Quantum Algorithms inspired by Regev's reduction

André Chailloux

Inria de Paris

January 24 2026 - QIP'26 Tutorial Part II, Riga

In the previous episode

$$\boxed{\sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle|\mathbf{c}\rangle} \xrightarrow{\text{DP Solver}} \boxed{\sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle} \xrightarrow{H^{\otimes n}} \boxed{\sum_{\mathbf{y}\in\mathcal{C}^\perp} \widehat{f}(\mathbf{y})|\mathbf{y}\rangle} \Rightarrow \boxed{\text{SCP Solver}}$$

DP solver $\mathcal{A}_{Dec} : \mathbf{c}+\mathbf{e} \to \mathbf{c}$, used to construct the unitary

$$U_{Dec}|\mathbf{c}+\mathbf{e}\rangle|\mathbf{0}\rangle = |\mathbf{c}+\mathbf{e}\rangle|\mathbf{c}\rangle \quad \text{for } \mathbf{e} \leftarrow |f|^2.$$

It is used to perform the operation

$$\sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle|\mathbf{c}\rangle \to \sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle|\mathbf{0}\rangle.$$

Overkill?

- Let $|\Psi_{\mathbf{c}}\rangle = \sum_{\mathbf{e}\in\mathbb{F}_2^n} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle$. We want to the operation

$$\sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle|\mathbf{c}\rangle \to \sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle|\mathbf{0}\rangle.$$

- We rewrite as

$$\sum_{\mathbf{c}\in\mathcal{C}} |\Psi_{\mathbf{c}}\rangle|\mathbf{c}\rangle \to |\Psi_{\mathbf{c}}\rangle|\mathbf{0}\rangle.$$

- If we have a unitary $V : |\Psi_{\mathbf{c}}\rangle|\mathbf{0}\rangle \to |\Psi_{\mathbf{c}}\rangle|\mathbf{c}\rangle$ then $V^\dagger$ works.
- **Rewrite the reduction**

Definition (Decoding Problem $\mathrm{DP}(\mathcal{C}, p)$)

Input: Error distribution $p : \mathbb{F}_2^n \to [0, 1]$.
Sample: $\mathbf{c} \leftarrow \mathcal{C}$ and $\mathbf{e} \leftarrow p$.
Goal: Given $\mathbf{c} + \mathbf{e}$, recover $\mathbf{c}$.

Definition (Quantum Decoding Problem $\mathrm{QDP}(\mathcal{C}, f)$)

Input: Error function $f : \mathbb{F}_2^n \to \mathbb{C}$ with $\|f\|_2 = 1$.
Sample: $\mathbf{c} \leftarrow \mathcal{C}$.
Goal: Given $|\Psi_{\mathbf{c}}\rangle = \sum_{\mathbf{e} \in \mathbb{F}_2^n} f(\mathbf{e}) |\mathbf{c} + \mathbf{e}\rangle$, recover $\mathbf{c}$.

$\mathrm{QDP}(\mathcal{C}, f)$ is a problem with a **quantum state as input**. It is **easier** than $\mathrm{DP}(\mathcal{C}, |f|^2)$ (measure the input).
Case where $\sum_{\mathbf{e} \in \mathbb{F}_2^n} f(\mathbf{e}) = \bigotimes_{i=1}^n \sqrt{1-t}|0\rangle + \sqrt{t}|1\rangle$: $\mathbf{QDP}(\mathcal{C}, t)$.

$$\boxed{\sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle|\mathbf{c}\rangle} \xrightarrow[\text{Solver}]{\text{QDP}} \boxed{\sum_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{e}\in\mathbb{F}_2^n}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle} \xrightarrow{H^{\otimes n}} \boxed{\sum_{\mathbf{y}\in\mathcal{C}^\perp} \widehat{f}(\mathbf{y})|\mathbf{y}\rangle} \Rightarrow \boxed{\text{SCP Solver}}$$

We also have

Theorem (Informal)

For a random choice of $\mathcal{C}$ (i.e. of $\mathbf{G}$), if we have an efficient algorithm to solve $QDP(\mathcal{C}, t)$ then we have an efficient quantum algorithm to solve $SCP(\mathcal{C}^\perp, t^*)$ with $t^* = \frac{1}{2} - \sqrt{t(1-t)}$.

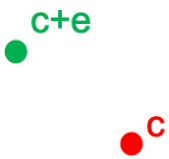
What is the complexity of $\mathbf{QDP}(\mathcal{C}, t)$?

How to reshape the error function with quantum information tools.

Wait, we're going to talk about Unambiguous State Discrimination now?

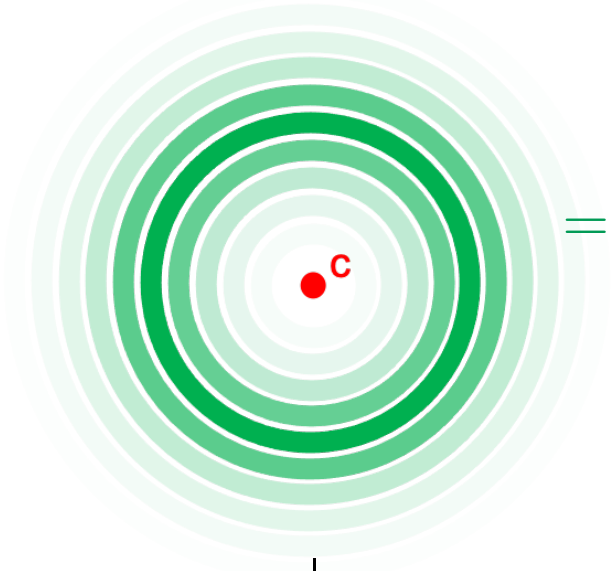
Difference between classical and quantum decoding problem

Classical decoding problem



Recover $\mathbf{c}$ from $\mathbf{c}+\mathbf{e}$.

Quantum decoding problem

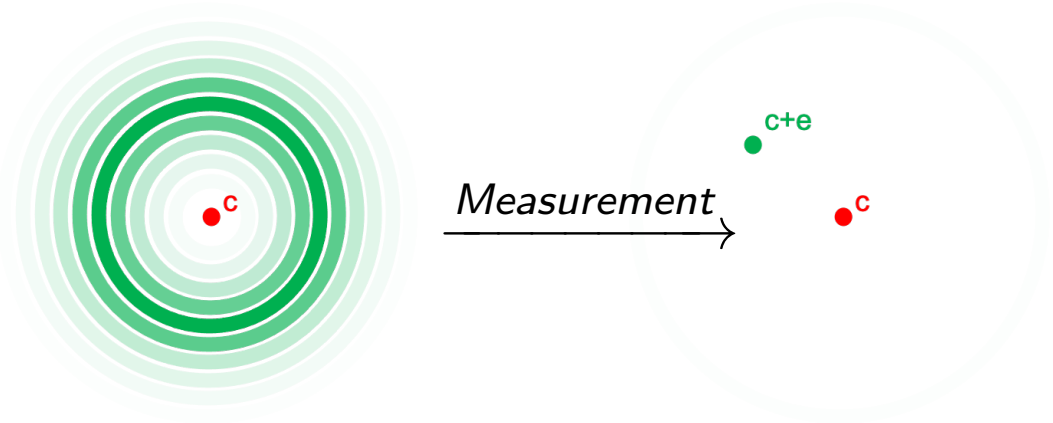


$$= \sum_{e \in \mathbb{F}_2^n} \sqrt{f(\mathbf{e})} |\mathbf{c}+\mathbf{e}\rangle$$

Recover $\mathbf{c}$ from
$|\psi_{\mathbf{c}}\rangle = \sum_{e \in \mathbb{F}_2^n} \sqrt{f(\mathbf{e})} |\mathbf{c}+\mathbf{e}\rangle$.

Advantage in having errors in quantum superposition?

$$|\Psi_{\mathbf{c}}\rangle = \sum_{e\in\mathbb{F}_2^n} \sqrt{f(\mathbf{e})}|\mathbf{c}+\mathbf{e}\rangle$$

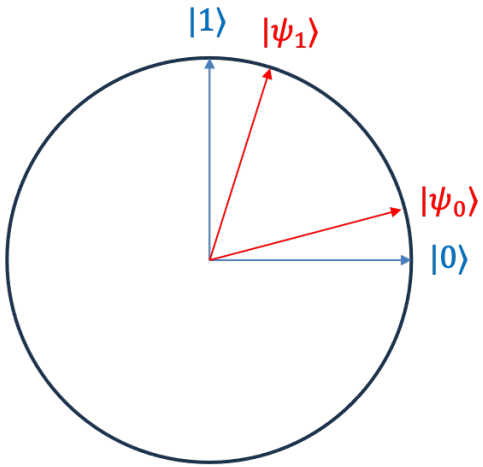


No advantage!

- If we start from $|\Psi_{\mathbf{c}}\rangle$ and we measure, we obtain a noisy codeword $\mathbf{c}+\mathbf{e}$ as in the classical setting: **no advantage!**
- **Noise model example:** binary symmetric noise of parameter t. For $\mathbf{c} = c_1, \ldots, c_n \in \mathbb{F}_2^n$,

$$|\Psi_{\mathbf{c}}\rangle = \bigotimes_{i=1}^{n} |\psi_{c_i}\rangle \quad \text{with} \quad |\psi_{c_i}\rangle = \sqrt{1-t}|c_i\rangle + \sqrt{t}|1-c_i\rangle.$$

There is a randomly chosen $\mathbf{c} = c_1, \ldots, c_n \in \mathcal{C}$ and we are given $|\Psi_{\mathbf{c}}\rangle = \bigotimes_{i=1}^{n} |\psi_{c_i}\rangle$, with $|\psi_{c_i}\rangle = \sqrt{1-t}|c_i\rangle + \sqrt{t}|1-c_i\rangle$. Our goal is to recover $\mathbf{c}$.



- Is there any use in performing other measurements than the $\{|0\rangle, |1\rangle\}$? **Idea: Perform Unambiguous State Discrimination**

$$|\psi_{c_i}\rangle = \sqrt{1-t}|c_i\rangle + \sqrt{t}|1-c_i\rangle.$$

Proposition ((USD) Unambiguous state discrimination)

There exists a quantum measurement such that

$$|\psi_{c_i}\rangle \xrightarrow{USD} \begin{cases} \text{Outcome } c_i & wp.\ 1-2\sqrt{t(1-t)} \\ \text{Outcome } 2 & wp.\ 2\sqrt{t(1-t)} \end{cases}$$

Corresponds to an erasure channel ($2 =$ erased) that erases each bit c_i wp. $2\sqrt{t(1-t)}$.

Huge change!. For a code $\mathcal{C}$ of dimension k, if we can recover $k(1+o(1))$ bits c_i, then we can efficiently recover $\mathbf{c}$ using Gaussian elimination.

Why are k code bits essentially enough?

Recall that $\mathbf{c} = \mathbf{sG}$ with

$$\mathbf{sG} = (\mathbf{s}\cdot\mathbf{g}_1, \mathbf{s}\cdot\mathbf{g}_2, \mathbf{s}\cdot\mathbf{g}_3, \mathbf{s}\cdot\mathbf{g}_4, \mathbf{s}\cdot\mathbf{g}_5, \mathbf{s}\cdot\mathbf{g}_6, \mathbf{s}\cdot\mathbf{g}_7, \mathbf{s}\cdot\mathbf{g}_8, \ldots, \mathbf{s}\cdot\mathbf{g}_n).$$

- If we add noise

$$\mathbf{sG}+\mathbf{e} = (\mathbf{s}\cdot\mathbf{g}_1, \mathbf{s}\cdot\mathbf{g}_2+1, \mathbf{s}\cdot\mathbf{g}_3, \mathbf{s}\cdot\mathbf{g}_4, \mathbf{s}\cdot\mathbf{g}_5, \mathbf{s}\cdot\mathbf{g}_6+1, \mathbf{s}\cdot\mathbf{g}_7, \mathbf{s}\cdot\mathbf{g}_8, \ldots, \mathbf{s}\cdot\mathbf{g}_n).$$

Hard problem even with small fraction of errors

- If we erase some parities

$$\text{Erase}(\mathbf{sG}) = (\mathbf{s}\cdot\mathbf{g}_1, \perp, \perp, \mathbf{s}\cdot\mathbf{g}_4, \perp, \perp, \mathbf{s}\cdot\mathbf{g}_7, \perp, \ldots, \mathbf{s}\cdot\mathbf{g}_n).$$

Easy if k linearly independent parities of s remain.

Applications to quantum decoding

We start from a binary linear code $\mathcal{C}$ of dimension k and length n. From any codeword $\mathbf{c}$ + noise, we want to recover $\mathbf{c}$.

$$\mathbf{c} = 0011101000111 \xrightarrow{BSC(t)} 0011001010101 \quad \text{Hard to recover } \mathbf{c}$$

$$\mathbf{c} = 0011101000111 \xrightarrow{QBSC(t)}$$

$$|\Psi_{\mathbf{c}}\rangle = |\psi_0\rangle|\psi_0\rangle|\psi_1\rangle|\psi_1\rangle|\psi_1\rangle|\psi_0\rangle|\psi_1\rangle|\psi_0\rangle|\psi_0\rangle|\psi_0\rangle|\psi_1\rangle|\psi_1\rangle|\psi_1\rangle$$

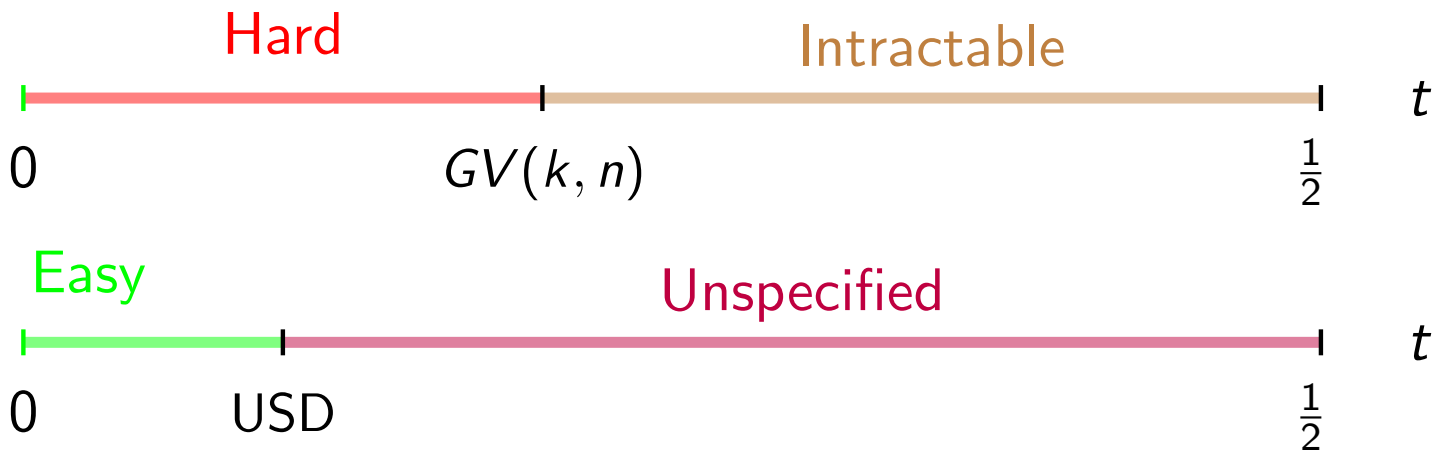
$$\downarrow USD$$

$$0022101020122 \quad \text{Easy to recover } \mathbf{c}$$

Unambiguous State Discrimination allows us to **reshape the error function** f, from a **binary symmetric channel** to an **erasure channel**.

Comparing the problems

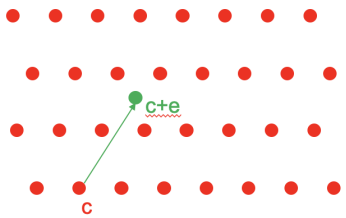
Figure 1: Complexity of $\mathrm{DP}(\mathcal{C}, t)$ and $\mathrm{QDP}(\mathcal{C}, t)$ for random $\mathcal{C}$ of dim. k and length n.



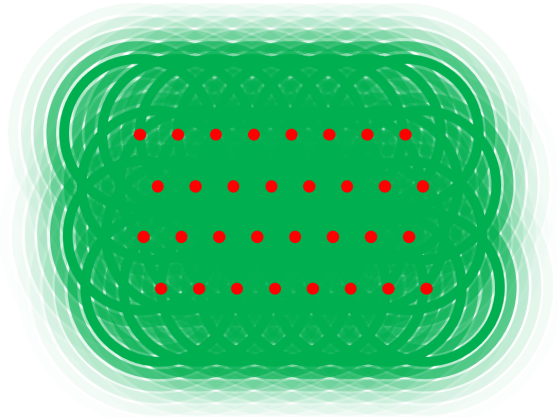
What about the untractability? Can it be tractable beyond GV(k,n)?

Decoding beyond GV

Classical decoding beyond GV

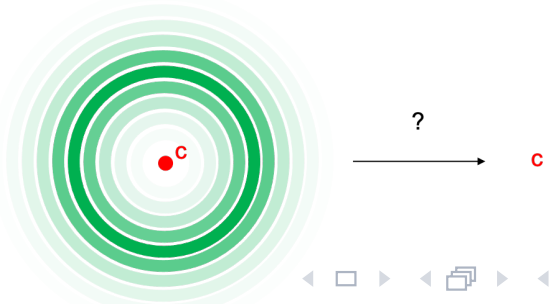


Quantum decoding beyond GV



We cannot recover $\mathbf{c}$ from $\mathbf{c}+\mathbf{e}$ as there are exponentially many points close to $\mathbf{c}+\mathbf{e}$.

In this mess, can we recover $\mathbf{c}$ from $|\Psi_{\mathbf{c}}\rangle$?



Recall

Definition (Quantum Decoding Problem $\mathrm{QDP}(\mathcal{C}, f)$)

Input: Error function $f : \mathbb{F}_2^n \to \mathbb{C}$.
Sample: $\mathbf{c} \leftarrow \mathcal{C}$.
Goal: Given $|\Psi_{\mathbf{c}}\rangle = \sum_{\mathbf{e}\in\mathbb{F}_2^n} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle$, recover $\mathbf{c}$.

- $\mathrm{QDP}(\mathcal{C}, f)$ is a quantum state discrimination problem on $\{|\Psi_{\mathbf{sG}}\rangle\}_{\mathbf{s}\in\mathbb{F}_2^k}$.
- **Pretty Good Measurement**: generic measurement s.t.

$$P_{OPT}^2 \leq P_{PGM} \leq P_{OPT}.$$

- To know whether $P_{OPT} = 1 - o(1)$ or $P_{OPT} = o(1)$, enough to look at P_{PGM}.

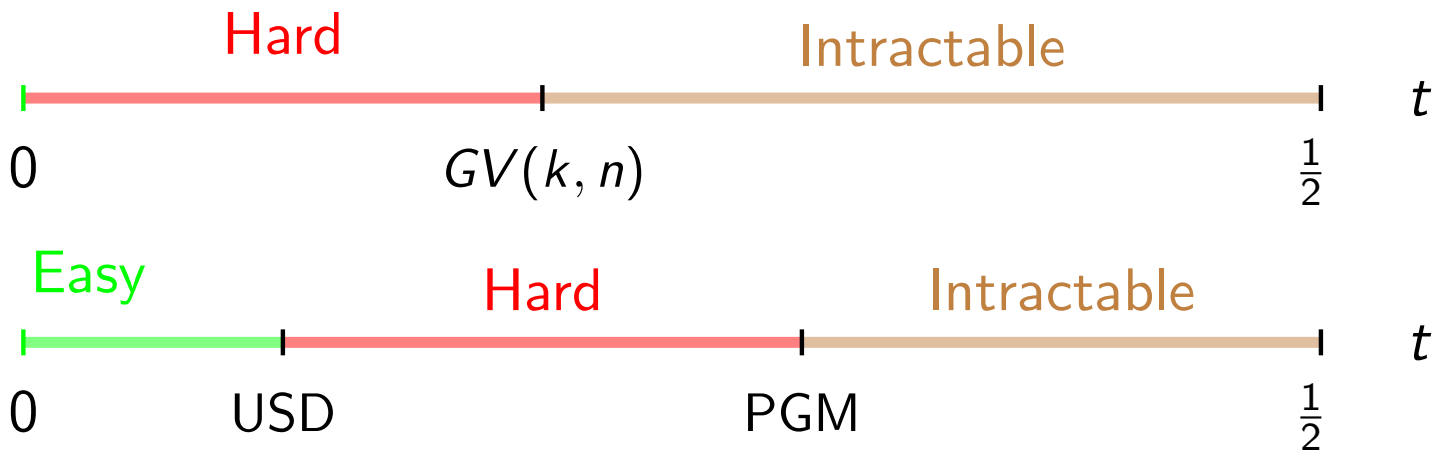
- PGM $= \{M_{\mathbf{s}}\}_{\mathbf{s}\in\mathbb{F}_2^k}$ with

$$M_{\mathbf{s}} = \rho^{-1/2}|\Psi_{\mathbf{sG}}\rangle\langle\Psi_{\mathbf{sG}}|\rho^{-1/2} \quad \text{and} \quad \rho = \sum_{\mathbf{s}\in\mathbb{F}_2^k} |\psi_{\mathbf{sG}}\rangle\langle\psi_{\mathbf{sG}}|.$$

- One can show that the PGM is a projective measurement easy to analyze.
- $\mathrm{QDP}(\mathcal{C}, t)$ is tractable **significantly beyond the GV bound.**

Comparing the problems: full analysis

Figure 2: Complexity of $\mathrm{DP}(\mathcal{C}, t)$ and $\mathrm{QDP}(\mathcal{C}, t)$ for random $\mathcal{C}$ of dim. k and length n.



The QDP problem is easier and more tractable! What about the reduction?

Analysis of the reduction in light of this complexity

Figure 3: Complexity of $\mathrm{QDP}(\mathcal{C}, t)$ for random $\mathcal{C}$ of dim. k and length n.

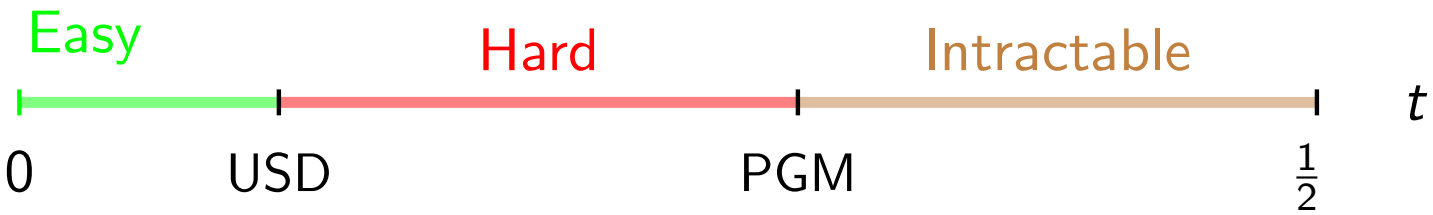
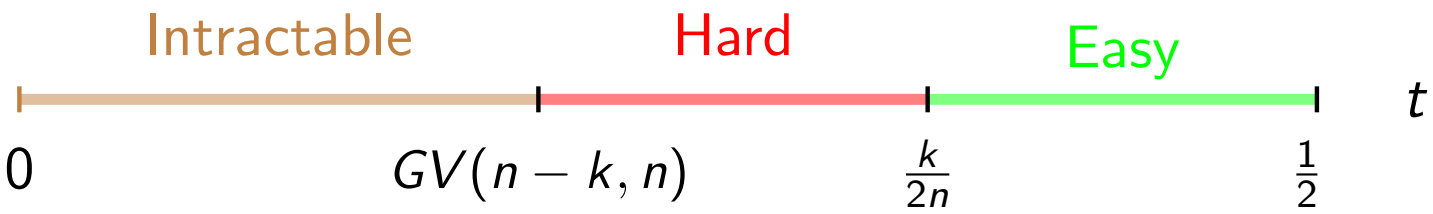


Figure 4: Complexity of $\mathrm{SCP}(\mathcal{C}^{\perp}, t)$ for random $\mathcal{C}$ of dim. k and length n.

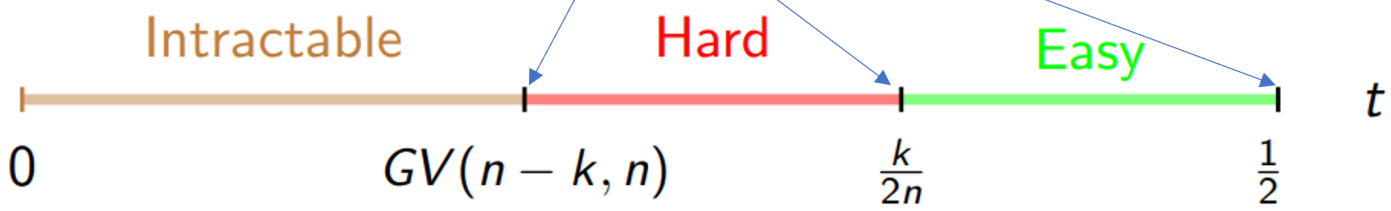


$$\boxed{\text{Algo for } \mathrm{QDP}(\mathcal{C}, t)} \Rightarrow \boxed{\text{Quatum Algo for } \mathrm{SCP}(\mathcal{C}^{\perp}, t^*)}$$

Tight reduction

Figure 3: Complexity of $\mathrm{QDP}(\mathcal{C}, t)$ for random $\mathcal{C}$ of dim. k and length n.

Figure 4: Complexity of $\mathrm{SCP}(\mathcal{C}^{\perp}, t)$ for random $\mathcal{C}$ of dim. k and length n.



Algo for $\mathrm{QDP}(\mathcal{C}, t)$ $\Rightarrow$ Quatum Algo for $\mathrm{SCP}(\mathcal{C}^{\perp}, t^*)$

Matches perfectly!

How a butterfly's flap in the decoder can cause a tornado in the algorithm.

Generic reduction with failures?

Theorem (Regev's reduction, v1)

Let $T = \{\mathbf{y} \in \mathbb{F}_2^n : |\mathbf{y}| \leq tn\}$. *Let* $f : \mathbb{F}_q^n \to \mathbb{C}$ *s.t.* $Supp(\widehat{f}) \subseteq T$ *and* $\|f\|_2 = 1$. *Then:*

Perfect algorithm for $QDP(\mathcal{C}, f) \Rightarrow$ *Quantum algorithm for* $SCP(\mathcal{C}^\perp, t)$.

The above theorem works only if the decoder is perfect: strongly limits applications. **Do we have?**

Algorithm for $\mathrm{QDP}(\mathcal{C}, f)$ with failure $o(1) \Rightarrow$
Quantum algorithm for $\mathrm{SCP}(\mathcal{C}, t)$ with failure $o(1)$

No! Examples where a negl(n) failure in the QDP algo. leads to a total failure of the SCP algo.

Why failures in the decoder are an issue

We have

Algorithm for $\mathrm{QDP}(\mathcal{C}, f)$ with failure $o(1) \Rightarrow$

Quantum algorithm for constructing $\sum_{\mathbf{y} \in \mathcal{C}^\perp} \widehat{g}(\mathbf{y})|\mathbf{y}\rangle$

with $\widehat{f} \approx \widehat{g}$.

But we don't have $\widehat{f}_{|\mathcal{C}^\perp} \approx \widehat{g}_{|\mathcal{C}^\perp}$. We can find examples where $supp(\widehat{f}) = T$ and $supp(\widehat{g}_{|\mathcal{C}^\perp}) \cap T = \emptyset$.

Consequences

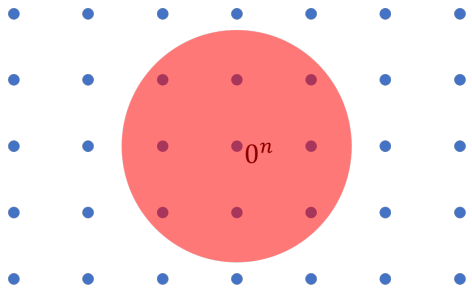
Not allowing failures on the decoder puts some strong constraint on the error function.

Consequences

- Each paper in the literature performs tailored analysis to show this doesn't hinder their algorithm.
- Sometimes, uses a worst decoder to avoid failures.
- Solution to all these problems: consider the **inhomogeneous setting**.

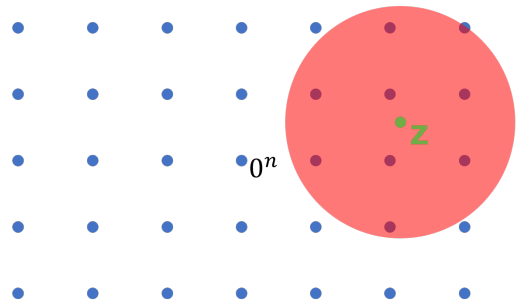
The inhomogeneous setting

Short codeword problem: find a non-zero small codeword (here in the red region)



Code $\mathcal{C}$

Inhomogeneous Short codeword problem: find a codeword not too far from a random point z (here in the red region)



Code $\mathcal{C}$

Both problems are essentially interchangeable in the world of code-based and lattice-based problems.

Close Codeword Problem: Definition

In the reduction, we will replace SCP with CCP.

Definition (Short Codeword Problem $\mathrm{SCP}(\mathcal{C}, t)$)

Goal: Find $\mathbf{c} \in \mathcal{C} \backslash \mathbf{0}, |\mathbf{c}| \leq tn$.

Definition (Close Codeword Problem $\mathrm{CCP}(\mathcal{C}, t)$)

Sample: $\mathbf{z} \leftarrow \mathbb{F}_2^n$.
Goal: Find $\mathbf{c} \in \mathcal{C}, |\mathbf{c} - \mathbf{z}| \leq tn$.

Extension to any target set.

Definition (Close Codeword Problem $\mathrm{CCP}(\mathcal{C}, T)$)

Sample: $\mathbf{z} \leftarrow \mathbb{F}_2^n$.
Goal: Find $\mathbf{c} \in \mathcal{C}, (\mathbf{c} - \mathbf{z}) \in T$.

Regev's reduction for $\mathrm{CCP}(\mathcal{C}, t)$

Take random $\mathbf{z} \in \mathbb{F}_2^n$.

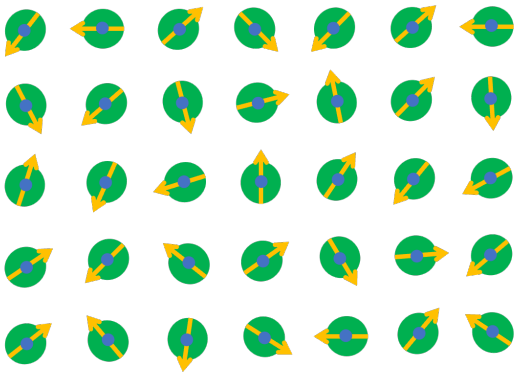
$$\frac{1}{\sqrt{2^k}} \sum_{\mathbf{c}\in\mathbb{F}_2^k} |\mathbf{c}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{F}_2^n} f(e)|\mathbf{e}\rangle \to \frac{1}{\sqrt{2^k}} \sum_{\mathbf{c}\in\mathbb{F}_2^k \mathbf{e}\in\mathbb{F}_2^n} (-1)^{-\mathbf{c}\cdot\mathbf{z}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle|\mathbf{c}\rangle$$

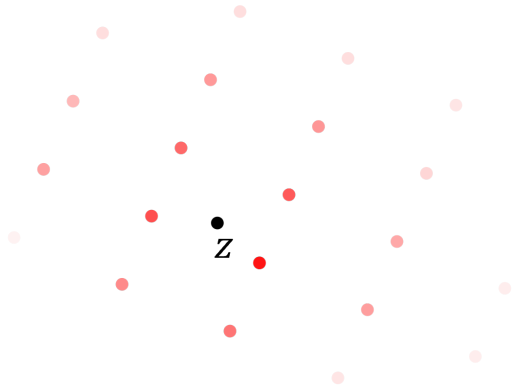
$$\xrightarrow{\text{QDP Solver}} \frac{1}{\sqrt{2^k}} \sum_{\mathbf{c}\in\mathcal{C},\mathbf{e}\in\mathbb{F}_2^n} (-1)^{-\mathbf{c}\cdot\mathbf{z}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle$$

$$\xrightarrow{H^{\otimes n}} \sim \sum_{\mathbf{y}\in\mathcal{C}^\perp} \widehat{f}(\mathbf{y}-\mathbf{z})|\mathbf{y}\rangle$$

We can easily adapt the reduction to solve CCP instead of SCP;

Second step in pictures





$$\frac{1}{\sqrt{Z}} \sum_{\mathbf{c}\in\mathcal{C},\mathbf{e}\in\mathbb{F}_q^n} (-1)^{-\mathbf{z}\cdot\mathbf{c}} f(\mathbf{e})|\mathbf{c}+\mathbf{e}\rangle \quad \xrightarrow{H^{\otimes n}} \quad \sim \sum_{\mathbf{y}\in\mathcal{C}^\perp} \widehat{f}(\mathbf{y}-\mathbf{z})|\mathbf{y}\rangle.$$

Failures in the inhomogeneous setting

We have

Algorithm for $\mathrm{QDP}(\mathcal{C}, f)$ with failure $o(1) \Rightarrow$

Quantum algorithm for constructing $\sum_{\mathbf{y} \in \mathcal{C}^\perp} \widehat{g}(\mathbf{y} - \mathbf{z})|\mathbf{y}\rangle$

with $\widehat{f} \approx \widehat{g}$.

This implies on average on z:

$$\widehat{f}_{|\mathcal{C}^\perp + \mathbf{z}} \approx \widehat{g}_{|\mathcal{C}^\perp + \mathbf{z}},$$

where $\mathcal{C}^\perp + \mathbf{z} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} + \mathbf{z} \in \mathcal{C}^\perp\}$.

Generic reduction with errors

Theorem (Regev's reduction, v3)

Let $T \subseteq \mathbb{F}_2^n$. *Let* $f : \mathbb{F}_2^n \to \mathbb{C}$ *s.t.* $Supp(\widehat{f}) \subseteq T$ *and* $\|f\|_2 = 1$.

Algorithm for $QDP(\mathcal{C}, f)$ *with failure* $\varepsilon \Rightarrow$

Quantum algorithm for $\mathrm{CCP}(\mathcal{C}^\perp, T)$ *with failure* $\leq \varepsilon + \eta + 2\sqrt{\varepsilon(1-\varepsilon)\eta}$

We can even relax the constraint on the support.

Theorem (Regev's reduction, v3)

Let $T \subseteq \mathbb{F}_2^n$. *Let* $f : \mathbb{F}_2^n \to \mathbb{C}$ *s.t.* $\sum_{\mathbf{x}\in T} |\widehat{f}(\mathbf{x})|^2 \geq 1 - \eta$ *and* $\|f\|_2 = 1$.

Algorithm for $QDP(\mathcal{C}, f)$ *with failure* $\varepsilon \Rightarrow$

Quantum algorithm for $\mathrm{CCP}(\mathcal{C}^\perp, T)$ *with failure* $\leq \varepsilon$

Theorem (Regev's reduction, v3)

Let $T \subseteq \mathbb{F}_2^n$. *Let* $f : \mathbb{F}_2^n \to \mathbb{C}$ *s.t.* $\sum_{\mathbf{x}\in T} |\widehat{f}(\mathbf{x})|^2 \geq 1-\eta$ *and* $\|f\|_2 = 1$.

Algorithm for $QDP(\mathcal{C}, f)$ *with failure* $\varepsilon \Rightarrow$

Quantum algorithm for $\mathrm{CCP}(\mathcal{C}^\perp, T)$ *with failure* $\leq \varepsilon + \eta + 2\sqrt{\varepsilon(1-\varepsilon)\eta}$

Takeaways:

- We have a **generic recipe** for constructing interesting quantum algorithms!
- Works for all codes and all functions. A lot of freedom in the choice of $\mathcal{C}$ and f.

$$\boxed{\mathrm{QDP}(\mathcal{C}, f) \text{ Algo}} \Rightarrow \boxed{\mathrm{CCP}(C^\perp, T) \text{ Quantum Algo.}}$$

$$\boxed{\mathrm{DP}(\mathcal{C}, |f|^2) \text{ Algo}} \Rightarrow \boxed{\mathrm{CCP}(C^\perp, T) \text{ Quantum Algo.}}$$