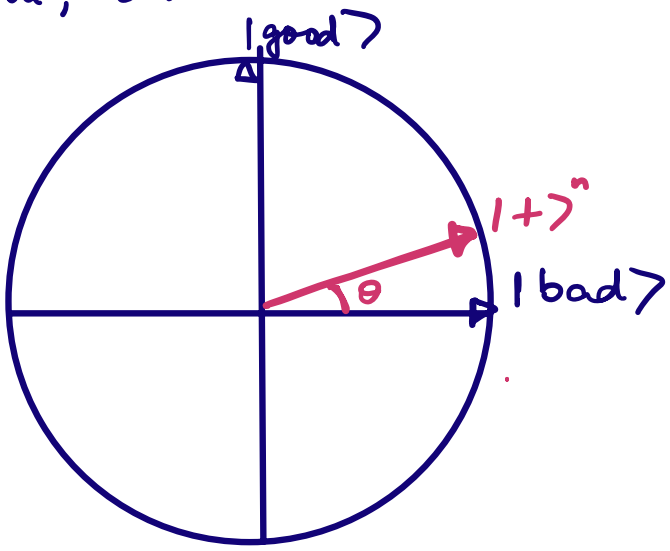
PICTORIAL REPRESENTATION OF GROVER

(Goal: Find x^* s.t. $f(x^*)=1$)

There is a "good" state : $|x^*\rangle$

and a "bad" state : $\frac{1}{\sqrt{N-1}} \sum_{x \neq x^*} |x\rangle$

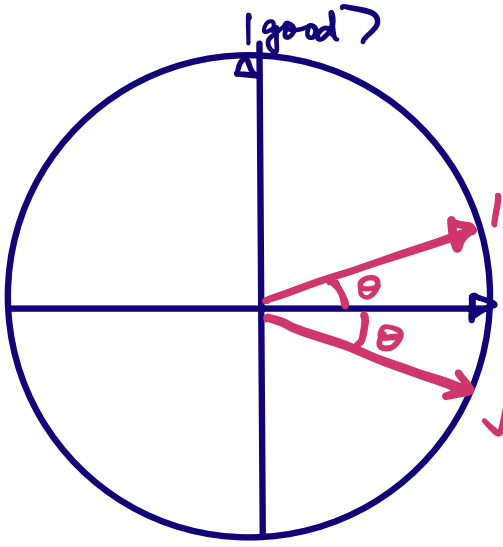
These are orthogonal, so:



1. Start with $\boxed{|+\rangle^{\otimes n}} = \boxed{\frac{\sqrt{N-1}}{\sqrt{N}}|bad\rangle + \frac{1}{\sqrt{N}}|good\rangle}$ ← note +

2. $\boxed{O_{f\pm}(|bad\rangle) = |bad\rangle \text{ and } O_{f\pm}|good\rangle = -|good\rangle}$

$O_{f\pm}$ "reflects about $|bad\rangle$"

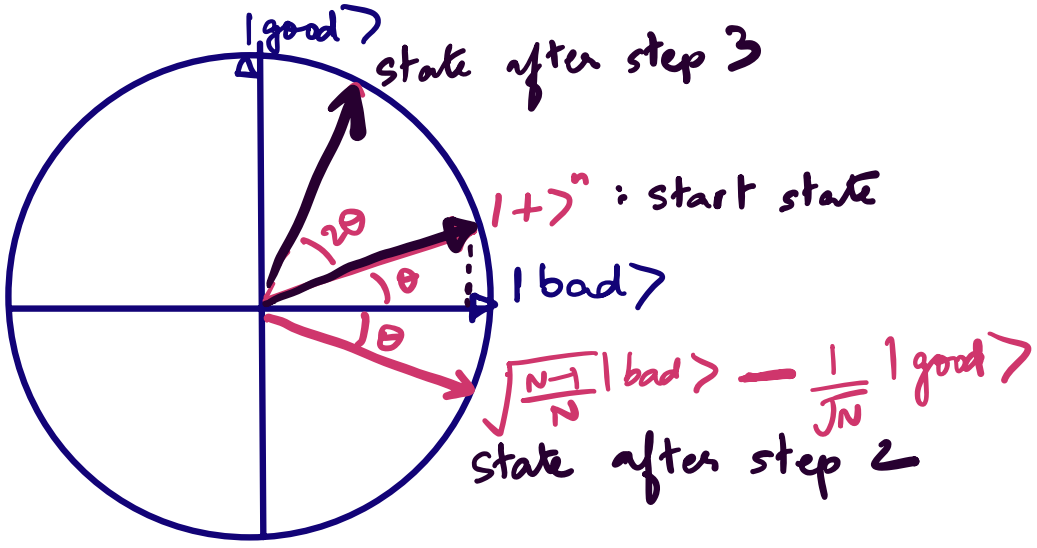


← note −

$\sqrt{\frac{N-1}{N}}|bad\rangle - \frac{1}{\sqrt{N}}|good\rangle$

3. $D(|+\rangle^{\otimes n}) = |+\rangle^{\otimes n}$ and $D(|y\rangle) = -|y\rangle$ for $|y\rangle$ orthogonal to $|+\rangle^{\otimes n}$

D "reflects about $|+\rangle^{\otimes n}$"



4. Result:

$$\sin\theta = \frac{1}{\sqrt{N}} \sim \theta.$$

Steps 2,3 rotate by $2\theta \sim \frac{2}{\sqrt{N}}$ towards $|good\rangle$

5. Repeat.

(Roughly) $O(\sqrt{N})$ iterations : $|good\rangle$

LOWER BOUNDS ON SEARCH

One of the most important problems in Computer Science: Is P = NP?

Equivalently, can NP-complete problems (eg., SAT) be solved in quantum polynomial time?

BOOLEAN 3-SAT:

Is there an assignment to $x_1, x_2 \ldots x_n$ such that:

$$(x_1 \underset{\text{or}}{\vee} x_2 \vee x_3) \underset{\text{and}}{\wedge} (\bar{x}_1 \vee x_3 \vee x_5) \ldots (x_1 \vee \bar{x}_2 \vee x_n) = 1?$$

Let $x = x_1 x_2 \cdots x_n$

and define

$$f(x) := (x_1 \underset{\text{or}}{\vee} x_2 \vee x_3) \underset{\text{and}}{\wedge} (\bar{x}_1 \vee x_3 \vee x_5) \ldots (x_1 \vee \bar{x}_2 \vee x_n)$$

The question above is equivalent to asking,

Is there an x^* such that $f(x^*) = 1$?

Suppose (Grover) search on arbitrary data (i.e. not necessary that $f(x^*)=1$ for unique x^*) took poly(n) calls to $O_{f^\pm}$, instead of $O(2^{n/2})$.

Then you could use it to solve 3-SAT!

More generally solve any problem in NP polynomial time with a quantum algorithm

This would be very surprising!!!

So, can we rule out super-efficient black-box search?

Yes! How?

Any search algorithm can be written as

$$U_T O_f U_{T-1} O_f \cdots O_f U_1 |0^n\rangle$$

... why? (H.W.)

where $T \leq N = 2^n$ is # calls to O_f

Denote by $|\phi_t\rangle$ the state

$$U_{t-1} O_f U_{t-2} \cdots O_f U_1 |0^n\rangle$$

when f is the zero function.

Let $|\phi_t\rangle = \sum_{x \in \{0,1\}^n} \alpha_{xt} |x\rangle$.

Note that: $\sum_{x \in \{0,1\}^n} (\alpha_{xt})^2 = 1$

$$\Rightarrow \sum_{t \in [T]} \sum_{x \in \{0,1\}^n} (\alpha_{xt})^2 = T$$

$$\Rightarrow \exists\, x^* \text{ such that } \sum_{t \in T} (\alpha_{x^* t})^2 \leq \frac{T}{N}$$

(Pigeonhole Principle)

Now consider two possibilities for f.

① f is the zero function (i.e. $f(x) = 0 \ \forall x$)

② $\tilde{f}$ is zero everywhere except on x^*.

Any search algorithm should distinguish ① from ②.

Let $|\tilde{\phi}_t\rangle$ denote

$$U_{t-1}\tilde{O}_f U_{t-2} \cdots \tilde{O}_f U_1 |0^n\rangle$$

Distinguishing ① from ② is same as distinguishing $|\tilde{\phi}_T\rangle$ from $|\phi_T\rangle$.

$$\| |\phi_T\rangle - |\tilde{\phi}_T\rangle \|$$

$$= \| U_T O_f U_{T-1} O_f \cdots U_1 |0^n\rangle - U_T \tilde{O}_f U_{T-1} \tilde{O}_f \cdots U_1 |0^n\rangle \|$$

Let $|\psi_T\rangle_i = U_T O_f U_{T-1} O_f \cdots O_f U_i \tilde{O}_f \cdots \tilde{O}_f U_1 |0^n\rangle$

$|\phi_T\rangle = |\psi_T\rangle_1$ and $|\tilde{\phi}_T\rangle = |\psi_T\rangle_T$

Then, $1 = \| |\phi_T\rangle - |\tilde{\phi}_T\rangle \|$

$= \| |\psi_T\rangle_1 - |\psi_T\rangle_T \|$

$= \| |\psi_T\rangle_1 - |\psi_T\rangle_2 + |\psi_T\rangle_2 - |\psi_T\rangle_3 \ldots \ldots - |\psi_T\rangle_T \|$

$\leq \underbrace{\| |\psi_T\rangle_1 - |\psi_T\rangle_2 \|}_{E_1} + \underbrace{\| |\psi_T\rangle_2 - |\psi_T\rangle_3 \|}_{E_2} \ldots$

$\| E_1 \| + \| E_2 \| \ldots + \| E_T \|$ and $\| E_i \|^2 = 4\alpha_{xt}^2$ (why?)

$\leq \sqrt{\sum_{i \in [T]} \| E_i \|^2 \cdot \sum_{i \in [T]} 1^2}$ (Cauchy-Schwarz)

$\leq \sqrt{4 \sum_{i \in [T]} \alpha_{xi}^2} \sqrt{T} = \sqrt{4 \frac{T^2}{N}} = \frac{2T}{\sqrt{N}}$

$\Rightarrow T \geq O(\sqrt{N})$.