An Introduction to Quantum Computing

Lecture 14:

Quantum Counting

Paolo Zuliani

Dipartimento di Informatica
Università di Roma “La Sapienza”, Rome, Italy

Agenda

- Counting Problem
- Quantum Search Recap
- Quantum Counting Algorithm

Counting Problem

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
78	655	***9797***	3249	6	13	877	56	8789	10	999	1548	***354***	75	1875	9

An array of N elements of which M are "solution" elements. Grover's algorithm can find the index of a solution element with only $O(\sqrt{N})$ array queries.

Counting Problem

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
78	655	***9797***	3249	6	13	877	56	8789	10	999	1548	***354***	75	1875	9

An array of N elements of which M are "solution" elements. Grover's algorithm can find the index of a solution element with only $O(\sqrt{N})$ array queries.

Definition (Counting Problem)

Find out M, *i.e.*, how many solution elements are contained in the array.

Counting Problem

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
78	655	*9797*	3249	6	13	877	56	8789	10	999	1548	*354*	75	1875	9

An array of N elements of which M are "solution" elements. Grover's algorithm can find the index of a solution element with only $O(\sqrt{N})$ array queries.

Definition (Counting Problem)

Find out M, *i.e.*, how many solution elements are contained in the array.

Classically: $\Theta(N)$ accesses to the array.

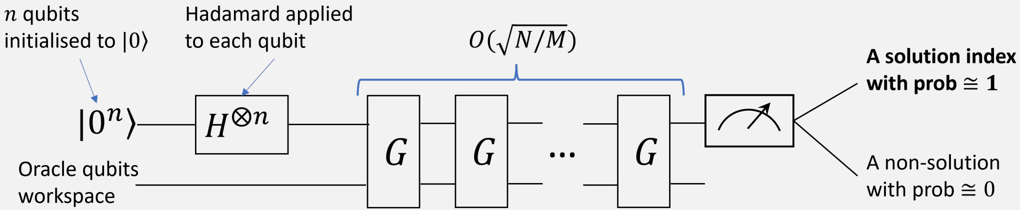
Quantumly: $O(\sqrt{N})$ accesses suffices, with high probability.

Counting Problem

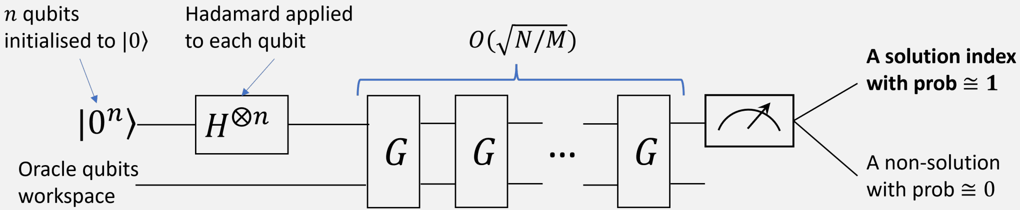
Applications of counting:

1. using Grover's search algorithm without knowing M (the number of solutions) in advance (first get an estimate for M by counting, then use Grover);
2. decide whether a problem has a solution or not (just compute the solutions count and compare it to zero);
3. computing the average value of a function, integration, solving differential equations, ...

Quantum Search Recap



Quantum Search Recap



After the Hadamards, the state of the top register is:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

The Grover operator G is:

$$G = (2\,|\psi\rangle\langle\psi| - I)O_f$$

where the "oracle" O_f flips the sign of the amplitudes of the solution elements.

Quantum Search Recap

Let S be the set of solution indices, and define the two orthonormal vectors:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \bar{S}} |x\rangle \qquad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle$$

Quantum Search Recap

Let S be the set of solution indices, and define the two orthonormal vectors:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \bar{S}} |x\rangle \qquad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle$$

We can the rewrite ψ as:

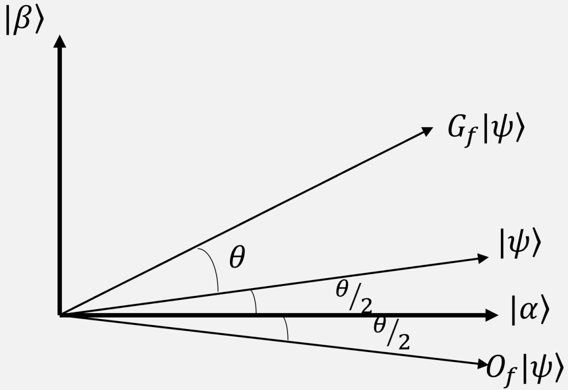
$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$$

and by choosing θ such that $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$ we can write

$$|\psi\rangle = \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle$$

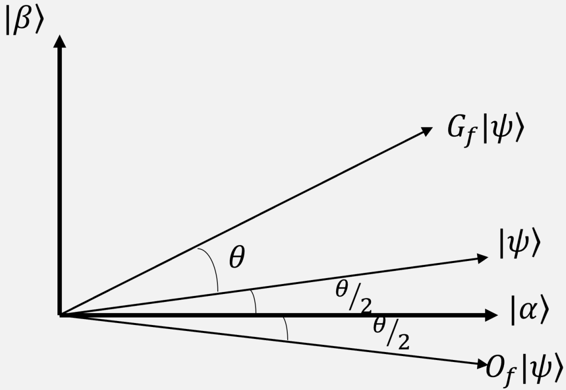
Quantum Search Recap

The Grover iteration G corresponds to a rotation of an angle θ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$.



Quantum Search Recap

The Grover iteration G corresponds to a rotation of an angle θ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$.



In general, for $k = 0, 1, 2, \ldots$

$$G^k |\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

Quantum Search

Proposition

The Grover operator G can be written, in the basis $\{|\alpha\rangle, |\beta\rangle\}$, as the matrix:

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

with $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$.

Quantum Search

Proposition

The Grover operator G can be written, in the basis $\{|\alpha\rangle, |\beta\rangle\}$, as the matrix:

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

with $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$.

Proof: we need to compute $G|v\rangle$ for a generic $|v\rangle = a|\alpha\rangle + b|\beta\rangle$; recall that $G = (2|\psi\rangle\langle\psi| - I)O_f$.

Quantum Search

Proposition

The Grover operator G can be written, in the basis $\{|\alpha\rangle, |\beta\rangle\}$, as the matrix:

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

with $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$.

Proof: we need to compute $G|v\rangle$ for a generic $|v\rangle = a|\alpha\rangle + b|\beta\rangle$; recall that $G = (2|\psi\rangle\langle\psi| - I)O_f$.

$|\psi\rangle\langle\psi| = (\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle)(\cos\frac{\theta}{2}\langle\alpha| + \sin\frac{\theta}{2}\langle\beta|)$.

Quantum Search

Proposition

The Grover operator G can be written, in the basis $\{|\alpha\rangle, |\beta\rangle\}$, as the matrix:

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

with $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$.

Proof: we need to compute $G|v\rangle$ for a generic $|v\rangle = a|\alpha\rangle + b|\beta\rangle$; recall that $G = (2|\psi\rangle\langle\psi| - I)O_f$.

$|\psi\rangle\langle\psi| = (\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle)(\cos\frac{\theta}{2}\langle\alpha| + \sin\frac{\theta}{2}\langle\beta|)$.

O_f flips the sign of the solution indices, so $O_f|v\rangle = a|\alpha\rangle - b|\beta\rangle$. Thus

$$G|v\rangle = (2|\psi\rangle\langle\psi| - I)(a|\alpha\rangle - b|\beta\rangle) = 2|\psi\rangle\langle\psi|(a|\alpha\rangle - b|\beta\rangle) - (a|\alpha\rangle - b|\beta\rangle)$$

Quantum Search

$$G|v\rangle = 2|\psi\rangle\langle\psi|\,(a|\alpha\rangle - b|\beta\rangle) - (a|\alpha\rangle - b|\beta\rangle)$$

Quantum Search

$$
\begin{aligned}
G\,|v\rangle &= 2\,|\psi\rangle\!\langle\psi|\,(a\,|\alpha\rangle - b\,|\beta\rangle) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= 2\,|\psi\rangle\,(\cos\frac{\theta}{2}\,\langle\alpha| + \sin\frac{\theta}{2}\,\langle\beta|)(a\,|\alpha\rangle - b\,|\beta\rangle) - (a\,|\alpha\rangle - b\,|\beta\rangle)
\end{aligned}
$$

Quantum Search

$$
\begin{aligned}
G |v\rangle &= 2 |\psi\rangle\langle\psi| (a |\alpha\rangle - b |\beta\rangle) - (a |\alpha\rangle - b |\beta\rangle) \\
&= 2 |\psi\rangle (\cos\frac{\theta}{2} \langle\alpha| + \sin\frac{\theta}{2} \langle\beta|)(a |\alpha\rangle - b |\beta\rangle) - (a |\alpha\rangle - b |\beta\rangle) \\
&= 2 |\psi\rangle (a \cos\frac{\theta}{2} - b \sin\frac{\theta}{2}) - (a |\alpha\rangle - b |\beta\rangle)
\end{aligned}
$$

Quantum Search

$$
\begin{aligned}
G|v\rangle &= 2|\psi\rangle\langle\psi|(a|\alpha\rangle - b|\beta\rangle) - (a|\alpha\rangle - b|\beta\rangle) \\
&= 2|\psi\rangle(\cos\frac{\theta}{2}\langle\alpha| + \sin\frac{\theta}{2}\langle\beta|)(a|\alpha\rangle - b|\beta\rangle) - (a|\alpha\rangle - b|\beta\rangle) \\
&= 2|\psi\rangle(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a|\alpha\rangle - b|\beta\rangle) \\
&= 2(\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle)(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a|\alpha\rangle - b|\beta\rangle)
\end{aligned}
$$

Quantum Search

$$
\begin{aligned}
G\,|v\rangle &= 2\,|\psi\rangle\langle\psi|\,(a\,|\alpha\rangle - b\,|\beta\rangle) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= 2\,|\psi\rangle\,(\cos\frac{\theta}{2}\,\langle\alpha| + \sin\frac{\theta}{2}\,\langle\beta|)(a\,|\alpha\rangle - b\,|\beta\rangle) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= 2\,|\psi\rangle\,(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= 2(\cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle)(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= (2\cos\frac{\theta}{2}(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - a)\,|\alpha\rangle + (2\sin\frac{\theta}{2}(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - b)\,|\beta\rangle
\end{aligned}
$$

Quantum Search

$$
\begin{aligned}
G\,|v\rangle &= 2\,|\psi\rangle\langle\psi|\,(a\,|\alpha\rangle - b\,|\beta\rangle) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= 2\,|\psi\rangle\,(\cos\frac{\theta}{2}\,\langle\alpha| + \sin\frac{\theta}{2}\,\langle\beta|)(a\,|\alpha\rangle - b\,|\beta\rangle) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= 2\,|\psi\rangle\,(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= 2(\cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle)(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a\,|\alpha\rangle - b\,|\beta\rangle) \\
&= (2\cos\frac{\theta}{2}(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - a)\,|\alpha\rangle + (2\sin\frac{\theta}{2}(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - b)\,|\beta\rangle \\
&= (a\cos\theta - b\sin\theta)\,|\alpha\rangle + (a\sin\theta + b\cos\theta)\,|\beta\rangle = \left|v'\right\rangle
\end{aligned}
$$

Quantum Search

$$
\begin{aligned}
G|v\rangle &= 2|\psi\rangle\langle\psi|(a|\alpha\rangle - b|\beta\rangle) - (a|\alpha\rangle - b|\beta\rangle) \\
&= 2|\psi\rangle(\cos\frac{\theta}{2}\langle\alpha| + \sin\frac{\theta}{2}\langle\beta|)(a|\alpha\rangle - b|\beta\rangle) - (a|\alpha\rangle - b|\beta\rangle) \\
&= 2|\psi\rangle(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a|\alpha\rangle - b|\beta\rangle) \\
&= 2(\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle)(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - (a|\alpha\rangle - b|\beta\rangle) \\
&= (2\cos\frac{\theta}{2}(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - a)|\alpha\rangle + (2\sin\frac{\theta}{2}(a\cos\frac{\theta}{2} - b\sin\frac{\theta}{2}) - b)|\beta\rangle \\
&= (a\cos\theta - b\sin\theta)|\alpha\rangle + (a\sin\theta + b\cos\theta)|\beta\rangle = |v'\rangle
\end{aligned}
$$

Now,

$$
\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a\cos\theta - b\sin\theta \\ a\sin\theta + b\cos\theta \end{pmatrix}
$$

Quantum Counting

Note that G has only two eigenvectors. (Why?)

Quantum Counting

Note that G has only two eigenvectors. (Why?)

The eigenvalues of G (Exercise!) are $e^{i\theta}$ and $e^{i(2\pi-\theta)}$, where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.

Quantum Counting

Note that G has only two eigenvectors. (Why?)

The eigenvalues of G (Exercise!) are $e^{i\theta}$ and $e^{i(2\pi-\theta)}$, where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.

M is encoded in the phase of the eigenvalues of the *unitary* operator G:

$$\Downarrow$$

we can use QPE to estimate the phase and thus M!!

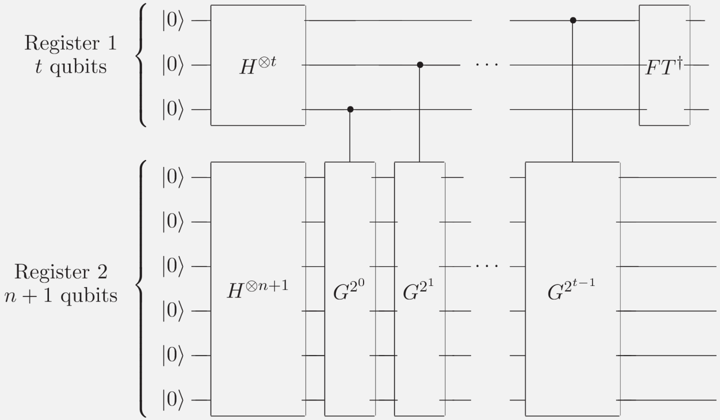
Quantum Counting

[We double the array length to $2N$, so to ensure $M \leqslant \frac{N}{2}$.]

Quantum Counting

[We double the array length to $2N$, so to ensure $M \leqslant \frac{N}{2}$.]

We estimate θ (where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{2N}}$) to m bits of accuracy with probability $1-\epsilon$, using:



$$\begin{cases} t = m + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil \\ N = 2^n \end{cases}$$

Quantum Counting

The quantum counting circuit estimates θ or $2\pi - \theta$ to accuracy $|\Delta\theta| \leqslant 2^{-m}$ (with probability at least $1 - \epsilon$.)

Quantum Counting

The quantum counting circuit estimates θ or $2\pi - \theta$ to accuracy $|\Delta\theta| \leqslant 2^{-m}$ (with probability at least $1 - \epsilon$.)

Recall that $\sin \frac{\theta}{2} = \sqrt{\frac{M}{2N}}$. How does an error on θ affect the estimate of M?

Quantum Counting

The quantum counting circuit estimates θ or $2\pi - \theta$ to accuracy $|\Delta\theta| \leqslant 2^{-m}$ (with probability at least $1 - \epsilon$.)

Recall that $\sin\frac{\theta}{2} = \sqrt{\frac{M}{2N}}$. How does an error on θ affect the estimate of M?

One can show that:

$$|\Delta M| < (2\sqrt{MN} + \frac{N}{2^{m+1}})2^{-m}$$

Choosing, *e.g.*, $m = \lceil n/2 \rceil + 1$ and $\epsilon = 1/6$, we get $t = \lceil n/2 \rceil + 3$ and $|\Delta M| < \sqrt{\frac{M}{2} + \frac{1}{4}} = O(\sqrt{M})$ with $O(2^t) = O(\sqrt{N})$ iterations of the Grover operator, *i.e.*, array accesses.

Classically, we would need $O(N)$ accesses.

Quantum Counting

Quantum counting can be used to decide whether $M = 0$ or not:

- if $M = 0$ then $|\Delta M| < \frac{1}{4}$, so we get the estimate 0 with probability at least $5/6$;
- if $M \neq 0$ then we get a non-null estimate with probability at least $5/6$.

Quantum Counting

Quantum counting can be used to decide whether $M = 0$ or not:

- if $M = 0$ then $|\Delta M| < \frac{1}{4}$, so we get the estimate 0 with probability at least $5/6$;
- if $M \neq 0$ then we get a non-null estimate with probability at least $5/6$.

Also, we can use quantum counting to find a solution to a search problem when M is not known.