7. Quantum algorithms (part 2)

(i) Grover's search algorithm (NC 6.1, KLM 8.1-8.2, M 4)

7. Quantum algorithms (part 2)

(i) Grover's search algorithm (NC 6.1, KLM 8.1-8.2, M 4)

Differences from factoring algorithm:
- intuitive
- easily visualized
- very little analysis needed

Discussion will be relatively brief.

(ii) Optimality of Grover's algorithm (NC 6.6, KLM 9.3)

Unstructured search: (variation 1)

Given: $N \in \mathbb{N}$

black box for a function $f:\{1,\ldots,N\} \longrightarrow \{0,1\}$

Problem: determine if there is an x s.t. $f(x) = 1$.

such an x is called a "marked" item

Unstructured search: (variation 1)

Given: $N \in \mathbb{N}$

black box for a function $f: \{1,\ldots,N\} \longrightarrow \{0,1\}$

Problem: determine if there is an x s.t. $f(x) = 1$.

such an x is called a "marked" item

Motivation I: This models problems in NP.

e.g., 3-SAT. Each instance of size n is a formula of n binary variables and poly(n) clauses:

$$(x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_3 \vee x_8) \wedge \ldots =: f(x)$$

Unstructured search: (variation 1)

Given: $N \in \mathbb{N}$

black box for a function $f:\{1,\ldots,N\} \longrightarrow \{0,1\}$

Problem: determine if there is an x s.t. $f(x) = 1$.

such an x is called a "marked" item

Motivation I: This models problems in NP.

e.g., 3-SAT. Each instance of size n is a formula of n binary variables and poly(n) clauses:

$$(x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_3 \vee x_8) \wedge \cdots =: f(x)$$

Goal: determine if there is an $x = x_1 x_2 \cdots x_n$ with $f(x) = 1$ (x is called a "satisfying assignment").

Unstructured search: (variation 1)

Given: $N \in \mathbb{N}$

black box for a function $f: \{1,\ldots,N\} \longrightarrow \{0,1\}$

Problem: determine if there is an x s.t. f(x) = 1.

such an x is called a "marked" item

Motivation I: This models problems in NP.

e.g., 3-SAT. Each instance of size n is a formula of n binary variables and poly(n) clauses:

$$(x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_3 \vee x_8) \wedge \cdots =: f(x)$$

Goal: determine if there is an $x = x_1 x_2 \cdots x_n$ with f(x) = 1 (x is called a "satisfying assignment").

For each x, checking if f(x) = 1 takes poly(n)-time, and is modeled by a query to the blackbox.

Unstructured search: (variation 2)

Given: $N \in \mathbb{N}$

black box for a function $f:\{1,\ldots,N\} \longrightarrow \{0,1\}$

M = # of marked items.

Problem: find an x s.t. $f(x) = 1$. (a "marked" item)

Variation 3: M is unknown.

Unstructured search: (variation 2)

Given: $N \in \mathbb{N}$

black box for a function $f:\{1,\dots,N\} \longrightarrow \{0,1\}$

M = # of marked items.

Problem: find an x s.t. $f(x) = 1$. (a "marked" item)

Variation 3: M is unknown.

Motivation II: This models database search.

e.g., given a phone book sorted by names and a specific phone number, find whose number it is. Here, $M=1$, N = # of entries in the phone book.

Focus on variation 2 for now.

Unstructured search: (variation 2)

Given: $N \in \mathbb{N}$

black box for a function $f:\{1,\ldots,N\} \longrightarrow \{0,1\}$

M = # of marked items.

Problem: find an x s.t. $f(x) = 1$. (a "marked" item)

Classical query complexity: $\Omega\left(\frac{N}{M}\right)$ (counting argument)

Unstructured search: (variation 2)

Given: $N \in \mathbb{N}$

black box for a function $f: \{1,\ldots,N\} \longrightarrow \{0,1\}$

M = # of marked items.

Problem: find an x s.t. $f(x) = 1$. (a "marked" item)

Classical query complexity: $\Omega\left(\frac{N}{M}\right)$ (counting argument)

Quantum query complexity: $O\left(\sqrt{\frac{N}{M}}\right)$ (Grover's algorithm)

NB. Quantum is advantageous only when the fraction of marked items is vanishing (needle in a haystack).

Claim: classical query complexity: $\Omega\left(\frac{N}{M}\right)$

Proof: With M marked items among N,
probability not seeing a marked item after t queries

$$= \frac{N-M}{N} \; \frac{N-M-1}{N-1} \; \frac{N-M-2}{N-2} \cdots \frac{N-M-t+1}{N-t+1}$$

Claim: classical query complexity: $\Omega\left(\frac{N}{M}\right)$

Proof: With M marked items among N,
probability not seeing a marked item after t queries

$$= \frac{N-M}{N} \frac{N-M-1}{N-1} \frac{N-M-2}{N-2} \cdots \frac{N-M-t+1}{N-t+1}$$

$$= \left(1-\frac{M}{N}\right)\left(1-\frac{M}{N-1}\right)\left(1-\frac{M}{N-2}\right) \cdots \left(1-\frac{M}{N-t+1}\right)$$

$$\geq \left(1-\frac{M}{N-t+1}\right)^t$$

Claim: classical query complexity: $\Omega\left(\frac{N}{M}\right)$

Proof: With M marked items among N,
probability not seeing a marked item after t queries

$$= \frac{N-M}{N} \, \frac{N-M-1}{N-1} \, \frac{N-M-2}{N-2} \cdots\cdots \frac{N-M-t+1}{N-t+1}$$

$$= \left(1-\frac{M}{N}\right)\left(1-\frac{M}{N-1}\right)\left(1-\frac{M}{N-2}\right)\cdots \left(1-\frac{M}{N-t+1}\right)$$

$$\geq \left(1-\frac{M}{N-t+1}\right)^{t}$$

recall $e^{x} = \lim_{k\to\infty}\left(1+\frac{x}{k}\right)^{k}$

$$= \left(1+\frac{(-1)}{\frac{N-t+1}{M}}\right)^{\frac{N-t+1}{M}\cdot\frac{M}{N-t+1}t}$$

Claim: classical query complexity: $\Omega\left(\frac{N}{M}\right)$

Proof: With M marked items among N,
probability not seeing a marked item after t queries

$$= \frac{N-M}{N} \frac{N-M-1}{N-1} \frac{N-M-2}{N-2} \cdots \frac{N-M-t+1}{N-t+1}$$

$$= \left(1-\frac{M}{N}\right)\left(1-\frac{M}{N-1}\right)\left(1-\frac{M}{N-2}\right)\cdots\left(1-\frac{M}{N-t+1}\right)$$

$$\geq \left(1-\frac{M}{N-t+1}\right)^t$$

recall $e^x = \lim_{k\to\infty}\left(1+\frac{x}{k}\right)^k$

$$= \left(1+\frac{(-1)}{\frac{N-t+1}{M}}\right)^{\frac{N-t+1}{M}\cdot\frac{M}{N-t+1}t}$$

let x = -1, k = $\frac{N-t+1}{M}$

$$\approx \left(\frac{1}{e}\right)^{\frac{M}{N-t+1}t}$$

Claim: classical query complexity: $\Omega\left(\frac{N}{M}\right)$

Proof: With M marked items among N, probability not seeing a marked item after t queries

$$= \frac{N-M}{N} \cdot \frac{N-M-1}{N-1} \cdot \frac{N-M-2}{N-2} \cdots \frac{N-M-t+1}{N-t+1}$$

$$= \left(1-\frac{M}{N}\right)\left(1-\frac{M}{N-1}\right)\left(1-\frac{M}{N-2}\right)\cdots\left(1-\frac{M}{N-t+1}\right)$$

$$\geq \left(1-\frac{M}{N-t+1}\right)^{t}$$

recall $e^{x} = \lim_{k\to\infty}\left(1+\frac{x}{k}\right)^{k}$

$$= \left(1+\frac{(-1)}{\frac{N-t+1}{M}}\right)^{\frac{N-t+1}{M}\cdot\frac{M}{N-t+1}t}$$

let $x = -1$, $k = \frac{N-t+1}{M}$

$$\approx \left(\frac{1}{e}\right)^{\frac{M}{N-t+1}t} \approx 1$$

unless exponential is far from 0

i.e., $Mt = \Omega(N)$

$\therefore\ t \sim \Omega\left(\frac{N}{M}\right)$ queries are needed.

Grover's algorithm:

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$, $V = 2|\psi\rangle\langle\psi| - I$

"reflection" about $|\psi\rangle$

$$V|\psi\rangle = (2|\psi\rangle\langle\psi| - I)|\psi\rangle$$

$$= 2|\psi\rangle - |\psi\rangle = |\psi\rangle$$

$\forall |\phi\rangle \perp |\psi\rangle$

$$V|\phi\rangle = (2|\psi\rangle\langle\psi| - I)|\phi\rangle = -|\phi\rangle$$

Grover's algorithm:

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$, $V = 2|\psi\rangle\langle\psi| - I$

Blackbox: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase kick back: $U_f |x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

Grover's algorithm:

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$, $V = 2|\psi\rangle\langle\psi| - I$

Blackbox: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase kick back: $U_f |x\rangle|-\rangle = (-1)^{f(x)} |x\rangle|-\rangle$

1. Initialize state to $|\psi\rangle|-\rangle$

Grover's algorithm:

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle, \quad V = 2|\psi\rangle\langle\psi| - I$

Blackbox: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase kick back: $U_f |x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

1. Initialize state to $|\psi\rangle|-\rangle$

2. Apply Grover's iteration $G = (V \otimes I)\, U_f$ k times, for k to be determined.

Grover's algorithm:

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$, $V = 2|\psi\rangle\langle\psi| - I$

Blackbox: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase kick back: $U_f |x\rangle|-\rangle = (-1)^{f(x)} |x\rangle|-\rangle$

1. Initialize state to $|\psi\rangle|-\rangle$

2. Apply Grover's iteration $G = (V \otimes I) U_f$ k times, for k to be determined.

3. Measure 1st register in the computational basis.

Grover's algorithm:

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$, $V = 2|\psi\rangle\langle\psi| - I$

Blackbox: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase kick back: $U_f |x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

1. Initialize state to $|\psi\rangle|-\rangle$

2. Apply Grover's iteration $G = (V \otimes I)\, U_f$ k times, for k to be determined.

3. Measure 1st register in the computational basis.

4. Check if the measurement outcome is a marked item by using U_f.

Example: $N=4$, $M=1$ (1-out-of-4 search)

Let 3 be the marked item ($f(3)=1$, $f(x)=0$ if $x \neq 3$).

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item (f(3)=1, f(x)=0 if x≠3).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle + |3\rangle + |4\rangle\right)|-\rangle$

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item ($f(3)=1$, $f(x)=0$ if $x \neq 3$).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}(|1\rangle + |2\rangle + |3\rangle + |4\rangle)|-\rangle$

2a. Apply U_f: $U_f|\psi\rangle|-\rangle = \frac{1}{2}(|1\rangle + |2\rangle - |3\rangle + |4\rangle)|-\rangle$

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item (f(3)=1, f(x)=0 if x$\neq$3).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle + |3\rangle + |4\rangle\right)|-\rangle$

2a. Apply U_f : $U_f|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle - |3\rangle + |4\rangle\right)|-\rangle$

$$= \frac{1}{2}\left(|1\rangle + |2\rangle + |3\rangle + |4\rangle\right)|-\rangle - |3\rangle|-\rangle$$

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item (f(3)=1, f(x)=0 if x$\neq$3).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle + |3\rangle + |4\rangle\right)|-\rangle$

2a. Apply U_f : $U_f|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle - |3\rangle + |4\rangle\right)|-\rangle$

$$= \frac{1}{2}\left(|1\rangle + |2\rangle + |3\rangle + |4\rangle\right)|-\rangle$$

$$- |3\rangle|-\rangle$$

$$= \left(|\psi\rangle - |3\rangle\right)|-\rangle$$

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item ($f(3)=1$, $f(x)=0$ if $x \neq 3$).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle + |3\rangle + |4\rangle\right)|-\rangle$

2a. Apply U_f : $U_f|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle - |3\rangle + |4\rangle\right)|-\rangle$

$$= \left(|\psi\rangle - |3\rangle\right)|-\rangle$$

2b. Apply $V = 2|\psi\rangle\langle\psi| - I$ to 1st register :

$$(V \otimes I)\,U_f|\psi\rangle|-\rangle = (V \otimes I)\left(|\psi\rangle - |3\rangle\right)|-\rangle$$

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item ($f(3)=1$, $f(x)=0$ if $x \neq 3$).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle + |3\rangle + |4\rangle\right)|-\rangle$

2a. Apply U_f : $U_f|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle + |2\rangle - |3\rangle + |4\rangle\right)|-\rangle$

$$= \left(|\psi\rangle - |3\rangle\right)|-\rangle$$

2b. Apply $V = 2|\psi\rangle\langle\psi| - I$ to 1st register :

$$(V \otimes I)\,U_f|\psi\rangle|-\rangle = (V \otimes I)\left(|\psi\rangle - |3\rangle\right)|-\rangle$$

$$= V\left(|\psi\rangle - |3\rangle\right) \otimes |-\rangle$$

$$= \left(2|\psi\rangle\langle\psi| - I\right)\left(|\psi\rangle - |3\rangle\right) \otimes |-\rangle$$

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item ($f(3)=1$, $f(x)=0$ if $x\neq 3$).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle+|2\rangle+|3\rangle+|4\rangle\right)|-\rangle$

2a. Apply U_f : $U_f|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle+|2\rangle-|3\rangle+|4\rangle\right)|-\rangle$

$$= \left(|\psi\rangle-|3\rangle\right)|-\rangle$$

2b. Apply $V = 2|\psi\rangle\langle\psi| - I$ to 1st register :

$$(V\otimes I)\,U_f|\psi\rangle|-\rangle = (V\otimes I)\left(|\psi\rangle-|3\rangle\right)|-\rangle$$

$$= V\left(|\psi\rangle-|3\rangle\right)\otimes|-\rangle$$

$$= \underbrace{\left(2|\psi\rangle\langle\psi| - I\right)\left(|\psi\rangle-|3\rangle\right)}_{2|\psi\rangle-|\psi\rangle-|\psi\rangle+|3\rangle \;=\; |3\rangle\,!}\otimes|-\rangle$$

Example: N=4, M=1 (1-out-of-4 search)

Let 3 be the marked item ($f(3)=1$, $f(x)=0$ if $x\neq 3$).

1. Initial state: $|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle+|2\rangle+|3\rangle+|4\rangle\right)|-\rangle$

2a. Apply U_f : $U_f|\psi\rangle|-\rangle = \frac{1}{2}\left(|1\rangle+|2\rangle-|3\rangle+|4\rangle\right)|-\rangle$

$$= \left(|\psi\rangle-|3\rangle\right)|-\rangle$$

2b. Apply $V = 2|\psi\rangle\langle\psi| - I$ to 1st register :

$$\begin{aligned}(V\otimes I)U_f|\psi\rangle|-\rangle &= (V\otimes I)\left(|\psi\rangle-|3\rangle\right)|-\rangle \\ &= V\left(|\psi\rangle-|3\rangle\right)\otimes|-\rangle \\ &= \underbrace{\left(2|\psi\rangle\langle\psi|-I\right)\left(|\psi\rangle-|3\rangle\right)}_{2|\psi\rangle-|\psi\rangle-|\psi\rangle+|3\rangle\,=\,|3\rangle\,!}\otimes|-\rangle\end{aligned}$$

3. Meas 1st register
 outcome=3 !

Observations from the example:

1. By symmetry, the algorithm works for any marked item (1, 2, 3, or 4).

Observations from the example:

1. By symmetry, the algorithm works for any marked item (1, 2, 3, or 4).

2. Due to phase-kick back, 2nd register is always in the state $|-\rangle$. Grover's iteration acts on 1st register as $V\tilde{U}_f$ where $\tilde{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$.

Observations from the example:

1. By symmetry, the algorithm works for any marked item (1, 2, 3, or 4).

2. Due to phase-kick back, 2nd register is always in the state $|-\rangle$. Grover's iteration acts on 1st register as $V\tilde{U}_f$ where $\tilde{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$.

3. Throughout, the linear combination "$|1\rangle + |2\rangle + |4\rangle$" is left "as a piece". The state in the 1st register is a linear combination of "$|1\rangle + |2\rangle + |4\rangle$" & $|3\rangle$.

Observations from the example:

1. By symmetry, the algorithm works for any marked item (1, 2, 3, or 4).

2. Due to phase-kick back, 2nd register is always in the state $|-\rangle$. Grover's iteration acts on 1st register as $V\tilde{U}_f$ where $\tilde{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$.

3. Throughout, the linear combination "$|1\rangle + |2\rangle + |4\rangle$" is left "as a piece". The state in the 1st register is a linear combination of "$|1\rangle + |2\rangle + |4\rangle$" & $|3\rangle$.

or of $|\psi\rangle$ & $|3\rangle$.

Observations from the example:

1. By symmetry, the algorithm works for any marked item (1, 2, 3, or 4).

2. Due to phase-kick back, 2nd register is always in the state $|-\rangle$. Grover's iteration acts on 1st register as $V\tilde{U}_f$ where $\tilde{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$.

3. Throughout, the linear combination "$|1\rangle + |2\rangle + |4\rangle$" is left "as a piece". The state in the 1st register is a linear combination of "$|1\rangle + |2\rangle + |4\rangle$" & $|3\rangle$.

   or of $|\psi\rangle$ & $|3\rangle$.

   Proof: $\tilde{U}_f(|1\rangle + |2\rangle + |4\rangle) = |1\rangle + |2\rangle + |4\rangle$, $\tilde{U}_f|3\rangle = -|3\rangle$,

Observations from the example:

1. By symmetry, the algorithm works for any marked item (1, 2, 3, or 4).

2. Due to phase-kick back, 2nd register is always in the state $|-\rangle$. Grover's iteration acts on 1st register as $V\tilde{U}_f$ where $\tilde{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$.

3. Throughout, the linear combination "$|1\rangle + |2\rangle + |4\rangle$" is left "as a piece". The state in the 1st register is a linear combination of "$|1\rangle + |2\rangle + |4\rangle$" & $|3\rangle$.

   or of $|\psi\rangle$ & $|3\rangle$.

   Proof: $\tilde{U}_f(|1\rangle + |2\rangle + |4\rangle) = |1\rangle + |2\rangle + |4\rangle$, $\tilde{U}_f|3\rangle = -|3\rangle$,

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

Observations from the example:

1. By symmetry, the algorithm works for any marked item (1, 2, 3, or 4).

2. Due to phase-kick back, 2nd register is always in the state $|-\rangle$. Grover's iteration acts on 1st register as $V\tilde{U}_f$ where $\tilde{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$.

3. Throughout, the linear combination "$|1\rangle + |2\rangle + |4\rangle$" is left "as a piece". The state in the 1st register is a linear combination of "$|1\rangle + |2\rangle + |4\rangle$" & $|3\rangle$.

or of $|\psi\rangle$ & $|3\rangle$.

Proof: $\tilde{U}_f\left(|1\rangle + |2\rangle + |4\rangle\right) = |1\rangle + |2\rangle + |4\rangle$, $\tilde{U}_f|3\rangle = -|3\rangle$,

$$V|\psi\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi\rangle = 2|\psi\rangle - |\psi\rangle = |\psi\rangle,$$

$$V|3\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|3\rangle = |\psi\rangle - |3\rangle.$$

Observations for Grover's algorithm in general:

1. 2nd register stays in the state $|-\rangle$ throughout.

   1st register is evolved by $\tilde{G} = V\tilde{U}_f$, where

   $\tilde{U}_f |x\rangle = (-1)^{f(x)} |x\rangle$.

Observations for Grover's algorithm in general:

2. 1st register stays in the span of:

$$|\alpha\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$$

$|\alpha\rangle$: equal superposition of all marked items

$|\beta\rangle$: equal superposition of all unmarked items

Observations for Grover's algorithm in general:

2. 1st register stays in the span of:

$$|\alpha\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle \qquad \left(|\alpha\rangle = |3\rangle \text{ in example} \right)$$

$$|\beta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle \qquad \left(|\beta\rangle = \frac{1}{\sqrt{3}}\left(|1\rangle + |2\rangle + |4\rangle\right) \text{ in example} \right)$$

$|\alpha\rangle$: equal superposition of all marked items

$|\beta\rangle$: equal superposition of all unmarked items

<u>Observations for Grover's algorithm in general:</u>

2. 1st register stays in the span of:

$$|\alpha\rangle = \frac{1}{\sqrt{M}} \sum_{x: f(x)=1} |x\rangle \qquad \left(|\alpha\rangle = |3\rangle \text{ in example} \right)$$

$$|\beta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x: f(x)=0} |x\rangle \qquad \left(|\beta\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |2\rangle + |4\rangle) \text{ in example} \right)$$

$|\alpha\rangle$: equal superposition of all marked items

$|\beta\rangle$: equal superposition of all unmarked items

Intuition: symmetry among all marked items, and symmetry among all unmarked items.

Observations for Grover's algorithm in general:

2. 1st register stays in the span of:

$$|\alpha\rangle = \frac{1}{\sqrt{M}} \sum_{x : f(x)=1} |x\rangle , \quad |\beta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x : f(x)=0} |x\rangle$$

Proof:

Initial state = $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle$

Observations for Grover's algorithm in general:

2. 1st register stays in the span of:

$$|\alpha\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle, \quad |\beta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$$

Proof:

Initial state = $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle$

$$= \frac{1}{\sqrt{N}} \left(\sum_{x:f(x)=1} |x\rangle + \sum_{x:f(x)=0} |x\rangle \right)$$

Observations for Grover's algorithm in general:

2. 1st register stays in the span of:

$$|\alpha\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle, \quad |\beta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$$

Proof:

Initial state = $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle$

$$= \frac{1}{\sqrt{N}} \left(\sum_{x:f(x)=1} |x\rangle + \sum_{x:f(x)=0} |x\rangle \right)$$

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

Observations for Grover's algorithm in general:

2. 1st register stays in the span of:

$$|\alpha\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle, \quad |\beta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$$

Proof:

Initial state = $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$

$$= \frac{1}{\sqrt{N}} \left(\sum_{x:f(x)=1} |x\rangle + \sum_{x:f(x)=0} |x\rangle \right)$$

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

NB. $|\alpha\rangle \perp |\beta\rangle$, $\langle\psi|\alpha\rangle = \sqrt{\frac{M}{N}}$, $\langle\psi|\beta\rangle = \sqrt{\frac{N-M}{N}}$.

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

$\tilde{U}_f : |\alpha\rangle \to -|\alpha\rangle, \quad |\beta\rangle \to |\beta\rangle$

Initial state $= |\Psi\rangle = \frac{\sqrt{M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|\beta\rangle$.

$$\tilde{U}_f : |\alpha\rangle \to -|\alpha\rangle, \quad |\beta\rangle \to |\beta\rangle$$

$$V = 2|\Psi\rangle\langle\Psi| - I, \qquad V|\alpha\rangle = 2\langle\Psi|\alpha\rangle|\Psi\rangle - |\alpha\rangle$$

Initial state $= |\psi\rangle = \dfrac{\sqrt{M}}{\sqrt{N}}|\alpha\rangle + \dfrac{\sqrt{N-M}}{\sqrt{N}}|\beta\rangle.$

$$\tilde{U}_f : |\alpha\rangle \to -|\alpha\rangle, \quad |\beta\rangle \to |\beta\rangle$$

$$V = 2|\psi\rangle\langle\psi| - I, \quad V|\alpha\rangle = 2\langle\psi|\alpha\rangle|\psi\rangle - |\alpha\rangle$$

$$V|\beta\rangle = 2\langle\psi|\beta\rangle|\psi\rangle - |\beta\rangle$$

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

$\tilde{U}_f : |\alpha\rangle \to -|\alpha\rangle, \quad |\beta\rangle \to |\beta\rangle$

$V = 2|\psi\rangle\langle\psi| - I, \quad V|\alpha\rangle = 2\langle\psi|\alpha\rangle\,|\psi\rangle - |\alpha\rangle$

$V|\beta\rangle = 2\langle\psi|\beta\rangle\,|\psi\rangle - |\beta\rangle$

Since $|\psi\rangle$ is in the span of $|\alpha\rangle, |\beta\rangle$, so are $V|\alpha\rangle, V|\beta\rangle$.

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

$\tilde{U}_f : |\alpha\rangle \to -|\alpha\rangle, \quad |\beta\rangle \to |\beta\rangle$

$V = 2|\psi\rangle\langle\psi| - I, \quad V|\alpha\rangle = 2\langle\psi|\alpha\rangle\,|\psi\rangle - |\alpha\rangle$

$V|\beta\rangle = 2\langle\psi|\beta\rangle\,|\psi\rangle - |\beta\rangle$

Since $|\psi\rangle$ is in the span of $|\alpha\rangle, |\beta\rangle$, so are $V|\alpha\rangle, V|\beta\rangle$.

So, each of V and $\tilde{U}_f$ preserves the span of $|\alpha\rangle, |\beta\rangle$.

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

$\tilde{U}_f : |\alpha\rangle \to -|\alpha\rangle, \; |\beta\rangle \to |\beta\rangle$

$V = 2|\psi\rangle\langle\psi| - I$, $\quad V|\alpha\rangle = 2\langle\psi|\alpha\rangle\,|\psi\rangle - |\alpha\rangle$

$V|\beta\rangle = 2\langle\psi|\beta\rangle\,|\psi\rangle - |\beta\rangle$

Since $|\psi\rangle$ is in the span of $|\alpha\rangle, |\beta\rangle$, so are $V|\alpha\rangle, V|\beta\rangle$.

So, each of V and $\tilde{U}_f$ preserves the span of $|\alpha\rangle, |\beta\rangle$.

Algorithm starts with $|\psi\rangle$ (in the span of $|\alpha\rangle, |\beta\rangle$) and applies $V\tilde{U}_f$ k times. So, 1st register is always in the span of $|\alpha\rangle, |\beta\rangle$.

Analysis of Grover's algorithm:

We can restrict the analysis to the span of $|\alpha\rangle, |\beta\rangle$.

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

What does Grover's iteration $V\tilde{U}_f$ do?

Analysis of Grover's algorithm:

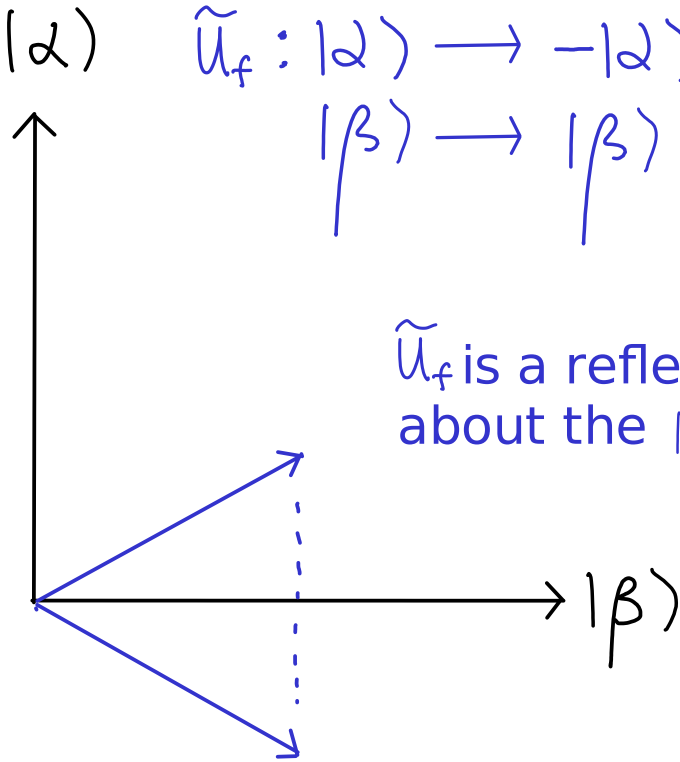
We can restrict the analysis to the span of $|\alpha\rangle, |\beta\rangle$.

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

What does Grover's iteration $V\tilde{U}_f$ do?

$$\tilde{U}_f : |\alpha\rangle \longrightarrow -|\alpha\rangle$$
$$|\beta\rangle \longrightarrow |\beta\rangle$$

$\tilde{U}_f$ is a reflection about the $|\beta\rangle$ axis



Analysis of Grover's algorithm:

We can restrict the analysis to the span of $|\alpha\rangle, |\beta\rangle$.

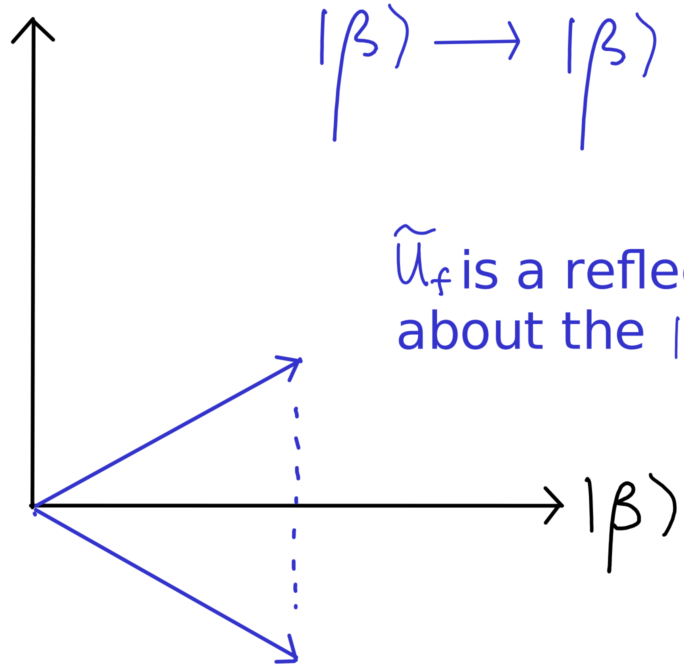
Initial state $= |\psi\rangle = \frac{\sqrt{M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|\beta\rangle$.

What does Grover's iteration $V\tilde{U}_f$ do?

$|\alpha\rangle$

$\tilde{U}_f : |\alpha\rangle \longrightarrow -|\alpha\rangle$

$\qquad |\beta\rangle \longrightarrow |\beta\rangle$



$\tilde{U}_f$ is a reflection about the $|\beta\rangle$ axis

$|\alpha\rangle$

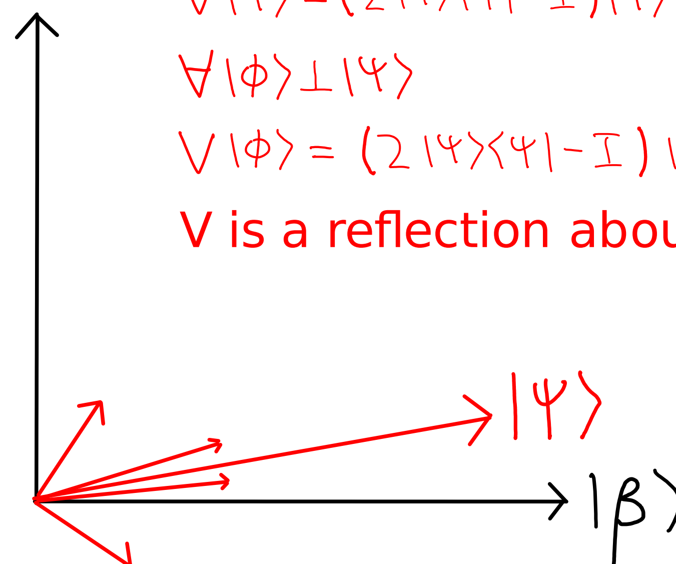
$V = 2|\psi\rangle\langle\psi| - I$

$V|\psi\rangle = (2|\psi\rangle\langle\psi| - I)|\psi\rangle = 2|\psi\rangle - |\psi\rangle = |\psi\rangle$

$\forall |\phi\rangle \perp |\psi\rangle$

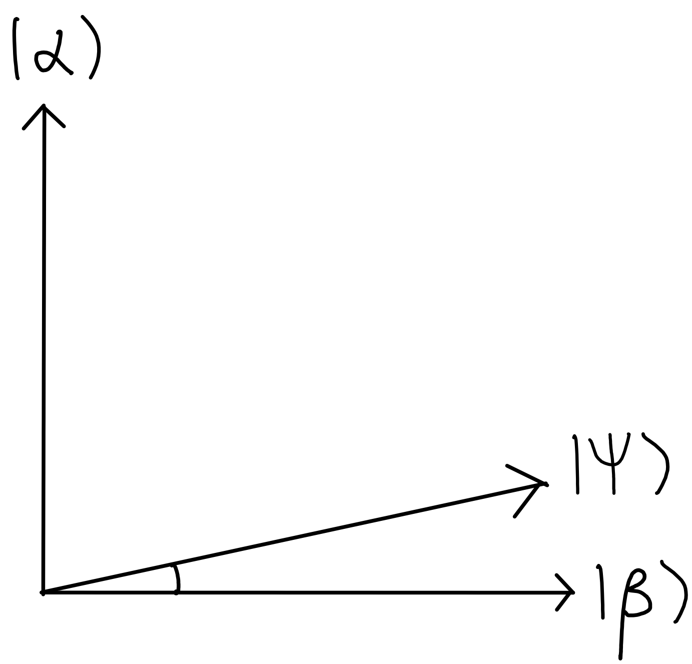
$V|\phi\rangle = (2|\psi\rangle\langle\psi| - I)|\phi\rangle = -|\phi\rangle$

V is a reflection about the $|\psi\rangle$ axis.



What does Grover's iteration $V\tilde{U}_f$ do?

By linearity, suffices to check its action on a spanning set: $|\beta\rangle, |\psi\rangle$.



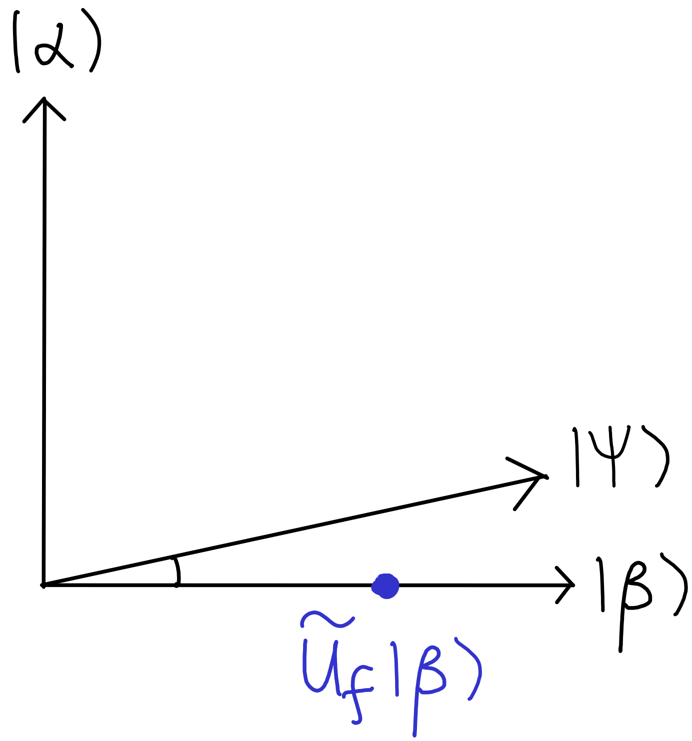
Each marked angle is $\theta/2$

where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.

What does Grover's iteration $V\tilde{U}_f$ do?

By linearity, suffices to check its action on a spanning set: $|\beta\rangle$, $|\Psi\rangle$.

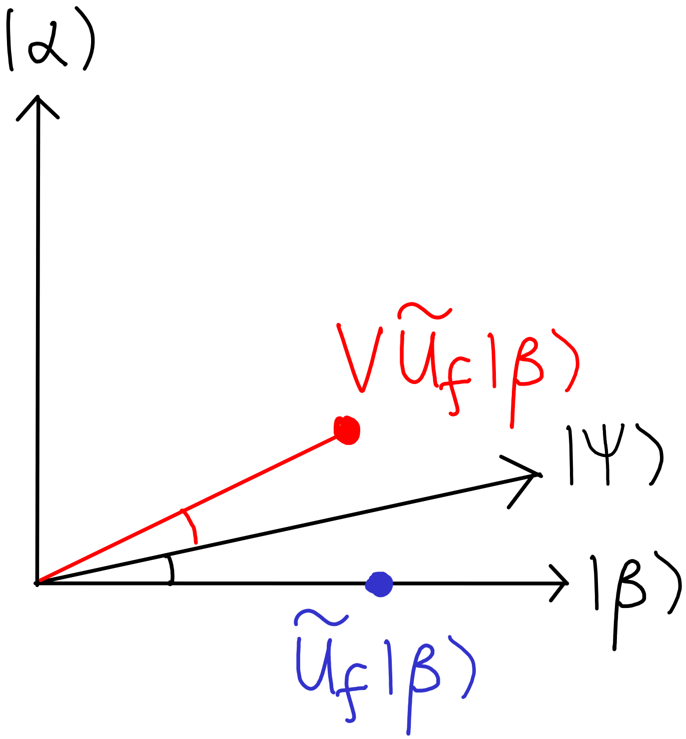
Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.



For the initial state $|\beta\rangle$

What does Grover's iteration $V\tilde{U}_f$ do?

By linearity, suffices to check its action on a spanning set: $|\beta\rangle, |\Psi\rangle$.



Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.

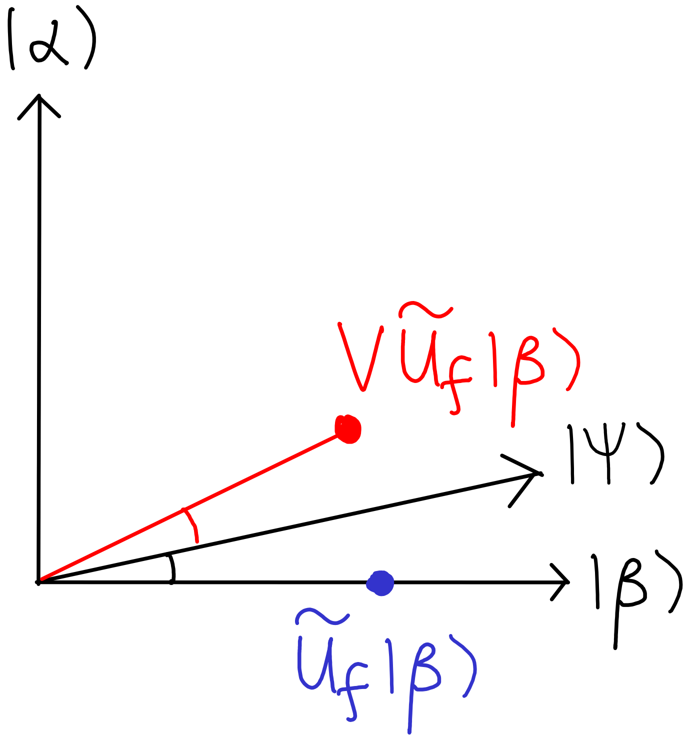
For the initial state $|\beta\rangle$

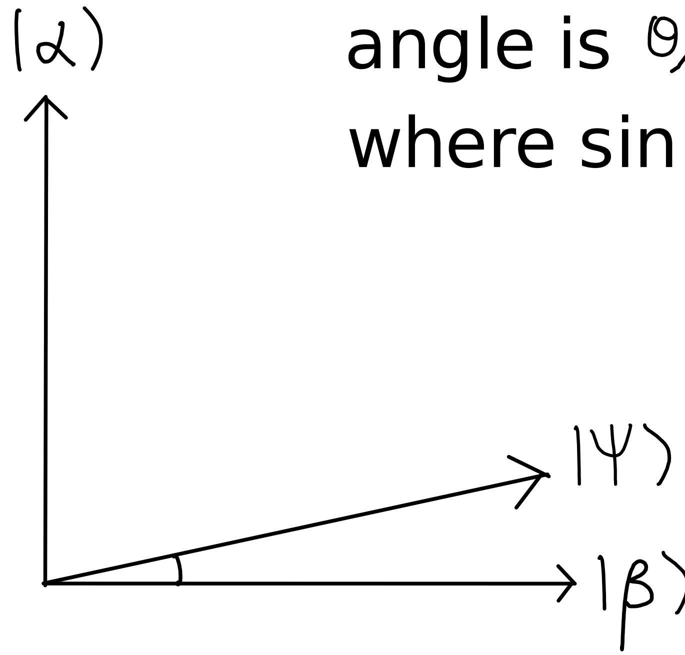
rotation of angle θ

What does Grover's iteration $V\tilde{U}_f$ do?

By linearity, suffices to check its action on a spanning set: $|\beta\rangle$, $|\psi\rangle$.

Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.





For the initial state $|\beta\rangle$

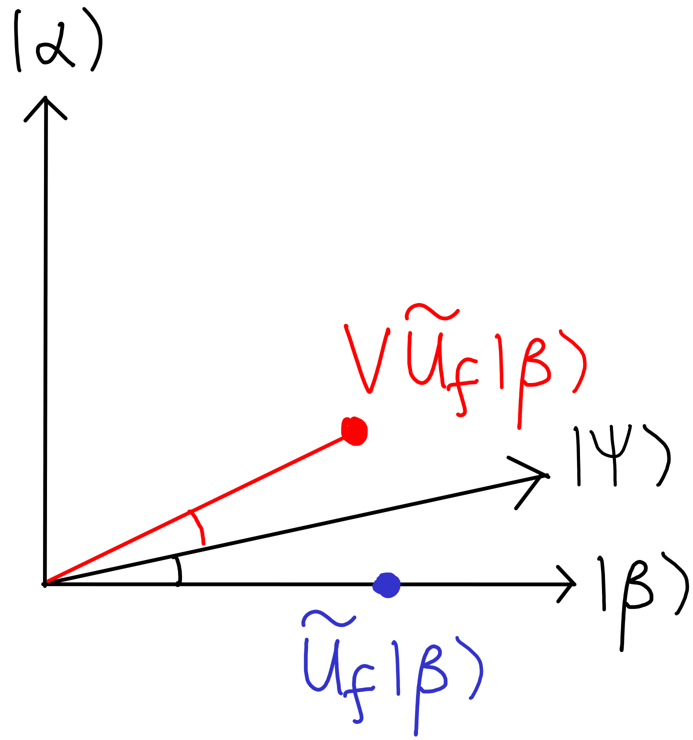
rotation of angle θ

For the initial state $|\psi\rangle$

What does Grover's iteration $V\tilde{U}_f$ do?

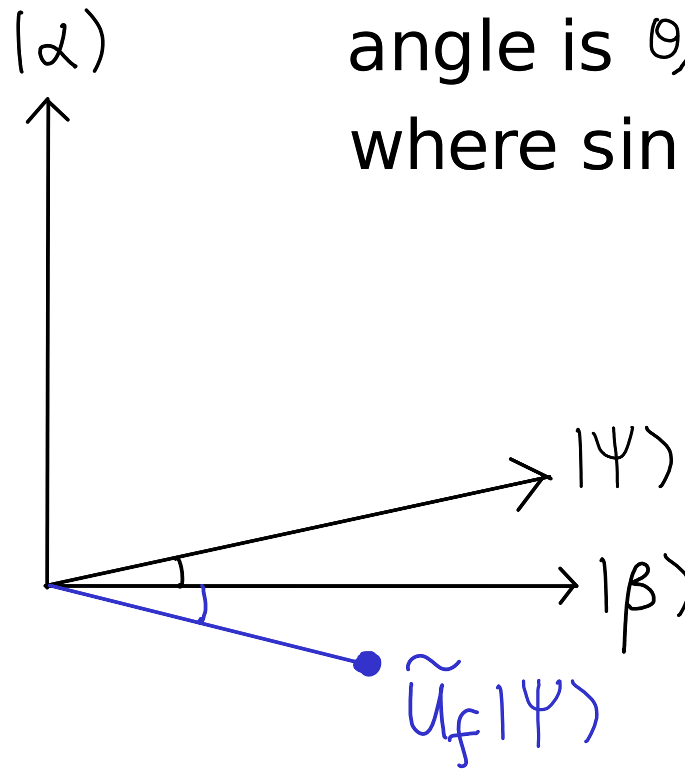
By linearity, suffices to check its action on a spanning set: $|\beta\rangle$, $|\Psi\rangle$.

Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.



For the initial state $|\beta\rangle$

rotation of angle θ

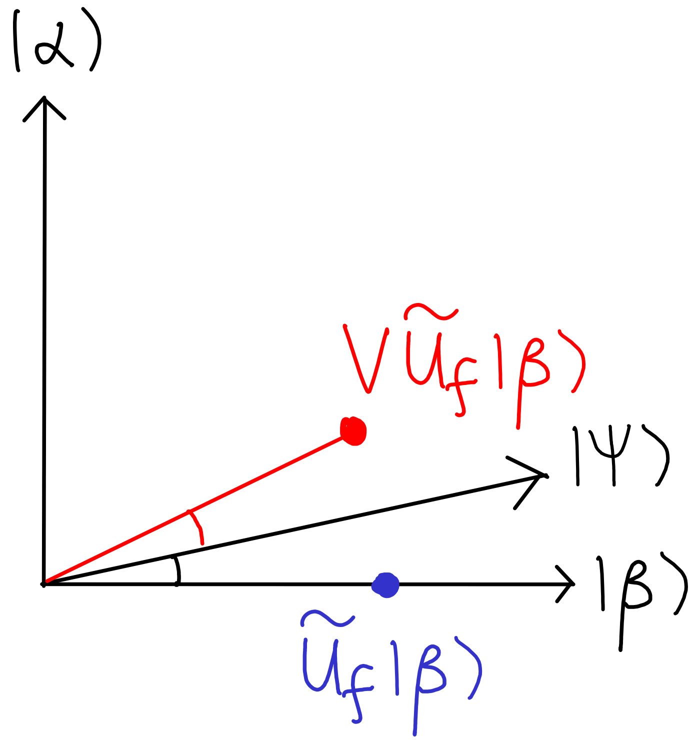


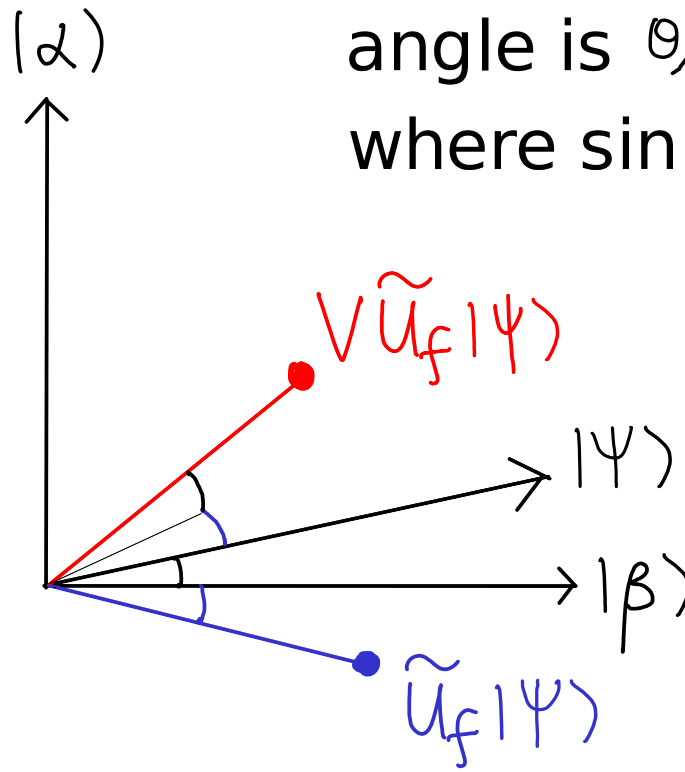
For the initial state $|\Psi\rangle$

What does Grover's iteration $V\tilde{U}_f$ do?

By linearity, suffices to check its action on a spanning set: $|\beta\rangle$, $|\psi\rangle$.

Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.





For the initial state $|\beta\rangle$

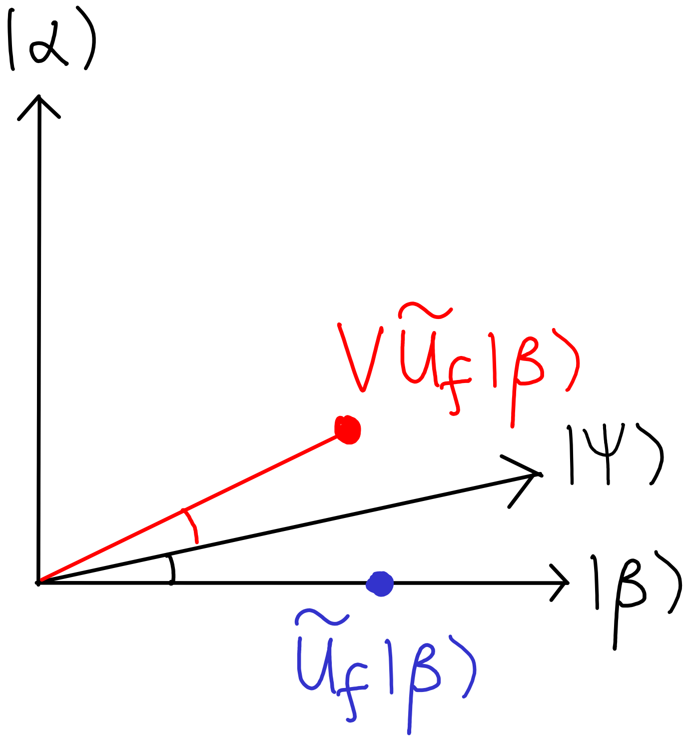
rotation of angle θ

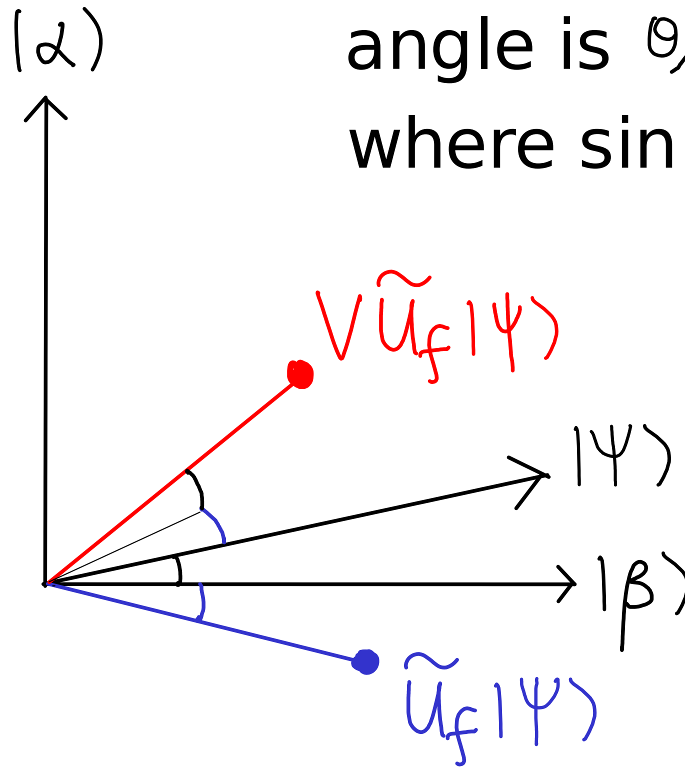
For the initial state $|\psi\rangle$

rotation of angle θ

What does Grover's iteration $V\tilde{U}_f$ do?

By linearity, suffices to check its action on a spanning set: $|\beta\rangle$, $|\psi\rangle$.



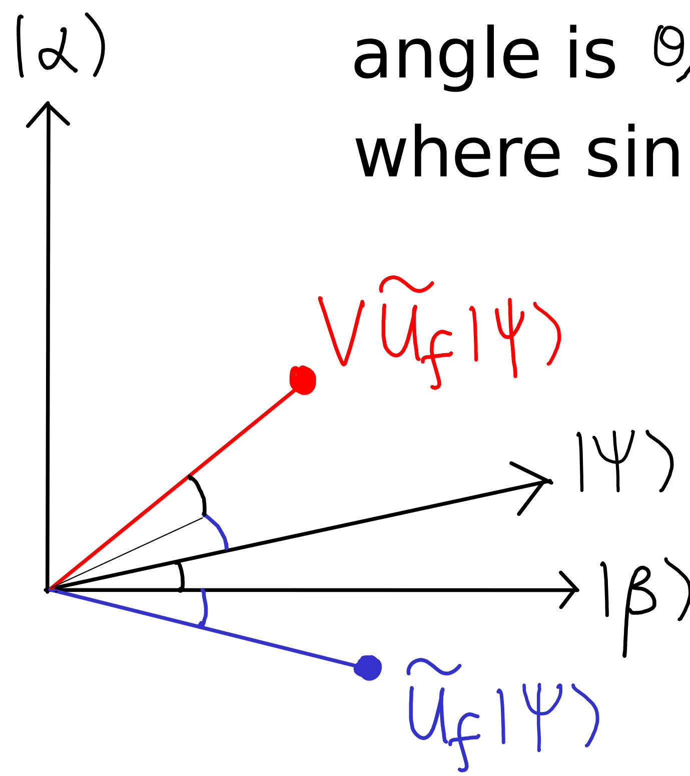


Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.

$\therefore$ $V\tilde{U}_f$ is a rotation of angle θ in the $|\beta\rangle, |\alpha\rangle$ plane. (anti-clockwise)

2 reflections make a rotation!

Optimal # of Grover's iteration



Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.

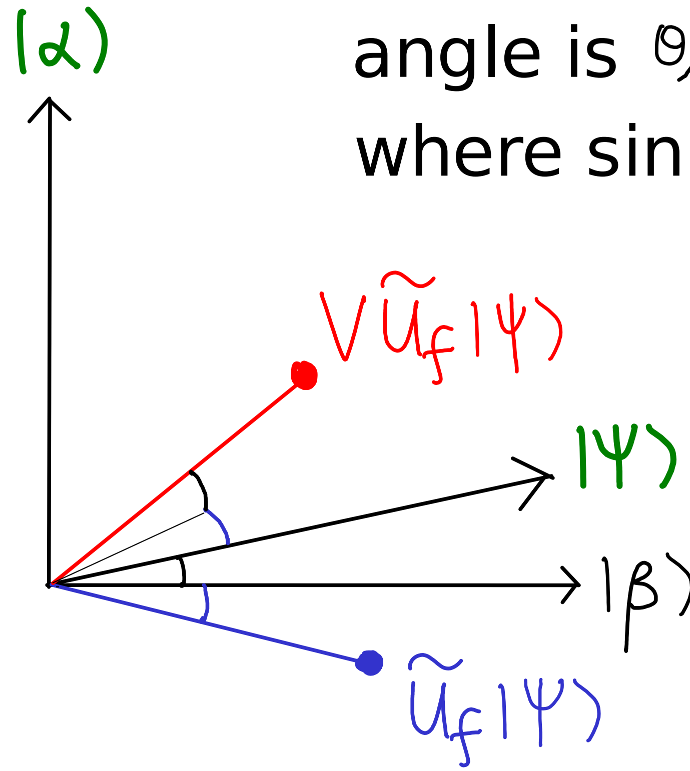
$\therefore$ $V\tilde{U}_f$ is a rotation of angle θ in the $|\beta\rangle, |\alpha\rangle$ plane. (anti-clockwise)

Optimal # of Grover's iteration

Goal: rotate $|\psi\rangle$ to as close to $|\alpha\rangle$ as possible

superposition of marked states

Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.



initial state

$\therefore$ $V\tilde{U}_f$ is a rotation of angle θ in the $|\beta\rangle, |\alpha\rangle$ plane.
(anti-clockwise)

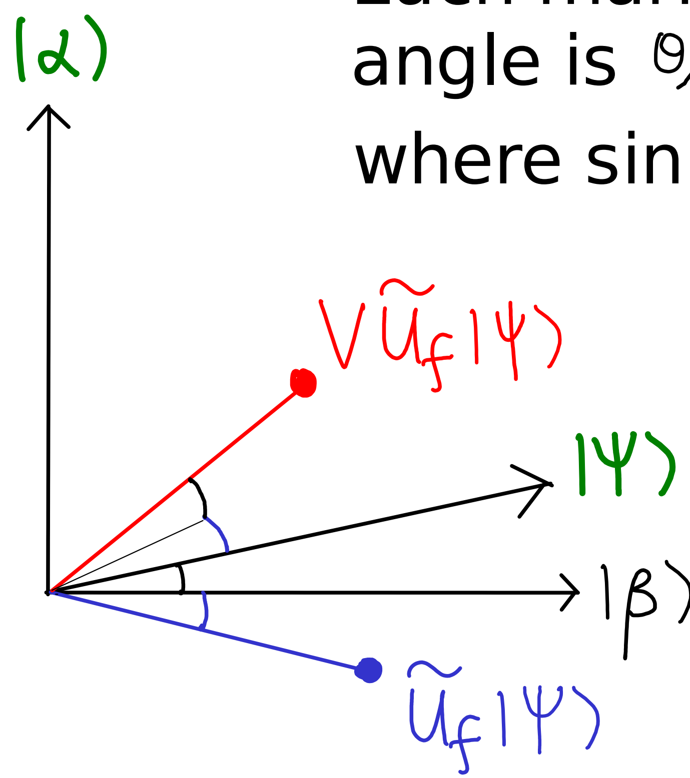
Optimal # of Grover's iteration

Goal: rotate $|\psi\rangle$ to as close to $|\alpha\rangle$ as possible

superposition of marked states

(meas $|\alpha\rangle$ in comp basis gives an outcome that is a marked item.)

Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.



initial state

$\therefore$ $V\tilde{U}_f$ is a rotation of angle θ in the $|\beta\rangle, |\alpha\rangle$ plane. (anti-clockwise)

Optimal # of Grover's iteration

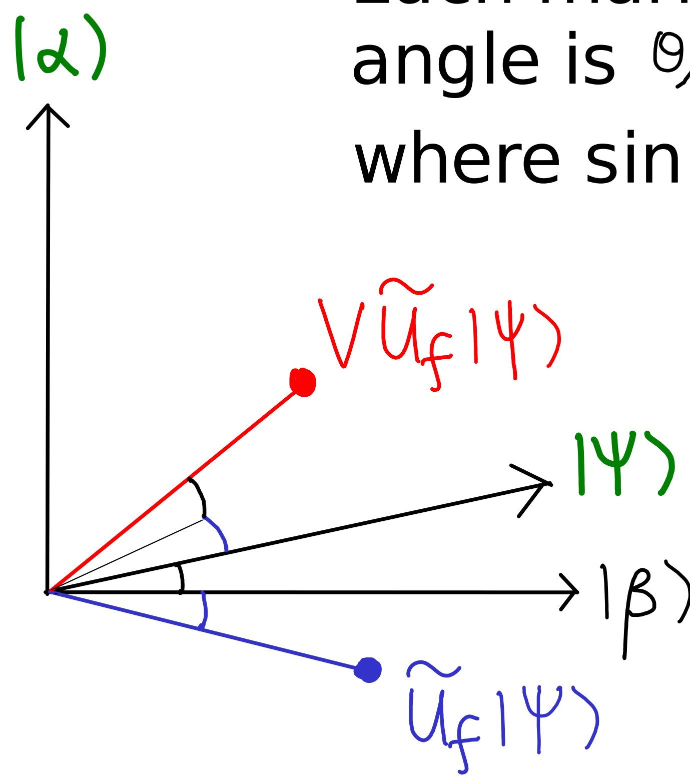
Goal: rotate $|\psi\rangle$ to as close to $|\alpha\rangle$ as possible

(meas $|\alpha\rangle$ in comp basis gives an outcome that is a marked item.)

After k iterations, state is $\left(k+\frac{1}{2}\right)\theta$ from the $|\beta\rangle$ axis. Want $\left(k+\frac{1}{2}\right)\theta \approx \frac{\pi}{2}$.

superposition of marked states

Each marked angle is $\theta/2$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.



initial state

$\therefore$ $V\tilde{U}_f$ is a rotation of angle θ in the $|\beta\rangle, |\alpha\rangle$ plane.
(anti-clockwise)

Want $\left(K+\frac{1}{2}\right)\theta \approx \frac{\pi}{2}$.

Recall $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$ is very small, so, $\frac{\theta}{2} \approx \sqrt{\frac{M}{N}}$.

Want $\left(k+\frac{1}{2}\right)\theta \approx \frac{\pi}{2}$.

Recall $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$ is very small, so, $\frac{\theta}{2} \approx \sqrt{\frac{M}{N}}$.

Solving $\left(k+\frac{1}{2}\right)2\sqrt{\frac{M}{N}} \approx \frac{\pi}{2}$,

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2}.$$

We take k to be the integer closest to $\frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2}$.

Grover's algorithm:

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$, $V = 2|\psi\rangle\langle\psi| - I$

Blackbox: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase kick back: $U_f |x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

1. Initialize state to $|\psi\rangle|-\rangle$
2. Apply Grover's iteration $G = (V \otimes I)\, U_f$ k times, for k to be determined.
3. Measure 1st register in the computational basis.
4. Check if the measurement outcome is a marked item by using U_f.

Yes with prob close to 1.

Repeat t = O(1) times, prob failure $\sim$ exp(-t).

Summary:

We proved that quantum query complexity of the unstructured search problem (variation 2) is $O\left(\sqrt{\frac{N}{M}}\right)$.

Optimality: part (ii) of topic07-2

Further question:

What is the circuit complexity of the algorithm?

Circuit complexity of Grover's algorithm

For simplicity, $N = 2^n$.

State initialization:
(n+1) $|0\rangle$ states, apply X to the last qubit,
and then apply Hadamard gates to all.

Circuit complexity of Grover's algorithm

For simplicity, $N = 2^n$.

State initialization:
(n+1) $|0\rangle$ states, apply X to the last qubit, and then apply Hadamard gates to all.

Computational basis measurement:
n "individual-qubit" measurements along $|0\rangle, |1\rangle$

Remains to implement V $= 2|\psi\rangle\langle\psi| - I$.

Implementing V

Lemma: V = $2|\psi\rangle\langle\psi| - I = H^{\otimes n}\left(2|0\rangle\langle 0| - I\right)H^{\otimes n}$.

$00\cdots0$

$\leftarrow n \rightarrow$

Proof:

Implementing V

Lemma: $V = 2|\psi\rangle\langle\psi| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$.

$00\cdots0$

$\leftarrow n \rightarrow$

Proof:

Since $H^{\otimes n}|0\rangle = |\psi\rangle$,

$$H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} = |\psi\rangle\langle\psi|.$$

Implementing V

Lemma: V = $2|\psi\rangle\langle\psi| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$.

$$\underbrace{00\cdots0}_{n}$$

Proof:

Since $H^{\otimes n}|0\rangle = |\psi\rangle$,

$$H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} = |\psi\rangle\langle\psi|.$$

$$\therefore V = 2|\psi\rangle\langle\psi| - I$$

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

Implementing V

Lemma: V = $2|\psi\rangle\langle\psi| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}.$

$00\cdots0$

$\leftarrow n \rightarrow$

Proof:

Since $H^{\otimes n}|0\rangle = |\psi\rangle,$

$$H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} = |\psi\rangle\langle\psi|.$$

$$\begin{aligned}\therefore V &= 2|\psi\rangle\langle\psi| - I \\ &= 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I \\ &= H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} \qquad \because (H^{\otimes n})^2 = I\end{aligned}$$

Implementing V

Lemma: V = $2|\psi\rangle\langle\psi| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$.

$$|0\rangle = |\underbrace{00\cdots0}_{n}\rangle$$

Proof:

Since $H^{\otimes n}|0\rangle = |\psi\rangle$,

$$H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} = |\psi\rangle\langle\psi|.$$

$$\begin{aligned}
\therefore V &= 2|\psi\rangle\langle\psi| - I \\
&= 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I \\
&= H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} \qquad \because (H^{\otimes n})^2 = I
\end{aligned}$$

So we can implement V by applying n Hadamard gates, then $2|0\rangle\langle 0| - I$, and n Hadamard gates again.

Implementing $2|0\rangle\langle 0| - I$

This gate takes |0> to |0>, and |x> to -|x> on all other computational basis states.

Implementing $2|0\rangle\langle 0| - I$

This gate takes |0> to |0>, and |x> to -|x> on all other computational basis states.

Flipping the sign of this gate incurs an overall "-" sign to the state in the algorithm, with no effect on meas statistics.

Implementing $2|0\rangle\langle 0| - I$

This gate takes |0> to |0>, and |x> to -|x> on all other computational basis states.

Flipping the sign of this gate incurs an overall "-" sign to the state in the algorithm, with no effect on meas statistics.

After the sign change, the gate takes |0> to -|0>, and all other |x> to |x>.

Implementing $2|0\rangle\langle 0| - I$

This gate takes |0> to |0>, and |x> to -|x> on all other computational basis states.

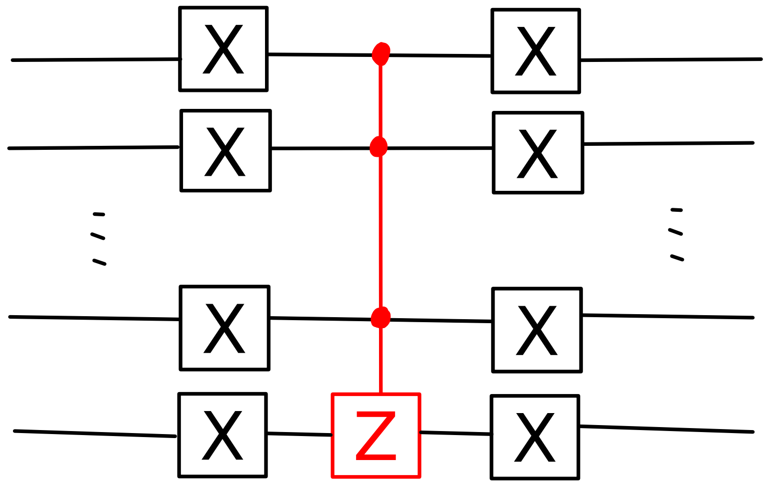
Flipping the sign of this gate incurs an overall "-" sign to the state in the algorithm, with no effect on meas statistics.

After the sign change, the gate takes |0> to -|0>, and all other |x> to |x>.

Same as negating all n bits,
then mapping |1..1> to -|1...1> & keeping all other |x>'s the same (this is a control-control-...-control-Z), and finally negating all n bits again.

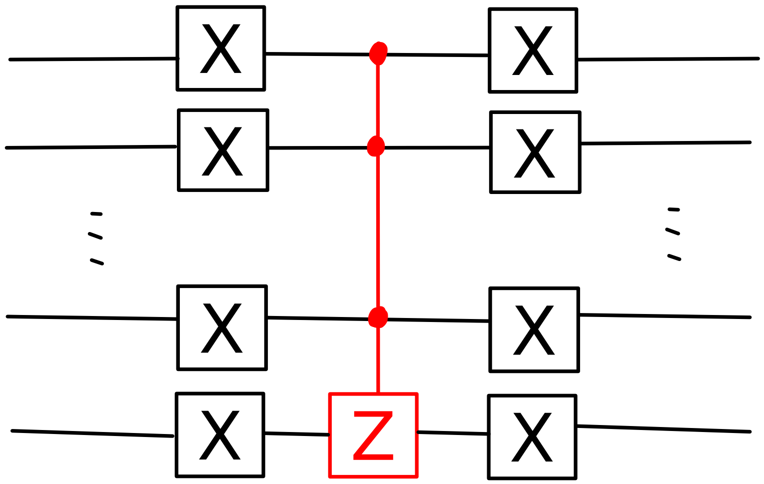
Implementing $2|0\rangle\langle 0| - I$ up to a "-" sign:

n qubits



Implementing $2|0\rangle\langle 0| - I$ up to a "-" sign:

n qubits



1 c-Z
2(n-2) Toffoli's

n-1 qubits

n-2 qubits

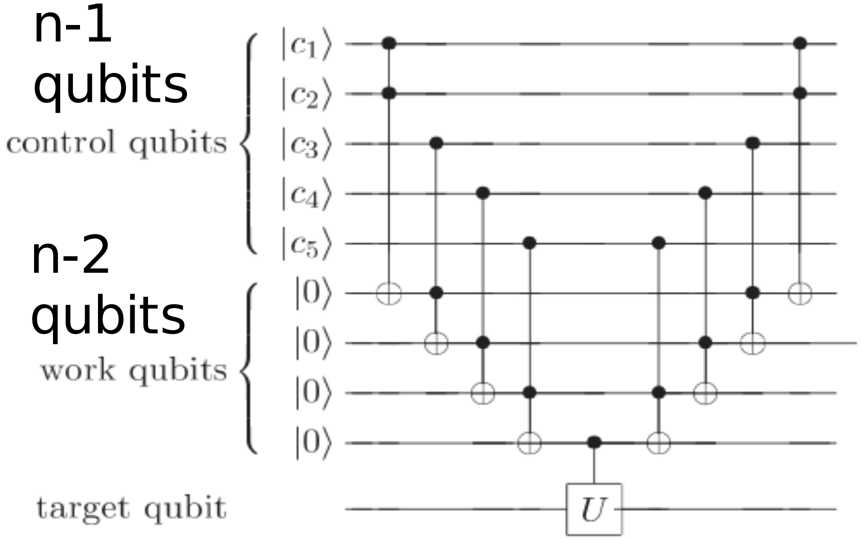
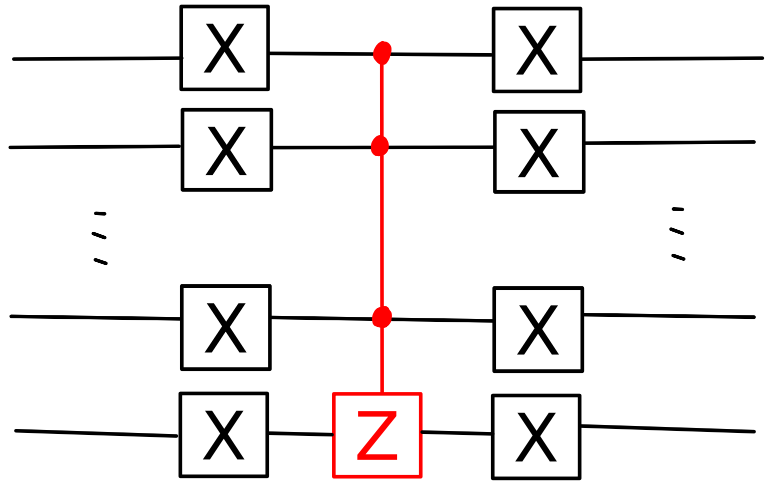


Figure 4.10. Network implementing the $C^n(U)$ operation, for the case $n = 5$.

from NC

Implementing $2|0\rangle\langle 0| - I$ up to a "-" sign:

n qubits



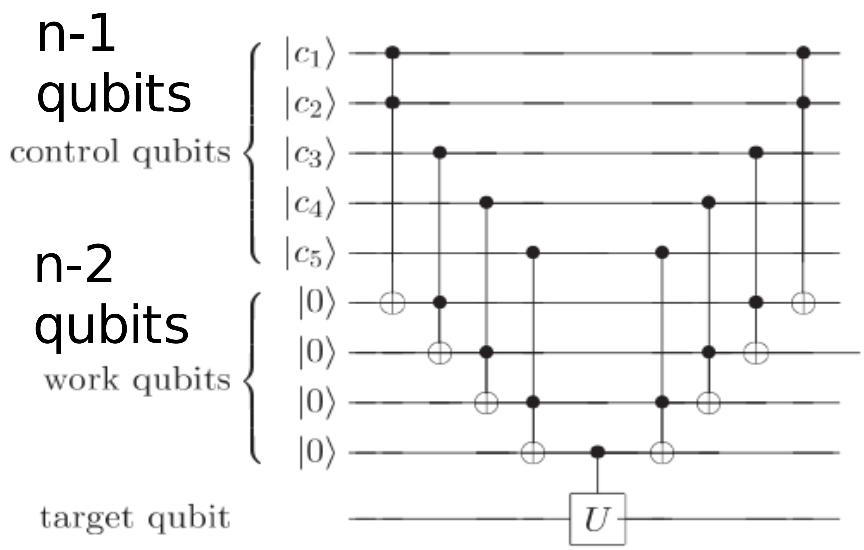


Figure 4.10. Network implementing the $C^n(U)$ operation, for the case $n = 5$.

1 c-Z
2(n-2) *
(6 CNOTs, 9 T's, 2 H's).

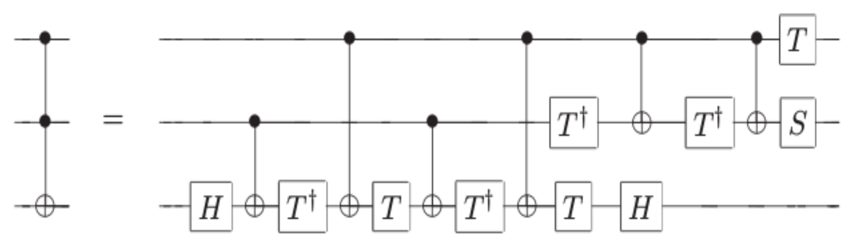
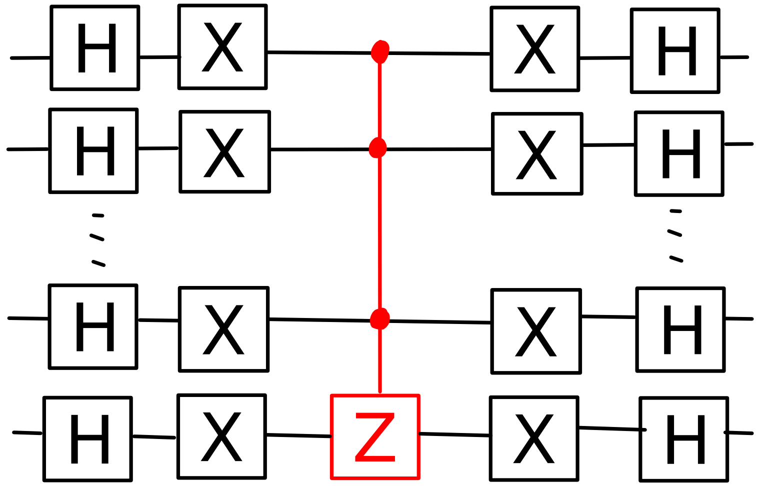


Figure 4.9. Implementation of the Toffoli gate using Hadamard, phase, controlled-NOT and $\pi/8$ gates.

from NC

Implementing $V = 2|\psi\rangle\langle\psi| - I$ up to a "-" sign:

n qubits



total: O(n)

$2n+4(n-2)+2$

$= 6n-6$ H's

$12(n-2)+1$ CNOT's

$18(n-2)$ T's

$2n$ X's

each X: 2H's,4T's

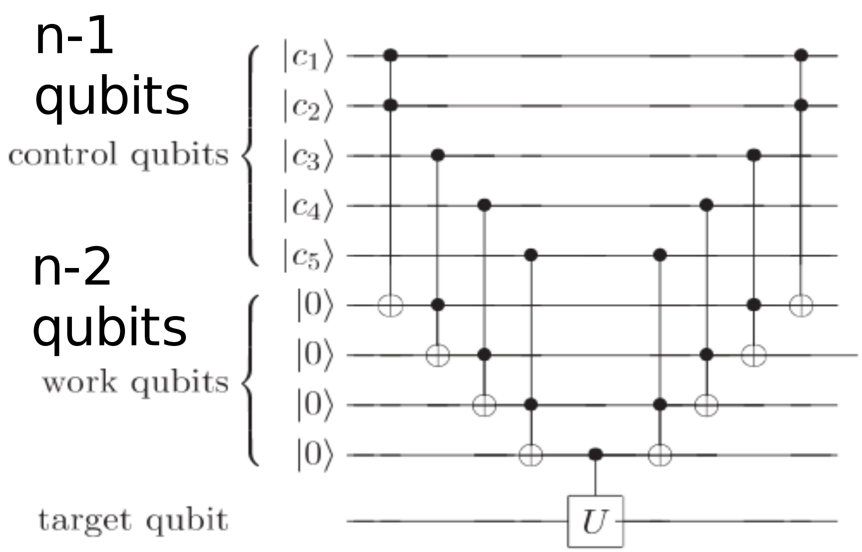


Figure 4.10. Network implementing the $C^n(U)$ operation, for the case $n = 5$.

1 c-Z

$2(n-2)$ *

(6 CNOTs, 9 T's, 2 H's).

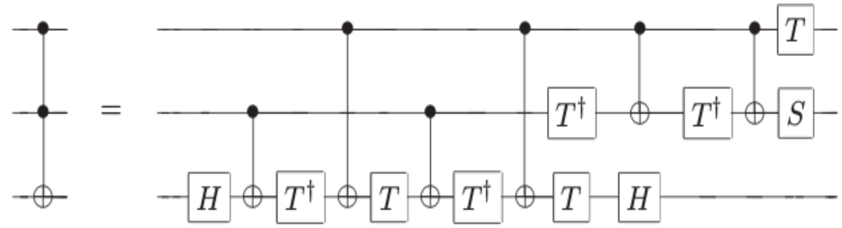
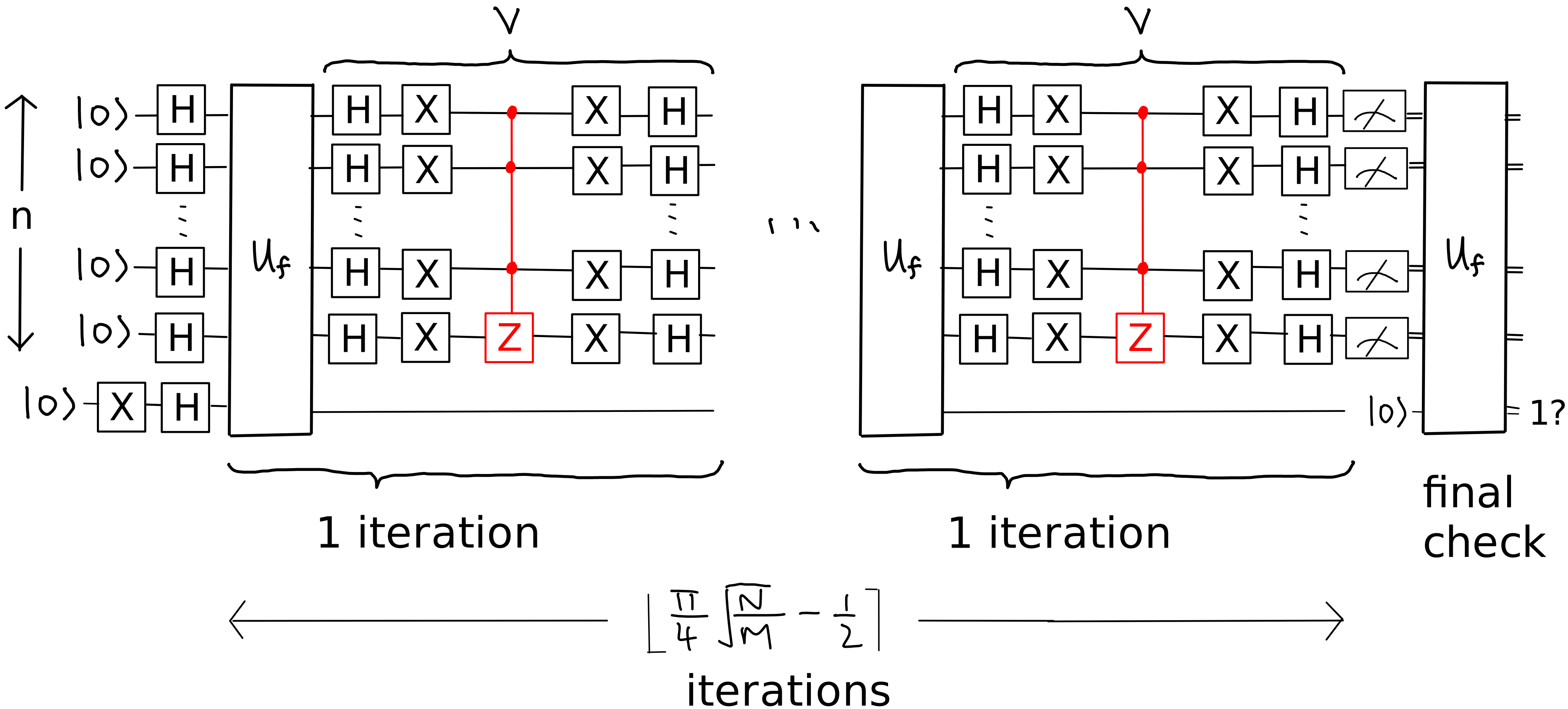


Figure 4.9. Implementation of the Toffoli gate using Hadamard, phase, controlled-NOT and $\pi/8$ gates.

Grover algorithm summary:



$$\approx O\left(\sqrt{\frac{N}{M}}\right) \text{ queries}, \quad O\left(\sqrt{\frac{N}{M}}\,\underset{\substack{\| \\ n}}{\log N}\right) \text{ gates}$$

What if M (the # marked items) is unknown? (vars 1,3)

Use a quantum algorithm to estimate M using $O(\sqrt{N})$ queries, with accuracy $O(\sqrt{M})$.

Such algorithms can be Grover like or based on phase estimation. (Reading exercise)

Alternative: trying M=1,2,4,8,... etc works too.
You see the marked item in the final check
if and only if M is about right.

7. Quantum algorithms (part 2)

√ (i) Grover's search algorithm (NC 6.1, KLM 8.1-8.2, M 4)

Differences from factoring algorithm:
- intuitive
- easily visualized
- very little analysis needed

Discussion will be relatively brief.

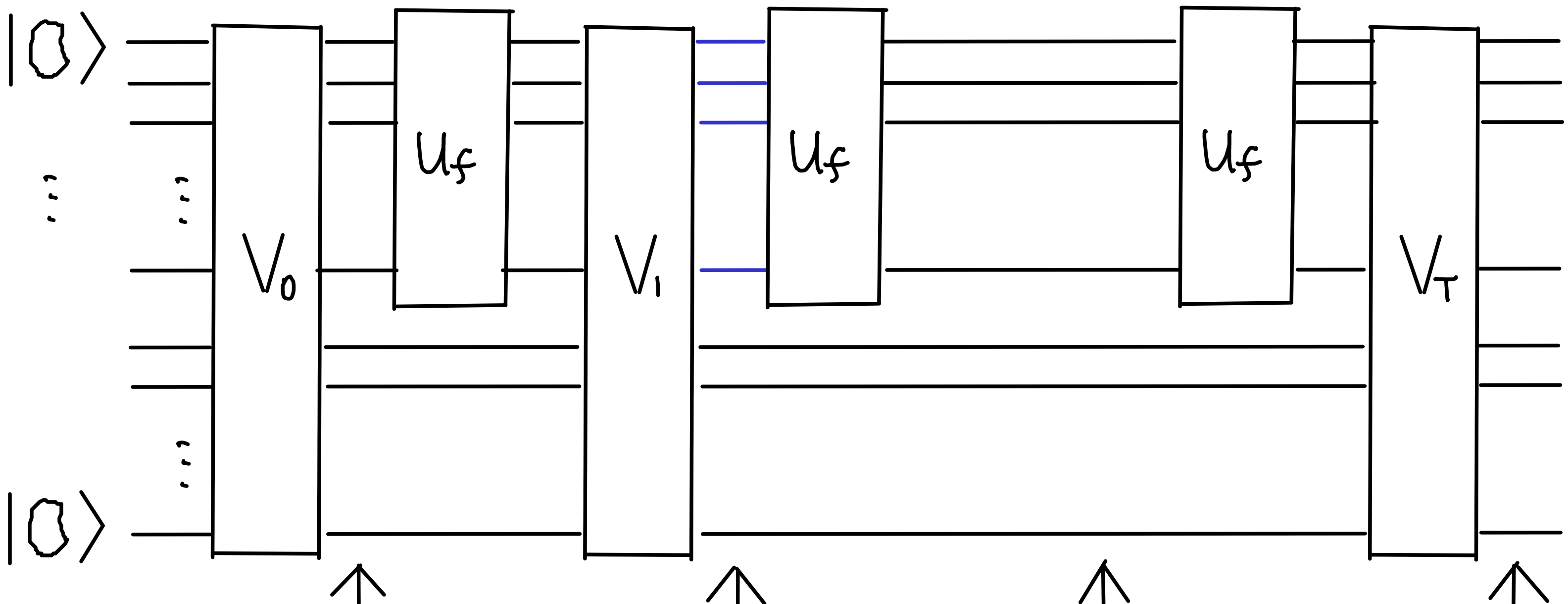
→ (ii) Optimality of Grover's algorithm (NC 6.6, KLM 9.3)

Optimality of Grover's algorithm

Theorem Given there is either no marked item or a unique marked item, $\Omega(\sqrt{N})$ queries are required to determine which case holds.

Corollary $\Omega(\sqrt{N})$ queries are required to determine if there is a marked item, or to find one.

Proof: Most general algorithm with T queries



if no mark-ed items $\quad |\psi_0\rangle \quad |\psi_1\rangle \quad |\psi_{T-1}\rangle \quad |\psi_T\rangle$

$\quad ||$

if marked item = x $\quad |\psi_0^x\rangle \quad |\psi_1^x\rangle \quad |\psi_{T-1}^x\rangle \quad |\psi_T^x\rangle$

The "no marked item case" also corresponds to Uf = I.

Let $|\psi_t\rangle$ be the state before the (t+1)-st query, in the absence of marked items.

Let $|\psi_t^x\rangle$ be the state before the (t+1)-st query, if the marked item is x.

Let $|\psi_t\rangle$ be the state before the (t+1)-st query, in the absence of marked items.

Let $|\psi_t^x\rangle$ be the state before the (t+1)-st query, if the marked item is x.

Recall Holevo-Helstrom Theorem (topic04) that two non-orthogonal states $|a\rangle, |b\rangle$ are hard to distinguish if $\| |a\rangle - |b\rangle \|$ is too small.

If $|a\rangle, |b\rangle$ are somewhat distinguishable, it is necessary that $\| |a\rangle - |b\rangle \| \geq c$ (some constant).

Let $|\psi_t\rangle$ be the state before the (t+1)-st query, in the absence of marked items.

Let $|\psi_t^x\rangle$ be the state before the (t+1)-st query, if the marked item is x.

If t queries enable us to determine if there is a marked item, it holds that: $\| \, |\psi_t\rangle - |\psi_t^x\rangle \, \| \geq c$.

Let $|\psi_t\rangle$ be the state before the (t+1)-st query, in the absence of marked items.

Let $|\psi_t^x\rangle$ be the state before the (t+1)-st query, if the marked item is x.

If t queries enable us to determine if there is a marked item, it holds that: $\| |\psi_t\rangle - |\psi_t^x\rangle \| \geq c.$

When we say "the algorithm works", it works for any marked item x, so:

$$D_t := \sum_{x=1}^{N} \| |\psi_t\rangle - |\psi_t^x\rangle \| \geq cN.$$

(Similar if alg works for average case input.)

How does D_t change with each query?

For one x:

$$\| \, |\psi_{t+1}\rangle - |\psi^{x}_{t+1}\rangle \, \|$$

$$= \| \, V_t |\psi_t\rangle - V_t U_f |\psi^{x}_t\rangle \, \|$$

For one x:

$$\| \, |\psi_{t+1}\rangle - |\psi^{x}_{t+1}\rangle \, \|$$

$$= \| \, V_t |\psi_t\rangle - V_t U_f |\psi^{x}_t\rangle \, \|$$

$$= \| \, |\psi_t\rangle - U_f |\psi^{x}_t\rangle \, \|$$

$$\left\{ \begin{aligned} & \| W|a\rangle - W|b\rangle \|^2 \\ &= (\langle a|W^\dagger - \langle b|W^\dagger)(W|a\rangle - W|b\rangle) \\ &= (\langle a| - \langle b|)(|a\rangle - |b\rangle) \\ &= \| |a\rangle - |b\rangle \|^2 \end{aligned} \right.$$

For one x:

$$\| |\psi_{t+1}\rangle - |\psi^x_{t+1}\rangle \|$$

$$= \| V_t |\psi_t\rangle - V_t U_f |\psi^x_t\rangle \|$$

$$= \| \quad |\psi_t\rangle - \quad U_f |\psi^x_t\rangle \|$$

$$\left\{\begin{aligned} & \| W|a\rangle - W|b\rangle \|^2 \\ &= (\langle a|W^\dagger - \langle b|W^\dagger)(W|a\rangle - W|b\rangle) \\ &= (\langle a| - \langle b|)(|a\rangle - |b\rangle) \\ &= \| |a\rangle - |b\rangle \|^2 \end{aligned}\right.$$

$$= \| |\psi_t\rangle - |\psi^x_t\rangle + |\psi^x_t\rangle - U_f |\psi^x_t\rangle \|$$

$$= \underbrace{\| |\psi_t\rangle - |\psi^x_t\rangle \|}_{\text{bound this recursively}} + \underbrace{\| |\psi^x_t\rangle - U_f |\psi^x_t\rangle \|}_{\text{diff induced by 1 use of } U_f \text{ on } |\psi^x_t\rangle}$$ by Δ inequality

Let $|\psi_t^x\rangle = \sum_{y=1}^{N} \alpha_{y,t} |y\rangle |\phi_y^t\rangle .$

Use method 2 to express bipartite state, topic03-02, p7.

computational basis on input to Uf

register not acted on by Uf

Let $|\Psi_t^x\rangle = \sum_{y=1}^{N} \alpha_{y,t} |y\rangle |\phi_y^t\rangle$.

Use method 2 to express bipartite state, topic03-02, p7.

computational basis on input to Uf

register not acted on by Uf

$$U_f |\Psi_t^x\rangle - |\Psi_t^x\rangle = \left(-2|x\rangle\langle x| + I\right)|\Psi_t^x\rangle - |\Psi_t^x\rangle$$

$$= -2|x\rangle\langle x|\,|\Psi_t^x\rangle$$

$$= -2|x\rangle\ \alpha_{x,t}\,|\phi_x^t\rangle$$

WLOG, Uf used with phase kick-back (use blackboard).

Let $|\psi_t^x\rangle = \sum_{y=1}^{N} \alpha_{y,t} |y\rangle |\phi_y^t\rangle$.

Use method 2 to express bipartite state, topic03-02, p7.

computational basis on input to Uf

register not acted on by Uf

$$
\begin{aligned}
U_f |\psi_t^x\rangle - |\psi_t^x\rangle &= (-2|x\rangle\langle x| + I)|\psi_t^x\rangle - |\psi_t^x\rangle \\
&= -2|x\rangle\langle x| \, |\psi_t^x\rangle \\
&= -2|x\rangle \; \alpha_{x,t} \, |\phi_x^t\rangle
\end{aligned}
$$

WLOG, Uf used with phase kick-back (use blackboard).

$$
\| U_f |\psi_t^x\rangle - |\psi_t^x\rangle \| = 2 |\alpha_{x,t}|
$$

$$
\begin{aligned}
\therefore \; \| |\psi_{t+1}\rangle - |\psi_{t+1}^x\rangle \| &\leq \| |\psi_t\rangle - |\psi_t^x\rangle \| + \| |\psi_t^x\rangle - U_f |\psi_t^x\rangle \| \\
&= \| |\psi_t\rangle - |\psi_t^x\rangle \| + 2 |\alpha_{x,t}| \\
&\leq 2 \sum_{j=0}^{t} |\alpha_{x,j}| \quad \text{(recursive argument)}
\end{aligned}
$$

Combining all possible x's:

$$c N \leq \sum_{x=1}^{N} \| \, |\psi_T\rangle - |\psi_T^x\rangle \, \|$$

$$\leq \sum_{x=1}^{N} 2 \sum_{j=0}^{T-1} |\alpha_{x,j}|$$

from last page

Combining all possible x's:

$$CN \leq \sum_{x=1}^{N} \| |\psi_T\rangle - |\psi_T^x\rangle \|$$

$$\leq \sum_{x=1}^{N} 2 \sum_{j=0}^{T-1} |\alpha_{x,j}|$$

from last page

$$= 2 \sum_{j=0}^{T-1} \sum_{x=1}^{N} |\alpha_{x,j}|$$

Combining all possible x's:

$$CN \leq \sum_{x=1}^{N} \| \, |\psi_T\rangle - |\psi_T^x\rangle \, \|$$

$$\leq \sum_{x=1}^{N} 2 \sum_{j=0}^{T-1} |\alpha_{x,j}|$$

from last page

$$= 2 \sum_{j=0}^{T-1} \sum_{x=1}^{N} |\alpha_{x,j}|$$

$$= 2 \sum_{j=0}^{T-1} \sqrt{N} \cdot \sqrt{\sum_{x=1}^{N} |\alpha_{x,j}|^2}$$

Cauchy-Schwarz ineq

$|a \cdot b| \leq \sqrt{(a \cdot a)(b \cdot b)}$

Here $b = (1, 1, \ldots, 1)$.

Combining all possible x's:

$$cN \leq \sum_{x=1}^{N} \left\| |\psi_T\rangle - |\psi_T^x\rangle \right\|$$

$$\leq \sum_{x=1}^{N} 2 \sum_{j=0}^{T-1} |\alpha_{x,j}|$$

from last page

$$= 2 \sum_{j=0}^{T-1} \sum_{x=1}^{N} |\alpha_{x,j}|$$

Cauchy-Schwarz ineq

$$|a \cdot b| \leq \sqrt{(a \cdot a)(b \cdot b)}$$

Here $b = (1, 1, \ldots, 1)$.

$$= 2 \sum_{j=0}^{T-1} \sqrt{N} \cdot \underbrace{\sqrt{\sum_{x=1}^{N} |\alpha_{x,j}|^2}}_{1,\ \text{by def of } |\psi_j^x\rangle}$$

$$= 2 \sum_{j=0}^{T-1} \sqrt{N} = 2T\sqrt{N}.$$

Combining all possible x's:

$$cN \le \sum_{x=1}^{N} \left\| |\psi_T\rangle - |\psi_T^x\rangle \right\|$$

$$\le \sum_{x=1}^{N} 2 \sum_{j=0}^{T-1} |\alpha_{x,j}|$$

from last page

$$= 2 \sum_{j=0}^{T-1} \sum_{x=1}^{N} |\alpha_{x,j}|$$

Cauchy-Schwarz ineq

$|a \cdot b| \le \sqrt{(a \cdot a)(b \cdot b)}$

Here $b = (1, 1, \ldots, 1)$.

$$= 2 \sum_{j=0}^{T-1} \sqrt{N} \cdot \sqrt{\sum_{x=1}^{N} |\alpha_{x,j}|^2}$$

1, by def of $|\psi_j^x\rangle$

$$= 2 \sum_{j=0}^{T-1} \sqrt{N} = 2T\sqrt{N}.$$

$$\therefore T \ge \Omega(\sqrt{N})$$