Portland State University

S'20 CS410/510
Intro to quantum computing

Fang Song

Week 7

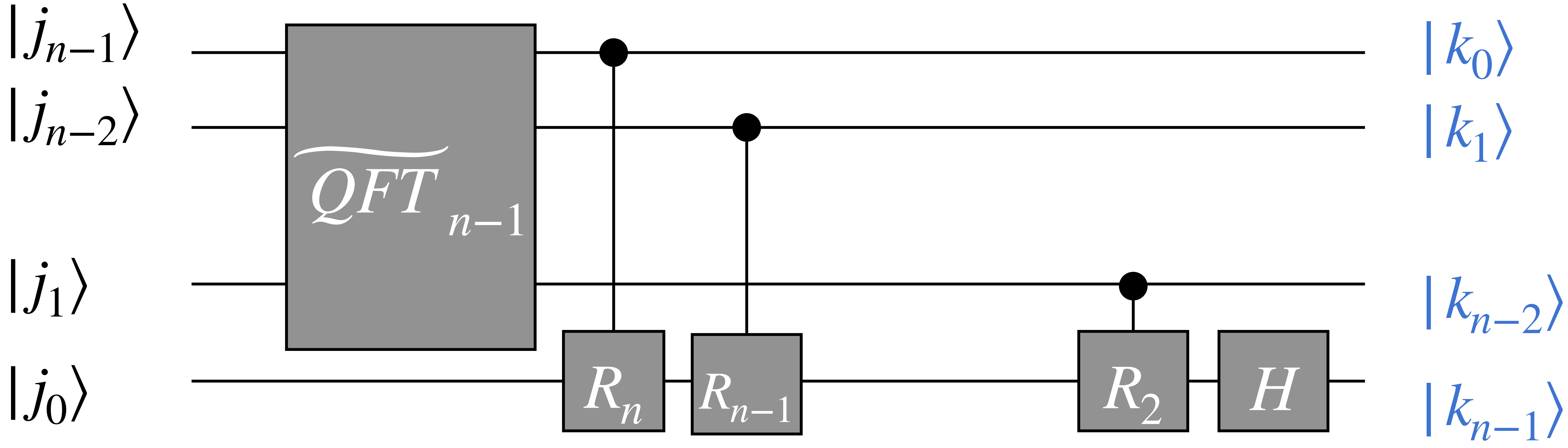
- QFT recap
- Grover's algorithm
- Optimality of Grover's alg.

Credit: based on slides by Richard Cleve

Review: QFT

$$QFT_n : |j_{n-1}j_{n-2}\ldots j_0\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_{2^n}^{jk} |k_{n-1}k_{n-2}\ldots k_0\rangle$$

$$\widetilde{QFT}_n : |j_{n-1}j_{n-2}\ldots j_0\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_{2^n}^{jk} |k_0 k_1 \ldots k_{n-2}k_{n-1}\rangle$$



$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \omega_{2^k} \end{pmatrix}$$

Exercise

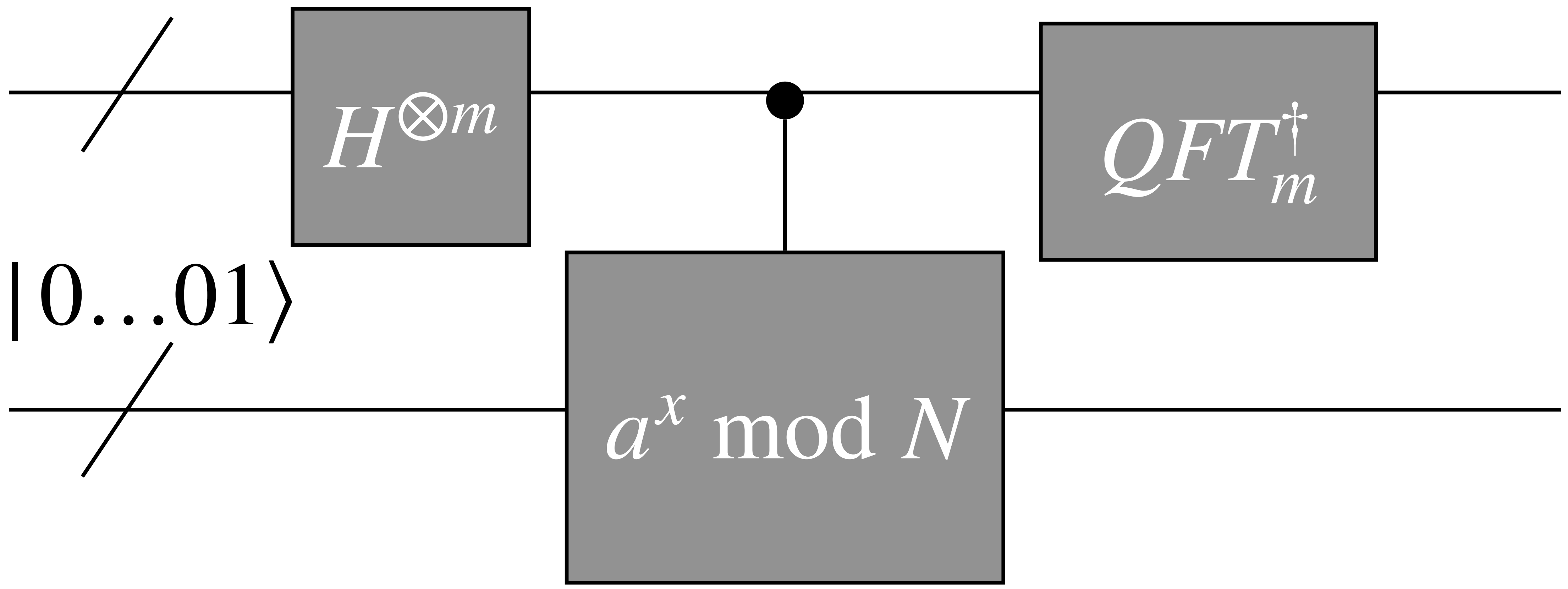
$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4 & \omega_4^2 & \omega_4^3 \\ 1 & \omega_4^2 & \omega_4^4 & \omega_4^6 \\ 1 & \omega_4^3 & \omega_4^6 & \omega_4^9 \end{pmatrix}$$

1. Let $\overrightarrow{x} = (\frac{1}{\sqrt{2}}, 0, 0, \frac{i}{\sqrt{2}})^T$. Compute $\overrightarrow{y} = F_4 \overrightarrow{x}$.

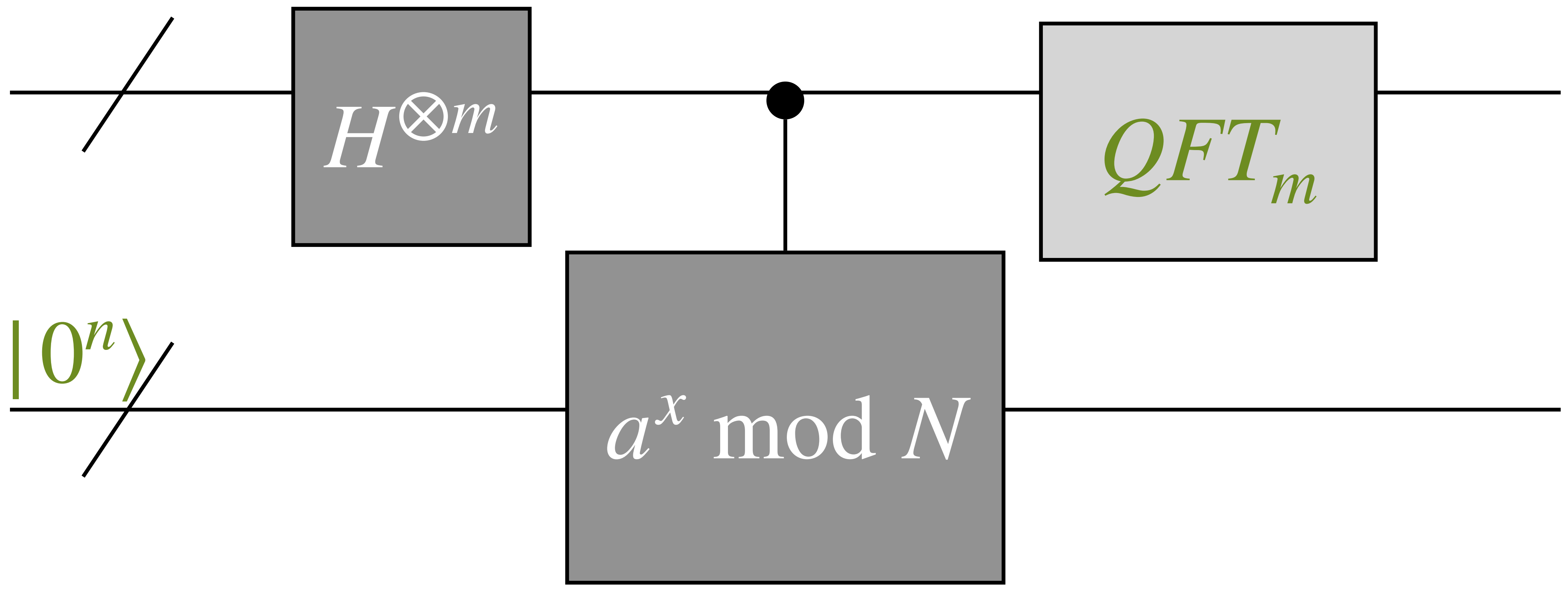
2. Draw the QFT circuit implementing F_4 (i.e. QFT_2). How about $QFT_2^\dagger$?

Quantum order finding/factorization

- Order finding à la phase estimation [Kitaev'95]



- Shor's algorithm à la quantum Fourier sampling [Shor'94]



Quantum speedup for "structured" problems

Problem	Deterministic	Randomized	Quantum
Deutsch	2	2	1
Deutsch-Josza	$2^n/2$	$O(n)$	1
Simon	$2^n/2$	$\sqrt{2^n}$	$O(n^2)$
Order-finding Factoring N	$2^{O((\log N)^{1/3}(\log\log N)^{2/3})}$		$(\log N)^3$

Oracle/Query model

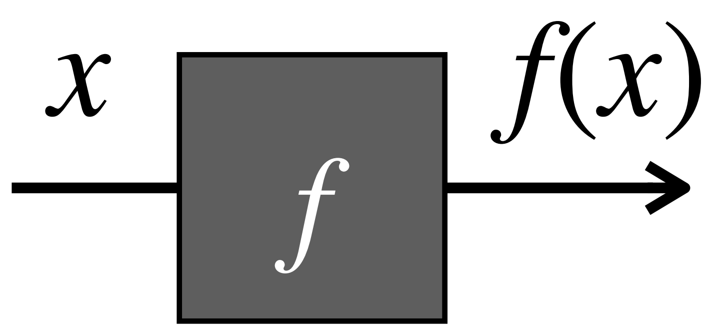
- **Today.** Generic quantum speedup for unstructured search.

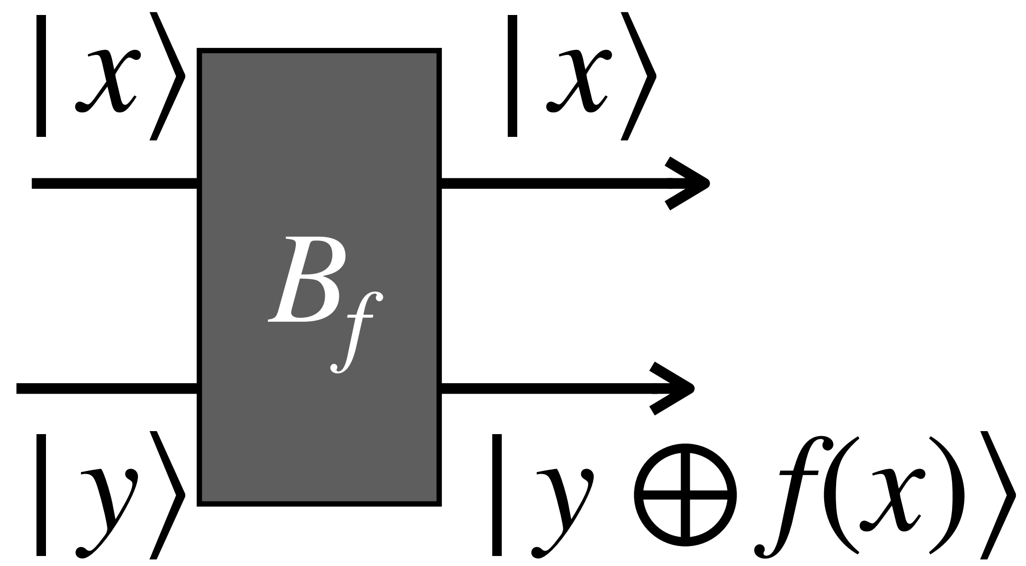
Grover's quantum search algorithm

Unstructured search

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

Goal: find x such that $f(x) = 1$ (if there is one).

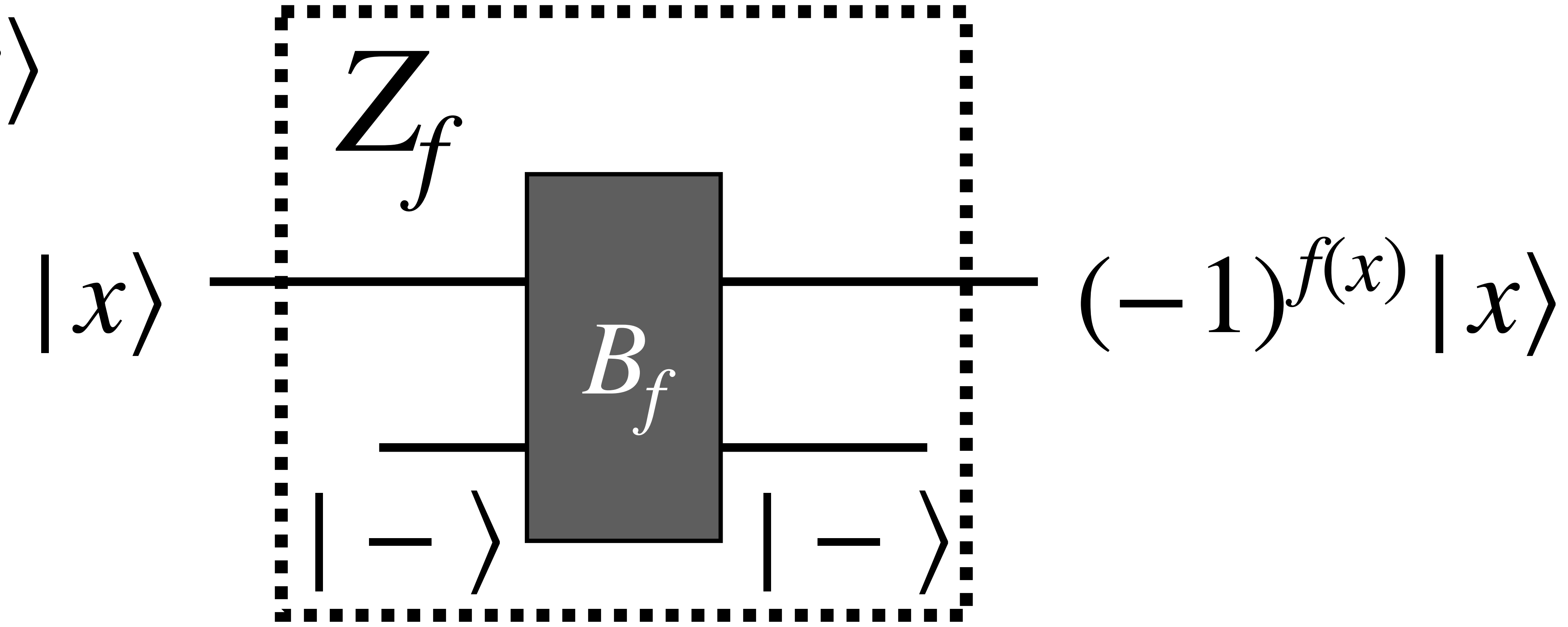




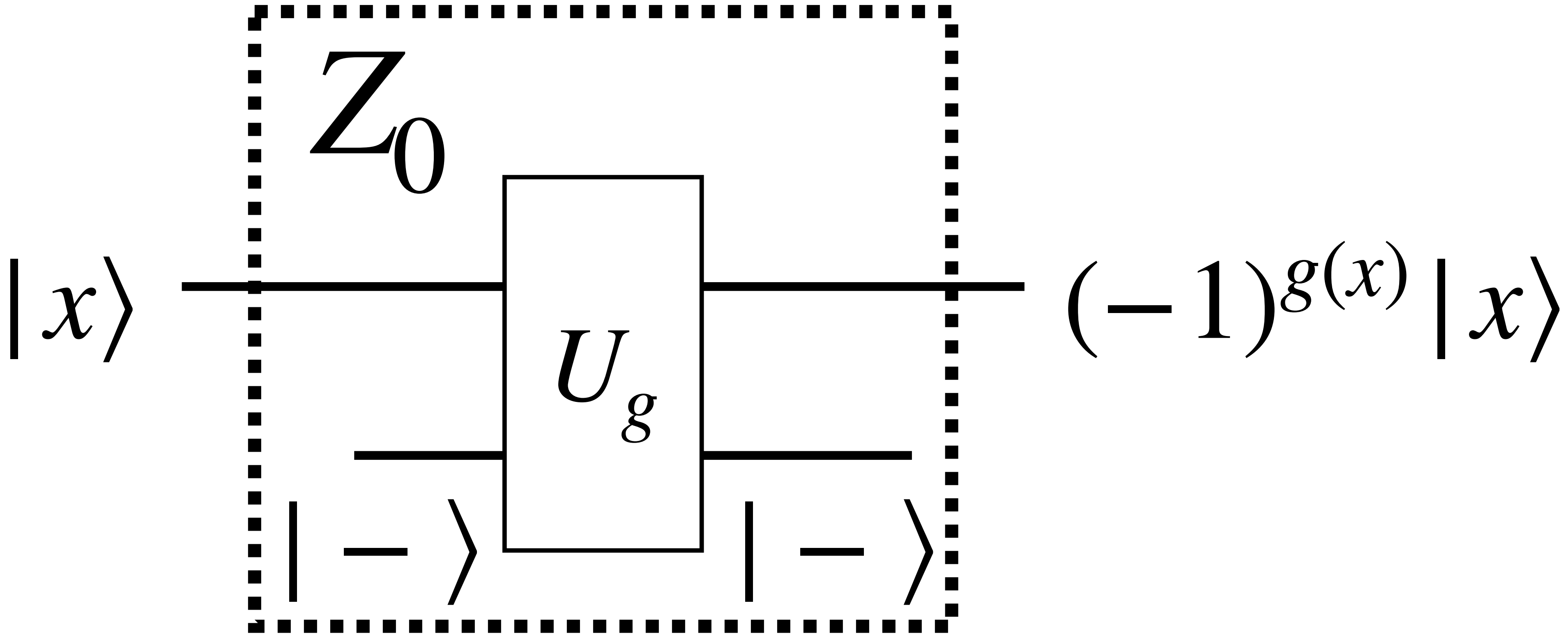
- Example.
  - $x \in \{0,1\}^n$ represents a record of a patient at a hospital
  - $f(x) = 1$ if x is tested positive for DIVOC-91
- Classical algorithms: 2^n queries necessary
- Grover's quantum algorithm: $O(\sqrt{2^n})$ queries

Grover's algorithm: basic operations

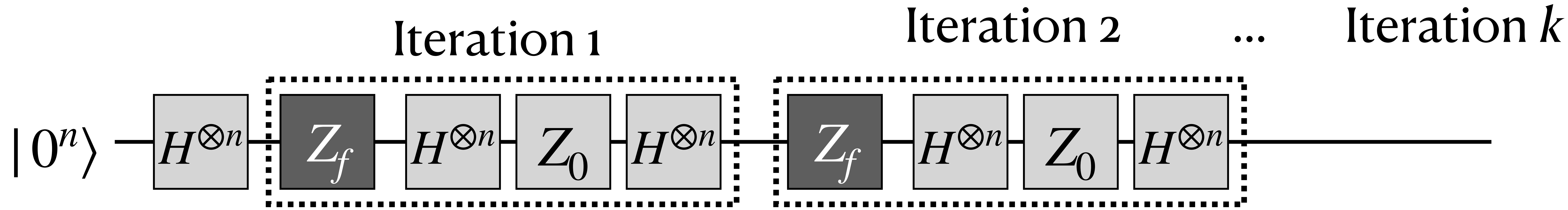
- $Z_f : |x\rangle \mapsto \begin{cases} -|x\rangle, & f(x) = 1 \\ |x\rangle, & f(x) = 0 \end{cases} = (-1)^{f(x)}|x\rangle$



- $Z_0 : |x\rangle \mapsto \begin{cases} -|x\rangle, & x = 0^n \\ |x\rangle, & x \neq 0^n \end{cases} = (-1)^{g(x)}|x\rangle$
  - $g(x) = 1$ **iff.** $x = 0^n$.

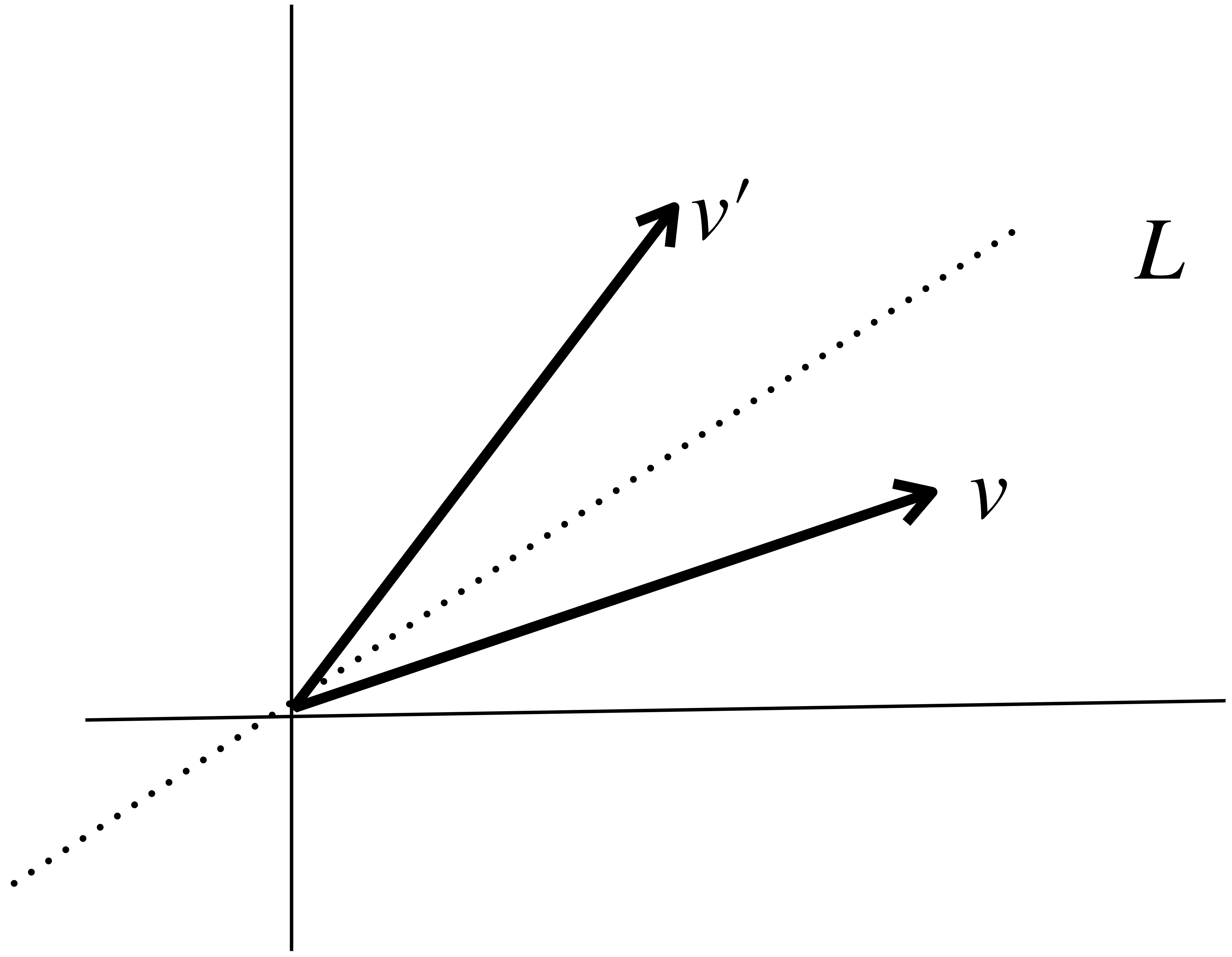


Grover's algorithm

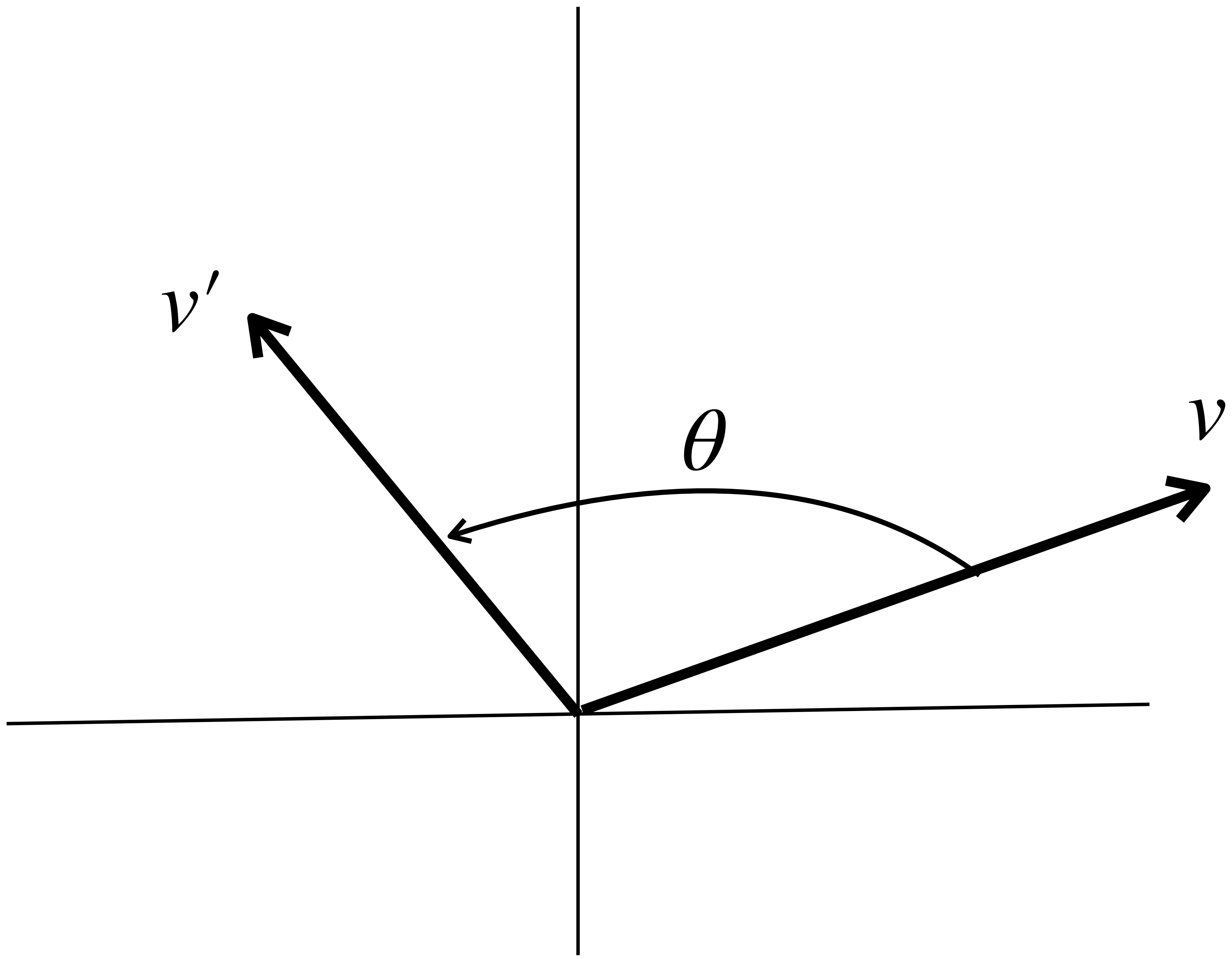


- **Prepare** $|h\rangle := H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$
- **Repeat k times:** $(HZ_0H)Z_f$.
- **Measure and get** x**, check if** $f(x) = 1$.

Reflections and rotations

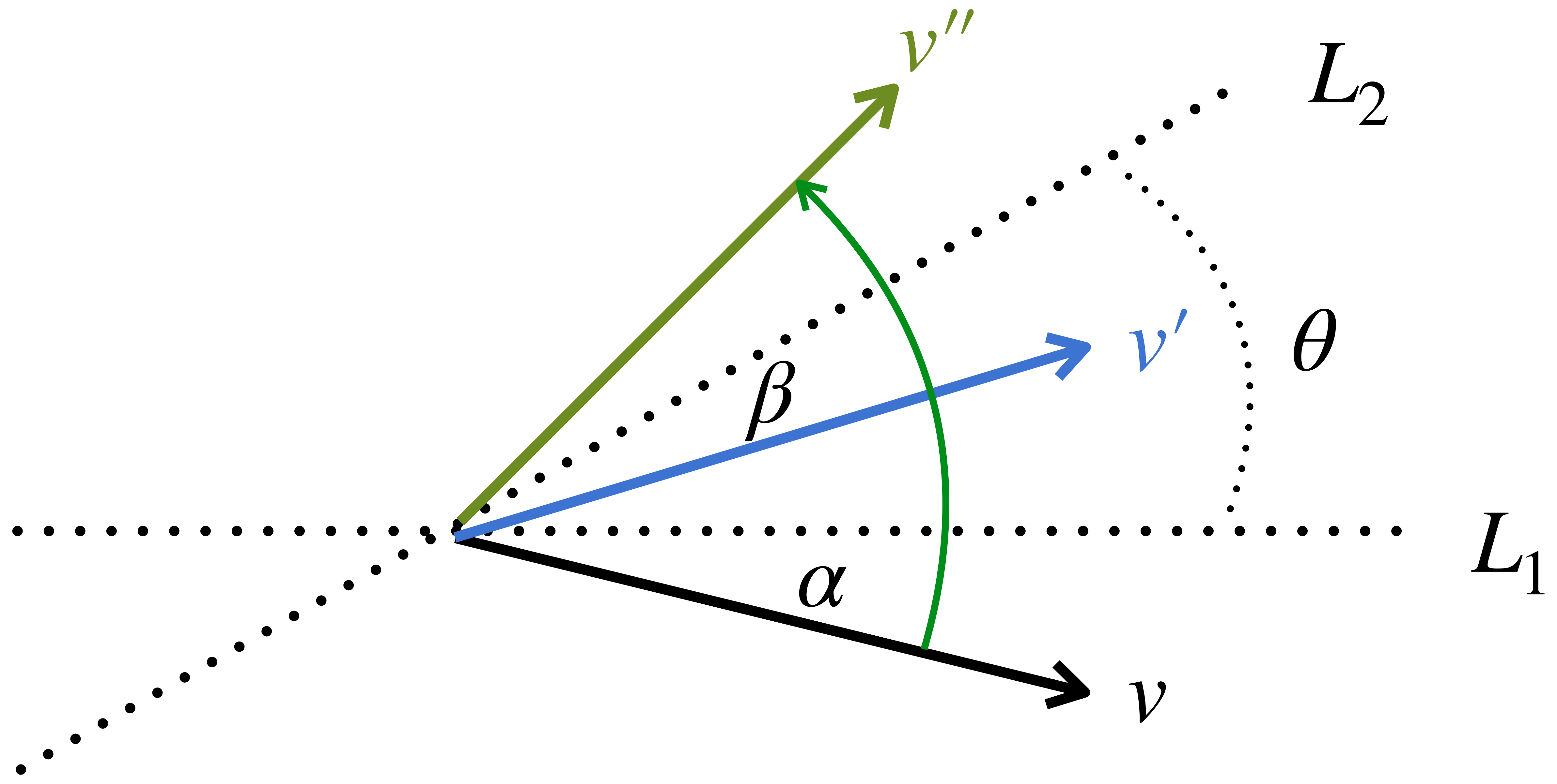


Reflection



Rotation

2 reflections = 1 rotation

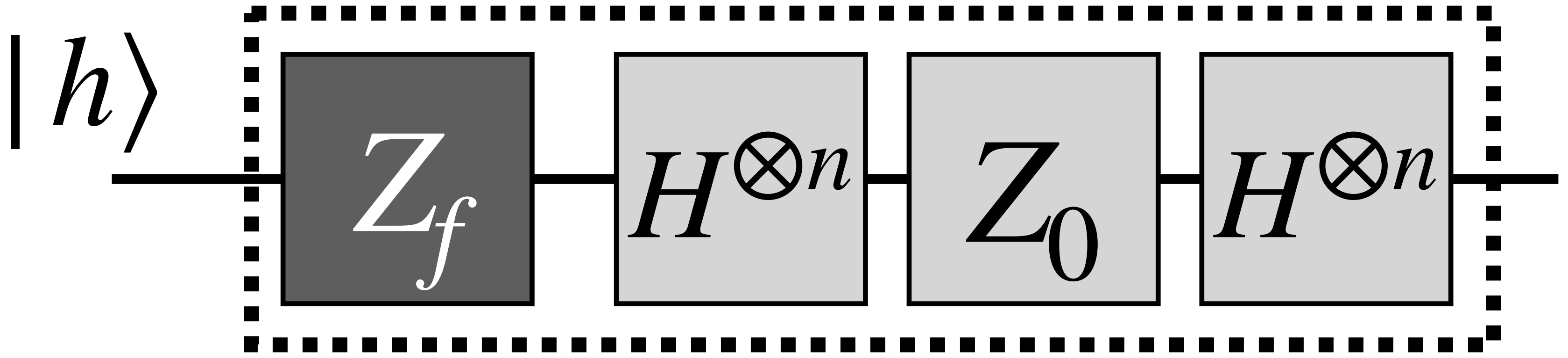


$(L_1, L_2) = \theta$

Reflection about L_1 and L_2 $\equiv$ Rotation by 2θ

Grover's algorithm: analysis

Grover Iteration

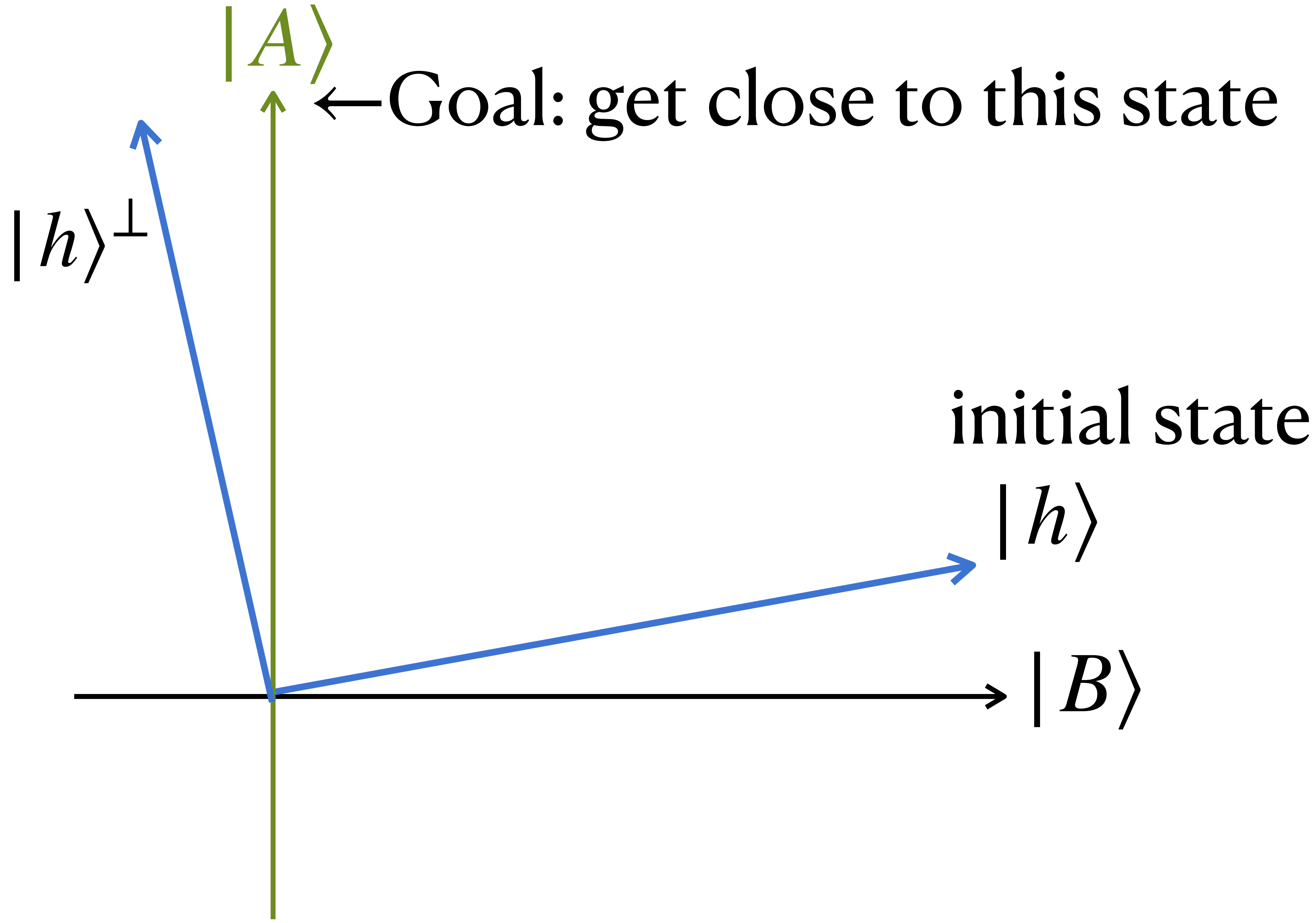


Notations

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

A fundamental 2D-plane

- $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, \ |B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$
- $|h\rangle^\perp$: orthogonal to $|h\rangle$ on span$\{|A\rangle, |B\rangle\}$



Exercise

Notations

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

A fundamental 2D-plane

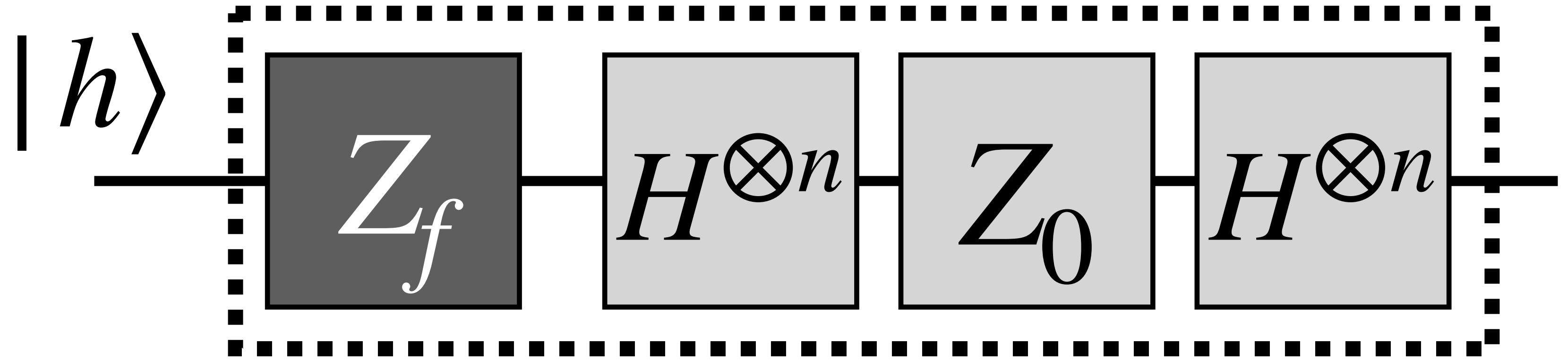
- $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, \ |B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n} |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$
- $|h\rangle^{\perp}$: orthogonal to $|h\rangle$ on span$\{|A\rangle, |B\rangle\}$

1. Show that $\langle B | A \rangle = 0$.

2. Find α and β so that $|h\rangle = \alpha |A\rangle + \beta |B\rangle$

Grover's algorithm: analysis

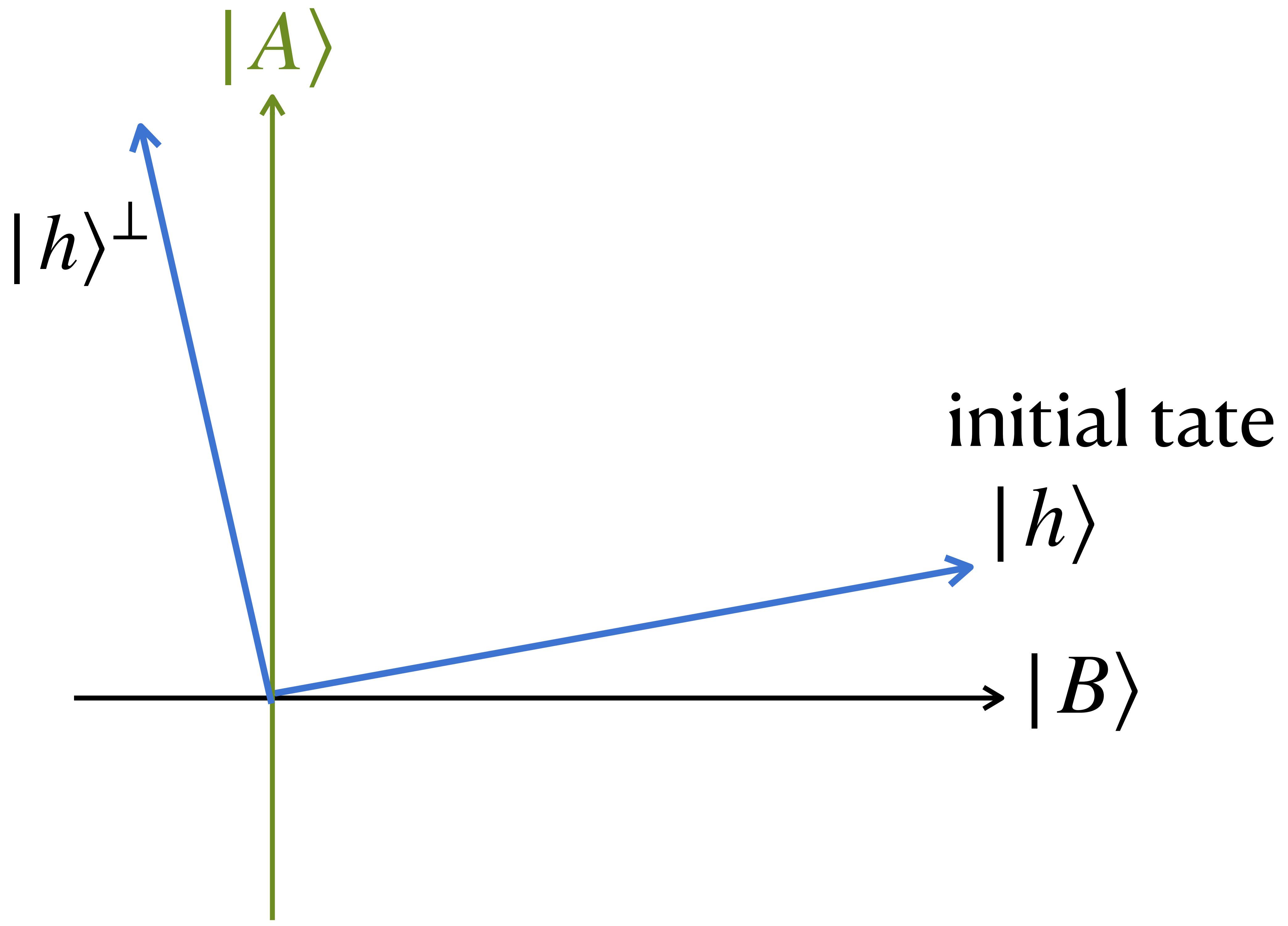
Grover Iteration



A fundamental 2D-plane

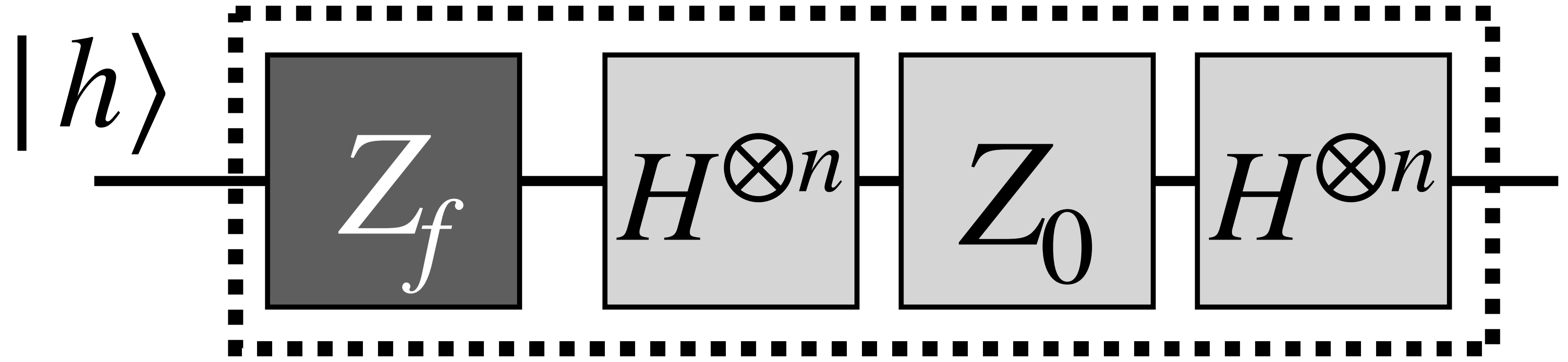
- $|A\rangle := 1/\sqrt{a}\sum_{x\in A}|x\rangle$, $|B\rangle := 1/\sqrt{b}\sum_{x\in B}|x\rangle$
- $|h\rangle := H^{\otimes n}|0^n\rangle$, $|h\rangle^{\perp} \perp |h\rangle$

◉ **Obs. 1.** Z_f is a reflection about $|B\rangle$



Grover's algorithm: analysis

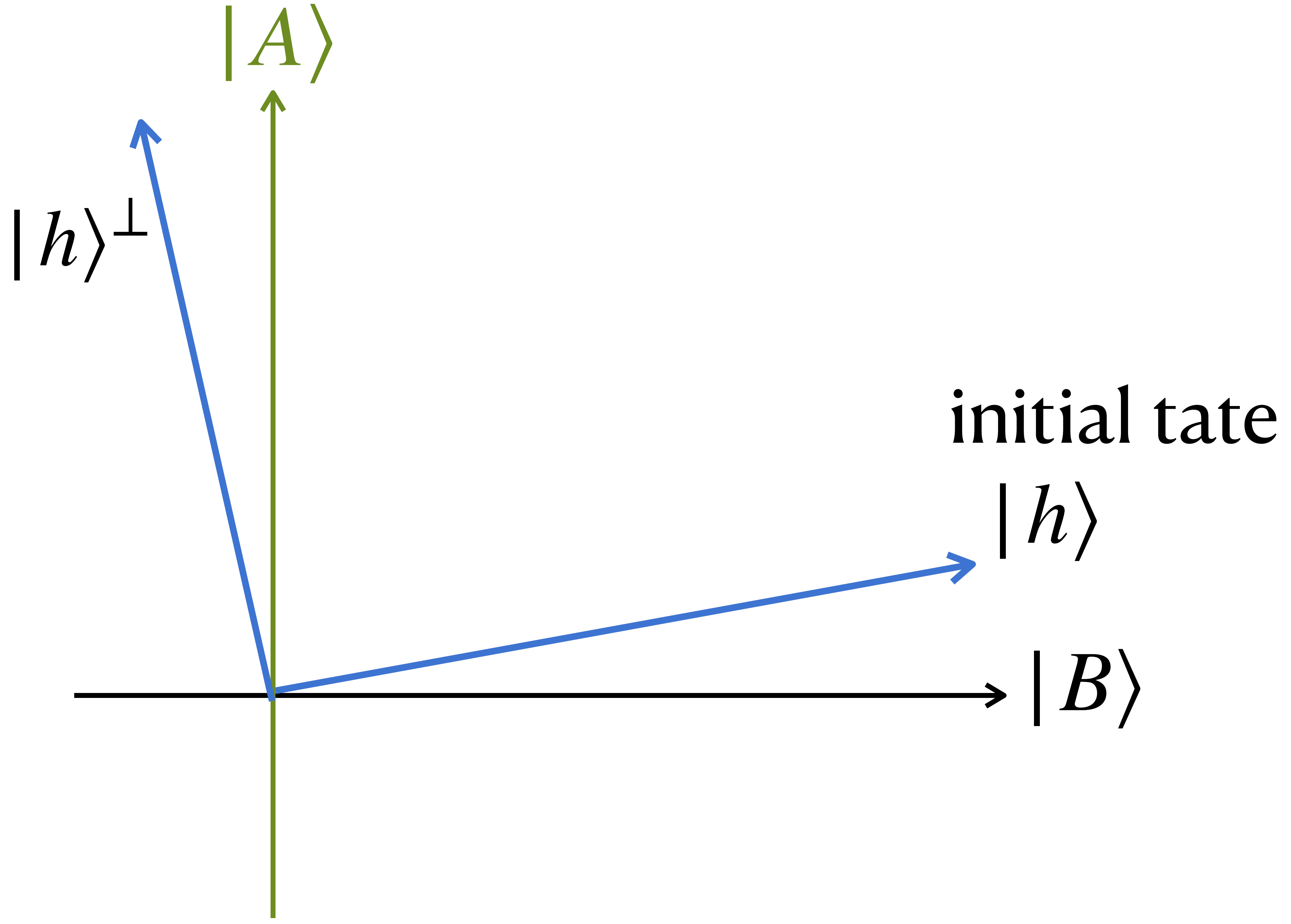
Grover Iteration



A fundamental 2D-plane

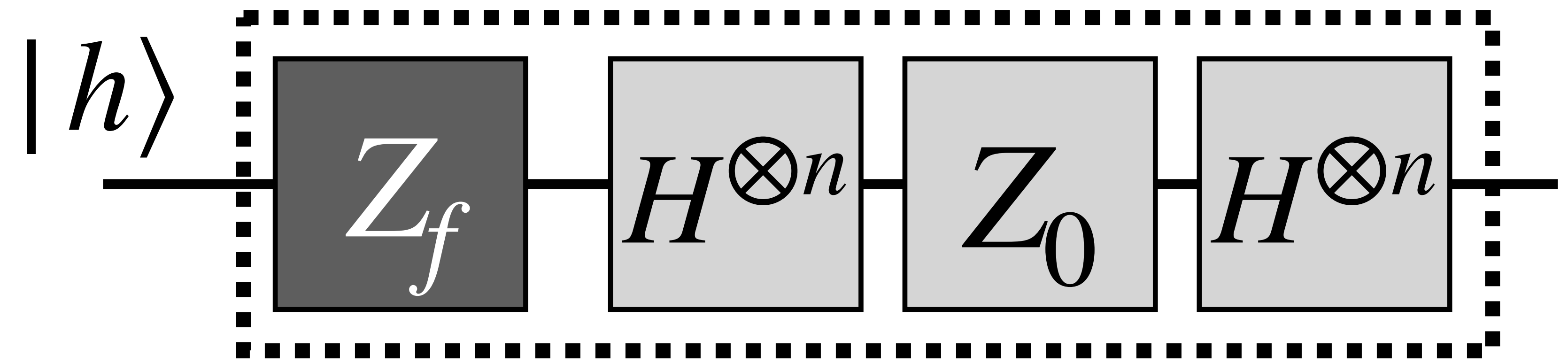
- $|A\rangle := 1/\sqrt{a} \sum_{x \in A} |x\rangle$, $|B\rangle := 1/\sqrt{b} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n}|0^n\rangle$, $|h\rangle^{\perp} \perp |h\rangle$

◉ **Obs 2.** HZ_0H is a reflection about $|h\rangle$.

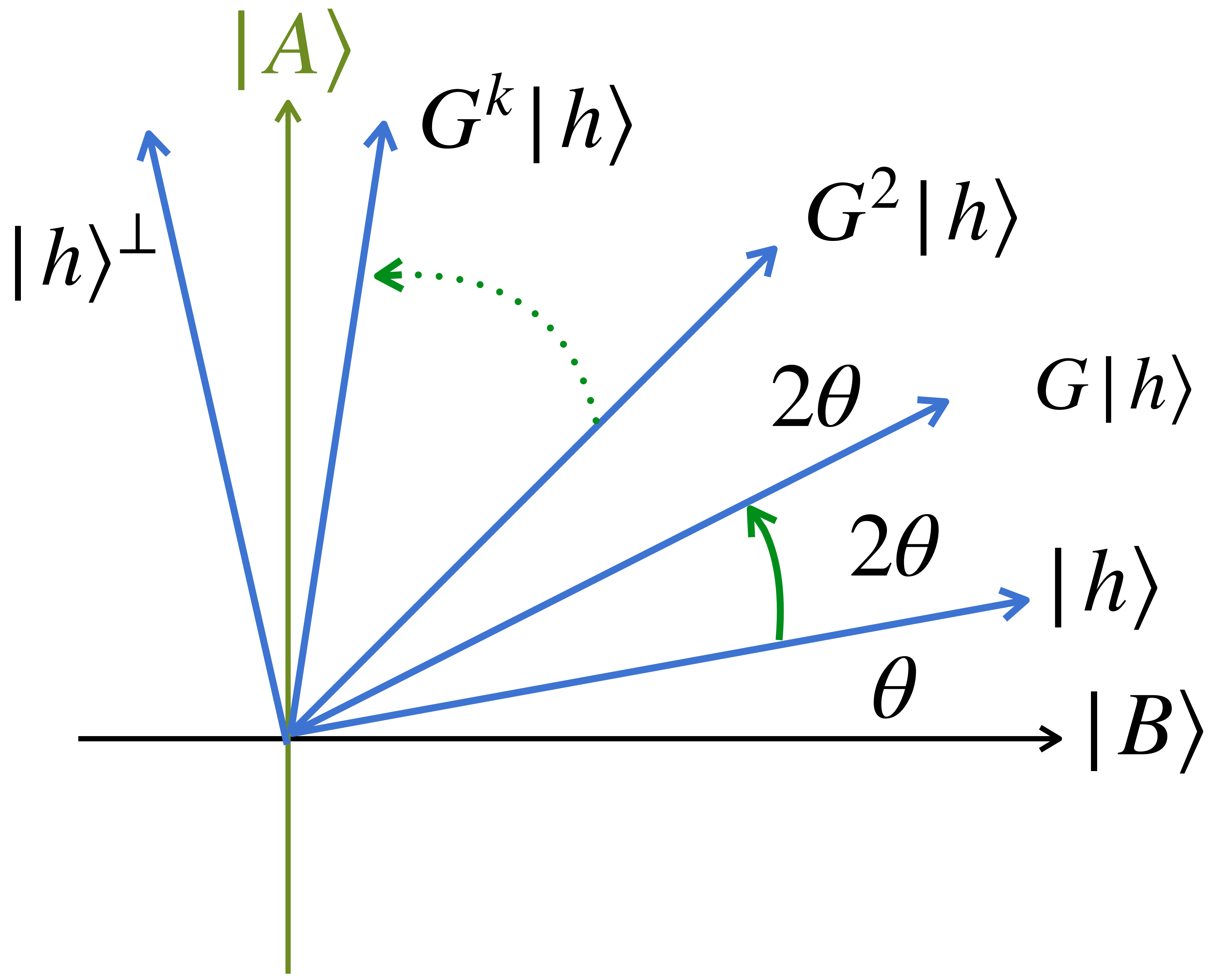


Grover's algorithm: analysis

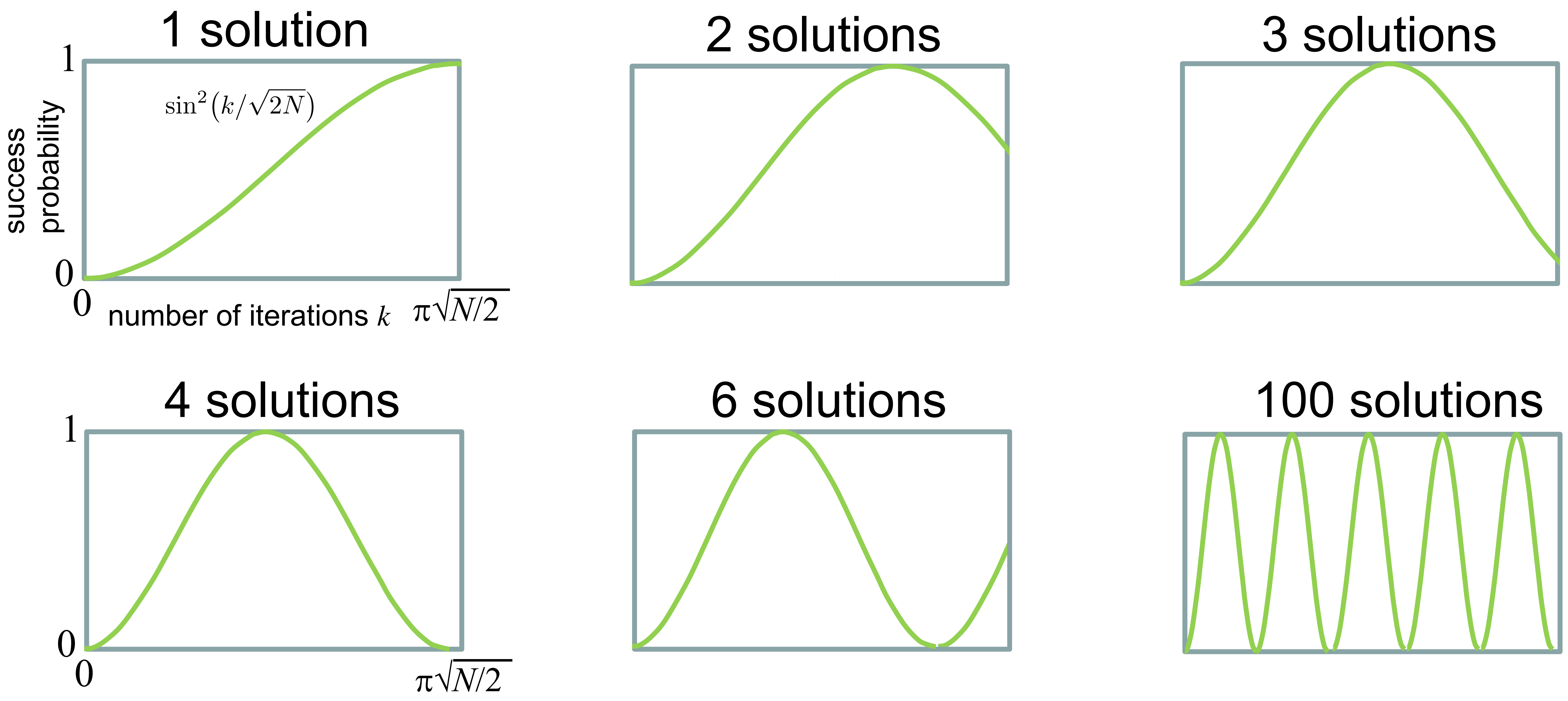
Grover Iteration G

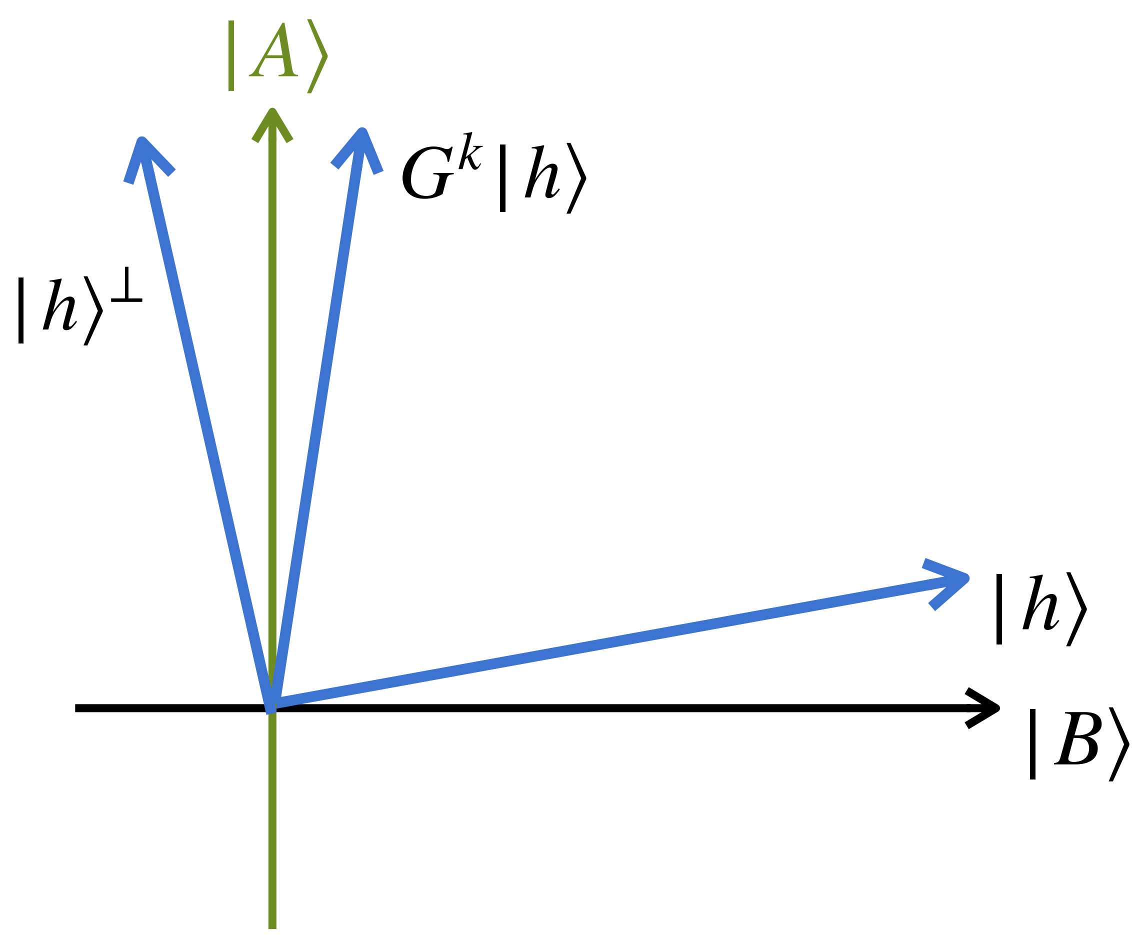


- **Obs.** Each Grover iteration is a rotation of $2\theta, \theta = sin^{-1}\left(\sqrt{a/N}\right)$.
- **Goal**: $(2k+1)\theta \approx \pi/2$
- **Theorem.** $k = \Omega(\sqrt{N/a})$ suffice for $\Omega(1)$ success prob.



Unknown number of solutions





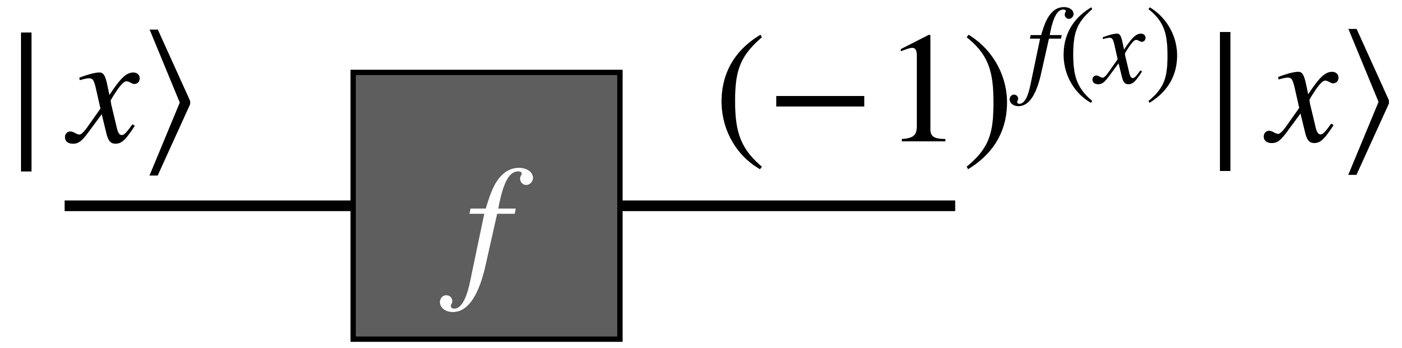
- **One approach: if random k, then success prob. is the area under the curve**
  - … It turns out to be always > 0.4
- **Read more if interested https://arxiv.org/abs/1709.01236**

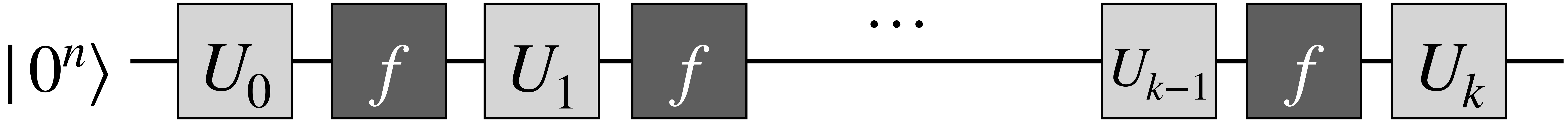
Optimality of Grover's algorithm

An unfortunate news ...

- **Theorem**. Any quantum algorithm must make $\Omega(\sqrt{2^n})$ queries to f (assuming a **single** marked item).

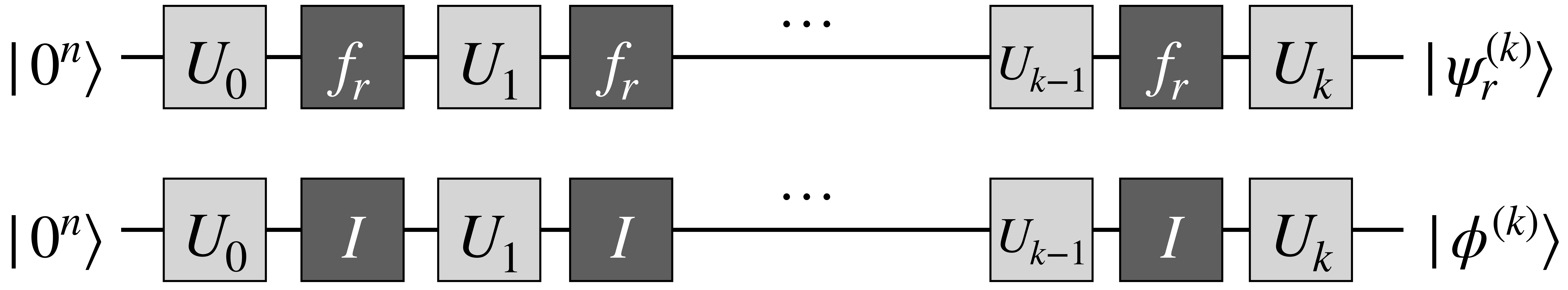
- A k-query quantum algorithm if of the form below
  - $f = Z_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$
  - $U_0, U_1, \ldots, U_k$ are arbitrary unitary operations





Optimality of Grover's algorithm: proof sketch

- For every $r \in \{0,1\}^n$, let $f_r : \{0,1\}^n \to \{0,1\}$ be such that $f_r(x) = 1$ iff. $x = r$.

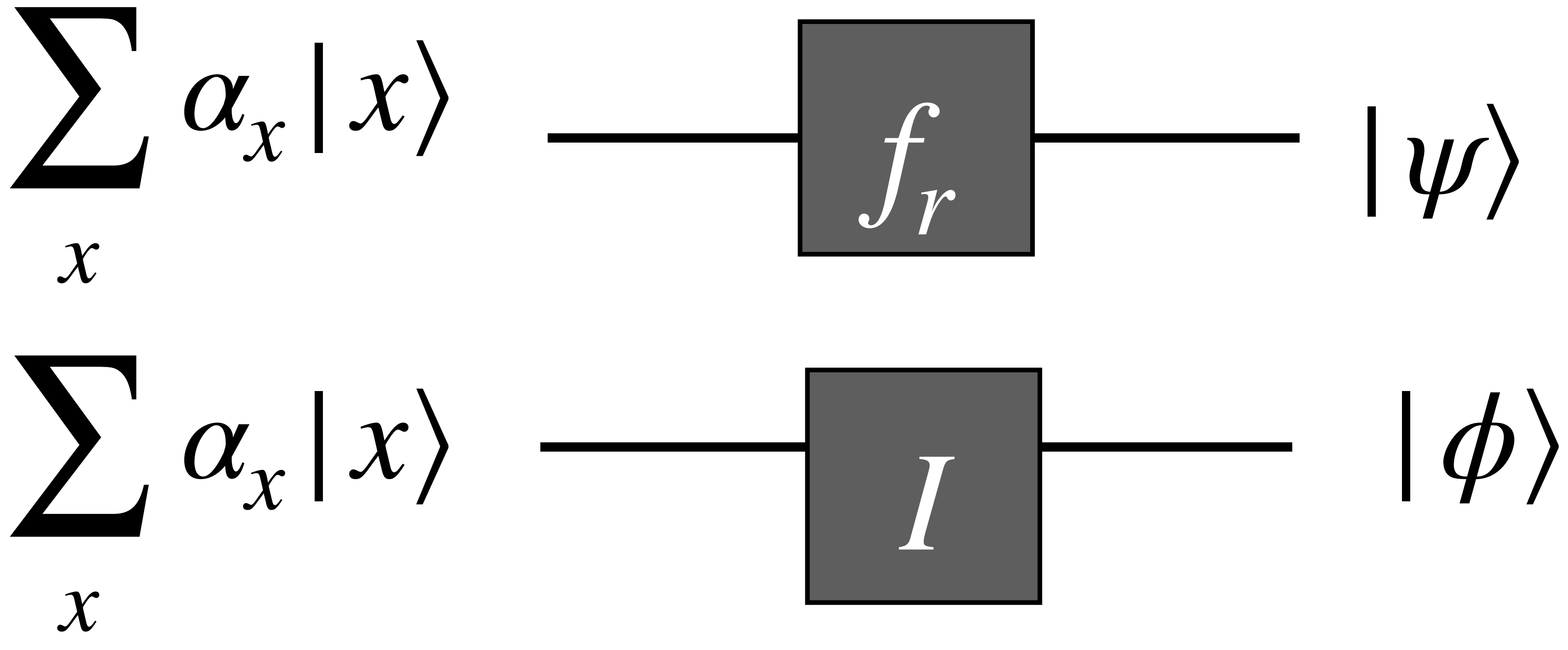


- Averaging over $r \in \{0,1\}^n$, $\| |\psi_r^{(k)}\rangle - |\phi^{(k)}\rangle \| \leq 2k/\sqrt{2^n}$
  - each query only drifts the states apart by a tiny bit

Exercise

1. **Show that** $\| |\psi\rangle - |\phi\rangle \| \leq 2|\alpha_r|$

$f_r(x) = 1$ **iff.** $x = r$.



Logistics

- **HW5 due Sunday**
  - One more to go! Keep up the good work
- **Project [Sign up on google spreadsheet]**
  - Week8. Progress check-up
    - Office hour + after Friday's lecture: mandatory meetings. Sign up ASAP.
  - Week10. Presentations
    - Office hour: voluntary meetings, sign up as you wish
    - Friday's lecture: presentations from you! Sign up a slot ASAP. Details to follow.

Discussion: quantum factoring experiments

- [SSV13] Oversimplifying quantum factoring
  - What are the main critique of prior experiments?
- [MNM+16] Realization of a scalable Shor algorithm
  - Does it address adequately the criticisms in the SSV13? Why and why not?
- Recent estimate on quantum Factoring [hear more from a final presentation]

Scratch