Lecture 24

Unstructured search

We consider a database that consists of various locations, one of which is marked. Suppose that

* the database requires n bits
* the total number of database locations is $N = 2^n$
* the database locations are labeled

$$x = 0, 1, 2, \ldots, N-1$$

In terms of locating the marked item, we consider the situation:

* there is exactly one marked item
* the database has no structure, meaning that any location is just as likely as any other.
* there is an oracle function that can identify whether any given location is marked or not:

$$f(x) = \begin{cases} 0 & \text{if } x \text{ is not marked} \\ 1 & \text{if } x \text{ is marked.} \end{cases}$$

For example with three bits a possible oracle is

$$f(x_2, x_1, x_0) = x_2 x_1 x_0 \oplus x_2 x_0 \oplus x_1 x_0 \oplus x_0$$

and it emerges that the location of the marked item is

$$x_2 = 0 \qquad x_1 = 0 \qquad x_0 = 1$$

The <u>classical strategy</u> for locating the marked item is

Repeatedly query the oracle

$f(0) = ?$

$f(1) = ?$

$f(2) = ?$

$f(3) = ?$

Halt when one attains $f(x) = 1$. This locates the marked item

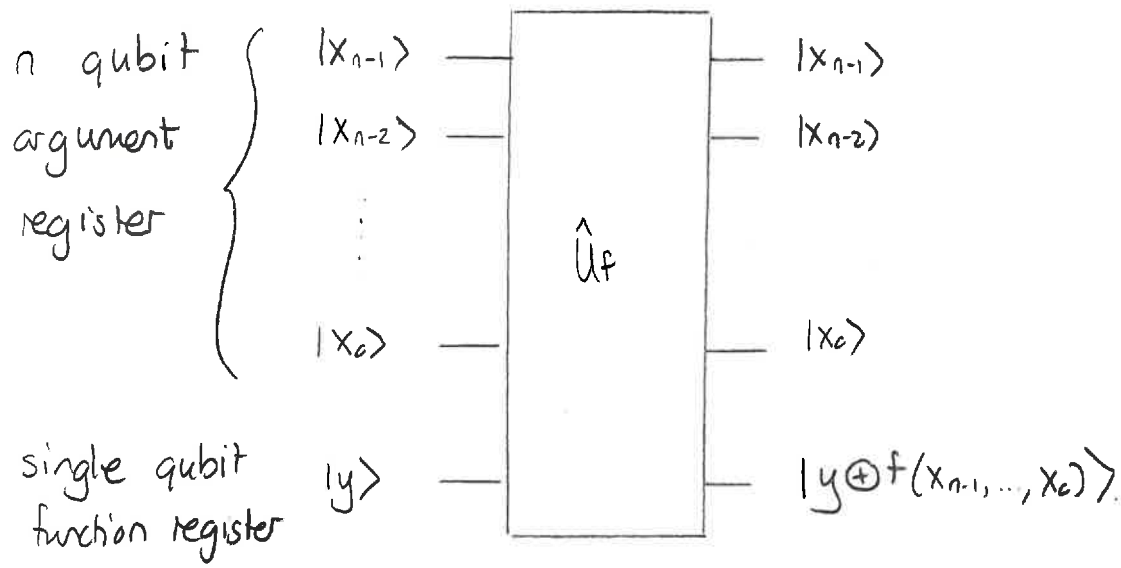
We would like to locate the marked item with the fewest number of oracle queries. A detailed analysis shows:

In order to locate the marked item with certainty one needs $N-1$ oracle queries in the worst case.

On average one needs about $N/2$ oracle queries to locate the marked item

Quantum oracle for database search

We can assume the usual type of quantum oracle which acts on $n+1$ qubits



We use the "decimal" notation

$$|x\rangle_d = |\underbrace{x_{n-1} \dots x_0}\rangle$$

decimal x = binary rep $x_{n-1} \dots x_0$

and then

$$|x\rangle_d |y\rangle \xrightarrow{\hat{U}_f} |x\rangle_d |y \oplus f(x)\rangle$$

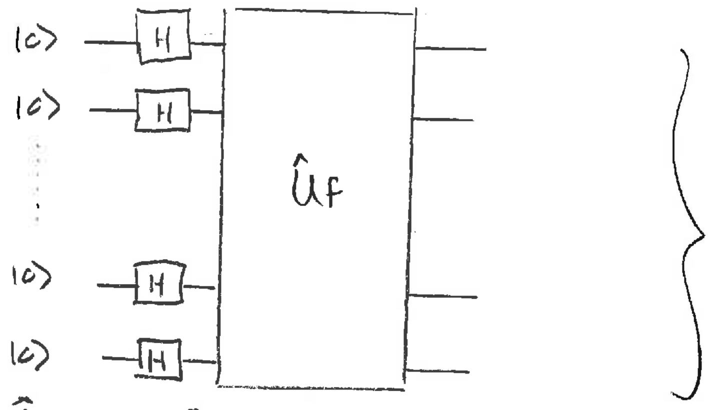
Now with $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ we can show that

$$|x\rangle_d |-\rangle = (-1)^{f(x)} |x\rangle_d |-\rangle.$$

Thus we use a modified n-qubit oracle in order to analyze the search:

$$|x\rangle_d \xrightarrow{\hat{U}_f} (-1)^{f(x)} |x\rangle_d$$

As with other quantum algorithms, we can supply a superposition of states to the oracle. Thus with a single qubit Hadamard gate on each qubit



$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle_d$$

$$|\Psi_0\rangle = |0\rangle_d$$

$$\left(\frac{1}{\sqrt{2}}\right)^n \sum |x\rangle_d = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_d$$

So for example with

$$f(x_2, x_1, x_0) = x_2 x_1 x_0 \oplus x_2 x_0 \oplus x_1 x_0 \oplus x_0$$

we get that, after the oracle, the state is

$$\frac{1}{\sqrt{8}} \left\{ |0\rangle_d - |1\rangle_d + |2\rangle_d + |3\rangle_d + |4\rangle_d + |5\rangle_d + |6\rangle_d + |7\rangle_d \right\}$$

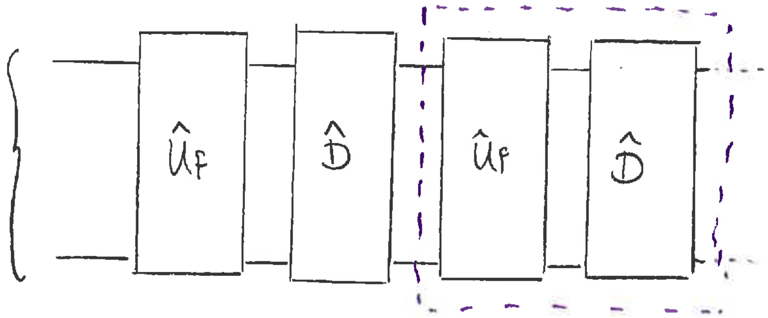
and a computational basis measurement would not reveal anything about the marked location.

I turns out that if we apply a carefully constructed unitary that does not depend on the particular search oracle and iterate the entire process we can eventually locate the marked item.

Iteration process

We will define an "inversion - about - the - average" operation $\hat{D}$ and then do:

$\frac{1}{\sqrt{N}} \sum |x\rangle_d$



$$\hat{G} = \hat{D}\,\hat{U}_f$$

where we repeatedly apply the pair of operations, which are jointly denoted $\hat{G} = \hat{D}\,\hat{U}_f$.

To do so, we define the inversion - about - the - average operation as follows.

If

$$|\psi\rangle = \alpha_0 |0\rangle_d + \alpha_1 |1\rangle_d + \dots + \alpha_{N-1} |N-1\rangle_d$$

then

$$\hat{D}|\psi\rangle = \beta_0 |0\rangle_d + \beta_1 |1\rangle_d + \dots + \beta_{N-1} |N-1\rangle_d$$

where

$$\beta_x = -\alpha_x + 2\langle\alpha\rangle$$

and $\langle\alpha\rangle = \frac{1}{N}(\alpha_0 + \dots + \alpha_{N-1})$

1 Invesrion about the average example

Let

$$|\Psi\rangle = \frac{1}{2}\Big(|0\rangle_d + |1\rangle_d - |2\rangle_d + |3\rangle_d\Big)$$

and $\hat{D}$ be the inversion about the average operation. Determine $\hat{D}\,|\Psi\rangle$.

Answer: Here

$$\alpha_0 = \frac{1}{2}$$
$$\alpha_1 = 1/2$$
$$\alpha_2 = -1/2$$
$$\alpha_3 = 1/2$$

and

$$\langle\alpha\rangle = \frac{1}{4}\left(\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3\right) = \frac{1}{4}\left(\frac{1}{2} + \frac{1}{2} \cancel{-\frac{1}{2}} \cancel{+\frac{1}{2}}\right) = \frac{1}{4}$$

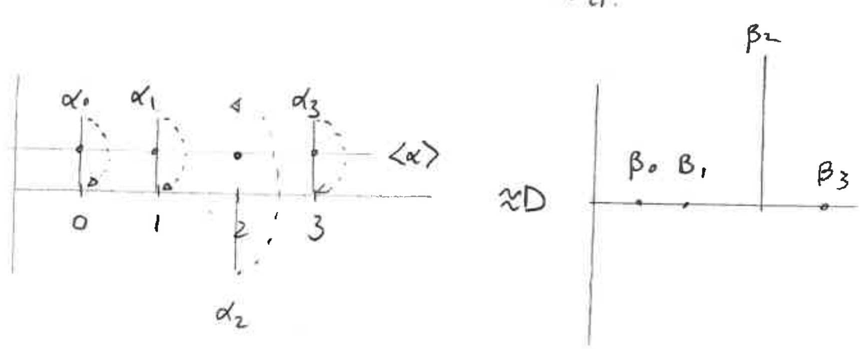
So

$$\beta_0 = -\alpha_0 + 2\langle\alpha\rangle = -1/2 + 2\,\frac{1}{4} = 0$$
$$\beta_1 = -\alpha_1 + 2\langle\alpha\rangle = -\frac{1}{2} + 2\,\frac{1}{4} = 0$$
$$\beta_2 = -\alpha_2 + 2\langle\alpha\rangle = +\frac{1}{2} + 2\,\frac{1}{4} = 1$$
$$\beta_3 = -\alpha_3 + 2\langle\alpha\rangle = -\frac{1}{2} + 2\,\frac{1}{4} = 0$$

Thus:

$$\hat{D}\,|\Psi\rangle = 0|0\rangle_d + 0|1\rangle_d + 1|2\rangle_d + |3\rangle_d = |2\rangle_d.$$

Note that



2 Inversion about the average: ~~uintary~~ unitary?

Let

$$|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle_d .$$

a) By acting on an arbitrary state

$$|\Psi\rangle = \sum_x \alpha_x |x\rangle_d$$

show that

$$\hat{D} = 2|\Phi\rangle\langle\Phi| - \hat{I}.$$

b) Show that $\hat{D}$ is unitary.

Solution

a) $$\hat{D}|\Psi\rangle = 2|\Phi\rangle\langle\Phi|\Psi\rangle - |\Psi\rangle$$

Now $$\langle\Phi|\Psi\rangle = \frac{1}{\sqrt{N}}\left\{{}_d\langle 0| + {}_d\langle 1| + \dots + {}_d\langle N-1|\right\}\left\{\alpha_0|0\rangle_d + \dots + \alpha_{N-1}|N-1\rangle_d\right\}$$

$$= \frac{1}{\sqrt{N}}(\alpha_0 + \dots + \alpha_{N-1}) = \langle\alpha\rangle\sqrt{N}$$

Thus $$\hat{D}|\Psi\rangle = 2|\Phi\rangle\langle\alpha\rangle\sqrt{N} - |\Psi\rangle$$

$$= 2\langle\alpha\rangle\cancel{\sqrt{N}}\frac{1}{\cancel{\sqrt{N}}}\sum_x |x\rangle_d - \sum_x \alpha_x|x\rangle_d$$

$$= \sum_x \left(2\langle\alpha\rangle - \alpha_x\right)|x\rangle_d$$

$$= \sum_x \beta_x|x\rangle_d$$

where $\beta_x = 2\langle\alpha\rangle - \alpha_x$ This is what is required.

b) $$\hat{D}^{+} = \left(2|\Phi\rangle\langle\Phi|\right)^{+} - I^{+}$$

$$= 2|\Phi\rangle\langle\Phi| - \hat{I}$$

Then:

$$\hat{D}^{+}\hat{D} = \left(2|\Phi\rangle\langle\Phi| - \hat{I}\right)\left(2|\Phi\rangle\langle\Phi| - \hat{I}\right)$$

$$= 4|\Phi\rangle\overset{1}{\cancel{\langle\Phi|\Phi\rangle}}\langle\Phi| - 2|\Phi\rangle\langle\Phi| \times 2 + \hat{I}^{2}$$

$$= \hat{I}$$

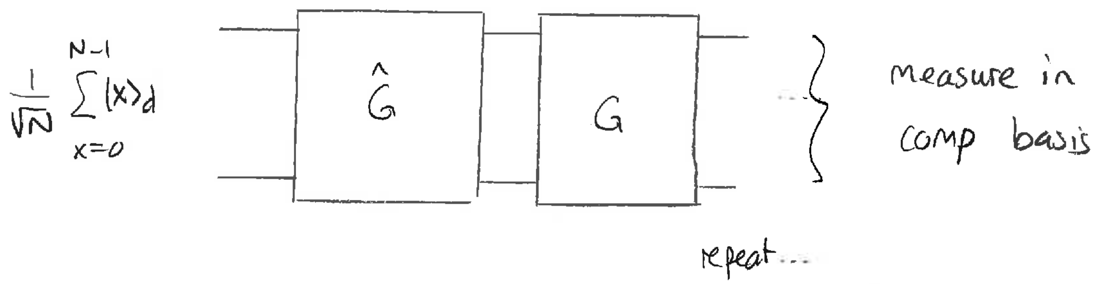
So it is unitary.

Grover's search algorithm

Grover's algorithm consists of repeatedly applying

$$\hat{G} = \hat{D}\,\hat{U}_f$$

until the coefficient of the computational basis state associated with the marked location becomes sufficiently large.



Then a measurement in the computational basis will yield the marked item's location with high probability.

3 Grover's algorithm for two qubits

Suppose that, for a two bit database search, the location of the marked item is $x = 3$.

a) Evaluate the state of the system after a single iteration of $\hat{G}$. What would a computational basis measurement yield at this point?

b) Evaluate the state of the system after two iterations of $\hat{G}$. What would a computational basis measurement yield at this point?

Answer:

a) Initial state

$$|\Psi_0\rangle \equiv \frac{1}{\sqrt{N}} \sum |x\rangle_d = \frac{1}{\sqrt{4}} \sum |x\rangle_d$$

$$|\Psi_0\rangle = \frac{1}{2} \left\{ |0\rangle_d + |1\rangle_d + |2\rangle_d + |3\rangle_d \right\}$$

Then let $|\Psi_1\rangle = \hat{G}|\Psi_0\rangle$. Now

$$\hat{U}_f |\Psi_0\rangle = \frac{1}{2}\left\{ |0\rangle_d + |1\rangle_d + |2\rangle_d - |3\rangle_d \right\}$$

and for $\hat{D}$ $\quad \langle\alpha\rangle = \frac{1}{4}$

Thus if $\alpha_x = \frac{1}{2}$ then $\beta_x = 2\langle\alpha\rangle - \alpha_x = 0$

if $\alpha_x = -\frac{1}{2}$ then $\beta_x = 2\langle\alpha\rangle - \alpha_x = 1$

So $\hat{D}\hat{U}_f|\Psi_0\rangle = |3\rangle_d$

$\Rightarrow \quad |\Psi_1\rangle = |3\rangle_d$

A comp basis measurement would yield $x=3$ with certainty $\rightarrow$ reveals marked item

b) $$\hat{U}_f |\Psi_1\rangle = -|3\rangle_d$$

and we need

$$\hat{D}\hat{U}_f|\Psi_1\rangle$$

Here $\langle\alpha\rangle = -\frac{1}{4}$. Thus

if $\alpha_x = 0$ then $\beta_x = 2\langle\alpha\rangle - \alpha_x = -\frac{1}{2}$

$\alpha_x = -1$ " $\beta_x = 2\langle\alpha\rangle - \alpha_x = \frac{1}{2}$

$$\Rightarrow \hat{D}\hat{U}_f|\Psi_1\rangle = \frac{1}{2}\left(-|0\rangle_d - |1\rangle_d - |2\rangle_d + |3\rangle_d\right)$$

$$= (-1)\,\frac{1}{2}\left(|0\rangle_d + |1\rangle_d + |2\rangle_d - |3\rangle_d\right)$$

comp basis measurement would yield $x=3$ with prob $1/4$

$x \neq 3$ " " $3/4$