Quantum Search Algorithms

Consider shortest route problem:

N cities on a map.

What is the shortest route that takes in all N cities?

Classical Answer: Try all possible N routes - $O(N)$ operations

Quantum Answer: Grover's algorithm - $O(\sqrt{N})$ operations.

The Oracle

Consider search space of N elements, with indeces, 0 to $N-1$.

Let $N = 2^n$.

Let there be M solutions, $1 \leq M \leq N$.

Define $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$,

$f(x) = 1$ if x is a solution, otherwise $f(x) = 0$.

We have an oracle (black box).

It can recognize solutions to the search problem.

... Recognition signalled by making use of an oracle qubit.

i.e. the oracle is a unitary operator, O, where

$$O: |x\rangle|q\rangle \rightarrow |x\rangle|q \oplus f(x)\rangle,$$

where $|q\rangle$ is a single qubit

To check whether x is a solution, prepare $|x\rangle|0\rangle$, apply O, check to see if oracle qubit is 1

Instead, apply O to $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$.

Thus:

$$O : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \rightarrow (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

.... observe ... only the phase is changed.
... the oracle qubit is unchanged.

From now on we ignore the oracle qubit:

$$O : |x\rangle \longrightarrow (-1)^{f(x)}|x\rangle.$$

For an N item search with M solutions, we need only apply the search oracle $O(\sqrt{N/M})$ times

Example, Factoring:

Let $m = pq$, p and q large primes.

Classically: Search all numbers from 2 to $m^{\frac{1}{2}}$ using trial division:

$O(m^{\frac{1}{2}})$ operations.

Quantum: Define $f(x)=1$ if x divides m, $f(x)=0$ otherwise.

Construct quantum circuit taking

$$|x\rangle|q\rangle \rightarrow |x\rangle|q \oplus f(x)\rangle.$$

Key Point: without knowing the factors of m, we can construct an oracle recognizing a solution when it sees one..

... using a quantum version of trial division.

Complexity?

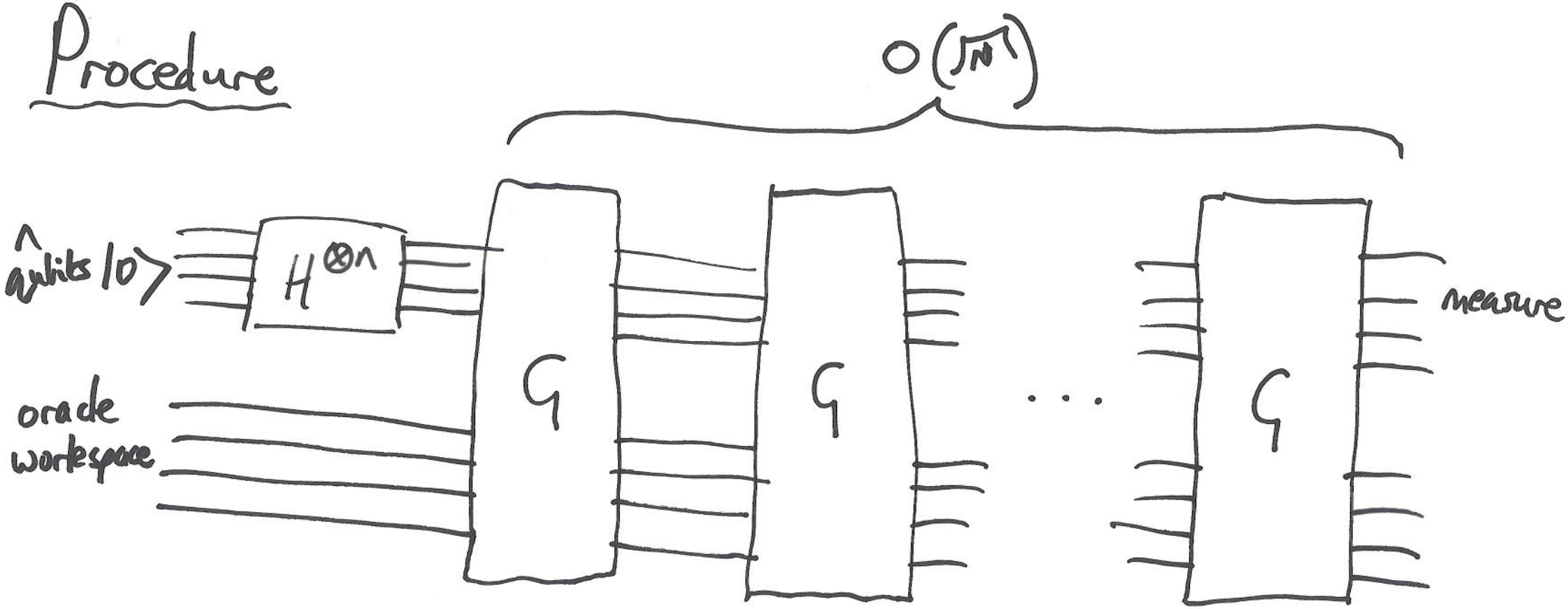
Using the oracle with the quantum search algorithm, 2 to $m^{\frac{1}{2}}$ can be searched using

$O(m^{\frac{1}{4}})$ operations.

.... instead of $O(m^{\frac{1}{2}})$ classically.

... but classical algorithms known which work much faster.

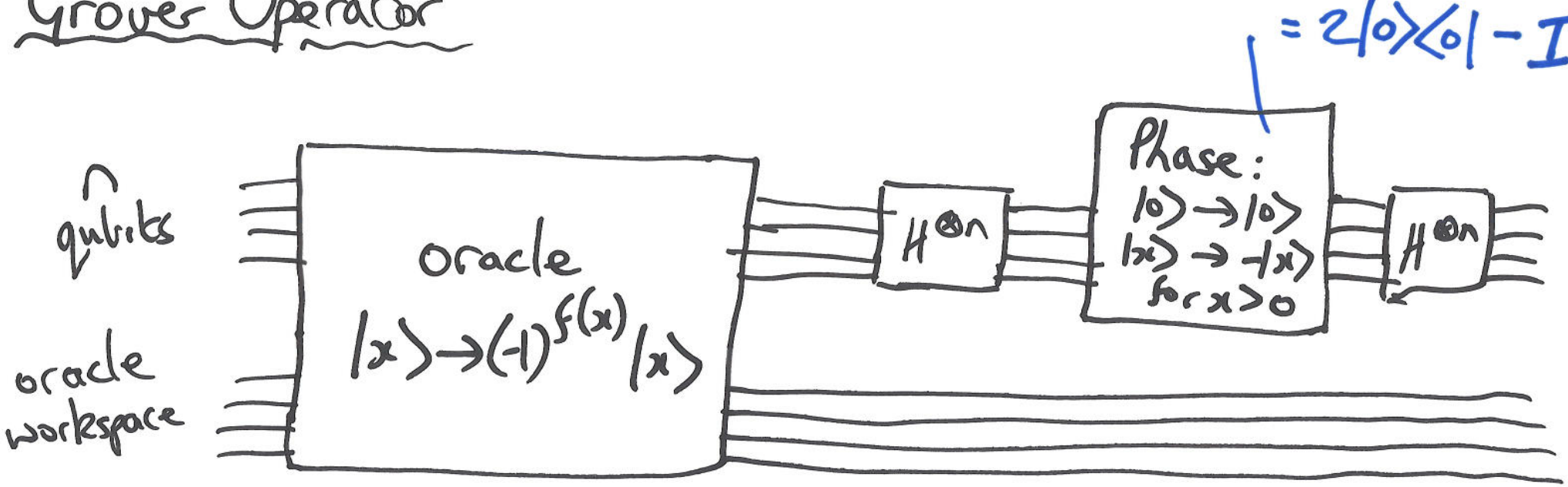
Procedure



After $H^{\otimes n}$, $|k\rangle = \frac{1}{N^{k_2}} \sum_{x=0}^{N-1} |x\rangle$.

G is the Grover iteration or Grover operator.

Grover Operator



Grover iteration:

1. Apply oracle O
2. Apply $H^{\otimes n}$
3. Conditional phase shift: every state except $|0\rangle$ receives phase shift of -1.
   $|x\rangle \to -(-1)^{\delta_{x0}}|x\rangle$
4. Apply $H^{\otimes n}$

Efficiency?

$H^{\otimes n}$ requires $n = \log(N)$ operations

conditional phase shift requires $O(n)$ gates

oracle – depends on application
... a single oracle call.

Observe:

$$H^{\otimes n} \cdot \underset{\text{phase shift}}{\text{conditional}} \cdot H^{\otimes n}$$

$$= H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I,$$

where $|\psi\rangle = \frac{1}{N^{\frac{1}{2}}} \sum_{x=0}^{N-1} |x\rangle$.

Observe:

$$(2|\psi\rangle\langle\psi| - I)\left(\Sigma_k \alpha_k |k\rangle\right)$$



inversion about mean

$$= \sum_k \left[-\alpha_k + 2\langle\alpha\rangle\right]|k\rangle,$$

where $\langle\alpha\rangle = \sum_k \alpha_k / N$.

Geometric Visualization

Observe: $G = (2|\psi\rangle\langle\psi| - I)O$.

. . . rotation in two-dimensional space spanned by $|\psi\rangle$ and the state consisting of a uniform superposition of search solutions.

Let $\sum_x'$ denote a sum over all search solutions, x.

Let $\sum_x''$ denote a sum over all search non-solutions.

Let $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$

$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_x' |x\rangle.$

Then,

$$|\psi\rangle = \frac{1}{N^{\frac{1}{2}}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle,$$

... so initial state, $|\psi\rangle$, is spanned by $|\alpha\rangle$ and $|\beta\rangle$.

Effect of G

Oracle O performs reflection about $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$:

$$O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle.$$

$(2|\psi\rangle\langle\psi| - I)$ performs reflection about $|\psi\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$

Therefore,

$(2|\psi\rangle\langle\psi| - I)O$ is a rotation. ← product of two reflections.

Therefore ...

If $G|\psi\rangle$ is a rotation,

then

$G^k|\psi\rangle$ is a rotation

... in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$

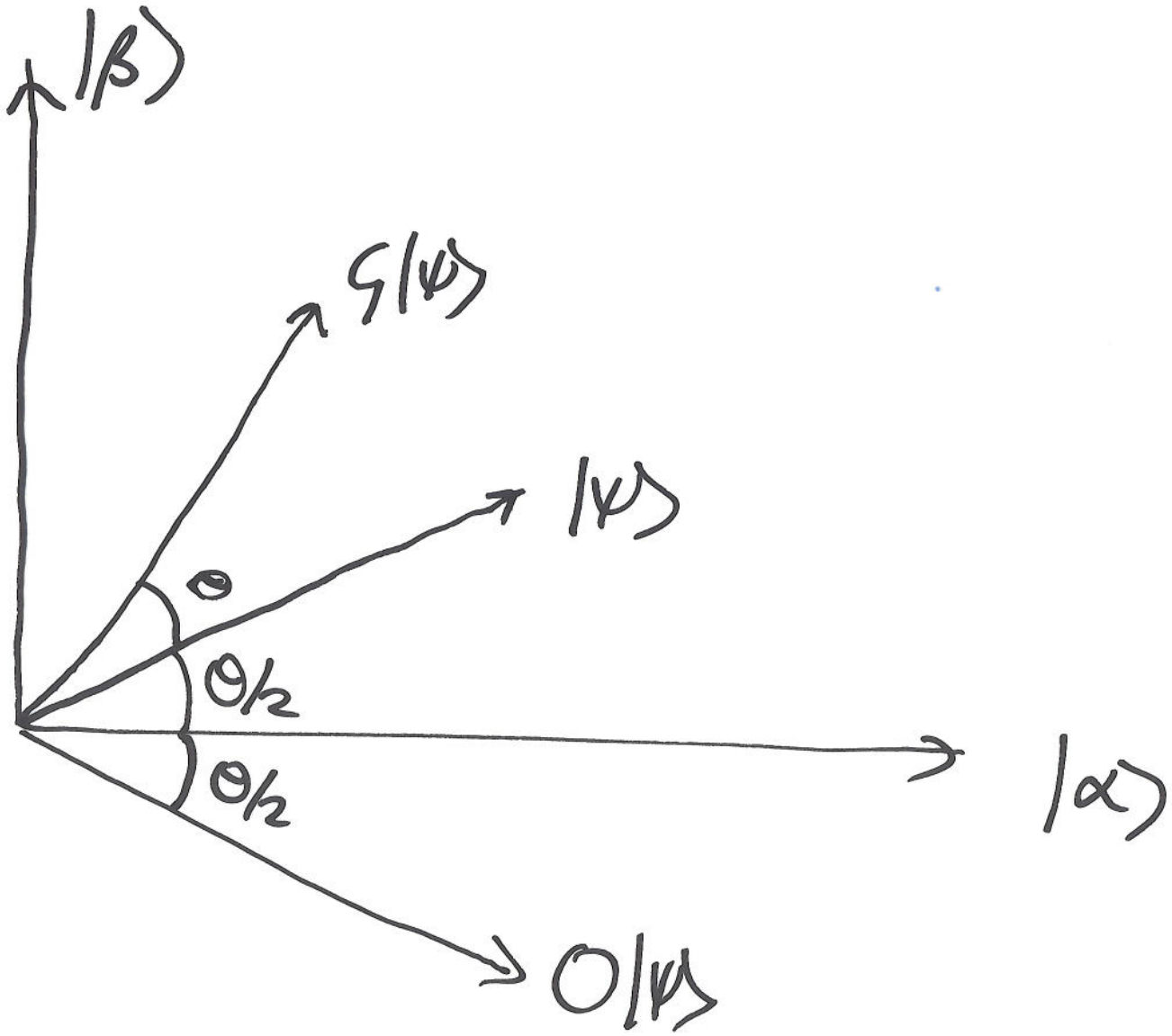
Rotation Angle:

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle,$$

where, $\cos\frac{\theta}{2} = \sqrt{(N-M)/N}$ and $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$.

Action of a Single Grover iteration

all vectors including $|\alpha\rangle$ and $|\beta\rangle$ should be unit vectors.



In the $|\alpha\rangle$, $|\beta\rangle$ basis, the Grover iteration may be written as,

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \quad 0 \leq \theta \leq \frac{\pi}{2}$$

assuming $M \leq \frac{N}{2}$,

where

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}.$$

Performance

How Many iterations to rotate $|\psi\rangle$ near to $|\beta\rangle$?

Initial state:

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

rotating by $\arccos\sqrt{M/N}$ radians takes system to $|\beta\rangle$.

Let $CI(x)$ denote integer closest to real x.

Then, repeating Grover iteration

$$R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$$ times rotates $|\psi\rangle$

to within $\theta/2 \leq \pi/4$ of $|\beta\rangle$.

Remember: Repeating iteration

$R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$ times

rotates $|\psi\rangle$ to within $\frac{\theta}{2} \leq \frac{\pi}{4}$ of $|\beta\rangle$.

then,

Measurement yields solution with

probability $\geq \frac{1}{2}$.

For some M and N a much higher probability is possible:

When $M \ll N$, we have $\theta \approx \sin\theta \approx 2\sqrt{M/N}$,

so angular error is $\leq \frac{\theta}{2} \approx \sqrt{\frac{M}{N}}$,

so $pr(\text{error}) \leq \frac{M}{N}$.

Number of repetitions, R, depends on number of solutions, M,

but not on identity of solutions.

...later it will be shown how to remove knowledge of M.

Remember:

$$R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right).$$

Observe that $R \leq \lceil \pi/2\theta \rceil$,

so a lower bound on θ gives an upper bound on R.

Assuming $M \leq \frac{N}{2}$, then, $\frac{\theta}{2} \geq \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$,

so

upper bound on #iterations is

$$R \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil.$$

... Quantum complexity is $O(\sqrt{N/M})$, (classical complexity is $O(N/M)$.

Algorithm: Quantum search - one solution.

Inputs: Black box $O: |x\rangle|q\rangle \to |x\rangle|q \oplus f(x)\rangle$,
$f(x) = 0$ $0 \le x < 2^n$ except x_0. $f(x_0) = 1$.
$n+1$ qubits in state $|0\rangle$.

Outputs: x_0

Runtime: $O(\sqrt{2^n})$ operations. Success probability $O(1)$.

Procedure:

1. $|0\rangle^{\otimes n}|0\rangle$

2. $\to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

3. $\to \left[(2|\psi\rangle\langle\psi| - I)O\right]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

$\approx |x_0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

4. $\to x_0$.

init.
apply $H^{\otimes n}$ to first n qubit
and HX to last qubit.

Grover iteration
$R \approx \lceil \pi\sqrt{2^n}/4 \rceil$
times

measure first n qubits.

What about when $M \geq \frac{N}{2}$?

$$\theta = \arcsin\left(2\sqrt{M(N-M)}/N\right),$$

so θ gets smaller as M increases from $\frac{N}{2}$ to N.

... so # iterations increases with M for $M \geq \frac{N}{2}$.

If M is known, then randomly pick, and check using oracle.

If M is not known then,

... double # elements in search space by adding N new non-solutions.

... then less than half items in new search space are solutions.

Double # items by ..

Adding a qubit $|q\rangle$ ... $\Rightarrow$ # search items is $2N$.

Construct augmented oracle O'. ... constructed using one call to O, and elementary gates using $|q\rangle$.

Now, $R = \frac{\pi}{4}\sqrt{2N/M}$ iterations required,

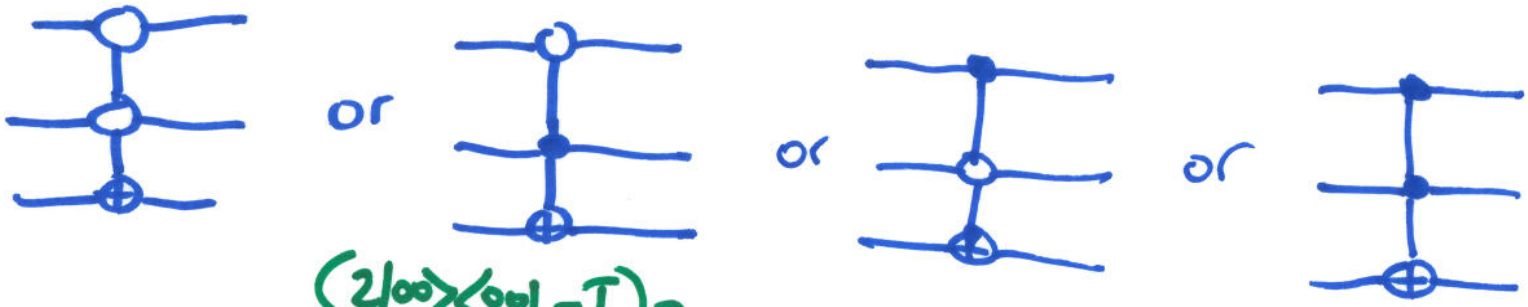
so $O(\sqrt{N/M})$ complexity.

Example:

$N=4$, $f(x)=0$ unless $x=x_0$, where $f(x_0)=1$.

Oracle:

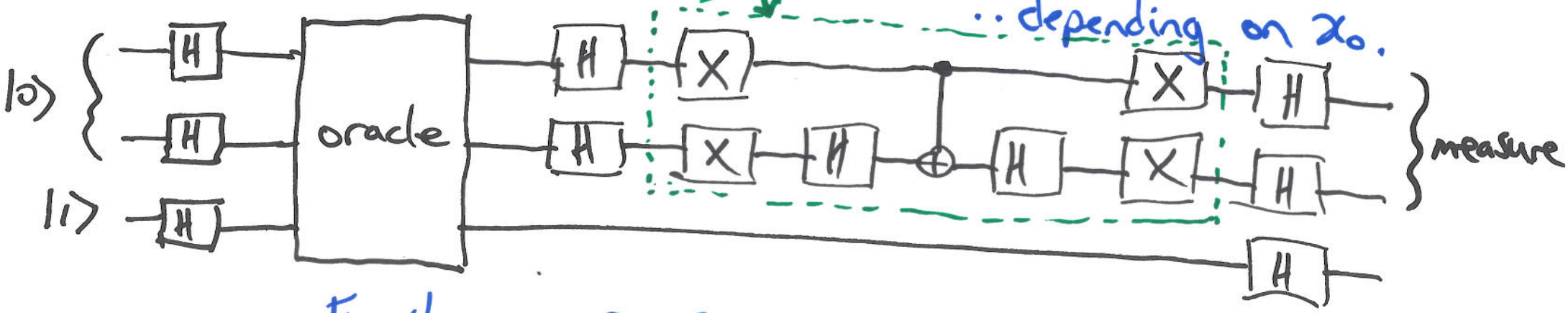
either



or or or

$(2|00\rangle\langle 00|-I)$

: depending on x_0.



For this case $\theta=\frac{\pi}{3}$, so exactly one iteration required.

$|\psi\rangle=(|00\rangle+|01\rangle+|10\rangle+|11\rangle)/2$ is 30° from $|\alpha\rangle$. Rotation by $\theta=60°$ moves $|\psi\rangle$ to $|\beta\rangle$.

Quantum: 1 oracle query

Classical: 2.25 oracle queries.