Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 17 (2017)

Jon Yard

QNC 3126

jyard@uwaterloo.ca

http://math.uwaterloo.ca/~jyard/qic710

Grover’s quantum search algorithm

Quantum search problem

Given: a black box computing $f: \{0,1\}^n \to \{0,1\}$

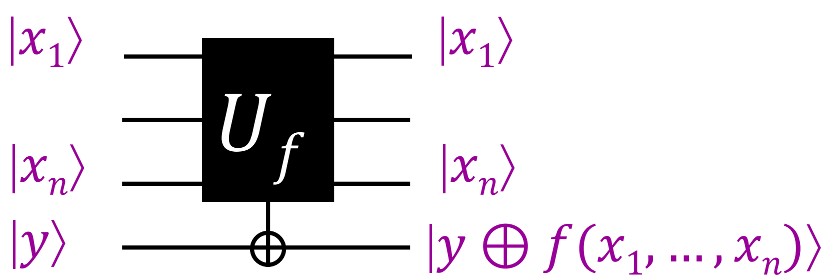
Goal: determine if f is ***satisfiable*** (if $\exists x \in \{0,1\}^n$ s.t. $f(x) = 1$).

In positive instances, it makes sense to also ***find*** such a satisfying assignment x.

Classically, using probabilistic procedures, order 2^n queries are necessary to succeed—even with probability $3/4$. (say)

Grover's ***quantum*** algorithm makes only $O\left(\sqrt{2^n}\right)$ queries

Query:



[Grover '96]

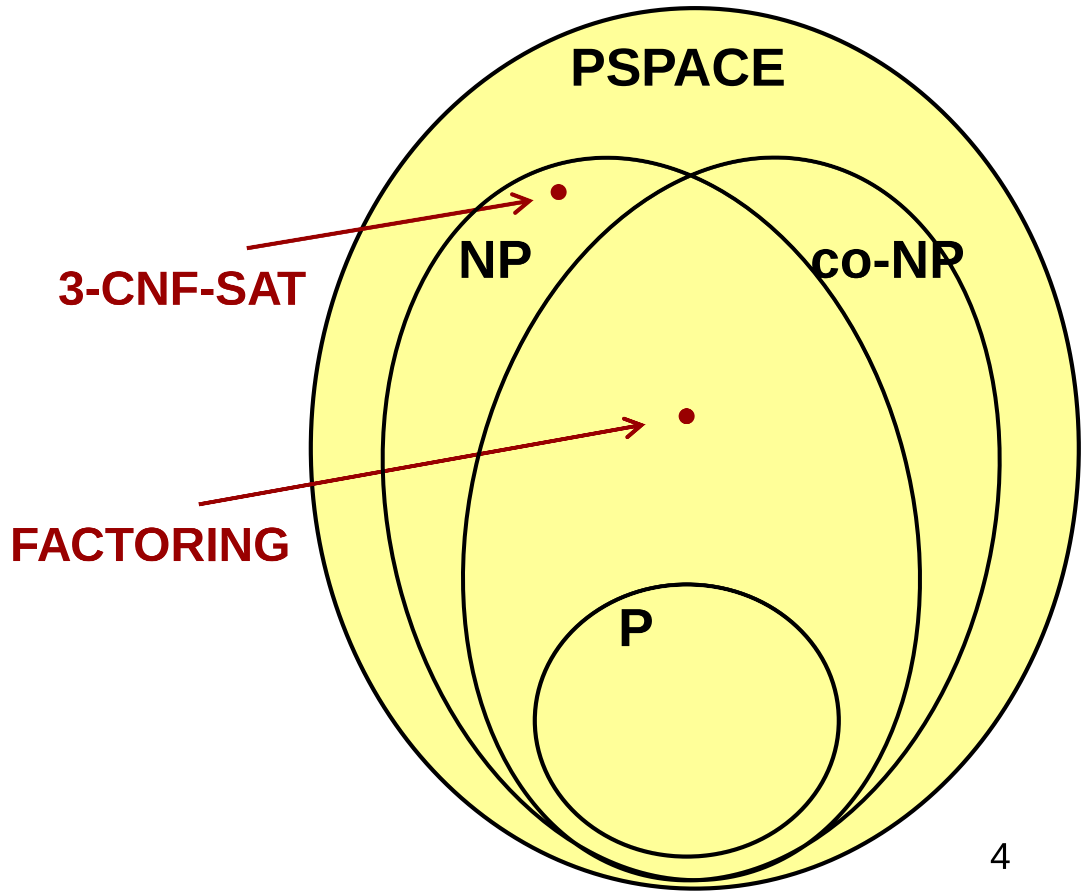
Applications of quantum search

The function f could be realized as a **3-CNF formula**:

$$f(x_1, \ldots, x_n) = (x_1 \vee \bar{x}_3 \vee x_4) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge \cdots \wedge (\bar{x}_1 \vee x_5 \vee \bar{x}_n)$$

Alternatively, the search could be for a certificate for any problem in **NP**

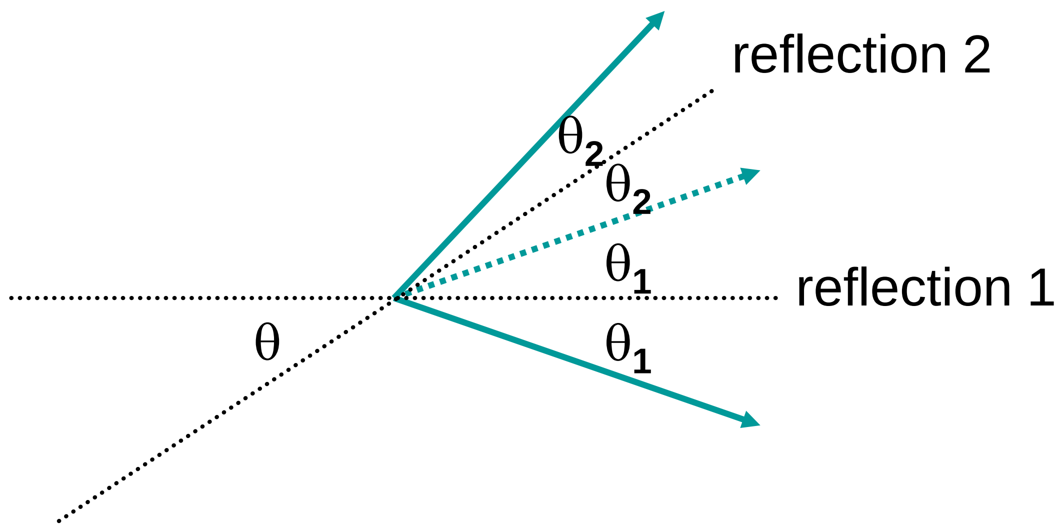
The resulting quantum algorithms appear to be ***quadratically*** more efficient than the best classical algorithms known



Prelude to Grover's algorithm:

two reflections = a rotation

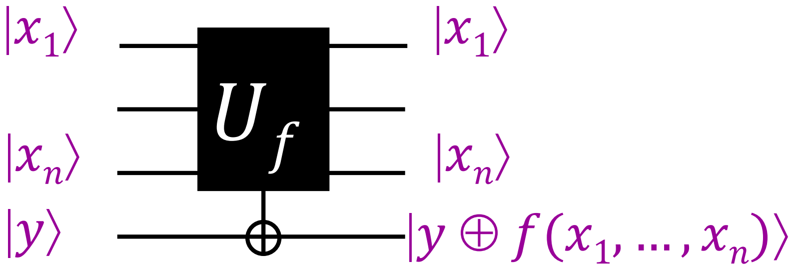
Consider two lines with intersection angle θ:



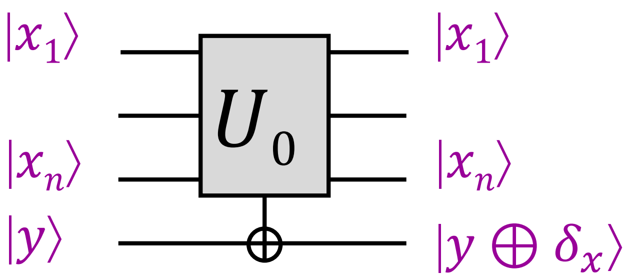
Net effect: rotation by angle 2θ, ***regardless of starting vector***

Grover's algorithm: description I

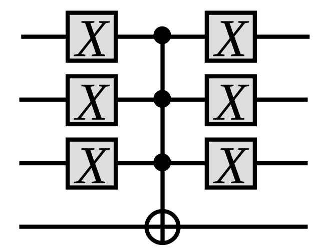
Basic operations used:



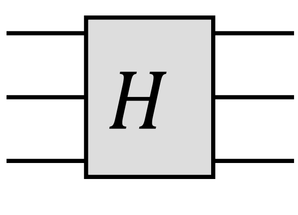
$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$



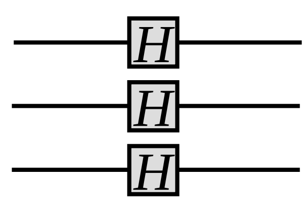
Implementation?



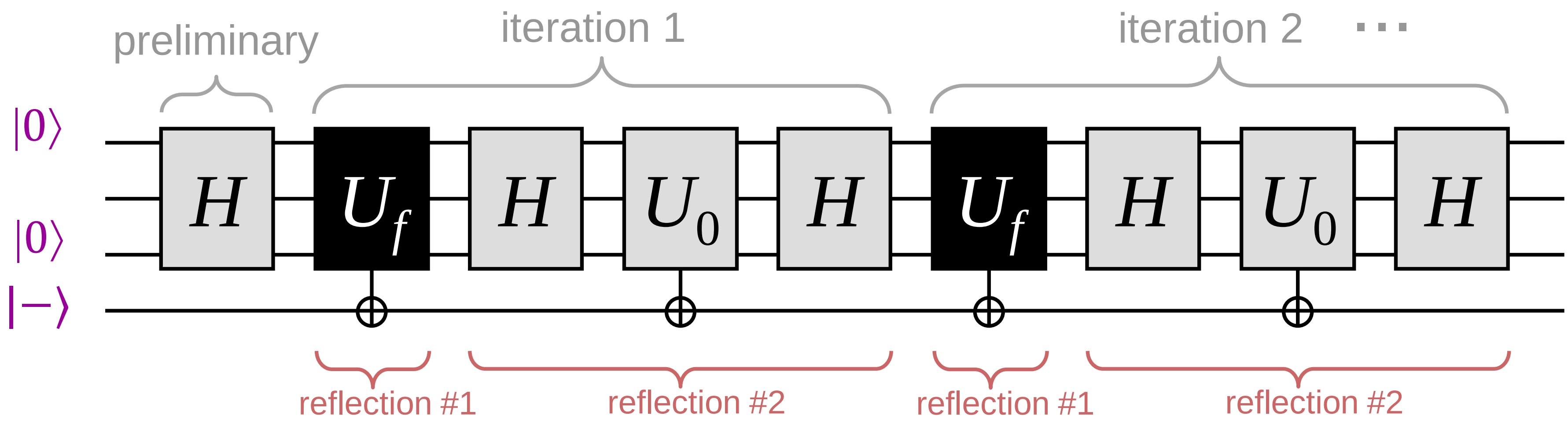
$$U_0|x\rangle|-\rangle = (-1)^{\delta_x}|x\rangle|-\rangle$$



Hadamard



Grover's algorithm: description II



1. construct state $H|0\cdots0\rangle|-\rangle$
2. <u>repeat</u> k <u>times</u>:
   apply $-HU_0HU_f$ to state
3. measure state, check if result $x \in \{0,1\}^n$ satisfies $f(x) = 1$

(The setting of k will be determined later)

From now on, we ignore the $|-\rangle$ qubit, writing $U_f|x\rangle = (-1)^{f(x)}|x\rangle$, etc.

Grover's algorithm: analysis I

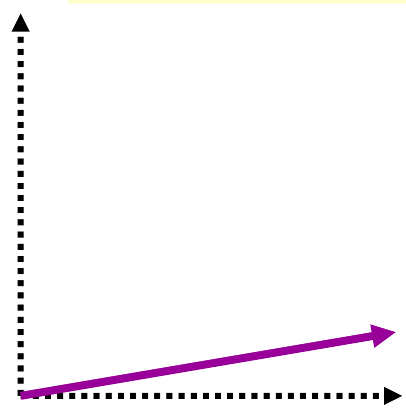
Let $A = f^{-1}(1) = \{x \in \{0,1\}^n : f(x) = 1\}$
$B = f^{-1}(0) = \{x \in \{0,1\}^n : f(x) = 0\}$
$N = 2^n,\ a = |A|,\ b = |B|$

interesting case: $a \ll N$

Let $|A\rangle = \dfrac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$ and $|B\rangle = \dfrac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$

Consider the space spanned by $|A\rangle$ and $|B\rangle$

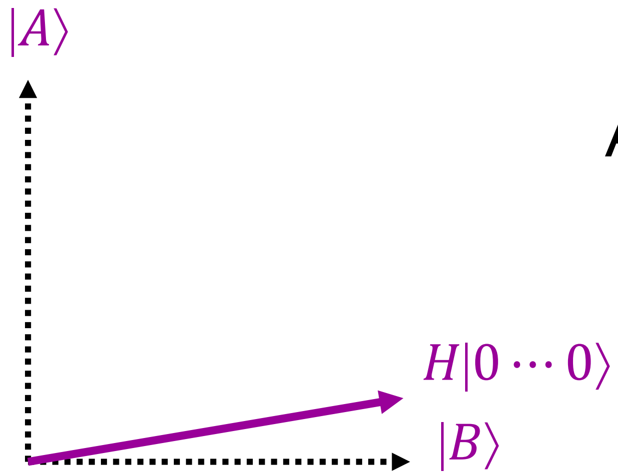
$|A\rangle$ ← goal is to get close to this state



$$H|0\cdots 0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = \sqrt{\frac{a}{N}}\,|A\rangle + \sqrt{\frac{b}{N}}\,|B\rangle$$

$|B\rangle$

Grover's algorithm: analysis II



Algorithm: $\left(-HU_0HU_f\right)^k H|0\cdots0\rangle$

Observation:

U_f is a reflection about $|B\rangle$: $U_f|A\rangle = -|A\rangle$ and $U_f|B\rangle = |B\rangle$.

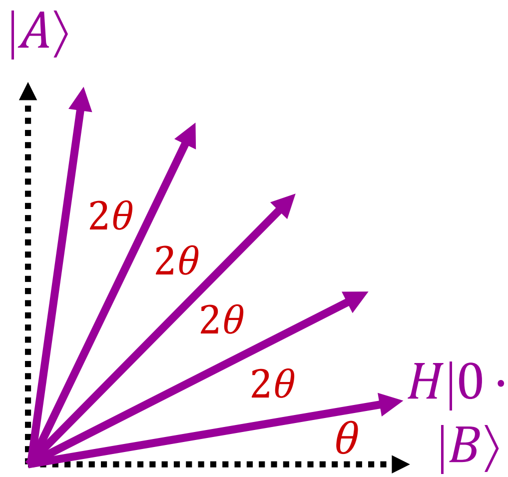
Question: what is $-HU_0H$? **Answer:** a reflection about $H|0\cdots0\rangle$

Proof:

$$-HU_0H(H|0\cdots0\rangle) = -HU_0|0\cdots0\rangle = -H(-|0\cdots0\rangle) = H|0\cdots0\rangle$$

$$-HU_0H(H|0\cdots0\rangle)^{\perp} = -HU_0|0\cdots0\rangle^{\perp} = -H|0\cdots0\rangle^{\perp} = -(H|0\cdots0\rangle)^{\perp}$$

Grover's algorithm: analysis III



Algorithm: $\left(-HU_0HU_f\right)^k H|0\cdots 0\rangle$

$$H|0\cdots 0\rangle = \sin(\theta)|A\rangle + \cos(\theta)\,|B\rangle = \sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle$$

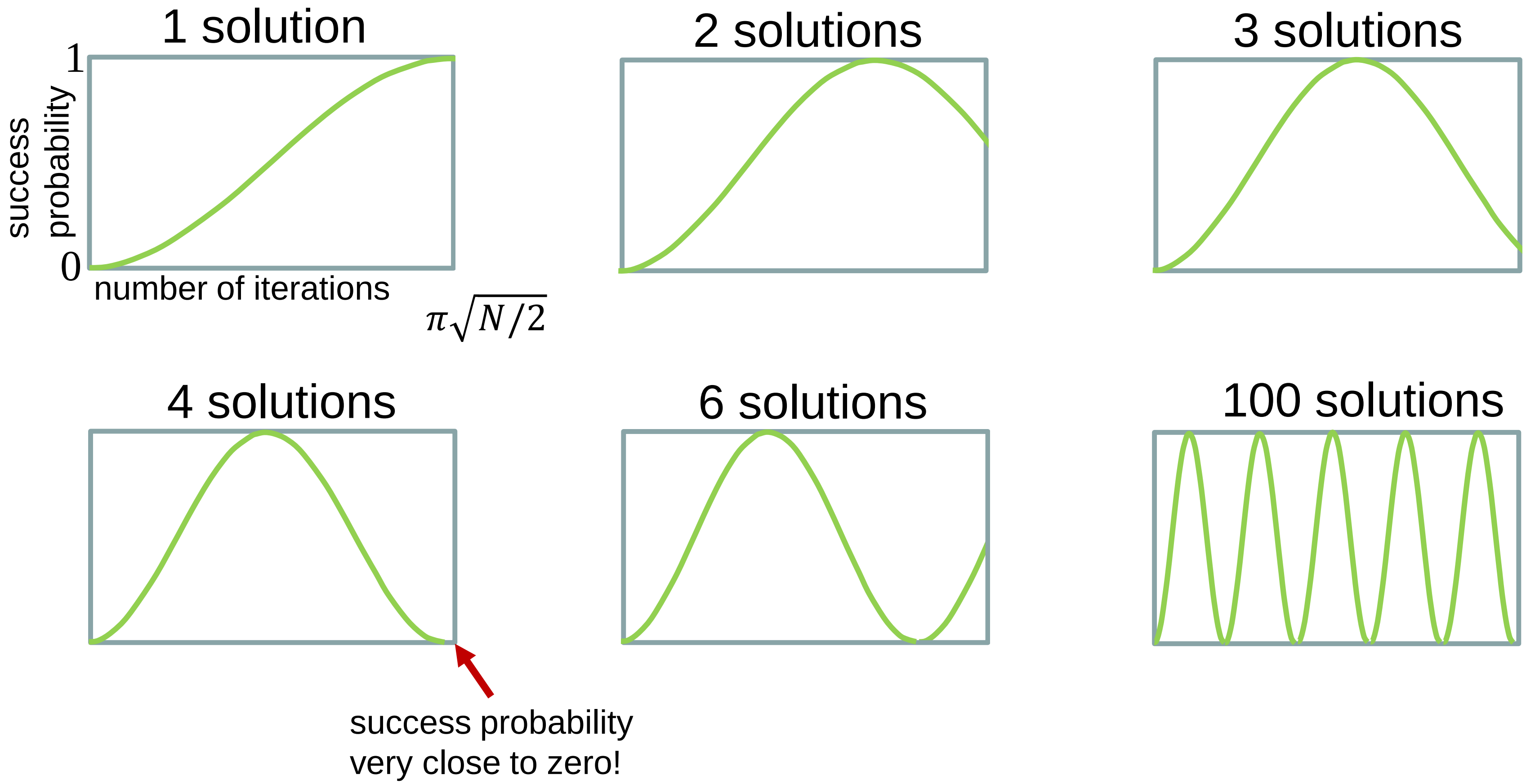
Since $-HU_0HU_f$ is a composition of two reflections, it is a rotation by $\mathbf{2\theta}$, where $\sin(\theta) = \sqrt{a/N}$ so $\theta \approx \sqrt{a/N}$.

When $a = 1$, we want $(2k+1)\left(1/\sqrt{N}\right) \approx \pi/2$, so $k \approx (\pi/4)\sqrt{N}$.

More generally, it suffices to set $k \approx (\pi/4)\sqrt{N/a}$.

Question: what if a is not known in advance?

Unknown number of solutions



Choose a ***random*** k in the range to get good success probability.

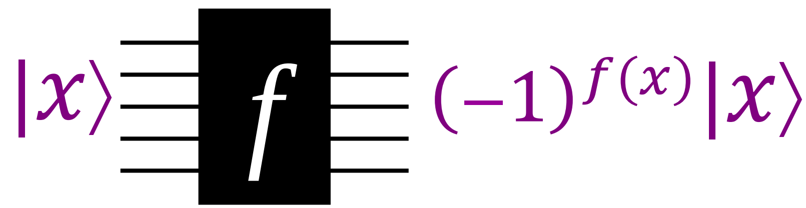
Optimality of Grover’s algorithm

Optimality of Grover's algorithm I

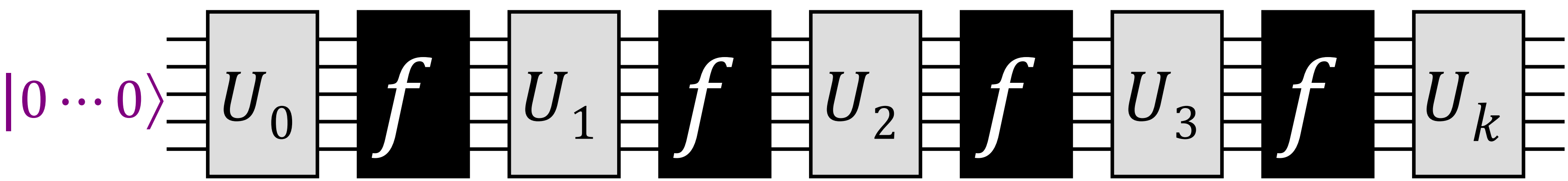
Theorem: any quantum search algorithm for $f:\{0,1\}^n \to \{0,1\}$ must make $\Omega(\sqrt{2^n})$ queries to f (if f is used as a black-box).

Proof (of a slightly simplified version)**:**

Assume queries are of the form



and that a k-query algorithm is of the form

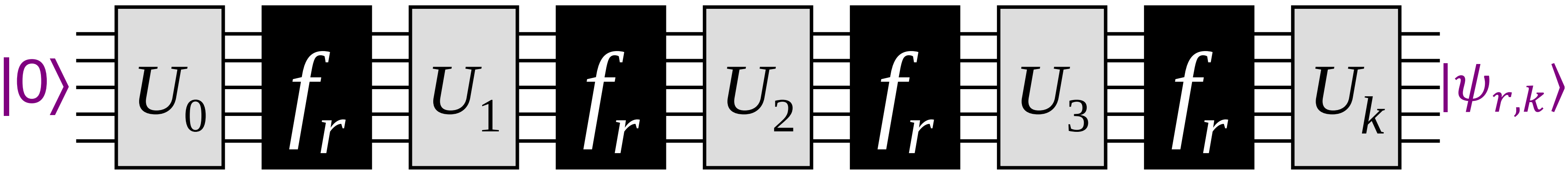


Where $U_0, U_1, U_2, \ldots, U_k$ are arbitrary unitary operations.

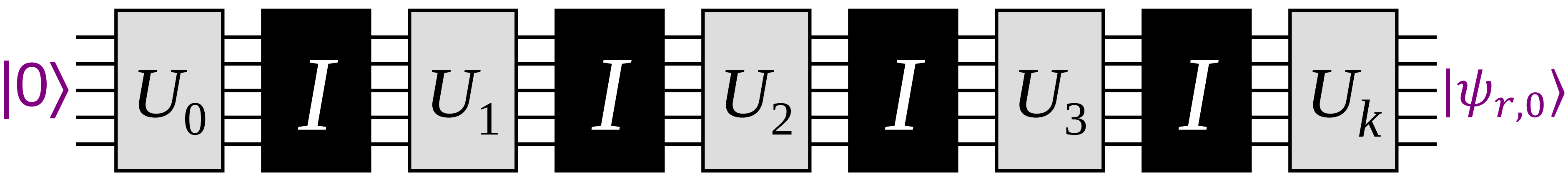
Optimality of Grover's algorithm II

Define $f_r\colon \{0,1\}^n \to \{0,1\}$ as $f_r(x) = 1$ iff $x = r$.

Consider



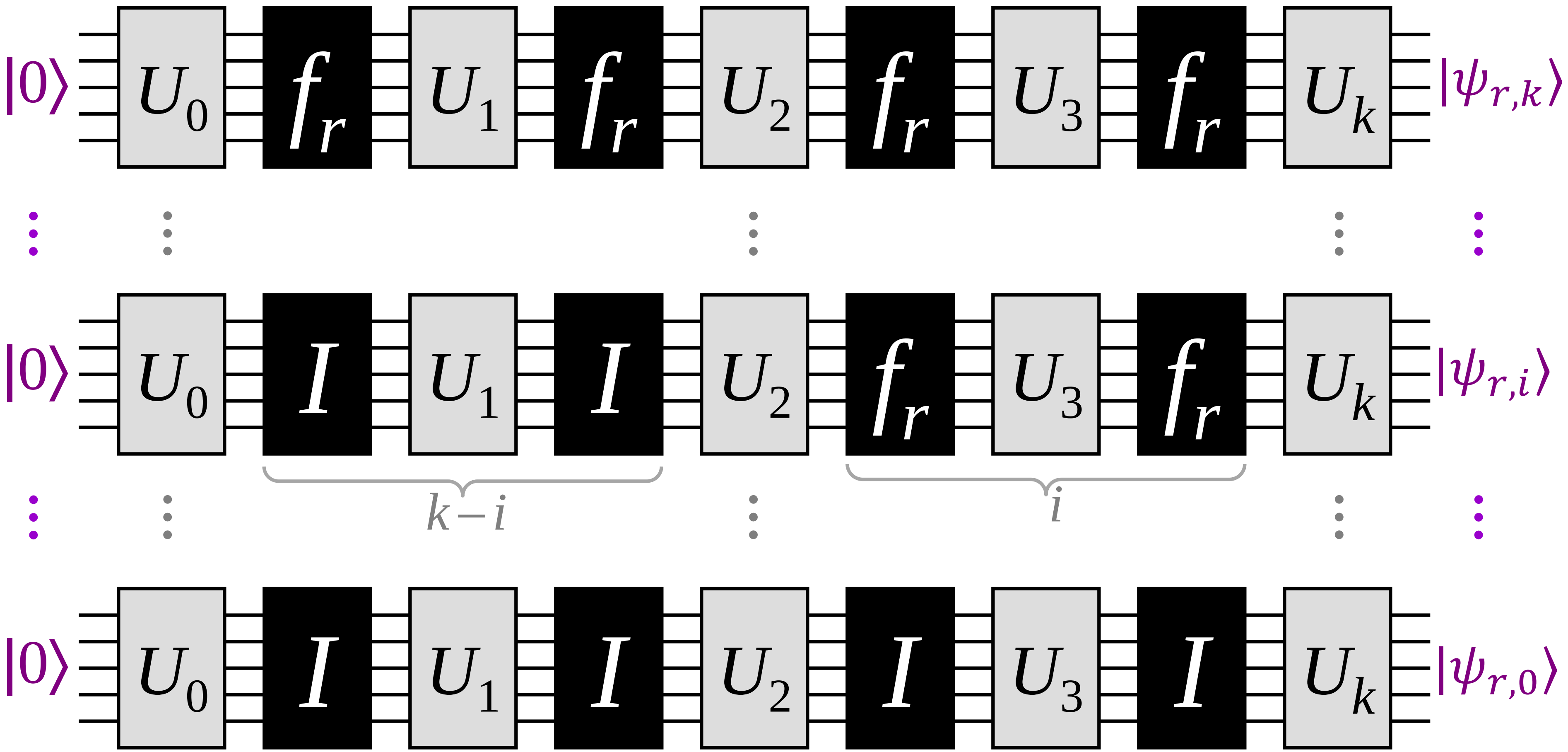
versus



We'll show that, averaging over all $r \in \{0,1\}^n$,

$$\left\| \, |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \, \right\| \leq \frac{2k}{\sqrt{2^n}}.$$

Optimality of Grover's algorithm III

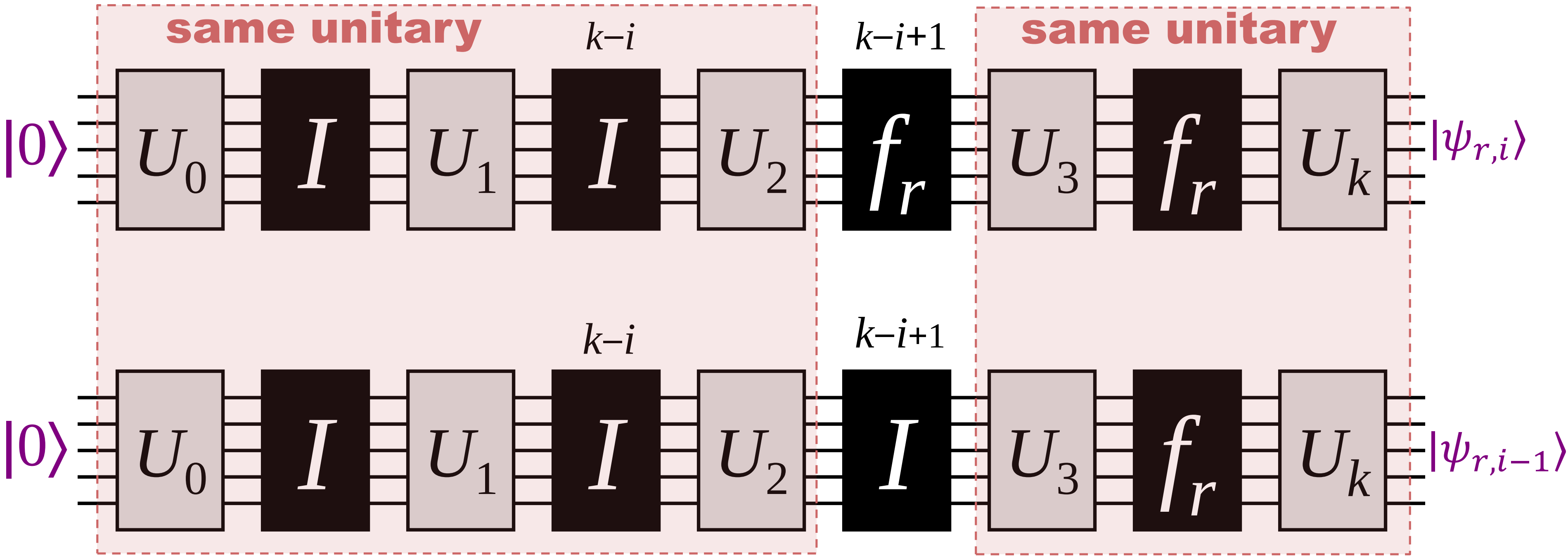


$$|\psi_{r,k}\rangle - |\psi_{r,0}\rangle = (|\psi_{r,k}\rangle - |\psi_{r,k-1}\rangle) + (|\psi_{r,k-1}\rangle - |\psi_{r,k-2}\rangle) + \cdots + (|\psi_{r,1}\rangle - |\psi_{r,0}\rangle)$$

implies that $\| |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \| \leq \| |\psi_{r,k}\rangle - |\psi_{r,k-1}\rangle \| + \cdots + \| |\psi_{r,1}\rangle - |\psi_{r,0}\rangle \|$.

Optimality of Grover's algorithm IV

Consider the difference between any two consecutive layers (i and $i-1$):



$$\sum_{x\in\{0,1\}^n} \alpha_{i,x}|x\rangle \qquad \sum_{x\in\{0,1\}^n} (-1)^{[x=r]}\alpha_{i,x}|x\rangle \quad \text{(top layer)}$$

Therefore $\left\| |\psi_{r,i}\rangle - |\psi_{r,i-1}\rangle \right\| = |2\alpha_{i,r}|$ (since only amplitude of $|r\rangle$ negated)

so that $\left\| |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \right\| \le \sum_{i=0}^{k-1} 2|\alpha_{i,r}|$

Optimality of Grover's algorithm V

Now, averaging over all $r \in \{0,1\}^n$,

$$\frac{1}{2^n}\sum_{r\in\{0,1\}^n} \| |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \| \leq \frac{1}{2^n}\sum_{r\in\{0,1\}^n}\left(\sum_{i=0}^{k-1} 2|\alpha_{i,r}|\right)$$ (we just showed this)

$$= \frac{1}{2^n}\sum_{i=0}^{k-1} 2\left(\sum_{r\in\{0,1\}^n}|\alpha_{i,r}|\right)$$ (reordering sums)

$$\leq \frac{1}{2^n}\sum_{i=0}^{k-1} 2\left(\sqrt{2^n}\right)$$ (by Cauchy-Schwarz) $\langle u, v\rangle \leq \|u\| \cdot \|v\|$

$$= \frac{2k}{\sqrt{2^n}}$$

Therefore, for ***some*** $r \in \{0,1\}^n$, the number k of queries must be $\Omega\left(\sqrt{2^n}\right)$ in order to distinguish f_r from the all-zero function (using the bound $\| \, |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \, \|_1 \leq \| \, |\psi\rangle - |\varphi\rangle\|^2$).

This completes the proof.