Chapter 5

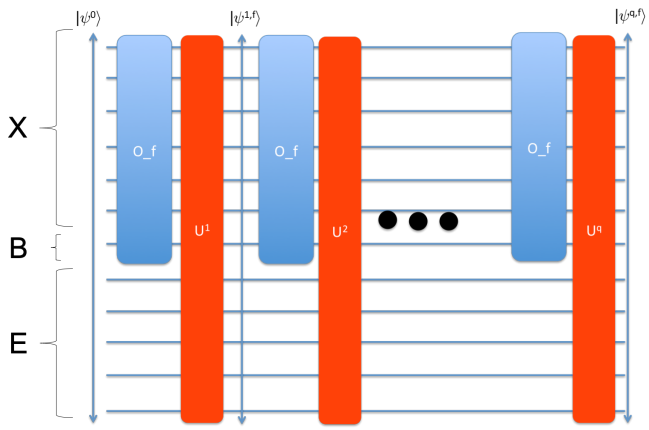
Lower bound for Grover's algorithm

5.1 Lower bound for Grover's algorithm and quantum complexity

Here, we show that for the search problem, Grover's algorithm is essentially optimal so we cannot expect anything better than $2^{n/2}$.

Framework

- Input: function $f : \{0,1\}^n \to \{0,1\}$. Goal: find x st. $f(x) = 1$.
- Access to $O_f(|x\rangle_X |b\rangle_B) = |x\rangle_X |b \oplus f(x)\rangle_B$.
- How many calls do I have to make to O_f to find x in the worst case?
- Result here: need $\Omega(2^{n/2})$ calls to O_f to work wp. 1.



General structure of a q-query search algorithm

- Initialize:

$$|\psi^{0,f}\rangle = |\psi^0\rangle = \sum_{x\in\{0,1\}^n} \sum_{b\in\{0,1\}} \alpha^0_{x,b} |x,b\rangle_{XB} |E^0_{x,b}\rangle_E \quad \text{st.} \quad \sum_{x,b} |\alpha^0_{x,b}|^2 = 1$$

- 1 step: apply a unitary O_f on XB and U^{i+1} independent of f on XBE.

$$\begin{aligned}|\psi^{i+1,f}\rangle &= U^{i+1}(O_f \otimes I_E)(|\psi^{i,f}\rangle) \\ &= \sum_{x\in\{0,1\}^n} \sum_{b\in\{0,1\}} \alpha_{x,b}^{i+1,f} |x,b\rangle_{XB} |E_{x,b}^{i+1,f}\rangle_E\end{aligned}$$

  Again, $\sum_{x,b} |\alpha_{x,b}^{i+1,f}|^2 = 1$.

- Final state: $|\psi^{q,f}\rangle$. Procedure to extract a solution from this state.

Main idea

- For any $y \in \{0,1\}^n$, we define f_y satisfying $f_y(y) = 1$ and $f_y(x) = 0$ for $x \neq y$.
- Consider any $y, z \in \{0,1\}^n$. The search procedure should output y when querying f_y and z when querying f_z.
  $\Rightarrow |\psi^{q,f_y}\rangle$ and $|\psi^{q,f_z}\rangle$ are orthogonal.
- But $|\psi^{0,f_y}\rangle = |\psi^{0,f_z}\rangle$. Idea is to show that each query cannot separate those 2 states too much (on average on y, z).

The Euclidian norm on quantum states We consider the Euclidian $\left|\left|\cdot\right|\right|$. Recall that

$$\left|\left|\sum_i \alpha_i |i\rangle\right|\right| = \sqrt{\sum_i |\alpha_i|^2}.$$

For any 2 quantum states $|\phi_1\rangle, |\phi_2\rangle$ and any Unitary U, we have $\left|\left||\phi_1\rangle - |\phi_2\rangle\right|\right| = \left|\left|U(|\phi_1\rangle) - U(|\phi_2\rangle)\right|\right|$. One can also check that if $|\phi_1\rangle \perp |\phi_2\rangle$ then $\left|\left||\phi_1\rangle - |\phi_2\rangle\right|\right| = \sqrt{2}$. We use an intermediate function, the all 0 function denoted $f_\emptyset$. Notice that $O_{f_\emptyset} = I$. We first show

Lemma 2. $\frac{1}{2^n}\sum_y \left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_y}\rangle\right|\right| \geq \sqrt{2} \cdot \frac{2^n-1}{2^n}$.

Proof. Let $y_0 \in \{0,1\}^n$ that minimizes $\left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_{y_0}}\rangle\right|\right|$. We have

$$\frac{1}{2^n-1}\sum_{y\neq y_0} \left|\left||\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle\right|\right| = \sqrt{2}.$$

from the orthogonality of those states. Moreover, by triangle inequality, we have

$$\begin{aligned}\frac{1}{2^n-1}\sum_{y\neq y_0} \left|\left||\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle\right|\right| &\leq \frac{1}{2^n-1}\sum_{y\neq y_0} \left|\left||\psi^{q,f_y}\rangle - |\psi^{q,f_\emptyset}\rangle\right|\right| + \frac{1}{2^n-1}\sum_{y\neq y_0} \left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_{y_0}}\rangle\right|\right| \\ &\leq \frac{2}{2^n-1}\sum_{y\neq y_0} \left|\left||\psi^{q,f_y}\rangle - |\psi^{q,f_\emptyset}\rangle\right|\right|\end{aligned}$$

From there, we get the result:

$$\frac{1}{2^n}\sum_y \left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_y}\rangle\right|\right| \geq \frac{1}{2^n}\sum_{y\neq y_0} \left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_y}\rangle\right|\right| \geq \frac{1}{\sqrt{2}} \cdot \frac{2^n-1}{2^n}.$$

□

So now, our goal is to bound this quantity as a function of q. This will give us the desired lower bound on q. We first prove the following:

Lemma 3. *For any $i \in [0, q-1]$, for any $y \in \{0,1\}^n$, we have*

$$\left|\left||\psi^{i+1,f_\emptyset}\rangle - |\psi^{i+1,f_y}\rangle\right|\right| \leq \left|\left||\psi^{i,f_\emptyset}\rangle - (O_{f_y} \otimes I)|\psi^{i,f_\emptyset}\rangle\right|\right| + \left|\left||\psi^{i,f_\emptyset}\rangle - |\psi^{i,f_y}\rangle\right|\right|.$$

Proof. We have

$$\begin{aligned}
\left|\left||\psi^{i+1,f_\emptyset}\rangle - |\psi^{i+1,f_y}\rangle\right|\right| &= \left|\left|U^{i+1}|\psi^{i,f_\emptyset}\rangle - U^{i+1}(O_{f_y} \otimes I)|\psi^{i,f_y}\rangle\right|\right| \\
&\leq \left|\left|U^{i+1}|\psi^{i,f_\emptyset}\rangle - U^{i+1}(O_{f_y} \otimes I)|\psi^{i,f_\emptyset}\rangle\right|\right| + \\
&\quad \left|\left|U^{i+1}(O_{f_y} \otimes I)|\psi^{i,f_\emptyset}\rangle - U^{i+1}(O_{f_y} \otimes I)|\psi^{i,f_y}\rangle\right|\right| \\
&= \left|\left||\psi^{i,f_\emptyset}\rangle - (O_{f_y} \otimes I)|\psi^{i,f_\emptyset}\rangle\right|\right| + \left|\left||\psi^{i,f_\emptyset}\rangle - |\psi^{i,f_y}\rangle\right|\right|.
\end{aligned}$$

□

We now prove our main proposition

Proposition 1.

$$\frac{1}{2^n}\sum_y \left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_y}\rangle\right|\right| \leq \frac{2q}{2^{n/2}}.$$

Proof. Fix i and y. We write

$$|\psi^{i,f_\emptyset}\rangle = \sum_{x\in\{0,1\}^n}\sum_{b\in\{0,1\}} \alpha^i_{x,b}|x,b\rangle_{XB}|E^i_{x,b}\rangle_E$$

From the definition of O_{f_y}, we also have

$$(O_{f_y} \otimes I)|\psi^{i,f_\emptyset}\rangle = \sum_{x\neq y}\sum_{b\in\{0,1\}} \alpha^i_{x,b}|x,b\rangle_{XB}|E^i_{x,b}\rangle_E + \sum_{b\in\{0,1\}} \alpha^i_{x,\bar{b}}|y,b\rangle_{XB}|E^i_{y,\bar{b}}\rangle_E$$

for some unknown amplitudes $\alpha^i_{x,b}$ (the superscripts $f_\emptyset$ are omitted). For each y, i, this gives

$$\begin{aligned}
\left|\left||\psi^{i,f_\emptyset}\rangle - (O_{f_y} \otimes I)|\psi^{i,f_\emptyset}\rangle\right|\right| &= \sqrt{\sum_{x\neq y,b} |\alpha^i_{x,b} - \alpha^i_{x,b}|^2 + \sum_b |\alpha^i_{y,b} - \alpha^i_{y,\bar{b}}\langle E^i_{y,b}|E^i_{y,\bar{b}}\rangle|^2} \\
&\leq 2\sqrt{|\alpha^i_{y,0}|^2 + |\alpha^i_{y,1}|^2}
\end{aligned}$$

Plugging this into the inequality of Lemma 2 and performing a recursion, we get

$$\left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_y}\rangle\right|\right| \leq \sum_{i=0}^{q-1} 2\sqrt{|\alpha^i_{y,0}|^2 + |\alpha^i_{y,1}|^2}$$

We average this over all y and get.

$$\begin{aligned}
\frac{1}{2^n}\sum_y \left|\left||\psi^{q,f_\emptyset}\rangle - |\psi^{q,f_y}\rangle\right|\right| &\leq \frac{1}{2^n}\sum_{y\in\{0,1\}^n}\sum_{i=0}^{q-1} 2\sqrt{|\alpha^i_{y,0}|^2 + |\alpha^i_{y,1}|^2} \\
&\leq \frac{1}{2^{n/2}}\sum_{i=0}^{q-1} 2\sqrt{\underbrace{\sum_y |\alpha^i_{y,0}|^2 + |\alpha^i_{y,1}|^2}_{=1}} \\
&\leq \frac{2q}{2^{n/2}}.
\end{aligned}$$

Using Lemma 2, we immediately have $q \geq \Omega(2^{n/2})$. □

5.2 Quantum complexity

5.2.1 Definitions

This part will be self contained but will be easier to read with basic notions of complexity theory. We start with the definitions of basic complexity classes.

Definition 1. *A language L is in* P *iff. there exists an algorithm $\mathscr{A}(x)$ running in polynomial time (in its input's size $|x|$) such that*

- $\forall x \in L,\ \mathscr{A}(x)$ *outputs* 1.
- $\forall x \notin L,\ \mathscr{A}(x)$ *outputs* 0.

Definition 2. *A language L is in* BPP *iff. there exists a randomized algorithm $\mathscr{A}(x)$ running in expected polynomial time (in its input's size $|x|$) such that*

- $\forall x \in L,\ \Pr[\mathscr{A}(x)$ *outputs* $1] \geq 2/3$.
- $\forall x \notin L,\ \Pr[\mathscr{A}(x)$ *outputs* $1] \leq 1/3$.

Definition 3. *A language L is in* BQP *iff. there exists a quantum algorithm $\mathscr{A}(x)$ running in expected polynomial time (in its input's size $|x|$) such that*

- $\forall x \in L,\ \Pr[\mathscr{A}(x)$ *outputs* $1] \geq 2/3$.
- $\forall x \notin L,\ \Pr[\mathscr{A}(x)$ *outputs* $1] \leq 1/3$.

Definition 4. *A language L is in* NP *iff. there exists an algorithm $\mathscr{A}(x,y)$ running in polynomial time (in its input's size $|x|, |y|$) such that*

- $\forall x \in L,\ \exists y \in \{0,1\}^{\mathsf{poly}(|x|)},\ \mathscr{A}(x,y)$ *outputs* 1.
- $\forall x \notin L,\ \forall y \in \{0,1\}^{\mathsf{poly}(|x|)},\ \mathscr{A}(x,y)$ *outputs* 0.

2.1 Does P = NP?

The following is a chart of what my 2002 poll said and what the 2012 poll says. DK stands for Don't Know, DC stands for Don't Care. Ind stands for Independent. I assume they mean Independent of ZFC.

	P $\neq$ NP	P = NP	Ind	DC	DK	DK and DC	other
2002	61(61%)	9(9%)	4(4%)	1(1%)	22(22%)	0(0%)	3(3%)
2012	126 (83%)	12 (9%)	5 (3%)	5 (3%)	1(0.6%)	1 (0.6%)	1 (0.6%)

Figure 5.1: Poll on P vs. NP, taken from [Gas12]

5.2.2 Comparing BQP and NP

Chapter 2 showed that factoring can be solved in polynomial time with a quantum computer. In terms of complexity this means in terms of complexity that the decision problem FACTOR_D (see Figure 1) is in BQP. While we have by definition that $\mathsf{P} \subseteq \mathsf{BPP} \subseteq \mathsf{BQP}$, we have no idea if those inclusions are tight. For example, many people believe that BPP can be *derandomized* meaning that $\mathsf{P} = \mathsf{BPP}$. Also, we could also have $\mathsf{BPP} = \mathsf{BQP}$ but this would have drastic consequences. In particular, this would imply $\text{FACTOR}_\text{D} \in \mathsf{BPP}$, where FACTOR_D is a decision problem associated to factoring.

FACTOR_D Problem
Input: a number N of n bits and a number $k \in \mathbb{N}$. $(N, k) \in \text{FACTOR}_\text{D}$ iff. $\exists M \in [2, k]$ st. $M \mid N$.

Remark: If one has a polynomial algorithm (classical or quantum) to solve the FACTOR_D Problem then one can use it to solve the Factoring problem defined in Chapter 2 also in polynomial time in n. Can you find how?

So we have $\text{FACTOR}_\text{D} \in \mathsf{BQP}$ while we don't know (and don't believe) that $\text{FACTOR}_\text{D} \in \mathsf{BPP}$. $\text{FACTOR}_\text{D} \in \mathsf{NP}$ but is not an NP-complete problem. However, we also don't know and don't believe that $\mathsf{NP} \subseteq \mathsf{BQP}$. This means that we have no polynomial algorithm for NP-complete problems such as 3-SAT. The black box quantum lower bound for Grover's algorithm is one of the reasons why we don't believe $\mathsf{NP} \subseteq \mathsf{BQP}$.

Of course, we could have $P = NP$ (or even $P = PSPACE$) but this not believed, see Figure 5.1.

5.2.3 Quantum equivalent of NP

The natural quantum equivalent of quantum NP is QMA.

Definition 5. *A language L is in* QMA *iff. there exists a quantum algorithm $\mathscr{A}(x)$ running in expected polynomial time (in its input's size $|x|$) such that*

- $\forall x \in L, \exists |\phi\rangle$ *of size* $\mathsf{poly}(|x|)$, $\Pr[\mathscr{A}(x, |\phi\rangle)$ *outputs* $1] \geq 2/3$.

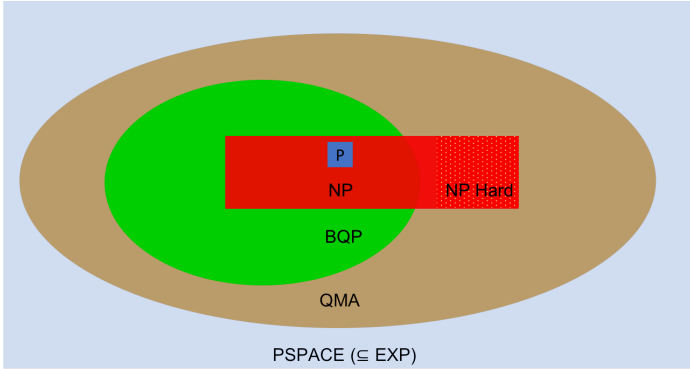


Figure 5.2: Currently believed inclusions of complexity classes

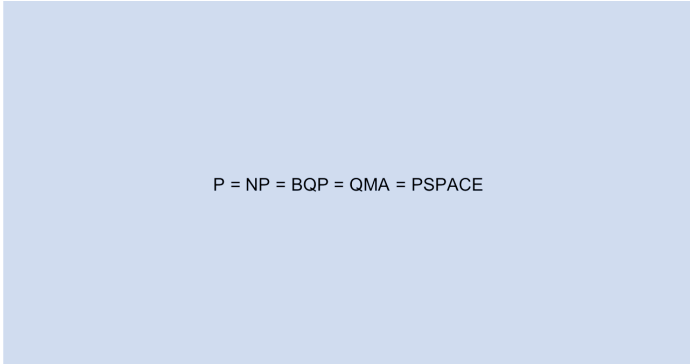


Figure 5.3: Another possibility: full collapse

- $\forall x \notin L, \exists |\phi\rangle$ *of size* $\mathsf{poly}(|x|)$, $\Pr[\mathscr{A}(x, |\phi\rangle)$ *outputs* $1] \leq 1/3$.

There aren't actually many problems which are known to be in QMA but not in MA (the probabilistic version of NP). The more we go higher in complexity, the less difference there is between classical and quantum. We even have $QPSPACE = PSPACE$, where $PSPACE$ (resp. $QSPACE$) is the complexity class of languages that can be solved with an algorithm (resp. quantum algorithm) running in polynomial space - but potentially exponential time.