώς χρησιμοποιεί φίλτρα, δεν παράγει στην έξοδο τις πολλαπλότητες των ριζών και δεν χειρίζεται πραγματικούς αλγεβρικούς αριθμούς.

Στις κατηγορίες Α και Β οι χρόνοι του s^3 είναι σχεδόν ίδιοι με μια μικρή επιβάρυνση που προκύπτει από το γεγονός ότι το δυαδικό μήκος των συντελεστών των πολυωνύμων του Β είναι μεγαλύτερο. Οι χρόνοι στις Α, Γ και Δ είναι σχεδόν οι ίδιοι καθώς τα πολυώνυμα έχουν σχεδόν το ίδιο δυαδικό μήκος και το s^3 δεν εξαρτάται από τον τύπο των πολυωνύμων. Στην κατηγορία Β υπάρχει μια μικρή επιβάρυνση που προκύπτει από το γεγονός ότι το δυαδικό μήκος των συντελεστών του Β είναι πολύ μεγάλο. Το fs^3 είναι σχεδόν πάντα γρηγορότερο εκτός από την Β και αυτό εξηγείται από το γεγονός ότι το μεγάλο δυαδικό μήκος των αριθμών προκαλεί αποτυχία στα φίλτρα και συνεπώς οι υπολογισμοί γίνονται δύο φορές. Ωστόσο ακόμα και σε αυτή την περίπτωση το fs^3 είναι τουλάχιστον 2 φορές πιο γρήγορο από το NIX που χρησιμοποιεί φίλτρα ενγενώς. Αξιοσημείωτη είναι και η μεγάλη διαφορά που έχουν τα s^3 και fs^3 στην κατηγορία Δ, όπου υπάρχουν πολλαπλές ρίζες. Οι άλλες υλοποιήσεις σε αυτή την κατηγορία δυσκολεύονται πολύ καθώς όταν οι ρίζες έχουν πολλαπλότητες οι εκλεπτύνσεις των διαστημάτων είναι πολύ χρονοβόρα υπολογιστικά εργασία.

msec	$\mathbb{Z}$	$\mathbb{Q}$	far	M$-\mathbb{Q}$	M	$\mathbb{Z}$	$\mathbb{Q}$	far	M$-\mathbb{Q}$	M
AXIOM	38.0	57.4	77.3	67.2	82.3					
MAPLE 9	33.2	52.4	69.0	75.5	74.7					
CORE	8.41	5.67	6.76	9.31	10.1					
BERNSTEIN	1.097	0.820	0.596	1.480	2.114	2.687	2.693	2.780	3.764	5.698
GKR	1.249	0.921	0.991	1.582	1.544	23.74	64.4	7.3	4.121	54.7
s^3	0.077	0.083	0.082	0.074	0.077	0.117	0.190	0.115	0.161	0.129

Πίνακας 6.2: Επίλυση και σύγκριση πραγματικών ριζών ακέραιων πολυωνύμων βαθμού 4

Μια δεύτερη κατηγορία πειραμάτων παρουσιαζεται στον Πίνακα 6.2. Σε αυτά τα πειράματα έχουμε συγκρίνει με μια υλοποίηση πραγματικών αλγεβρικών αριθμών στο μαθηματικό λογισμικό AXIOM, η οποία οφείλεται στον Rioboo [225, 226, 227]. Επίσης συγκρίναμε με μια υλοποίηση που υπάρχει στο MAPLE. Ωστόσο χρησιμοποιήσαμε τα δύο παραπάνω λογισμικά μόνο για λόγους παρουσίασης καθώς η επιβάρυνση που προκύπτει από περιβάλλον τους είναι πολύ μεγάλη.

Συγκρίναμε επίσης με την CORE, με το GKR και με την υλοποίηση του αλγορίθμου BERNSTEIN στην SYNAPS.

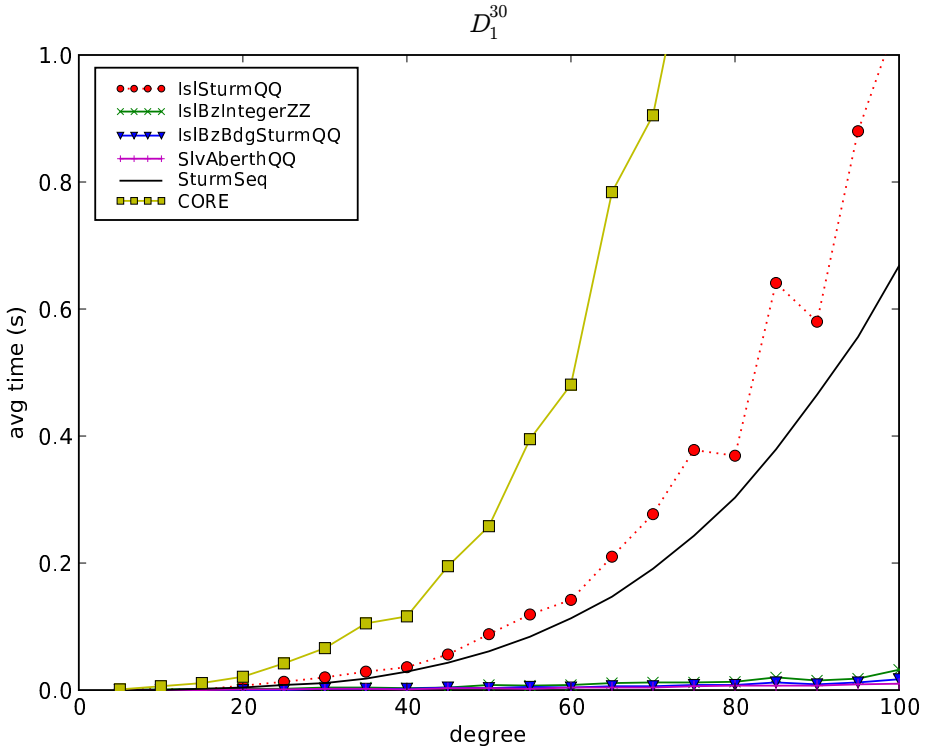
Όπως και στην πρώτη ομάδα πειραμάτων οι χρόνοι είναι σε msec και είναι ο μέσος όρος από 10000 τρεξίματα. Η στήλη $\mathbb{Z}$ αφορά πολυώνυμα με 4 ακέραιες ρίζες, η στήλη $\mathbb{Q}$ πολυώνυμα με 4 ρητές ρίζες. Η στήλη far αφορά πολυώνυμα, τέτοια ώστε οι ρίζες τους ανά δύο να είναι πολύ μακριά, στήλη $M-\mathbb{Q}$ αφορά πολυώνυμα τέτοια ώστε το ένα να είναι Mignotte και το άλλο να έχει μόνο ρητές ρίζες και τέλος η στήλη M αφορά Mignotte πολυώνυμα. Το αριστερό μισό του Πίνακα 6.2 αναφέρεται σε πολυώνυμα με 4 πραγματικές ρίζες στο διάστημα $[-20, 20]$ πολλαπλασιασμένα με ένα ακέριαιο $\in [1, 20]$, έτσι ώστε οι συντελεστές να είναι ακέραιοι μέτρου $\leq 32 \cdot 10^5$ και τα πολυώνυμα Mignotte είναι της μορφής $a(x^4 - 2(Lx-1)^2)$, όπου τα a, L είναι τυχαίοι ακέραιοι στο $[3, 30]$. Το δεξί μισό του πίνακα αναφέρεται σε πολυώνυμα με ρίζες τυχαίους αριθμούς στο $\in [10 \cdot 10^4, 11 \cdot 10^4]$ και σε Mignotte πολυώνυμα με a και L τυχαίους αριθμούς στο $[10 \cdot 10^4, 11 \cdot 10^4]$.

Πρέπει να τονίσουμε ότι το MAPLE δεν μπορεί να συγκρίνει τις ρίζες δύο πολυωνύμων Mignotte. Το s^3 είναι καθαρά η γρηγορότερη υλοποίηση. Στο πειράματα του αριστερού μέρους του Πίνακα 6.2 το s^3 είναι 103, 15 και 16 τιμες γρηγορότερο από την CORE, το BERNSTEIN και το GKR, αντίστοιχα κατά μέσο όρο. Αυξάνοντας το δυαδικό μήκος των συντελεστών μειώνουμε το φράγμα διαχωρισμού και έτσι στο δεξί μέρος του πίνακα η διαφορά στην ταχύτητα της υλοποίησής μας είναι πάρα πολύ μεγάλη, καθώς ο αριθμός των υποδιαιρέσεων που πραγματοποιούν οι άλλες υλοποιήσεις και το κόστος της κάθε μίας είναι πολύ μεγάλος. Στο δεξί μέρος δεν αναφέρουμε χρόνους για AXIOM, MAPLE και CORE, γιατί οι χρόνοι τους είναι πάρα πολύ μεγάλοι. Παρατηρούμε ότι οι χρόνοι του s^3 είναι σχεδόν οι ίδιοι για όλα τα είδη πολυωνύμων και αλγεβρικών αριθμών καθώς δεν εξαρτώμαστε από το φράγμα διαχωρισμού.

Συμπερασματικά, οι συμβολικοί αλγόριθμοι που υλοποιεί η υλοποίηση s^3 κατασκευάζουν και συγκρίνουν πραγματικούς αλγεβρικούς αριθμούς με κάποιο καθορισμένο αριθμό πράξεων, ανεξάρτητα από το φράγμα διαχωρισμού. Κατά συνέπεια δεν επηρεάζονται από τον τύπο των πο-

λυωνύμων ή από το πόσο κοντά βρίσκονται δύο πραγματικοί αλγεβρικοί αριθμοί. Επιπρόσθετα, οι ίδιες ποσότητες που χρησιμοποιούνται για να απομονώσουν τις πραγματικές ρίζες, χρησιμοποιούνται τόσο για να κατασκευαστεί ο αλγεβρικός αριθμός όσο και για να υπολογιστεί η πολλαπλότητά του. Αυτός είναι ο λόγος που η υλοποίησηυ s^3 είναι η γρηγορότερη διαθέσιμη αυτή τη στιγμή για πολυώνυμα και αλγεβρικούς αριθμούς μικρού βαθμού.

Πολυώνυμα αυθαίρετου βαθμού

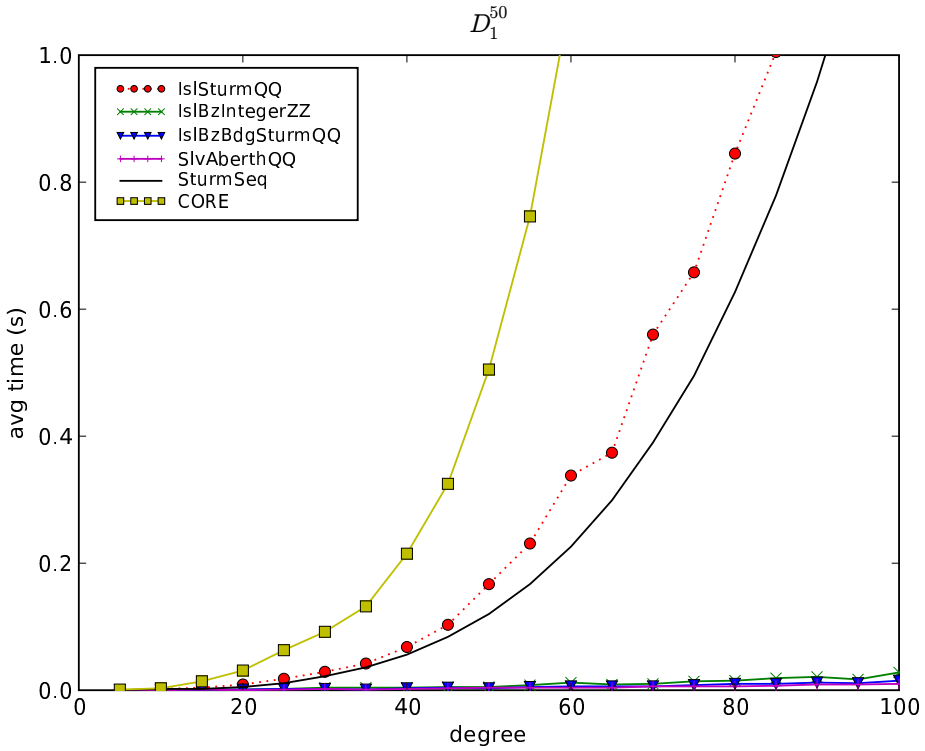


Σχήμα 6.1: Τυχαία πολυώνυμα, χωρίς τετράγωνα, με λίγες πραγματικές ρίζες και δυαδικό μήκος συντελεστών 30 bits.

Στην παρούσα παράγραφο θα μελετήσουμε την πρακτική συμπεριφορά των αλγορίθμων του Κεφ. 3 για την απομόνωση των πραγματικών ριζών ακέραιων πολυωνύμων σε μία μεταβλητή. Τα πειράματα αφορούν υλοποιήσεις των αλγορίθμων STURM, BERNSTEIN και SB.

Η υλοποίηση του STURM βασίζεται στον αλγόριθμο που παρουσιάσαμε στην Εν. 3.5. Για την υλοποίηση των προσημασμένων πολυωνυμικών υπολοίπων χρησιμοποιήσαμε τις ακολουθίες Sturm-Habicht (Εν. 2.3) και για την αριθμητική την υλοποίηση των ακεραίων και των ρητών της GMP.

Η υλοποίηση του BERNSTEIN βασίζεται στον αλγόριθμο που παρουσιάσαμε στην Εν. 3.5, και χρησιμοποιούμε μόνο αριθμητική ακεραίων. Το πολυώνυμο αρχικά μετατρέπεται στη βάση Bernstein στο αρχικό διάστημα που ψάχνουμε τις πραγματικές ρίζες και στη συνέχεια απαλοί-

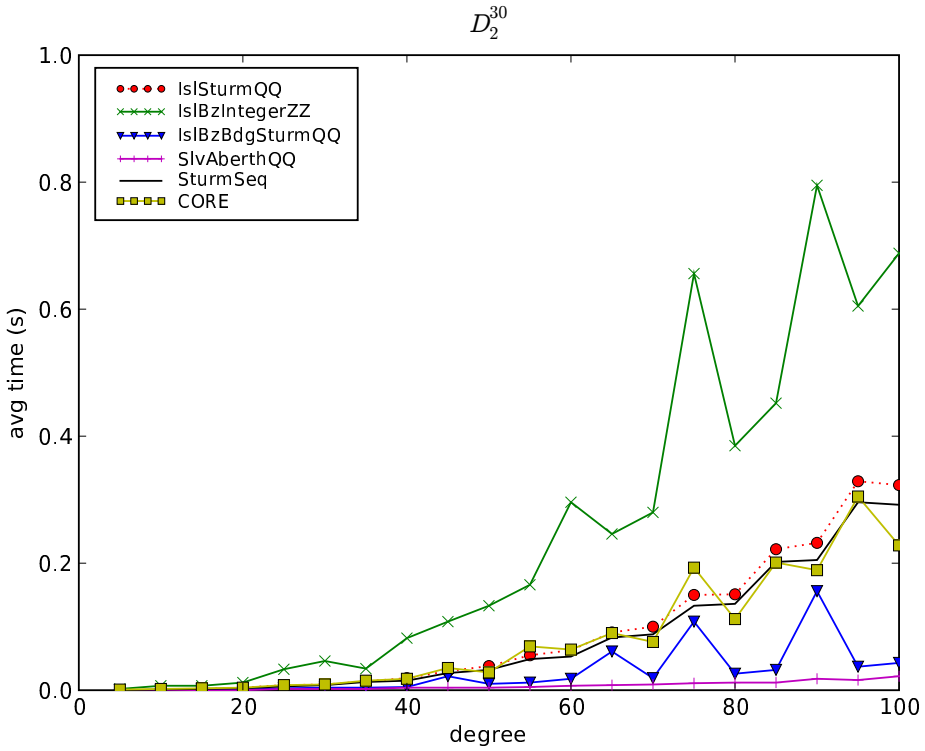


Σχήμα 6.2: Τυχαία πολυώνυμα, χωρίς τετράγωνα, με λίγες πραγματικές ρίζες και δυαδικό μήκος συντελεστών 50 bits.

φουμε τους παρανομαστές. Στη συνέχεια η υποδιαίρεση πραγματοποιείται με τον αλγόριθμο του de Casteljau, με την εφαρμογή των απεικονίσεων δ_L και δ_R (δείτε Εν. 2.4) σε κάθε βήμα υποδιαίρεσης.

Ο αλγόριθμος StBz είναι ένας συνδυασμός των αλγορίθμων STURM και BERNSTEIN, όπου εκμεταλλευόμαστε την αριθμητική ευστάθεια της αναπαράστασης Bernstein. Αρχικά το πολυώνυμο μετατρέπεται στη βάση Bernstein στο αρχικό διάστημα, χρησιμοποιώντας ακριβή αριθμητική, καθώς η μετατροπή είναι αριθμητικά ασταθής και οι συντελεστές (στη βάση Bernstein) του πολυωνύμου μετατρέπονται σε διαστήματα με άκρα doubles. Ο αλγόριθμος BERNSTEIN εφαρμόζεται, χρησιμοποιώντας αριθμούς κινητής υποδιαστολή και αριθμητική διαστημάτων, στο πολυώνυμο και σταματά είτε όταν είμαστε σίγουροι ότι έχουμε υπολογίσει ένα διάστημα που περιέχει μία και μόνο ρίζα είτε όταν δεν μπορούμε να αποφασίσουμε την ύπαρξη ή την μοναδικότητα μιας πραγματικής ρίζας από τα πρόσημα $(-, +, ?)$ των συντελεστών (που είναι διαστήματα). Σε αυτή την περίπτωση, για τα διαστήματα που έχουμε αμφιβολία, καλείται ο αλγόριθμος STURM με αριθμητική απεριόριστης ακρίβειας, προκειμένου να ολοκληρωθεί η διαδικασία του αλγορίθμου απομόνωσης.

Συγκρίνουμε με την CORE και με το MPSOLVE, που είναι ένα αριθμητικός αλγόριθμος επίλυσης (numerical solver) που βασίζεται στην μέθοδο του Aberth [22] και έχει υλοποιηθεί από τους Bini and Fiorentino [23]. Το MPSOLVE υπολογίζει κάποια προεγγιση για όλες τις μιγαδικές



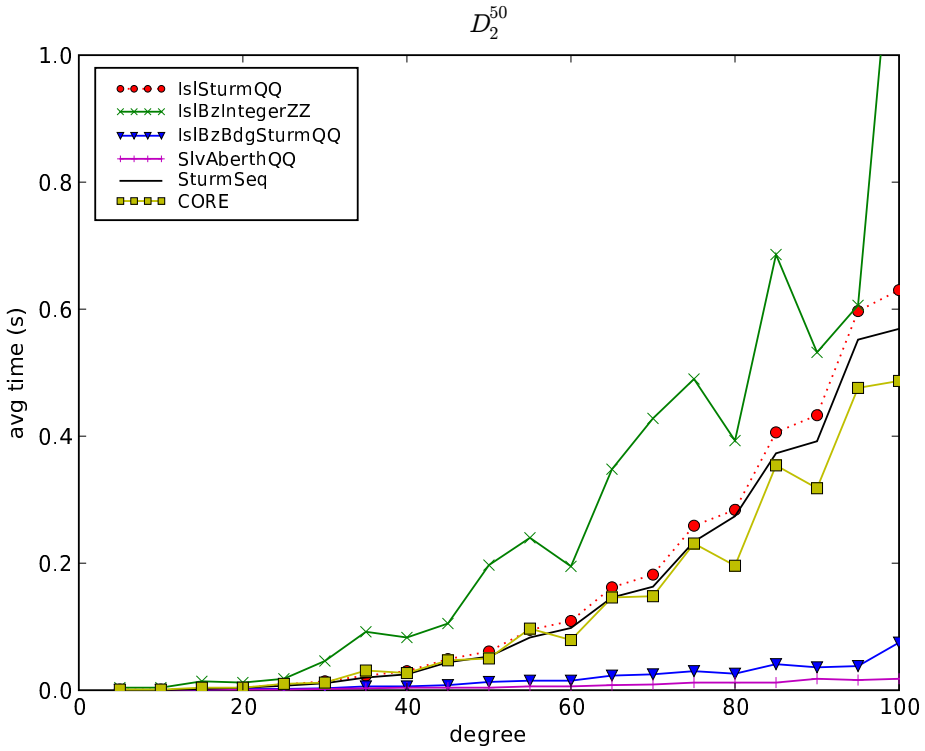
Σχήμα 6.3: Τυχαία πολυώνυμα, με λίγες πραγματικές ρίζες πολλαπλότητας > 1 και δυαδικό μήκος συντελεστών 30 bits.

ρίζες. Προκειμένου να συνάγουμε το πλήθος αλλά και την προσέγγιση των πραγματικών ριζών θεωρούμε ως πραγματικές εκείνες τις μιγαδικές των οποίων το φανταστικό μέρος είναι μικρότερο από κάποια ακρίβεια που δίνεται ως είσοδο στον αλγόριθμο. Προκειμένου να πάρουμε, σε κάθε περίπτωση, τα σωστά αποτελέσματα πρέπει η ακρίβεια να είναι ίση με το φράγμα διαχωρισμού, το οποίο είναι όμως πολύ μικρό. Επίσης παρουσιάζουμε και τον χρόνο που απαιτείται για τον υπολογισμό της ακολουθίας Sturm-Habicht και τον συμβολίζουμε με StHa.

Τα δεδομένα που έχουμε χρησιμοποιήσει [4] είναι πολυώνυμα βαθμού $d \in \{3, \ldots, 100\}$ και δυαδικού μήκους συντελεστών $\tau \in \{10, 20, 30, 40, 50\}$ και έχουν διάφορα χαρακτηριστικά. Πιο συγκεκριμένα οι διαφορετικές κατηγορίες πειραμάτων είναι οι εξής: η D_1^τ περιέχει τυχαία πολυώνυμα με λίγες πραγματικές ρίζες, η D_2^τ τυχαία πολυώνυμα με πολλαπλές ρίζες, η D_3^τ τυχαία πολυώνυμα με d ακέραιες ρίζες (με πολλαπλότητα), η D_4^τ τυχαία πολυώνυμα με d ρητές ρίζες (με πολλαπλότητα), η D_5^τ πολυώνυμα Mignotte της μορφής $x^d - 2(Lx-1)^2$, η D_6^τ πολυώνυμα που είναι το γινόμενο δύο πολυωνύμων Mignotte και τέλος η D_7^τ πολυώνυμα Mignotte με πολλαπλές ρίζες.

Θα παρουσιάσουμε τα πιο αντιπροσωπευτικά πειράματα· κείνα που μας βοηθούν να καταλάβουμε την (πρακτική) συμπεριφορά των αλγορίθμων. Παρουσιάζουμε περάματα στις κατηγορίες

[4] `http://www-sop.inria.fr/galaad/data/upol/`

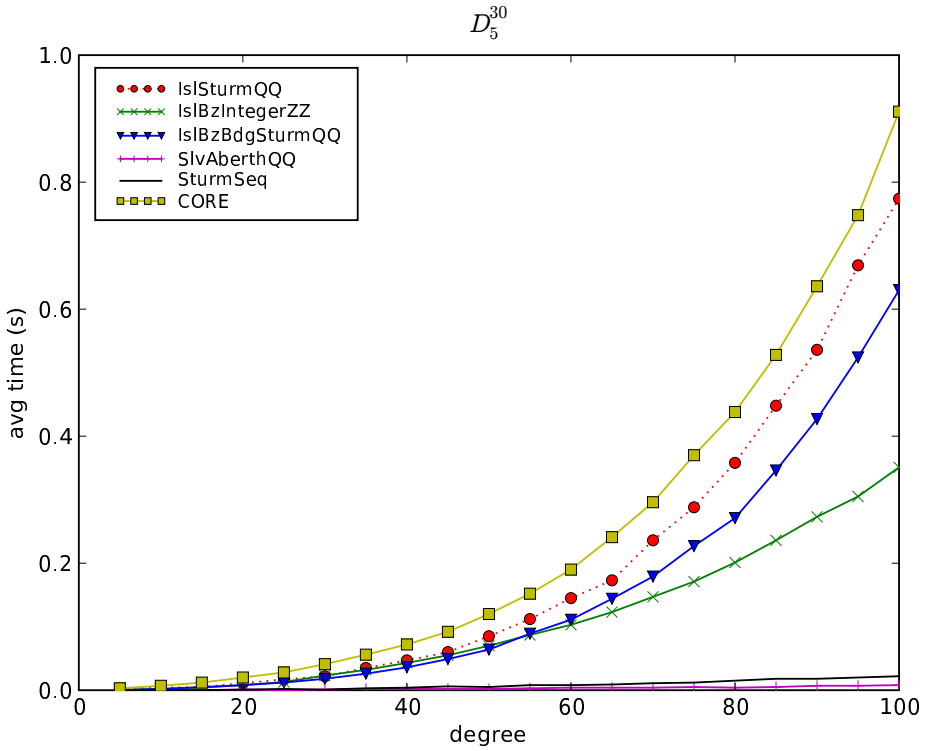


Σχήμα 6.4: Τυχαία πολυώνυμα, με λίγες πραγματικές ρίζες πολλαπλότητας > 1 και δυαδικό μήκος συντελεστών 50 bits.

D_1^{30}, D_1^{50}, D_2^{30}, D_2^{50}, D_5^{30}, D_5^{50}, D_7^{30} και D_7^{50}. Οι χρόνοι είναι σε δευτερόλεπτα, είναι ο μέσος όρος 100 τρεξιμάτων και παρουσιάζονται στα Γραφήματα 6.1 έως 6.8. Ο βαθμός των πολυωνύμων δεν είναι πολύ μεγάλος. Ωστόσο το δυαδικό μήκος των πολυωνύμων των πειραμάτων πλησιάζει ή ξεπερνά την ακρίβεια της μηχανής. Η πολυπλοκότητα των αλγορίθμων υποδιαίρεσης εξαρτάται αφενός από το βαθμός αφετέτρου δε από το δυαδικό μήκος. Συνεπώς ένας από τους τρόπους για να κατασκευαστούν, δύσκολα προς επίλυση πολυώνυμα, είναι να θεωρήσουμε μεγάλο δυαδικό μήκος συντελεστών. Πολυώνυμα μικρού σχετικά βαθμού αλλά μεγάλου δυαδικού μήκους είναι συνήθη στις εφαρμογές.

Για πολυώνυμα με λίγες, χωρίς πολλαπλότητα και καλά διαχωρισμένες πραγματικές ρίζες, αυτή είναι η περίπτωση των πειραμάτων D_1, D_2, η υλοποίηση STURM είναι καθαρά η χειρότερη επιλογή, καθώς απαιτεί πάρα πολύ χρόνο για αρχικοποίηση, δηλαδή για τον υπολογισμό της προσημασμένης ακολουθίας πολυωνυμικών υπολοίπων. Παρατηρήστε ο χρόνος αρχικοποίησης ξεπερνά κατά πολύ το χρόνο για όλες τις αποτιμήσεις. Ο χρόνος που καταναλώθηκε στις αποτιμήσεις είναι η διαφορά του συνολικού χρόνου του αλγορίθμου και της αρχικοποίησης. Από τα γραφήματα συμπεραίνουμε ότι για τέτοια δεδομένα ο αλγόριθμος bernstein ή ακόμα και αριθμητικές υλοποιήσεις πρέπει να προτιμούνται.

Ωστόσο, όταν υπάρχουν ρίζες με πολλαπλότητα ή όταν οι ρίζες είναι πάρα πολύ κοντά, αυ-



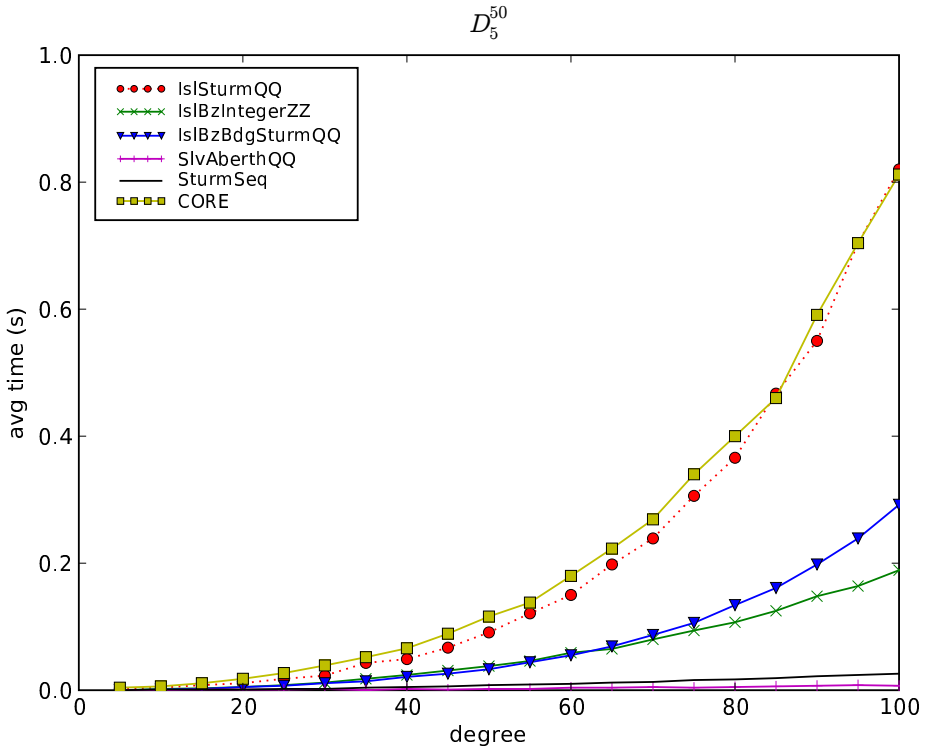
Σχήμα 6.5: Πολυώνυμα Mignotte με δυαδικό μήκος συντελεστών 30 bits.

τή είναι η περίπτωση των D_5 και D_7 τότε ο χρόνος αρχικοποίησης της υλοποίησης STURM είναι αμελητέος σε σχέση με το χρόνο που χρειαζόμαστε για υποδιαιρέσεις και τις αποτιμήσεις. Στα γραφήματα που αφορούν τα πολυώνυμα των D_5 και D_7 η γραμμή που αντιστοιχεί στον υπολογισμό της ακολουθίας υπολοίπων σχεδόν δεν φαίνεται. Παρατηρήστε, ότι όταν υπάρχουν πολλαπλότητες τότε πρέπει να υπολογίσουμε την ακολουθίας Sturm-Habicht για κάθε αλγόριθμο προκειμένου αφενός να βρούμε το χωρίς τετράγωνα μέρος του πολυωνύμου και αφετέτερου δε να υπολογίσουμε τις πολλαπλότητες των ριζών. Σε τέτοιες περιπτώσεις φαίνεται η υβριδική υλοποίηση StBz είναι αυτή που προκρίνεται καθώς απομονώνει πολύ γρήγορα τις ρίζες που είναι καλά διαχωρισμένες και επίσης προσφέρει στον αλγόριθμο STURM πολύ καλά αρχικά διαστήματα για να αρχίσει τις υποδιαιρέσεις για τις υπόλοιπες ρίζες.

Πρέπει να τονίζουμε ότι ούτε η CORE ούτε ο MPSOLVE υπολογίζει τις πολλαπλότητες των ριζών. Εκτιμούμε ότι η προσέγγιση του StBz είναι εξαιρετικά ενδιαφέρουσα καθώς είναι γρήγορος σε τυχαία πολυώνυμα και συγκρίσιμος με τον STURM στα δύσκολα στιγμυότυπα και χρήζει περαιτέρω θεωρητικής και πειραματικής μελέτης.

Ο αλγόριθμος CF

Τα επόμενα πειράματα αφορούν τον αλγόριθμο CF που παρουσιάσαμε στην Εν. 3.6. Θεωρούμε ότι στην πράξη ο CF είναι ο γρηγορότερος αλγόριθμος και θα παρουσιάσουμε ξεχωριστά πειραματικά

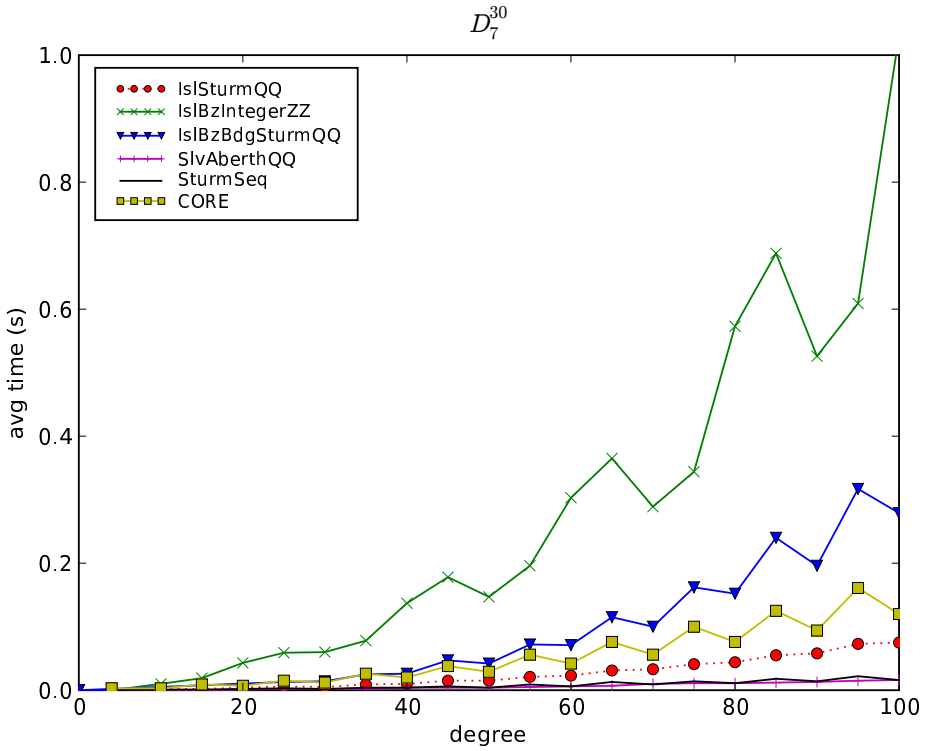


Σχήμα 6.6: Πολυώνυμα Mignotte με δυαδικό μήκος συντελεστών 50 bits.

αποτελέσματα γι' αυτόν πάνω σε πολυώνυμα που είναι τόσο θεωρητικά όσο και πρακτικά τα πιο δύσκολα προς επίλυση.

Η υλοποίηση του αλγορίθμου CF έγινε με τη βοήθεια της βιβλιοθήκης SYNAPS και θα είναι μέρος της στην επόμενή της μεγάλη έκδοση. Όπως και οι προηγούμενοι αλγόριθμοι βασίζεται μόνο σε αριθμητική ακεραιών της GMP, αλλά η υλοποίησή έχει γίνει με πολύ προσοχή έτσι ώστε να εκμεταλλευτούμε την ταχύτητα μερικών πολύ συγκεριμένων πράξεων. Για παράδειγμα χρησιμοποιούμε μόνο απεικονίσεις της μορφής $X \mapsto 2^{\beta} X$ και $X \mapsto X+1$ γιατί αφενός οι βρόγχοι του αλγορίθμου είναι πιο σφιχτοί και αφετετέρου υπάρχουν πολύ γρήγορες υλοποιήσεις στην GMP για τις αντίστοιχες πράξεις. Παρ' όλα αυτά η υλοποίησή μας ακολουθεί το παράδειγμα του γενικευμένου προγραμματισμού (generic programming) και είναι συμβατή, δηλαδή μπορεί να μεταγλωτιστεί, με οποιαδήποτε βιβλιοθήκη υποστηρίζει αριθμητική με ακεραίους απεριόριστης ακρίβειας. Επίσης έχουμε υλοποιήσει και διαάφορα τεχνάσματα που επιταχύνουν την επίλυση. Για παράδειγμα στα άρτια πολυώνυμα απομονώνουμε μόνο τις θετικές ρίζες καθώς στη συνέχεια μπορούμε εύκολα να συνάγουμε διαστήματα απομόνωσης για τις αρνητικές.

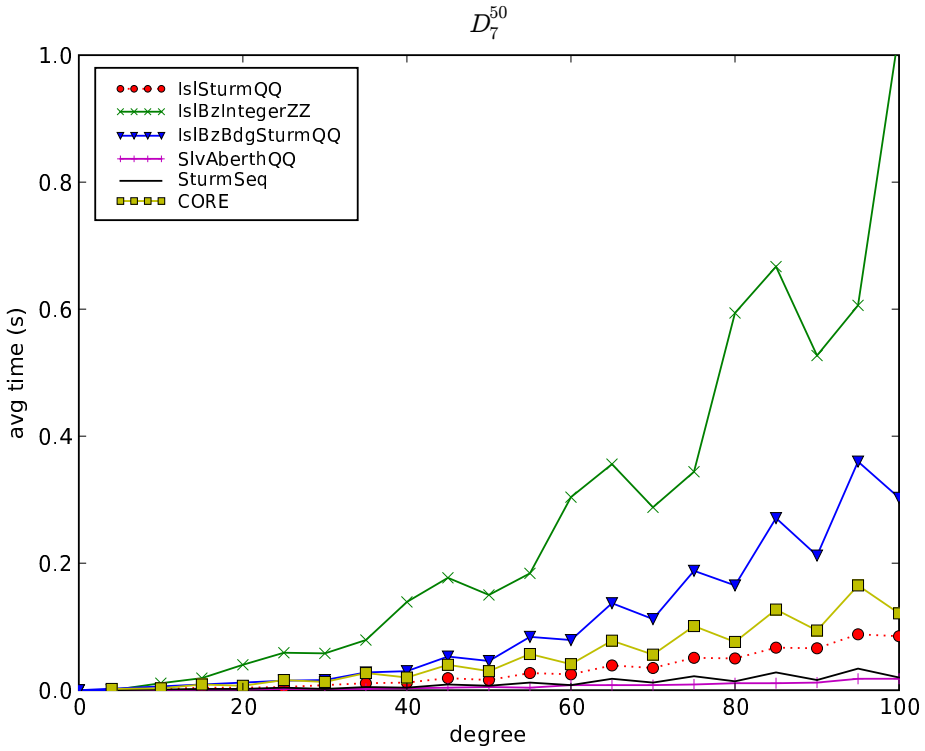
Τα πολυώνυμα των πειραμάτων είναι χωρίς τετράγωνα και ο βαθμός του είναι $\in \{100, 200, \ldots, 1000\}$. Η πρώτη ομάδα πειραμάτων αφορά πολυώνυμα Laguerre (L), πρώτου (C1) και δεύτερου (C2) τύπου Chebyshev πολυώνυμα και πολυώνυμα Wilkinson (Ω). Τα πολυώνυμα αυτά έχουν πολλές πραγματικές ρίζες, πολύ κοντά μεταξύ τους και είναι από τα πιο γνωστά 'δύσκολα' πολυώνυ-



Σχήμα 6.7: Πολυώνυμα των οποίων το ελεύθερο τετραγώνων μέρος είναι πολυώνυμο Mignotte με δυαδικό μήκος συντελεστών 30 bits.

μα προς επίλυση. Επίσης παρουσιάζουμε πειράματα με πολυώνυμα Mignotte (M1) της μορφής $X^d-2(101\cdot X-1)^2$, που έχουν 4 πραγματικές ρίζες αλλά οι δύο από αυτές είναι πάρα πολύ κοντά και πολυώνυμα που είναι το γινόμενο δύο πολυωνύμων Mignotte (M2) , δηλαδή είναι της μορφής $\left(X^d-2(101\cdot X-1)^2\right)\left(X^d-2((101+\frac{1}{101})X-1)^2\right)$. Αυτά τα πολυώνυμα έχουν 8 πραγματικές ρίζες, 4 εκ των οποίων είναι πολύ κοντά. Τέλος θεωρούμε πολυώνυμα με τυχαίους συντελεστές (R1) και μονικά πολυώνυμα με τυχαίους συντελεστές (R2) στο διάστημα $[-1000, 1000]$, τα οποία παρήχθησαν από το MAPLE, χρησιμοποιώντας το 101 ως γεννήτρια των ψευδοτυχαίων αριθμών. Τα τυχαία πολυώνυμα έχουν, γενικά, λίγες και καλά διαχωρισμένες πραγματικές ρίζες.

Συγκρίναμε με το RS και το MPSOLVE. Πρέπει να τονίσουμε ότι για το MPSOLVE δεν καταφέραμε σε όλες τις περιπτώσεις να το ρυθμίσουμε κατάλληλα προκειμένου να παράξει το ακριβή αριθμό των πραγματικών ριζών, δηλαδή δεν καταφέραμε προσδιορίσουμε την ακρίβεια εισόδου και εξόδου. Αν και στην SYNAPS υπάρχουν υλοποιημένοι πολλοί αλγόριθμοι για την επίλυση ακέραιων πολυωνύμων, η ιδιαίτερη υλοποίηση του CF τον καθιστά σαφώς γρηγορότερο και γι' αυτό και δεν συγκρίνουμε με άλλους αλγορίθμους στην SYNAPS. Αυτό που μπορούμε να πούμε με ασφάλεια είναι ότι ο πολύ μεγάλος βαθμός και το πολύ μεγάλο δυαδικό μήκος των πολυωνύμων των πειραμάτων, τα καθιστά μη επιλύσιμα με την παρούσα υλοποίηση του STURM που υπάρχει στη SYNAPS, όπως και με αυτή της CORE. Τα αποτελέσματα των πειραμάτων παρουσιάζονται στον Πίνακα 6.3,



Σχήμα 6.8: Πολυώνυμα των οποίων το ελεύθερο τετραγώνων μέρος είναι πολυώνυμο Mignotte με δυαδικό μήκος συντελεστών 50 bits.

όπου οι χρόνοι είναι σε δευτερόλεπτα. Ο αστερίσκος (*) δηλώνει ότι ο υπολογισμός δεν τελείωσε μετά από 12000s και το αγγλικό ερωτηματικό (?) ότι δεν μπορέσαμε να ρυθμίσουμε κατάλληλα το MPSOLVE.

Για τα πολυώνυμα (M1) και (M2) υπάρχουν ρητοί αριθμοί, με πολύ απλή ανάπτυξη σε συνεχή κλάσματα, που βρίσκονται ανάμεσα στις πραγματικές ρίζες που είναι πολύ κοντά. Αυτός είναι ο λόγος που το CF είναι πάρα πολύ γρήγορο σε αυτά τα στιγμυότυπα. Αξίζει να τονίσουμε ότι τα πολυώνυμα Mignotte θεωρούνται τα πιο δύσκολα τεστ για τους αλγόριθμους απομόνωσης πραγματικών ριζών. Αυτά τα πολυώνυμα είναι πάρα πολύ δύσκολα για το RS. Στο (M1) το MPSOLVE είναι το γρηγορότερο λογισμικό, αλλά στο (M2) που οι κοντινές ρίζες είναι 4, είναι πιο αργό από το CF. Το CF είναι επίσης πολύ γρήγορο στα πολυώνυμα Wilkinson καθώς από τη στιγμή που θα βρούμε μία (την πρώτη) ρίζα τότε οι απεικονίσεις της μορφής $X \mapsto X + 1$ πολύ γρήγορα μας επιτρέπουν να βρούμε και όλες τις υπόλοιπες (δείτε Εν. 3.6). Το MPSOLVE δεν καταφέραμε να το ρυθμίσουμε σε αυτά τα πολυώνυμα. Στα (L), (C1) και (C2) το CF είναι συγκρίσιμο με το RS και για μια ακόμα φορά αντιμετωπίσαμε ανυπέρβλητες δυσκολίες με το MPSOLVE. Τα πολυώνυμα στα (R1) και (R2) έχουν λίγες και καλά διαχωρισμένες ρίζες, γι' αυτό το λόγο το RS μπορεί να τις διαχωρίσει πάρα πολύ γρήγορα με μόνο 63 bits ακρίβεια στη χειρότερη περίπτωση. Το MPSOLVE είναι ακόμα γρηγορότερο σε αυτά τα πολυώνυμα. Ωστόσο, ακόμα και σε αυτή την περίπτωση το

		100	200	300	400	500	600	700	800	900	1000
L	CF	0.27	2.24	9.14	25.27	55.86	110.13	214.99	407.09	774.22	1376.34
	RS	0.65	3.65	13.06	35.23	77.21	151.17	283.43	527.42	885.86	1387.45
	#roots	100	200	300	400	500	600	700	800	900	1000
C1	CF	0.11	0.85	3.16	8.61	19.67	38.23	77.75	139.18	247.11	414.51
	RS	0.21	1.36	3.80	10.02	23.15	46.02	82.01	150.01	269.35	458.67
	#roots	100	200	300	400	500	600	700	800	900	1000
C2	CF	0.11	0.77	3.14	8.20	19.28	38.58	73.59	133.52	233.48	386.61
	RS	0.23	1.48	3.80	9.84	23.28	46.34	83.58	146.04	273.00	452.77
	#roots	100	200	300	400	500	600	700	800	900	1000
W	CF	0.11	0.76	2.54	6.09	12.07	21.43	34.52	53.35	81.88	120.21
	RS	0.09	0.59	2.25	6.34	14.62	29.82	55.47	104.56	179.23	298.45
	#roots	100	200	300	400	500	600	700	800	900	1000
M1	CF	0.02	0.08	0.21	0.42	0.73	1.19	1.84	2.75	4.16	6.22
	RS	7.83	287.27	1936.48	7328.86	*	*	*	*	*	*
	MPSOLVE	0.01	0.04	0.07	0.11	0.12	0.26	0.43	0.37	0.47	0.90
	#roots	4	4	4	4	4	4	4	4	4	4
M2	CF	0.08	0.43	1.10	2.78	4.71	8.67	18.26	25.28	40.15	60.10
	RS	1.24	144.64	1036.785	4278.275	12743.79	*	*	*	*	*
	MPSOLVE	0.04	0.78	3.24	?	?	?	?	?	?	?
	#roots	8	8	8	8	8	8	8	8	8	8
R1	CF	0.001	0.04	0.07	0.33	0.06	0.37	0.66	0.76	1.03	1.77
	RS	0.026	0.09	0.11	0.68	0.22	0.89	0.95	0.69	1.55	2.09
	MPSOLVE	0.02	0.03	0.07	0.14	0.21	0.31	0.44	0.51	0.64	0.80
	#roots	4	4	2	6	2	4	4	2	4	4
R2	CF	0.01	0.04	0.08	0.36	0.14	0.38	0.74	0.77	1.24	1.42
	RS	0.05	0.23	0.47	1.18	0.81	1.64	2.68	3.02	4.02	4.88
	MPSOLVE	0.01	0.05	0.08	0.14	0.23	0.33	0.44	0.55	0.67	0.83
	#roots	4	4	4	6	4	4	6	4	6	4

Πίνακας 6.3: Πειραματικά αποτελέσματα για τον αλγόριθμο CF.

CF είναι τουλάχιστον συγκρίσιμο με τις άλλες δύο υλοποιήσεις.

Επίσης, πειραματιστήκαμε με ένα ακέραιο πολυώνυμο που εμφανίζεται στο κατηγόρημα κ_3 στον υπολογισμό του διαγράμματος Voronoi ελλείψεων στο επίπεδο (Εν. 7.3). Το πολυώνυμο έχει βαθμό 184, δυαδικό μήκος συντελεστών 903 και έχει 8 πραγματικές ρίζες. Το CF το επιλύσει σε 0.12s, το RS σε 0.3s και το MPSOLVE σε 1.7s.

Οι χρόνοι του RS για τα πειράματα (L), (C1) και (C2) μπορούν να γίνουν κατά 30% γρηγορότεροι αν πειραματιστούμε με τις παραμέτρους του[5]. Ωστόσο, το RS χρησιμοποιεί φίλτρα, ενώ η υλοποίηση του ΣΦ όχι, οπότε μπορούμε να πούμε ότι οι δύο υλοποιήσεις είναι συγκρίσιμες.

Τα αποτελέσματα του αλγορίθμου CF είναι πολύ ελπιδοφόρα. Πιστεύουμε ότι αν χρησιμοποιήσουμε φίλτρα και συμβολικές-αριθμητικές τεχνικές [230] οι χρόνοι του θα βελτιωθούν ακόμα περισσότερο. Επίσης, η υλοποίηση του CF στηρίζεται σε κάτω φράγματα στις θετικές πραγματικές ρίζες. Πιστεύουμε ότι αν χρησιμοποιηθεί το φράγμα του Stefanescu (δείτε Θεωρ. 3.19) θα έχουμε δραματική βελτίωση.

[5]Προσωπική επικοινωνία με τον F. Rouillier

Πολυωνυμικά συστήματα σε δύο μεταβλητές

Τα πειραματικά αποτελέσματα που θα παρουσιάσουμε στη συνέχεια αφορούν την πραγματική επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές.

Συστήματα πολυωνύμων βαθμού ≤ 2

Σκοπός των πειραμάτων είναι να ελένξουμε στην πράξη τη συμπεριφορά των συμβολικών αλγορίθμων της Εν. 5.5 για την επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές συνολικού βαθμού ≤ 2.

Τα πειράματα εκτελούνται ως εξής: από μία λίστα με πολυώνυμα σε δύο μεταβλητές επιλέγουμε τυχαία δύο από αυτά και επιλύουμε στους πραγματικούς το σύστημα που ορίζουν. Οι λίστες των πολυωνύμων είναι δύο κατηγοριών. Η κατηγορία A περιέχει 1000 πολυώνυμα σε δύο μεταβλητές, με ακέραιους συντελεστές επιλεγμένους ομοιόμορφα από το διάστημα $[-10, 10]$. Τα συστήματα που ορίζονται δεν έχουν, γενικά, πραγματικές λύσεις. Πιο συγκεκριμένα κάθε πολυώνυμο της κατηγορίας A, έχει κοινά (πραγματικά) σημεία με 135 άλλα στη λίστα, κατά μέσο όρο. Η κατηγορία B περιέχει 1000 πολυώνυμα σε δύο μεταβλητές που είναι κωνικές τομές. Τα πολυώνυμα κατασκευάστηκαν με παρεμβολή από 5 ακέραια σημεία επιλεγμένα τυχαία από το χωρίο $[-10, 10] \times [-10, 10]$. Κάθε κωνική τομή έχει κοινά (πραγματικά) τομές με 970 άλλες στη λίστα, κατά μέσο όρο.

Συγκρίναμε το s^3 με το NEWMAC, το STH, το RES και το GBRS. Το NEWMAC [202] είναι η υλοποίηση ενός γενικού σκοπού αλγορίθμου για την επίλυση τετράγωνων πολυωνυμικών συστημάτων, οποιουδήποτε βαθμού και πλήθους μεταβλητών. Βασίζεται σε μια παραλλαγή των βάσεων Gröbner, τις κανονικές μορφές (normal forms) [198, 201]. Η επίλυση του συτήματος ανάγεται σε ένα πρόβλημα ιδιοτιμών και ιδιοδιανυσμάτων το οποίο επιλύεται με τη βοήθεια της βιλιοθήκης LAPACK. Το NEWMAC υπολογίζει όλες τις μιγαδικές λύσεις του συστήματος και είναι μέρος της SYNAPS.

Το STH, επίσης στη SYNAPS, βασίζεται στις ακολουθίες Sturm-Habicht και στην ουσία υλοποιεί τον αλγόριθμο που προτείνουν οι González-Vega and El Kahoui [116], Gonzalez-Vega and Necula [117] για τον υπολογισμό της τοπολογίας επίπεδων πραγματικών αλγεβρικών καμπυλών. Προκειμένου να υπολογίσει τις τεταγμένες των πραγματικών λύσεων χρησιμοποιεί μια αριθμητική προσέγγιση των τετμημένων. Η υλοποίηση βασίζεται σε **double** και δεν δίνει πάντοτε τα σωστά αποτελέσματα.

Το RES είναι ένας αλγόριθμος για τον επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές [43], ο οποίος με τη βοήθεια του πίνακα Bézout ανάγει την επίλυση του συστήματος σε ένα γενικευμένο πρόβλημα ιδιοτιμών και ιδιοδιανυσμάτων το οποίο επιλύεται με την βιβλιοθλήκη LAPACK. Η υλοποίηση βασίζεται σε **double** και δεν δίνει πάντοτε τα σωστά αποτελέσματα.

Το GBRS είναι επέκταση του RS και υλοποιεί αλγορίθμους που βασίζονται στις βάσεις Gröbner και στη ρητή αναπαράσταση με πολυώνυμο σε μία μεταβλητή (rational univariate representation) [229]. Όπως και για το RS, ο πηγαίος κώδικας δεν είναι διαθέσιμος και το εκτελέσιμο το χρησιμοποιήσαμε διαμέσου του MAPLE. Το GBRS δεν υπολογίζει τις πολλαπλότητες των λύσεων.

Όπως και στην περίπτωση της επίλυσης σε μία μεταβλητή, συμβολίζουμε την υλοποίηση του αλγορίθμου της Εν. 5.5 με s^3 και με fs^3 όταν χρησιμοποιούμε αριθμητική βασισμένη στον τύπο **Lazy_exact_nt**.

msec	A	B
s^3	0.17	0.18
fs^3	0.14	0.54
GBRS	6.40	6.90
STH	0.51	0.57
RES	0.36	-
NEWMAC	3.19	3.26

Πίνακας 6.4: Επίλυση πολυωνυμικού συστήματος σε δύο μεταβλητές, πολυωνύμων συνολικού βαθμού ≤ 2.

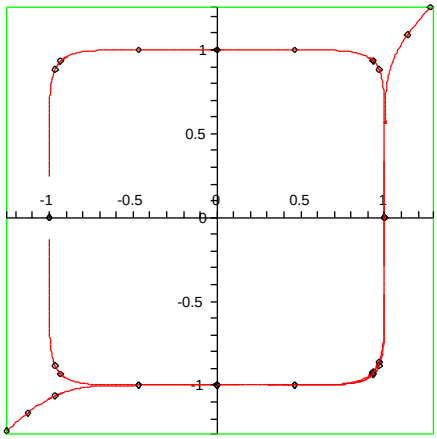
Τα αποτελέσματα των πειραμάτων παρουσιάζονται στον Πίνακα 6.4, όπου οι χρόνοι είναι σε msec και είναι ο μέσος όρος από 10000 τρεξίματα.

Παρατηρούμε ότι οι χρόνοι του s^3 είναι σχεδόν οι ίδιοι και για τις δύο κατηγορίες πειραμάτων. Αυτό εξηγείται από το γεγονός ότι το πιο χρονοβόρο τμήμα του αλγορίθμου είναι η προβολή στους άξονες. Ο χρόνος που απαιτείται για το ταίριασμα των ριζών είναι αμελητέος. Επίσης, πρέπει να τονίσουμε ότι η προσέγγισή μας είναι ακριβής, με την έννοια ότι παράγει ορθογώνια χωρία στα οποία κείται (εγγυημένα) μία και μόνο μία λύση του συστήματος, τα χωρία έχουν ρητά άκρα και η πολλαπλότητα της λύσης επίσης είναι έξοδος. Τέτοια έξοδο δεν παράγουν τα STH και RES και μάλιστα το RES δεν μπορεί να επιλύσει τα συστήματα της στήλης Β, καθώς η ακρίβεια που απαιτείται ξεπερνά αυτή που μπορεί να χειριστεί η βιβλιοθήκη LAPACK. Οι μεγάλοι χρόνοι του NEWMAC οφείλονται κυρίως στο γεγονός ότι υπολογίζει τις μιγαδικές λύσεις του συστήματος. Γι' αυτό και οι χρόνοι του είναι σχεδόν οι ίδιοι για τα πειράματα Α και Β καθώς και στις δύο περιπτώσεις υπολογίζει 4 ρίζες. Για το GBRS δεν μπορούν να εξαχθούν ασφαλή συμπεράσματα καθώς η επιβάρυνση που οφείλεται στο MAPLE είναι εξεραιτικά σημαντική για τόσο γρήγορους υπολογισμούς.

Συμπερασματικά το s^3 φαίνεται ότι είναι η πιο γρήγορη υλοποίηση καθώς με κάποιο προκαθορισμένο αριθμό πράξεων απομονώνει τις πραγματικές λύσεις του συστήματος και υπολογίζει τις πολλαπλότητές τους. Τα φίλτρα που χρησιμοποιεί το fs^3 βοηθούν στη γενική περίπτωση, όταν δηλαδή οι πραγματικές λύσεις είναι λίγες, αλλά σε αντίθετη περίπτωση αποτυγχάνουν και σχεδόν διαπλασιάζουν το χρόνο εκτέλεσης.

Συστήματα πολυωνύμων αυθαίρετου βαθμού

Σε αυτή την ενότητα θα παρουσιάσουμε πειραματικά αποτελέσματα σχετικά με τους δύο αλγορίθμους, NAIVE_SOLVE και MRUR_SOLVE, επίλυσης πολυωνυμικών συστημάτων σε δύο μεταβλητές



Σχήμα 6.9: Γραφική παράσταση των δύο αλγεβρικών καμπυλών που αντιστοιχούν στο σύστημα (M_4). Οι λύσεις του συστήματος είναι $(0,-1)$ και $(1,0)$. Το καμπυλωμένο τετράγωνο αντιστοιχεί στο δεύτερο πολυώνυμο του συστήματος.

που παρουσιάσαμε στο Κεφ. 4. Τα πειράματα αφορούν τα παρακάτω πολυωνυμικά συστήματα:

$$(R_1)\quad \begin{cases} 1+2X-2X^2Y-5XY+X^2+3X^2Y &= 0\\ 2+6X-6X^2Y-11XY+4X^2+5X^3Y &= 0 \end{cases}$$

$$(R_2)\quad \begin{cases} X^3+3X^2+3X-Y^2+2Y-2=0\\ 2X+Y-3=0 \end{cases}$$

$$(R_3)\quad \begin{cases} X^3-3X^2-3XY+6X+Y^3-3Y^2+6Y-5=0\\ X+Y-2=0 \end{cases}$$

$$(M_1)\quad \begin{cases} Y^2-X^2+X^3=0\\ Y^2-X^3+2X^2-X=0 \end{cases}$$

$$(M_2)\quad \begin{cases} X^4-2X^2Y+Y^2+Y^4-Y^3=0\\ Y-2X^2=0 \end{cases}$$

$$(M_3)\quad \begin{cases} X^6+3X^4Y^2+3X^2Y^4+Y^6-4X^2Y^2=0\\ Y^2-X^2+X^3=0 \end{cases}$$

$$(M_4)\quad \begin{cases} X^9-Y^9-1=0\\ X^{10}+Y^{10}-1=0 \end{cases}$$

$$(D_1)\quad \begin{cases} X^4-Y^4-1=0\\ X^5+Y^5-1=0 \end{cases}$$

$$(D_2)\quad \begin{cases} -312960-2640X^2-4800XY-2880Y^2+58080X+58560Y=0\\ -584640-20880X^2+1740XY+1740Y+274920X-59160Y=0 \end{cases}$$

msec	R_1	R_2	R_3	M_1	M_2	M_3	M_4	D_1	D_2
NAIVE_SOLVE	10	1	1	2	3	433	5010	50	1
MRUR_SOLVE	1	1	0.1	1	1	44	1010	11	1
NEWMAC	6	2	3	3	3	20	1020	20	20
RES	0.3	0.3	0.6	0.6	01.2	8.4	150	-	0.5
STH	1	0.2	0.2	0.5	0.4	1.3	-	280	0.4
GBRS	24	22	21	18	23	28	25	25	27

Πίνακας 6.5: Επιλύση πολυωνυμικών συστημάτων σε δύο μεταβλητές.

Τα συστήματα $R_{\{1,2,3\}}$ είναι από την εργασία των Keyser et al. [153], τα συστήματα $M_{\{1,2,3,4\}}$ από την εργασία των Busé et al. [43].

Συγκρίναμε τις υλοποιήσεις μας με το NEWMAC, το RES, το STH και το GBRS. Τα αποτελέσματα παρουσιάζονται στον Πίνακα 6.5, όπου οι χρόνοι είναι σε msec και είναι ο μέσος όρος από 100 τρεξίματα.

Για μια ακόμα φορά πρέπει να τονίσουμε ότι η προσέγγισή μας είναι ακριβής και δεν στηρίζεται/εξαρτάται από προσεγγίσεις όπως τα STH, `res` και NEWMAC. Το NAIVE_SOLVE είναι αρκετά ανταγωνιστικό για όλα τα συστήματα ενώ το MRUR_SOLVE σχεδόν πάντα πιο γρήγορο ακόμα και από υλοποιήσεις που στηρίζονται σε αριθμητική με **double**.

Ιδιαίτερη προσοχή πρέπει να δειχθεί στο σύστημα M_4, δείτε Σχ. 6.9. Οι λύσεις του συστήματος είναι $(0, -1)$ και $(1, 0)$ με πολλαπλότητα 9 και οι δύο. Το σύστημα είναι σε γενική θέση, οπότε όλοι οι αλγόριθμοι μπορούν να το επιλύσουν χωρίς να εφαρμόσουμε κάποια τυχαία μετατόπιση. Λόγω της πολύ μεγάλης πολλαπλότητας των ριζών το STH δεν μπορεί να το επιλύσει καθώς δεν επαρκεί η ακρίβεια των **double** και το `res` δίνει ως πρώτη λύση την $(-0.01, 1)$ η οποία έχει πολύ μεγάλο σφάλμα. Ο υπερβολικά μεγάλος χρόνος που απαιτεί το NEWMAC για να επιλύσει το σύστημα ερμηνεύεται από το γεγονός ότι πρέπει να υπολογίσει τις ιδιοτιμές ενός πίνακα 90×90. Το STH δεν μπορεί να επιλύσει το σύστημα καθώς δεν επαρκεί η ακρίβεια των **double**. Το MRUR_SOLVE είναι αρκετά ανταγωνιστικό σε αυτό το σύστημα. Ωστόσο, το γρηγορότερο λογισμικό είναι το GBRS καθώς η βάση Gröbner του συστήματος υπολογίζεται πάρα πολύ γρήγορα.

Παρατηρήσαμε ότι ο περισσότερος χρόνος των υλοποιήσεων NAIVE_SOLVE και MRUR_SOLVE σπαταλάται για τον υπολογισμό των δύο προβολών, στον X και στον Y άξονα και στην επίλυσής τους και όχι στο ταίριασμα των λύσεων.. Στα πειράματα μας επιλύουμε τα πολυώνυμα σε μία μεταβλητή με τον αλγόριθμο STURM. Προφάνως κάποιος πιο γρήγορος αλγόριθμος πρέπει να χρησιμοποιηθεί, όπως για παράδειγμα ο BERNSTEIN ή ο CF.

Όσον αφορά την προσέγγιση των Keyser et al. [153], αναφέρουν ότι σε ένα πιο γρήγορο μηχάνημα με 3GHz CPU, οι χρόνοι τους για να επιλύσουν τα συστήματα R_1, R_2 και R_3 είναι 2590, 86.5 και 103 msec αντίστοιχα. Διαφαίνεται ότι η προσέγγισή μας είναι πιο γρήγορη, αλλά πιο εμπεριστατωμένη πειραματική μελέτη χρειάζεται.

Συμπερασματικά, οι υλοποιήσεις των NAIVE_SOLVE και MRUR_SOLVE είναι αρκετά ελπιδοφόρες, αν και οι χρόνοι τους απέχουν από ώριμα πακέτα λογισμικού όπως το GBRS.

ΚΕΦΑΛΑΙΟ 7

Εφαρμογές στην γεωμετρία

> As long as algebra and geometry have been separated, their progress have been slow and their uses limited; but when these two sciences have been united, they have lent each mutual forces, and have marched together towards perfection.
>
> Joseph-Louis Lagrange

Περίληψη

Παρουσιάζουμε τα βασικά κατηγορήματα που απαιτούνται από τους αλγορίθμους για τον υπολογισμό της διάταξης ελλειπτικών τόξων στο επίπεδο και του Voronoi διαγράμματος ελλείψεων στο επίπεδο.

Τα αποτελέσματα παρουσιάστηκαν στις εργασίες [96, 98, 99].

Τα καμπύλα αντικείμενα γίνονται ολοένα και πιο σημαντικά για την υπολογιστική γεωμετρία. Ίσως ο πιο σημαντικός λόγος είναι ότι εμφανίζονται σε ένα πλήθος από εφαρμογές όπως το CAD, η μοριακή βιολογία, τα γεωγραφικά συστήματα πληροφοριών (GIS), η ρομποτική... Η εργασία μας ανήκει μια γενικότερη προσπάθεια για την επέκταση των υπαρχόντων αλγορίθμων και του υπάρχοντος λογισμικού έτσι ώστε να είναι εφικτοί και αποδοτικοί οι (γεωμετρικοί) υπολογισμοί με καμπύλα αντικείμενα. Μια σύγχρονη επισκόπηση αυτής της σχετικάς νέας και συναρπαστικής ερευνητικής περιοχής παρουσιάζεται από τους Boissonnat and Teillaud [30].

Στο παρόν κεφάλαιο θα ασχοληθούμε με τα κατηγορήματα που παρουσιάζονται στους αλγορίθμους για τον υπολογισμό διατάξεων ελλείψεων στο επίπεδο και για το υπολογισμό του διαγράμματος Voronoi ελλείψεων στο επίπεδο.

Τι είναι όμως τα κατηγορήματα; Είναι οι βασικές γεωμετρικές πράξεις που απαιτούνται από τους γεωμετρικούς αλγορίθμους, όπως για παράδειγμα η λεξικογραφική σύγκριση σημείων, ο υπολογισμός της θέσης ενός σημείου ως προς το σύνορο ενός γεωμετρικού αντικειμένου, η διάταξη γεωμετρικών αντικειμένων κατά μήκος μιας κατακόρυφης ευθείας, ο υπολογισμός των σημείων τομής γεωμετρικών αντικειμένων... Στην περίπτωση των καμπύλων αντικειμένων (και όχι μόνο) τα κατηγορήματα ανάγονται στον χειρισμό χειρισμό ριζών πολυώνυμων και πολυωνυμικών συστημάτων, δηλαδή σε αλγεβρικούς υπολογισμούς. Οι υπάρχουσες βιβλιοθήκες, όπως η CORE [1] ή η LEDA [2] προτείνουν τύπους οι οποίοι υποστηρίζουν ακριβείς (exact) συγκρίσεις πραγματικών αλγεβρικών αριθμών, υπό την προϋπόθεση ότι αυτοί καθορίζονται από μια έκραση η οποία περιέχει ριζικά και προσφάτως ρίζες πολυωνύμων σε μία μεταβλητή (οι αντίστοιχοι τελεστές είναι `rootOf` και `diamond` αντίστοιχα). Αυτοί οι υπολογισμοί βασίζονται σε συνεχείς βελτιώσεις αριθμητικών προσεγγίσεων με αριθμητική κινητής υποδιαστολής και σε φράγματα διαχωρισμού (*separation bounds*) [41, 172, 173]. Η κλάση γνωρισμάτων της CGAL για κωνικές τομές στο πακέτο για τις διατάξεις βασίζεται σε αριθμούς με αυτά τα χαρακτηριστικά. Εναλλακτικές προσεγγίσεις προκειμένου να επιτευχθεί η ακριβής σύγκριση πραγματικών αλγεβρικών αριθμών με αποτελεσματικό τρόπο, επιτυγχάνεται με το να υπολογίσουμε πρόσημα συγκεκριμένων πολυωνυμικών εκφράσεων στα δεδομένα εισόδου. Μια τέτοια προσέγγιση παρουσιάστηκε από τους Devillers et al. [70], Karavelas and Emiris [148] για πολυώνυμα βαθμού 2 και από τους Emiris and Tsigaridas [88, 90, 92] για βαθμό μέχρι 4. Αυτή η προσέγγιση βασίζεται σε αλγεβρικά εργαλεία όπως οι ακολουθίες Sturm, η επιλύσουσα, ο κανόνας προσήμων του Descartes και είναι αυτή που θα χρησιμοποιήσουμε για τα κατηγορήματα που θα παρουσιάσουμε.

Η υλοποίηση των αλγορίθμων με τους οποίους ασχολούμαστε βασίζεται στη βιβλιοθήκη CGAL [3]. Η CGAL είναι η πιο γνωστή και ευρέως χρησιμοποιούμενη βιβλιοθήκη για γεωμετρικούς υπολογισμούς. Ο κώδικάς της είναι σε `C++` και είναι ανοιχτό λογισμικό (open source).

7.1 Περί των ελλείψεων

Θεωρούμε μια έλλειψη στην πεπλεγμένη μοφρή της:

$$E : f(x,y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f \in \mathbb{Q}[x,y] \tag{7.1}$$

όπου ισχύει $a\,c \neq 0$. Έστω ότι το μήκος του μεγάλου και του μικρού άξονα είναι 2α και 2β αντίστοιχα, και έστω (x_c, y_c) το (ρητό) κέντρο της έλλειψης. Η αντίστοιχη παραμετρική αναπαράσταση

[1] `www.cs.nyu.edu/exact/core/`
[2] `www.algorithmic-solutions.com/enleda.htm`
[3] `www.cgal.org`

της έλλειψης δίνεται από τις εξισώσεις:

$$\begin{aligned} x(t) &= x_c + \alpha\left(\frac{1-w^2}{1+w^2}\right)\left(\frac{1-t^2}{1+t^2}\right) - \beta\left(\frac{2w}{1+w^2}\right)\left(\frac{2t}{1+t^2}\right) \\ &= x_c + \frac{-\alpha(1-w^2)t^2 - 4\beta w t + \alpha(1-w^2)}{(1+w^2)(1+t^2)} \\ y(t) &= y_c + \alpha\left(\frac{2w}{1+w^2}\right)\left(\frac{1-t^2}{1+t^2}\right) + \beta\left(\frac{1-w^2}{1+w^2}\right)\left(\frac{2t}{1+t^2}\right) \\ &= y_c + 2\frac{-\alpha w t^2 + \beta(1-w^2)t + \alpha w}{(1+w^2)(1+t^2)}, \end{aligned} \tag{7.2}$$

όπου $t = \tan(\theta/2) \in (-\infty, \infty)$, θ είναι η γωνία που διατρέχει η έλλειψη, $w = \tan(\omega/2)$ και ω είναι η γωνία στροφής ανάμεσα στον κύριο άξονα της έλλειψης και τους κάθετους άξονες. Η παραμετρική αναπαράσταση αφήνει έξω ένα σημείο της περιφέρειας της έλλειψης, το οποίο ονομάζουμε i-point.

Η συμμετρική έλλειψη, με κέντρο συμμετρίας το κέντρο της έλλειψης, καθορίζεται από τις (παραμετρικές) εξισώσεις:

$$\begin{aligned} \overline{x(t)} &= -x(-t) + 2x_c \\ \overline{y(t)} &= -y(t) + 2y_c \end{aligned}$$

και την ονομάζουμε *δίδυμη έλλειψη* (twin ellipse). Κάθε σημείο της έλλειψης, του i-point συμπεριλαμβανομένου, είναι διαφορετικό από το αντίστοιχό του στη δίδυμη έλλειψη. Συμβολίζουμε με $E_t(\alpha, \beta, w, x_c, y_c)$ ή απλούστερα με E_t μια έλλειψη η οποία έχει ως παράμετρο το t και με $\overline{E}_t$ τη δίδυμή της. Οι συντελεστές της (7.1) μπορούν να θεωρηθούν ως πολυώνυμα με μεταβλητές τους συντελεστές της (7.2). Πιο συγκεκριμένα:

$$\begin{aligned} \chi &= y_c w^2 + 2x_c w - y_c \\ \psi &= x_c w^2 - 2y_c w - x_c \\ (1+w^2)^2 a &= 4w^2\alpha^2 + (w-1)^2(w+1)^2\beta^2 \\ (1+w^2)^2 b &= 2(\alpha-\beta)(\alpha+\beta)w(w-1)(w+1) \\ (1+w^2)^2 c &= 4w^2\beta^2 + (w-1)^2(w+1)^2\alpha^2 \\ (1+w^2)^2 d &= -2w\chi\alpha^2 - (w-1)(w+1)\psi\beta^2 \\ (1+w^2)^2 e &= +2w\psi\beta^2 - (w-1)(w+1)\chi\alpha^2 \\ (1+w^2)^2 f &= \chi^2\alpha^2 + \psi^2\beta^2 - (1+w^2)^2\alpha^2\beta^2 \end{aligned} \tag{7.3}$$

Παρατηρούμε ότι οι εξισώσεις των χ και ψ εκφράζουν τις εξισώσεις ευθειών που διατρέχουν τον μεγάλο και τον μικρό άξονα της έλλειψης, όταν αυτές αποτιμηθούν πάνω στο σημείο (x_c, y_c). Οι ποσότητες

$$J_1 = a + c = \alpha^2 + \beta^2, \quad J_2 = ac - b^2 = \alpha^2\beta^2$$

είναι *αναλλοίωτες* ως προς τη στροφή και τη μετατόπιση, ενώ η $J_4 = J_2(x_c^2 + y_c^2 - J_1)$ είναι αναλλοίωτη ως προς τη στροφή. Επίσης, οι συντεταγμένες του κέντρου δίνονται από τους τύπους

$$x_c = (be - dc)/J_2, \quad y_c = (bd - ae)/J_2$$

Όταν η έλλειψη μας δίνεται με την παραμετρική της μορφή, ή κατασκευαστικά με τους άξονες στροφής, το κέντρο της και το w, οι εξισώσεις (7.3) μας επιτρέπουν να υπολογίσουμε την πεπλεγμένη μορφή.

7.2 Διατάξεις κωνικών τομών στο επίπεδο

Η διάταξη (arragement) γεωμετρικών αντικειμένων είναι ένα από τα πιο γνωστά προβλήματα και καλά μελετημένα στην υπολογιστική γεωμετρία. Δοθέντος μιας συλλογής S από γεωμτρικά αντικείμενα, για παράδειγμα ευθείες, κύκλους, κωνικές τομές, σφαίρες, η διάταξή τους $A(S)$ είναι η διαμέριση του χώρου στον οποίο ανήκουν σε κελιά, τα οποία επάγονται από τα γεωμετρικά αντικείμενα. Στο επίπεδο η διάταξη γεωμετρικών αντικειμένων, επάγει ένα επίπεδο γράφο, ο οποίος έχει ως κορυφές τις τομές των γεωμετρικών αντικειμένων και ως ακμές τα μέγιστα τμήματα των συνόρων των γεωμετρικών αντικειμένων που δεν περιέχουν καμία κορυφή. Ένα παράδειγμα διάταξης ελλειπτικών τόξων στο επίπεδο παρουσιάζεται στο Σχ. 7.2 Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία, για παράδειγμα [105, 126].

Στην παρούσα ενότητα θα ασχοληθούμε με τη διάταξη ελλείψεων και ελλειπτικών τόξων στο επίπεδο και πιο συγκεκριμένα με τα κατηγορήματα που χρειάζονται οι αλγόριθμοι που υπλογίζουν τη διάταξη. Η προσπάθειά μας εντάσσεται σε μια γενικότερη προσπάθεια επέκτασης της βιβλιοθήκης CGAL και εφοδιασμού της με έναν πυρήνα για καμπύλα αντικείμενα και υπολογισμούς με αυτά. Ένας τέτοιος πυρήνας βασίζεται σε πραγματικούς αλγεβρικούς αριθμούς, σε επίλυση πολυωνυμικών εξισώσεων και συστημάτων φραγμένου βαθμού. Τελικός μας στόχος είναι να παρουσιάσουμε μια αποτελεσματική επέκταση της CGAL έτσι ώστε να μπορεί να χειριστεί καμπύλα αντικείμενα.

Οι υπάρχουσες εργασίες στη διάταξη (arrangement) καμπυλών στο επίπεδο περιλαμβάνουν τη βιβλιοθήκη EXACUS [4] [17] όπως και το αντίστοιχο πακέτο στη CGAL [266]. Και οι δύο προσεγγίσεις υπολογίζουν τη διάταξη αυθαίρετων κωνικών τομών αλλά μόνο η δεύτερη προσέγγιση είναι διαθέσιμη ελεύθερα. Όσο αφορά τη διάταξη επιφανειών ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία [19, 113].

Τα κατηγορήματα που θα παρουσιάζουμε καλύπτουν τόσο τον αυξητικό όσο και τον αλγόριθμο σάρωσης (sweep-line). Για περισσότερες λεπτομέρειες σχετικά με τους αλγορίθμους υπολογισμού διατάξεων ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία [29, 67, 105, 126, 219].

Αναπαράσταση των ελλείψεων

Προκειμένου να αναπαραστήστουμε μια έλλειψη ή ένα ελλειπτικό τόξο με κάποια δομή μιας γλώσσας προγραμματισμού (στην περίπτωσή μας C++) κάνουμε τις ακόλουθες παραδοχές:

- Ένα ελλειπτικό τόξο είναι μια καμπύλη η οποία αναπαρίσταται από το πολυώνυμο σε δύο μεταβλητές, όπως στην (7.1), που αντιστοιχεί στην εξίσωση της έλλειψης που το ορίζει και δύο σημεία που είναι τα άκρα του.

[4] http://www.mpi-sb.mpg.de/projects/EXACUS

- Ένα ελλειπτικό τόξο είναι x-μονότονο, εκτός αν είναι αρχική είσοδος στον αλγόριθμό μας. Αναπαρίσταται από την αντίστοιχη κωνική τομή και από μία μεταβλητή Boolean η οποία δείχνει αν μας ενδιαφέρει το πάνω ή το κάτω μέρος.
- Οι συντεταγμένες των άκρων ενός ελλειπτικού τόξου (όπως και όλων των σημείων που εμφανίζονται στον αλγόριθμο υπολογισμού της διάταξης) αντιστοιχούν σε πραγματικούς αλγεβρικούς αριθμούς βαθμού ≤ 4, χωρίς να αποκλείεται η περίπτωση ακεραίων ή ρητών.

Κατηγορήματα για τη διάταξη κωνικών τομών

Θα παρουσιάσουμε τη θεωρητική θεμελίωση και την υλοποίηση των κατηγορημάτων που απαιτούνται για την υλοποίηση αλγορίθμων διάταξης κωνικών τομών. Θα χρησιμοποιήσουμε τα αποτελέσματα του Κεφ. 5. Η στρατηγική μας έγκειται στο να ανάγουμε συγκεκριμένα κατηγορήματα σε άλλα, προκειμένου να μειώσουμε στο ελάχιστο τον αριθμό των κατηγορημάτων που χρειάζονται.

COMPARE_X **και** COMPARE_Y

Στόχος των κατηγορημάτων είναι να συγκρίνουν λεξικογραφικά τις συντεταγμένες δύο σημείων που εμφανίζονται κατά τη διάρκεια του αλγορίθμου. Τα σημεία προκύπτουν ως τομές δύο ελλειπτικών τόξων. Τα ελλειπτικά τόξα αναπαρίστανται ως πολυώνυμα δύο μεταβλητών, όπως στην εξίσωση (7.1) και τα σημεία τομής υπολογίζονται αν επιλύσουμε το πολυωνυμικό σύστημα που ορίζουν οι δύο εξισώσεις τους. Γιαυτό χρησιμοποιούμε τον αλγόριθμο της Εν. 5.5. Οι λύσεις του συστήματος είναι πραγματικοί αλγεβρικοί αριθμοί βαθμού ≤ 4 και προκειμένου να τους συγκρίνουμε χρησιμοποιούμε τους αλγορίθμους της Εν. 5.3. Παρατηρούμε ότι η σύγκριση έχει πολυπλοκότητα $\mathcal{O}(1)$.

MAKE_X_MONOTONE

Στόχος του κατηγορήματος είναι να 'κόψει' μια έλλειψη (ή ένα ελλειπτικό τόξο) σε x-μονότονα τμήματα. Τα τμήματα αυτά οριοθετούνται από εκείνα τα σημεία της έλλειψης που έχουν κατακόρυφη εφαπτομένη, τα οποία για να τα υπολογίσουμε θεωρούμε μερικές παραγώγους ως προς x και y της εξίσωσης της έλλειψης:

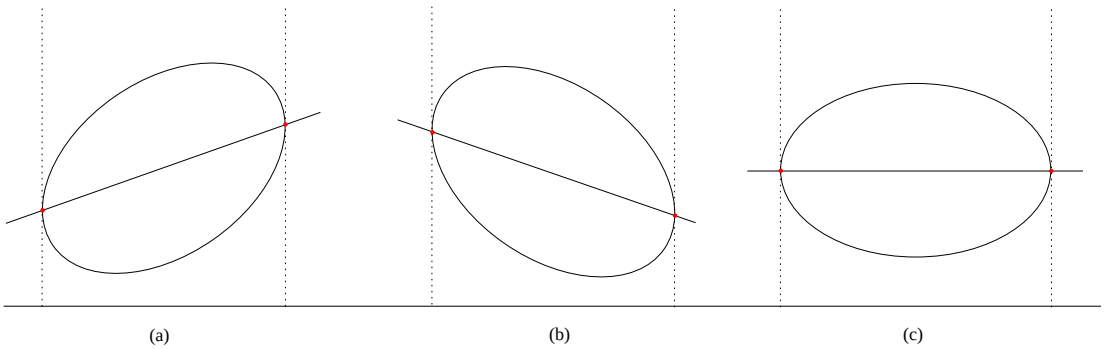
$$\begin{aligned} E_x &: f_x(x,y) = a\,x + b\,y + d \\ E_y &: f_y(x,y) = b\,x + c\,y + e \end{aligned} \tag{7.4}$$

Τα κοινά σημεία των f και f_y είναι τα σημεία της έλλειψης (κωνικής τομής) στα οποία η εφαπτομένη είναι κατακόρυφη.

Για να υπολογίσουμε την τετμημένη αυτών των σημείων θεωρούμε την επιλύσουσα των f και f_y, δηλαδή απαλοίφουμε το y.

$$R_x = \mathtt{res}_y(f, f_y) = c\left((ca - b^2)x^2 + 2(cd - 2\,eb)x - e^2 + cf\right) \tag{7.5}$$

Μπορούμε να ξεχάσουμε τον παράγοντα c εάν θεωρήσουμε μόνο ελλείψεις, δηλαδή $c \neq 0$. Προκειμένου να υπολογίσουμε τις τεταγμένες των σημείων, θεωρούμε την επιλύουσα των f και f_x,



Σχήμα 7.1: Οι τρεις περιπτώσεις, σχετικά με το πως μπορεί μια έλλειψη να διαχωριστεί σε x-μονότονα τμήματα.

δηλαδή απαλοίφουμε το x.

$$R_y = \mathtt{res}_x(f, f_x) = a\left((ca - b^2)y^2 + 2(ae - bd)y - d^2 + af\right) \tag{7.6}$$

Μπορούμε να υποθέσουμε ότι $a \neq 0$ αν περιοριστούμε σε ελλείψεις.

Τα R_x και R_y είναι δευτεροβάθμια και μπορούμε να υπολογίσουμε τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες τους σε $\mathcal{O}(1)$ (Εν 5.2) και άρα να υπολογίσουμε τις συντεταγμένες των σημείων που ενδιαφερόμαστε. Προκειμένου να ταιριάξουμε κατάλληλα τις λύσεις των R_x και R_y χρησιμοποιούμε τη γεωμετρία του προβλήματος.

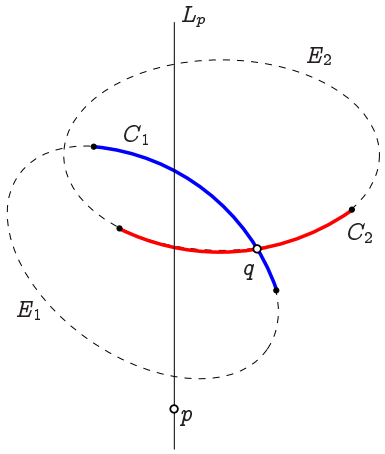
Ας θεωρήσουμε την κλίση της ευθείας E_y, η οποία είναι $s = -\frac{b}{c}$. Διακρίνουμε τις ακόλουθες περιπτώσεις (Σχ. 7.1):

- Αν $s > 0$, Σχ. 7.1 (a), τότε η μεγαλύτερη, κατά απόλυτη τιμή ρίζα του R_x αντιστοιχεί στη μεγαλύτερη ρίζα του R_y.
- Αν $s > 0$, Σχ. 7.1 (b), τότε η μεγαλύτερη ρίζα του R_x αντιστοιχεί στη μικρότερη ρίζα του R_y.
- Αν $s = 0$, Σχ. 7.1 (c), τότε η ευθεία E_y είναι οριζόντια και άρα η εξίσωση $R_y = 0$ έχει μια διπλή πραγματική ρίζα, η οποία είναι $-\frac{e}{c}$.

Σε κάθε περίπτωση μπορούμε να ταιριάξουμε τις ρίζες των R_x και R_y και άρα να υπολογίσουμε τις συντεταγμένες των σημείων με κατακόρυφη εφαπτομένη. Η έλλειψη διασπάται σε δύο τμήματα στο *άνω* και στο *κάτω*.

IS_ON_ARC

Μας δίνεται ένα x-μονότονο ελλειπτικό τόξο και ένα σημείο $\mathbf{p} = (p_x, p_y)$ και πρέπει να αποφασίσουμε αν το σημείο κείται εντός του τόξου. Τα p_x και p_y είναι πραγματικοί αλγεβρικοί αριθμοί, βαθμού ≤ 4. Καταρχάς, θα πρέπει το p_x να βρίσκεται εντός διαστήματος του x άξονα που ορίζουν οι x συντεταγμένες των άκρων του τόξου. Αυτό το ελέγχουμε με το κατηγόρημα COMPARE_X. Αν αυτό συμβαίνει τότε, θεωρούμε το πολυώνυμο f, όπως στην (7.1), που είναι η εξίσωση της έλλειψης που ορίζει το τόξο. Αν το $\mathbf{p}$ είναι σημείο του τόξου τότε πρέπει $\mathtt{sign}(f(p_x, p_y)) = 0$. Αυτό τον



Σχήμα 7.2: Τα κωνικά τόξα C_1 και C_2 ορίζονται από τις ελλείψεις E_1 και E_2. Η κατακόρυφη ευθεία L_p διέρχεται από το p. Η πλησιέστερη τομή των τόξων δεξιά από το p είναι το σημείο q. Στο σημείο p το τόξο C_1 είναι πάνω από το τόξο C_2.

έλεγχο τον κάνουμε με τον αλγόριθμο SIGN_AT (Εν. 5.5). Αν και αυτή η συνθήκη είναι αληθής τότε πρέπει να ελένξουμε αν το $\mathbf{p}$ βρίσκεται στο ίδιο (άνω ή κάτω) μέρος της έλλειψης με το τόξο. Θεωρούμε την εξίσωση f_y της ευθείας E_y από την (7.4) και ελέγχουμε το πρόσημό της όταν την αποτιμήσουμε πάνω στο $\mathbf{p} = (p_x, p_y)$, χρησιμοποιώντας πάλι τον αλγόριθμο SIGN_AT (Εν. 5.5). Αν $\mathrm{sign}(f_y(p_x, p_y)) < 0$ τότε το $\mathbf{p}$ είναι στο άνω μέρος, ενώ αν $\mathrm{sign}(f_y(p_x, p_y)) > 0$ τότε είναι στο κάτω.

NEAREST_INTERSECTION_TO_RIGHT

Δοθέντος ενός σημείου $\mathbf{p}$ και δύο x-μονότονων ελλειπτικών τόξων, C_1 και C_2, θέλουμε να υπολογίσουμε την πρώτη τομή των τόξων δεξιά από το $\mathbf{p}$ (Σχ. 7.2). Το $\mathbf{p}$ έχει προκύψει ως τομή κάποιων άλλων ελλειπτικών τόξων και άρα οι συντεταγμένες του είναι πραγματικοί αλγεβρικοί αριθμοί βαθμού ≤ 4. Θεωρούμε τις ελλείψεις E_1 και E_2 που ορίζουν τα τόξα C_1 και C_2 και χρησιμοποιώντας τον αλγόριθμο SOLVE (Εν. 5.5) υπολογίζουμε όλα τα σημεία τομής. Επιλέγουμε το σημείο τομής μικρότερη τετμημένη που είναι μεγαλύτερη από την τετμημένη του $\mathbf{p}$ ή με άλλα λόγια το σημείο τομής που είναι αμέσως δεξιά από την κατακόρυφη ευθεία L_p που περνά από το $\mathbf{p}$. Για να επιλέξουμε το σημείο πρέπει να συγκρίνουμε τις συντεταγμένες του με εκείνες του $\mathbf{p}$, χρησιμοποιώντας τα κατηγορήματα COMPARE_X και COMPARE_Y.

COMPARE_Y_AT_X

Το κατηγόρημα αποφασίζει αν ένα δοθέν ελλειπτικό τόξο είναι πάνω ή κάτω από ένα σημείο $\mathbf{p} = (p_x, p_y)$. Το κατηγόρημα υποθέτει ότι το $\mathbf{p}$ είναι εντός του τμήματος του x-άξονα που ορίζουν οι x συντεταγμένες των άκρων του τόξου και ότι δεν βρίσκεται πάνω στο τόξο. Έστω f, όπως στην (7.1), η εξίσωση της έλλειψης που ορίζει το τόξο και έστω ότι το τόξο είναι στο άνω μέρος της έλλειψης. Αν $\mathrm{sign}(f(p_x, p_y)) \leq 0$ τότε το σημείο είναι εντός της έλλειψης που ορίζει

το τόξο και συνεπώς το τόξο είναι πάνω από το $\mathbf{p}$. Διαφορετικά, το $\mathbf{p}$ κείται εκτός της έλλειψης και υπολογίζουμε τη θέση του σε σχέση με την ευθεία E_y, Εξ. (7.4), ελέγχοντας το πρόσημο $f_y(p_x, p_y)$. Αν το $\mathbf{p}$ είναι πάνω από την E_y τότε το τόξο είναι από κάτω, διαφορετικά είναι από πάνω. Αντίστοιχα επιχειρήματα ισχύουν και στην περίπτωση που το τόξο είναι στο κάτω μέρος της έλλειψης που το ορίζει. Οι υπολογισμοί του προσήμου γίνονται με τον αλγόριθμο SIGN_AT (Εν. 5.5).

COMPARE_Y_TO_RIGHT

Μας δίνονται δύο x-μονότονα ελλειπτικά τόξα, C_1 και C_2, τα οποία ορίζονται από ελλείψεις με εξισώσεις g_1 και g_2, αντίστοιχα, και ένα σημείο τομής τους $\mathbf{p} = (p_x, p_y)$. Τα τόξα είναι τέτοια ώστε να ορίζονται δεξιά από το $\mathbf{p}$ (δηλαδή για x μεγαλύτερο από p_x). Το κατηγόρημα αποφασίζει τη διάταξη των τόξων (πιο είναι από πάνω και πιο παό κάτω) αμέσως δεξιά από το σημείο $\mathbf{p}$.

Αν το $\mathbf{p}$ είναι το δεξιότερη τομή των g_1 και g_2 τότε έστω $\mathbf{q}$ εκείνο το δεξί άκρο των C_1 και C_2 με τη μικρότερη x συντεταγμένη. Ο υπολογισμός αυτός πραγματοποιείται με το κατηγόρημα COMPARE_X. Αν το $\mathbf{q}$ είναι το δεξί άκρο του C_1 τότε το κατηγόρημα αποφασίζεται με το κατηγόρημα COMPARE_Y_AT_X$(\mathbf{q}, C_2)$. Αντίστοιχα, αν είναι το δεξί άκρο του C_2, το κατηγόρημα αποφασίζεται με το κατηγόρημα COMPARE_Y_AT_X$(\mathbf{q}, C_1)$.

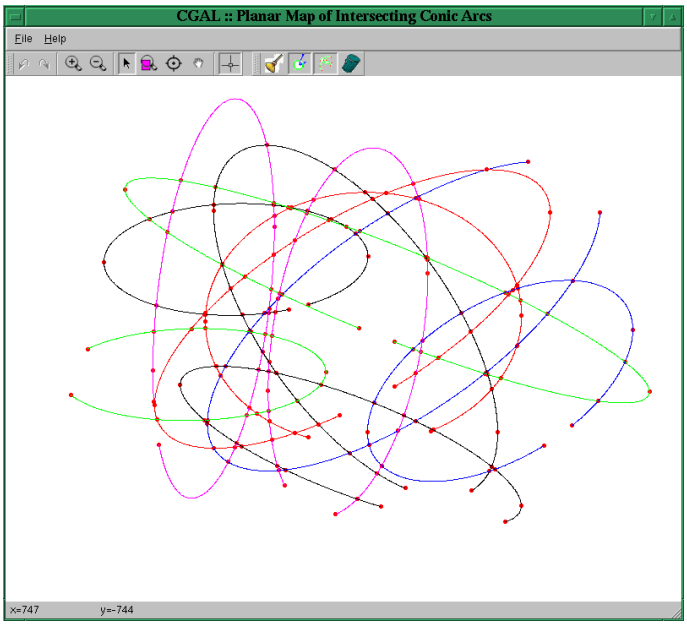
Αν το $\mathbf{p}$ δεν είναι η δεξιότερη τομή των g_1 και g_2, τότε εργαζόμαστε ως εξής: Οι συντεταγμένες του $\mathbf{p}$ είναι πραγματικοί αλγεβρικοί αριθμοί, βαθμού ≤ 4 και άρα το το p_x αναπαρίσταται ως $p_x \cong (A, \mathcal{I} = (\mathsf{a}, \mathsf{b}))$, όπου $A \in \mathbb{Z}[X]$, $\deg(A) \leq 4$ και $(\mathsf{a}, \mathsf{b}) \in \mathbb{Q}^2$.

Αφού το $\mathbf{p}$ δεν είναι η δεξιότερη τομή, υπάρχει κάποιο σημείο τομής $\mathbf{q} = (q_x, q_y)$, τέτοιο ώστε $p_x < q_x$. Επειδή οι πραγματικοί αλγεβρικοί αριθμοί είναι σε αναπαράσταση με διάστημα απομόνωσης θα πρέπει επίσης να ισχύει $p_x < \mathsf{b} < q_x$. Συνεπώς οι ελλείψεις ορίζονται για $x = \mathsf{b}$. Θεωρούμε τα πολυώνυμα $g_1(\mathsf{b}, y), g_2(\mathsf{b}, y) \in \mathbb{Z}[X]$, των οποίων οι ρίζες αντιστοιχούν στις y συντεταγμένες των τομών των C_1 και C_2 με την ευθεία $x = \mathsf{b}$. Ταξινομούμαι τις ρίζες των πολυωνύμων (συγκρίνοντάς τες) και συνάγουμε τη διάταξη των τόξων.

Περί της υλοποίησης

Έχουμε υλοποιήσει τον αλγόριθμο διάταξης ελλειπτικών τόξων στο επίπεδο. Αν και ευρέως θεωρείται ότι η υλοποίηση είναι πολύ λιγότερο σημαντική από τη θεωρητική ανάλυση των αλγορίθμων, αυτό δεν ισχύει για κανένα λόγο για τους γεωμετρικούς και αλγεβρικούς αλγορίθμους. Η υλοποίησή μας χρησιμοποιεί τις πιο σύγχρονες προγραμματιστικές τεχνικές γενικού προγραμματισμού σε C++ και βασίζεται στη βιβλιοθήκη SYNAPS για τους αλγερικούς υπολογισμούς και στη βιβλιοθήκη CGAL για τους γεωμετρικούς. Το κύριο μέρος του σχεδιασμού και της υλοποίησης οφείλεται στο Θάναση Κακαργιά και αποτέλεσε σημαντικό μέρος της διπλωματικής του εργασίας [141]. Η υλοποίηση προσφέρει και δυνατότητες οπτικοποίησης με τη χρήση της βιβλιοθήκης QT[5] και έγινε με χρήση της γεωμετρικής βιβλιοθήκης CGAL. Ο υπολογισμός της διάταξης πραγματοποιείται είτε με τον αυξητικό αλγόριθμο είναι με τον αλγόριθμο σάρωσης. Στη συνέχεια το αποτέλεσμα παρουσιάζεται ως ένα σύνολο από ελλειπτικά τόξα μαζί με τα άκρα τους, τα οποία είναι είτε x-ακρότατα σημεία, είτε σημεία τομής, είτε άκρα των αρχικών ελλειπτικών τόξων. Στο

[5] `http://www.trolltech.com/`



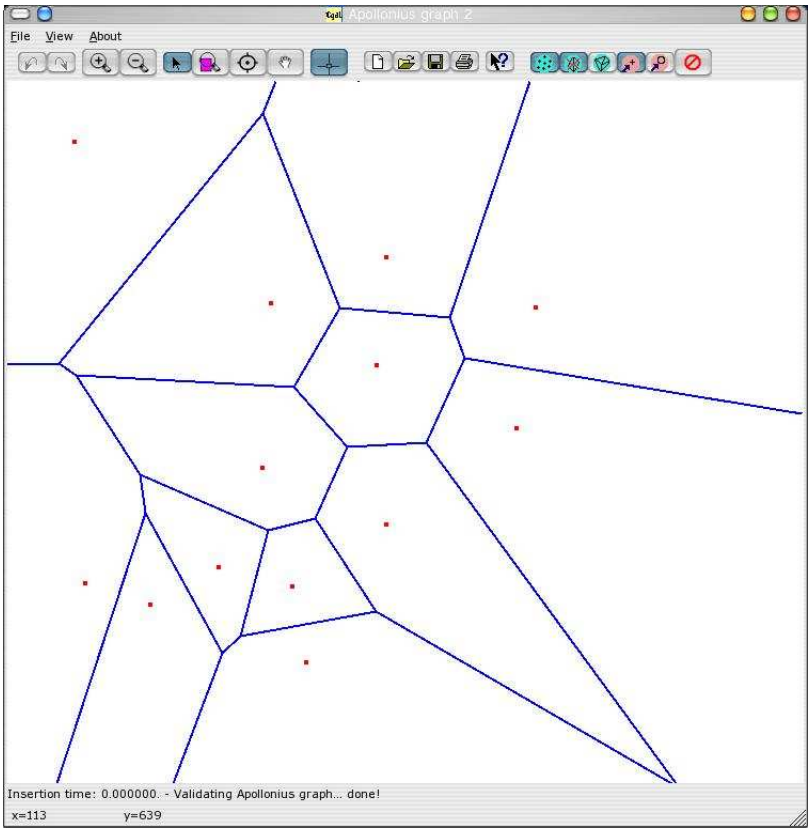
Σχήμα 7.3: Διάταξη ελλειπτικών τόξων στο επίπεδο

Σχ. 7.2 μπορείτε να δείτε μια διάταξη ελλειπτικών τόξων στο επίπεδο. Ο αναγνώστης που ενδιαφέρεται για τις λεπτομέρειες της υλοποίησης και για διάφορα πειραματικά αποτελέσματα μπορεί να ανατρέξει Emiris et al. [96], Fogel et al. [106], Kakargias [141], Kakargias and Pion [142].

7.3 Διάγραμμα Voronoi ελλείψεων στο επίπεδο

Στην παρούσα ενότητα θα παρουσιάζουμε τα κατηγορήματα που απαιτούνται από τους πλήρεις και ακριβείς αλγορίθμους για τον υπολογισμό των γενικών διαγραμμάτων Voronoi (abstract Voronoi diagrams) [158] και πιο συγκεκριμένα, από τον αυξητικό αλγόριθμο των Karavelas and Yvinec [150], για την περίπτωση όπου τα γεωμετρικά αντικείμενα είναι ολόκληρες και μη τεμνόμενες ελλείψεις. Για να είμαστε πιο ακριβείς, ο αλγόριθμος υπολογίζει τον γράφο της τριγωνοποίησης Delaunay, καθώς δεν απαιτεί υπολογισμό των συντεταγμένων των κορυφών ή των ακμών Voronoi. Ωστόσο, αν κάποιος θα ήθελε να σχεδιάσει, για παράδειγμα με κάποια καθορισμένη αριθμητική ακρίβεια, ο αλγόριθμος και οι μέθοδοι που παρουσιάζουμε προσφέρουν την απαραίτητη πληροφορία. Επίσης, μερικά από τα κατηγορήματα που θα παρουσιάσουμε απαιτούνται τόσο από τους αλγορίθμους που υπολογίζουν το πλέγμα ορατότητας (visibility complex) όσο και από τους αλγορίθμους που υπολογίζουν το κυρτό περίβλημα ελλείψεων. Ο τελικός μας στόχος είναι ένα πακέτο λογισμικού που θα ενσωματωθεί στη βιβλιοθήκη CGAL, το οποίο θα κατασκευάζει το διάγραμμα Voronoi ελλείψεων και θα βασίζεται στην υλοποίηση που υπάρχει για κύκλους [85, 149], και η οποία χρησιμοποιεί τον αυξητικό αλγόριθμο.

Δοθέντων ενός συνόλου n γεωμετρικών αντικειμένων, *εστίες* (sites), στον $\mathbb{R}^d$, το διάγραμμα Voronoi που επάγουν είναι μια διαμέριση του $\mathbb{R}^d$ σε κελιά (ή περιοχές), τέτοια ώστε τα σημεία που ανήκουν σε κάθε περιοχή να είναι *κοντύτερα*, με κάποια έννοια απόστασης, σε κάποια



Σχήμα 7.4: Διάγραμμα Voronoi σημείων στο επίπεδο.

εστία, από οποιαδήποτε άλλη εστία του συνόλου των εστιών. Μπορούμε να ορίσουμε διάφορα διαγράμματα Voronoi ανάλογα με τον γεωμτρικό τύπο των εστιών, την έννοια της απόστασης, το χώρο που ανήκουν οι εστίες κτλ. Συνήθως ως χώρο θεωρούμε έναν Ευκλείδιο χώρο και η απόσταση είναι η Ευκλείδια απόσταση. Η προσέγγισή μας αφορά εστίες που είναι ολόκληρες και μη τεμνόμνες ελλείψεις στο επίπεδο και ως απόσταση θεωρούμε την Ευκλείδια απόσταση.

Τα διαγράμματα Voronoi έχουν μελετηθεί πάρα πολύ, ωστόσο ο κύριος όγκος των εργασιών για το επίπεδο αφορά σημειακές ή γραμμικές εστίες. Ένα τέτοιο διάγραμμα παρουσιάζεται στο Σχ. 7.3, το οποίο υπολογίστηκε με το αντίστοιχο λογισμικό που υπάρχει στη CGAL και οφείλεται στον Karavelas [147]. Μια συναφή με τη δική μας προσέγγιση, η οποία υπολογίζει το διάγραμμα Voronoi κυρτών πολυγώνων είναι αυτή των McAllister et al. [182]. Είναι πολύ πρόσφατες οι προσπάθειες επέκτασης των διαγραμμάτων Voronoi σε περιπτώσεις όπου οι εστίες είναι αλγεβρικές καμπύλες [7, 9] ή που έχουν μη κενό εσωτερικό [28]. Πιο συγκεκριμένα, το διάγραμμα Voronoi κύκλων έχει υλοποιηθεί στη CGAL [85]· δείτε επίσης [10, 156].

Οι Harrington et al. [128] προτείνουν ένα βέλτιστο συνδυαστικό αλγόριθμο για την κατασκευή διαγραμμάτων Voronoi για αυστηρά κυρτά στρογγυλευμένα αντικείμενα στον $\mathbb{R}^3$, αλλά δεν ασχολήθηκαν με τα κατηγορήματα. Οι Boissonnat and Delage [27] παρουσιάζουν ένα δυναμικό αλγόριθμο για την κατασκευή δυναμικών διαγραμμάτων power diagrams σημείων στον $\mathbb{R}^d$. Αυτά τα διαγράμματα αντιστοιχούν σε διαγρμμάτα Voronoi κύκλων ή σφαιρών, αλλά δεν

φαίνεται να καλύπτουν την περίπτωση των κύκλων. Μια άλλη πρόσεγγιση, η οποία είναι αρκετά επιτυχημένη, είναι η προσέγγιση των καμπύλων εστιών με πολύγωνα [11]. Οι Boada et al. [26] υπολογίζουν μια πολυγωνική προσέγγιση ενός διαγράμματος Voronoi για διάφορα επίπεδα λεπτομέρειας (ακρίβειας). Αναμένουμε στις εφαρμογές, όπως για παράδειγμα στην πλοήγηση ανάμεσα σε αντικείμενα (εμπόδια), να επωφεληθούμε τα μάλλα από το ακριβές διάγραμμα των ελλείψεων, καθώς οι ελλείψεις μας δίνουν τη δυνατότητα να μοντελοποιήσουμε, με αρκετή ακρίβεια, διαφόρων ειδών εμπόδια.

Ίσως η πρόσεγγιση η οποία ομοιάζει περισσότερο στη δική μας να είναι αυτή των Hanniel et al. [127], οι οποίοι διατρέχουν τους διχοτόμους, προκειμένου να υπολογίσουν τα Voronoi κελλιά αυθαίρετων καμπυλών μέχρι την ακρίβεια της μηχανής. Ο αλγόριθμός τους χρησιμοποιεί αριθμητική κινητής υποδιαστολής και ισχυρίζονται ότι η προσέγγισή τους έχει πολύ καλά πρακτικά αποτελέσματα. Αν και ισχυρίζονται ότι η μέθοδός τους επεκτείνεται έτσι ώστε οι υπολογισμοί να εμπεριέχουν μόνο ακριβή αριθμητική, δεν εξηγούν το πως. Για παράδειγμα δεν σχολιάζουν καθόλου εκφυκισμένες καταστάσεις. Η υλοποίησή μας είναι ακριβής, αλλά μπορεί να τρέξει και με κάποια προκαθορισμένη ακρίβεια.

Τα 4 κατηγορήματα του αυξητικού αλγορίθμου των Karavelas and Yvinec [150] και τα οποία θα εξετάσουμε είναι:

κ_1 δοθέντων δύο ελλείψεων και ενός σημείου εξωτερικού και για τις δύο υπολογίζεται η έλλειψη που είναι κοντύτερα (με την έννοια της απόστασης) στο σημείο.

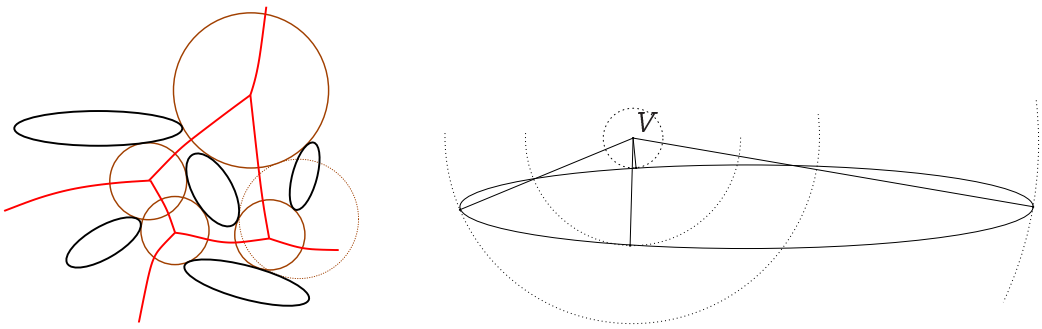
κ_2 δοθέντων δύο ελλείψεων, υπολογίζεται η σχετική θέση μιας τρίτης έλλειψης σχετικά με ευθεία που εφάπτεται εξωτερικά ταυτόχρονα στις δύο ελλείψεις.

κ_3 δοθέντων τριών ελλείψεων, υπολογίζεται η θέση μιας τέταρτης έλλειψης σχετικά με τον Voronoi κύκλο των τριών. Αυτό είναι το InCircle κατηγόρημα [29, 30].

κ_4 δοθέντων τεσσάρων ελλείψεων, υπολογίζεται πιο τμήμα της διχοτόμου μεταβάλλεται εξαιτίας της εισαγωγής μιας $5^{ης}$ έλλειψης.

Οι αλγόριθμοι για τα κατηγορήματα κ_1 και κ_2 που θα παρουσιάσουμε είναι βέλτιστοι όσον αφορά τον βαθμό των πραγματικών αλγεβρικών αριθμών που χρειαζόμαστε για τους υπολογισμούς. Στην πραγματικότητα με το κ_2 υπολογίσουμε και χαρακτηρίζουμε όλες τις εφαπτόμενες ευθείες ταυτόχρονα εφαπτόμνες σε δύο ελλείψεις και παρέχουν και επιπλέον πληροφορία. Οι αλγόριθμοι είναι ακριβείς, πλήρεις και υλοποιημένοι σε C++. Για την υλοποίηση των κ_1 και κ_2 και για διάφορα πειραματικά αποτελέσματα ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία [99]. Τα σημεία επαφής των εφαπτόμενων υπολογίζονται ή όχι ανάλογα με τον χρησιμοποιούμε την πεπλεγμένη ή την παραμετρική αναπαράσταση των ελλείψεων. Ένα παρόμοιο πρόβλημα είναι το πλέγμα ορατότητας ανάμεσα σε ελλείψεις [124], ή ανά δύο ξένων κυρτών συνόλων με σταθερή πολυπλοκότητα [8]. Πιο συγκεκριμένα, σε αυτά τα προβλήματα, απαιτείται ο υπολογισμός και ο καθορισμός (αν είναι εξωτερικές ή εσωτερικές) των ευθειών που είναι ταυτόχρονα εφαπτόμενες σε δύο ελλείψεις. Το κατηγόρημα κ_2 απαντά επιλύει αυτό το πρόβλημα.

Η υλοποίηση του κ_3 αντιστοιχεί στην (πραγματική) επίλυση ενός πολυωνυμικού συστήματος. Χρησιμοποιώντας την πεπλεγμένη αναπαράσταση, υπολογίζουμε το φράγμα στο πλήθος των μιγαδικών λύσεων του συστήματος και συνεπώς το φράγμα στον αριθμό των *μιγαδικών* κύκλων



Σχήμα 7.5: Αριστερά: Το Voronoi διάγραμμα 5 ελλείψεων. Δεξιά: ένα σημείο με 4 κανονικά διανύσματα.

που είναι εφαπτόμενοι σε 3 ελλείψεις. Το φράγμα είναι 184 και είναι βέλτιστο. Ο αριθμός των πραγματικών κύκλων είναι ακόμα ανοιχτό πρόβλημα. Ο Anton [9] εξετάζει το κατηγόρημα κ_3 για το διάγραμμα ελλείψεων αλλά το πολυωνυμικό σύστημα στο οποίο καταλήγει έχει πολύ μεγάλο μικτό όγκο, κατά συνέπεια η προσέγγισή του έχει πολύ μεγάλη πολυπλοκότητα και επίσης δεν εξασφαλίζει το ακριβές του αποτελέσματος.

Ωστόσο, ακόμα και το (βέλτιστο) πολυωνυμικό σύστημα που προκύπτει από τη μελέτη μας για το κ_3 είναι πολύ μεγάλης πολυπλοκότητας και επιπρόσθετα η επίλυσή του δεν αρκεί για την υλοποίηση του κατηγορήματος. Δια τούτο δεν είναι αποτελεσματική η επίλυσή του με αλγορίθμους και λογισμικά γενικού σκοπού για την επίλυση πολυωνυμικών συστημάτων. Αντ' αυτού έχουμε προτείνει [98, 99] έναν αλγόριθμο υποδιαίρεσης, ειδικά προσαρμοσμένο στο γεωμετρικό πρόβλημα που απαντά στο κατηγόρημα και είναι ακριβής και πλήρης. Όπως όλοι οι αλγόριθμοι υποδιαίρεσης εξαρτάται από τα φράγματα διαχωρισμού, καθώς πρέπει να είναι γνωστό εκ των προτέρων ποιος είναι ο μέγιστος αριθμός δυαδικών ψηφίων (στη χειρότερη περίπτωση) που απαιτείται για τους υπολογισμούς, προκειμένου το αποτέλεσμα να είναι ακριβές σε κάθε περίπτωση. Αυτή τη θεωρητική ανάλυση, η οποία ισχύει όχι μόνο για τον δικό μας αλγόριθμο υποδιαίρεσης αλλά και για οποιονδήποτε άλλο, για το κ_3 θα παρουσιάσουμε σε επόμενη ενότητα.

Η πλήρης υλοποίηση του κ_3, όπως και του πλήρους αλγορίθμου για το διάγραμμα Voronoi ελλείψεων στο επίπεδο, αποτελεί αντικείμενο της διδακτορικής διατριβής του Γιώργου Τζούμα και γιαυτό δεν την παρουσιάζουμε. Το κατηγόρημα κ_4 υλοποιείται με δύο κλήσεις του κατηγορήματος κ_3 [99, 150], και για τους ίδιους λόγους με προηγουμένως, επίσης δεν θα το παρουσιάσουμε. Ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία για περισσότερες πληροφορίες [94, 98, 99, 254].

Από όσο είμαστε σε θέση να γνωρίζουμε, η προσπάθειά μας είναι η πρώτη πλήρης προσέγγιση σχετικά με την υλοποίηση του διαγράμματος Voronoi ελλείψεων (δια μέσου του γράφου Delaunay) στο επίπεδο με ακριβείς υπολογισμούς. Ένα παράδειγμα διάγραμματος Voronoi ελλείψεων παρουσιάζεται στο Σχ.7.5.

Το κατηγόρημα κ_1

Στο κατηγόρημα κ_1, μας δίνονται 2 ελλείψεις και ένα σημείο έξω και από τις δύο και θέλουμε να υπολογίσουμε την κοντυνότερη, με την έννοια της Ευκλείδιας απόστασης, έλλειψη στο σημείο.

Καταρχάς υπολογίζουμε ένα κάτω φράγμα στην έμφυτη πολυπλοκότητα του προβλήματος. Αν θεωρήσουμε ένα σημείο V εκτός μιας έλλειψης τότε υπάρχουν μέχρι 4 κανονικά διανύσματα της έλλειψης, των οποίων οι ευθείες που ορίζουν διέρχονται από το V. Το ακριβές πλήθος των κανονικών διανυσμάτων εξαρτάται από από τη θέση του V σε σχέση με την *εξειλιγμένη* evolute) της καμπύλης (έλλειψης), η οποία είναι ένα αστροειδές. Υπάρχουν 4 κανονικά διανύσματα αν το V κείται εντός της εξειλιγμένης, 3 είναι σημείο της εξειλιγμένης αλλά όχι ακίδα (cusp) ή 2 αν το V είναι πάνω σε κάποια ακίδα ή εκτός της εξειλιγμένης. Ένα παράδειγμα σημείο με 4 κανονικά διανύσματα παρουσιάζεται στο Σχ. 7.5.

Θεωρούμε μια έλλειψη E, η οποία είναι σε πεπλεγμένη μορφή και ένα σημείο $V = (v_1, v_2)$ εκτός αυτής. Συμβολίζουμε με $C(V, \sqrt{s})$ έναν κύκλο, ο οποίος έχει κέντρο το V και ακτίνα ίση με $\sqrt{s}$, όπου $s > 0$. Εκφράζουμε την *Ευκλείδια απόσταση* $\delta(V, E)$ των V και E ως την *μικρότερη* θετική τιμή του $\sqrt{s}$ για την οποία ο κύκλος C είναι εφαπτόμενος στην E. Προκειμένου να συγκρίνουμε αποστάσεις αρκεί να θεωρήσουμε το τετράγωνο της απόστασης, δηλαδή το s.

Μια κωνική τομή μπορεί να αναπαρασταθεί με τη χρήση πινάκων ως

$$\left[\ x, y, 1\ \right]\ M\ \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

όπου M είναι κάποιος κατάλληλος πίνακας. Με αυτό τον συμβολισμό, οι πίνακες που αντιστοιχούν στα E και C είναι

$$A = \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}, \qquad B(s) = \begin{pmatrix} 1 & 0 & -v_1 \\ 0 & 1 & -v_2 \\ -v_1 & -v_2 & v_1^2 + v_2^2 - s \end{pmatrix}.$$

Η *δέσμη* (pencil) των E και C είναι $\lambda A + B$ και το χαρακτηριστικό της πολυώνυμο είναι

$$\varphi(\lambda) = \det(\lambda A + B(s)) = J_2^2\,\lambda^3 + c_2(s)\,\lambda^2 + c_1(s)\,\lambda + s \tag{7.7}$$

όπου

$$\begin{aligned} c_2(s) = J_2 s - T(v_1, v_2), \quad c_1(s) &= J_1 s - E(v_1, v_2), \\ T(v_1, v_2) &= J_2\left[(v_1 - x_c)^2 + (v_2 - y_c)^2 - J_1\right]. \end{aligned}$$

Παρατηρούμε ότι $\phi(\lambda)$ είναι ένα κυβικό πολυώνυμο ως προς λ, του οποίου η διακρίνουσα (Εν. 5.2) είναι:

$$\begin{aligned} \Delta(s) \;=\; & J_2^2(J_1^2 - 4J_2)\,s^4 + \\ & 2J_2(9J_1J_2^2 - J_1^2T + 6J_2T - 2J_1^3J_2 - J_1J_2E)\,s^3 + \\ & (-18J_2^3E + 4J_1J_2ET - 27J_2^4 + J_1^2T^2 - 18J_1J_2^2T \\ & + J_2^2E^2 + 12J_1^2J_2^2E - 12J_2T^2)\,s^2 + \\ & 2(2T^3 - J_1ET^2 - 6J_1J_2^2E^2 + 9J_2^2ET - J_2E^2T)\,s + \\ & E^2(T^2 + 4J_2^2E) \end{aligned} \tag{7.8}$$

όπου $E = E(v_1, v_2)$ και $T = T(v_1, v_2)$,

Ένας κύκλος είναι εξωτερικά εφαπτόμενος σε μία έλλειψη αν και μόνο αν το $\varphi(\lambda)$ έχει μια διπλή θετική ρίζα [265, Θεωρ. 8], [101, Εν. 4]. Εφόσον θέλουμε το $\phi(\lambda)$ να έχει πολλαπλή ρίζα, πρέπει η διακρίνουσά του, $\Delta(s)$, να μηδενίζεται. Το $\Delta(s)$ είναι ένα πολυώνυμο, ως προς s, βαθμού 4.

Η απόσταση $\delta(V, E)$ είναι η τετραγωνική ρίζα της μικρότερης θετικής ρίζας του $\Delta(s)$. Ο (συνολικός) αλγεβρικός βαθμός των συντελεστών του $\Delta(s)$, ως προς τις μεταβλητές v_1, v_2 και τις παραμέτρους της E (a, b, c, d, e, f), είναι 6, 8, 10, 12, και 14, θεωρώντας τους σε φθίνουσα διάταξη ως προς τη δύναμη του s. Αν θεωρήσουμε το Δ πολυώνυμο ως προς τρεις μεταβλητές, τις v_1, v_2 και s, τότε ο (συνολικός) αλγεβρικός βαθμός των συντελεστών του, που είναι πολυώνυμα ως προς τα a, b, c, d, e, f είναι 6.

Πρόταση 7.1. *Δοθέντων δύο ελλείψεων E_1, E_2 και ενός σημείου V εκτός και των δύο, μπορούμε να αποφασίσουμε ποια έλλειψη είναι κοντύτερα (με την έννοια της Ευκλείδιας απόστασης) σε αυτό συγκρίνοντας δύο πραγματικούς αλγεβρικούς αριθμούς βαθμού 4.*

Απόδειξη: Θεωρούμε τα δύο πολυώνυμα $\Delta_1(s)$ και $\Delta_2(s)$, των οποίων οι μικρότερες θετικές ρίζες εκφράζουν τις αποστάσεις $\delta(E_1, V)$ και $\delta(E_2, V)$. Οι αποστάσεις είναι πραγματικοί αλγεβρικοί αριθμοί βαθμού ≤ 4 τους οποίους κατασκευάζουμε και συγκρίνουμε χρησιμοποιώντας τους αλγορίθμους του Κεφ. 5. ΟΕΔ

Ο βαθμός είναι βέλτιστος ως προς τους πραγματικούς αλγεβρικούς αριθμούς που συγκρίνονται. Αυτό προκύπτει από το γεγονός ότι, στη χειρότερη περίπτωση, ένα σημείο εκτός μιας έλλειψης έχει μέχρι 4 κανονικά διανύσματα, που διέρχονται από αυτό. Συνεπώς η απόστασή του από μια έλλειψη εκφράζεται με ένα πραγματικό αλγεβρικό αριθμό βαθμού 4, στη χειρότερη περίπτωση.

Αξίζει να τονίσουμε ότι αν περιορίζόμασταν στην παραμετρική αναπαράσταση τότε πρέπει να συγκρίνουμε πραγματικούς αλγεβρικούς αριθμούς βαθμού 8. Συνεπώς για το κ_1 είναι προτιμότερη η πεπλεγμένη αναπαράσταση.

Το κατηγόρημα κ_2

Το κ_2 αποφασίζει τη θέση μιας έλλειψης σχετικά με μία ευθεία η οποία είναι ταυτόχρονα εφαπτόμενη σε δύο άλλες ελλείψεις. Με το όρο θέση εννοούμε το εξής: Η ευθεία χωρίζει το επίπεδο σε δύο ημιεπίπεδα, ανδιαφερόμαστε να υπολογίσουμε αν η τρίτη έλλειψη κείται εξολοκλήρου σε κάποιο από τα δύο, αν είναι εφαπτόμενη στην ευθεία ή αν την τέμνει. Στη πραγματικότητα ο αλγόριθμος που θα παρουσιάσουμε υπολογίζει επιπλέον πληροφορία σχετικά με ευθείες που είναι εφαπτόμενες σε δύο ελλείψεις. Αυτή την επιπλέον πληροφορία μπορούμε να τη χρησιμοποιήσουμε προκειμένου να διευκολύνουμε μελλοντικές κλήσεις στο κ_2.

Θεωρούμε την ευθεία $L : y = ux + v$ (η οποία δεν είναι κατακόρυφη) και την έλλειψη E στην πεπλεγμένη μορφή της, όπως στην (7.1). Τα σημεία τομής της L και της E είναι λύσεις του συστήματος $L = E = 0$. Ωστόσο καθώς η εξίσωση της L είναι γραμμική μπορούμε να λύσουμε

ως προς y και αντικαταστήσουμε στην εξίσωση της E. Έτσι προκύπτει το πολυώνυμο

$$R := \left(2\,bu + a + cu^2\right)x^2 + \left(2\,cvu + 2\,d + 2\,eu + 2\,bv\right)x + f + cv^2 + 2\,ev$$

που είναι δευτέρου βαθμού ως προς x και του οποίου οι ρίζες είναι οι x συντεταγμένες των σημείων τομής της L και της E. Η διακρίνουσα του R είναι

$$\begin{aligned}\Lambda(u,v) =&(-ac + b^2)v^2 + (2\,cd - 2\,eb)vu + (-fc + e^2)u^2\\ &+ (-2\,ae + 2\,db)v + (2\,de - 2\,fb)u + -af + d^2\end{aligned}$$

Το $\Lambda(u,v)$ είναι πολυώνυμο ως προς u και v (συνολικού) βαθμού 2. Αν η L είναι εφαπτόμενη στην E τότε πρέπει το L να έχει μία διπλή ρίζα, καθώς υπάρχει μόνο ένα σημείο τομής και συνεπώς πρέπει η διακρίνουσά του να μηδενίζεται, δηλαδή $\Lambda(u,v) = 0$.

Αν τώρα θεωρήσουμε δύο ελλείψεις E_1 και E_2 και μία ευθεία L τότε η L είναι εφαπτόμενη και στις δύο αν το σύστημα

$$\Lambda_1(u,v) = \Lambda_2(u,v) = 0$$

έχει (πραγματικές) λύσεις, όπου ο μηδενισμός της Λ_1 (Λ_2) εκφράζει το γεγονός ότι η L είναι εφαπτόμενη στην E_1 (E_2). Το σύστημα είναι συνολικού βαθμού δύο και μπορεί να επιλυθεί με τον αλγόριθμο SOLVE (Εν. 5.5), σταθερό χρόνο. Έχει (το πολύ) 4 πραγματικές λύσεις, η οποίες αντιστοιχούν σε 4 ευθείες που είναι ταυτόχρονα εφαπτόμενες σε δύο ελλείψεις. Μια (κοινή) εφαπτόμενη δύο ελλείψεων θα ονομάζεται εξωτερική όταν το ευθύγραμμο τμήμα που ορίζεται από τα δύο εφαπτομενικά σημεία ανήκει στο κυρτό περίβλημα των δύο ελλείψεων και εσωτερική όταν το τμήμα είναι εντός του κυρτού περιβλήματος.

Ας υποθέσουμε ότι έχουμε υπολογίσει τις 4 εφαπτόμενες ευθείες και έστω $\overline{L}: \; y = \overline{u}\,x + \overline{v}$ μία από αυτές. Υπενθυμίζουμε ότι τα $\overline{u}$ και $\overline{v}$ είναι πραγματικοί αλγεβρικοί αριθμοί βαθμού ≤ 4. Έστω (x_{c_1}, y_{c_1}) και (x_{c_2}, y_{c_2}) τα κέντρα των E_1 και E_2. Μια ευθεία είναι εξωτερικά εφαπτόμενη σε δύο ελλείψεις αν και μόνο αν η εξίσωσή της έχει το ίδιο πρόσημο όταν αποτιμηθεί σε εσωτερικά σημεία των ελλείψεων. Συνεπώς η $\overline{L}$ είναι εξωτερική αν και μόνο αν $\mathrm{sign}(L(x_{c_1}, y_{c_1})) \cdot \mathrm{sign}(L(x_{c_1}, y_{c_1})) > 0$. Ο υπολογισμός $\mathrm{sign}(L(x_{c_1}, y_{c_1}))$ μπορεί να αναχθεί σε σύγκριση πραγματικών αλγεβρικών αριθμών βαθμού ≤ 4 και για τον υπολογισμό χρησιμοποιούμε τον αλγόριθμο COMPARE (Εν. 5.3). Ο βαθμός είναι βέλτιστος, όσον αφορά τους πραγματικούς αλγεβρικούς αριθμούς που εμπλέκονται, καθώς υπάρχουν μέχρι 4 εφαπτόμενες. Αν η L είναι κατακόρυφη τότε αναγόμαστε σε πιο εύκολο σύστημα, γιαυτό και δεν εξετάζουμε αυτή την περίπτωση.

Κατά συνέπεια έχουμε υπολογίσει και χαρακτηρίσει τις 4 εφαπτόμενες. Πως όμως υπολογίζουμε το κ_2; Ας υποθέσουμε ότι μας έχουν δοθεί δύο ελλείψεις E_1 και E_2 και μια ευθεία $\overline{L}: \; y = \overline{u}\,x + \overline{v}$, που είναι εξωτερικά εφαπτόμενη και στις δύο. Η θέση μιας τρίτης έλλειψης E_3 ως προς την L, υπολογίζεται με τη βοήθεια της διακρίνουσας $\Lambda_3(\overline{u}, \overline{v})$ που προκύπτει από το σύστημα $\overline{L} = E_3 = 0$, Αν αποτιμήσουμε το Λ_3 πάνω στις πραγματικές λύσεις του συστήματος $\Lambda_1(u,v) = \Lambda_2(u,v) = 0$, τότε το πρόσημό του είναι αρνητικό, μηδέν ή θετικό αν και μόνο αν η E_3 έχει 0, 1 ή 2 κοινά σημεία με την $\overline{L}$, αντίστοιχα. Αν το πρόσημο είναι 0 ή 1 και (x_{c_3}, y_{c_3}) είναι το κέντρο της E_3 τότε το πρόσημο της αποτίμησης $\overline{L}(x_{c_3}, y_{c_3})$ καθορίζει σε ποιο από τα δύο ημιεπίπεδα που ορίζει η $\overline{L}$ κείται η E_3. Τα πρόσημα των αποτιμήσεων υπολογίζονται σε σταθερό χρόνο τον αλγόριθμο SIGN_AT (Εν. 5.5).

Οπότε καταλήγουμε στην ακόλουθη πρόταση:

Πρόταση 7.2. *Η σχετική θέση μιας έλλειψης E_3 ως προς μια εξωτερική εφαπτομένη των ελλείψεων E_1, E_2 απαιτεί υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς βαθμού ≤ 4.*

Μπορούμε ωστόσο να υλοποιήσουμε το κ_2 και στην περίπτωση που ελλείψεις είναι στην παραμετρική τους αναπαράσταση και μάλιστα με λιγότερους υπολογισμούς. Ας θεωρήσουμε ότι οι δύο αρχικές μας ελλείψεις είναι οι E_t και E_r και ότι η έλλειψη για την οποία γίνεται η ερώτηση είναι η E_s και ότι είναι στην παραμετρική τους αναπαράσταση, όπως στην (7.2) με παραμέτρους t, r και s, αντίστοιχα.

Ας θεωρήσουμε την εφαπτόμενη σε ένα σημείο $(x(t), y(t))$ της έλλειψης E_t. Η εξίσωση της πεπλεγμένης αναπαράστασης της (εφαπτόμενης) ευθείας είναι

$$(y - y(t))\ x'(t) - (x - x(t))\ y'(t) = 0.$$

Αν αντικαταστήσουμε τα $x(t)$ και $y(t)$ από την (7.2) προκύπτει ένα πολυώνυμο βαθμού 2 ως προς t, αφού απαλοίψουμε τον παρανομαστή $(1+w^2)(1+t^2)^2$. Οι συντελεστές του πολυωνύμου είναι πολυώνυμα ως προς x και y.

Αν αντικαστήσουμε τα x και y με $x(r)$ και $y(r)$ από την έλλειψη E_r τότε προκύπτει ένα δευτεροβάθμιο πολυώνυμο ως προς r, του οποίου οι ρίζες αντιστοιχούν στα σημεία όπου η εφαπτόμενη (ευθεία) στην E_t τέμνει την E_r. Η διακρίνουσα του πολυωνύμου, $\Lambda_{tr}(t)$, μηδενίζεται, όταν η ευθεία είναι εφαπτόμενη και στις δύο ελλείψεις. Υπενθυμίζουμε ότι μια ευθεία είναι εξωτερικά εφαπτόμενη σε δύο ελλείψεις αν και μόνο αν η εξίσωσή της έχει το ίδιο πρόσημο όταν αποτιμηθεί σε εσωτερικά σημεία των ελλείψεων. Για την E_t το πρόσημο είναι πάντοτε θετικό, καθώς η εξίσωσή της γίνεται $2\alpha\beta(1+w^2)(1+t^2)$. Συνεπώς, για να αποφασίσουμε τον τύπο της εφαπτόμενης ευθείας αρκεί να υπολογίσουμε το πρόσημο ενός δευτεροβαθμίου πολυωνύμου, όταν αυτό αποτιμηθεί πάνω σε ένα πραγματικό αλγεβρικό αριθμό βαθμού 4. Ο βαθμός είναι βέλτιστος, όσον αφορά τους πραγματικούς αλγεβρικούς αριθμούς που εμπλέκονται. Έστω $t_1 < t_2 < t_3 < t_4$ οι πραγματικές ρίζες του $\Lambda_{tr}(t)$. Έστω μ μια εσωτερική εφαπτόμενη και ϵ μια εξωτερική. Τότε η (t_1, t_2, t_3, t_4) αντιστοιχεί σε κάποια κυκλική μετάθεση των $(\mu\epsilon\epsilon\mu)$. Δοθέντων 2 ελλείψεων, προκειμένου να υπολογίσουμε την μετάθεση των εφαπτομένων, αρκεί να υπολογίσουμε τον τύπο δύο από αυτές.

Οπότε καταλήγουμε στην ακόλουθη πρόταση:

Θεώρημα 7.3

Η σχετική θέση μιας έλλειψης E_3 ως προς μια εξωτερική εφαπτομένη των ελλείψεων E_1, E_2 προκύπτει από το πρόσημο του $\Lambda_{ts}(t)$, το οποίο έχει βαθμό 4, όταν αποτιμηθεί πάνω στο $\hat{t}$, το οποίο είναι ρίζα του $\Lambda_{tr}(t)$ (επίσης βαθμού 4). Τώρα $\operatorname{sign}(\Lambda_{ts}(\hat{t})) = -1, 0$, ή 1 αν και μόνο αν E_s δεν τέμνει, είναι εφαπτόμενη, τέμνει την ευθεία, αντίστοιχα.

Το κατηγόρημα κ_3

Δοθέντων 3 ελλείψεων, E_1, E_2 και E_3, θεωρούμε ένα εξωτερικά εφαπτόμενο κύκλο και στις τρεις, οποίος είναι γνωστός ως Voronoi κύκλος. Εάν υπάρχουν 2 τέτοιοι κύκλοι, τότε υποθέτουμε ότι

αναφερόμαστε μόνο στον έναν Θέλουμε να υπολογίσουμε τη σχετική θέση μιας τέταρτης έλλειψης, E_0 ως προς αυτόν τον κύκλο, δηλαδή αν η τέταρτη έλλειψη είναι εκτός του κύκλου, αν είναι εντός, αν το τέμνει ή αν είναι εφαπτόμενη (εσωτερικά ή εξωτερικά) σε αυτόν.

Θα υπολογίσουμε τον αριθμό των δυαδικών ψηφίων που χρειάζεται οποιοσδήποτε αλγόριθμος για να απαντήσει σε αυτό το κατηγόρημα. Θεωρούμε ότι οι ελλείψεις είναι στην πεπλεγμένη τους μορφή και θα χρησιμοποιήσουμε συγκεκριμένα αλγεβρικές τεχνικές, για τις οποίες ο αναγνώστης μπορεί να ανατρέξει στους Cox et al. [60].

Έστω $\sqrt{s}$ η ακτίνα του κύκλου που είναι εξωτερικά εφαπτόμενος και στις τρεις ελλείψεις και έστω (v_1, v_2) το κέντρο του. Χρησιμοποιώντας τη διακρίνουσα, Εξ. (7.8), που προκύπτει θεωρώντας την εξίσωση του κύκλου και τις εξισώσεις των τριών ελλείψεων, έχουμε το σύστημα

$$\Delta_1(v_1, v_2, s) = \Delta_2(v_1, v_2, s) = \Delta_3(v_1, v_2, s) = 0. \tag{7.9}$$

Οι (μιγαδικές) λύσεις του συστήματος αντιστοιχούν στις συντεταγμένες και στην ακτίνα όλων των (μιγαδικών) κύκλων που είναι εφαπτόμενοι στις τρεις ελλείψεις.

Λήμμα 7.4. *Μία λύση $(\overline{v}_1, \overline{v}_2, \overline{s})$ του συστήματος (7.9) αντιστοιχεί σε έναν εξωτερικά εφαπτόμενο κύκλο αν και μόνο αν $\overline{s}$ είναι η μικρότερη θετική ρίζα (όλων) των $\Delta_i(\overline{v}_1, \overline{v}_2, s)$, $i = 1, 2, 3$. Αν s_0^-, s_0^+ είναι η μικρότερη και η μεγαλύτερη θετική πραγματική ρίζα του $\Delta_0(\overline{v}_1, \overline{v}_2, s)$, όπου Δ_0 είναι η διακρίνουσα που αντιστοιχεί στον κύκλο και στην έλλειψη E_4, τότε:*

- $\overline{s} \leq s_0^- \Leftrightarrow$ *η E_4 είναι εκτός του κύκλου και είναι εφαπτόμενη σε αυτόν αν $\overline{s} = s_0^-$.*
- $\overline{s} \in (s_0^-, s_0^+) \Leftrightarrow$ *η E_4 τέμνει του κύκλο.*
- $\overline{s} \geq s_0^+ \Leftrightarrow$ *η E_4 είναι εντός του κύκλου και είναι εφαπτόμενη σε αυτόν αν $\overline{s} = s_0^+$.*

Απόδειξη: Έστω $(\overline{v}_1, \overline{v}_2, \overline{s})$ η λύση του συστήματος.

($\Rightarrow$): Έστω $\overline{s}$ η μικρότερη θετική πραγματική ρίζα όλων των $\Delta_i(\overline{v}_1, \overline{v}_2, s)$, $i = 1, 2, 3$. Τότε ο κύκλος $(\overline{v}_1, \overline{v}_2, \overline{s})$ είναι εξωτερικά εφαπτόμενος και στις τρεις ελλείψεις, κατά συνέπεια είναι εξωτερικά εφαπτόμενος.

($\Leftarrow$): Έστω ότι ο κύκλος $(\overline{v}_1, \overline{v}_2, \overline{s})$ είναι εξωτερικά εφαπτόμενος και στις τρεις ελλείψεις. Τότε πρέπει $\overline{s}$ να είναι η μικρότερη θετική πραγματική ρίζα όλων των $\Delta_i(\overline{v}_1, \overline{v}_2, s)$, $i = 1, 2, 3$.

Θεωρούμε όλους τους κύκλους $C(\overline{v}_1, \overline{v}_2, s)$, καθώς το s αυξάνει από το μηδέν στο άπειρο, υποθέτωντας ότι το σημείο $(\overline{v}_1, \overline{v}_2)$ κείται εκτός της έλλειψης E_0. Όταν $s = 0$, ο κύκλος C εκφυλίζεται σε ένα σημείο εκτός της E_0. Όταν το s είναι άπειρο ο C γίνεται ένας απείρου ακτίνας κύκλος (ευθεία) που περικλύει την E_0. Καθώς το s αυξάνει από το μηδέν, περνά από τις ρίζες του $\Delta_0(\overline{v}_1, \overline{v}_2, s)$. Για κάθε μία από αυτές (υπάρχουν το πολύ 4), ο C είναι εφαπτόμενος στην E_0. Όταν $s < s_0^-$ ο C είναι εκτός της E_0, και όταν $s > s_0^+$ ο C περικλύει την E_0. Σε όλες τις άλλες περιπτώσεις, ο C τέμνει την E_0 λόγω της τοπολογίας των δύο κλειστών καμπυλών C και E_0. ΟΕΔ

Ανάμεσα στις λύσεις του συστήματος, ο εξωτερικά εφαπτόμενος κύκλος και στις τρεις ελλείψεις που μας ενδιαφέρει μπορεί (αλλά μπορεί και όχι) να είναι αυτός με την μικρότερη ακτίνα.

Ένα φράγμα στο πλήθος των λύσεων ενός πολυωνυμικού συστήματος μπορεί να υπολογιστεί με τη βοήθεια του μικτού όγκου. Ο μικτός όγκος υπολογίζεται θεωρώντας το κυρτό περίβλημα των σημείων που ορίζουν τα διανύσματα των εκθετών των αγνώστων [60, 114]. Ο μεικτός όγκος του συστήματος (7.9), είναι 256. Μπρούμε ωστόσο να το μειώσουμε απομακρύνοντας τις λύσεις στο άπειρο. Θέτουμε

$$q = v_1^2 + v_2^2 - s. \tag{7.10}$$

Τώρα το σύστημα των διακρινουσών (7.9) γίνεται

$$\Delta_1(v_1, v_2, q) = \Delta_2(v_1, v_2, q) = \Delta_3(v_1, v_2, q) = 0, \tag{7.11}$$

το οποίο έχει μικτό όγκο 184. Η επιλύσουσα του συστήματος, είναι ένα πολυώνυμο ως προς q, βαθμού 184. Προσθέτοντας την εξίσωση (7.10) στο σύστημα (7.11) προκύπτει ένα υπερπροσδιορισμένο σύστημα ως προς τα v_1, v_2, q, s το οποίο έχει, επίσης, μικτό όγκο 184.

Κάθε Δ_i είναι μια διακρίνουσα ενός πολυωνύμου $\phi(\lambda_i)$, Εξ. (7.7) και ο μηδενισμός της εκφράζει το γεγονός ότι το $\phi(\lambda_i)$ έχει πολλαπλή ρίζα, δηλαδή κοινή ρίζα με την παραγωγό του. Συνεπώς, ένα ισοδύναμο σύστημα με αυτό της (7.11), με τον ίδιο μικτό όγκο, είναι το

$$\varphi_i = 0, \frac{\partial}{\partial \lambda_i}\varphi_i = 0, \quad i = 1, 2, 3$$

όπου φ_i είναι το χαρακτηριστικό πολυώνυμο της έλλειψης i και του Voronoi κύκλου, Εξ. (7.7). Αυτό το σύστημα έχει σημαντικά μικρότερου δυαδικού μήκους συντελεστές από το (7.11). και έχει 3 εξισώσεις συνολικού βαθμού 3 και 3 συνολικού βαθμού 2.

Όποιο σύστημα και να θεωρήσουμε, το συνολικό πλήθος των μιγαδικών λύσεων είναι 184.

Θεώρημα 7.5

Τρεις ελλείψεις έχουν το πολύ 184 μιγαδικούς κύκλους εφαπτόμενους και στις τρεις. Το φράγμα είναι βέλτιστο καθώς υπάρχει τριάδα ελλείψεων με αυτόν το αριθμό.

Απόδειξη: Ο μικτός όγκος μας δίνει ένα άνω φράγμα και ο βαθμός της επιλύουσας (από ένα παράδειγμά μας) μας δίνει το κάτω φράγμα. ΟΕΔ

Υπενθυμίζουμε ότι στην περίπτωση των 3 κύκλων, ο αριθμός των κύκλων που είναι εφαπτόμενες σε 3 κύκλους, είναι 8 και ότι το αντίστοιχο κατηγόρημα έχει αλγεβρικό βαθμό 2. Το θεώρημα γενικεύεται σε όλων των ειδών τις κωνικές τομές, σύμφωνα με τον F. Sottile[6]. Ένα εξαιρετικά ενδιαφέρον (ανοιχτό) ερώτημα είναι πόσοι από αυτούς τους κύκλους είναι πραγματικοί. Ο F. Ronga προτείνει μια κατασκευή όπου τρεις κωνικές τομές έχουν τουλάχιστον 136 πραγματικούς τέτοιους κύκλους. Ωστόσο, μέχρι στιγμής δεν έχουμε καταφέρει να φτιάξουμε μια τέτοια κατασκευή με τρεις μη τεμνόμενες ελλείψεις.

[6] Περσοναλ ϛομμυνιϛατιον, 2004.

Περί του πλήθους των απαιτούμενων δυαδικών ψηφίων

Προκειμένου να καταστήσουμε ένα αλγόριθμο επίλυσης του κ_3 ακριβή πρέπει να υπολογίσουμε τον αριθμό των δυαδικών ψηφίων που απαιτούνται. Γιαυτό θα χρησιμοποιήσουμε το σύστημα (7.11) μαζί με την (7.10), που έχει βέλτιστο μικτό όγκο. Πιο συγκεκριμένα, το σύστημά μας είναι:

$$\Delta_1(v_1, v_2, q) = \Delta_2(v_1, v_2, q) = \Delta_3(v_1, v_2, q) = q - v_1^2 - v_2^2 + s = 0$$

Μπορούμε να απαλείψουμε τα v_1, v_2, q και έτσι προκύπτει η επιλύσουσα, $R(s)$ που είναι πολυώνυμο ως προς s βαθμού 184 και δυαδικού μήκους συντελεστών $3 \cdot 56 \cdot \tau_\Delta = 168\tau_\Delta$ [60]. Εδώ το 56 ισούται με τον μικτό όγκο του συστήματος $\Delta_i, \Delta_j, q - v_1^2 - v_2^2 + s$, αν θεωρήσουμε το s ως παράμετρο και το τ_Δ είναι το δυαδικό μήκος των συντελεστών του Δ_i, όπου $1 \leq i, j \leq 3$ και $i \neq j$. Το φράγμα διαχωρισμού του πολυωνύμου P (Εν. 3.2) βαθμού d και δυαδικού μήκους τ είναι $sep(P) \geq d^{-(d+2)/2}(d+1)^{(1-d)/2}2^{\tau(1-d)}$ [275], συνεπώς ο αριθμός των δυαδικών ψηφίων που χρειαζόμαστε προκειμένου να υπολογίσουμε το s είναι το πολύ $1389 + 30744\,\tau_\Delta$.

Προκειμένου να συγκρίνουμε δύο ακτίνες s_1 και s_2, οι οποίες είναι ρίζες δύο πολυωνύμων R_1 και R_2 αντίστοιχα, πρέπει να φράξουμε την ποσότητα $|s_1 - s_2|$. Παρατηρούμε ότι $|s_1 - s_2| \geq sep(R_1R_2)$ όπου το πολυώνυμο R_1R_2 έχει βαθμό 368, καθώς προκύπτει από τον πολλαπλασιασμό δύο πολυωνύμων βαθμού 184, και δυαδικό μήκος $8 + 336\tau_\Delta$. Το φράγμα στο δυαδικό μήκος προκύπτει καθώς πολλαπλασιάζουμε δύο πολυώνυμα με δυαδικό μήκος $168\tau_\Delta$, οπότε το γινόμενό τους, στην χειρότερη περίπτωση έχει δυαδικό μήκος $184 \cdot 2^{2 \cdot 168\tau_\Delta}$, ή $\lceil \lg 184 + 2 \cdot 168\tau_\Delta \rceil$. Συμπεραίνουμε [275] ότι ο αριθμός των δυαδικών ψηφίων που απαιτείται για να συγκρίνουμε δύο (πραγματικές) ρίζες των R_1 και R_2 και συνεπώς δύο ακτίνες s_1 και s_2 είναι $1508 + 30324\tau_\Delta$, το οποίο αντιστοιχεί στο $sep(R_1R_2)$ διαιρεμένο με 3.

Το προκύπτων φράγμα είναι σχεδόν βέλτιστο, καθώς τα πολυώνυμα R_1 και R_2 προκύπτουν ως επιλύουσες συστημάτων με βέλτιστο μικτό όγκο, συνεπώς το είναι, στη γενική περίπτωση βαθμού 184 και ανάγωγα. Επιπρόσθετα, το φράγμα διαχωρισμού είναι σφιχτό (εκτός από κάποιες σταθερές), καθώς (σχεδόν) το επιτυγχάνουν τα πολυώνυμα Mignotte (Σημ. 3.24).

ΚΕΦΑΛΑΙΟ 8

Διάσπαση Minkowski

> Η μαθηματική παιδεία αυτού του νεαρού φυσικού (Albert Einstein) δεν ήταν ιδιαίτερα στέρεα, και είμαι σε θέση να την αξιολογήσω γιατί την απέκτησε από εμένα στη Ζυρίχη, πριν από κάποιο διάστημα.
>
> Herman Minkowski

Περίληψη

Δοθέντος ενός κυρτού πολυγώνου με ακέραιες κορυφές στο επίπεδο, εξετάζουμε αλγορίθμους που μας επιτρέπουν να το διασπάσουμε σε δύο άλλα κυρτά πολύγωνα τέτοια ώστε το άθροισμα τους κατά Minkowski να είναι το αρχικό πολύγωνο.

Τα αποτελέσματα του παρόντος κεφαλαίου παρουσιάστηκαν στην εργασία [89].

Εξετάζουμε τη διάσπαση κυρτών πολυγώνων τα οποία έχουν κορυφές με ακέραιες συντεταγμένες, και τα οποία καλούνται ακέραια πολύγωνα (lattice polygons), ως αντίστροφη διαδικασία του αθροίσματος Minkowski, το οποίο ορίζεται ως εξής:

Ορισμός 8.1. *Έστω A και B δύο υποσύνολα του $\mathbb{Z}^2$. Το άθροισμα Minkowski (Minkowski sum) είναι $A \oplus B = \{a + b | a \in A, b \in B\}$. Ονομάζουμε τα A και B προσθετέους (summands) του αθροίσματος $A \oplus B$.*

Ο ορισμός του αθροίσματος Minkowski μπορεί να γενικευτεί σε οποιαδήποτε διάσταση.

Το πρόβλημα της διάσπασης παρουσιάζει εξαιρετικό ενδιαφέρον ως αυτόνομο πρόβλημα. Σχετικά πρόσφατες εργασίες που αφορούν σε τορικά μπαλώματα Bezier (toric Bézier patches) στη γεωμετρική μοντελοποίηση [δείτε για παράδειγμα 115, 164, 165], εγείρουν πολλές ερωτήσεις

σχετικά με το πρόβλημα αυτό. Οι περισσότερες εξ αυτών ενδιαφέρονται για το αν ένα ακέραιο πολύγωνο μπορεί να γραφτεί ως άθροισμα Minkowski δύο άλλων και αν η απάντηση είναι θετική να υπολογιστεί μία ή περισσότερες τέτοιες διασπάσεις.

Μια άλλη εφαρμογή του προβλήματος αυτού είναι στην κατασκευή πινάκων για τον υπολογισμό της αραιής απαλοίφουσας 3 πολυωνύμων σε δύο μεταβλητές [165, sec.10.3] ή [277]. Ίσως η πιο σημαντική σημαντική εφαρμογή της διάσπασης Minkowski είναι η παραγοντοποίηση πολυωνύμων δύο (και τελικά περισσότερων) μεταβλητών. Αυτό συμβαίνει γιατί δοθέντος ενός πολυωνύμου δύο (ή περισσότερων μεταβλητών) μπορούμε να αντιστοιχίσουμε σε αυτό το λεγόμενο πολύτοπο του Newton. Όπως παρατήρησε ο Ostrowski [208], εάν το πολυώνυμο παραγοντοποιείται τότε το πολύτοπο του Newton διασπάται κατά Minkowski. Αν η διάσπαση του πολυτόπου του Newton είναι διαθέσιμη τότε είναι ευκολότερη η εύρεση των συντελεστών.

Καταρχάς επικεντρωνόμαστε σε διασπάσεις κατά Minkowski όπου τουλάχιστον ένας από τους προσθετέους είναι σταθερού μεγέθους, δηλαδή είναι ευθύγραμμο τμήμα, τρίγωνο ή τετράπλευρο. Τέτοιες διασπάσεις είναι πολύ χρήσιμες στα τορικά μπαλώματα Bézier με βάθος. Οι Krasauskas and Goldman [165], αναφέρουν "extend blossoming, degree elevation and implicitization techniques to arbitrary toric Bézier patches. [...] The key idea to each of these algorithms is to employ decompositions based on the Minkowski sum"[1]. Και προσθέτουν [165, Sec. 10.1] ότι "This approach to evaluation, blossoming, and dual functionals works for any toric Bézier patch whose lattice polygon decomposes into the Minkowski sum of line segments and unit triangles"[2]. Ένα από τα σημαντικά βήματα στον αλγόριθμο του Zube [277], δείτε επίσης [165], για την κατασκευή πινάκων απαλοίφουσας στην αλγεβρικοποίηση είναι "decompose [Newton polygon] A into a Minkowski sum of simpler lattice polygons, typically line segments and triangles"[3].

Στο παρόν κεφάλαιο θα προσδιορίσουμε την ασυμπτωτική δυσκολία του προβλήματος και θα προτείνουμε αποδοτικούς, και σε μερικές περιπτώσεις βέλτιστους, αλγορίθμους για την περίπτωση που ένας προσθετέος είναι σταθερού μεγέθους. Συνδέουμε το πρόβλημα της διάσπασης με το πρόβλημα $k-$SUM για το οποίο υπάρχει αλγόριθμος με πολυπλοκότητα $\mathcal{O}(n^{\lceil k/2 \rceil})$ ή $\mathcal{O}(n^{\lceil k/2 \rceil} \lg n)$, ανάλογα αν το k είναι άρτιος ή περιττός, αλλά δεν υπάρχουν γνωστά κάτω φράγματα.

Επίσης έχουμε υλοποιήσει τους αλγορίθμους που προτείνουμε και τους εφαρμόζουμε σε όλα τα ακέραια πολύγωνα με ένα ή κανένα εσωτερικό ακέραιο σημείο. Επιπρόσθετα πραγματοποιούμε πειράματα με διάφορες εισόδους και συγκρίνουμε με τον αλγόριθμο των Gao and Lauder [111], ο οποίος αφορά το γενικό πρόβλημα της διάσπασης.

Το πρόβλημα απόφασης, δηλαδή εάν ένα ακέραιο πολύγωνο επιδέχεται διάσπαση Minkowski είναι NP-complete [111]. Επίσης, οι Gao and Lauder [111] προτείνουν έναν ψευδο-πολυωνυμικό αλγόριθμο της τάξης $\mathcal{O}((nDE)^3)$, όπου n είναι ο αριθμός των ακμών στο πολύγωνο και DE είναι

[1] Ελεύθερη μετάφραση: Η βασική ιδέα πίσω από τους αλγορίθμους ανθοφορίας (blossoming), ανύψωσης βαθμού και των αυθαιρέτων μπαλωμάτων Bézier είναι η εφαρμογή της διάσπασης κατά Minkowski.

[2] Ελεύθερη μετάφραση: Αυτή η προσέγγιση για την ανύψωση, την ανθοφορία και τα δυαδικά συναρτησοειδή δουλεύει για οποιοδήποτε τορικό (αραιό) μπάλωμα Bézier, του οποίου το ακέραιο πολύγωνο διασπάται ως Minkowski άθροισμα ευθυγράμμων τμημάτων και μοναδιαίων τριγώνων.

[3] Ελεύθερη μετάφραση: Διέσπασε το πολύγωνο του Newton του (πολυωνύμου) A ως το Minkowski άθροισμα πιο μικρών ακέραιων πολυγώνων, συνήθως ευθυγράμμων τμημάτων και τριγώνων.

το μέγιστο ακέραιο μήκος τους. Αξίζει να παρατηρήσουμε ότι το μέγεθος DE είναι εκθετικά μεγάλο σε σχέση με το δυαδικό μήκος της εισόδου, το οποίο είναι $\mathcal{O}(n \lg (DE))$.

Θα ανάγουμε το (γενικό) πρόβλημα της διάσπασης σε γνωστά και καλώς μελετημένα προβλήματα της συνδυαστικής βελτιστοποίησης, όπως για παράδειγμα το SUBSET-SUM πρόβλημα. Αυτή η αναγωγή μας επιτρέπει να προτείνουμε ένα αλγόριθμο ο οποίος βελτιώνει την πολυπλοκότητα του προβλήματος κατά ένα παράγοντα nD. Επιπρόσθετα, αυτή η προσέγγιση επιτρέπει τη δημιουργία γρήγορων υλοποιήσεων που βασίζονται σε πιθανοτικούς αλγορίθμους και ενδεχομένως να οδηγήσει και σε προσεγγιστικούς αλγορίθμους.

Τι θα ακολουθήσει

Στην επόμενη ενότητα παρουσιάζουμε τυπικά τα προβλήματα με τα οποία θα ασχοληθούμε και αναφερόμαστε στη γνωστή βιβλιογραφία. Η Εν. 8.2 παρουσιάζει την προσέγγισή μας για τη διάσπαση Minkowski ενός ακεραίου πολυγώνου σε δύο προσθετέους, όπου τουλάχιστον ο ένας έχει σταθερό πλήθος ακμών. Στην Εν. 8.3 παρουσιάζουμε την υλοποίηση των αλγορίθμων της ενότητας 8.2 και πειραματικά αποτελέσματα σε τυχαία ακέραια πολύγωνα και σε όλα τα ακέραια πολύγωνα με ένα κανένα εσωτερικό ακέραιο σημείο. Στην Εν. 8.4 προτείνουμε έναν αλγόριθμο για το γενικό πρόβλημα της διάσπασης ενός πολυγώνου, ο οποίος έχει καλύτερη πολυπλοκότητα από την μέχρι σήμερα γνωστή. Στην τελευταία ενότητα παρουσιάσουμε τις μελλοντικές επεκτάσεις της προσέγγισής μας.

8.1 Ορισμοί και προηγούμενες εργασίες

Το γενικό πρόβλημα με το οποίο ασχολούμαστε είναι το εξής:

Πρόβλημα 8.2. MINKOWSKI-DECOMPOSITION
Δοθέντος ενός ακέραιου πολυγώνου Q με n κορυφές, πρέπει να αποφασίσουμε εάν είναι διασπάσιμο (decomposable), δηλαδή εάν υπάρχουν ακέραια πολύγωνα A και B τέτοια ώστε $A \oplus B = Q$, όπου το σύμβολο $\oplus$ δηλώνει το άθροισμα κατά Minkowski.

Μας δίδεται ένα ακέραιο πολύγωνο Q με κορυφές $v_0, v_1, \ldots, v_{n-1}$, όπου $v_j \in \mathbb{Z}^2, 0 \leq j \leq n-1$. Σε κάθε ακμή του πολυγώνου αντιστοιχούμε ένα διάνυσμα $u_1 = (v_1 - v_0), \ldots, u_n = (v_0 - v_{n-1})$. Το πολύγωνο χαρακτηρίζεται πλήρως (ταυτοποιείται) από την ακολουθία των διανυσμάτων $\{u_i\}_{1 \leq i \leq n}$ και την αρχική κορυφή v_0. Σε ό,τι θα ακολουθήσει ακμή και διάνυσμα θα σημαίνουν το ίδιο και το αυτό.

Ορισμός 8.3. *Έστω διάνυσμα $u = (a, b)$ και έστω $d = \gcd(a, b)$. Το πρωταρχικό διάνυσμα (primitive vector) του u είναι $e = (a/d, b/d)$.*

Θα συμβολίσουμε την ακολουθία όλων των διανυσμάτων u_i ως $\mathcal{U}$ και θα την ονομάσουμε ακολουθία ακμών (edge sequence). Σε κάθε διάνυσμα $u_i = (a_i, b_i)$ του Q αντιστοιχούμε το πρωταρχικό διάνυσμα e_i, $1 \leq i \leq n$. Ονομάζουμε την ακολουθία των όλων των πρωταρχικών διανυσμάτων πρωταρχική ακολουθία διανυσμάτων (primitive edge sequence) και θα τη συμβολίζουμε με $\mathcal{E}$. Επιπρόσθετα συμβολίζουμε με $\mathcal{A}$ το σύνολο όλων των δυνατών διανυσμάτων, τέτοιων ώστε:

$$\mathcal{A} = \{k_i e_i \mid 1 \leq i \leq n, 1 \leq k_i \leq d_i\}$$

όπου $d_i = \gcd(a_i, b_i)$. Έστω

$$\begin{aligned} D &= \max\{d_1, \ldots, d_n\}, \\ E &= \max\{e_{1x}, e_{1y}, \ldots, e_{nx}, e_{ny}\}, \end{aligned}$$

όπου (e_{ix}, e_{iy}) είναι οι συντεταγμένες του πρωταρχικού διανύσματος e_i. Επιπρόσθετα συμβολίζουμε με g το χρόνο που απαιτείται για τον υπολογισμό του gcd (ΕΚΠ) δύο αριθμών μέτρου DE. Αν χρησιμοποιήσουμε τον αλγόριθμο HALF-GCD [263, 275] η πολυπλοκότητα του gcd (δείτε και Κεφ. 2)

$$g := \mathcal{O}_B(\lg(DE)\lg^2\lg(DE)\lg\lg\lg(DE))$$

Το κόστος για τον υπολογισμό του $\mathcal{A}$ είναι $\mathcal{O}_B\left(ng + nD\,\mathsf{M}(\max\{D,E\})\right) = \mathcal{O}_B(nD\mathsf{M}(\max\{D,E\}))$, όπου $\mathsf{M}(\tau)$ είναι ο χρόνος που απαιτείται για τον πολλαπλασιασμό δύο αριθμών δυαδικού μήκους τ. Εάν χρησιμοποιήσουμε το αλγόριθμο FFT [263, 275] η πολυπλοκότητα του πολλαπλασιασμού είναι:

$$\mathsf{M}(\tau) = \tau\lg\tau\lg\lg\tau \tag{8.1}$$

Εάν ενδιαφερόμαστε για την αριθμητική πολυπλοκότητα του υπολογισμού του $\mathcal{A}$ τότε αυτή είναι $\mathcal{O}(nD)$. Ωστόσο, όταν απαιτείται ο υπολογισμός $\mathcal{A}$, το κόστος αυτό είναι μικρότερο σε σχέση με την πολυπλοκότητα των άλλων βημάτων των αλγορίθμων που θα παρουσιάσουμε.

Λήμμα 8.4. *Έστω ακέραιο πολύγωνο Q, τέτοιο ώστε $Q = A \oplus B$. Κάθε ακμή του Q προσδιορίζεται μοναδικά ως το άθροισμα Minkowski μιας ακμής του A και μιας κορυφής του B, ή ως το άθροισμα μιας κορυφής του A και μιας ακμής του B, ή ως το άθροισμα δύο παράλληλων ακμών του A και του B.*

Κατά συνέπεια, το σύνολο των κανονικών διανυσμάτων (των ακμών) του Q είναι η ένωση των συνόλων των κανονικών διανυσμάτων του A και του B.

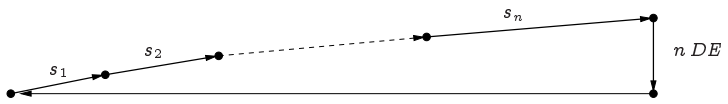
Αν χρησιμοποιήσουμε το Λήμμα 8.4, μπορούμε να δείξουμε εύκολα ότι [111]:

Λήμμα 8.5. *Ένα (ακέραιο) πολύγωνο είναι προσθετέος του Q εάν και μόνο εάν η ακολουθία των ακμών του είναι της μορφής $\{k_j e_j\}_{j\in J}$, όπου $J \subseteq \{1,\ldots n\}$, $0 \le k_j \le d_j$, $k_j \in \mathbb{Z}$ και $\sum_{j\in J} k_j e_j = (0,0)$ (το άθροισμα των διανυσμάτων που αντιστοιχούν στις ακμές του είναι μηδέν).*

Θεώρημα 8.6

[111] Το πρόβλημα απόφασης σχετικά με το εάν ένα ακέραιο πολύγωνο επιδέχεται διάσπαση κατά Minkowski είναι NP-complete. Υπάρχει αλγόριθμος που απαντά εάν ένα ακέραιο πολύγωνο είναι διασπάσιμο και ο οποίος έχει πολυπλοκότητα $\mathcal{O}(nDT)$, όπου T είναι το πλήθος των εσωτερικών ακέραιων σημείων του πολυγώνου. Λαμβάνοντας υπ' όψιν ότι $T = \mathcal{O}((nDE)^2)$, η πολυπλοκότητα του αλγορίθμου είναι $\mathcal{O}(n^3D^3E^2)$.

Μια σημαντική παρατήρηση είναι ότι εάν ένα πολύγωνο είναι διασπάσιμο τότε ενδέχεται το πλήθος των πιθανών διασπάσεων να είναι εκθετικά μεγάλο, σε σχέση με το πλήθος των κορυφών και το μέγεθος των ακμών. Ο αλγόριθμος των Gao and Lauder [111] είναι ψευδο-πολυωνυμικός γιατί η πολυπλοκότητά του είναι πολυωνυμική σε σχέση με το μέτρο των ακμών του πολυγώνου και όχι σε σχέση με τον λογάριθμό τους, δηλαδή το δυαδικό τους μήκος, όπως θα επιθυμούσαμε



Σχήμα 8.1: Ένα ακέραιο πολύγωνο με εμβαδόν $\mathcal{O}((nDE)^2)$.

για ένα πολυωνυμικό αλγόριθμο. Στην Εν. 8.4 θα προτείνουμε έναν αλγόριθμο που θα βελτιώνει την πολυπλοκότητα κατά έναν παράγοντα nD.

Το φράγμα $T = \mathcal{O}(n^2D^2E^2)$ [110], [121, Chap. 7] είναι σφιχτό. Ένας τρόπος για να το δούμε αυτό είναι ο ακόλουθος. Καταρχάς θα χρειαστούμε το ακόλουθο θεώρημα που οφείλεται στον Pick [215]:

Θεώρημα 8.7

Έστω A το εμβαδόν ενός απλού κλειστού ακέραιου πολυγώνου. Έστω B το πλήθος των ακέραιων σημείων που βρίσκονται στις ακμές του πολυγώνου και I το πλήθος των εσωτερικών ακέραιων σημείων του. Τότε

$$A = I + \frac{B}{2} - 1$$

Ο τύπος του Pick μπορεί να γενικευτεί σε οποιαδήποτε διάσταση με τη βοήθεια των πολυωνύμων Ehrhart.

Θεωρούμε το πολύγωνο του Σχ. 8.1, όπου η ακολουθία ακμών είναι

$$s_1 = (1, DE), s_2 = (2, DE), \ldots, s_n = (n, DE), (0, -nDE), (-\frac{n(n+1)}{2}, 0)$$

Το εμβαδόν του πολυγώνου είναι $\Theta(n^3DE)$. Εάν υποθέσουμε ότι $n = \Theta(DE)$, τότε το εμβαδόν είναι $\Theta(n^2D^2E^2)$. Το πλήθος των εσωτερικών ακέραιων σημείων είναι ασυμπτωτικά μεγαλύτερο από το πλήθος των ακέραιων σημείων στο σύνορο του πολυγώνου. Παρατηρούμε επίσης ότι #(Boundary points) $= B = \mathcal{O}(n^2)$ και από τον τύπο του Pick συμπεραίνουμε ότι ο αριθμός των εσωτερικών ακέραιων σημείων είναι ασυμπτωτικά $\Theta((nDE)^2)$.

8.2 Προσθετέοι σταθερού μεγέθους

Επικεντρώνομαστε τώρα στο πρόβλημα της διάσπασης όταν είναι γνωστό εκ των προτέρων ότι τουλάχιστον ένας προσθετέος είναι σταθερού μεγέθους. Υπενθυμίζουμε ότι η είσοδος είναι μία ακολουθία σημείων μεγέθους n. Θα μας απασχολήσουν δύο διαφορετικά προβλήματα:

Πρόβλημα 8.8. *Decision $k-$*SUMMAND

Δοθέντος ακέραιου πολυγώνου αποφάσισε εάν υπάρχει διάσπαση κατά Minkowski σε δύο προσθετέους τέτοια ώστε τουλάχιστον ένας από αυτούς να έχει k ακμές.

Πρόβλημα 8.9. *Enumeration $k-$*SUMMAND

Δοθέντος ακέραιου πολυγώνου απαρίθμησε όλες τις διασπάσεις κατά Minkowski σε δύο προσθετέους τέτοιες ώστε τουλάχιστον ένας από αυτούς να έχει k ακμές.

Θα εξετάσουμε λεπτομερώς τις περιπτώσεις όπου ο ένας προσθετέος είναι ευθύγραμμο τμήμα ($2-$SUMMAND), τρίγωνο ($3-$SUMMAND) ή τετράπλευρο ($4-$SUMMAND). Η τελευταία περίπτωση γενικεύεται και για προσθετέους οποιουδήποτε σταθερού πλήθους ακμών. Θα ασχοληθούμε τόσο με το πρόβλημα της απόφασης όσο και το πρόβλημα της απαρίθμησης.

Το πρόβλημα απόφασης $k-$SUMMAND μπορεί να επιλυθεί χρησιμοποιώντας το πρόβλημα $k-$SUM, το οποίο ορίζεται ως εξής:

Πρόβλημα 8.10. $k-$SUM

Δοθέντος ενός συνόλου m ακεραίων αριθμών και ενός στόχου S, αποφάσισε εάν υπάρχουν k από αυτούς, τέτοιοι ώστε το άθροισμά τους να είναι S.

Ο καλύτερος γνωστός αλγόριθμος για το πρόβλημα $k-$SUM έχει χρονική και χωρική πολυπλοκότητα $\mathcal{O}(m^{\lceil k/2 \rceil} \lg m)$ και $\mathcal{O}(m^{\lceil k/2 \rceil})$, αντίστοιχα [271, 272]. Όταν το k είναι περιττός τότε η χρονική πολυπλοκότητα βελτιώνεται σε $\mathcal{O}(m^{\lceil k/2 \rceil})$. Ωστόσο, είναι πολύ δύσκολο πρόβλημα η απόδειξη ενός μη τετριμμένου κάτω φράγματος για το $k-$SUM. Η απόδειξη ενός τέτοιου φράγματος είτε στο μοντέλο αλγεβρικού δένδρου απόφασης (algebraic decision tree model) είτε στο μοντέλο αλγεβρικού υπολογιστικού δένδρου (algebraic computational tree model) είναι ένα πολύ σημαντικό ανοικτό πρόβλημα. Το μόνο γνωστό αποτέλεσμα οφείλεται στον Erickson [100], ο οποίος απέδειξε ένα κάτω φράγμα της τάξης του $\Omega(m^{\lceil k/2 \rceil})$ σε μια συγκεκριμένη (και περιοριστική) παραλλαγή του του μοντέλου του γραμμικού δένδρου απόφασης (linear decision tree model), δείτε επίσης την εργασία των Baran et al. [13].

Θεώρημα 8.11

Ένα στιγμιότυπο του προβλήματος $k-$SUMMAND μπορεί να μετασχηματιστεί σε ένα στιγμιότυπο του προβλήματος $k-$SUM, έτσι ώστε το στιγμιότυπο του $k-$SUMMAND να έχει λύση αν και μόνο αν το αντίστοιχο στιγμιότυπο του $k-$SUM έχει λύση.

Απόδειξη: Θεωρούμε ένα ακέραιο πολύγωνο με n κορυφές. Υπολογίζουμε το σύνολο $\mathcal{A}$ σε χρόνο $O(nD)$. Για κάθε διάνυσμα του $\mathcal{A}$ που είναι της μορφής $ke_i = k(e_{ix}, e_{iy})$, όπου $1 \leq i \leq n$ και $1 \leq k \leq d_i$. Σε κάθε διάνυσμα του $\mathcal{A}$ αντιστοιχούμε τον αριθμό $\alpha_{ik} = k(e_{ix} + Le_{iy})$, όπου $L = (k+1)DE$.

Το σύνολο των α_{ik} έχει το πολύ nD στοιχεία. Ας υποθέσουμε ότι ο στόχος είναι $S = 0$. Εάν βρούμε k στοιχεία από αυτό το σύνολο έτσι ώστε όλα να αντιστοιχούν σε διαφορερικά πρωταρχικά διανύσματα και επιπρόσθετα να αθροίζουν σε μηδέν τότε ένας $k-$summand υπάρχει.

Παρατηρούμε ότι το μέγεθος του στιγμιότυπου του $k-$SUM είναι $O(nD)$. ΟΕΔ

Ο προηγούμενος μετασχηματισμός μας επιτρέπει να επιλύσουμε το $k-$SUMMAND πρόβλημα χρησιμοποιώντας απευθείας του αλγόριθμους που αφορούν το πρόβλημα $k-$SUM και επιπρόσθετα μας παρέχει πάνω φράγματα τόσο για τη χρονική όσο και για την χωρική πολυπλοκότητα. Για $k = 2, 3, 4$ έχουμε :

- Το Decision $2-$SUMMAND μπορεί να επιλυθεί σε $O(nD \lg(nD))$ χρόνο και $O(nD)$ χώρο.
- Το Decision $3-$SUMMAND μπορεί να επιλυθεί σε $O(n^2D^2)$ και $O(nD)$ χώρο.

- Το Decision 4−SUMMAND μπορεί να επιλυθεί σε $O(n^2D^2 \lg(nD))$ χρόνο και $O(nD)$ χώρο.

Η γενική περίπτωση του decision k−SUMMAND προβλήματος μπορεί να επιλυθεί σε χρόνο $O\left((nD)^{\lceil k/2 \rceil} \lg(nD)\right)$ ή $O\left((nD)^{\lceil k/2 \rceil}\right)$, για k άρτιο ή περιττό αντίστοιχα, και $O\left((nD)^{\lceil k/2 \rceil}\right)$ χώρο.

Θα βελτιώσουμε όλα τα παραπάνω φράγματα στις παραγράφους που ακολουθούν.

Ακολουθώντας τους Gajentaan and Overmars [109], δίνουμε τον ακόλουθο ορισμό:

Ορισμός 8.12. *Δοθέντων δύο προβλημάτων* PR_1 *και* PR_2 *λέμε ότι το* PR_1 *είναι* $f(n)$−*επιλύσιμο με τη χρήση του* PR_2 *εάν και μόνο εάν κάθε στιγμιότυπο του* PR_1 *μεγέθους* n *μπορεί να επιλυθεί με τη χρήση ενός σταθερού αριθμού στιγμιοτύπων του* PR_2 *και με χρονική επιβάρυνση το πολύ* $O(f(n))$. *Την αναγωγή αυτή θα την συμβολίζουμε με*

$$\mathrm{PR}_1 \lll_{f(n)} \mathrm{PR}_2$$

Παρατηρούμε ότι η προηγούμενη αναγωγή υποδηλώνει ότι όταν η συνάρτηση $f(\cdot)$ είναι αρκούντος μικρή, κάτω φράγματα στη χρονική πολυπλοκότητα του PR_1 μεταφέρονται στο PR_2 και τα πάνω φράγματα του PR_2 ισχύουν και για το PR_1.

Προκειμένου να δείξουμε κάτω φράγματα για το k−SUMMAND πρόβλημα χρησιμοποιούμε την ακολουθη αναγωγή:

Θεώρημα 8.13

k−SUM $\lll_{n \lg n}$ k−SUMMAND

Απόδειξη: Θεωρούμε την ακολουθία $\{a_i\}_{1 \le i \le n}$, όπου $a_i \in \mathbb{Z}$. Υποθέτουμε ότι η ακολουθία είναι ταξινομημένη και αν όχι τότε την ταξινομούμε σε χρόνο $\mathcal{O}(n \lg n)$. Έστω $M = \max_i |a_i|$ και $L = (k+1)M$. Σχηματίζουμε την ακολουθία $\{s_i = a_i + L\}_{1 \le i \le n}$, όπου $0 \le s_1 \le \cdots \le s_n$.

Στη συνέχεια θεωρούμε την ακολουθία ακμών (δείτε στο Σχ. 8.2):

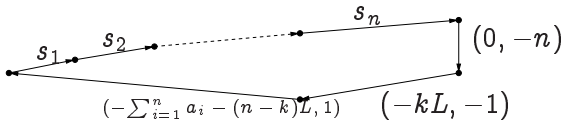
$$(s_1, 1), (s_2, 1), \ldots, (s_n, 1), (0, -n), (-kL, -1), (-\sum_{i=1}^{n} a_i - (n-k)L, 1)$$

Αυτή η ακολουθία αποτελεί την ακολουθία ακμών κάποιου ακέραιου πολυγώνου, καθώς τόσο το άθροισμα των τετμημένων όσο και το άθροισμα των τεταγμένων των διανυσμάτων που την αποτελούν είναι μηδέν. Επιπροσθέτως οι γωνίες των ακμών είναι ταξινομημένες, σύμφωνα με τη φορά των δεικτών του ρολογιού.

Το πολύγωνο αυτό έχει έναν k−SUMMAND αν και μόνο αν υπάρχουν k αριθμοί στην ακολουθία $\{a_i\}$ που να αθροίζουν σε μηδέν. Σε αυτή την περίπτωση η ακολουθία ακμών του k−SUMMAND θα είναι της μορφής

$$(s_{i_1}, 1), (s_{i_2}, 1), \ldots, (s_{i_k}, 1), (0, -(k-1)), (-kL, -1)$$

όπου $i_j \in J$ και J είναι ένα υποσύνολο του $\{1, \ldots, n\}$ με πληθικότητα k. Η απόδειξη του ευθύ σκέλους είναι εύκολη. Το αντίστροφο αποδεικνύεται με το να θεωρήσουμε όλες τις περιπτώσεις των προσθετέων και να εξετάσουμε εάν οι y συντεταγμένες τους αθροίζουν σε μηδέν. ΟΕΔ



Σχήμα 8.2: Αναγωγή από το $k-$SUM στο $k-$SUMMAND πρόβλημα.

Η προηγούμενη αναγωγή υποδεικνύει ότι το $k-$SUMMAND πρόβλημα είναι τουλάχιστον τόσο δύσκολο όσο και το $k-$SUM πρόβλημα, και ίσως δυσκολότερο. Στην πραγματικότητα είναι δυσκολότερο όταν $D > 1$.

Θα θεωρήσουμε ως κατεύθυνση ενός διανύσματος τον ρητό αριθμό που εκφράζει την εφαπτομένη της γωνίας που σχηματίζει το διάνυσμα με τον θετικό x ημιάξονα, και με φορά αντίθετη των δεικτών του ρολογιού. Η διεύθυνση (και στην ουσία η εφαπτομένη) αναπαρίσταται με ένα ζευγάρι ακεραίων, που ο καθένας έχει μέγεθος το πολύ DE. Μπορούμε να συγκρίνουμε δύο διευθύνσεις σε χρόνο $\tilde{\mathcal{O}}_B(\mathsf{M}(\lg(DE)))$, όπου $\mathsf{M}(\tau)$ είναι ο χρόνος που απαιτείται για τον πολλαπλασιασμό δύο αριθμών μεγέθους τ (δείτε Εξ. (8.1)).

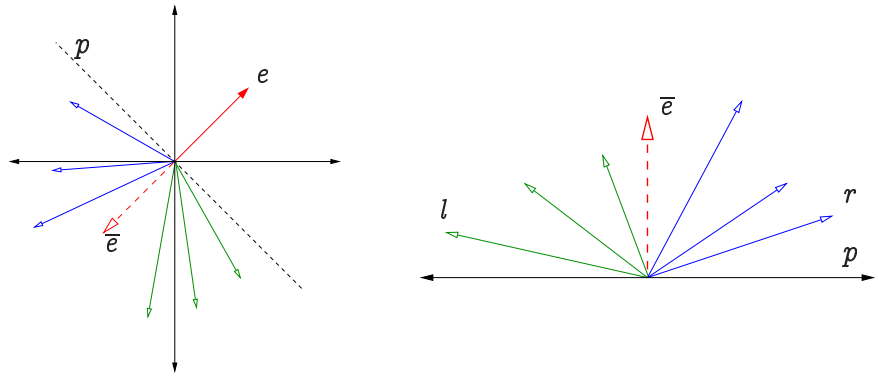
Σε ότι θα ακολουθήσει υπολογίζουμε την πολυπλοκότητα των αλγορίθμων χρησιμοποιώντας το αριθμητικό μοντέλο, real RAM [219]. Ωστόσο, μπορούμε να συνάγουμε την δυαδική πολυπλοκότητα εάν πολλαπλασιάσουμε την αριθμητική πολυπλοκότητα είτε με $\mathsf{M}(\lg(DE))$, εάν ο αλγόριθμος απαιτεί σύγκριση διευθύνσεων, είτε με $\lg(DE)$, εάν ο αλγόριθμος απαιτεί σύγκριση των συντεταγμένων.

Επιπλέον, θεωρούμε ότι v_0 είναι η κάτω αριστερά κορυφή, το οποίο σημαίνει ότι v_1 είναι η κορυφή με την μικρότερη διεύθυνση. Η παραπάνω θεώρηση είναι χωρίς βλάβη της γενικότητας καθώς μπορούμε να υπολογίσουμε την κορυφή v_0 σε χρόνο $\mathcal{O}(n)$. Η σημαντική παρατήρηση είναι ότι τα διανύσματα που ανήκουν τόσο στο σύνολο $\mathcal{U}$ όσο και στο σύνολο $\mathcal{E}$ είναι ταξινομημένα σε αύξουσα διάταξη σε σχέση με τη διεύθυνση και ότι αυτό ισχύει για κάθε ακέραιο πολύγωνο. Αυτή η παρατήρηση μας επιτρέπει να προτείνουμε αλγορίθμους για τα προβλήματα $\{2,3,4\}-$SUMMAND.

Προσθετέος ευθύγραμμο τμήμα

Παρατηρούμε ότι υπάρχει ένας $2-$SUMMAND αν και μόνο αν υπάρχουν δύο παράλληλες ακμές. Προκειμένου να αποφασίσουμε για την ύπαρξη ενός ευθύγραμμου τμήματος ως προσθετέου, υπολογίζουμε τα διανύσματα που αντιστοιχούν στις ακμές του πολυγώνου, δηλαδή την ακολουθία $\mathcal{U}$, σε χρόνο $\mathcal{O}(n)$.

Καθώς η ακολουθία $\mathcal{U}$ είναι ταξινομημένη σε σχέση με τη διεύθυνση, τη χωρίζουμε σε δύο υποακολουθίες. Η πρώτη, έστω $\mathcal{U}_1$, αποτελείται από διανύσματα με διευθύνσεις στο $[0,\pi)$, και η δεύτερη, έστω $\mathcal{U}_2$, αποτελείται από διανύσματα με διευθύνσεις στο $[\pi,2\pi)$. Η κατασκευή των $\mathcal{U}_1$ και $\mathcal{U}_2$ απαιτεί $\mathcal{O}(n)$ χρόνο. Θεωρούμε δείκτες i και j οι οποίοι διατρέχουν τις ακολουθίες $\mathcal{U}_1$ και $\mathcal{U}_2$, αντίστοιχα. Αυτό σημαίνει ότι ο δείκτης i ξεκινά με την ελάχιστη διεύθυνση στην $\mathcal{U}_1$ και κινείται προς την μέγιστη διεύθυνση του $\mathcal{U}_1$. Το ίδιο συμβαίνει και για τον δείκτη j και την ακολουθία $\mathcal{U}_2$. Εάν η διεύθυνση του διανύσματος $\mathcal{U}_1[i]$ είναι μικρότερη (αντ. μεγαλύτερη) από $\delta-\pi$, όπου δ είναι η διεύθυνση του διανύσματος $\mathcal{U}_2[j]$, τότε προχωράμε τον δείκτη i (αντ. j). Εάν η διεύθυνση του διανύσματος $\mathcal{U}_1[i]$ είναι μικρότερη της διεύθυνσης του διανύσματος $\mathcal{U}_2[j]$



Σχήμα 8.3: Υπολογισμών προσθετέων που είναι τρίγωνα.

κατά π ακριβώς, τότε υπάρχει ένας προσθετέος που είναι ευθύγραμμο τμήμα. Τόσο η χρονική όσο και η χωρική πολυπλοκότητα είναι $\mathcal{O}(n)$.

Εάν ενδιαφερόμαστε για το enumeration $2-$SUMMAND πρόβλημα τότε πρέπει να βρούμε όλα τα διανύσματα των οποίων οι διευθύνσεις διαφέρουν κατά π και για κάθε τέτοιο ζευγάρι, το οποίο ας υποθέσουμε ότι αντιστοιχεί σε δείκτες i και j αντίστοιχα, υπολογίζουμε τα αντίστοιχα πρωταρχικά διανύσματα, έστω e_i και e_j, και επιστρέψουμε d ζευγάρια διανυσμάτων, (ke_i, ke_j), όπου $1 \leq k \leq d$ και $d = \min\{d_i, d_j\}$. Στη συνέχεια αυξάνουμε τους δείκτες i και j και συνεχίζουμε τον αλγόριθμο. Ο αλγόριθμος έχει χρονική πολυπλοκότητα $\mathcal{O}(n+t)$, όπου t είναι το αριθμός όλων των πιθανών προσθετέων που είναι ευθύγραμμα τμήματα, και είναι το πολύ $\frac{nD}{2}$.

Τα προηγούμενα μας οδηγούν στο ακόλουθο θεώρημα:

Θεώρημα 8.14

*Υπάρχει ένας αλγόριθμος για το δεσισιον $2-$*SUMMAND *πρόβλημα με χρονική πολυπλοκότητα $\mathcal{O}(n)$. Υπάρχει ένας αλγόριθμος για το $2-$*SUMMAND *πρόβλημα με χρονική πολυπλοκότητα $\mathcal{O}(n+t)$. Η χρονική πολυπλοκότητα είναι και στις δύο περιπτώσεις $\mathcal{O}(n)$.*

Και στις δύο περιπτώσεις οι αλγόριθμοι είναι βέλτιστοι.

Προσθετέος τρίγωνο

Προκειμένου να επιλύσουμε το $3-$SUMMAND πρόβλημα καταρχάς υπολογίσουμε την ακολουθία πρωταρχικών ακμών $\mathcal{E}$ και την ακολουθία $\mathcal{A}$, σε χρόνο $O(nD)$. Παρατηρούμε ότι $|\mathcal{A}| = O(nD)$. Αφού $\mathcal{A}$ περιέχει ένα πολλαπλάσια των διανυσμάτων που περιέχονται στην $\mathcal{E}$, μπορούμε να υποθέσουμε ότι τα διανύσματα είναι ταξινομημένα σε αύξουσα διάταξη, πρώτα σε σχέση με τη διεύθυνση και στη συνέχεια σε σχέση με τις x και y συντεταγμένες

Αν υπαρχει ένα προσθετέος τρίγωνο τότε για κάποιο πρωταρχικό διάνυσμα $e \in \mathcal{E}$ υπάρχουν δύο δείκτες r και l, όπου $1 \leq r, l \leq |\mathcal{A}|$, τέτοιοι ώστε η διεύθυνση του διανύσματος $w = \mathcal{A}[r] + \mathcal{A}[l]$ να είναι αντίθετη από αυτή του e.

Επικεντρωνόμαστε στο αριστερό μισό του Σχ. 8.3. Το διάνυσμα $e = (e_x, e_y)$ είναι πρωταρχικό και το στιγματισμένο διάνυσμα $\overline{e} = (\overline{e}_x, \overline{e}_y) = (-e_x, -e_y)$ είναι το αντίθετό του. Θεωρούμε

έναν άξονα κάθετο στο e, αυτή είναι η ευθεία p στο σχήμα, και μόνο τα διανύσματα του $\mathcal{A}$ που βρίσκονται στο ίδιο ημιεπίπεδο με το $\overline{e}$. Μπορούμε να βρούμε αυτά τα διανύσματα σε χρόνο $\mathcal{O}(nD)$, καθώς η $\mathcal{A}$ είναι ταξινομημένη σε σχέση με τη διεύθυνση. Συμβολίζουμε επίσης με $\mathcal{A}$ αυτή την ακολουθία και επίσης παρατηρούμε ότι είναι και αυτή ταξινομημένη σε σχέση με τη διεύθυνση.

Με κατάλληλη στροφή των αξόνων, μετασχηματίζουμε το αριστερό του Σχ. 8.3 στο δεξί. Στη συνέχεια αναφερόμαστε στο δεξί μέρος γιατί είναι πιο εύκολο διαισθητικά. Όλα τα διανύσματα, εκτός από το $\overline{e}$ είναι στοιχεία του $\mathcal{A}$.

Προκειμένου να βρούμε εάν ένας προσθετέος είναι τρίγωνο, ξεκινούμε με δείκτες $r = 1$ και $l = |\mathcal{A}|$ υποθέτοντας ότι η ακολουθία $\mathcal{A}$ είναι ταξινομημένη από αριστερά προς δεξιά, όπως στο Σχ. 8.3 (δεξιό μέρος). Στη συνέχεια εξετάζουμε όλα τα διανύσματα του $\mathcal{A}$ και προσπαθούμε να βρούμε τιμές για τους δείκτες r και l τέτοιες ώστε το διάνυσμα $w = \mathcal{A}[r] + \mathcal{A}[l]$ να έχει διεύθυνση ίδια με αυτή του $\overline{e}$. Εάν αυτό επιτευχθεί τότε ελέγχουμε εάν τα κλάσματα $-\frac{w_x}{e_x}$ και $-\frac{w_y}{e_y}$ είναι ο ίδιος ακέραιος αριθμός μεταξύ 1 και d. Αν είναι ο ίδιος αριθμός τότε υπάρχει ένας προσθετέος τρίγωνο, αλλιώς αυξάνουμε και τους δύο δείκτες r και l. Αν η διεύθυνση του w είναι μικρότερη, αντίστοιχα μεγαλύτερη, από τη διεύθυνση του $\overline{e}$, τότε αυξάνουμε τον r, αντίστοιχα μειώνουμε τον l, κατά 1.

Η διάτρεξη της ακολουθίας $\mathcal{A}$ απαιτεί χρόνο $\mathcal{O}(nD)$ και καθώς πρέπει να τη διατρέξουμε για κάθε διάνυσμα που ανήκει στην ακολουθία πρωρχικών ακμών, η συνολική πολυπλοκότητα για το πρόβλημα απόφασης είναι $\mathcal{O}(n^2D)$ και η χωρική πολυπλοκότητα είναι $\mathcal{O}(nD)$.

Εάν ενδιαφερόμαστε για το πρόβλημα απαρίθμησης τότε αυξάνουμε και τους δύο δείκτες r και l, όταν διαπιστώνουμε ισότητα στις διευθύνσεις, και με αυτό τον τρόπο απαριθμούμε όλα τους πιθανούς προσθετέους τρίγωνα. Ο συνολικός χρόνος που απαιτεί ο αλγόριθμος είναι $\mathcal{O}(n^2D+t)$, όπου t είναι ο αριθμός όλων των πιθανών τριγώνων προσθετέων.

Τα παραπάνω μας οδηγούν στο ακόλουθο θεώρημα:

Θεώρημα 8.15

Υπάρχει ένας αλγόριθμος για το δεσισιου 3−SUMMAND *πρόβλημα με χρονική πολυπλοκότητα* $\mathcal{O}(n^2D)$. *Υπάρχει ένας αλγόριθμος για το* 3−SUMMAND *πρόβλημα με χρονική πολυπλοκότητα* $\mathcal{O}(n^2D+t)$. *Η χρονική πολυπλοκότητα είναι και στις δύο περιπτώσεις* $\mathcal{O}(nD)$.

Υπάρχει ένας ενναλακτικός αλγόριθμος για το πρόβλημα απόφασης ο οποίος έχει αριθμητική πολυπλοκότητα $\mathcal{O}(n^3)$ ή $\widetilde{\mathcal{O}}_B(n^3g)$ δυαδική πολυπλοκότητα και χωρική πολυπλοκότητα $\mathcal{O}(n\lg(DE))$. Πρώτα υπολογίζουμε την ακολουθία πρωταρχικών ακμών $\mathcal{E}$, σε χρόνο $\widetilde{\mathcal{O}}_B(ng)$. Εάν υπαρχει τρίγωνο προσθετέος τότε τουλάχιστον ένα από τα $\mathcal{O}(n^3)$ συστήματα γραμμικών Διοφαντικών εξισώσεων και ανισώσεων:

$$\begin{aligned} a_ie_{ix} + a_je_{jx} + a_ke_{kx} &= 0 \\ a_ie_{iy} + a_je_{jy} + a_ke_{ky} &= 0 \\ 1 \le a_i \le d_i, 1 \le a_j \le d_j, 1 \le a_k \le d_k & \end{aligned}$$

όπου $1 \le i < j < k \le n$, πρέπει να έχει λύση. Όσο για την δυαδική πολυπλοκότητα η επίλυση ενός από τα παραπάνω συστήματα άγεται από από τον υπολογισμό του υπολογισμού των $\gcd(e_{ix}, e_{jx}, e_{kx})$ και $\gcd(e_{iy}, e_{jy}, e_{ky})$ και άρα είναι $\widetilde{\mathcal{O}}_B(g)$.

Όσο αφορά το πρόβλημα απαρίθμησης, πρέπει να επιλύσουμε όλα τα παραπάνω συστήματα και κατά συνέπεια ο αλγόριθμος έχει αριθμητική πολυπλοκότητα $\mathcal{O}(n^3 + t)$ ή $\widetilde{\mathcal{O}}_B(n^3 g + t)$ δυαδική πολυπλοκότητα.

Τα παραπάνω μας οδηγούν στο συμπέρασμα ότι το decision $3-$SUMMAND πρόβλημα μπορεί να επιλυθεί πολυωνυμικά. Συνήθως όμως το n είναι πολύ μεγάλο σε σχέση με το D, και έτσι το Θεωρ. 8.15 είναι προτιμότερο και γιαυτό το λόγο δεν επεκτεινόμαστε παραπάνω σε αυτή την προσέγγιση.

Προσθετέος τετράπλευρο

Προκειμένου να προτείνουμε έναν αλγόριθμο για το δεσισιον $4-$SUMMAND πρόβλημα, υπολογίζουμε την πρωταρχική ακολουθία ακμών $\mathcal{E}$ και στη συνέχεια την ακολουθία $\mathcal{A}$, σε χρόνο $\mathcal{O}(nD)$. Υπολογίζουμε το σύνολο όλων των διανυσμάτων τέτοιων που είναι το άθροισμα δύο διαφορετικών διανυσμάτων του $\mathcal{A}$ σε χρόνο $\mathcal{O}(n^2D^2)$. Συμβολίζουμε αυτή την ακολουθία με $\mathcal{A}_2$ την ταξινομούμε πρώτα σε σχέση με την x συντεταγμένη και στη συνέχεια σε σχέση με την y συντεταγμένη. Ο χρόνος για την ταξινόμηση είναι το πολύ $\mathcal{O}(n^2D^2 \lg(nD))$.

Για κάθε διάνυσμα της $\mathcal{A}_2$, αναζητούμε στην $\mathcal{A}_2$ ένα διάνυσμα με αντίθετες x και y συντεταγμένες. Η αναζήτηση απαιτεί $\mathcal{O}(\lg(nD))$ χρόνο. Έτσι η συνολική πολυπλοκότητα του αλγορίθμου απόφασης είναι $\mathcal{O}(n^2D^2 \lg(nD))$ και η χωρική πολυπλοκότητα είναι $\mathcal{O}(n^2D^2)$.

Εάν θέλουμε να απαριθμήσουμε όλα τα δυνατά τετράπλευρα που είναι προσθετέοι τότε διεξάγουμε την αναζήτηση για κάθε διάνυσμα της $\mathcal{A}_2$. Συνεπώς η πολυπλοκότητα του αλγορίθμου απαρίθμησης είναι $\mathcal{O}(n^2D^2 \lg(nD) + t)$, όπου t είναι ο αριθμός των πιθανών τετραπλεύρων προσθετέων.

Στην πράξη δυνάμεθα να απαλλείψουμε τους λογαριθμικούς παράγοντες στην πολυπλοκότητα χρησιμοποιώντας δομές κατακερματισμού (hash functions) για την αποθήκευση των στοιχείων της $\mathcal{A}_2$. Εάν επιθυμούμε να μειώσουμε της απαιτήσεις σε χώρο τότε μπορούμε να χρησιμοποιήσουμε μια ειδική δομή δεδομένων η οποία παράγει (σε αύξουσα ή φθίνουσα σειρά) όλα τα πιθανά αθροίσματα δύο διανυσμάτων [για λεπτομέρειες δείτε 272] και η οποία έχει χωρική πολυπλοκότητα $\mathcal{O}(nD)$ και χρόνο πρόσβασης $\mathcal{O}(\lg(nD))$.

Η παραπάνω συζήτηση μας οδηγεί στο ακόλουθο θεώρημα:

Θεώρημα 8.16

Υπάρχει ένας αλγόριθμος για το δεσισιον $4-$SUMMAND πρόβλημα με χρονική πολυπλοκότητα $O(n^2D^2 \lg(nD))$. Υπάρχει ένας αλγόριθμος για το $4-$SUMMAND πρόβλημα με χρονική πολυπλοκότητα $O(n^2D^2 \lg(nD) + t)$. Η χρονική πολυπλοκότητα είναι και στις δύο περιπτώσεις $\mathcal{O}(nD)$.

Προσθετέος με k ακμές

Για το γενικό $k-$SUMMAND πρόβλημα διαχωρίζουμε δύο περιπτώσεις, όταν το k είναι άρτιος ή περιττός. Όπως και στις προηγούμενες παραγράφους πρώτα θα εξετάσουμε το πρόβλημα απόφασης.

Σε κάθε περίπτωση πρώτα υπολογίζουμε τις ακολουθίες $\mathcal{E}$ και $\mathcal{A}$ και στη συνέχεια υπολογίζουμε όλα τα πιθανά αθροίσματα από $\lfloor \frac{k}{2} \rfloor$ διανύσματα της $\mathcal{A}$. Αφού η πληθικότητα της $\mathcal{A}$ είναι

$\mathcal{O}(nD)$, αυτός ο υπολογισμός απαιτεί $\mathcal{O}((nD)^{\lfloor \frac{k}{2} \rfloor})$ χρόνο και χώρο της ίδιας τάξης μεγέθους. Συμβολίζουμε αυτή την ακολουθία με $\mathcal{A}_{\frac{k}{2}}$.

Εάν το k είναι περιττός τότε ταξινομούμε την $\mathcal{A}_{\frac{k}{2}}$, πρώτα σε σχέση με τη διεύθυνση, στη συνέχεια σε σχέση με την x και y συντεταγμένη. Η ταξινόμηση απαιτεί $\mathcal{O}((nD)^{\lfloor \frac{k}{2} \rfloor} \lg(nD))$ χρόνο. Συνεχίζουμε όπως και στην περίπτωση του προβλήματος $3-$SUMMAND. Για κάθε πρωταρχικό διάνυσμα $e \in \mathcal{E}$, διατρέχουμε την $\mathcal{A}_{\frac{k}{2}}$ με δύο δείκτες: Έναν από τα αριστερά στα δεξιά και έναν με αντίθετη φορά, προκειμένου να βρούμε δύο διανύσματα της $\mathcal{A}_{\frac{k}{2}}$ τέτοια ώστε η διεύθυνση του αθροίσματός τους να είναι αντίθετη αυτής του e. Η πολυπλοκότητα του αλγορίθμου είναι $\mathcal{O}(n^{\lceil \frac{k}{2} \rceil} D^{\lfloor \frac{k}{2} \rfloor} + (nD)^{\lfloor \frac{k}{2} \rfloor} \lg(nD))$ ή $\mathcal{O}(n^{\lceil \frac{k}{2} \rceil} D^{\lfloor \frac{k}{2} \rfloor})$ αν υποθέσουμε ότι $n > \lg(nD)$.

Εάν το k είναι άρτιος τότε προχωρούμε όπως στην περίπτωση του προβλήματος $4-$SUMMAND. Δηλαδή ταξινομούμε την $\mathcal{A}_{\frac{k}{2}}$, πρώτα σε σχέση με την x συντεταγμένη και στη συνέχεια σε σχέση με την y. Η ταξινόμηση απαιτεί $\mathcal{O}(n^{\lceil \frac{k}{2} \rceil} D^{\lfloor \frac{k}{2} \rfloor} \lg(nD))$ χρόνο. Παρατηρούμε ότι αφού το k είναι άρτιος, τότε $\lceil \frac{k}{2} \rceil = \lfloor \frac{k}{2} \rfloor$. Τέλος, για κάθε διάνυσμα της $\mathcal{A}_{\frac{k}{2}}$, αναζητούμε ένα άλλο διάνυσμα με αντίθετες x και y συντεταγμένες. Η αναζήτηση απαιτεί $\mathcal{O}(\lg(nD))$ χρόνο. Άρα η πολυπλοκότητα του αλγορίθμου είναι $\mathcal{O}(n^{\lceil \frac{k}{2} \rceil} D^{\lfloor \frac{k}{2} \rfloor} \lg(nD))$.

Όσο αφορά το πρόβλημα απαρίθμησης, και στις δύο περιπτώσεις, k άρτιος ή περιττός, συνεχίσουμε την αναζήτηση ακόμα και όταν βρούμε έναν $k-$SUMMAND.

Η παραπάνω συζήτηση μας επιτρέπει να διατυπώσουμε το παρακάτω θεώρημα:

Θεώρημα 8.17

*Υπάρχει ένας αλγόριθμος για το δεσισιου $k-$*SUMMAND *πρόβλημα με χρονική πολυπλοκότητα $\mathcal{O}(n^{\lceil \frac{k}{2} \rceil} D^{\lfloor \frac{k}{2} \rfloor} \lambda)$, όπου $\lambda = 1$ αν ο k είναι περιττός και $\lambda = \lg(nD)$ αν ο k είναι άρτιος.*

*Υπάρχει ένας αλγόριθμος για το ευυμερατιου $k-$*SUMMAND *πρόβλημα με χρονική πολυπλοκότητα $\mathcal{O}(n^{\lceil \frac{k}{2} \rceil} D^{\lfloor \frac{k}{2} \rfloor} \lambda + t)$, όπου t είναι το πλήθος όλων των (διαφορετικών) διασπάσεων σε δύο προσθετέους, όπου τουλάχιστον ο ένας έχει k ακμές.*

Η χωρική πολυπλοκότητα και στις δύο περιπτώσεις είναι $\mathcal{O}((nD)^{\lfloor \frac{k}{2} \rfloor})$.

8.3 Υλοποίηση και πολύγωνα με ένα και κανένα εσωτερικό ακέραιο σημείο

Στην παρούσα παράγραφο σκιαγραφούμε την υλοποίησή μας στους αλγορίθμους που έχουμε αναφέρει και παρουσιάζουμε και μία εφαρμογή που αφορά όλες τις δυνατές διασπάσεις κατά Minkowski όλων των ακέραιων πολυγώνων με ένα και κανένα εσωτερικό ακέραιο σημείο. Επίσης παρουσιάζουμε και πειράματα σε διάφορα τυχαία δεδομένα.

Η υλοποίηση των αλγορίθμων έγινε σε γλώσσα C++ και χρησιμοποιήσαμε την γεωμετρική βιβλιοθήκη CGAL [50]. Η CGAL παρέχει αντικείμενα και λειτουργίες για σημεία, διανύσματα και πολύγωνα. Επιπρόσθετα παρέχει μία κλάση για τη διεύθυνση διανυσμάτων και συγκρίσεις μεταξύ τους. Ο κώδικάς είναι ελεύθερα διαθέσιμος στη διεύθυνση http://www.di.uoa.gr/~et.

Τα πειράματα εκτελέστηκαν σε έναν υπολογιστή 2.6GHz Pentium, με 1GB RAM, με λειτουργικό σύστημα Linux, με πυρήνα έκδοσης 2.6.10. Για την μεταγλώτισση των προγραμμάτων χρησιμοποιήθηκε ο μεταγλωτιστής g++, v. 3.3.5, με επιλογές -O3 -DNDEBUG.

Πειράματα με τυχαία ακέραια πολύγωνα

Πραγματοποιήσαμε διάφορα πειράματα προκείμενου να ελένξουμε την αποδοτικότητα των αλγορίθμων που προτείνουμε για τα δεσισιον $\{2,3,4\}-$SUMMAND προβλήματα. Θα συμβολίσουμε τους αλγορίθμους με `ET(s)`, `ET(t)` και `ET(q)` αντίστοιχα. Επίσης υλοποιήσαμε στη CGAL τον αλγόριθμο των Γαο ανδ Λαυδερ [111], ο οποίος αναφέρεται στο γενικό πρόβλημα της διάσπασης κατά Minkowski. θα συμβολίσουμε αυτόν τον αλγόριθμο με `GL`. Οι χρόνοι των πειραμάτων παρουσιάζονται στον Πίνακα 8.1 και είναι σε msec.

Οι στήλες A_k, B_k, C_k και D_k, όπου $k \in \{10,20,30,40,50,60,70\}$, αναφέρονται σε 500 ακέραια πολύγωνα με k ακμές, δειγματολειπτημένα στο χωρίο $[0,3000]\times[0,3000]$. Τα πολύγωνα των δεδομένων B_k, C_k και D_k, κατασκευάστηκαν έτσι ώστε να επιδέχονται τουλάχιστον μία διάσπαση με προσθετέο ευθύγραμμο τμήμα, τρίγωνο και τετράπλευρο, αντίστοιχα. Η στήλη E_k αναφέρεται σε 500 ακέραια πολύγωνα τα οποία είναι η κυρτή θήκη 50 τυχαίων ακέραιων σημείων στο χωρίο $[0,k]\times[0,k]$.

Σε όλες τις περιπτώσεις οι αλγόριθμοι που προτείνουμε είναι σημαντικά γρηγορότεροι. Αυτό συμβαίνει λόγω του γεγονότος ότι οι `ET` αλγόριθμοι είναι ειδικευμένοι για διασπάσεις σε προσθετέους μικρού μεγέθους και άρα επιλύουν ένα πολυωνυμικό πρόβλημα ενώ αντίθετα ο αλγόριθμος `GL` επιλύει το γενικό πρόβλημα που είναι NP-complete. Ιδιαίτερα πρέπει να προσεχθεί ότι οι χρόνοι του αλγορίθμου `ET(s)` είναι σχεδόν οι ίδιοι σε όλα τα δεδομένα. Ο λόγος γιαυτό είναι ότι η πολυπλοκότητά του εξαρτάται γραμμικά (και μόνο) από το πλήθος της εισόδου. Επιπρόσθετα ο περισσότερο χρόνος του `GL` αλγορίθμου δαπανάται για τον υπολογισμό των εσωτερικών ακέραιων σημείων και συνεπεία αυτού οι χρόνοι για τα δεδομένα A_k, B_k, C_k, D_k δεν είναι καθόλου ικανοποιητικοί. Ωστόσο στην περίπτωση E_k, όπου τα πολύγωνα έχουν λίγα εσωτερικά ακέραια σημεία οι χρόνοι του `GL` είναι αρκετά ανταγωνιστικοί.

Σε κάθε περίπτωση, αν και τα πειράματα δείχνουν την υπεροχή των αλγορίθμων που προτείνουμε απαιτείται μια προσεκτική και αποδοτική υολοποίηση αλλά και ένας πιο εμπεριστατωμένος πειραματισμός.

Ακέραια πολύγωνα χωρίς εσωτερικά ακέραια σημεία

Υπάρχουν μόνο 16 ακέραια πολύγωνα με ένα εσωτερικό ακέραιο σημείο (modulo unimodular transformations), όπως απέδειξε ο Rabinowitz [220] [δείτε επίσης 237]. Υπολογίζουμε όλες τις δυνατές διασπάσεις κατά Minkowski. Τα αποτελέσματα εμφανίζονται στο Σχ. 8.4 και στο Σχ. 8.5. Τέτοιου είδους ακέραια πολύγωνα παρουσιάζουν ιδιαίτερο ενδιαφέρον για τα Bézier patches [115, 164, 165].

Ακέραια πολύγωνα με κανένα εσωτερικό ακέραιο σημείο

Υπολογίσαμε όλες τις διασπάσεις ακεραίων πολυγώνων με κενένα εσωτερικό σημείο και εμβαδό μικρότερο ή ίσο από 3. Όλες οι δυνατές διασπάσεις εμφανίζονται στο Σχ. 8.6.

Αν χρησιμοποιήσουμε τους αλγορίθμους για $\{2,3,4\}-$SUMMAND των προήγουμενων παραγράφων μπορούμε να διασπάσουμε όλα τα ακέραια πολύγωνα (up to unimodular transformations) με κανένα εσωτερικό ακέραιο σημείο. Όλες οι δυνατές διασπάσεις παρουσιάζονται στο Σχ. 8.7.

	A_{10}	A_{20}	A_{30}	A_{40}	A_{50}	A_{60}	A_{70}
ET(s)	0.007	0.01	0.02	0.03	0.04	0.04	0.05
ET(t)	1.1	5.1	9.6	16.5	30.1	40.3	56.2
ET(q)	1.6	6.2	11.6	19.1	34.4	46.1	65.1
GL	11150	15270	22050	23995	23370	26205	27315

	B_{10}	B_{20}	B_{30}	B_{40}	B_{50}	B_{60}	B_{70}
ET(s)	0.004	0.006	0.008	0.01	0.01	0.02	0.02
ET(t)	4.3	7.2	9.7	17.3	25.5	39.3	49.9
ET(q)	3.3	9.2	12.1	19.2	29.7	44.8	57.4
GL	27330	50105	37930	53635	46345	54205	36475

	C_{10}	C_{20}	C_{30}	C_{40}	C_{50}	C_{60}	C_{70}
ET(s)	0.003	0.006	0.008	0.01	0.01	0.02	0.02
ET(t)	1.8	3.6	10.4	16.3	27.8	37.5	53.7
ET(q)	2.6	5.3	12.7	18.2	33.0	43.2	62.1
GL	25630	27065	52810	37215	84510	86555	51465

	D_{10}	D_{20}	D_{30}	D_{40}	D_{50}	D_{60}	D_{70}
ET(s)	0.003	0.006	0.008	0.01	0.01	0.02	0.02
ET(t)	1.6	5.2	9.4	19.3	28.3	43.2	54.3
ET(q)	1.9	5.5	11.2	22.4	33.5	49.5	63.1
GL	32950	78840	72230	71240	75805	64690	73335

	E_{10}	E_{20}	E_{30}	E_{40}	E_{50}	E_{60}	E_{70}
ET(s)	0.002	0.003	0.003	0.003	0.004	0.004	0.004
ET(t)	0.1	0.4	0.3	0.4	0.4	0.5	0.5
ET(q)	0.1	0.3	0.4	0.4	0.5	0.6	0.6
GL	0.1	0.2	0.4	0.7	1.2	1.6	2.2

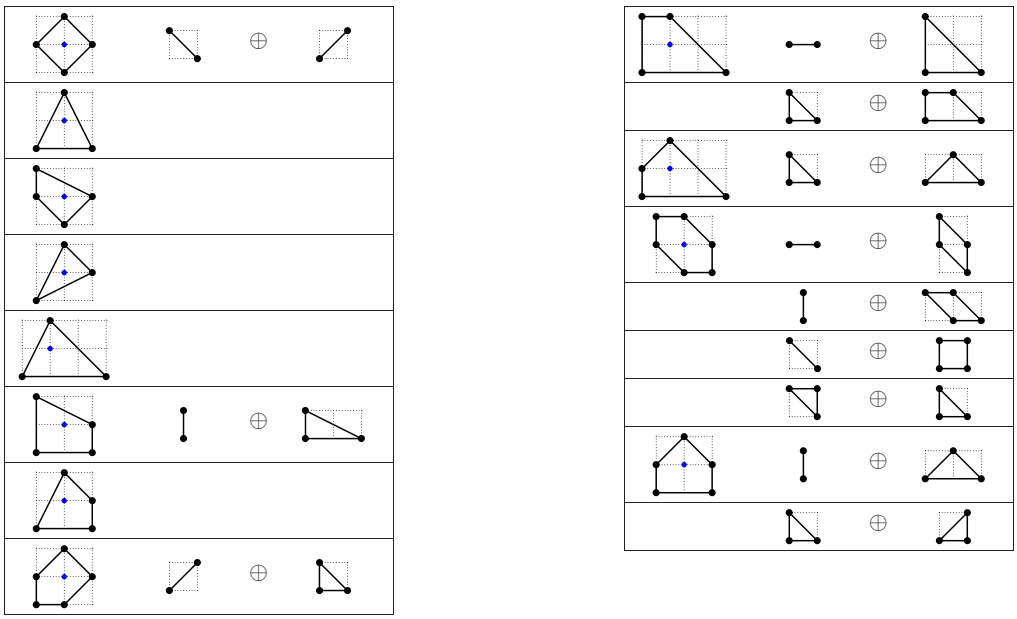
Πίνακας 8.1: Πειραματικά αποτελέσματα

Καταρχάς πρέπει υπολογίσουμε όλα τα ακέραια πολύγωνα με κανένα εσωτερικό σημείο και γιαυτό χρειαζόμαστε το παρακάτω θεώρημα:

Θεώρημα 8.18

[237] Κάθε ακέραιο πολύγωνο με κάνένα εσωτερικό ακέραιο σημείο είναι, κάτω από ένα μετασχηματισμό ο οποίος έχει πίνακα με ορίζουσα 1 (unimodular transformation) ισοδύναμο με ένα πολύγωνο $T_{m,n}$ με κορυφές $\{(0,0),(0,1),(m+n,0),(n,1)\}$, όπου $m,n \geq 0$, ή ένα τρίγωνο Δ_2 με κορυφές $\{(0,0),(2,0),(0,2)\}$.

Η ακολουθία ακμών του Δ_2 είναι $\{2(1,0), 2(-1,1), 2(0,-1)\}$. Εύκολα μπορούμε να διαπιστώσουμε ότι το Δ_2 επιδέχεται διάσπαση κατά Minkowski σε δύο ίσους προσθετέους που είναι



Σχήμα 8.4: Διάσπαση κατά Minkowski ακέραιων πολυγώνων με ένα εσωτερικό ακέραιο σημείο (συνεχίζεται στο επόμενο σχήμα).

τρίγωνα. Αν το Δ_1 είναι τρίγωνο με κορυφές $\{(0,0),(1,0),(0,1)\}$ τότε $\Delta_2 = \Delta_1 \oplus \Delta_1 = 2\Delta_1$. Παρατηρούμε ότι τα Δ_2 και Δ_1 είναι ομοθετικά. Η διάσπαση παρουσιάζονται στην πρώτη γραμμή του Σχ. 8.7.

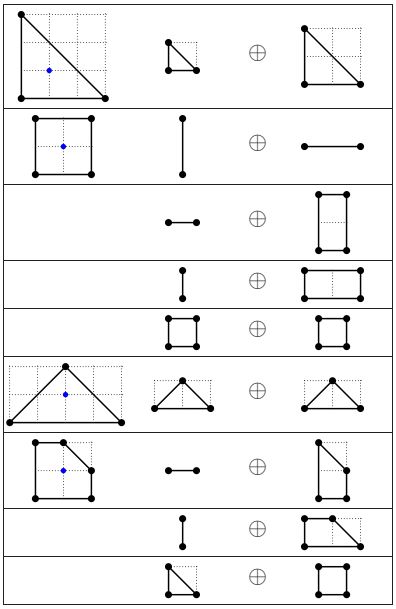
Προκειμένου να διασπάσουμε όλα τα ακέραια πολύγωνα $T_{m,n}$ διακρίνουμε τις ακόλουθες περιπτώσεις:

- $m \geq 1, n = 0$

  Σε αυτή την περίπτωση το πολύγωνο $T_{1,0}$ είναι τρίγωνο με κορυφές $\{(0,0),(m,0),(0,1)\}$ και η ακολουθία ακμών του είναι $\{(m,0),(-m,1),(0,1)\}$. Εύκολα μπορούμε να ελένξουμε ότι το τρίγωνο δεν επιδέχεται διάσπαση κατά Minkowski. Στο ίδιο συμπέρασμα μπορούμε να φτάσουμε αν χρησιμοποιήσουμε την προσέγγιση των Gao and Lauder [111, Th. 8] ελέγχοντας ότι $\gcd(0,1,m) = 1$.

- $m = 0, n \geq 1$

  Σε αυτή την περίπτωση το πολύγωνο $T_{0,n}$ είναι τετράπλευρο με κορυφές $\{(0,0),(n,0),(n,1),(0,1)\}$ και η ακολυθία ακμών του είναι $\{(n,0),(0,1),(-n,0),(0,-1)\}$. Οι δύο προσθετέοι της διάσπασης κατά Minkowksi του πολυγώνου είναι είτε δύο ευθύγραμμα τμήματα (αυτή είναι η

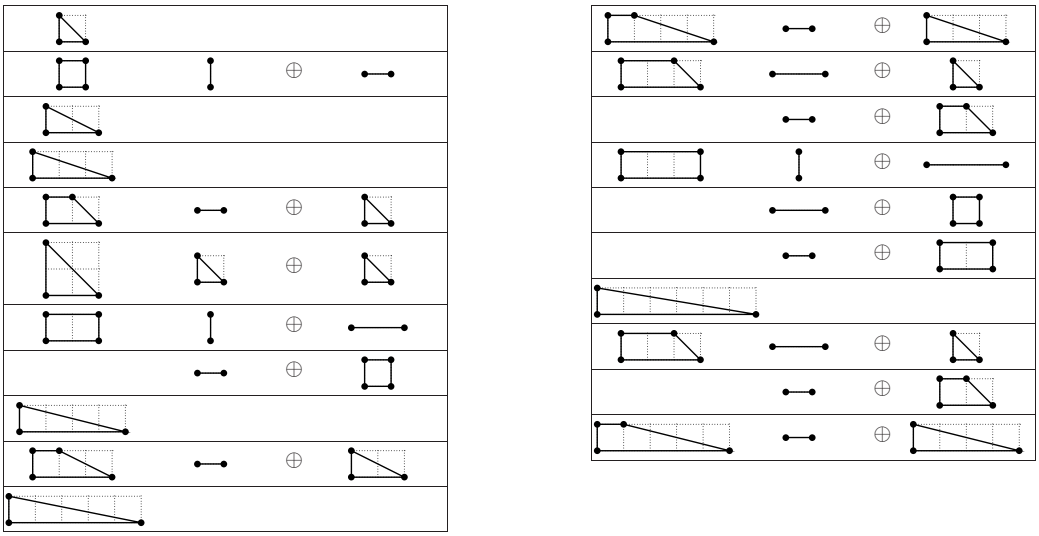


Σχήμα 8.5: Συνέχεια: Διάσπαση κατά Minkowski ακέραιων πολυγώνων με ένα εσωτερικό ακέραιο σημείο.

πρώτη ισότητα της δεύτερης γραμμής του Σχ. 8.7) ή ένα ευθύγραμμο τμήμα και ένα ορθογώνιο (αυτή είναι η δεύτερη ισότητα της δεύτερης γραμμής του Σχ. 8.7), όπου $1 \leq k \leq n$. Η τελευταία ισότητα της δεύτερης γραμμής του Σχ. 8.7 αντιπροσωπεύει τη μοναδική διάσπαση κατά Minkowski του πολυγώνου $T_{0,n}$ σε $n+1$ μη περαιτέρω διασπάσιμους προσθετέους.

- $m \geq 1, n \geq 1$

  Σε αυτή την περίπτωση το πολύγωνο $T_{m,n}$ είναι ένα τραπέζιο με κορυφές $\{(0,0),(m+n,0),(n,1),(0,1)\}$ και η ακολουθία ακμών του είναι $\{(m+n,0),(-m,1),(-n,0),(0,-1)\}$. Μπορούμε να διασπάσουμε το $T_{m,n}$ σε δύο προσθετέους είτε σε ένα ευθύγραμμο τμήμα και ένα τραπέζιο (αυτή είναι η πρώτη ισότητα της τρίτης γραμμής του Σχ. 8.7, όπου $1 \leq k \leq n$) είτε στο σε ένα τρίγωνο και ένα ευθύγραμμο τμήμα (αυτή είναι η δεύτερη ισότητα της τρίτης γραμμής του Σχ. 8.7). Η τελευταία ισότητα της τρίτης γραμμής του Σχ. 8.7 παρουσιάζει τη μοναδική διάσπαση κατά Minkowski του $T_{0,n}$ σε μη περαιτέρω διασπάσιμους προσθετέους.



Σχήμα 8.6: Διάσπαση κατά Minkowski ακέραιων πολυγώνων με κανένα εσωτερικό ακέραιο σημείο και εμβαδόν μικρότερο από 3.

8.4 Βελτίωση του γενικού αλγόριθμου διάσπασης

Σε αυτό το εδάφιο επανερχόμαστε στο γενικό πρόβλημα του MINKOWSKI-DECOMPOSITION και προτείνουμε μια διαφορετική προσέγγιση για την επίλυση του από αυτή των Gao and Lauder [111] η οποία θα μας επιτρέψει να βελτιώσουμε την ασυμπτωτική πολυπλοκότητα του προβλήματος. Θεωρούμε ωστόσο πιο σημαντικό το γεγονός ότι αναμένουμε αυτή η εναλλακτική προσέγγιση να οδηγήσει σε πολύ γρήγορες υλοποιήσεις για πρακτικά προβλήματα και να επιτρέψει την ανάπτυξη πιθανοτικών και προσεγγιστικών αλγορίθμων.

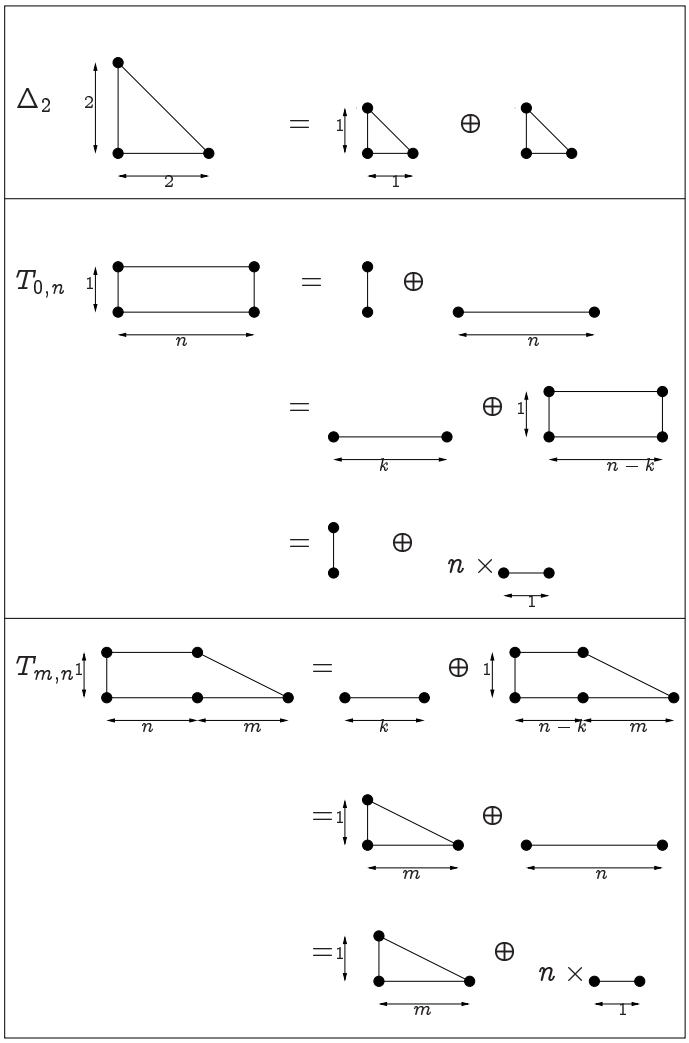
Η βασική ιδέα είναι ότι αρκεί η εύρεση συνδυασμών των διανυσμάτων των οποίων το (διανυσματικό) άθροισμα είναι μηδέν. Παρατηρούμε ότι το άθροισμα ενός υποσυνόλου του αρχικού συνόλου των διανυσμάτων είναι μηδέν αν και μόνο αν το άθροισμα τόσο των x όσο και των y συντεταγμένων είναι μηδέν.

Για τα επόμενα θα χρειαστούμε τον ορισμό του προβλήματος SUBSET-SUM, το οποίο είναι NP-complete:

Πρόβλημα 8.19. SUBSET-SUM

Δοθέντος ενός συνόλου n θετικών ακεραίων και ενός στόχου S, αποφάσισε εάν υπάρχει ένα υποσύνολό τους τέτοιο ώστε τα στοιχεία του να αθροίζουν σε S.

Θα χρησιμοποιήσουμε τον ακόλουθο μετασχηματισμό:



Σχήμα 8.7: Διάσπαση κατά Minkowski όλων των ακέραιων πολυγώνων με κανένα εσωτερικό ακέραιο σημείο.

Λήμμα 8.20. *Ένα στιγμιότυπο του προβλήματος* MINKOWSKI-DECOMPOSITION *μπορεί να μετασχηματιστεί σε ένα στιγμιότυπο του προβλήματος* SUBSET-SUM*, έτσι ώστε το στιγμιότυπο του* MINKOWSKI-DECOMPOSITION *να επιδέχεται λύσης αν και μόνο αν το στιγμιότυπο του* SUBSET-SUM *επιδέχεται λύσης.*

Απόδειξη: Έστω Q ακέραιο πολύγωνο με n κορυφές και έστω DE ο μεγαλύτερος ακέραιος που εμφανίζεται στις συντεταγμένες. Υπολογίζουμε την ακολουθία πρωταρχικών ακμών $\mathcal{E}$. Θεωρούμε τις συντεταγμένες των πρωταρχικών ακμών e_i και αντιστοιχούμε σε κάθε διάνυσμα τον θετικό αριθμό $a_i = e_{ix} + Le_{iy} + DE$ όπου $1 \leq i < n$ και L αρκούντως μεγάλο, για παράδειγμα $L = nDE$. Προσθέτουμε την ποσότητα DE σε κάθε a_i έτσι ώστε $a_i > 0, 1 \leq i < n$. Θεωρούμε d_i αντίγραφα κάθε a_i, και έτσι ο συνολικός τους αριθμός είναι $\sum_{i=1}^{n} d_i = \mathcal{O}(nD)$.

Τώρα έχουμε ολοκληρώσει τον μετασχηματισμό και αφού το πολύγωνο Q επιδέχεται διάσπασης αν και μόνο αν υπάρχει ένα υποσύνολο των a_i του οποίου τα στοιχεία να αθροίζουν σε

μηδέν. Η βασική ιδέα είναι ότι εάν ένα a_i ανήκει στο εν λόγω υποσύνολο τότε η ακμή στην οποία αντιστοιχεί ανήκει σε προσθετέο του πολυγώνου και το αντίστροφο.

Παρατηρούμε ότι ο μετασχηματισμός απαιτεί $\mathcal{O}(nD)$ χρόνο, και ότι ίδιας τάξης είναι και το μέγεθος του προβλήματος SUBSET-SUM. ΟΕΔ

Η πολυπλοκότητα επίλυσης του SUBSET-SUM με τη χρήση δυναμικού προγραμματισμού είναι $\mathcal{O}(N^2W)$ [δείτε για παράδειγμα 135], [56] όπου N είναι η πληθικότητα του συνόλου και W είναι ένα άνω φράγμα στην απόλυτη τιμή κάθε στοιχείου. Στην περίπτωσή μας $N = \mathcal{O}(nD)$ και $W = \mathcal{O}(nDE^2)$, συνεπώς η συνολική πολυπλοκότητα του αλγορίθμου είναι $\mathcal{O}(n^3D^3E^2)$. Η πολυπλοκότητα είναι η ίδια με αυτή του αλγορίθμου των Gao and Lauder [111].

Ωστόσο, η προσέγγιση που υιοθετήσαμε μας επιτρέπει να χρησιμοποιήσουμε το πρότυπο του δυναμικού προγραμματισμού και είναι εντελώς διαφορετική από αυτή των Gao and Lauder [111], καθώς αποφεύγουμε τον ρητό υπολογισμό των εσωτερικών ακέραιων σημείων του πολυγώνου. Επιπρόσθετα, εάν χρησιμοποιήσουμε τον αλγόριθμο ισοζυγίου (balancing algorithm) του Pisinger [217] για να επιλύσουμε το αντίστοιχο SUBSET-SUM πρόβλημα, και ο οποίος έχει την καλύτερη δυνατή πολυπλοκότητα, $\mathcal{O}(NW)$, τότε η πολυπλοκότητα του αλγόριθμου διάσπασης είναι $\mathcal{O}(n^2D^2E^2)$. Με αυτή την τεχνική βελτιώνουμε την πολυπλοκότητα του προβλήματος κατά ένα παράγοντα nD.

Η προηγούμενη συζήτηση μας επιτρέπει να διατυπώσουμε το παρακάτω θεώρημα:

Θεώρημα 8.21

Υπάρχει ένας αλγόριθμος για το δεσισιου MINKOWSKI-DECOMPOSITION *πρόβλημα με αριθμητική πολυπλοκότητα* $\mathcal{O}(n^2D^2E^2)$.

8.5 Μελλοντικές επεκτάσεις

Προκειμένου να απαριθμήσουμε όλους τους δυνατούς προσθετέους ενός ακέραιου πολυγώνου, ακολουθούμε την προσέγγιση της Παραγράφου 8.4 και μπορούμε να χρησιμοποιήσουμε κάποιον από τους διάφορους αλγορίθμους που είναι διαθέσιμοι για το πρόβλημα PARTITION [135]. Ωστόσο απαιτείται μια ενδελεχής πειραματική μελέτη προκειμένου να υιοθετήσουμε ή να συνάδουμε τον βέλτιστο αλγόριθμο.

Επιπρόσθετα, η προσέγγιση της Εν. 8.4 μπορεί εύκολα να οδηγήσει σε ένα πιθανοτικό αλγόριθμο. Επιλέγουμε $L = nDE$. Οι ποσότητες είναι της μορφής $a_i = e_{ix} + Le_{iy}$, με μέγιστη τιμή $E(L+1)$, και υπάρχουν $d_i \leq D$ αντίγραφα από κάθε a_i. Συμπεραίνουμε ότι η μέγιστη τιμή αθροίσματος είναι $nDE(L+1) = \mathcal{O}((nDE)^2)$.

Προκειμένου να ελέγξουμε εάν το άθροισμα μηδενίζεται $\bmod p$, όπου $p > 0$ είναι ένας τυχαίος ακέραιος, πρέπει να φράξουμε την πιθανότητα $\mathbf{Prob}[failure]$ ότι ένα τυχαίο άθροισμα $S \in [0, nDE(L+1)]$ μηδενίζεται $\bmod p$, όταν $S \neq 0$, όπου p είναι ένα πρώτος αριθμός επιλεγμένος τυχαία από στο διάστημα $[2, \ldots, x]$.

Μπορούμε να επιτύχουμε το στόχο μας χρησιμοποιώντας τον πιθανοτικό αλγόριθμο ελέγχου ισότητα αλφαριθμητικών από το βιβλίο των Motwani and Raghavan [196].

Λήμμα 8.22. *γ [196] Έστω a, b δύο αριθμοί με τ δυαδικά ψηφία (bits) ο καθένας. Αν $a \neq b$, τότε*

$$\mathbf{Prob}[failure] = \mathbf{Prob}[a = b \mod p] < \frac{1}{2}$$

όπου p είναι ένας πρώτος αριθμός ομοιόμορφα κατανεμημένος στο διάστημα $[2, \ldots, 4\tau^2]$.

Στην περίπτωσή μας $a = 0$ και $b = S$, οπότε χρειαζόμαστε $\tau \simeq 2 \lg (nDE)$ bits για να τους κωδικοποιήσουμε. Έτσι μπορούμε να χρσιμοποιήσουμε το προηγούμενο Λήμμα, επιλέγοντας έναν πρώτο αριθμό από το διάστημα $[2, \ldots, 4\tau^2]$, προκειμένου να επιτύχουμε $\mathbf{Prob}[failure] < \frac{1}{2}$.

Καταλήγοντας, η αναγωγή του προβλήματος της διάσπασης στο SUBSET-SUM πρόβλημα ενδέχεται να οδηγήσει σε προσεγγιστικούς αλγορίθμους. Ένα πρώτο βήμα σε αυτή την κατεύθυνση πιθανόν να είναι η υιοθέτηση του πρώτου πραγματικά πολυωνυμικού χρόνου προσσεγγιστικού σχήματος για το SUBSET-SUM πρόβλημα των Ibarra and Kim [137] ή η υιοθέτηση του γρηγορότερου μέχρι σήμερα προσεγγιστικού αλγορίθμου των Kellerer et al. [151].

Βιβλιογραφία

[1] A. Akritas. There is no "Uspensky's method". Extended Abstract. In *Proc. Symposium on Symbolic and Algebraic Computation*, pages 88–90, Waterloo, Ontario, Canada, 1986.

[2] A. Akritas. An implementation of Vincent's theorem. *Numerische Mathematik*, 36:53–62, 1980.

[3] A. Akritas and A. Strzebonski. A comparative study of two real root isolation methods. *Nonlinear Analysis: Modelling and Control*, 10(4):297–304, 2005.

[4] A. Akritas, A. Bocharov, and A. Strzébonski. Implementation of real root isolation algorithms in Mathematica. In *Abstracts of the International Conference on Interval and Computer-Algebraic Methods in Science and Engineering (Interval '94)*, pages 23–27, St. Petersburg, Russia, March 1994.

[5] A.G. Akritas. *Elements of Computer Algebra with Applications*. J. Wiley & Sons, New York, 1989.

[6] A. Alesina and M. Galuzzi. A new proof of Vincent's theorem. *L'Enseignement Mathématique*, 44:219–256, 1998.

[7] H. Alt, O. Cheong, and A. Vigneron. The Voronoi Diagram of Curved Objects. *Discrete and Computational Geometry*, 34(3):439–453, Sep 2005.

[8] P. Angelier and M. Pocchiola. A sum of squares theorem for visibility. In *Procs of 17th SoCG*, pages 302–311. ACM Press, 2001.

[9] F. Anton. *Voronoi diagrams of semi-algebraic sets*. PhD thesis, The University of British Columbia, January 2004.

[10] F. Anton, J.-D. Boissonnat, D. Mioc, and M. Yvinec. An exact predicate for the optimal construction of the additively weighted Voronoi diagram. In *Europ. Workshop Comput. Geom.*, 2002.

[11] D. Attali and J.-D. Boissonnat. Complexity of the delaunay triangulation of points on polyhedral surfaces. *Discr. & Comp. Geometry*, 30(3):437–452, 2003.

[12] D. Bailey, J. Borwein, and R. Crandall. On the Khintchine Constant. *Mathematics of Computation*, 66:417–431, 1997.

[13] I. Baran, E. Demaine, and M. Patrascu. "subquadratic algorithms for 3sum". *LNCS*, pages 409–425, 2005.

[14] S. Basu, R. Pollack, and M-F.Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2003. ISBN 3-540-00973-6.

[15] M. Ben-Or, D. Kozen, and J. H. Reif. The complexity of elementary algebra and geometry. *J. Comput. Syst. Sci.*, 32:251–264, 1986.

[16] M. Ben-Or, D. Feig, E.and Kozen, and P. Tiwari. A fast parallel algorithm for determining all roots of a polynomial with real roots. *SIAM J. Comput.*, 17(6):1081–1092, 1988.

[17] E. Berberich, A. Eigenwillig, M. Hemmer, S. Hert, K. Mehlhorn, and E. Schömer. A computational basis for conic arcs and boolean operations on conic polygons. In *Proc. 10th European Symposium on Algorithms*, volume 2461 of *Lecture Notes Comput. Sci.*, pages 174–186, 2002.

[18] E. Berberich, A. Eigenwillig, M. Hemmer, S. Hert, L. Kettner, K. Mehlhorn, J. Reichel, S. Schmitt, E. Schömer, and N. Wolpert. EXACUS: Efficient and Exact Algorithms for Curves and Surfaces. In *ESA*, volume 1669 of *LNCS*, pages 155–166. Springer, 2005.

[19] Bernard Mourrain and Jean-Pierre Técourt and Monique Teillaud. On the computation of an arrangement of quadrics in 3d. *Computational Geometry*, 30(2):145–164, 2005.

[20] P. Bikker. *The Bézout Construction of the Resultant*. PhD thesis, RISC, Univ. of Linz, Austria, 2001.

[21] P. Bikker and A. Yu. Uteshev. On the Bézout construction of the resultant. *J. Symbolic Computation*, 28(1–2):45–88, July/August 1999.

[22] D. Bini. Numerical computation of polynomial zeros by means of Aberth's method. *Numerical Algorithms*, 13(3–4):179–200, 1996.

[23] D. Bini and G. Fiorentino. Design, analysis, and implementation of a multiprecision polynomial rootfinder. *Numerical Algorithms*, pages 127–173, 2000.

[24] D. Bini and V. Y. Pan. *Fundamental Algorithms*, volume 1 of *Polynomial and Matrix Computations*. Birkhäuser, Boston, MA, 1994.

[25] D. Bini and V.Y. Pan. *Polynomial and Matrix Computations*, volume 1: Fundamental Algorithms. Birkhäuser, Boston, 1994.

[26] I. Boada, N. Coll, and J.A. Sellarès. Multiresolution approximations of generalized Voronoi diagrams. In *Proc. Intern. Conf. Comp. Science*, pages 98–106, 2004.

[27] J.-D. Boissonnat and C. Delage. Convex hull and Voronoi diagram of additively weighted points. In *Proc. 13th Annu. European Sympos. Algorithms*, volume 3669 of *Lecture Notes Comput. Sci.*, pages 367–378. Springer-Verlag, 2005.

[28] J.-D. Boissonnat and M. Karavelas. On the combinatorial complexity of Euclidean Voronoi cells and convex hulls of d-dimensional spheres. In *Proc. SODA*, pages 305–312, 2003.

[29] J-D. Boissonnat and M. Yvinec. *Algorithmic Geometry*. Cambridge University Press, Cambridge, 1999.

[30] Jean-Daniel Boissonnat and Monique Teillaud, editors. *Effective Computational Geometry for Curves and Surfaces*, volume (to appear) of *Mathematics and Visualization*. Springer, 2006.

[31] E. Bombieri and A. van der Poorten. Continued fractions of algebraic numbers. In *Computational algebra and number theory (Sydney, 1992)*, pages 137–152. Kluwer Acad. Publ., Dordrecht, 1995.

[32] C. B. Boyer. *A history of mathematics*. Wiley and Sons, Inc, New York, 1991.

[33] R. Brent, A. van der Poorten, and H. Riele. A Comparative Study of Algorithms for Computing Continued Fractions of Algebraic Numbers. In Henri Cohen, editor, *ANTS*, LNCS, pages 35–47. Springer, 1996.

[34] W. Brown. On Euclid's algorithm and the computation of polynomial greatest common divisors. *Journal of the ACM*, 18(4):478–504, 1971.

[35] W. Brown and J. Traub. On euclid's algorithm and the theory of subresultants. *Journal of The ACM*, 18(4):505–514, October 1971.

[36] W. S. Brown. The subresultant PRS algorithm. *ACM Trans. Math. Software*, 4:237–249, 1978.

[37] W. S. Brown. On the subresultant PRS algorithm. In *SYMSAC '76: Procs of the 3rd ACM symposium on Symbolic and Algebraic Computation*, page 271, New York, NY, USA, 1976. ACM Press.

[38] B. Buchberger, G. E. Collins, R. Loos, and R. Albrecht, editors. *Computer Algebra: Symbolic and Algebraic Computation*. Springer-Verlag, 2nd edition, 1983.

[39] C. Burnikel, K. Mehlhorn, and S. Schirra. The LEDA class real number. Technical Report MPI-I-96-1-001, Max-Planck Institut Inform., Saarbrücken, Germany, January 1996.

[40] C. Burnikel, S. Funke, K. Mehlhorn, S. Schirra, and S. Schmitt. A separation bound for real algebraic expressions. In *Proc. Europ. Symp. Algor.*, volume 2161 of *LNCS*, pages 254–265, Berlin, 2001. Springer.

[41] Christoph Burnikel, Stefan Funke, Kurt Mehlhorn, Stefan Schirra, and Susanne Schmitt. A separation bound for real algebraic expressions. In Friedhelm Meyer auf der Heide, editor, *Proc. 9th European Symposium on Algorithms*, volume 2161 of *Lecture Notes Comput. Sci.*, pages 254–265, 2001.

[42] Christoph Burnikel, Stefan Funke, Kurt Mehlhorn, Stefan Schirra, and Susanne Schmitt. A separation bound for real algebraic expressions. Technical Report ECG-TR-123101-02, MPI Saarbrücken, 2002.

[43] Laurent Busé, Houssam Khalil, and Bernard Mourrain. Resultant-based methods for plane curves intersection problems. In Victor G. Ganzha, Ernst W. Mayr, and Evgenii V. Vorozhtsov, editors, *Proc 8th Int. Workshop Computer Algebra in Scientific Computing*, volume 3718 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2005.

[44] J. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. ACM Symp. Theory of Computing*, pages 460–467, 1988.

[45] J. Canny. Improved algorithms for sign determination and existential quantifier elimination. *The Computer Journal*, 36(5):409–418, 1993.

[46] J. Canny. *The Complexity of Robot Motion Planning*. ACM – MIT Press Doctoral Dissertation Award Series. MIT Press, Cambridge, MA, 1987. ISBN 0-262-03136-1.

[47] D. Cantor, P. Galyean, and H. Zimmer. A continued fraction algorithm for real algebraic numbers. *Mathematics of Computation*, 26(119):785–791, July 1972. ISSN 0025-5718.

[48] D. G. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 36(154):587–592, 1981.

[49] J.P. Cardinal. On two iterative methods for approximating the roots of a polynomial. In J. Renegar, M. Shub, and S. Smale, editors, *The Mathematics of Numerical Analysis*, volume 32 of *Lectures in Applied Math*. AMS, 1996.

[50] CGAL. CGAL: Computational geometry algorithms library. www.cgal.org.

[51] H. Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate text in mathematics*. Springer, 1996.

[52] G. Collins and A. Akritas. Polynomial real root isolation using Descartes' rule of signs. In *SYMSAC '76*, pages 272–275, New York, USA, 1976. ACM Press.

[53] G. Collins and J. Johnson. Quantifier elimination and the sign variation method for real root isolation. In *ISSAC*, pages 264–271, 1989.

[54] G.E. Collins. Subresultants and reduced polynomial remainder sequences. *J. ACM*, 14: 128–142, 1967.

[55] G.E. Collins and R. Loos. Real zeros of polynomials. In B. Buchberger, G.E. Collins, and R. Loos, editors, *Computer Algebra: Symbolic and Algebraic Computation*, pages 83–94. Springer-Verlag, Wien, 2nd edition, 1982.

[56] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms*. MIT Press, Cambridge, MA, 2nd edition, 2001.

[57] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein. *Introduction to Algorithms*. MIT Press, 2nd edition, 2001.

[58] M. Coste and M. F. Roy. Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. *J. Symb. Comput.*, 5(1/2):121–129, 1988.

[59] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition, 1997.

[60] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Number 185 in GTM. Springer, New York, 2nd edition, 2005.

[61] J. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symbolic Computation*, 31(1/2):71–87, 2001.

[62] J. E. Cremona. Reduction of binary cubic and quartic forms. *LMS J. Computation and Mathematics*, 2:62–92, 1999.

[63] F. Cucker, H. Lanneau, B. Mishra, P. Pedersen, and M-F. Roy. NC Algorithms for Real Algebraic Numbers. *Appl. Algebra Eng. Commun. Comput.*, 3:79–98, 1992.

[64] A. Díaz, I. Z. Emiris, E. Kaltofen, and V.Y. Pan. Algebraic algorithms. In M.J. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 16. CRC Press, Boca Raton, Florida, 1999.

[65] J. H. Davenport. Cylindrical algebraic decomposition. Technical Report 88–10, School of Mathematical Sciences, University of Bath, England, available at: http://www.bath.ac.uk/masjhd/, 1988.

[66] J.H. Davenport, Y. Siret, and E. Tournier. *Computer Algebra*. Academic Press, London, 1988.

[67] Mark de Berg, Marc van Kreveld, Mark Overmars, and Otfried Schwarzkopf. *Computational Geometry: Algorithms and Applications*. Springer-Verlag, Berlin, Germany, 2nd edition, 2000.

[68] J-P. Dedieu and J-C. Yakoubsohn. Computing the real roots of a polynomial by the exclusion algorithm. *Numerical Algorithms*, 4(I–II):1–24, 1993.

[69] Olivier Devillers, Alexandra Fronville, Bernard Mourrain, and Monique Teillaud. Algebraic methods and arithmetic filtering for exact predicates on circle arcs. In *Proc. 16th Annu. ACM Sympos. Comput. Geom.*, pages 139–147, 2000.

[70] Olivier Devillers, Alexandra Fronville, Bernard Mourrain, and Monique Teillaud. Algebraic methods and arithmetic filtering for exact predicates on circle arcs. *Comput. Geom. Theory Appl.*, 22:119–142, 2002.

[71] A. Díaz, E. Kaltofen, and V. Pan. Algebraic algorithms. In A. B. Tucker, editor, *The Computer Science and Engineering Handbook*, chapter 10, pages 226–248. CRC Press, Boca Raton, Florida, 1997.

[72] A. Dickenstein and I. Z. Emiris. Multihomogeneous resultant matrices. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 46–54, Lille, France, 2002. ACM Press. Distinguished Paper Award.

[73] A. Dickenstein and I. Z. Emiris. Multihomogeneous resultant formulae by means of complexes. *J. Symbolic Computation*, 36(3-4):317–342, 2003.

[74] A. Dickenstein and I. Z. Emiris, editors. *Solving Polynomial Equations: Foundations, Algorithms and Applications*, volume 14 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, May 2005.

[75] G. Dos Reis, B. Mourrain, R. Rouillier, and P. Trébuchet. An environment for symbolic and numeric computation. In *Proc. Int. Conf. Math. Software*, World Scientific, pages 239–249, 2002.

[76] Z. Du, V. Sharma, and C. K. Yap. Amortized bound for root isolation via Sturm sequences. In D. Wang and L. Zhi, editors, *Int. Workshop on Symbolic Numeric Computing*, pages 81–93, School of Science, Beihang University, Beijing, China, 2005.

[77] L. Ducos. Optimizations of the subresultant algorithm. *J. Pure & Applied Algebra*, 145 (2):149–163, 2000.

[78] W. Dunham. *The mathematical universe: an alphabetical journey through great proofs, problems and personalities*. Wiley and Sons, Inc, New York, 1994.

[79] Laurent Dupont, Daniel Lazard, Sylvain Lazard, and Sylvain Petitjean. Near-optimal parameterization of the intersection of quadrics. In *Proc. Annual ACM Symp. on Comp. Geometry*, pages 246–255. ACM, June 2003.

[80] A. Eigenwillig, L. Kettner, W. Krandick, K. Mehlhorn, S. Schmitt, and N. Wolpert. A Descartes Algorithm for Polynomials with Bit-Stream Coefficients. In V. Ganzha, E. Mayr, and E. Vorozhtsov, editors, *CASC*, volume 3718 of *LNCS*, pages 138–149. Springer, 2005. ISBN 3-540-28966-6.

[81] A. Eigenwillig, V. Sharma, and C. K. Yap. Almost tight recursion tree bounds for the descartes method. In *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, pages 71–78, New York, NY, USA, 2006. ACM Press. ISBN 1-59593-276-3.

[82] Arno Eigenwillig, Lutz Kettner, Elmar Schömer, and Nicola Wolpert. Complete, exact, and efficient computations with cubic curves. In *Symposium on Computational Geometry*, pages 409–418, 2004.

[83] M. El Kahoui. An elementary approach to subresultants theory. *J. Symb. Comput.*, 35 (3):281–292, 2003.

[84] I. Z. Emiris. A general solver based on sparse resultants, March 1995. Available also as Tech. Report 3110, INRIA Sophia-Antipolis, Jan. 1997.

[85] I. Z. Emiris and M.I. Karavelas. The predicates of the Apollonius diagram: algorithmic analysis and implementation. *Comp. Geom.: Theory & Appl., Spec. Issue on Robust Geometric Algorithms and their Implementations*, 33(1-2):18–57, 2006.

[86] I. Z. Emiris and B. Mourrain. Matrices in elimination theory. *J. Symbolic Computation, Special Issue on Elimination*, 28:3–44, 1999.

[87] I. Z. Emiris and E. P. Tsigaridas. Real solving of bivariate polynomial systems. In V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov, editors, *In Proc. Computer Algebra in Scientific Computing (CASC)*, LNCS, pages 150–161. Springer Verlag, 2005.

[88] I. Z. Emiris and E. P. Tsigaridas. Real algebraic numbers and polynomial systems of small degree. submitted for journal publication, June 2005.

[89] I. Z. Emiris and E. P. Tsigaridas. Minkowski decomposition of convex lattice polygons. In M. Elkadi, B. Mourrain, and R. Piene, editors, *Algebraic geometry and geometric modeling*, pages 207–224. Springer, 2005.

[90] I. Z. Emiris and E. P. Tsigaridas. Computations with real algebraic numbers of degree up to 4. In *Proc. ICPSS (in honor of D. Lazard)*, pages 64–66, Paris, 2004.

[91] I. Z. Emiris and E. P. Tsigaridas. Computations with one and two algebraic numbers. Technical report, ArXiv, Dec 2005. URL `www.arxiv.org/abs/cs.SC/0512072`.

[92] I. Z. Emiris and E. P. Tsigaridas. Computing with real algebraic numbers of small degree. In S. Albers and T. Radzik, editors, *Proc. ESA*, volume 3221 of *LNCS*, pages 652–663. Springer Verlag, 2004.

[93] I. Z. Emiris and E. P. Tsigaridas. Computations with real algebraic numbers of degree up to 4. In *ICPSS (in honor of D. Lazard)*, pages 64–66, Paris, 2004.

[94] I. Z. Emiris and G. M. Tzoumas. Algebraic study of the apollonius circle of three ellipses. In *Proc. European Workshop Computat. Geometry*, pages 147–150, Eindhoven, Holland, March 2005.

[95] I. Z. Emiris and J. Verschelde. How to count efficiently all affine roots of a polynomial system. *Discrete Applied Math., Special Issue on Comput. Geom.*, 93(1):21–32, 1999.

[96] I. Z. Emiris, A. Kakargias, S. Pion, M. Teillaud, and E. P. Tsigaridas. Towards an open curved kernel. In *Proc. Annual ACM Symp. on Computational Geometry*, pages 438–446, New York, 2004. ACM Press.

[97] I. Z. Emiris, B. Mourrain, and E. P. Tsigaridas. Real Algebraic Numbers: Complexity Analysis and Experimentation. In P. Hertling, C. Hoffmann, W. Luther, and N. Revol, editors, *Reliable Implementations of Real Number Algorithms: Theory and Practice*, LNCS (to appear). Springer Verlag, 2006. also available in www.inria.fr/rrrt/rr-5897.html.

[98] I. Z. Emiris, E. P. Tsigaridas, and G. M. Tzoumas. The InCircle predicates for ellipses. In *In Proc. European Workshop Computat. Geometry*, pages 225–228, Delphi, Greece, 2006.

[99] I. Z. Emiris, E. P. Tsigaridas, and G. M. Tzoumas. The predicates for the Voronoi diagram of ellipses. In *Proc. 22th Annual ACM Symp. on Computational Geometry*, pages 227–236, Sedona, USA, 2006.

[100] Jeff Erickson. Lower bounds for satisfiability problems. *Chicago J. of Theoretical Computer Science*, 8, 1999.

[101] F. Etayo, L. Gonzalez-Vega, and N. del Rio. A new approach to characterizing the relative position of two ellipses depending on one parameter. *Comp.-Aided Geom. Design*, 2005. (to appear).

[102] G. Farin. *Curves and Surfaces for Computer Aided Geometric Design*. Academic Press, Boston, 1988.

[103] G. Farin, J. Hoschek, and M-S. Kim, editors. *Handbook of Computer Aided Geometric Design*. Elsevier, 2002.

[104] R. T. Farouki and V. T. Rajan. Algorithms for polynomials in Bernstein form. Report ??, Manufacturing Res. Dept., IBM T. J. Watson Res. Center, Yorktown Heights, NY, 1987.

[105] Efi Fogel, Dan Halperin, Lutz Kettner, Monique Teillaud, Ron Wein, and Nicola Wolpert. Arrangements. In Jean-Daniel Boissonnat and Monique Teillaud, editors, *Effective Computational Geometry for Curves and Surfaces*, volume (to appear) of *Mathematics and Visualization*, chapter 1. Springer, 2006.

[106] Efraim Fogel, Dan Halperin, Ron Wein, Sylvain Pion, Monique Teillaud, Ioannis Emiris, Athanasios Kakargias, Elias Tsigaridas, Eric Berberich, Arno Eigenwillig, Michael Hemmer, Lutz Kettner, Kurt Mehlhorn, Elmar Schomer, and Nicola Wolpert. An empirical comparison of software for constructing arrangements of curved arcs (preliminary version). Technical Report ECG-TR-361200-01, Tel-Aviv University, INRIA Sophia-Antipolis, MPI Saarbrücken, 2004.

[107] J.-B. Fourier. Analyse des Équations Détermines. *Didot, Paris*, 1831.

[108] J. Fraleigh. *A First Course in Abstract Algebra*. Addison-Wesley, 4 edition, 1989.

[109] Anka Gajentaan and Mark H. Overmars. On a class of $O(n^2)$ problems in computational geometry. *Computational Geometry*, 5(3):165–185, October 1995.

[110] S. Gao and A. Lauder. Fast absolute irreducibility testing via Newton polytopes. *preprint*, 2004.

[111] S. Gao and A. Lauder. Decomposition of polytopes and polynomials. *Discrete and Computational Geometry*, 26:89–104, 2001.

[112] K. Geddes, S. Czapor, and G. Labahn. *Algorithms of Computer Algebra*. Kluwer Academic Publishers, Boston, 1992.

[113] N. Geismann, M. Hemmer, and E. Schömer. Computing a 3-dimensional cell in an arrangement of quadrics: Exactly and actually! In *Proc. 17th Annu. ACM Sympos. Comput. Geom.*, pages 264–273, 2001.

[114] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser, Boston, 1994.

[115] R. Goldman. *Pyramid Algorihtms: A dynamic approach to curves and surfaces for geometric modelling*. Morgan Kaufmann, 2002.

[116] L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *J. Complexity*, 12(4):527–544, 1996.

[117] L. Gonzalez-Vega and I. Necula. Efficient topology determination of implicitly defined algebraic plane curves. *Computer Aided Geometric Design*, 19(9):719–743, December 2002.

[118] L. González-Vega, H. Lombardi, T. Recio, and M-F. Roy. Sturm-Habicht Sequence. In *ISSAC*, pages 136–146, 1989.

[119] L. González-Vega, H. Lombardi, T. Recio, and M-F. Roy. Spécialisation de la suite de Sturm et sous-résulants. *ITA*, 24:561–, 1990.

[120] L. Gonzalez-Vega, H. Lombardi, T. Recio, and M.-F. Roy. Determinants and real roots of univariate polynomials. In *Proc. 25 Years of Quantifier Elimination and Cylindrical Algebraic Decomposition, Linz, Oct. 1993*, Texts and Monographs in Symbolic Computation. Springer-Verlag, 1995.

[121] J. E Goodman and J. O' Rourke. *Handbook of computational geometry*. Elsevier science, Amsterdam, 1995.

[122] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics*. Addison-Wesley, second edition, 1994. ISBN 0-201-55802-5.

[123] L.J. Guibas, M.I. Karavelas, and D. Russel. A computational framework for handling motion. In *Proc. 6th Workshop Algor. Engin. & Experim. (ALENEX)*, pages 129–141, Jan 2004.

[124] L. Habert. Computing bitangents for ellipses. In *Proc. 17th Canad. Conf. Comp. Geom.*, pages 294–297, 2005.

[125] W. Habicht. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. *Comment. Math. Helv.*, 21:99–116, 1948.

[126] D. Halperin. Arrangements. In Jacob E. Goodman and Joseph O'Rourke, editors, *Handbook of Discrete and Computational Geometry*, chapter 21, pages 389–412. CRC Press LLC, Boca Raton, FL, 1997.

[127] I. Hanniel, R. Muthuganapathy, G. Elber, and M.-S. Kim. Precise Voronoi cell extraction of free-form rational planar closed curves. In *Proc. 2005 ACM Symp. Solid and phys. modeling*, pages 51–59, Cambridge, Massachusetts, 2005.

[128] P. Harrington, C.O. Dúnlaing, and C. Yap. Optimal Voronoi diagram construction with n convex sites in three dimensions. Tech. Rep. TCDMATH 04-21, School of Mathematics, Dublin, 2004.

[129] L. E. Heindel. Integer arithmetic algorithms for polynomial real zero determination. *Journal of the Association for Computing Machinery*, 18(4):533–548, October 1971.

[130] M. Hemmer, E. Schömer, and N. Wolpert. Computing a 3-dimensional cell in an arrangement of quadrics: Exactly and actually! In *Proc. Annual ACM Symp. Comput. Geometry*, pages 264–273, 2001.

[131] P. Henrici. *Applied and computational complex analysis*. John Wiley & Sons, New York, NY, 1977.

[132] D. Hensley. The largest digit in the continued fraction expansion of a rational number. *Pacific Journal of Mathematics*, 151(2):237–255, 1991.

[133] Chung-Jen Ho and Chee Keng Yap. The Habicht approach to subresultants. *Journal of Symbolic Computation*, 21(1):1–14, January 1996.

[134] H. Hong. Quantifier elimination for formulas constrained by quadratic equations. In *ISSAC*, pages 264–274, 1993.

[135] E. Horowitz and S. Shani. Computing partitions with applications to the knapsack problem. *Journal of ACM*, 21(2):277–292, April 1974.

[136] X Hou and D. Wang. Subresultants with the Bézout Matrix . In X. S. Gao and D. Wang, editors, *Fourth Asian Symposium in Computer Mathematics (ASCM 2000)*, pages 19–28, Singapore New Jersey, 2000. World Scientific.

[137] O. Ibarra and C. Kim. Fast approximation algorithms for the knapsack and sum of subset problems. *J. ACM*, 22(4):463–468, 1975.

[138] C. G. J. Jacobi. De eliminatione variabilis e duabus aequationibus algebraicis. *J. Reine Angew. Math*, 15:101–124, 1836.

[139] J. Johnson. Algorithms for polynomial real root isolation. In B. Cavinsess and J. Johnson, editors, *Quantifier elimination and cylindrical algebraic decomposition*, pages 269–299. Springer, 1998.

[140] J. R. Johnson. Real algebraic number computation using interval arithmetic. In *ISSAC '92: Papers from the international symposium on Symbolic and algebraic computation*, pages 195–205, New York, NY, USA, 1992. ACM Press. ISBN 0-89791-489-9.

[141] A. Kakargias. Arrangements of Conic Arcs. Master's thesis, Department of Informatics and Telecommunications, National Kapodistrian University of Athens, 2004.

[142] Athanasios V. Kakargias and Sylvain Pion. Experimenting with the curved kernel. Technical Report ECG-TR-302206-02, INRIA Sophia-Antipolis, MPI Saarbrücken, 2003.

[143] Erich Kaltofen. Challenges of symbolic computation: My favorite open problems. *J. Symb. Comput.*, 29(6):891–919, 2000.

[144] D. Kaplan and J. White. Polynomial equations and circulant matrices. *The Mathematical Association of America (Monthly)*, 108:821–840, November 2001.

[145] V. Karamcheti, C. Li, I. Pechtchanski, and C. Yap. *The CORE Library Project*, 1.2 edition, 1999. URL `http://www.cs.nyu.edu/exact/core`.

[146] V. Karamcheti, C. Li, I. Pechtchanski, and C. Yap. A Core Library For Robust Numeric and Geometric Computation. In *Proc. 15th Annual ACM Symp. on Comp. Geometry*, pages 351–359, 1999.

[147] M. Karavelas. Voronoi diagrams in CGA. In I. Emiris, M. Karavelas, and L. Palios, editors, *22nd European Workshop on Computational Geometry (EWCG06)*, pages 229–232, Delphi, Greece, 2006.

[148] Menelaos I. Karavelas and Ioannis Z. Emiris. Root comparison techniques applied to computing the additively weighted Voronoi diagram. In *Proc. 14th ACM-SIAM Sympos. Discrete Algorithms (SODA)*, pages 320–329, 2003.

[149] M.I. Karavelas and I. Z. Emiris. Root comparison techniques applied to the planar additively weighted Voronoi diagram. In *Proc. SODA*, pages 320–329, January 2003.

[150] M.I. Karavelas and M. Yvinec. Voronoi diagram of convex objects in the plane. In *Proc. ESA*, pages 337–348, 2003.

[151] H. Kellerer, R. Mansini, U. Pferschy, and M. Speranza. An efficient fully polynomial approximation scheme for the subset-sum problem. *J. Comput. Syst. Sci.*, 66(2):349–370, 2003.

[152] J. Keyser, T. Culver, D. Manocha, and S. Krishnan. ESOLID: A system for exact boundary evaluation. *Comp. Aided Design*, 36(2):175–193, 2004.

[153] J. Keyser, K. Ouchi, and M. Rojas. The Exact Rational Univariate Representation for Detecting Degeneracies. In *DIMACS: Series in Discrete Mathematics and Theoretical Computer Science*. AMS Press, 2004. to appear.

[154] A. Khetan. The resultant of an unmixed bivariate system. *J. Symb. Comput.*, 36:425–442, 2003.

[155] A. Khintchine. *Continued Fractions*. University of Chicago Press, Chicago, 1964.

[156] D.-S. Kim, D. Kim, and K. Sugihara. Voronoi diagram of a circle set from Voronoi diagram of a point set: II. Geometry. *CAGD*, 18:563–585, 2001.

[157] J. Kioustelidis. Bounds for the positive roots of polynomials. *Journal of Computational and Applied Mathematics*, 16:241–244, 1986.

[158] R. Klein, K. Mehlhorn, and S. Meiser. Randomised incremental construction of abstract Voronoi diagrams. *Comput. Geom. Theory & Appl.*, 3(3):157–184, 1993.

[159] J. Klose. Binary segmentation for multivariate polynomials. *J. Complexity*, 11(3):330–343, 1995.

[160] D. E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, 3rd edition, 1998.

[161] D. E. Knuth. *Sorting and Searching*, volume 3 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, 1973.

[162] W. Krandick. Isolierung reeller nullstellen von polynomen. In J. Herzberger, editor, *Wissenschaftliches Rechnen*, pages 105–154. Akademie-Verlag, Berlin, 1995.

[163] W. Krandick and K. Mehlhorn. New bounds for the Descartes method. *JSC*, 41(1):49–66, Jan 2006.

[164] R. Krasauskas. Toric surface patches: Advances in geometrical algorithms and representations. *Adv. Comput. Math.*, 17(1-2):89–113, 2002.

[165] R. Krasauskas and R. Goldman. Toric Bezier Patches with Depth. In R. Goldman and R. Krasauskas, editors, *Topics in Geometric Modeling and Algebraic Geometry*, volume 334, pages 65–91. AMS Mathematics of Computation, 2003.

[166] L. Kronecker. Über den zahlbergriff. *Crelle J. reine und angew. Mathematik*, 101:337–395, 1887.

[167] J. L. Lagrange. Traité de la résolution des équations numériques. *Paris (n.p.)*, 1798.

[168] Y.N. Lakshman and D. Lazard. On the complexity of zero-dimensional algebraic systems. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 217–225, Boston, 1991. Birkhäuser. (Proc. MEGA '90, Livorno, Italy).

[169] J. M. Lane and R. F. Riesenfeld. Bounds on a polynomial. *BIT*, 21:112–117, 1981.

[170] Daniel Lazard. Quantifier elimination: optimal solution for two classical examples. *J. Symb. Comput.*, 5(1-2):261–266, 1988. ISSN 0747-7171.

[171] L. Lazard, S.and Peñaranda and S. Petitjean. Intersecting quadrics: an efficient and exact implementation. In *Symposium of Computational Geometry*, pages 419–428, 2004.

[172] Chen Li and Chee Yap. A new constructive root bound for algebraic expressions. In *12th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, January 2001.

[173] Chen Li, Sylvain Pion, and Chee Yap. Recent progress in exact geometric computation. *J. of Logic and Algebraic Programming*, 64(1):85–111, 2004. Special issue on "Practical Development of Exact Real Number Computation".

[174] T. Lickteig and M.-F. Roy. Semi-algebraic complexity of quotients and sign determination of remainders. *J. Complexity*, 12(4):545–571, December 1996.

[175] T. Lickteig and M-F. Roy. Sylvester-Habicht Sequences and Fast Cauchy Index Computation. *J. Symb. Comput.*, 31(3):315–341, 2001.

[176] H. Lombardi, M-F. Roy, and M. Safey El Din. New Structure Theorem for Subresultants. *J. Symb. Comput.*, 29(4-5):663–689, 2000.

[177] R. Loos. Computing in algebraic extensions. In B. Buchberger, G. E. Collins, R. Loos, and R. Albrecht, editors, *Computer Algebra: Symbolic and Algebraic Computation*, pages 173–187. Springer-Verlag, 1983.

[178] R. Loos. Generalized polynomial remainder sequences. In B. Buchberger, G. E. Collins, R. Loos, and R. Albrecht, editors, *Computer Algebra: Symbolic and Algebraic Computation*, pages 115–137. Springer-Verlag, Wien, 1983.

[179] Rüdiger Loos and Volker Weispfenning. Applying linear quantifier elimination. *The Computer Journal*, 36(5):450–462, 1993.

[180] K. Mahler. An application of jensen's formulae to polynomials. *Mathematica*, 7:98–100, 1960.

[181] M. Marden. Geometry of polynomials. In *AMS Surveys*. American Mathematical Society, second edition, 1966.

[182] M. McAllister, D. Kirkpatrick, and J. Snoeyink. A compact piecewise-linear Voronoi diagram for convex sites in the plane. *Discrete Comput. Geom.*, 15:73–105, 1996.

[183] John Michael McNamee. A 2002 update of the supplementary bibliography on roots of polynomials. *J. Comput. Appl. Math.*, 142(2):433–434, 2002.

[184] John Michael McNamee. A bibliography on roots of polynomials. *J. Comput. Appl. Math.*, 47(3):391–394, 1993.

[185] John Michael McNamee. An updated supplementary bibliography on roots of polynomials. *J. Comput. Appl. Math.*, 110(2):305–306, 1999. ISSN 0377-0427.

[186] K. Mehlhorn and S. Näher. *LEDA: A Platform for Combinatorial and Geometric Computing*. Cambridge University Press, Cambridge, UK, 2000.

[187] M. Mignotte. *Mathematics for computer algebra*. Springer-Verlag, New York, 1991.

[188] M. Mignotte. An inequality about factors of polynomials. *Math. of Comp.*, 28:1153–1157, 1974.

[189] M. Mignotte. Some useful bounds. In B. Buchberger, G.E. Collins, and R. Loos, editors, *Computer Algebra: Symbolic and Algebraic Computation*, pages 259–263. Springer-Verlag, Wien, 2nd edition, 1982.

[190] M. Mignotte and D. Stefanescu. *Polynomials: An algorithmic approach*. Springer, 1999.

[191] Maurice Mignotte. On the Distance Between the Roots of a Polynomial. *Appl. Algebra Eng. Commun. Comput.*, 6(6):327–332, 1995.

[192] G. Milovanovic and T. Rassias. Inequalities for polynomial zeros. In T. Rassias, editor, *Survey on Classical Inequalities*, volume 517 of *Mathematics and its Applications*, pages 165–202. Kluwer, 2000.

[193] B. Mishra. *Algorithmic Algebra*. Springer-Verlag, New York, 1993.

[194] B. Mishra and P. Pedersen. Arithmetic with real algebraic numbers is in NC. In *ISSAC '90: Proceedings of the international symposium on Symbolic and algebraic computation*, pages 120–126, New York, NY, USA, 1990. ACM Press. ISBN 0-201-54892-5.

[195] M. Moreno Maza and R. Rioboo. Polynomial gcd computations over towers of algebraic extensions. In *AAECC-11*, pages 365–382. Springer, 1995.

[196] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[197] B. Mourrain. Enumeration problems in geometry, robotics and vision. In L. Gonzalez-Vega and T. Recio, editors, *Effective Methods in Algebraic Geometry*, Progress in Mathematics. Birkhäuser, 1996. (Proc. MEGA '94, Santander, Spain).

[198] B. Mourrain. A new criterion for normal form algorithms. In M. Fossorier, H. Imai, Shu Lin, and A. Poli, editors, *Proc. AAECC*, volume 1719 of *LNCS*, pages 430–443, 1999.

[199] B. Mourrain and V.Y. Pan. Solving special polynomial systems by using structured matrices and algebraic residues. In F. Cucker and M. Shub, editors, *Proc. Workshop on Foundations of Computational Mathematics*, pages 287–304, Berlin, 1997. Springer-Verlag.

[200] B. Mourrain and V.Y. Pan. Asymptotic acceleration of solving polynomial systems. In *Proc. ACM Symp. Theory of Computing*, pages 488–496. ACM Press, New York, 1998.

[201] B. Mourrain and P. Trébuchet. A new approach to normal form algorithms. *J. Symbolic Computation*, 2001. submitted.

[202] B. Mourrain and Ph. Trébuchet. Algebraic methods for numerical solving. In *Proc. of the 3rd International Workshop on Symbolic and Numeric Algorithms for Scientific Computing'01 (Timisoara, Romania)*, pages 42–57, 2002.

[203] B. Mourrain, M. Vrahatis, and J.C. Yakoubsohn. On the complexity of isolating real roots and computing with certainty the topological degree. *J. Complexity*, 18(2), 2002.

[204] B. Mourrain, J. P. Pavone, P. Trébuchet, and E. Tsigaridas. SYNAPS, a library for symbolic-numeric computation. In *8th Int. Symposium on Effective Methods in Algebraic Geometry, MEGA*, Sardinia, Italy, May 2005. Software presentation.

[205] B. Mourrain, F. Rouillier, and M.-F. Roy. *Bernstein's basis and real root isolation*, pages 459–478. Mathematical Sciences Research Institute Publications. Cambridge University Press, 2005.

[206] B. Mourrain, S. Pion, S. Schmitt, J.-P. Técourt, E. P. Tsigaridas, and N. Wolpert. Algebraic issues in Computational Geometry. In J.-D. Boissonnat and M. Teillaud, editors, *Effective Computational Geometry for Curves and Surfaces*, volume (to appear) of *Mathematics and Visualization*, chapter 3. Springer, 2006.

[207] N. Obreschkoff. Sur les zéros réelles des polynómes. *Mathematica*, 10:132–136, 1935.

[208] A. M. Ostrowski. "Uber die Bedeutung der Theorie der konvexen Polyeder für die formale Algebra. *Jahresberichte Deutsche Marth. Verein*, 30:98–99, 1921.

[209] A.M. Ostrowski. *Solution of Equations and Systems of Equations*. Pure and Applied Mathematics. Academic Press, New York, 2nd edition, 1966.

[210] V. Pan. Solving polynomial equation: Some history and recent progress. *SIAM Review*, 39:187–220, 1997.

[211] V. Pan. Solving polynomials with computers. *American Scientist*, 86:62–69, Jan-Feb 1998.

[212] Victor Pan. The bit-complexity of arithmetic algorithms. *Journal of Algorithms*, 2(2): 144–163, June 1981.

[213] V.Y. Pan. Univariate polynomials: Nearly optimal algorithms for factorization and rootfinding. In *Proc. ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 253–267, 2001.

[214] V.Y. Pan. Univariate polynomials: Nearly optimal algorithms for numerical factorization and rootfinding. *J. Symbolic Computation*, 33(5):701–733, 2002.

[215] G. Pick. Geometrisches zur zahlentheorie. *Sitzenber*, 19:311–319, 1899.

[216] Sylvain Pion and Chee K. Yap. Constructive root bound for k-ary rational input numbers. In *Proc. 19th Annu. ACM Sympos. Comput. Geom.*, pages 256–263, 2003.

[217] D. Pisinger. *Algorithms for the Knapsack problems*. PhD thesis, Department of Computer Science, University of Kopehagen, February 1995.

[218] V. Prasolov. *Polynomials*, volume 11 of *Algorithms and computations in mathematics*. Springer Verlag, 2004. Translated form the Russian by Dimitry Leites.

[219] F. P. Preparata and M. I. Shamos. *Computational Geometry: An Introduction*. Springer-Verlag, 3rd edition, October 1990. ISBN 3-540-96131-3.

[220] S. Rabinowitz. A census of convex lattice polygons with at most one interior lattice point. *Ars Combinatorica*, 28:83–96, 1989.

[221] A. Ralston and P. Rabinowitz. *A first cource in numerical analysis*. Mathematics series. McGraw-Hill, 9th edition, 1988.

[222] D. Reischert. Asymptotically fast computation of subresultants. In *ISSAC*, pages 233–240, 1997.

[223] J. Renegar. On the worst-case arithmetic complexity of approximating zeros of systems of polynomials. *SIAM J. Computing*, 18:350–370, 1989.

[224] R. Richtmyer, M. Devaney, and N. Metropolis. Continued fraction expansions of algebraic numbers. *Mumerische Mathematik*, 4:68–64, 1962.

[225] R. Rioboo. Towards faster real algebraic numbers. *J. Symb. Comput.*, 36(3-4):513–533, 2003.

[226] Renaud Rioboo. Real algebraic closure of an ordered field: implementation in axiom. In *Proc. Annual ACM ISSAC*, pages 206–215. ACM Press, 1992. ISBN 0-89791-489-9.

[227] Renaud Rioboo. Towards faster real algebraic numbers. In Teo Mora, editor, *Proc. Annual ACM ISSAC*, pages 221–228, New York, NY 10036, USA, 2002. ACM Press. ISBN 1-58113-484-3.

[228] D. Rosen and J. Shallit. A continued fraction algorithm for approximating all real polynomial roots. *Math. Mag*, 51:112–116, 1978.

[229] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Journal of Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[230] F. Rouillier and Z. Zimmermann. Efficient isolation of polynomial's real roots. *J. of Computational and Applied Mathematics*, 162(1):33–50, 2004.

[231] M-F. Roy and A. Szpirglas. Complexity of the Computation on Real Algebraic Numbers. *J. Symb. Comput.*, 10(1):39–52, 1990.

[232] S. Rump. On the sign of a real algebraic number. In *SYMSAC '76: Proceedings of the third ACM symposium on Symbolic and algebraic computation*, pages 238–241, New York, NY, USA, 1976. ACM Press.

[233] S. M. Rump. Ten methods to bound multiple roots of polynomials. *J. Comput. Appl. Math.*, 156(2):403–432, 2003. ISSN 0377-0427.

[234] T. Sakkalis. Signs of algebraic numbers. *Computers and Mathematics*, pages 131–134, 1989.

[235] T. Sakkalis and R. Farouki. Singular points of algebraic curves. *J. Symb. Comput.*, 9 (4):405–421, 1990.

[236] G. Salmon. *Modern Higher Algebra*. G.E. Stechert and Co., New York, 1885. Reprinted 1924.

[237] J. Schicho. Simplification of surface parametrizations - a lattice polygon approach. *J of Symbolic Computation*, 36:535–554, 2003.

[238] G. Schmeisser. Cauchy polynomials. submitted to "Some Recent Advances in the Theory of Polynomials and Their Applications", available at www.mi.uni-erlangen.de/∼schmeis/publiste/, 2005.

[239] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. Manuscript. Univ. of Tübingen, Germany, 1982.

[240] Arnold Schönhage. Asymptotically fast algorithms for the numerical multiplication and division of polynomials with complex coeficients. In Jacques Calmet, editor, *EUROCAM*, volume 144 of *LNCS*, pages 3–15, 1982.

[241] J. Schwartz and M. Sharir. On the piano movers problem. II general techniques for computing topological properties of real algebraic manifolds. *Advances in applied mathematics*, 4:298–351, 1983.

[242] T. W. Sederberg and Geng-Zhe Chang. Isolating the real roots of polynomials using isolator polynomials. In C. Bajaj, editor, *Algebraic Geometry and Applications*. Springer, 1993.

[243] M. Shaw and J. F. Traub. On the number of multiplications for the evaluation of a polynomial and some of its derivatives. *Journal of the ACM*, 21(1):161–167, January 1974.

[244] D. Stefanescu. New bounds for the positive roots of polynomials. *Journal of Universal Computer Science*, 11(12):2132–2141, 2005.

[245] D. Stefanescu. Inequalities on polynomial roots. *Mathematical Inequalities and Applications*, 5(3):335–347, 2002.

[246] H. Stetter. *Numerical polynomial algebra*. SIAM, 2004.

[247] V. Strassen. The computational complexity of continued fractions. In *SYMSAC '81: Proceedings of the fourth ACM symposium on Symbolic and algebraic computation*, pages 51–67, New York, NY, USA, 1981. ACM Press. ISBN 0-89791-047-8.

[248] C. Sturm. Mémoire sur la résolution des equations numériques. *Mém. Savants Étranger*, 6:271–318, 1835.

[249] B. Sturmfels. *Solving Systems of Polynomial Equations*. Number 97 in CBMS Regional Conference Series in Math. AMS, Providence, RI, 2002. ISBN 0-8218-3251-4.

[250] B. Sturmfels. *Algorithms in Invariant Theory*. RISC Series on Symbolic Computation. Springer Verlag, Vienna, 1993.

[251] B. Sturmfels. Introduction to resultants. In D.A. Cox and B. Sturmfels, editors, *Applications of Computational Algebr. Geometry, (San Diego, 1997)*, volume 53 of *Proc. Symp. Applied Math.*, pages 25–39. AMS, 1998.

[252] E. P. Tsigaridas and I. Z. Emiris. Univariate polynomial real root isolation: Continued fractions revisited. In Y. Azar and T. Erlebach, editors, *In Proc. 14th European Symposium of Algorithms (ESA)*, volume 4168 of *LNCS*, pages 817–828, Zurich, Switzerland, 2006. Springer Verlag.

[253] E. P. Tsigaridas and I. Z. Emiris. On the complexity of real root isolation using Continued Fractions. (submitted for journal publication), Sep 2006.

[254] G.M. Tzoumas. Predicates for computing the Apollonius diagram of ellipses. Master's thesis, Department of Informatics and Telecommunications, National University of Athens, May 2005.

[255] J. V. Uspensky. *Theory of Equations*. McGraw-Hill, 1948.

[256] A. van der Poorten. An introduction to continued fractions. In *Diophantine analysis*, pages 99–138. Cambridge University Press, 1986.

[257] A. van der Sluis. Upper bounds for the roots of polynomials. *Numerische Mathematik*, 15:250–262, 1970.

[258] B. van der Waerden. *Modern Algebra*. Ungar, 1953. Volumes 1-2.

[259] Todd L. Veldhuizen. Scientific computing: C++ versus Fortran: C++ has more than caught up. *Dr. Dobb's Journal of Software Tools*, 22(11):34, 36–38, 91, November 1997. ISSN 1044-789X. URL `http://extreme.indiana.edu/~tveldhui/papers/`.

[260] Todd L. Veldhuizen. Arrays in blitz++. In *Proceedings of the 2nd International Scientific Computing in Object-Oriented Parallel Environments (ISCOPE'98)*, Lecture Notes in Computer Science. Springer-Verlag, 1998.

[261] A. J. H. Vincent. Sur la résolution des équations numériques. *J. Math. Pures Appl.*, 1: 341–372, 1836.

[262] J. von zur Gathen and J. Gerhard. Fast Algorithms for Taylor Shifts and Certain Difference Equations. In *ISSAC*, pages 40–47, 1997.

[263] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge Univ. Press, Cambridge, U.K., 2nd edition, 2003.

[264] J. von zur Gathen and T. Lücking. Subresultants revisited. *Theor. Comput. Sci.*, 1-3 (297):199–239, 2003.

[265] W. Wang, J. Wang, and M. Kim. An algebraic condition for the separation of two ellipsoids. *Comp. Aided Geom. Design*, 18:531–539, 2001.

[266] Ron Wein. High-level filtering for arrangements of conic arcs. In *Proc. 10th European Symposium on Algorithms*, volume 2461 of *Lecture Notes Comput. Sci.*, pages 884–895, 2002.

[267] V. Weispfenning. Quantifier elimination for real algebra - the cubic case. In *ISSAC*, pages 258–263, 1994.

[268] V. Weispfenning. The complexity of linear problems in fields. *J. Symb. Comput.*, 5(1/2): 3–27, 1988.

[269] V. Weispfenning. A new approach to quantifier elimination for real algebra and geometry. In *Abstracts 9th European Workshop Comput. Geom.*, pages 31–35. FernUniversität Hagen, 1993.

[270] V. Weispfenning. Quantifier elimination for real algebra - the quadratic case and beyond. *Applicable Algebra in Engineering, Communication and Computing*, 8(2):85–101, 1997.

[271] G. Woeginger. Exact algorithms for NP-hard problems: A survey. In M. Juenger, G. Reinelt, and G. Rinaldi, editors, *Combinatorial Optimization - Eureka! You shrink!*, volume 2570, pages 185–207. LNCS, Springer, 2003.

[272] G. Woeginger. Open problems around exact algorithms. Manuscript, TU Eindhoven, 2004.

[273] L. Yang. Recent advances on determining the number of real roots of parametric polynomials. *J. Symbolic Computation*, 28:225–242, 1999.

[274] Chee Yap. On guaranteed accuracy computation. In Falai Chen and Dongming Wang, editors, *Geometric Computation*, chapter 12, pages 322–373. World Scientific Publishing Co., Singapore, 2004.

[275] C.K. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, New York, 2000.

[276] R. Zippel. *Effective Polynomial Computation*. Kluwer Academic Publishers, Boston, 1993.

[277] S. Zube. The n-sided toric patches and the A-resultants. *Computer Aided Geometric Design*, 17:695–714, 2000.