Quantum computation: lecture 10

Grover's algorithm (cont'd)

Reminder: The algorithm starts from state

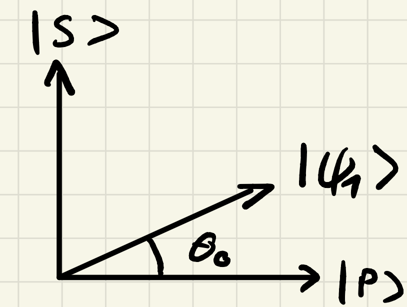
$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = \sqrt{\frac{N-M}{N}} \cdot |P\rangle + \sqrt{\frac{M}{N}} \cdot |s\rangle$$

$$= \cos\theta_0 \, |P\rangle + \sin\theta_0 \, |s\rangle$$

where

$$\begin{cases} |P\rangle = \dfrac{1}{\sqrt{N-M}} \displaystyle\sum_{x \in A^c} |x\rangle \\[2em] |s\rangle = \dfrac{1}{\sqrt{M}} \displaystyle\sum_{x \in A} |x\rangle \end{cases}$$

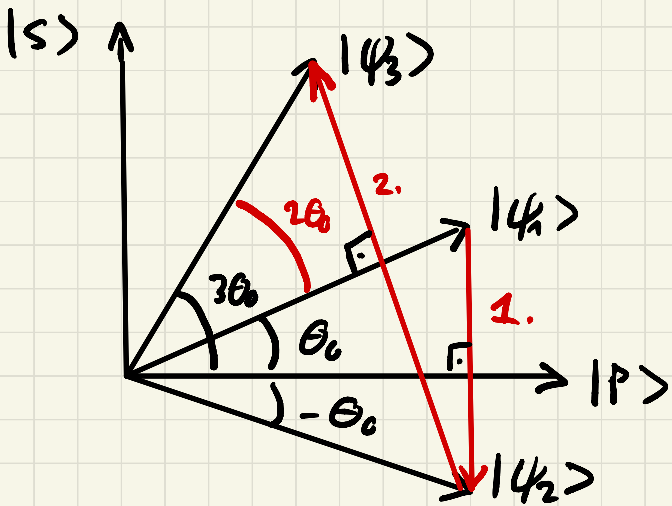
← what we want



Then two gates are used successively:

1. $U_f \longleftrightarrow$ reflection w.r.t. $|P\rangle \quad \rightsquigarrow |\psi_2\rangle$

2. $R \longleftrightarrow$ reflection w.r.t. $|\psi_1\rangle \quad \rightsquigarrow |\psi_3\rangle$

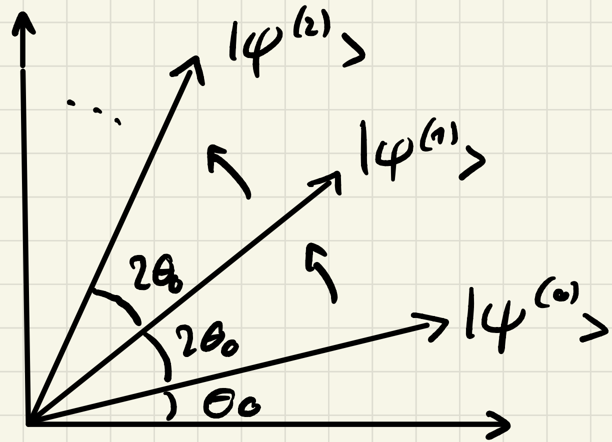


So $G = R \cdot U_f$

$\longleftrightarrow$ rotation of angle $2\theta_0$

Therefore, after k iterations of the $G = R \cdot U_f$ gate, the state becomes

$$|\psi^{(k)}\rangle = \cos((2k+1)\theta_0) \cdot |P\rangle + \sin((2k+1)\cdot\theta_0) \cdot |S\rangle$$



The question is then: how to choose k so as to end up as close as possible to state $|s\rangle$?

1. Let us first assume that M is known.

a) Assume $M=1$ (i.e. $A=\{x^*\}$) and N relatively large:

In this case, $\sin\theta_0 = \frac{1}{\sqrt{N}}$ i.e. $\theta_0 \simeq \frac{1}{\sqrt{N}}$

We target $\sin((2k+1)\theta_0) = 1$, i.e. $(2k+1)\theta_0 = \frac{\pi}{2}$

Therefore, we should choose $k = \left\lfloor \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \right\rfloor$

Let x be the output state. With the above choice of k, we obtain

$$P(x = x^*) = |\langle s | \psi^{(k)} \rangle|^2 = \sin((2k+1)\theta_0)^2$$
$$= 1 - O(\tfrac{1}{N})$$

Grover's algorithm therefore finds $x = x^*$ with high probability in $k = O(\sqrt{N})$ calls to the oracle U_f ($\ll O(N)$ calls classically).

b) <u>Special case $M = \frac{N}{4}$</u>:

In this case, $\sin \theta_0 = \sqrt{\frac{M}{N}} = \frac{1}{2}$ so $\theta_0 = \frac{\pi}{6}$

and therefore:

$$\sin((2k+1)\theta_0) = \frac{\pi}{2} \quad \text{for } k = 1 \,!$$

A single iteration suffices then to reach <u>exactly</u> the state $|s\rangle$, i.e. $P(x \in A) = 1$

c) <u>general M</u>:

- if $M \geq \frac{3}{4} N$, then $P(\text{success}) \geq \frac{3}{4}$ with a classical algorithm and a single call to the oracle f
- assume therefore $M < \frac{3}{4} N$:

this means $\sin(\theta_0) < \frac{\sqrt{3}}{2}$, i.e. $\theta_0 < \frac{\pi}{3}$

choose then $k = \lfloor \frac{\pi}{4\theta_0} \rfloor$

<u>Claim</u>: in this case, $P(\text{success}) \geq \frac{1}{4}$

(so we can make this probability arbitrarily close to 1 by repeating multiple times the experiment)

<u>Proof</u>: by design, $k = \frac{\pi}{4\theta_0} - \frac{1}{2} + \delta$ with $|\delta| < \frac{1}{2}$

so $(2k+1)\theta_0 = \frac{\pi}{2} + 2\delta\theta_0$ with $2|\delta|\theta_0 < 2|\delta|\frac{\pi}{3} < \frac{\pi}{3}$

i.e. $\sin((2k+1)\theta_0)^2 > \sin\left(\frac{\pi}{2} - \frac{\pi}{3}\right)^2 = \sin\left(\frac{\pi}{6}\right)^2 = \frac{1}{4}$

#

2. Let us now assume that M is unknown

How to choose k in this case? Seems like mission impossible... Let us apply the following algorithm:

- choose $x \in \{0,1\}^n$ uniformly at random; if it turns out $x \in A$, then done.
- choose $k \in \{0 \dots \sqrt{N}-1\}$ uniformly at random and apply k iterations of $G = R \cdot U_f$; then output the state measured.

Claim: again, in this case, $P(\text{success}) \geq \frac{1}{4}$!

Proof:

- If $M \geq \frac{3}{4}N$, then the first step is succesful with probability $\geq \frac{3}{4} \geq \frac{1}{4}$. Assume therefore $M < \frac{3}{4}N$.
- In this case, we have

$$P(\text{success}) = \sum_{k=0}^{\sqrt{N}-1} P(\text{success} \mid K=k) \cdot \underbrace{P(K=k)}_{= 1/\sqrt{N}}$$

That said, $P(\text{success} \mid K=k) = \sin((2k+1)\theta_0)^2$

So $$P(\text{success}) = \frac{1}{\sqrt{N}} \sum_{k=0}^{\sqrt{N}-1} \sin((2k+1)\theta_0)^2$$

$$= \frac{1}{2} - \frac{\sin(4\theta_0\sqrt{N})}{4\sqrt{N}\,\sin(2\theta_0)} \quad \text{(trigonometric identity)}$$

But $|\sin(4\theta_0\sqrt{N})| < 1$

and $$\sin(2\theta_0) = 2\sin\theta_0 \cdot \cos\theta_0 = 2\sqrt{\frac{M}{N}} \cdot \overbrace{\sqrt{\frac{N-M}{N}}}^{>\sqrt{\frac{1}{4}}} > \sqrt{\frac{M}{N}} \geq \frac{1}{\sqrt{N}}$$

So $$P(\text{success}) \geq \frac{1}{2} - \frac{1}{4} = \frac{1}{4} \quad \#$$

Conclusion

Even if M is not known, using Grover's circuit a random number of times ($< \sqrt{N}$) outputs a state $x \in A$ with probability $\geq \frac{1}{4}$

And by repeating the experiment, this success probability can be amplified arbitrarily close to 1.

Applications

As mentioned last week, we should be able to build the circuit U_f ...

1. SAT formulas

Let us consider a Boolean function of the form:

OR NOT AND

$$f(\underbrace{x_1, x_2, x_3, x_4}_{n=4 \text{ variables here}}) = (x_1 \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_3 \vee x_4)$$

Such Boolean functions are called SAT formulas (SAT as in satisfiability). When n is large, and the number m of clauses (= expressions in parentheses) of the formula is also large, it is unclear how to find value(s) of x such that $f(x)=1$. Nevertheless, it is straightforward to implement the circuit U_f associated to f.

2. Factoring (again)

There is a (non-trivial) way to apply Grover's algorithm in order to reduce the search space for factoring large values of N into products of primes.
The improvement is not exponential, but still quadratic, which is noticeable.