Quantum Amplitude Amplification and Estimation

(COM-611) Quantum Information Theory and Computation

Alexandre Carlier

EPFL, Lausanne

January 24, 2019

Introduction

- Given a set $X = \{0, 1, \ldots N-1\}$ and a boolean function $\chi : X \longrightarrow \{0, 1\}$, we want to find a *good* element, i.e. an $x \in X$ such that $\chi(x) = 1$.
- If there is only one good element, a classical search algorithm has an average complexity of $\sum_{i=1}^{N} i \times \frac{1}{N} = \frac{N+1}{2}$.
- Quantum approach: given an equal superposition of states $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$, if we measure $|\Psi\rangle$, we get the correct $|x\rangle$ with probability $1/N$: so, the average number of iterations is N.
- **Grover's algorithm** [Grover, 1996]: we can transform $|\Psi\rangle$ in $\mathcal{O}(\sqrt{N})$ iterations so that performing a measurement on it gives the correct $|x\rangle$ with high probability.

Introduction

- **Amplitude amplification** [Brassard et al., 2002] is a generalization of Grover's algorithm where the input is given as an arbitrary superposition of elements of X: $|\Psi\rangle = \mathcal{A}|0\rangle = \sum_{x \in X} \alpha_x |x\rangle$ and more than one element may be good elements.
- We can write:

$$|\Psi\rangle = \sum_{x:\chi(x)=1} \alpha_x |x\rangle + \sum_{x:\chi(x)=0} \alpha_x |x\rangle = |\Psi_1\rangle + |\Psi_0\rangle$$

  with $a = \langle \Psi_1 | \Psi_1 \rangle \ll 1$ is the probability that measuring $|\Psi\rangle$ produces a good state.
- The standard approach would thus need to iterate $1/a$ times to find a good state. Amplitude amplification enables a **quadratic speed-up** in $\mathcal{O}(1/\sqrt{a})$.

Outline

1. Quantum amplitude amplification
   - The amplitude amplification operator
   - Amplitude amplification when a is not known
   - Quantum de-randomization
2. Quantum amplitude estimation
3. Applications

Outline

The amplitude amplification operator

- $|\Psi\rangle = \mathcal{A}|0\rangle = |\Psi_1\rangle + |\Psi_0\rangle$.
- S_χ is the *oracle function*:

$$|x\rangle \longmapsto \begin{cases} -|x\rangle & \text{if } \chi(x) = 1 \\ |x\rangle & \text{otherwise} \end{cases}$$

$$S_\chi = \frac{2}{1-a}|\Psi_0\rangle\langle\Psi_0| - I$$

- $S_0 = I - 2|0\rangle\langle 0|$.
- The *amplitude amplification* operator is:

$$\begin{aligned} Q &= -\mathcal{A}S_0\mathcal{A}^\dagger S_\chi \\ &= (\mathcal{A}(2|0\rangle\langle 0| - I)\mathcal{A}^\dagger) \times S_\chi \\ &= (2|\Psi\rangle\langle\Psi| - I)(\frac{2}{1-a}|\Psi_0\rangle\langle\Psi_0| - I) \end{aligned}$$

Geometrical representation of Q

- We can rewrite $Q = U_\Psi U_{\Psi_0}$, where $U_\Psi = 2\left|\Psi\right\rangle\left\langle\Psi\right| - I$ and $U_{\Psi_0} = \frac{2}{1-a}\left|\Psi_0\right\rangle\left\langle\Psi_0\right| - I$.

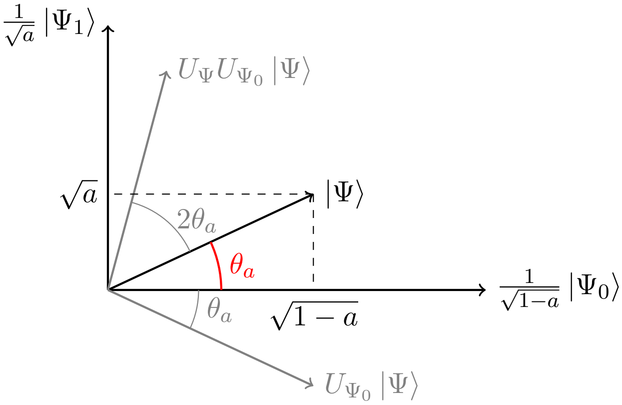


Figure 1: Operator Q as the composition of two reflections.

Matrix representation of Q

$$\begin{aligned}
Q\left|\Psi_1\right\rangle &= U_\Psi U_{\Psi_0}\left|\Psi_1\right\rangle = -U_\Psi\left|\Psi_1\right\rangle = (I - 2\left|\Psi\right\rangle\left\langle\Psi\right|)\left|\Psi_1\right\rangle \\
&= \left|\Psi_1\right\rangle - 2a\left|\Psi\right\rangle = (1-2a)\left|\Psi_1\right\rangle - 2a\left|\Psi_0\right\rangle \\
Q\left|\Psi_0\right\rangle &= U_\Psi\left|\Psi_0\right\rangle = (2\left|\Psi\right\rangle\left\langle\Psi\right| - I)\left|\Psi_0\right\rangle \\
&= 2(1-a)\left|\Psi\right\rangle - \left|\Psi_0\right\rangle = 2(1-a)\left|\Psi_1\right\rangle + (1-2a)\left|\Psi_0\right\rangle
\end{aligned}$$

Using $\sin^2(\theta_a) = a$ and $\cos^2(\theta_a) = 1 - a$, we get:

$$\begin{aligned}
Q\frac{\left|\Psi_1\right\rangle}{\sqrt{a}} &= (1-2a)\frac{\left|\Psi_1\right\rangle}{\sqrt{a}} - 2\sqrt{a(1-a)}\frac{\left|\Psi_0\right\rangle}{\sqrt{1-a}} \\
&= (1 - 2\sin^2(\theta_a))\frac{\left|\Psi_1\right\rangle}{\sqrt{a}} - 2\cos(\theta_a)\sin(\theta_a)\frac{\left|\Psi_0\right\rangle}{\sqrt{1-a}} \\
&= \cos(2\theta_a)\frac{\left|\Psi_1\right\rangle}{\sqrt{a}} - \sin(2\theta_a)\frac{\left|\Psi_0\right\rangle}{\sqrt{1-a}} \\
Q\frac{\left|\Psi_0\right\rangle}{\sqrt{1-a}} &= \sin(2\theta_a)\frac{\left|\Psi_1\right\rangle}{\sqrt{a}} + \cos(2\theta_a)\frac{\left|\Psi_0\right\rangle}{\sqrt{1-a}}
\end{aligned}$$

Matrix representation of Q

- Thus, Q is a rotation matrix in the basis $\{\frac{1}{\sqrt{a}}\left|\Psi_1\right\rangle, \frac{1}{\sqrt{1-a}}\left|\Psi_0\right\rangle\}$:

$$Q = \begin{pmatrix} \cos 2\theta_a & \sin 2\theta_a \\ -\sin 2\theta_a & \cos 2\theta_a \end{pmatrix}$$

- It has eigenvalues $e^{2i\theta_a}, e^{-2i\theta_a}$ with corresponding eigenvectors $\frac{1}{2}\begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ -i \end{pmatrix}$, noted $\left|\Psi_+\right\rangle$ and $\left|\Psi_-\right\rangle$.

Quantum amplitude amplification

- We can now write $|\Psi\rangle$ in the Q-eigenvector basis:

$$|\Psi\rangle = \frac{-i}{2}(e^{i\theta_a}|\Psi_+\rangle - e^{-i\theta_a}|\Psi_-\rangle)$$

and it follows that:

$$Q^j|\Psi\rangle = \frac{-i}{2}(e^{(2j+1)i\theta_a}|\Psi_+\rangle - e^{-(2j+1)i\theta_a}|\Psi_-\rangle)$$

- By writing it back in the original $\{\frac{1}{\sqrt{a}}|\Psi_1\rangle, \frac{1}{\sqrt{1-a}}|\Psi_0\rangle\}$ basis:

$$Q^j|\Psi\rangle = \sin((2j+1)\theta_a)\frac{1}{\sqrt{a}}|\Psi_1\rangle + \cos((2j+1)\theta_a)\frac{1}{\sqrt{1-a}}|\Psi_0\rangle$$

Quantum amplitude amplification

- After m applications of the operator Q, measuring the state $|\Psi\rangle$ produces a good state with probability equal to $\sin^2((2m+1)\theta_a)$.
- $x \mapsto \sin^2((2x+1)\theta_a)$ is maximized for $x = \frac{\pi}{4\theta} - \frac{1}{2}$.
- Thus the probability is maximized for $m = \lfloor \pi/(4\theta_a) \rfloor$ (when the value of a is known).
- We can show that $\sin^2((2m+1)\theta_a) \geq 1 - a$.

Complexity of the algorithm

- We use $2m+1$ applications of $\mathcal{A}$ and $\mathcal{A}^\dagger$.
- Since $\theta_a \approx \sin(\theta_a) = \sqrt{a}$, we get:

$$\begin{aligned} 2m+1 &= 2\left\lfloor \pi/(4\theta_a) \right\rfloor + 1 \\ &\approx 2\left\lfloor \pi/(4\sqrt{a}) \right\rfloor + 1 \\ &= \mathcal{O}(\frac{1}{\sqrt{a}}) \end{aligned}$$

- And the success probability is $1 - a \approx 1$.

Visual demo

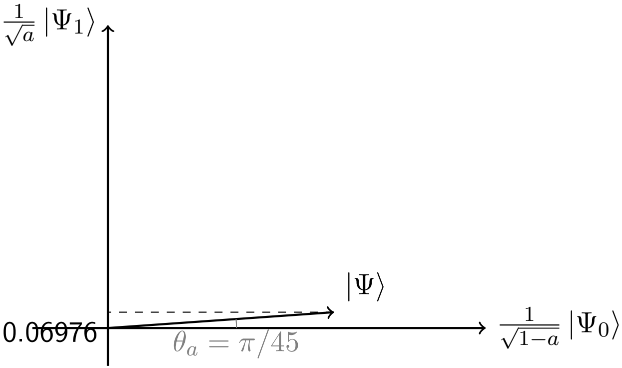


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

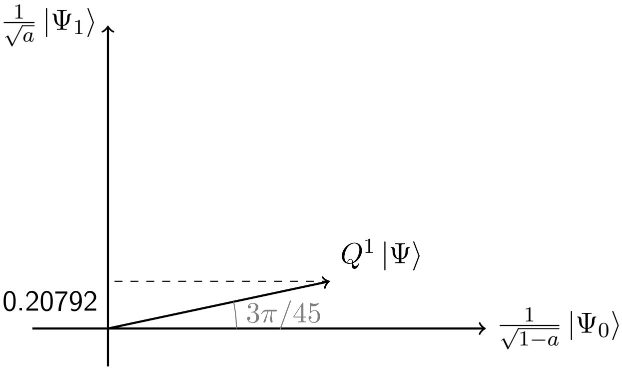


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

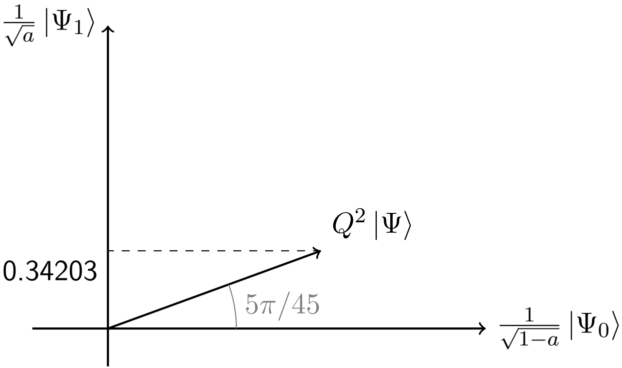


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

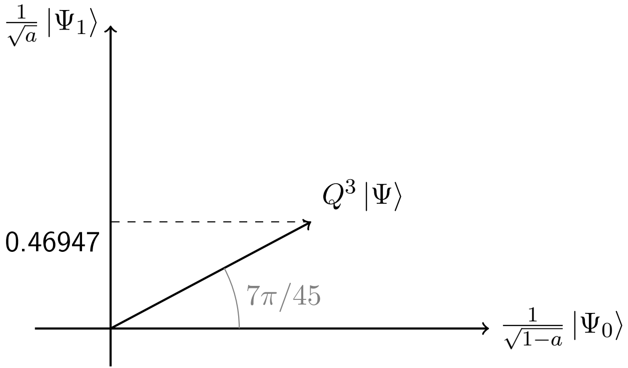


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

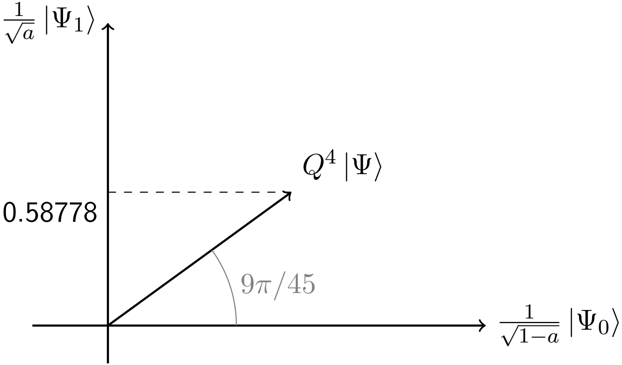


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

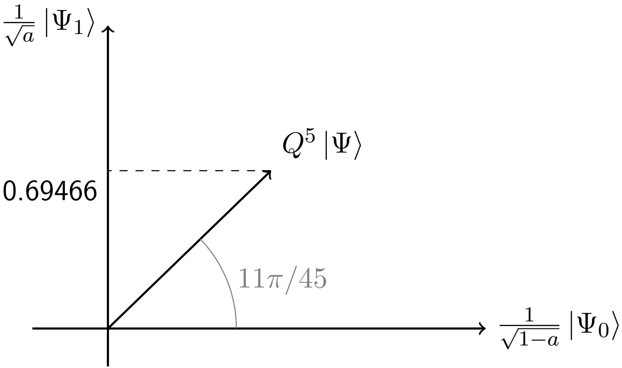


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

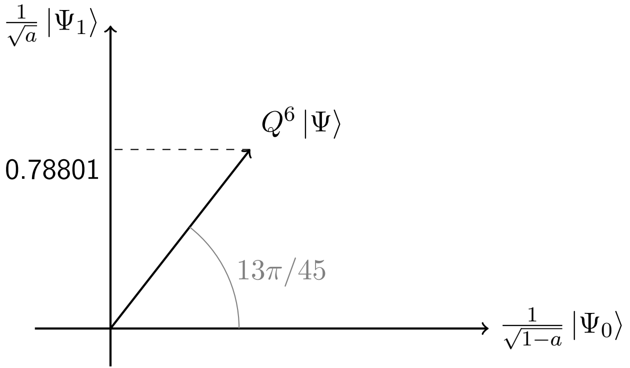


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

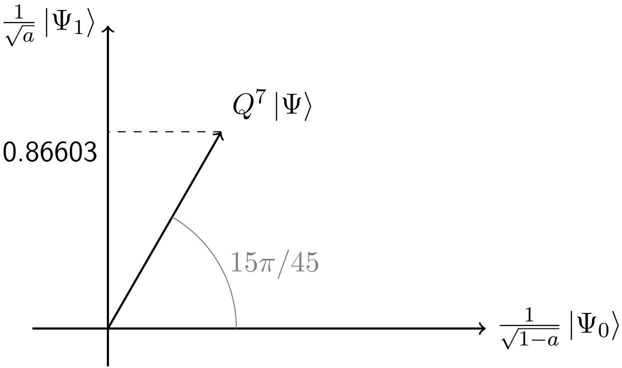


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

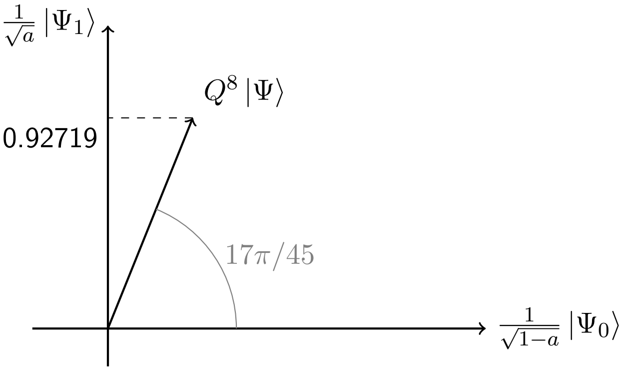


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

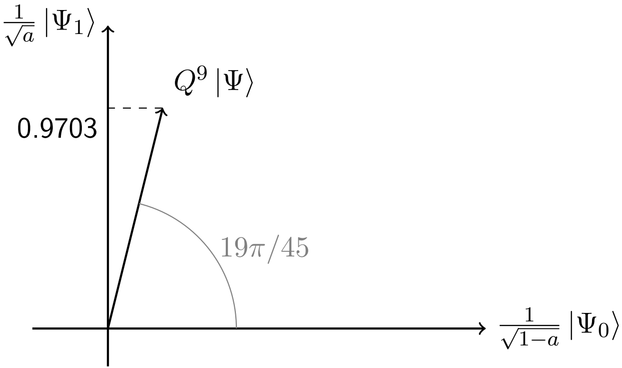


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

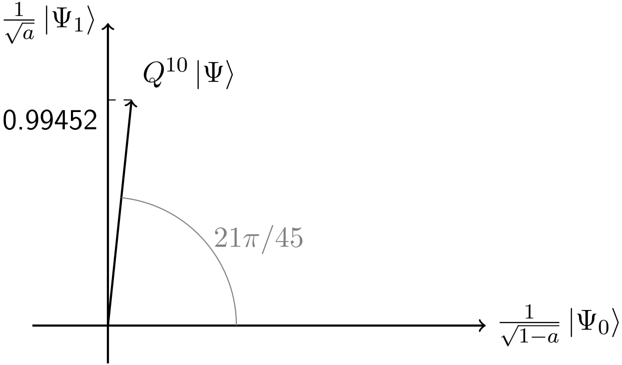


Figure 2: Visualization of the Quantum amplitude amplification algorithm

Visual demo

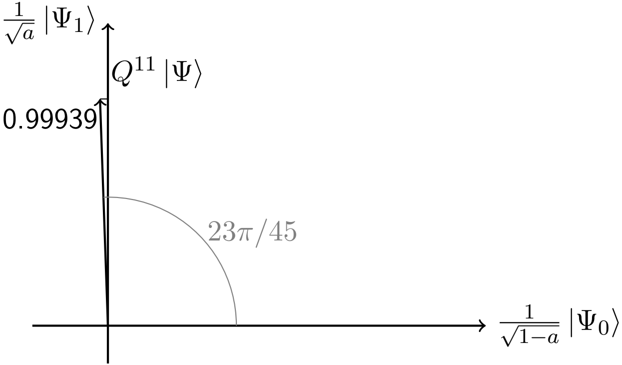


Figure 2: Visualization of the Quantum amplitude amplification algorithm

And indeed $m = \lfloor \pi/4\theta_a \rfloor = 11.$

Visual demo

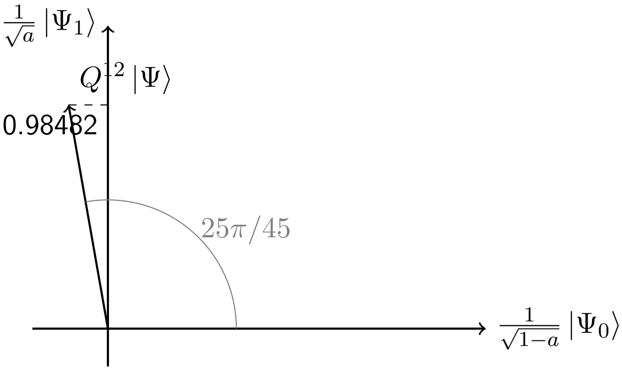


Figure 2: Visualization of the Quantum amplitude amplification algorithm

And indeed $m = \lfloor \pi/4\theta_a \rfloor = 11$.

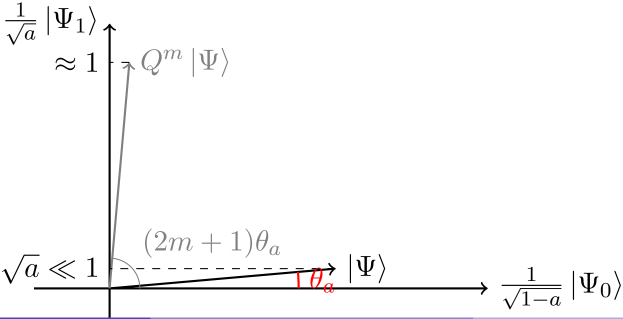
Grover's algorithm

Example

$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ and $\chi = \mathbb{1}_{x=0}$. Then $a = 1/N \ll 1$,

$$m = \left\lfloor \frac{\pi}{4\theta_a} \right\rfloor \approx \left\lfloor \frac{\pi}{4 \sin \theta_a} \right\rfloor = \left\lfloor \frac{\pi\sqrt{N}}{4} \right\rfloor = \mathcal{O}(\sqrt{N})$$

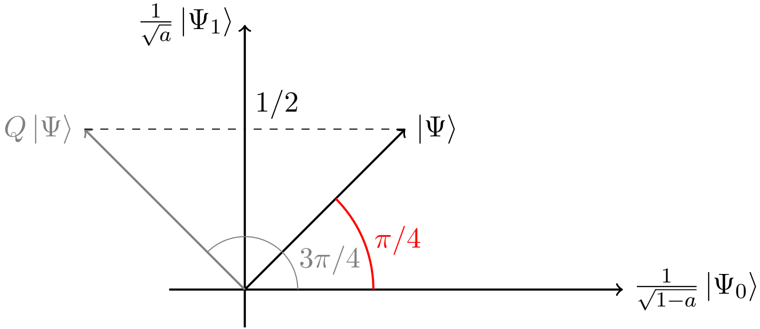
and we get the state $|0\rangle$ with probability $\sin^2((2m+1)\theta_a) \geq 1 - a \approx 1$.



A special case

Example

$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|x\rangle$ and $\chi = \mathbb{1}_{x=0}$. We have $a = 1/2$, $\theta_a = \frac{\pi}{4}$. Then, $m = 1$ and $\sin^2((2m+1)\theta_a) = \sin^2 \frac{3\pi}{4} = \frac{1}{2} = a$. Amplitude amplification has no effect.



Outline

Amplitude amplification when a is not known

- When a is not known, we can first estimate it using quantum amplitude estimation (see section 2) and then run the previous algorithm by replacing the exact a by its estimate.
- Another approach is to use **QSearch**. The intuition is the following: for $\theta \sim \mathcal{U}[0, 2\pi]$, $\mathbb{E}\left[\sin^2 \theta\right] = \frac{1}{2}$. By choosing M sufficiently large, $M\theta_a$ is large and by picking $j \in_U [\![1, M]\!]$, $j\theta_a \mod 2\pi$ follows a good approximation of $\mathcal{U}[0, 2\pi]$ (and so does $(2j+1)\theta_a \mod 2\pi$).
- Then, the probability $\sin^2((2j+1)\theta_a)$ that the measurement produces a good state is in average $\frac{1}{2}$.
- Since we don't know θ_a, we use an exponential search space for $M = c^l$ by iteratively incrementing the value of l for a constant c.

The QSearch algorithm

Initialization: $l = 0$.
Repeat: (while $|z\rangle$ is not a good state)

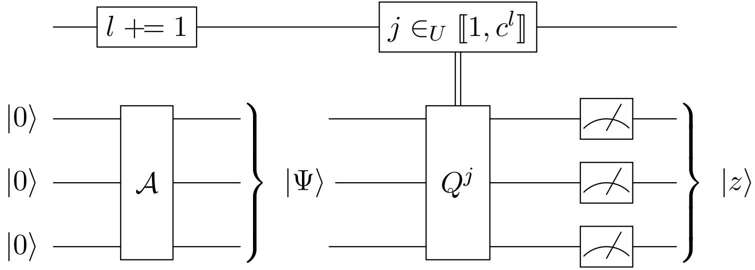


Figure 3: The **QSearch** algorithm

Outline

Quantum de-randomization when a is known

The success probability of the Quantum Amplitude Amplification algorithm is $1 - a$. It turns out we can actually find a good solution with *certainty*.

- $m \mapsto \sin^2((2m+1)\theta_a)$ is maximized for $\tilde{m} = \frac{\pi}{4\theta} - \frac{1}{2}$.
- If $\tilde{m}$ is an integer, $\sin^2((2\tilde{m}+1)\theta_a) = 1$.
- Else we use $m = \lceil \tilde{m} \rceil = \lfloor \pi/(4\theta_a) \rfloor$ iterations, which is slightly too much.

The de-randomization approach is the following:

- Apply Q only $\lfloor \tilde{m} \rfloor$ times. The resulting state is:

$$\sin((2\lfloor \tilde{m} \rfloor + 1)\theta_a)\frac{1}{\sqrt{a}}|\Psi_1\rangle + \cos((2\lfloor \tilde{m} \rfloor + 1)\theta_a)\frac{1}{\sqrt{1-a}}|\Psi_0\rangle$$

- We further define $Q'(\phi, \varphi) = -\mathcal{A}S_0(\phi)\mathcal{A}^\dagger S_\chi(\varphi)$

$$\text{where } \begin{cases} S_0(\phi) = e^{i\phi}|0\rangle\langle 0| + |1\rangle\langle 1| \\ S_\chi(\varphi) = \frac{e^{i\varphi}}{\sqrt{a}}|\Psi_1\rangle\langle\Psi_1| + \frac{1}{\sqrt{1-a}}|\Psi_0\rangle\langle\Psi_0| \end{cases}$$

Quantum de-randomization when a is known

- $Q = Q'(\phi = \pi, \varphi = \pi)$
- By applying one final $Q'(\phi, \varphi)$, we obtain:

$$\star\, |\Psi_1\rangle + \Big(e^{i\varphi}(1-e^{i\phi})\sqrt{a}\sin((2\lfloor\tilde{m}\rfloor+1)\theta_a) - ((1-e^{i\phi})a + e^{i\phi}) \frac{1}{\sqrt{1-a}}\cos((2\lfloor\tilde{m}\rfloor+1)\theta_a)\Big)|\Psi_0\rangle$$

- We can choose ϕ and φ so that the coefficient in front of $|\Psi_0\rangle = 0$:

$$\begin{aligned}
\iff \cot((2\lfloor\tilde{m}\rfloor+1)\theta_a) &= e^{i\varphi}2\sqrt{a(1-a)}\frac{1-e^{i\phi}}{2((1-e^{i\phi})a+e^{i\phi})} \\
&= e^{i\varphi}\sin(2\theta_a)(2\underbrace{a}_{=1-\cos(2\theta_a)}+\frac{2e^{i\phi}}{1-e^{i\phi}})^{-1} \\
&= e^{i\varphi}\sin(2\theta_a)(-\cos(2\theta_a)+\underbrace{\frac{1+e^{i\phi}}{1-e^{i\phi}}}_{=i\cot(\phi/2)})^{-1}
\end{aligned}$$

Outline

Quantum amplitude estimation

- Amplitude amplification: find $x \in X$ such that $\chi(x) = 1$.
- Amplitude estimation: estimate $a = \langle \Psi_1 | \Psi_1 \rangle$.
- By $a = \sin^2(\theta_a)$, an estimate for a translates into an estimate for θ_a.
- The eigenvalues of Q are $\lambda_+ = e^{2i\theta_a}$ and $\lambda_- = e^{-2i\theta_a}$, so we can instead estimate one of these eigenvalues.

Quantum amplitude estimation

- Let us define the operator

$$\Lambda_M(Q) : |j\rangle\,|y\rangle \mapsto |j\rangle\, Q^j\,|y\rangle$$

so that e.g:

$$\Lambda_M(Q)\,|j\rangle\,|\Psi_+\rangle = e^{2i\theta_a j}\,|j\rangle\,|\Psi_+\rangle$$

- We recall the quantum Fourier transform (for $x \in \{0, \ldots, M-1\}$):

$$F_M : |x\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i x y/M}\,|y\rangle$$

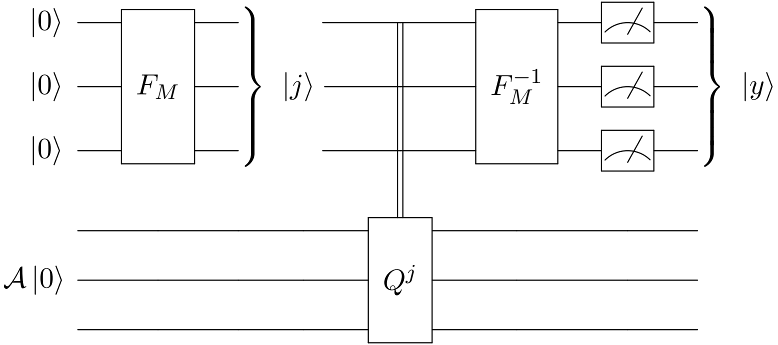
- And we define (for a real $0 \leq \omega < 1$):

$$|S_M(\omega)\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \omega y}\,|y\rangle$$

so that, for $x \in \{0, \ldots, M-1\}$: $|S_M(x/M)\rangle = F_M\ |x\rangle$.

Quantum circuit for amplitude estimation

$(F_M^{-1} \otimes I)(\Lambda_M(Q))(F_M \otimes I)$ applied on the state $|0\rangle \otimes \mathcal{A}|0\rangle$



(If M is a power of 2, we can replace the Quantum Fourier transforms by Hadamard gates)

Proof of correctness

The quantum circuit corresponds to the unitary transformation $(F_M^{-1} \otimes I)(\Lambda_M(Q))(F_M \otimes I)$ applied on the state $|0\rangle \otimes \mathcal{A}|0\rangle$, with

$$\mathcal{A}|0\rangle = -\frac{i}{\sqrt{2}}(e^{i\theta_a}|\Psi_+\rangle - e^{-i\theta_a}|\Psi_-\rangle)$$

By applying $F_M \otimes I$:

$$\frac{1}{\sqrt{2M}} \sum_{j=0}^{M-1} |j\rangle \otimes (e^{i\theta_a}|\Psi_+\rangle - e^{-i\theta_a}|\Psi_-\rangle)$$

After applying $\Lambda_M(Q)$:

$$\frac{e^{i\theta_a}}{\sqrt{2}}|S_M(\theta_a/\pi)\rangle \otimes |\Psi_+\rangle - \frac{e^{-i\theta_a}}{\sqrt{2}}|S_M(1-\theta_a/\pi)\rangle \otimes |\Psi_-\rangle$$

Proof of correctness

- Finally, after $F_M^{-1} \otimes I$, we have:

$$\frac{e^{i\theta_a}}{\sqrt{2}} F_M^{-1} |S_M(\theta_a/\pi)\rangle \otimes |\Psi_+\rangle - \frac{e^{-i\theta_a}}{\sqrt{2}} F_M^{-1} |S_M(1-\theta_a/\pi)\rangle \otimes |\Psi_-\rangle$$

- By tracing out the second register in the eigenvector basis $\{|\Psi_+\rangle, |\Psi_-\rangle\}$, we obtain a $\frac{1}{2}$-$\frac{1}{2}$ mixture of $F_M^{-1} |S_M(\theta_a/\pi)\rangle$ and $F_M^{-1} |S_M(1-\theta_a/\pi)\rangle$.

- By symmetry (since $\sin^2(\pi\frac{y}{M}) = \sin^2(\pi(1-\frac{y}{M})))$, we can assume the measured $|y\rangle$ is the result of measuring $F_M^{-1} |S_M(\theta_a/\pi)\rangle$.

- We thus have $\tilde{\theta_a} = \pi\frac{y}{M}$ is a good estimate of θ_a (see next slide).

Bounding the error of the estimate (1/6)

$\frac{1}{M} F_M^{-1} |S_M(\omega)\rangle$ is a good estimate of ω. Indeed, if $\omega = x/M$ for some $0 \leq x < M$, then $F_M^{-1} |S_M(x/M)\rangle = |x\rangle$. Otherwise:

Theorem

Let X be the r.v. corresponding to the result of measuring $F_M^{-1} |S_M(\omega)\rangle$. Then:

$$\mathbb{P}\left(\left|\frac{1}{M}X - \omega\right| \leq \frac{1}{M}\right) \geq \frac{8}{\pi^2} \approx 0.81$$

Lemma

Letting $\Delta = \left|\frac{1}{M}x - \omega\right|$ for some $x \in \{0, \ldots, M-1\}$, we have:

$$\mathbb{P}[X = x] = \frac{\sin^2(M\Delta\pi)}{M^2 \sin^2(\Delta\pi)}$$

Bounding the error of the estimate (2/6)

Proof of the Lemma.

$$
\begin{aligned}
\mathbb{P}[X = x] &= |\langle x| F_M^{-1} |S_M(\omega)\rangle|^2 \\
&= |(F_M |x\rangle)^\dagger |S_M(\omega)\rangle|^2 \\
&= |\langle S_M(x/M)|S_M(\omega)\rangle|^2 \\
&= \left|(\frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i x/M y} \langle y|)(\frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \omega y} |y\rangle)\right|^2 \\
&= \frac{1}{M^2} \left|\sum_{y=0}^{M-1} e^{2\pi i \Delta y}\right|^2 = \frac{\sin^2(M\Delta\pi)}{M^2 \sin^2(\Delta\pi)}
\end{aligned}
$$

□

Bounding the error of the estimate (3/6)

Proof of the Theorem.

$$\begin{aligned}\mathbb{P}[d(X/M,\omega) \leq 1/M] &= \mathbb{P}[X = \lfloor M\omega \rfloor] + \mathbb{P}[X = \lceil M\omega \rceil] \\ &= \frac{\sin^2(M\Delta\pi)}{M^2\sin^2(\Delta\pi)} + \frac{\sin^2(M(\frac{1}{M}-\Delta)\pi)}{M^2\sin^2((\frac{1}{M}-\Delta)\pi)} \\ &\geq \frac{8}{\pi^2}\end{aligned}$$

Since the minimum of this expression is reached at $\Delta = 1/(2M)$. □

Bounding the error of the estimate (4/6)

A bounding error on $\tilde{\theta_a}$ translates into a bound on $\tilde{a}$.

Lemma

Let $a = \sin^2(\theta_a)$ *and* $\tilde{a} = \sin^2(\tilde{\theta_a})$ *with* $0 \leq \theta_a, \tilde{\theta_a} \leq \frac{\pi}{2}$. *Then:*

$$|\tilde{\theta_a} - \theta_a| \leq \epsilon \Longrightarrow |\tilde{a} - a| \leq 2\epsilon\sqrt{a(1-a)} + \epsilon^2$$

Bounding the error of the estimate (5/6)

A bounding error on $\tilde{\theta_a}$ translates into a bound on $\tilde{a}$.

Proof.

$$\begin{aligned}
\tilde{a} - a &= \sin^2(\tilde{\theta_a}) - \sin^2(\theta_a) \leq \sin^2(\theta_a + \epsilon) - \sin^2(\theta_a) \\
&= (\sin(\theta_a)\cos(\epsilon) + \sin(\epsilon)\cos(\theta_a))^2 - \sin^2(\theta_a) \\
&= \sin^2(\theta_a)\cos(\epsilon) + \sin^2(\epsilon)\cos^2(\theta_a) + 2\cos(\theta_a)\sin(\theta_a)\cos(\epsilon)\sin(\epsilon) \\
&\quad - \sin^2(\theta_a) \\
&= \sin^2(\epsilon)(\cos^2(\theta_a) - \sin^2(\theta_a)) + \sqrt{a(1-a)}\sin^2(\epsilon) \\
&= \sqrt{a(1-a)}\sin(2\epsilon) + (1-2a)\sin^2(\epsilon) \\
&\leq 2\epsilon\sqrt{a(1-a)} + \epsilon^2
\end{aligned}$$

Same for $a - \tilde{a}$. □

Bounding the error of the estimate (6/6)

Combining those results, the Amplitude Estimation algorithm outputs $\tilde{\theta}_a$ such that

$$|\tilde{\theta}_a/\pi - \theta_a/\pi| \leq \frac{1}{M}$$

$$\iff |\tilde{\theta}_a - \theta_a| \leq \frac{\pi}{M}$$

with probability greater than $8/\pi^2$.

Thus, by setting $\epsilon = \frac{\pi}{M}$:

$$|\tilde{a} - a| \leq 2\pi \frac{\sqrt{a(1-a)}}{M} + \frac{\pi^2}{M^2}$$

Outline

1. Quantum amplitude amplification
   - The amplitude amplification operator
   - Amplitude amplification when a is not known
   - Quantum de-randomization
2. Quantum amplitude estimation
3. Applications

1. Application to counting

- The amplitude estimation algorithm can be used for counting the number of good elements $t = |\{x \in X \text{ s.t. } \chi(x) = 1\}|$.
- By choosing $\mathcal{A} = F_N$ the Quantum Fourier Transform:

$$F_N : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / M} |y\rangle$$

- we have:

$$\mathcal{A}|0\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle = \underbrace{\frac{1}{\sqrt{N}} \sum_{y:\chi(y)=1} |y\rangle}_{=|\Psi_1\rangle} + \underbrace{\frac{1}{\sqrt{N}} \sum_{y:\chi(y)=0} |y\rangle}_{=|\Psi_0\rangle}$$

Thus, $a = \langle \Psi_1 | \Psi_1 \rangle = \frac{1}{N}$, and so $t = a \times N$.

2. Application to Monte Carlo sampling

- Let X be a random variable taking values $\{0, \ldots, N\}$ with probability p_i. We want to compute $\mathbb{E}[f(X)]$.
- Using Monte Carlo sampling, with M evaluations of f, we get:

$$\frac{1}{M}\sum_{k=0}^{M} f(X_k) \approx \mathbb{E}[f(X)] \pm \frac{C}{\sqrt{M}}$$

- Quantum approach: define

$$|\Psi\rangle = \sum_{i=0}^{N-1} \sqrt{p_i}\,|i\rangle$$

and the operator

$$F : |i\rangle \otimes |0\rangle \mapsto |i\rangle \otimes (\sqrt{1-f(i)}\,|0\rangle + \sqrt{f(i)}\,|1\rangle)$$

Then:

$$F\,|\Psi\rangle \otimes |0\rangle = \sum_{i=0}^{N-1} \sqrt{1-f(i)}\sqrt{p_i}\,|i\rangle \otimes |0\rangle + \sqrt{f(i)}\sqrt{p_i}\,|i\rangle \otimes |1\rangle$$

2. Application to Monte Carlo sampling

Using amplitude estimation, we estimate the probability to measure $|1\rangle$ in the last Qbit: $\tilde{a} = \sum_{i=0}^{N-1} p_i f(i) = \mathbb{E}[f(X)]$, and using M evaluations of f:

$$|\tilde{a} - a| \leq 2\pi \frac{\sqrt{a(a-a)}}{M} + \frac{\pi^2}{M^2}$$

with a convergence rate of $\mathcal{O}(\frac{1}{M})$ to be compared to the classical $\mathcal{O}(\frac{1}{\sqrt{M}})$ rate.

3. Application to Quantum Risk Analysis

- *Quantum Risk Analysis* [Woerner and Egger, 2018] (IBM Research - Zurich):
  In quantitative finance, VaR (Value at Risk) and CVaR (Conditional Value at Risk) are typically estimated using Monte Carlo sampling of the relevant probability distribution.
- For a confidence value $\alpha \in [0,1]$, $\text{VaR}_\alpha(X)$ is the smallest l such that $\mathbb{P}[X \leq l] \geq (1-\alpha)$.
- By defining $f_l(x) = 1$ if $\mathbb{1}_{x \leq l}$, we thus want to approximate $\mathbb{P}[X \leq l] = \mathbb{E}[f_l(X)]$ of a random variable X taking values $\{0, \ldots, N\}$ with probability p_i.

Conclusion

- Quadratic speedup: this speedup is in fact the best we can attain [Bennett et al., 1997].
- Even if *amplitude amplification* and *estimation* doesn't solve NP-complete problems in polynomial time, we can apply it to more than just search problems, such as Monte Carlo sampling with a non-negligible speedup.

References

Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. (1997).
Strengths and weaknesses of quantum computing.
SIAM journal on Computing, 26(5):1510–1523.

Brassard, G., Hoyer, P., Mosca, M., and Tapp, A. (2002).
Quantum amplitude amplification and estimation.
Contemporary Mathematics, 305:53–74.

Grover, L. K. (1996).
A fast quantum mechanical algorithm for database search.
In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM.

Woerner, S. and Egger, D. J. (2018).
Quantum risk analysis.
arXiv preprint arXiv:1806.06893.