Introduction to Quantum Information Processing

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

Lecture 17–18 (2019)

Richard Cleve
DC 2117 / QNC 3129
cleve@uwaterloo.ca

Grover's quantum search algorithm

Quantum search problem

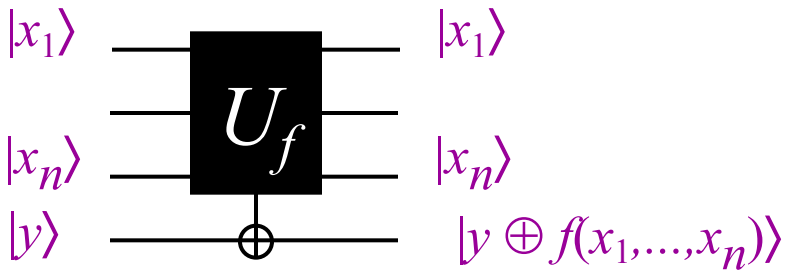
Given: a black box computing $f: \{0,1\}^n \rightarrow \{0,1\}$

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 ¾ (say)

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



[Grover '96]

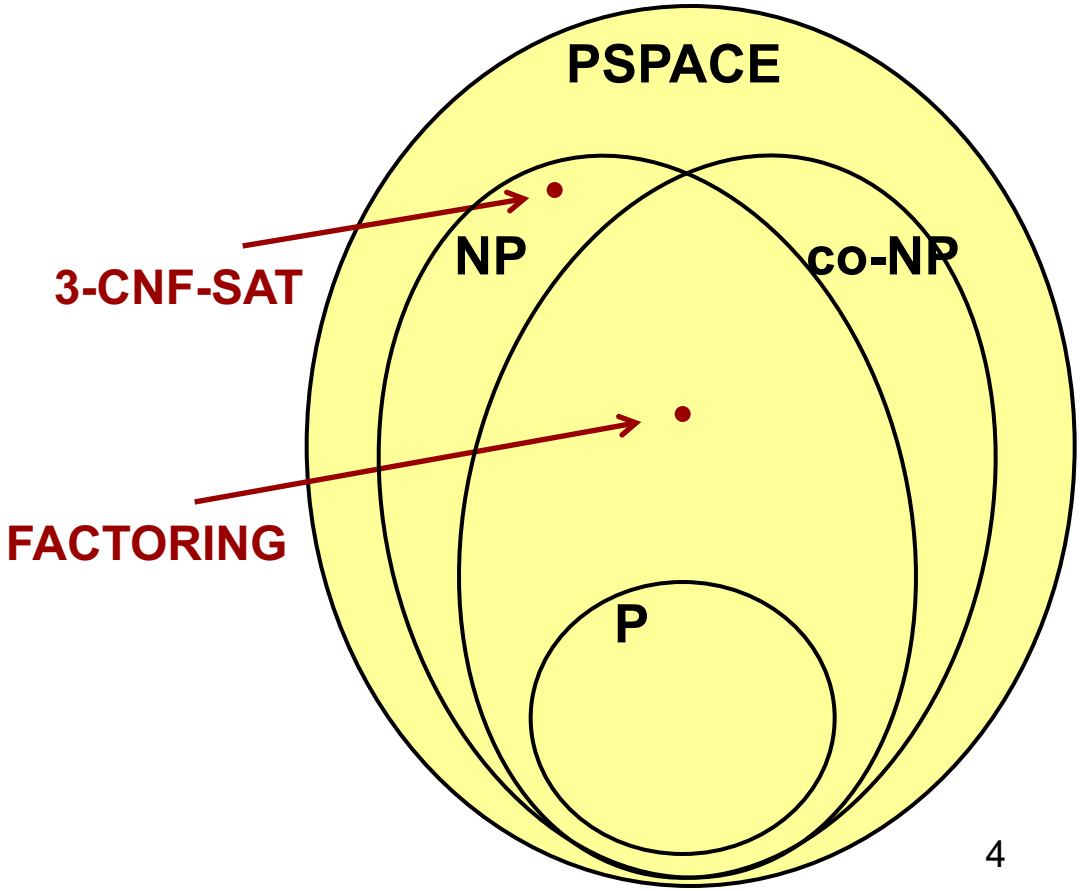
Applications of quantum search

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**

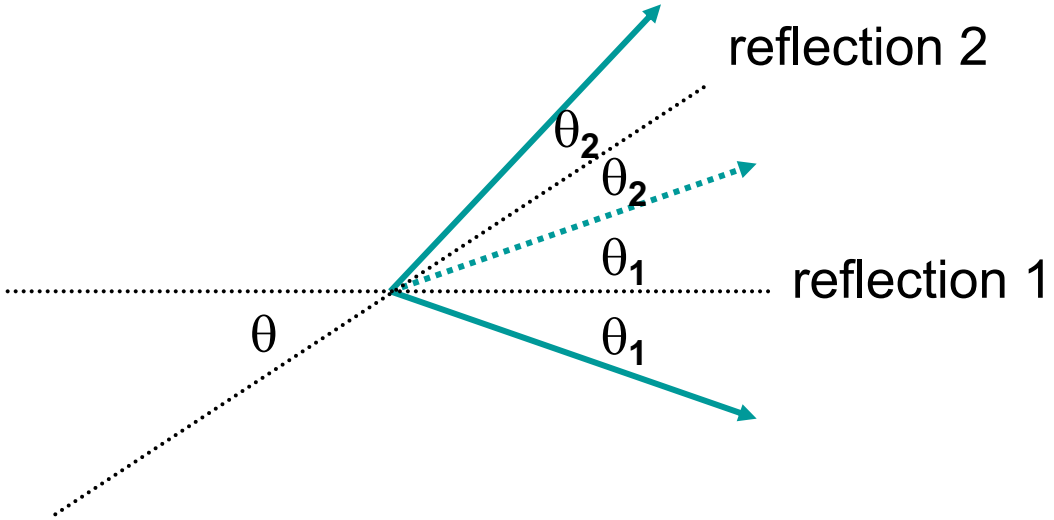
The resulting quantum algorithms appear to be ***quadratically*** more efficient than the best classical algorithms known



Prelude to Grover's algorithm:

two reflections = a rotation

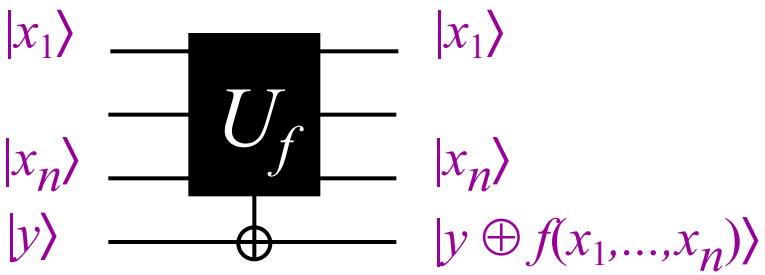
Consider two lines with intersection angle θ:



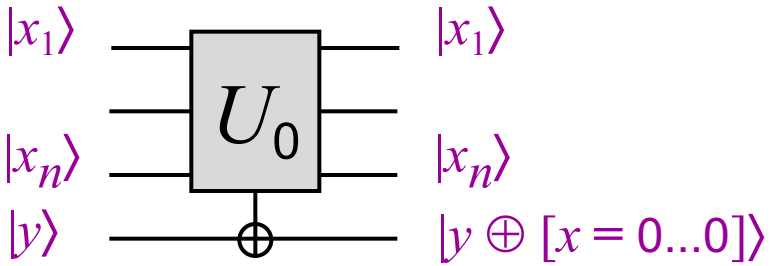
Net effect: rotation by angle 2θ, ***regardless of starting vector***

Grover's algorithm: description I

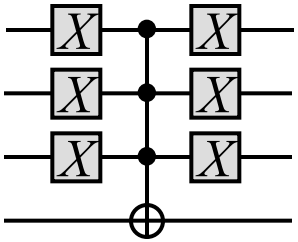
Basic operations used:



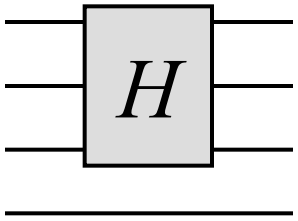
$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$



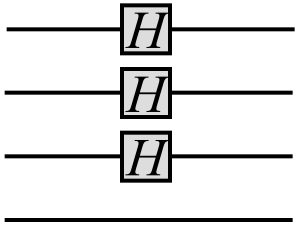
Implementation?



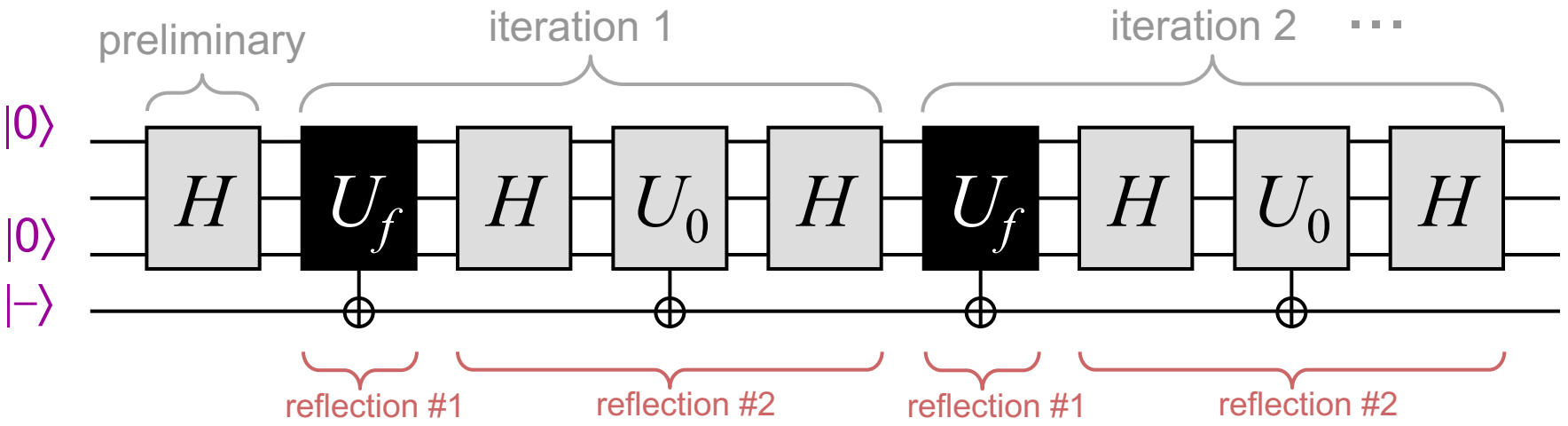
$$U_0|x\rangle|-\rangle = (-1)^{[x\,=\,0\ldots0]}|x\rangle|-\rangle$$



Hadamard



Grover's algorithm: description II



1. construct state $H|0...0\rangle|-\rangle$
2. repeat k times:

   apply $-HU_0HU_f$ to state

3. measure state, to get $x \in \{0,1\}^n$, and check if $f(x)=1$

(The setting of k will be determined later)

Grover's algorithm: analysis I

Let $A = \{x \in \{0,1\}^n : f(x) = 1\}$ and $B = \{x \in \{0,1\}^n : f(x) = 0\}$

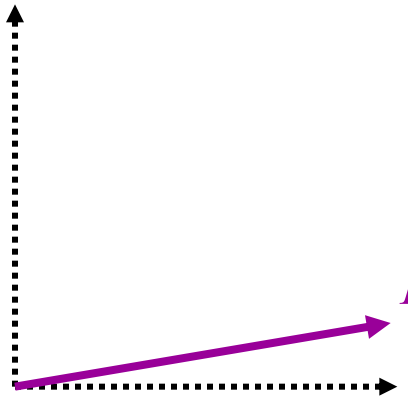
and $N = 2^n$ and $a = |A|$ and $b = |B|$

interesting case: $a \ll N$

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

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

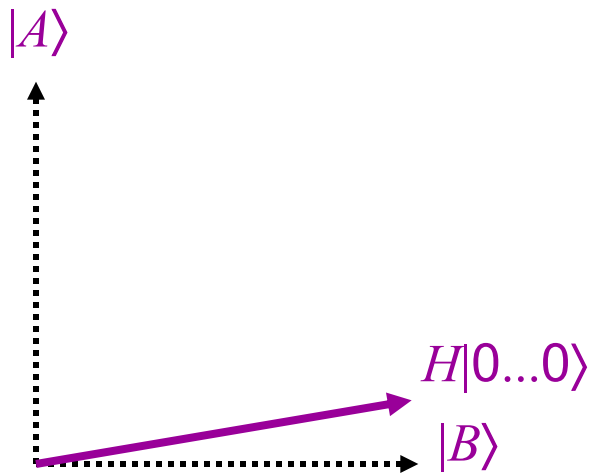
$|A\rangle$ ← goal is to get close to this state



$$H|0\ldots0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = \sqrt{\frac{a}{N}}\,|A\rangle + \sqrt{\frac{b}{N}}\,|B\rangle$$

sin(θ) cos(θ)

Grover's algorithm: analysis II



Algorithm: $(-HU_0HU_f)^k H|0...0\rangle$

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 $-HU_0H$?

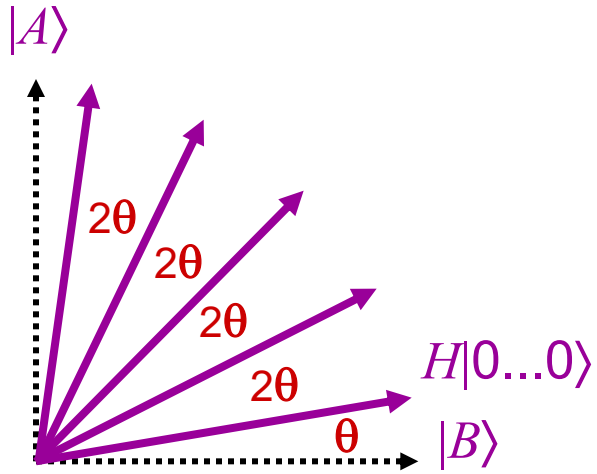
Answer: a reflection about $H|0...0\rangle$

Proof:

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

$$-HU_0H(H|0...0\rangle)^\perp = -HU_0|0...0\rangle^\perp = -H|0...0\rangle^\perp = -(H|0...0\rangle)^\perp$$

Grover's algorithm: analysis III



Algorithm: $(-HU_0HU_f)^k H|0...0\rangle$

Since $-HU_0HU_f$ is a composition of two reflections, it is a rotation by 2θ,

where $\sin(\theta) = \sqrt{a/N}$ so $\theta \approx \sqrt{a/N}$ (if $a \ll N$)

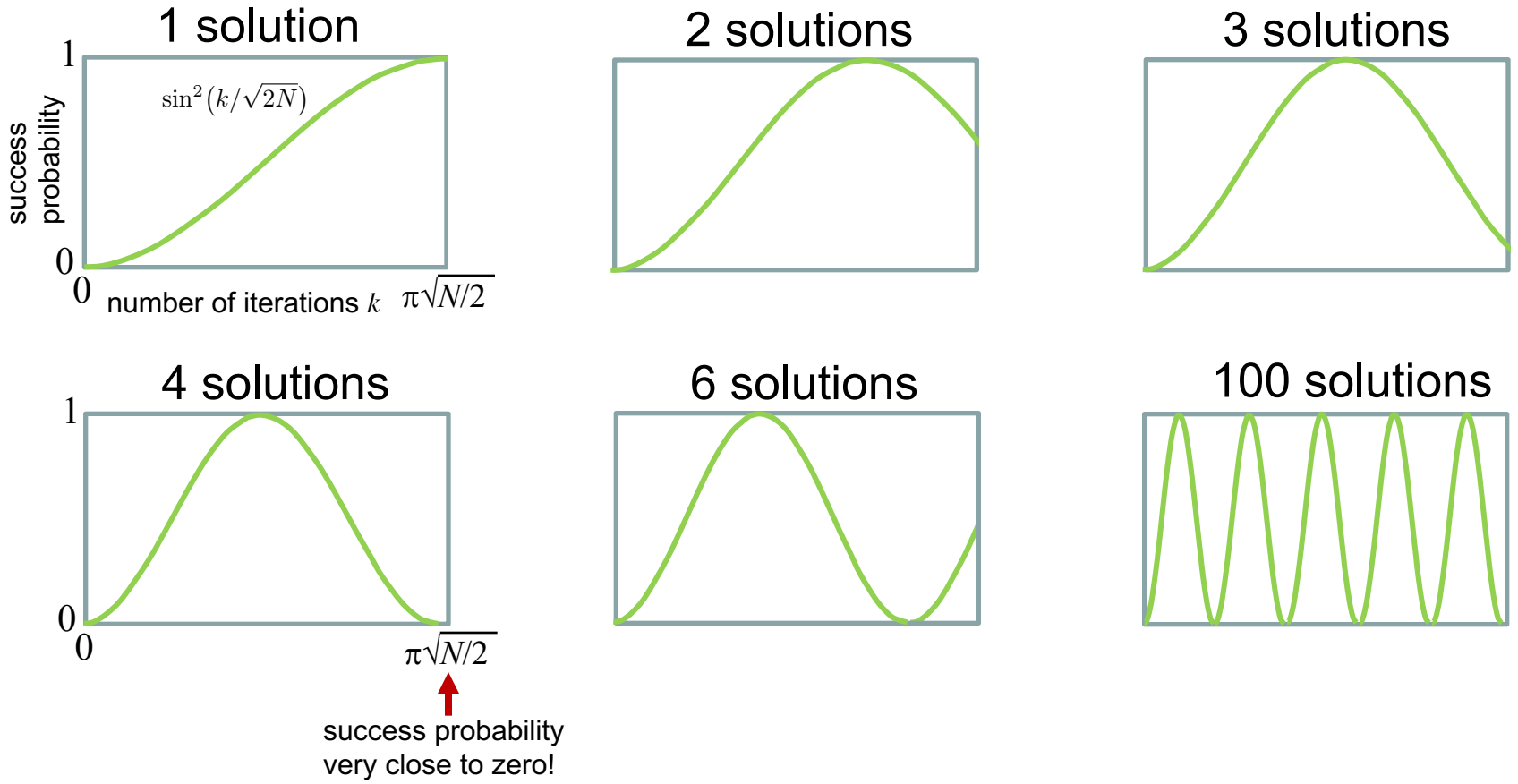
When $a = 1$, we want $(2k+1)\left(1/\sqrt{N}\right) \approx \pi/2$, so $k \approx (\pi/4)\sqrt{N}$

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

E.g., half as many iterations if $a = 4$

Question: what if a is not known in advance?

Unknown number of solutions



Note that if we choose a ***random*** k in the range then the success probability is the area under the curve (with normalized domain)

It turns out that this area is always > $0.43\ldots$

Optimality of Grover's algorithm

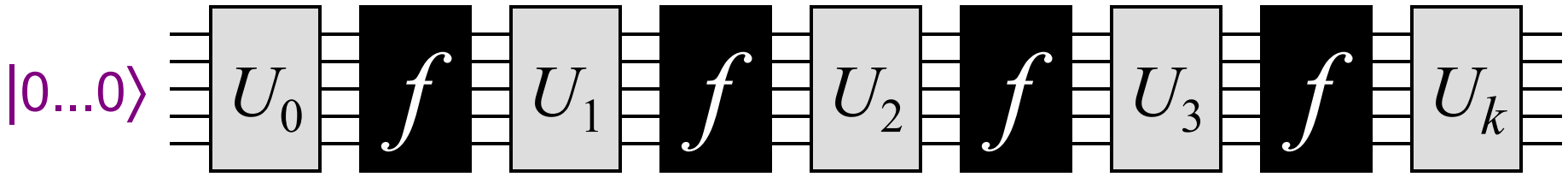
Optimality of Grover's algorithm I

Theorem: any quantum search algorithm for $f: \{0,1\}^n \rightarrow \{0,1\}$ 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

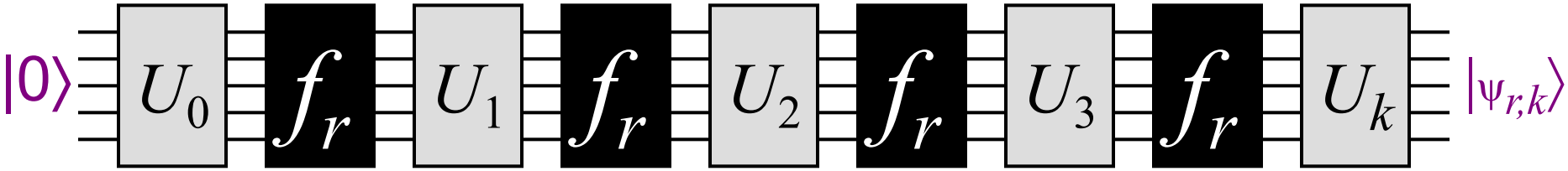


where $U_0, U_1, U_2, ..., U_k$, are arbitrary unitary operations

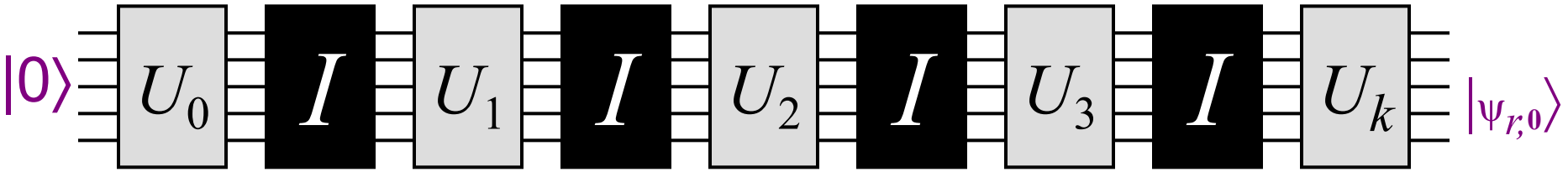
Optimality of Grover's algorithm II

For every $r \in \{0,1\}^n$, define $f_r : \{0,1\}^n \rightarrow \{0,1\}$ as $f_r(x) = 1$ iff $x = r$

Consider

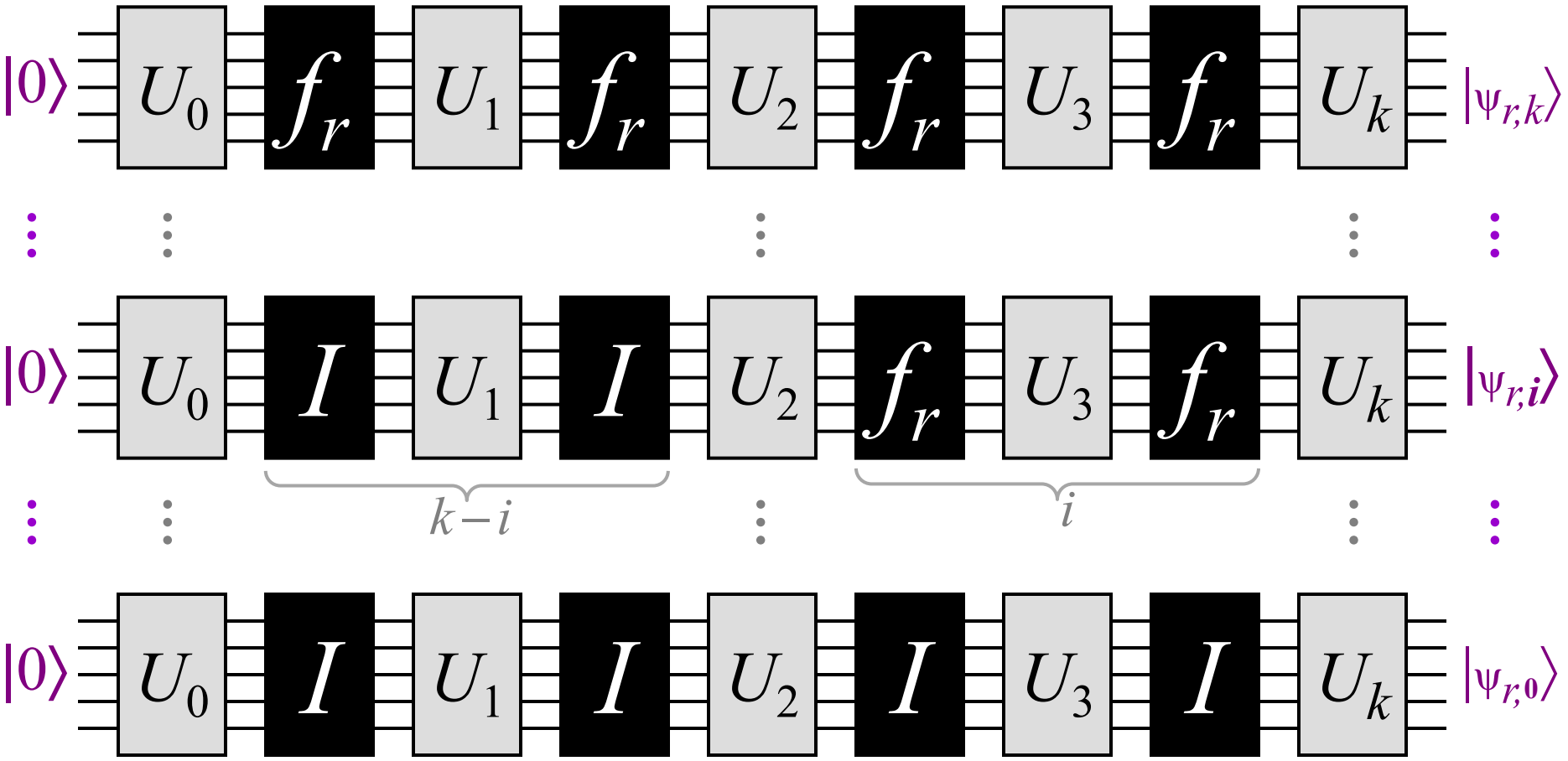


versus



We'll show that, averaging over all $r \in \{0,1\}^n$, $\| \, |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \, \| \leq 2k/\sqrt{2^n}$

Optimality of Grover's algorithm III

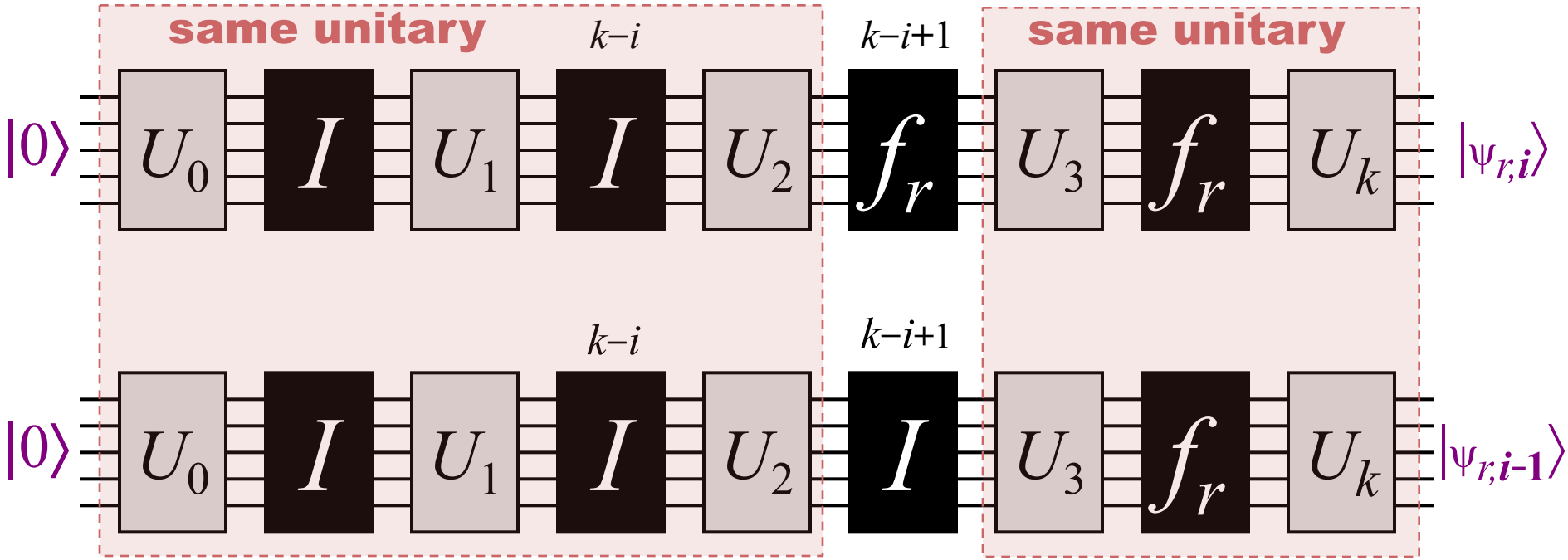


Note that $|\psi_{r,k}\rangle - |\psi_{r,0}\rangle = \left(|\psi_{r,k}\rangle - |\psi_{r,k-1}\rangle\right) + \left(|\psi_{r,k-1}\rangle - |\psi_{r,k-2}\rangle\right) + \ldots + \left(|\psi_{r,1}\rangle - |\psi_{r,0}\rangle\right)$

which implies $\| \, |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \, \| \leq \| \, |\psi_{r,k}\rangle - |\psi_{r,k-1}\rangle \, \| + \ldots + \| \, |\psi_{r,1}\rangle - |\psi_{r,0}\rangle \, \|$

Optimality of Grover's algorithm IV

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



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

Therefore $\| \, |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \, \| \leq |2\alpha_{0,r}| + \ldots + |2\alpha_{k,r}| = \sum_{i=0}^{k-1} 2|\alpha_{i,r}|$

Optimality of Grover's algorithm V

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

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

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

$$\leq \frac{1}{2^n} \sum_{i=0}^{k-1} 2 \left(\sqrt{2^n} \right) \quad \text{(by Cauchy-Schwarz)}$$

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

Therefore, for ***some*** $r \in \{0,1\}^n$, the number of queries k must be $\Omega\left(\sqrt{2^n}\right)$, in order to distinguish f_r from the all-zero function

This completes the proof