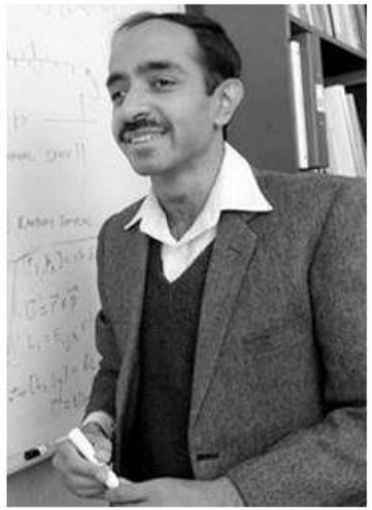
GROVER'S QUANTUM SEARCH ALGORITHM

Grover's Search



- $\mathbb{Z}_2$ with a unique input $\mathbf{b}_0$ such that

VOLUME 79, NUMBER 2 PHYSICAL REVIEW LETTERS 14 JULY 1997

Quantum Mechanics Helps in Searching for a Needle in a Haystack

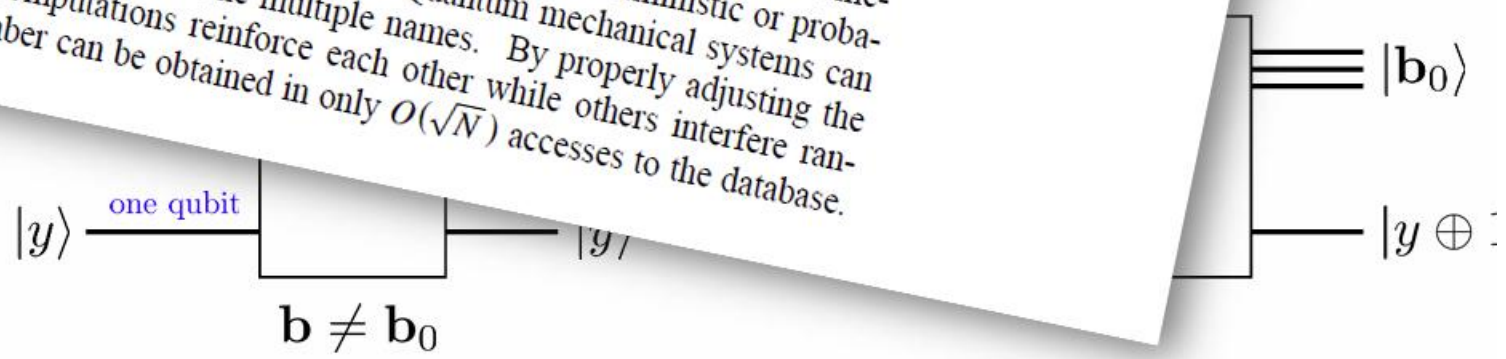
Lov K. Grover*
3C-404A Bell Labs, 600 Mountain Avenue, Murray Hill, New Jersey 07974

(Received 4 December 1996)

Quantum mechanics can speed up a range of search applications over unsorted data. For example, imagine a phone directory containing N names arranged in completely random order. To find someone's phone number with a probability of 50%, any classical algorithm (whether deterministic or probabilistic) will need to access the database a minimum of $0.5N$ times. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ accesses to the database.

[S0031-9007(97)03564-3]

- A quantum oracle for f:



Performing Search with a Quantum Computer

- *Search* is one of the most pervasive tasks in computer science
- Many important problems can be solved by enumerating the possible solutions and then searching amongst them, systematically or randomly, to determine which are correct
- In some cases, determining that certain possibilities are incorrect allows you to eliminate others and hence narrow the search for a true solution
- These search problems are said to be *structured*

Performing Search with a Quantum Computer

- Alternatively, there are other search problems in which you learn nothing useful upon discovering certain possibilities are incorrect, other than the futility of trying those possibilities again
- These search problems are said to be *unstructured*
- Unstructured search is commonly referred to as the *find-the-needle-in-the-haystack problem*

The Unstructured Search Problem

- The concept of an **unstructured** search problem can be demonstrated using a **standard telephone directory**

Name	Phone Number
Alice	314-1592
Bob	271-8281
Charlie	105-4571
Dave	885-4187
Eve	125-6637
Frank	299-7924
Grace	729-7352
⋮	⋮
Zoe	200-2319

The Unstructured Search Problem

- A standard telephone directory contains a list of names, ordered alphabetically, together with their associated telephone numbers
- To find someone's telephone number given knowledge of their name you proceed as follows: open the directory at a random page; if the names on the page alphabetically precede the name you want, mark the current page and open the directory again at a later page

The Unstructured Search Problem

- If the names alphabetically succeed the name you want, mark the page and open the directory again at an earlier page
- For a telephone directory containing N entries, repeating this process, delimited by the marked points, will take you to the sought after entry in roughly $O(\log N)$ steps
- Hence, this algorithm is said to have a complexity of $O(\log N)$, which is deemed “efficient” since it is logarithmic in the number of entries in the telephone directory, or equivalently, polynomial in the number of bits, $n = \log_2 N$, needed to assign a unique index to each entry, i.e., $O(n)$

The Unstructured Search Problem

- If the names alphabetically succeed the name you want, mark the page and open the directory again at an earlier page
- For a telephone directory containing N entries, repeating this process, delimited by the marked points, will take you to the sought after entry in roughly $O(\log N)$ steps
- Hence, this algorithm is said to have a complexity of $O(\log N)$, which is deemed “efficient” since it is logarithmic in the number of entries in the telephone directory, or equivalently, polynomial in the number of bits, $n = \log_2 N$, needed to assign a unique index to each entry, i.e., $O(n)$

The Unstructured Search Problem

- The fundamental reason that telephone directory look-up can be performed so efficiently is that when you fail to find the sought after name on a given page you nevertheless gain reliable information as to the direction in which to search next
- In other words the alphabetically ordered search space is structured and you can exploit this structure to narrow the search for a solution

The Unstructured Search Problem

- Now contrast this with the task of using the same telephone directory to find someone's name given their telephone number
- That is, we are now using the telephone directory to do a reverse lookup
- In this case, because the telephone directory is unordered with respect to telephone numbers, whenever you find a telephone number that is not the given number, you learn nothing useful regarding in which direction to search next, namely, amongst the predecessors or successors of the last telephone number found
- In this case, the search process you are forced to perform is essentially "generate-and-test"

The Unstructured Search Problem

- This consists of opening the phone book at a random page, if that page contains the given number reading off the corresponding name and stopping

- Else marking the page a “dead-end” and picking one of the unread pages at random, repeating this process until the sought after item is found or all the entries have been exhausted

- If there are N entries in the telephone directory it would therefore take you, on average, $O(N/2)$ repetitions of the algorithm to find the given telephone number and hence the associated name

The Unstructured Search Problem

- In the worst case, it is conceivable a really unlucky person would have to search every entry in the directory only to find the given number at the last trial
- So, in the worst case it could take $O(N)$ steps
- We will show very shortly that a quantum computer only takes $O(\sqrt{N})$ using Grover's algorithm
- We can use the aforementioned example of searching a telephone directory to motivate a more formal statement of the unstructured search problem, as follows

The Oracle

- Suppose we wish to search through a search space of N elements
- Rather than search the elements directly, we concentrate on the index to those elements, which is just a number in the range 0 to $N - 1$
- For convenience we assume $N = 2^n$, so the *index* can be stored in n bits, and that the search problem has exactly M solutions, with $1 \leq M \leq N$

The Oracle

- A particular instance of the search problem can conveniently be represented by a function *f*, which takes as input an integer *x*, in the range 0 to $N - 1$
- By definition,

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is a solution to the search problem} \\ 0 & \text{if } x \text{ is NOT a solution to the search problem} \end{cases}$$

where 0 stands for “no” and 1 stands for “yes”

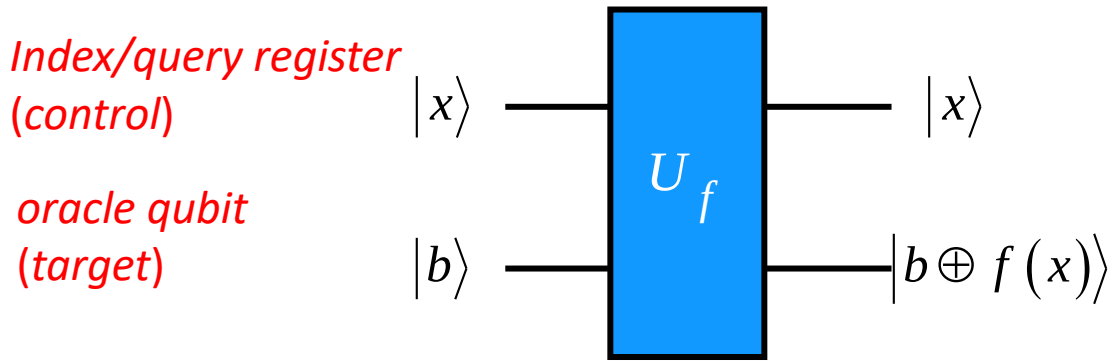
The Oracle

- Suppose we are supplied with a quantum oracle - a black box whose internal workings we discuss later, but which are not important at this stage - with the ability to recognize solutions to the search problem
- This recognition is signaled by making use of an *oracle qubit*

The Oracle

- More precisely, the oracle is a unitary operator, U_f, defined by its action on the **computational basis**:

$$|x\rangle|b\rangle \mapsto U_f\left(|x\rangle|b\rangle\right) = |x\rangle\left|b \oplus f(x)\right\rangle$$

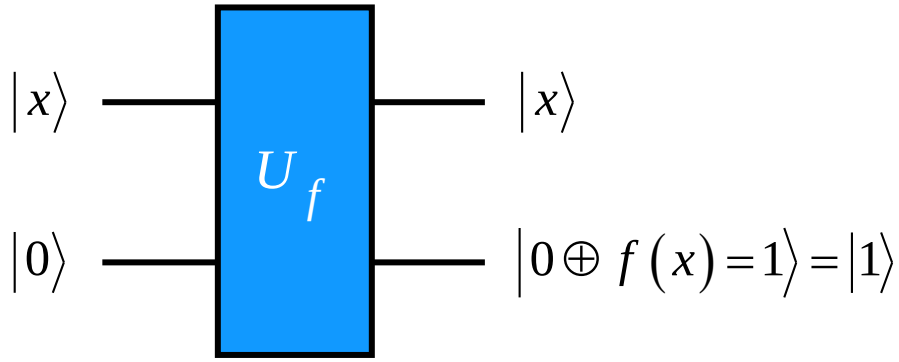


NOTE: Both, the input and output of the quantum oracle, are separable

where $|x\rangle$ is the *query register*, $\oplus$ denotes addition modulo 2, and the *oracle (target) qubit* $|b\rangle$ is a single qubit which is flipped if $f(x) = 1$, and is unchanged otherwise

The Oracle

- We can check whether *x* is a solution to our search problem by preparing $|x\rangle|0\rangle$, applying the oracle and checking to see if the oracle qubit has been flipped to $|1\rangle$



- But this is no better than just applying the oracle for *f* classically
- As in the case of the *QFT* algorithms, to gain a *quantum advantage,* we need to use *quantum superpositions*

The Oracle

- We can easily prepare the first register in a superposition of all possible query values

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle, \quad \left(\text{where } N = 2^n\right)$$

- We can split the above sum into two parts
- The first part is a sum over all the *x* for which $f(x) = 0$; that is, the *bad x* that are not solutions to the search problem
- Let X_{bad} be the set of such *bad x*

The Oracle

- The second part is a sum over all the x for which $f(x) = 1$; that is, the *good* solutions to the search problem
- Let X_{good} be the set of such *good x*
- For convenience, let us **assume** for now that there is only one solution, w, so $X_{good} = \{w\}$

The Oracle

- Define the states

$$\left|\psi_{\text{good}}\right\rangle = \left|w\right\rangle$$

$$\left|\psi_{\text{bad}}\right\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \in X_{\text{bad}}} \left|x\right\rangle$$

- Suppose we prepare the *oracle qubit* of U_f in the state $\left|0\right\rangle$ and the *query register* in a superposition of the form

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \left|x\right\rangle = \frac{1}{\sqrt{N}} \left(\left|w\right\rangle + \sum_{x \neq w} \left|x\right\rangle \right) = \frac{1}{\sqrt{N}} \left|w\right\rangle + \frac{1}{\sqrt{N}} \sum_{x \neq w} \left|x\right\rangle$$

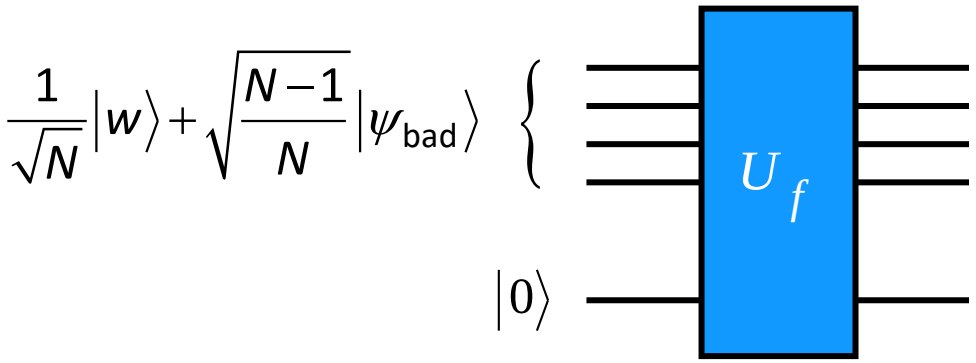
$$= \frac{1}{\sqrt{N}} \left|w\right\rangle + \sqrt{\frac{N-1}{N}} \underbrace{\frac{1}{\sqrt{N-1}} \sum_{x \neq w} \left|x\right\rangle}_{\left|\psi_{\text{bad}}\right\rangle}$$

The Oracle

- Therefore

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|\psi_{\text{bad}}\rangle$$

and the input of the Oracle is shown in Figure



The Oracle

- The output can be easily derived by exploiting the U_f definition

$$|x\rangle|b\rangle \mapsto U_f\left(|x\rangle|b\rangle\right) = |x\rangle\left|b \oplus f(x)\right\rangle$$

- Thus, for $|b\rangle = |0\rangle$

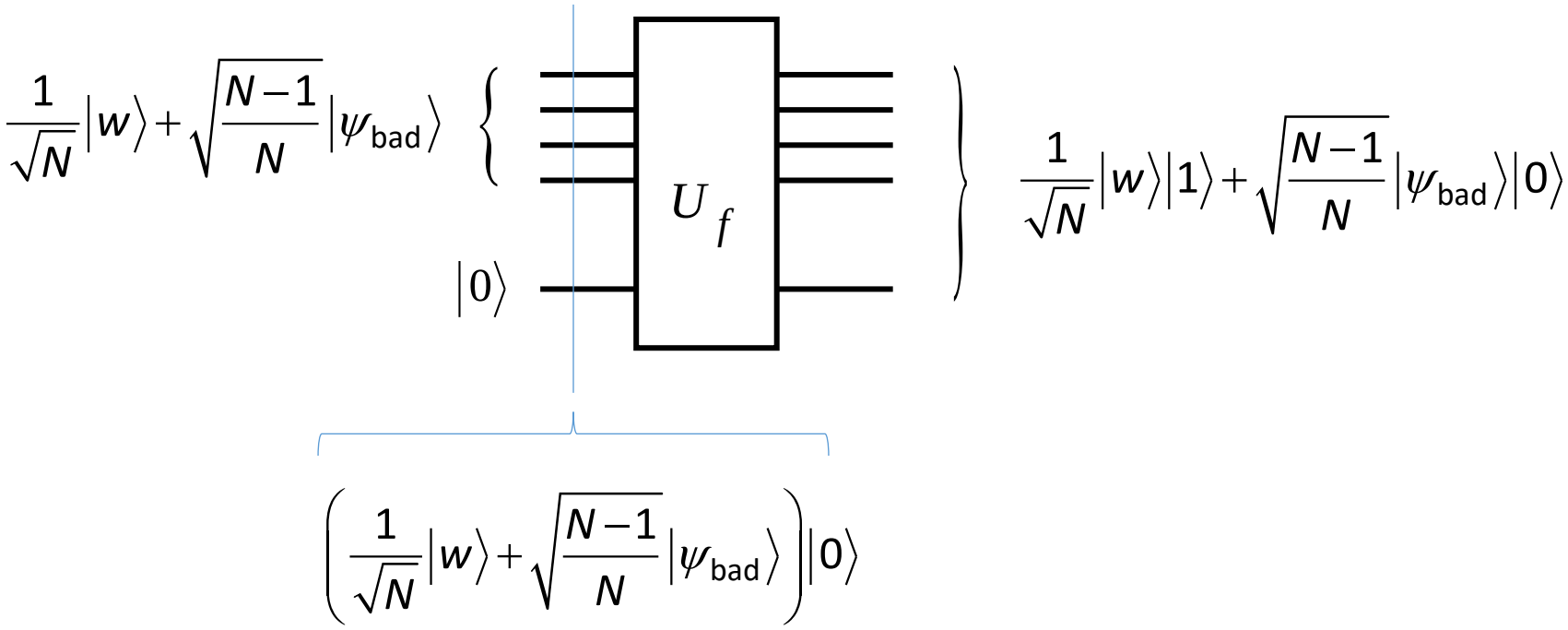
$$U_f\left(\left(\frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|\psi_{\text{bad}}\rangle\right)|0\rangle\right) = \frac{1}{\sqrt{N}}U_f\left(|w\rangle|0\rangle\right) + \sqrt{\frac{N-1}{N}}U_f\left(|\psi_{\text{bad}}\rangle|0\rangle\right)$$

$$= \frac{1}{\sqrt{N}}|w\rangle\left|0 \oplus \underbrace{f(w)}_{=1}\right\rangle + \sqrt{\frac{N-1}{N}}|\psi_{\text{bad}}\rangle\left|0 \oplus \underbrace{f(\psi_{\text{bad}})}_{=0}\right\rangle$$

$$= \frac{1}{\sqrt{N}}|w\rangle|1\rangle + \sqrt{\frac{N-1}{N}}|\psi_{\text{bad}}\rangle|0\rangle \quad \square$$

The Oracle

- The input and output of the Oracle are shown in Figure

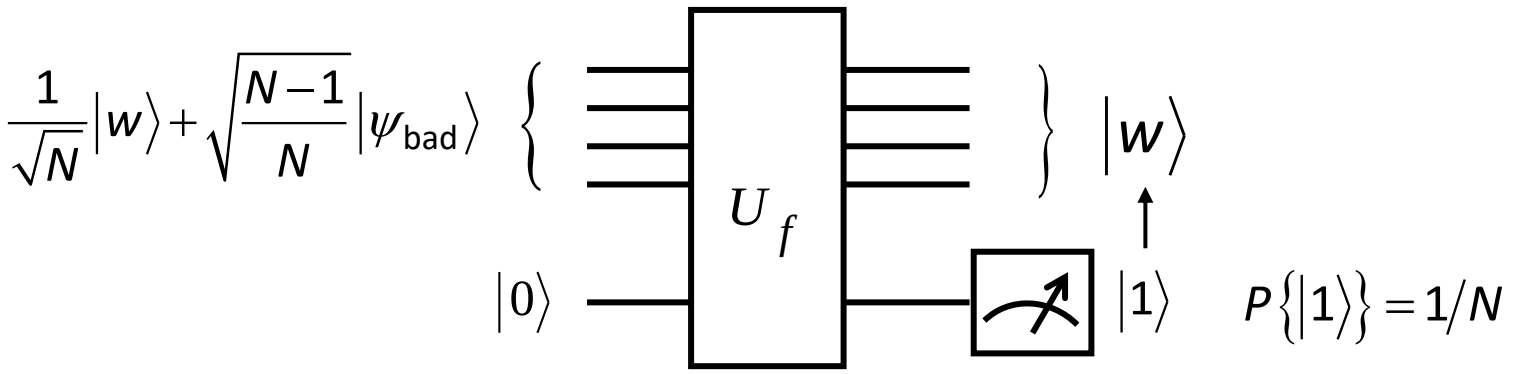


The Oracle

$$\frac{1}{\sqrt{N}}|w\rangle|1\rangle+\sqrt{\frac{N-1}{N}}|\psi_{\text{bad}}\rangle|0\rangle$$

- Now with probability $1/N$ a measurement of the target qubit will give $|1\rangle$, and the query qubits will be left in the good state $|w\rangle$

- Although this procedure uses the **quantum superposition principle**, it does not make any use of **quantum interference**.



The Oracle

- In the quantum search algorithm, it is useful to apply the oracle with the oracle qubit initially in the state $\left(|0\rangle - |1\rangle\right)/\sqrt{2}$, just as was done in the Deutsch–Jozsa algorithm
- If *x* is NOT a solution to the search problem, i.e. *f*(*x*) = 0, applying the oracle to the state $|x\rangle\left(|0\rangle - |1\rangle\right)/\sqrt{2}$ does not change the state, as shown below

$$U_f\left(|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) = \frac{1}{\sqrt{2}}U_f\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) = \frac{1}{\sqrt{2}}U_f\left(|x\rangle|0\rangle\right) - \frac{1}{\sqrt{2}}U_f\left(|x\rangle|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}|x\rangle\left|0 \oplus \underbrace{f(x)}_{=0}\right\rangle - \frac{1}{\sqrt{2}}|x\rangle\left|1 \oplus \underbrace{f(x)}_{=0}\right\rangle = |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

The Oracle

- Conversely, if *x* IS a solution to the search problem, i.e. $f(x) = 1$, then $|0\rangle$ and $|1\rangle$ are interchanged by the action of the oracle, giving a final state $-|x\rangle\left(\left(|0\rangle-|1\rangle\right)/\sqrt{2}\right)$ as shown below

$$U_f\left(|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right)=\frac{1}{\sqrt{2}}U_f\left(|x\rangle|0\rangle-|x\rangle|1\rangle\right)=\frac{1}{\sqrt{2}}U_f\left(|x\rangle|0\rangle\right)-\frac{1}{\sqrt{2}}U_f\left(|x\rangle|1\rangle\right)$$

$$=\frac{1}{\sqrt{2}}|x\rangle\Big|0\oplus\underbrace{f(x)}_{=1}\Big\rangle-\frac{1}{\sqrt{2}}|x\rangle\Big|1\oplus\underbrace{f(x)}_{=1}\Big\rangle=\frac{1}{\sqrt{2}}|x\rangle|0\oplus1\rangle-\frac{1}{\sqrt{2}}|x\rangle|1\oplus1\rangle$$

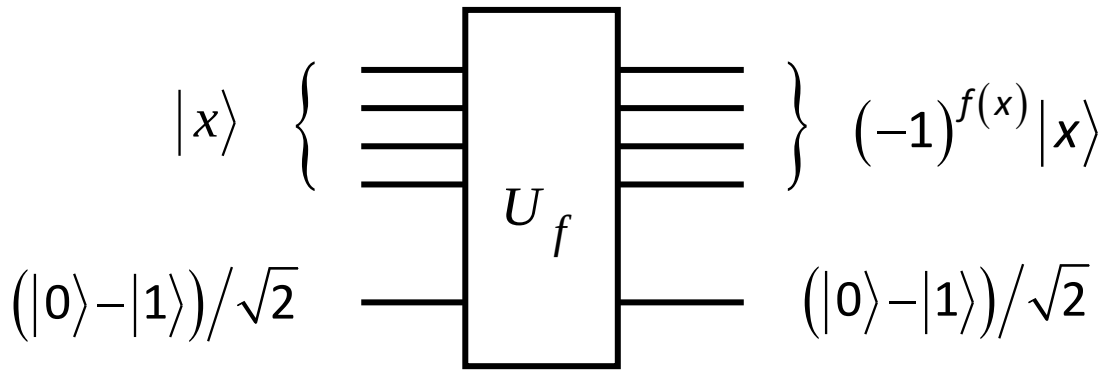
$$=\frac{1}{\sqrt{2}}|x\rangle|1\rangle-\frac{1}{\sqrt{2}}|x\rangle|0\rangle=-|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

The Oracle

- The action of the oracle is thus:

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\xrightarrow{U_f}(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

- Notice that the state of the oracle qubit is NOT changed



It turns out that this $(|0\rangle-|1\rangle)/\sqrt{2}$ remains throughout the quantum search algorithm, and can therefore be omitted from further discussion of the algorithm, simplifying our description

The Oracle

- With this convention, the action of the oracle may be written:

$$|x\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle \qquad \text{or} \qquad U_f|x\rangle = \begin{cases} -|x\rangle & \text{if } x = w \\ +|x\rangle & \text{if } x \neq w \end{cases}$$

- So, the effect is to encode the answer to the Oracle query in a *phase shift*
- Recall this idea of encoding an answer in a quantum phase was key to the operation of the *QFT* algorithms as well
- It is convenient, for the rest of this chapter, to redefine U_f to be the *n*-qubit operator that performs the above transformation

The Oracle

- On the basis

$$\left\{|w\rangle, |\psi_{\text{bad}}\rangle\right\}$$

the matrix associated to U_f is

$$U_f = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

The Oracle

- We will also define an *n*-qubit *phase shift operator* $U_{0^\perp}$ that acts as follows

$$U_{0^\perp} : \begin{cases} |x\rangle \mapsto -|x\rangle, & x \neq 0 \\ |0\rangle \mapsto |0\rangle \end{cases}$$

- This operator applies a phase shift of −1 to all *n*-qubit states orthogonal to the state $|00\ldots0\rangle$
- Thus, $U_{0^\perp}$ is a reflection about the all zeros state $|00\ldots0\rangle = |0\rangle^{\otimes n}$

The Oracle

- Note that $U_{0^\perp}$ can also be written as

$$U_{0^\perp} = 2|0\rangle\langle 0| - I$$

- Proof

$$U_{0^\perp} = |0\rangle\langle 0| + (-1)\sum_{x\neq 0}|x\rangle\langle x| = |0\rangle\langle 0| + (-1)\left(\underbrace{\sum_{x=0}^{N-1}|x\rangle\langle x|}_{=I} + (-1)|0\rangle\langle 0|\right)$$

$$= |0\rangle\langle 0| + (-1)\left(I + (-1)|0\rangle\langle 0|\right) = |0\rangle\langle 0| - I + |0\rangle\langle 0| = 2|0\rangle\langle 0| - I \qquad \square$$

Grover's Quantum Search Algorithm

- Now we can define the operator that does the job of increasing the amplitude of $|\psi_{\text{good}}\rangle = |w\rangle$
- This operator

$$G = HU_{0^{\perp}}HU_f$$

is called the *Grover iteration, Grover operator, or quantum search iterate*

Grover's Quantum Search Algorithm

$$G = HU_{0^\perp}HU_f$$

- Let $|\psi\rangle = H^{\otimes n}|00\ldots0\rangle \equiv H|00\ldots0\rangle$. It can be shown that

To simplify writing

$$HU_{0^\perp}H = 2|\psi\rangle\langle\psi| - I$$

- Proof

$$\begin{aligned} 2|\psi\rangle\langle\psi| - I &= 2H|00\ldots0\rangle\langle00\ldots0|H^\dagger - HH^\dagger \\ &= 2H|00\ldots0\rangle\langle00\ldots0|H - HIH \\ &= H\left(2|00\ldots0\rangle\langle00\ldots0| - I\right)H \\ &= HU_{0^\perp}H \end{aligned}$$

H is Unitary

$$U_{0^\perp} = 2|0\rangle\langle0| - I$$

□

- Therefore, *G* can be written as

$$G = \left(HU_{0^\perp}H\right)U_f = \left(2|\psi\rangle\langle\psi| - I\right)U_f$$

Grover's Quantum Search Algorithm

- Let's denote by $U_{\psi^\perp}$ the operator

$$U_{\psi^\perp} = HU_{0^\perp}H = 2|\psi\rangle\langle\psi| - I$$

- In the following we will show that $U_{\psi^\perp}$ applied to a general state $|\phi\rangle = \sum_k \alpha_k |k\rangle$ produces

$$U_{\psi^\perp}|\phi\rangle = U_{\psi^\perp}\left(\sum_k \alpha_k |k\rangle\right) = \sum_k (-\alpha_k + 2\mu)|k\rangle, \qquad [1]$$

where $\mu = \sum_k \alpha_k / N$ is the mean value of the amplitudes α_k

- For this reason, $U_{\psi^\perp}$ is sometimes referred to as the *inversion about the mean operation*

Grover's Quantum Search Algorithm

- Proof

$$U_{\psi^\perp}|\phi\rangle = \left(2|\psi\rangle\langle\psi| - I\right)\sum_k \alpha_k |k\rangle = 2|\psi\rangle\langle\psi|\left(\sum_k \alpha_k |k\rangle\right) - \sum_h \alpha_h |k\rangle \qquad [2]$$

- Since

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle \rightarrow |\psi\rangle\langle\psi| = \left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\langle i|\right) = \frac{1}{N}\sum_{j,i=0}^{N-1}|j\rangle\langle i|$$

- It follows that

$$2|\psi\rangle\langle\psi|\left(\sum_k \alpha_k |k\rangle\right) = 2\sum_{k,j,i=0}^{N-1}\alpha_k \frac{1}{N}|j\rangle\langle i|k\rangle = 2\sum_{k,i,j=0}^{N-1}\alpha_k \frac{1}{N}|j\rangle\delta_{ik}$$

$$= 2\sum_{i,j=0}^{N-1}\alpha_i \frac{1}{N}|j\rangle = 2\left(\sum_{i=0}^{N-1}\frac{\alpha_i}{N}\right)\left(\sum_{j=0}^{N-1}|j\rangle\right) = 2\mu\sum_{i=0}^{N-1}|j\rangle \qquad [3]$$

Grover's Quantum Search Algorithm

By putting [3] into [2] we obtain [1], i.e., the inversion about the mean operation

$$U_{\psi^{\perp}} \left|\phi\right\rangle = \sum_{k} \left(-\alpha_k + 2\mu\right) \left|k\right\rangle$$

□

Grover's Quantum Search Algorithm

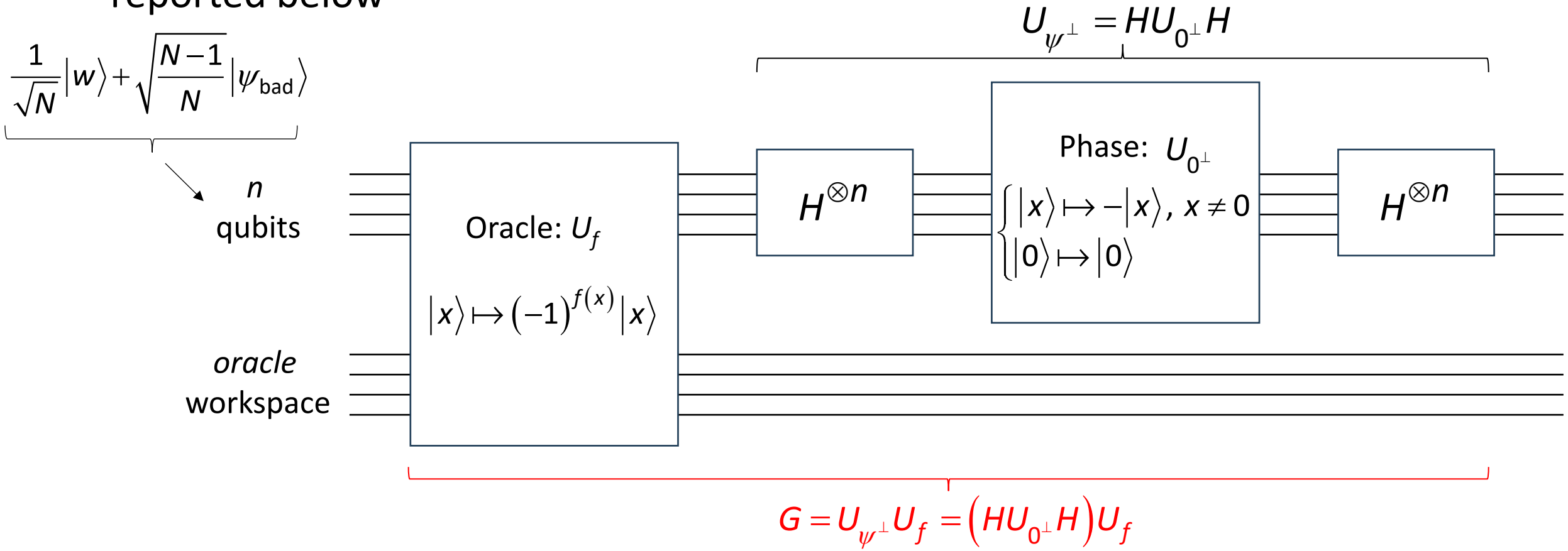
- The Grover iteration *G* is **defined** by the following sequence of transformations....

THE GROVER ITERATION

1) Apply the oracle U_f
2) Apply the Hadamard transform $H^{\otimes n}$
3) Apply $U_{0^\perp}$
4) Apply the Hadamard transform $H^{\otimes n}$

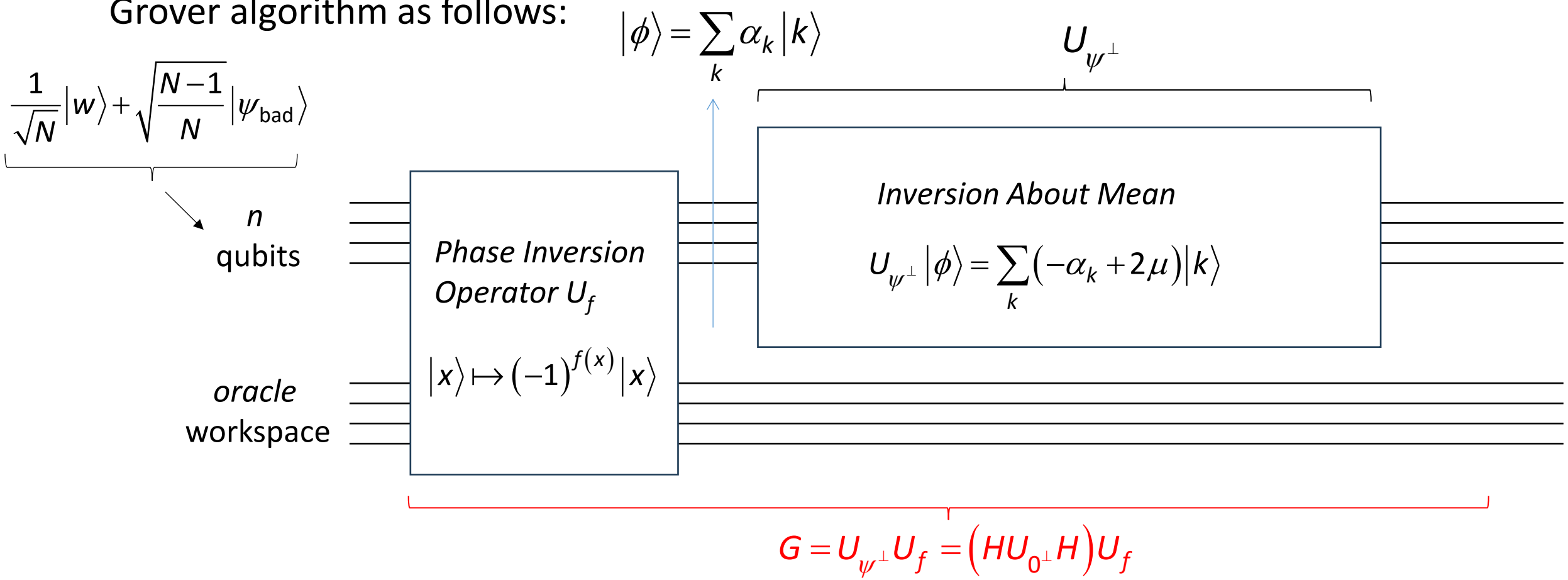
Grover's Quantum Search Algorithm

....while the circuit that implements the Grover iteration, $G = HU_{0^\perp}HU_f$, is reported below



Grover's Quantum Search Algorithm

Since $U_{\psi^\perp}$ performs the inversion about the mean operation we can also represent the Grover algorithm as follows:



Grover's Quantum Search Algorithm

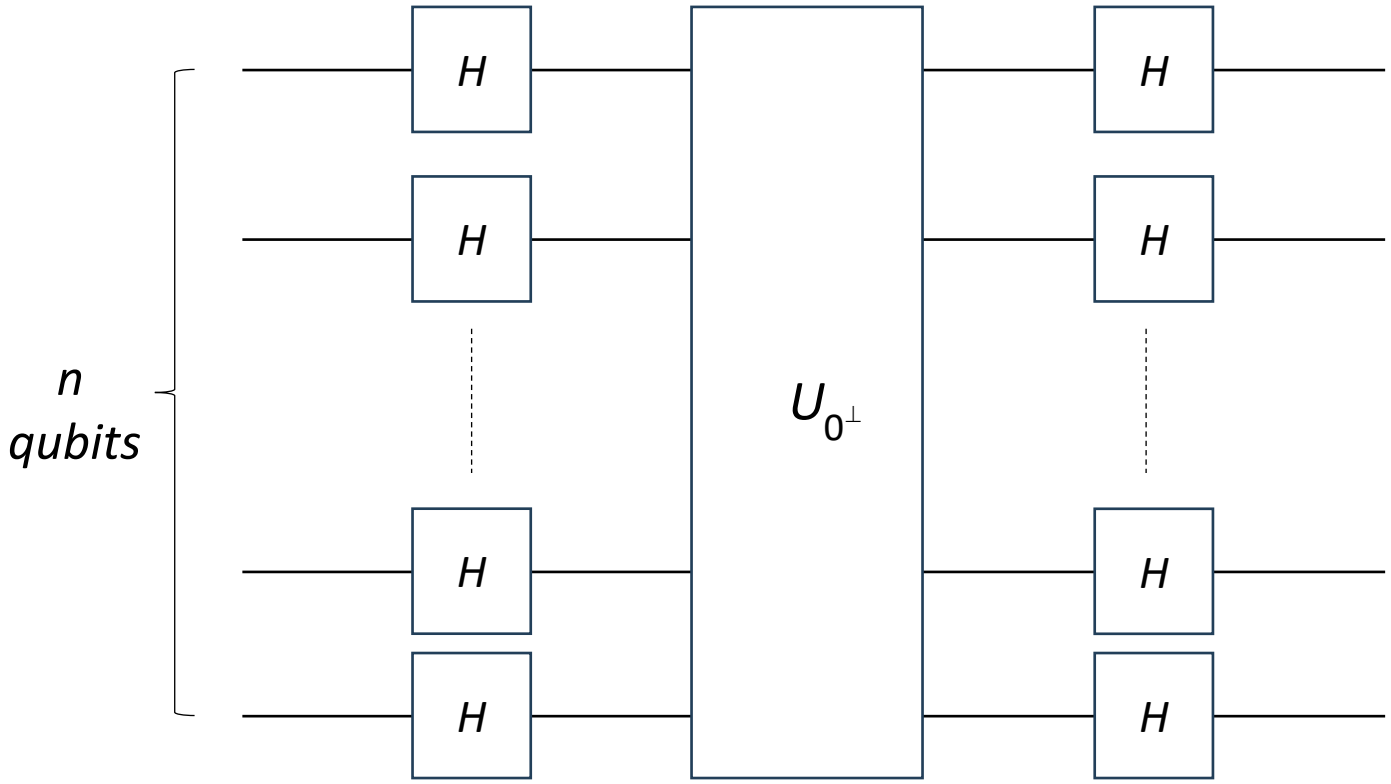
- The internal workings of the oracle, including the possibility of it needing extra work qubits, are not important to the description of the quantum search algorithm

- On the other hand, we want to derive the quantum circuit of the $U_{\psi^{\perp}}$ operator reported in the previous slide

Grover's Quantum Search Algorithm

$$U_{0^\perp}: \begin{cases} |x\rangle \mapsto -|x\rangle, & x \neq 0 \\ |0\rangle \mapsto |0\rangle \end{cases}$$

As we said earlier, $U_{0^\perp}$ is a reflection about the all zeros state $|00\ldots0\rangle = |0\rangle^{\otimes n}$



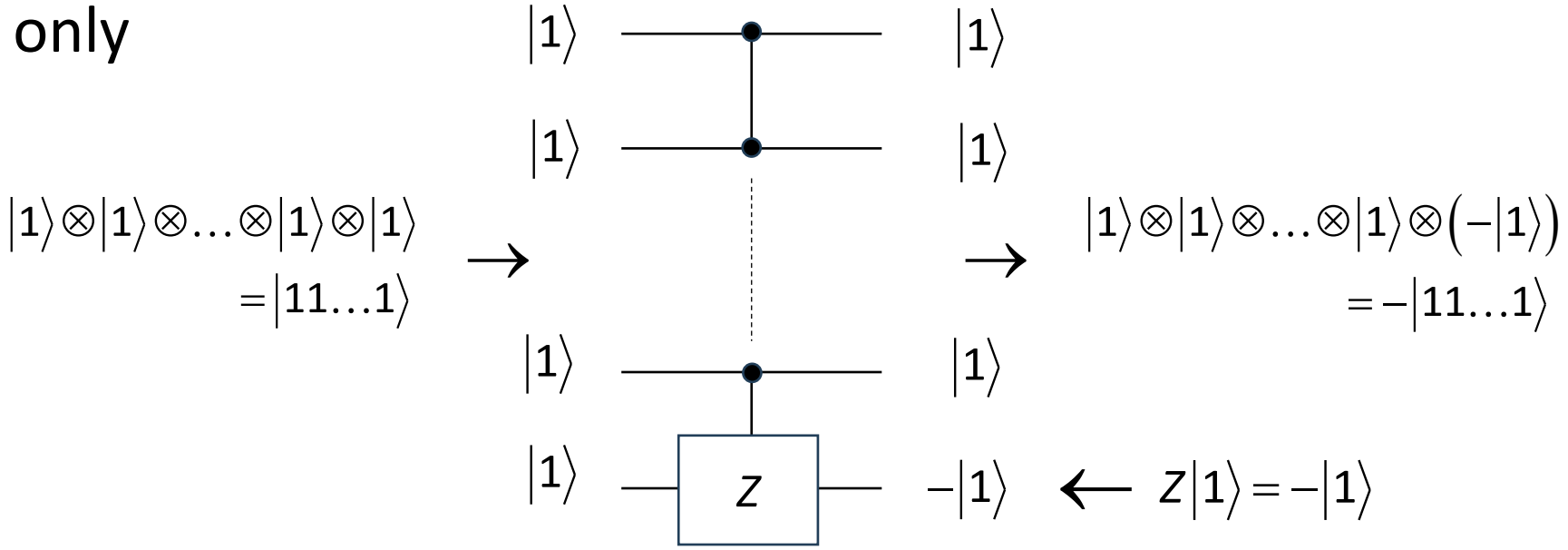
$U_{\psi^\perp} = HU_{0^\perp}H$ structure

Grover's Quantum Search Algorithm

- To create a circuit for $U_{0^\perp}$, recall

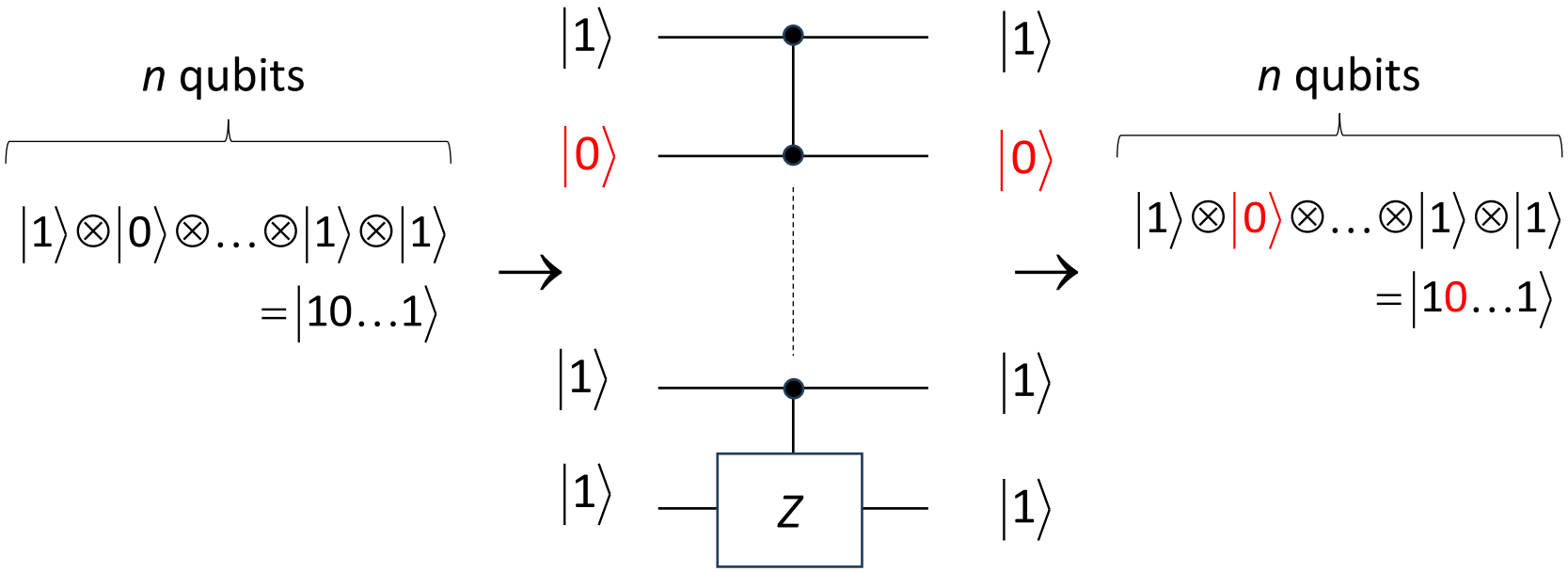
$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

- Then the following circuit flips the sign of all one's state $|11\ldots1\rangle = |1\rangle^{\otimes n}$ only



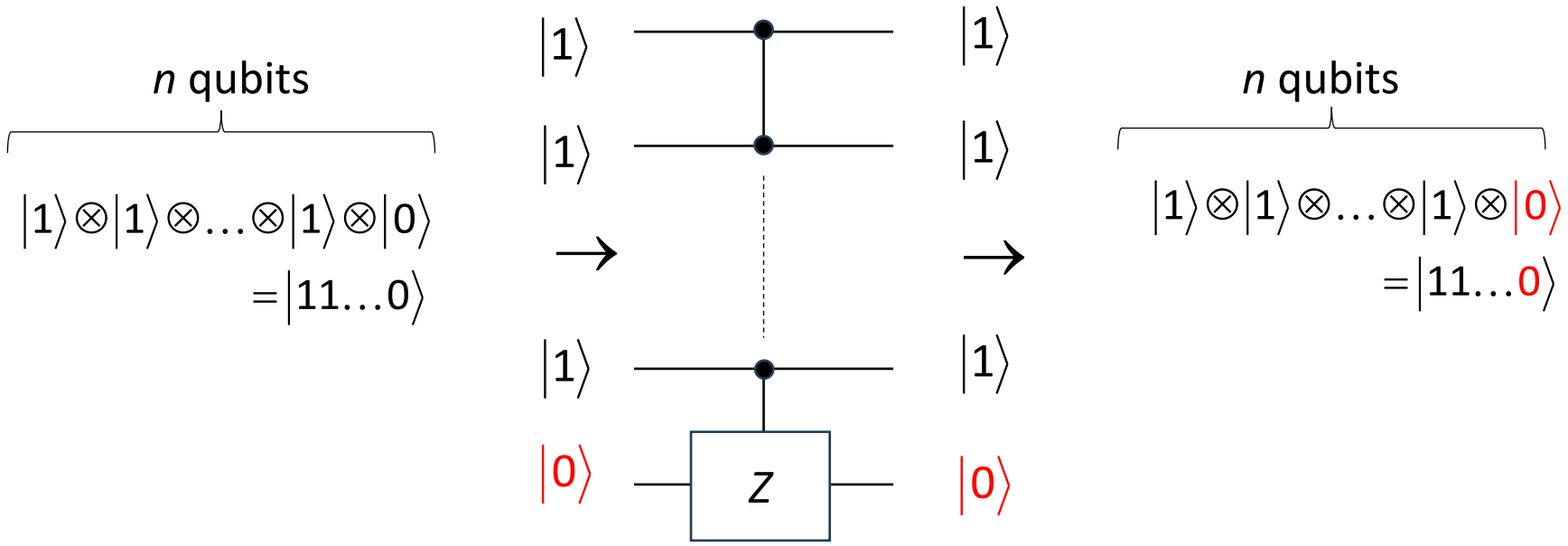
Grover's Quantum Search Algorithm

- For any input different from $|11\ldots1\rangle = |1\rangle^{\otimes n}$, the state remains unchanged
- Example #1



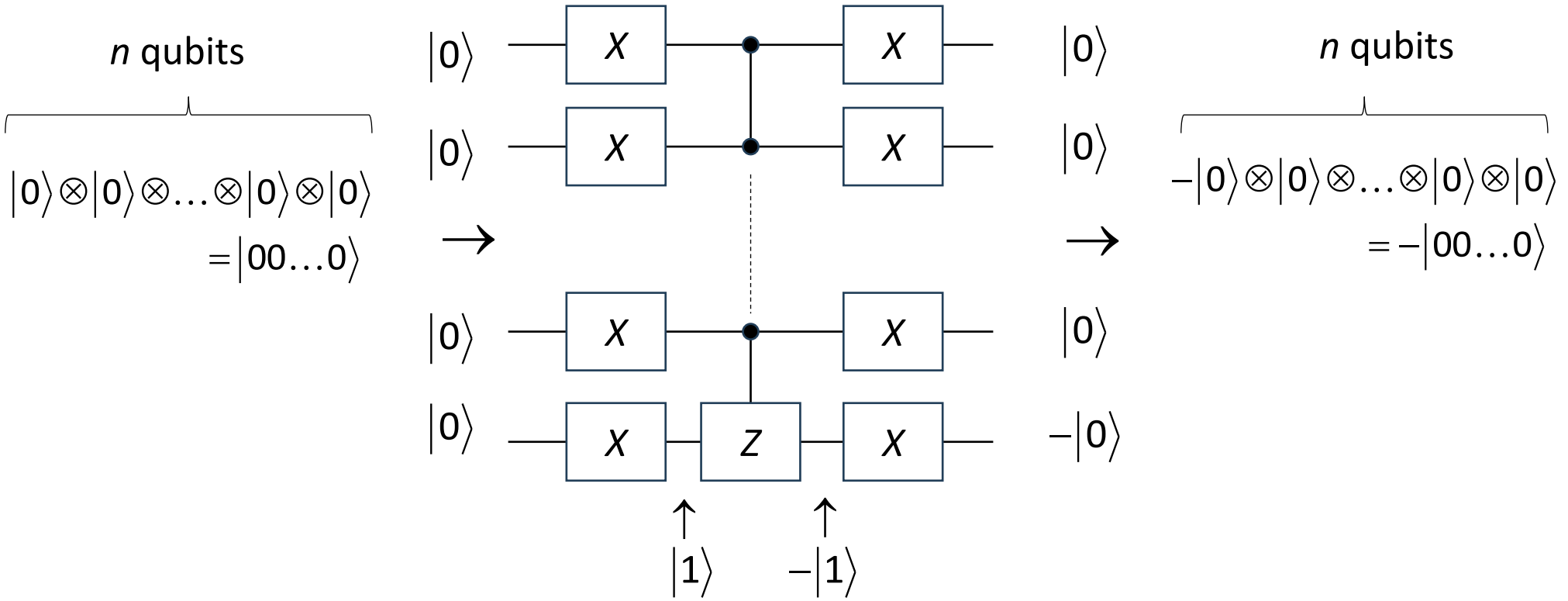
Grover's Quantum Search Algorithm

- Example #2



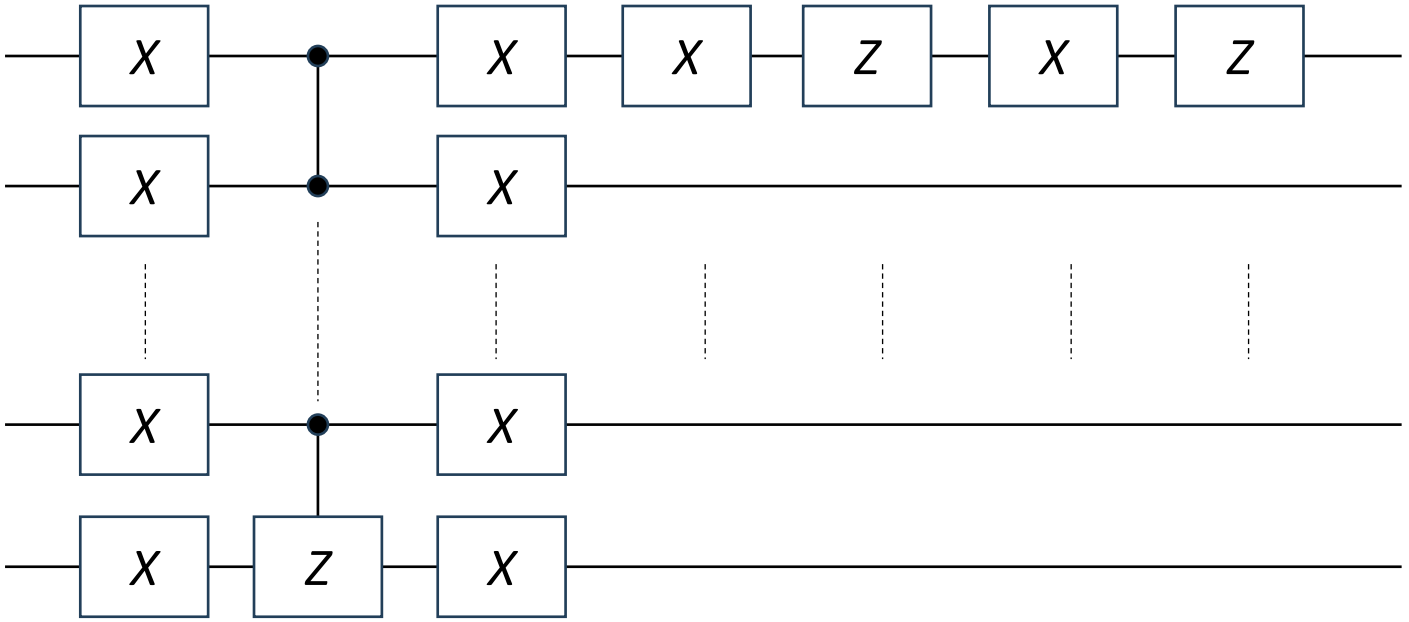
Grover's Quantum Search Algorithm

- If we multiply this on both sides by *X* gates, the resulting circuit *will flip the sign* of the all zeros state $|00\ldots0\rangle = |0\rangle^{\otimes n}$ only:



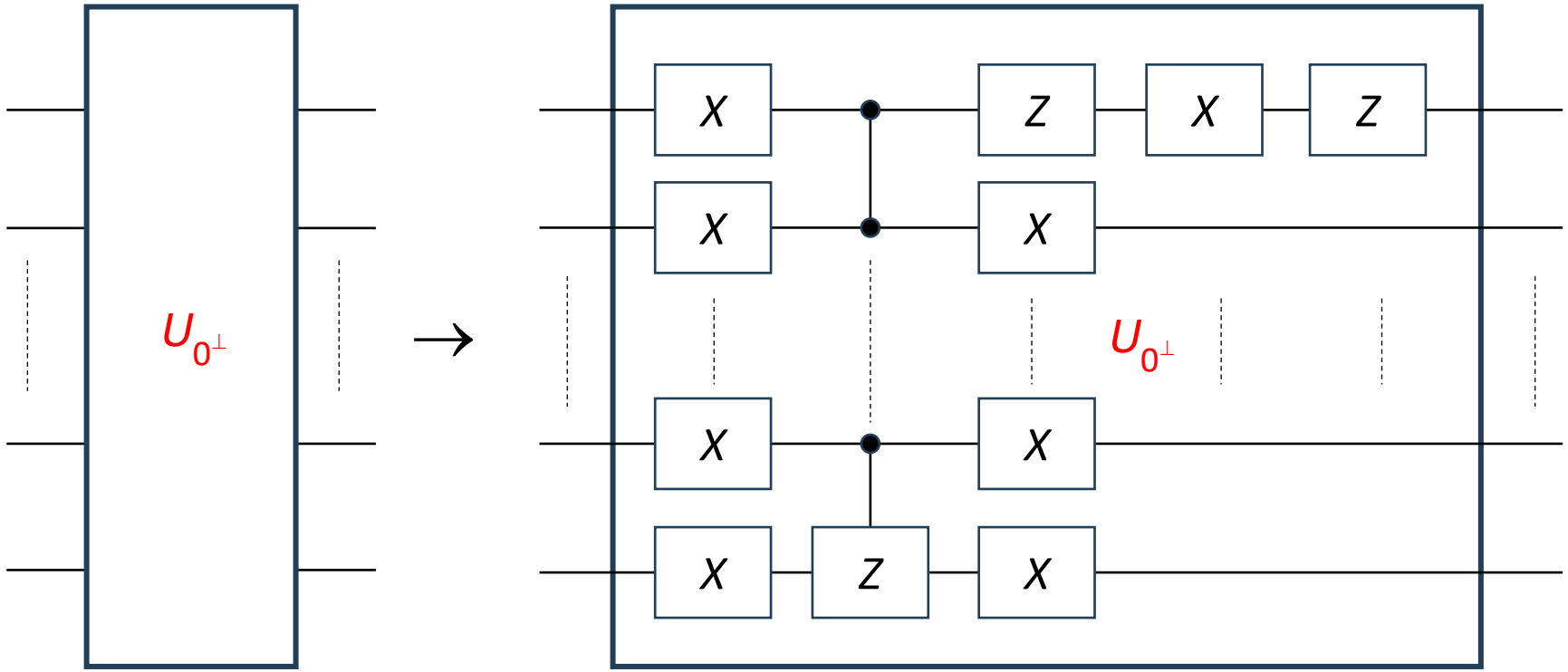
Grover's Quantum Search Algorithm

- But, the all zeros state should be unchanged, while all other states are flipped
- We use *ZXZX* to **flip the sign of the top qubit**, which flips the sign of the entire state



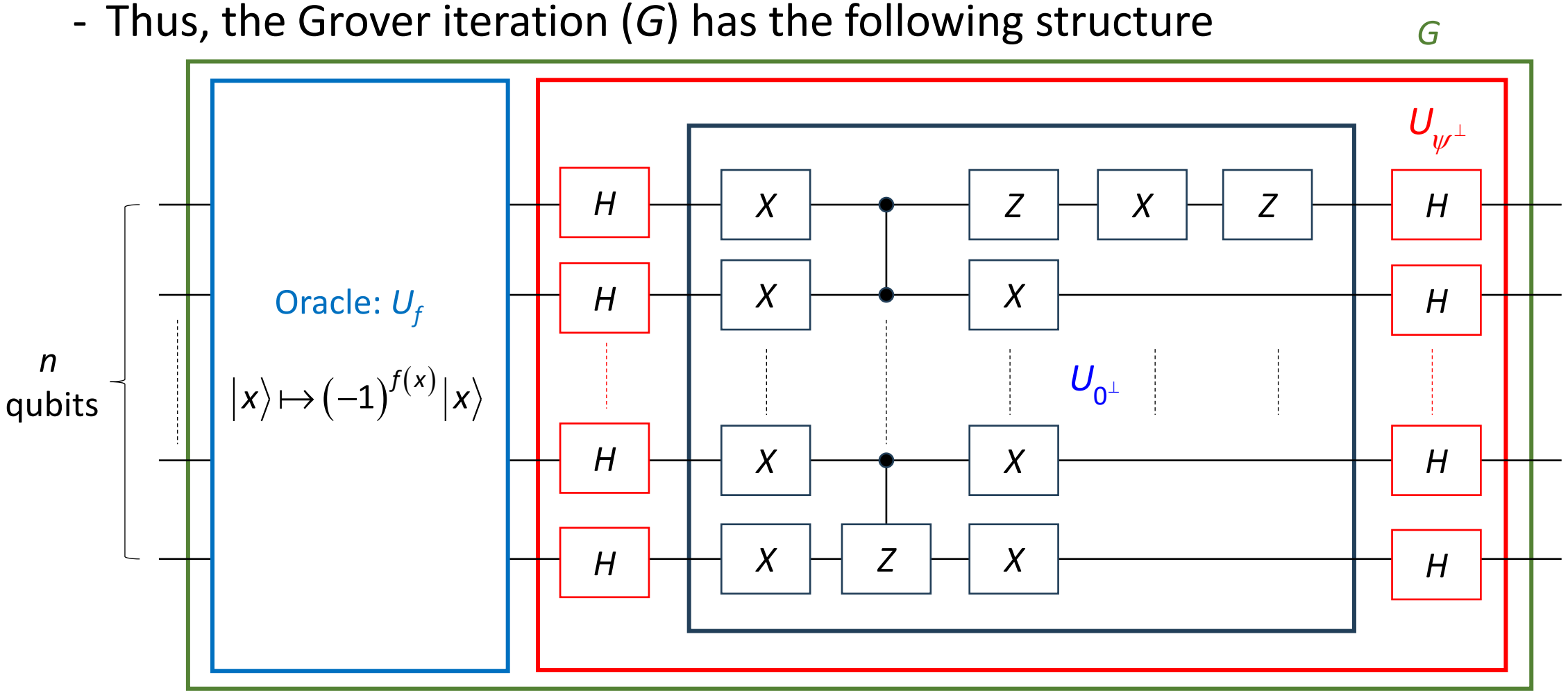
Grover's Quantum Search Algorithm

- Using $X^2 = I$, the gate structure of $U_{0^\perp}$ is:



Grover's Quantum Search Algorithm

- Thus, the Grover iteration (G) has the following structure



Grover's Quantum Search Algorithm

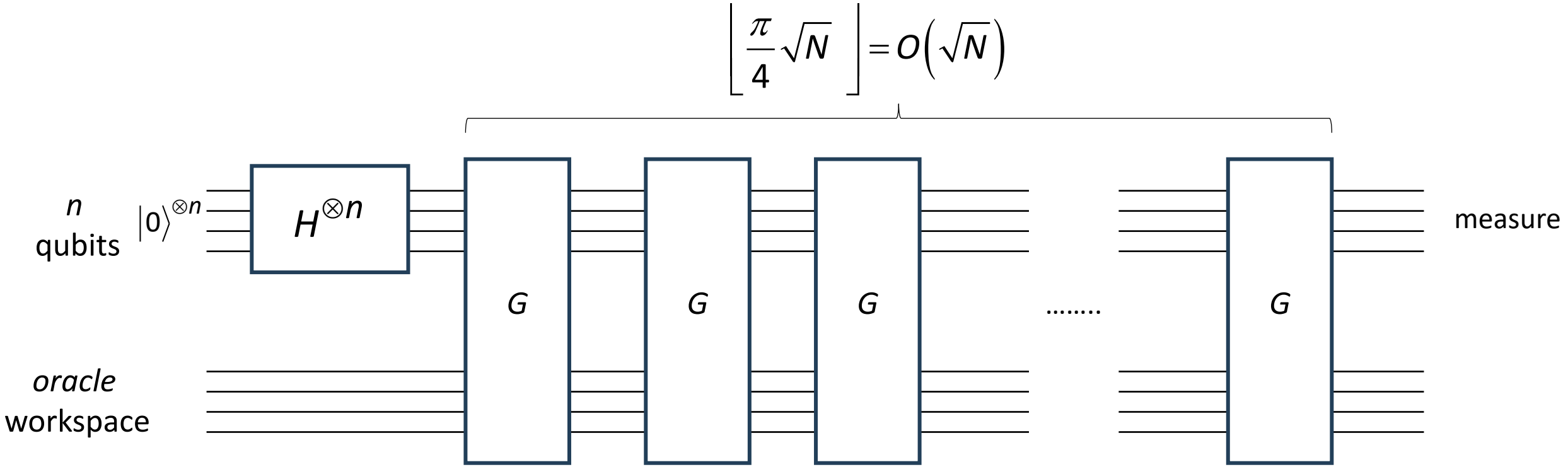
- Now the Grover's quantum searching algorithm can be written succinctly as follows

GROVER'S QUANTUM SEARCH ALGORITHM

1) Start with the n-qubit state $|00\ldots0\rangle \equiv |0\rangle^{\otimes n}$
2) Apply the n-qubit Hadamard gate $H^{\otimes n}$ to prepare the state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$, (where $N = 2^n$)
3) Apply the Grover iteration G a total of $\left\lfloor \frac{\pi}{4} \frac{1}{\sqrt{N}} \right\rfloor$ times
4) Measure the resulting state

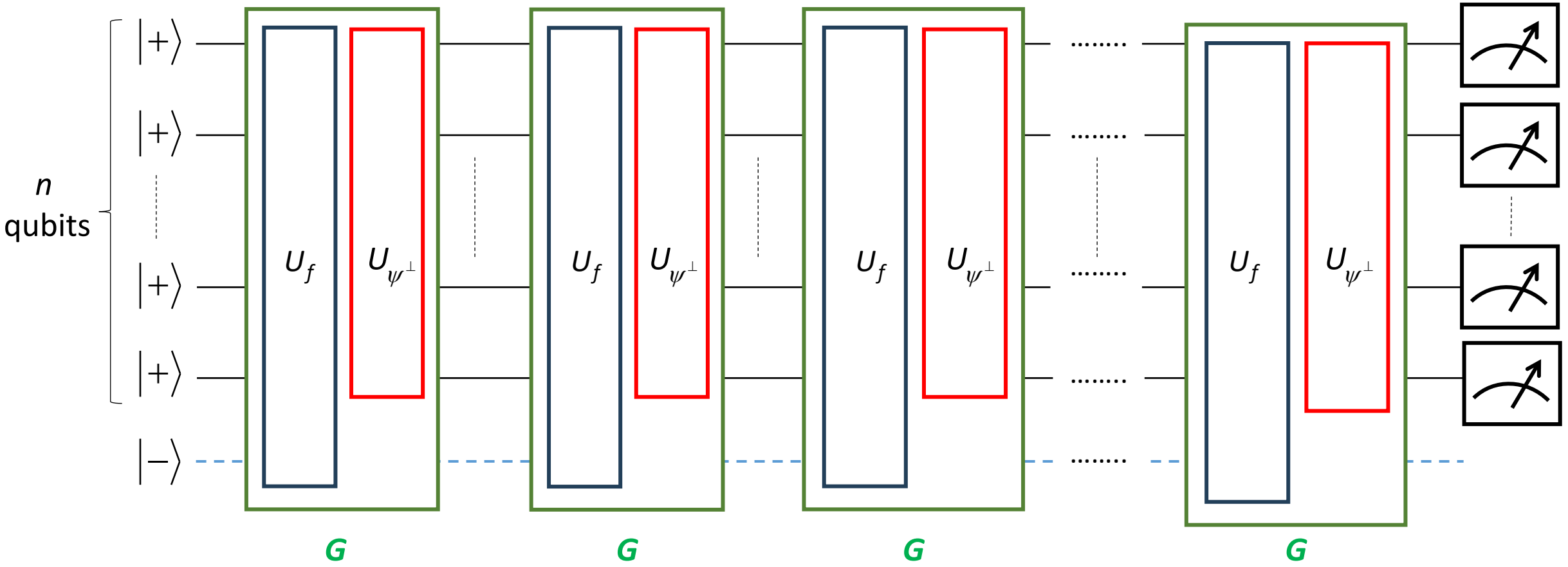
Grover's Quantum Search Algorithm

…while the circuit that implements the Grover algorithm is reported below



Grover's Quantum Search Algorithm

The Grover's algorithm with the oracle (target) qubit in state $|-\rangle$



Grover's Quantum Search Algorithm

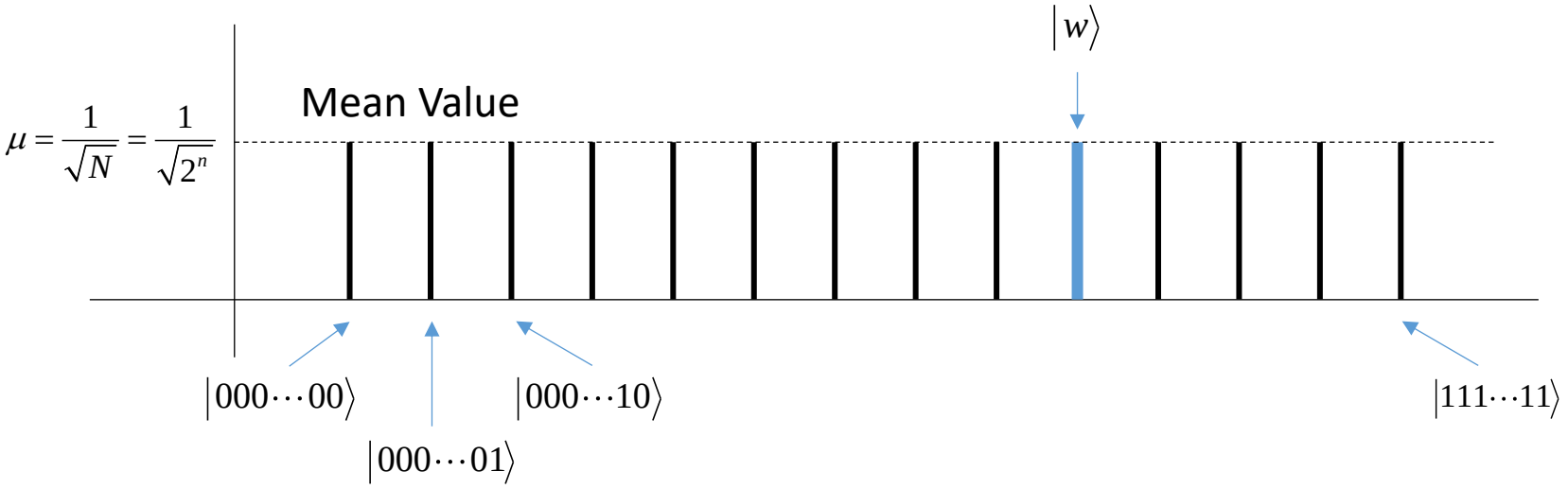
- Since

$$H\left|00\ldots0\right\rangle \equiv H^{\otimes n}\left|0\right\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\left|x\right\rangle, \text{ where } N = 2^n,$$

  has only real amplitudes, and the Grover iteration does not introduce any complex phases, then the amplitudes always remain real

- This allows us to represent the amplitudes as lines above (for positive amplitudes) or below (for negative amplitudes), an axis labelled by the *N* possible inputs, as done in the next Figure

Grover's Quantum Search Algorithm



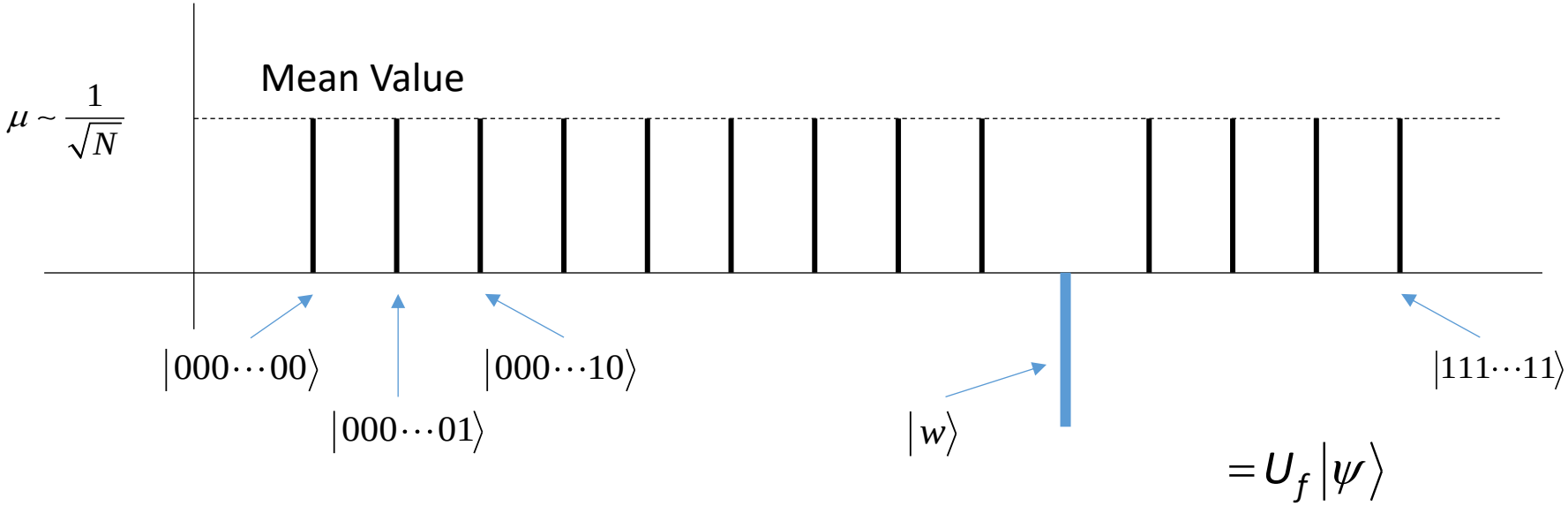
$$= H|00\ldots0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle, \quad \text{where } N = 2^n$$
$$= |\psi\rangle$$

$$\downarrow$$

$$\mu = \text{Mean Value of the Amplitudes} = \frac{N \times \left(1/\sqrt{N}\right)}{N} = \frac{1}{\sqrt{N}}$$

Grover's Quantum Search Algorithm

- $|\psi\rangle$ is now given as input to the Grover Iteration *G*
- After the application of U_f to $|\psi\rangle$, the amplitude of $|w\rangle$ picks up a −1 phase shift, and thus the mean value of the amplitudes shifts down slightly, as illustrated in the Figure below



Grover's Quantum Search Algorithm

- Formally,

$$U_f|\psi\rangle = -\frac{1}{\sqrt{N}}|w\rangle + \underbrace{\frac{1}{\sqrt{N}}\sum_{\substack{x\in\{0,1\}^n \\ x\neq w}}|x\rangle}_{N-1 \text{ states}}, \quad \text{where } N = 2^n$$

$$\mu = \text{Mean Value of the Amplitudes} = \frac{-1/\sqrt{N} + (N-1)\times\left(1/\sqrt{N}\right)}{N} = \frac{N-2}{N\sqrt{N}}$$

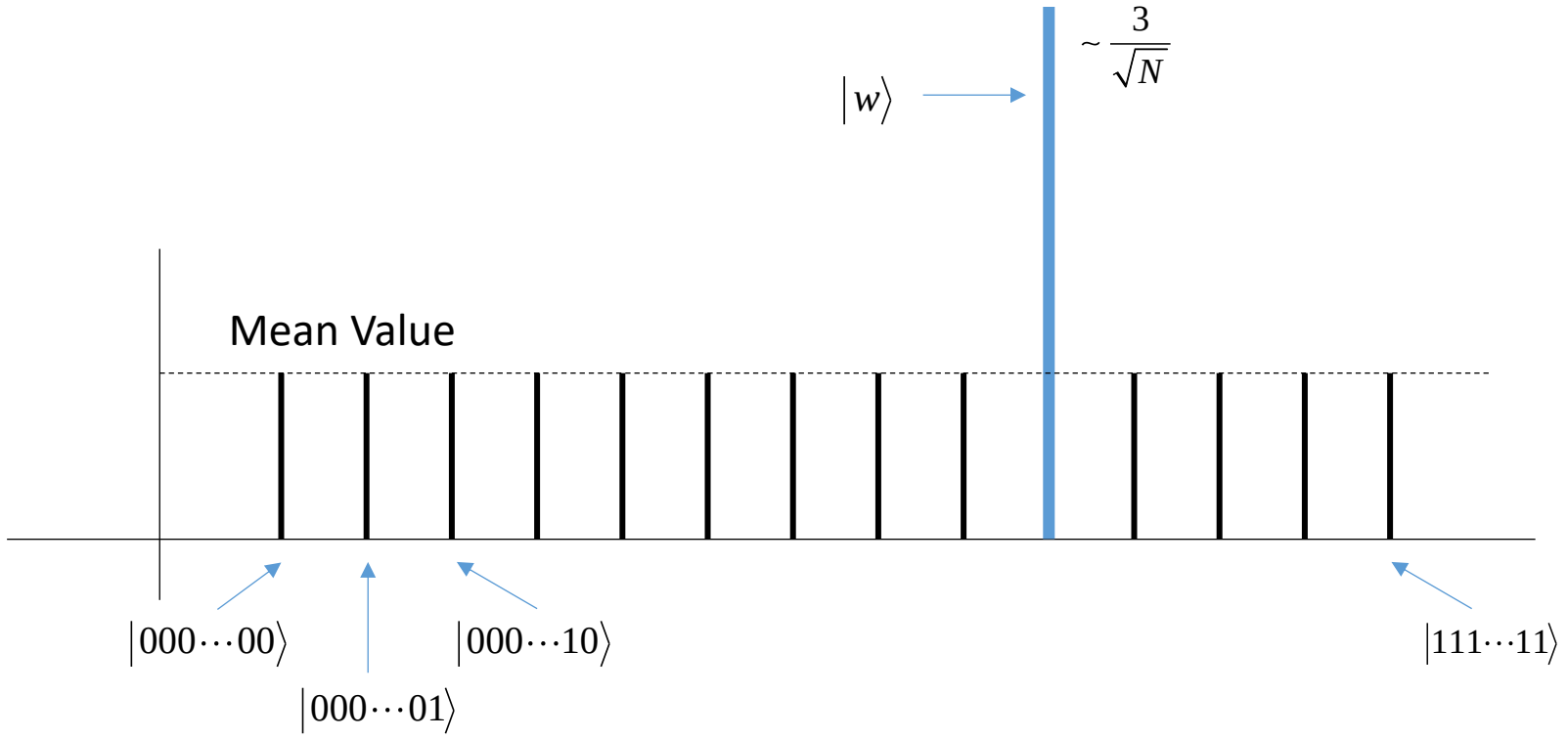
$$\text{For } N \gg 1 \quad \rightarrow \quad \mu \sim \frac{1}{\sqrt{N}}$$

- Therefore, for N>>1 the mean value of the amplitude is $1/\sqrt{N}$ minus an insignificant amount

Grover's Quantum Search Algorithm

- Now, remember that $G = \left(2|\psi\rangle\langle\psi| - I\right)U_f = U_{\psi^\perp}U_f$
- Therefore, the operator $2|\psi\rangle\langle\psi| - I$ will be applied to $U_f|\psi\rangle$ which produces an *inversion about the mean,* which nearly triples the size of the amplitude of $|w\rangle$, and slightly nudges down the amplitudes of all the other basis states, as illustrated in the next slide

Grover's Quantum Search Algorithm



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

Grover's Quantum Search Algorithm

- Another application of U_f makes the amplitude of $|w\rangle$ negative again, slightly pushing down the mean value of the amplitudes, and the inversion about the mean operation adds roughly another $2/\sqrt{N}$ to the size of the amplitude of $|w\rangle$ and slightly nudges down the amplitudes of all the other basis states

Grover's Quantum Search Algorithm

- Now we can define the operator that does the job of increasing the amplitude of $|\psi_{\text{good}}\rangle = |w\rangle$
- This operator

$$G = HU_{0^{\perp}}HU_f$$

is called the *Grover iteration, Grover operator, or quantum search iterate*

Grover's Quantum Search Algorithm

$$G = HU_{0^\perp}HU_f$$

- Let $|\psi\rangle = H^{\otimes n}|00\ldots0\rangle \equiv H|00\ldots0\rangle$. It can be shown that

To simplify writing

$$HU_{0^\perp}H = 2|\psi\rangle\langle\psi| - I$$

- Proof

$$\begin{aligned} 2|\psi\rangle\langle\psi| - I &= 2H|00\ldots0\rangle\langle00\ldots0|H^\dagger - HH^\dagger \\ &= 2H|00\ldots0\rangle\langle00\ldots0|H - HIH \\ &= H\left(2|00\ldots0\rangle\langle00\ldots0| - I\right)H \\ &= HU_{0^\perp}H \end{aligned}$$

H is Unitary

$$U_{0^\perp} = 2|0\rangle\langle0| - I$$

□

- Therefore, *G* can be written as

$$G = \left(HU_{0^\perp}H\right)U_f = \left(2|\psi\rangle\langle\psi| - I\right)U_f$$

Grover's Quantum Search Algorithm

- Let's denote by $U_{\psi^\perp}$ the operator

$$U_{\psi^\perp} = HU_{0^\perp}H = 2|\psi\rangle\langle\psi| - I$$

- In the following we will show that $U_{\psi^\perp}$ applied to a general state $|\phi\rangle = \sum_k \alpha_k |k\rangle$ produces

$$U_{\psi^\perp}|\phi\rangle = U_{\psi^\perp}\left(\sum_k \alpha_k |k\rangle\right) = \sum_k (-\alpha_k + 2\mu)|k\rangle, \qquad [1]$$

where $\mu = \sum_k \alpha_k / N$ is the mean value of the amplitudes α_k

- For this reason, $U_{\psi^\perp}$ is sometimes referred to as the *inversion about the mean operation*

Grover's Quantum Search Algorithm

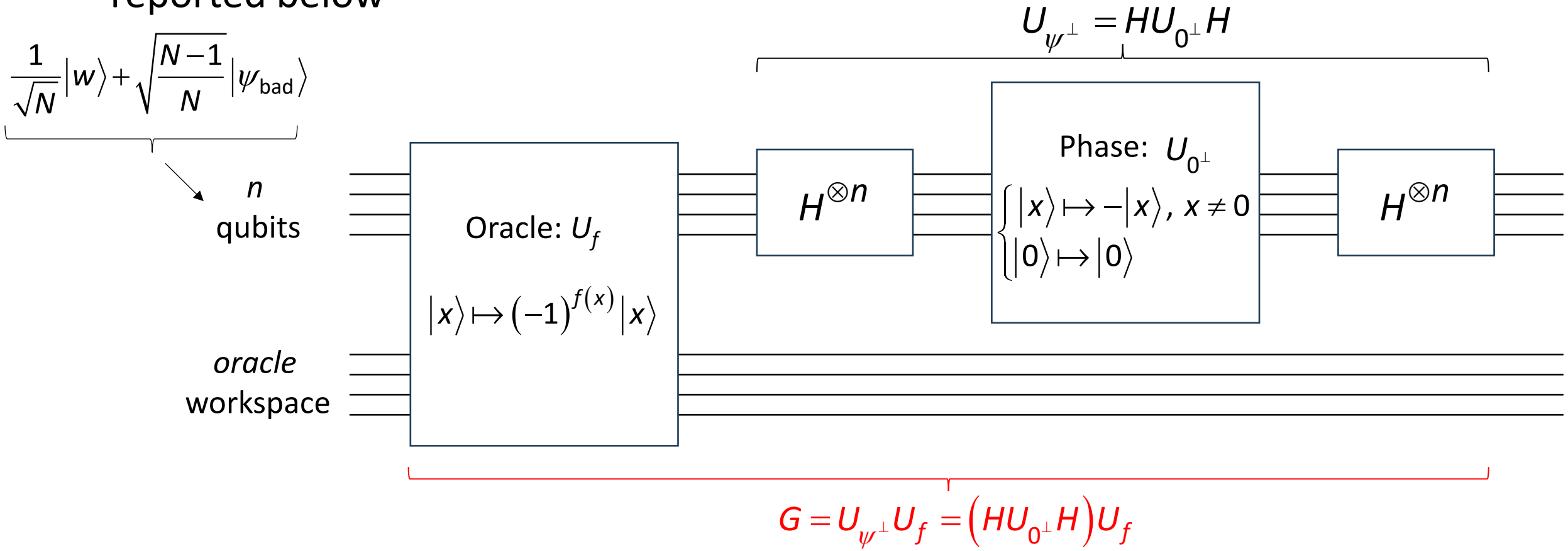
- The Grover iteration *G* is **defined** by the following sequence of transformations....

THE GROVER ITERATION

1) Apply the oracle U_f
2) Apply the Hadamard transform $H^{\otimes n}$
3) Apply $U_{0^\perp}$
4) Apply the Hadamard transform $H^{\otimes n}$

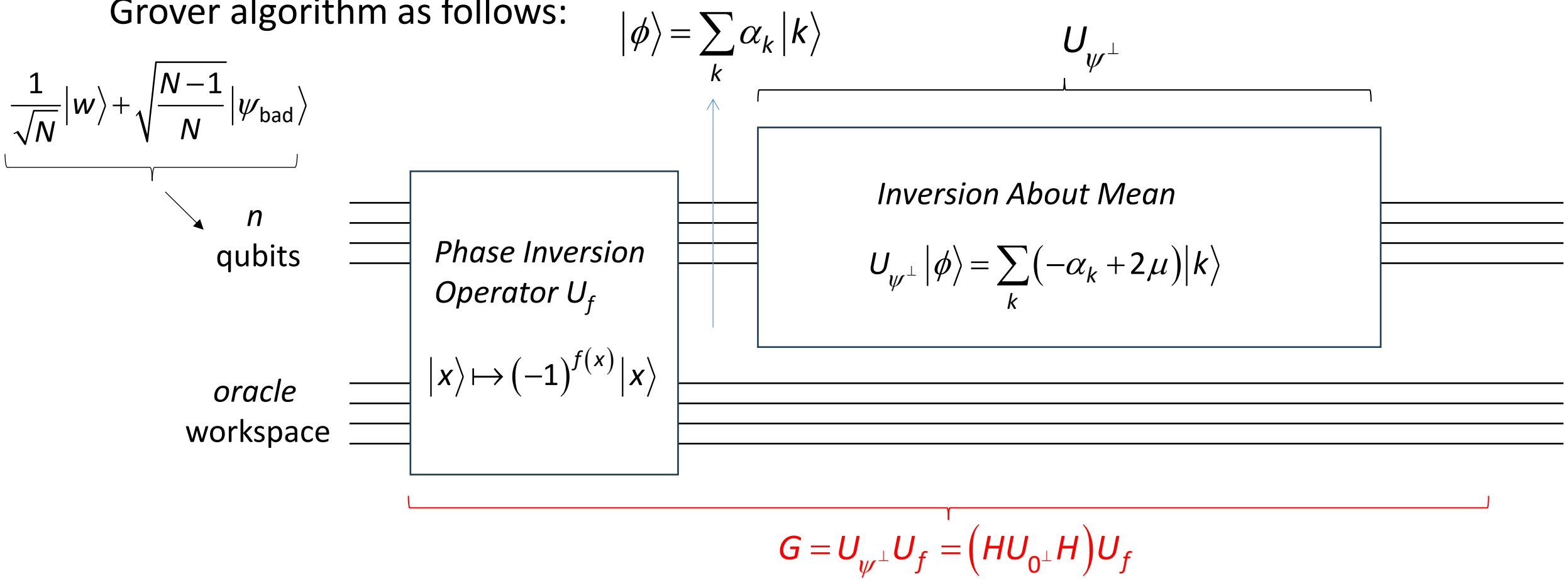
Grover's Quantum Search Algorithm

....while the circuit that implements the Grover iteration, $G = HU_{0^\perp}HU_f$, is reported below



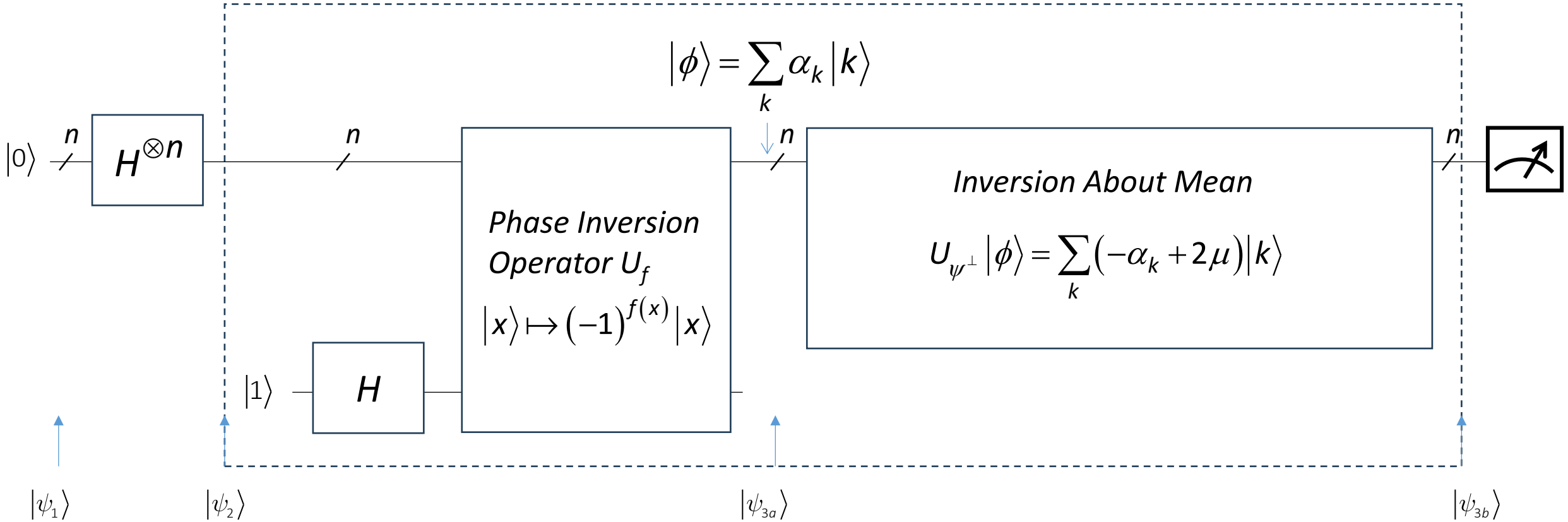
Grover's Quantum Search Algorithm

Since $U_{\psi^\perp}$ performs the inversion about the mean operation we can also represent the Grover algorithm as follows:



Example

Let us look at an example of an execution of this algorithm



Example

- Let *f* be a function that picks out the string “101”
- The states after each step will be

$$|\psi_1\rangle = \begin{bmatrix} \underset{0}{000} & \underset{0}{001} & \underset{0}{010} & \underset{0}{011} & \underset{0}{100} & \underset{0}{101} & \underset{0}{110} & \underset{0}{111} \end{bmatrix}^T$$

$$|\psi_2\rangle = \begin{bmatrix} \underset{\frac{1}{\sqrt{8}}}{000}, & \underset{\frac{1}{\sqrt{8}}}{001}, & \underset{\frac{1}{\sqrt{8}}}{010}, & \underset{\frac{1}{\sqrt{8}}}{011}, & \underset{\frac{1}{\sqrt{8}}}{100}, & \underset{\frac{1}{\sqrt{8}}}{101}, & \underset{\frac{1}{\sqrt{8}}}{110}, & \underset{\frac{1}{\sqrt{8}}}{111} \end{bmatrix}^T$$

Example

- The output from the phase inversion process is

$$|\psi_{3a}\rangle = \begin{matrix} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \end{matrix}$$
$$\left[\frac{1}{\sqrt{8}}, \quad \frac{1}{\sqrt{8}}, \quad \frac{1}{\sqrt{8}}, \quad \frac{1}{\sqrt{8}}, \quad \frac{1}{\sqrt{8}}, \quad -\frac{1}{\sqrt{8}}, \quad \frac{1}{\sqrt{8}}, \quad \frac{1}{\sqrt{8}}\right]^T$$

Example

- The average of these amplitudes is

$$\mu = \frac{7\times\frac{1}{\sqrt{8}} - \frac{1}{\sqrt{8}}}{8} = \frac{6\times\frac{1}{\sqrt{8}}}{8} = \frac{3}{4\sqrt{8}}$$

- Calculating the inversion about the mean we obtain

$$-\alpha_k + 2\mu = -\frac{1}{\sqrt{8}} + \left(2\times\frac{3}{4\sqrt{8}}\right) = \frac{1}{2\sqrt{8}}, \quad k = \{0,1,2,3,4,6,7\}$$

$$-\alpha_5 + 2\mu = \frac{1}{\sqrt{8}} + \left(2\times\frac{3}{4\sqrt{8}}\right) = \frac{5}{2\sqrt{8}}$$

Example

- Thus, we have

$$|\psi_{3b}\rangle = \left[\underset{000}{\frac{1}{2\sqrt{8}}}, \underset{001}{\frac{1}{2\sqrt{8}}}, \underset{010}{\frac{1}{2\sqrt{8}}}, \underset{011}{\frac{1}{2\sqrt{8}}}, \underset{100}{\frac{1}{2\sqrt{8}}}, \underset{101}{\frac{5}{2\sqrt{8}}}, \underset{110}{\frac{1}{2\sqrt{8}}}, \underset{111}{\frac{1}{2\sqrt{8}}} \right]^T$$

- A phase inversion will give us

$$|\psi_{3a}\rangle = \left[\underset{000}{\frac{1}{2\sqrt{8}}}, \underset{001}{\frac{1}{2\sqrt{8}}}, \underset{010}{\frac{1}{2\sqrt{8}}}, \underset{011}{\frac{1}{2\sqrt{8}}}, \underset{100}{\frac{1}{2\sqrt{8}}}, \underset{101}{-\frac{5}{2\sqrt{8}}}, \underset{110}{\frac{1}{2\sqrt{8}}}, \underset{111}{\frac{1}{2\sqrt{8}}} \right]^T$$

Example

- The average of the new amplitudes is

$$\mu = \frac{7\times\frac{1}{2\sqrt{8}} - \frac{5}{2\sqrt{8}}}{8} = \frac{6\times\frac{1}{\sqrt{8}}}{8} = \frac{1}{8\sqrt{8}}$$

- Calculating the inversion about the mean we have

$$-\alpha_k + 2\mu = -\frac{1}{2\sqrt{8}} + \left(2\times\frac{1}{8\sqrt{8}}\right) = -\frac{1}{4\sqrt{8}}, \quad k = \{0,1,2,3,4,6,7\}$$

$$-\alpha_5 + 2\mu = \frac{5}{2\sqrt{8}} + \left(2\times\frac{1}{8\sqrt{8}}\right) = \frac{11}{4\sqrt{8}}$$

Example

- Hence, we have

$$|\psi_{3b}\rangle = \begin{bmatrix} \overset{000}{-\frac{1}{4\sqrt{8}}}, & \overset{001}{-\frac{1}{4\sqrt{8}}}, & \overset{010}{-\frac{1}{4\sqrt{8}}}, & \overset{011}{-\frac{1}{4\sqrt{8}}}, & \overset{100}{-\frac{1}{4\sqrt{8}}}, & \overset{101}{\frac{11}{4\sqrt{8}}}, & \overset{110}{-\frac{1}{4\sqrt{8}}}, & \overset{111}{-\frac{1}{4\sqrt{8}}} \end{bmatrix}^T$$

- For the record,

$$\frac{11}{4\sqrt{8}} = 0.97227 \text{ and } -\frac{1}{4\sqrt{8}} = -0.08839$$

- Squaring the numbers gives us the probability of measuring those numbers

Example

- When we measure the state after $\left\lfloor \pi/4 \sqrt{2^3} \right\rfloor = 2$ iterations of the *G* operator, we will most likely get the state

$$|\psi_4\rangle = \begin{bmatrix} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}^T$$

which is exactly what we wanted

Grover's Quantum Search Algorithm

- We can see that roughly $\sqrt{N}/2$ iterations of the Grover iteration should boost the amplitude of $|w\rangle$ to be close to 1
- The following is a precise analysis
- First note that we can write

$$|\psi\rangle = H|00\ldots0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|\psi_{\text{bad}}\rangle \qquad [20]$$

- It is important to observe that starting in the state $|\psi\rangle$ and repeatedly applying U_f and $U_{\psi^\perp}$ leaves the state of the system in the subspace spanned by $|w\rangle$ and $|\psi_{\text{bad}}\rangle$ that is, a 2-dimensional subspace of the $N = 2^n$-dimensional state space

Grover's Quantum Search Algorithm

- To analyze Grover's algorithm, it helps to define two bases for this 2-dimensional subspace:

$$\left\{|w\rangle, |\psi_{\text{bad}}\rangle\right\} \quad \text{and} \quad \left\{|\psi\rangle, |\bar{\psi}\rangle\right\} \qquad [21]$$

where we define the state $|\bar{\psi}\rangle$ orthogonal to $|\psi\rangle$

$$|\bar{\psi}\rangle = \sqrt{\frac{N-1}{N}}|w\rangle - \frac{1}{\sqrt{N}}|\psi_{\text{bad}}\rangle \qquad [22]$$

- Define θ so that

$$\sin\theta = \frac{1}{\sqrt{N}} \quad \rightarrow \quad \cos\theta = \sqrt{\frac{N-1}{N}} \qquad [23]$$

Grover's Quantum Search Algorithm

- Putting [23] in [22] and [20] we obtain

$$\begin{aligned} |\psi\rangle &= \sin\theta\,|w\rangle + \cos\theta\,|\psi_{\text{bad}}\rangle \\ |\bar{\psi}\rangle &= \cos\theta\,|w\rangle - \sin\theta\,|\psi_{\text{bad}}\rangle \end{aligned} \qquad [24]$$

from where

$$\begin{aligned} |w\rangle &= \sin\theta\,|\psi\rangle + \cos\theta\,|\bar{\psi}\rangle \\ |\psi_{\text{bad}}\rangle &= \cos\theta\,|\psi\rangle - \sin\theta\,|\bar{\psi}\rangle \end{aligned} \qquad [25]$$

Note that

$\{|w\rangle, |\psi_{\text{bad}}\rangle\}$ and $\{|\psi\rangle, |\bar{\psi}\rangle\}$

are orthonormal bases for the same 2-dimensional subspace

- Thus, we can easily convert between the two bases

Grover's Quantum Search Algorithm

- The quantum searching algorithm starts in the state

$$|\psi\rangle = \sin\theta|w\rangle + \cos\theta|\psi_{\text{bad}}\rangle$$

- The operator U_f gives the state

$$U_f|w\rangle = -|w\rangle$$

$$U_f|\psi_{\text{bad}}\rangle = |\psi_{\text{bad}}\rangle$$

$$U_f|\psi\rangle = -\sin\theta|w\rangle + \cos\theta|\psi_{\text{bad}}\rangle = \cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle \quad [26]$$

[25]

$$|w\rangle = \sin\theta|\psi\rangle + \cos\theta|\bar{\psi}\rangle$$

$$|\psi_{\text{bad}}\rangle = \cos\theta|\psi\rangle - \sin\theta|\bar{\psi}\rangle$$

Grover's Quantum Search Algorithm

$$U_f|\psi\rangle = -\sin\theta|w\rangle + \cos\theta|\psi_{\text{bad}}\rangle = \cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle$$

- Then the inversion about the mean, $U_{\psi^\perp}$, gives the state

$$U_{\psi^\perp}U_f|\psi\rangle = \cos 2\theta|\psi\rangle + \sin 2\theta|\bar{\psi}\rangle = \sin 3\theta|w\rangle + \cos 3\theta|\psi_{\text{bad}}\rangle \quad [27]$$

Proof

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right) = U_{\psi^\perp}\left(-\sin\theta|w\rangle + \cos\theta|\psi_{\text{bad}}\rangle\right) = U_{\psi^\perp}\left(\cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle\right) \quad [28]$$

Let's start developing the second equality

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right) = U_{\psi^\perp}\left(\cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle\right) = (\cos 2\theta)U_{\psi^\perp}|\psi\rangle - (\sin 2\theta)U_{\psi^\perp}|\bar{\psi}\rangle \quad [29]$$

Since $U_{\psi^\perp} = 2|\psi\rangle\langle\psi| - I \rightarrow$

$$U_{\psi^\perp}|\psi\rangle = 2|\psi\rangle\langle\psi|\psi\rangle - I|\psi\rangle = 2|\psi\rangle - |\psi\rangle = |\psi\rangle$$

$$U_{\psi^\perp}|\bar{\psi}\rangle = 2|\psi\rangle\langle\psi|\bar{\psi}\rangle - I|\bar{\psi}\rangle = -I|\bar{\psi}\rangle = -|\bar{\psi}\rangle$$

Grover's Quantum Search Algorithm

$$U_f|\psi\rangle = -\sin\theta|w\rangle + \cos\theta|\psi_{\text{bad}}\rangle = \cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle$$

- Thus

$$U_{\psi^\perp}|\psi\rangle = |\psi\rangle$$
$$U_{\psi^\perp}|\bar{\psi}\rangle = -|\bar{\psi}\rangle \qquad [30]$$

- Putting [30] into [29]

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right) = \cos 2\theta|\psi\rangle + \sin 2\theta|\bar{\psi}\rangle \qquad [31]$$

- Putting [24] into [28] we obtain the [27] □

- Since $G = U_{\psi^\perp}U_f$, then the [27] can be rewritten

$$G|\psi\rangle = \cos 2\theta|\psi\rangle + \sin 2\theta|\bar{\psi}\rangle = \sin 3\theta|w\rangle + \cos 3\theta|\psi_{\text{bad}}\rangle$$

Quantum Amplitude Estimation and Quantum Counting

$G|\psi\rangle = \sin 3\theta |w\rangle + \cos 3\theta |\psi_{\text{bad}}\rangle$

- Thus, the effect of *G* is to rotate the initial state

$$|\psi\rangle = \sin\theta |w\rangle + \cos\theta |\psi_{\text{bad}}\rangle$$

through an angle of 2θ in the space spanned by $\{|\psi_{\text{good}}\rangle, |\psi_{\text{bad}}\rangle\}$

- Hence, in the $\{|\psi_{\text{good}}\rangle, |\psi_{\text{bad}}\rangle\}$ basis, G takes the

$$G = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix}$$

where

$$\sin\theta = \frac{1}{\sqrt{N}} \quad \rightarrow \quad \cos\theta = \sqrt{\frac{N-1}{N}}$$

Quantum Amplitude Estimation and Quantum Counting

- When G is so defined, we have

$$G|\psi\rangle = G\left(\sin\theta|w\rangle + \cos\theta|\psi_{\text{bad}}\rangle\right)$$

$$= \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix} \begin{bmatrix} \sin\theta \\ \cos\theta \end{bmatrix} = \begin{bmatrix} \cos 2\theta \sin\theta + \sin 2\theta \cos\theta \\ -\sin 2\theta \sin\theta + \cos 2\theta \cos\theta \end{bmatrix}$$

$$= \begin{bmatrix} \sin 3\theta \\ \cos 3\theta \end{bmatrix} = \sin 3\theta|w\rangle + \cos 3\theta|\psi_{\text{bad}}\rangle$$

- Hence, in the $\left\{|\psi_{\text{good}}\rangle, |\psi_{\text{bad}}\rangle\right\}$ basis, we obtain the [27]

Grover's Quantum Search Algorithm

- It is easy to verify by induction that after *k* iterations of the Grover iterate starting with state

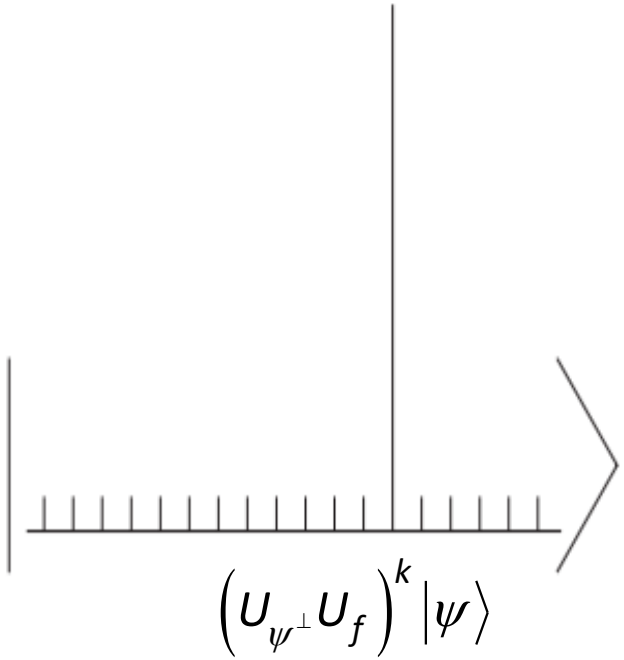
$$\left|\psi\right\rangle = H\left|00\ldots0\right\rangle$$

we are left with the

$$G^k\left|\psi\right\rangle \equiv \left(U_{\psi^\perp}U_f\right)^k\left|\psi\right\rangle = \cos\left(2k\theta\right)\left|\psi\right\rangle + \sin\left(2k\theta\right)\left|\bar{\psi}\right\rangle$$
$$= \sin\left(\left(2k+1\right)\theta\right)\left|w\right\rangle + \cos\left(\left(2k+1\right)\theta\right)\left|\psi_{\text{bad}}\right\rangle$$

as illustrated in the following slide

Grover’s Quantum Search Algorithm



Grover's Quantum Search Algorithm

- To have a high probability of obtaining $|w\rangle$, we wish to select *k* so that

$$\sin\left(\left(2k+1\right)\theta\right)\approx 1$$

which means that we would like

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

and thus

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

Notation

- Hereafter, we will adopt the notation $\left|\psi_{\text{good}}\right\rangle$ for $\left|w\right\rangle$, which means that the following equivalence holds:

$$\left|\psi_{\text{good}}\right\rangle \equiv \left|w\right\rangle$$

Amplitude Amplification

- Grover's search algorithm can be generalized substantially to apply to any algorithm *A* for 'guessing' a solution
- In the previous section we had $A = H^{\otimes n}$ which guessed the solution by setting up a uniform superposition of all possible solutions
- More generally, consider any algorithm *A* that starts with the generic input state $|00....0\rangle$, which can include additional workspace, and maps to some superposition of guesses

$$|\psi\rangle = \sum_x \alpha_x |x\rangle |\text{junk}(x)\rangle$$

which might have some 'junk' information left in the workspace qubits

Amplitude Amplification

$$|\psi\rangle \equiv A|00\ldots0\rangle = \sum_x \alpha_x |x\rangle|\text{junk}(x)\rangle.$$

Note that we can naturally split $|\psi\rangle$ into two parts:

$$|\psi\rangle = \sum_{x \in X_{\text{good}}} \alpha_x |x\rangle|\text{junk}(x)\rangle + \sum_{x \in X_{\text{bad}}} \alpha_x |x\rangle|\text{junk}(x)\rangle.$$

Note that

$$p_{\text{good}} = \sum_{x \in X_{\text{good}}} |\alpha_x|^2$$

is the probability of measuring a good state x, and

$$p_{\text{bad}} = \sum_{x \in X_{\text{bad}}} |\alpha_x|^2 = 1 - p_{\text{good}}$$

is the probability of measuring a bad state x.

Amplitude Amplification

If $p_{\text{good}} = 1$, no amplification is necessary, and if $p_{\text{good}} = 0$, amplification will not help since there is no good amplitude to amplify. In the interesting cases that $0 < p_{\text{good}} < 1$, we can renormalize the good and the bad components into

$$|\psi_{\text{good}}\rangle = \sum_{x \in X_{\text{good}}} \frac{\alpha_x}{\sqrt{p_{\text{good}}}} |x\rangle |\text{junk}(x)\rangle$$

and

$$|\psi_{\text{bad}}\rangle = \sum_{x \in X_{\text{bad}}} \frac{\alpha_x}{\sqrt{p_{\text{bad}}}} |x\rangle |\text{junk}(x)\rangle.$$

Amplitude Amplification

We can then write

$$|\psi\rangle = \sqrt{p_{\text{good}}}|\psi_{\text{good}}\rangle + \sqrt{p_{\text{bad}}}|\psi_{\text{bad}}\rangle$$

or

$$|\psi\rangle = \sin(\theta)|\psi_{\text{good}}\rangle + \cos(\theta)|\psi_{\text{bad}}\rangle$$

where $\theta \in \left(0, \frac{\pi}{2}\right)$ satisfies $\sin^2(\theta) = p_{\text{good}}$.

We define a more general search iterate to be $Q = AU_0^{\perp}A^{-1}U_f$, which one can easily verify to be equivalent to $U_{\psi}^{\perp}U_f$, where as before we define $U_{\psi}^{\perp}|\psi\rangle = |\psi\rangle$ and $U_{\psi}^{\perp}|\phi\rangle = -|\phi\rangle$ for all states $|\phi\rangle$ that are orthogonal to $|\psi\rangle$.

Geometric Interpretation of the Grover's Algorithm

- Since

$$|\psi\rangle = H|00\ldots0\rangle \equiv H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle, \text{ where } N = 2^n,$$

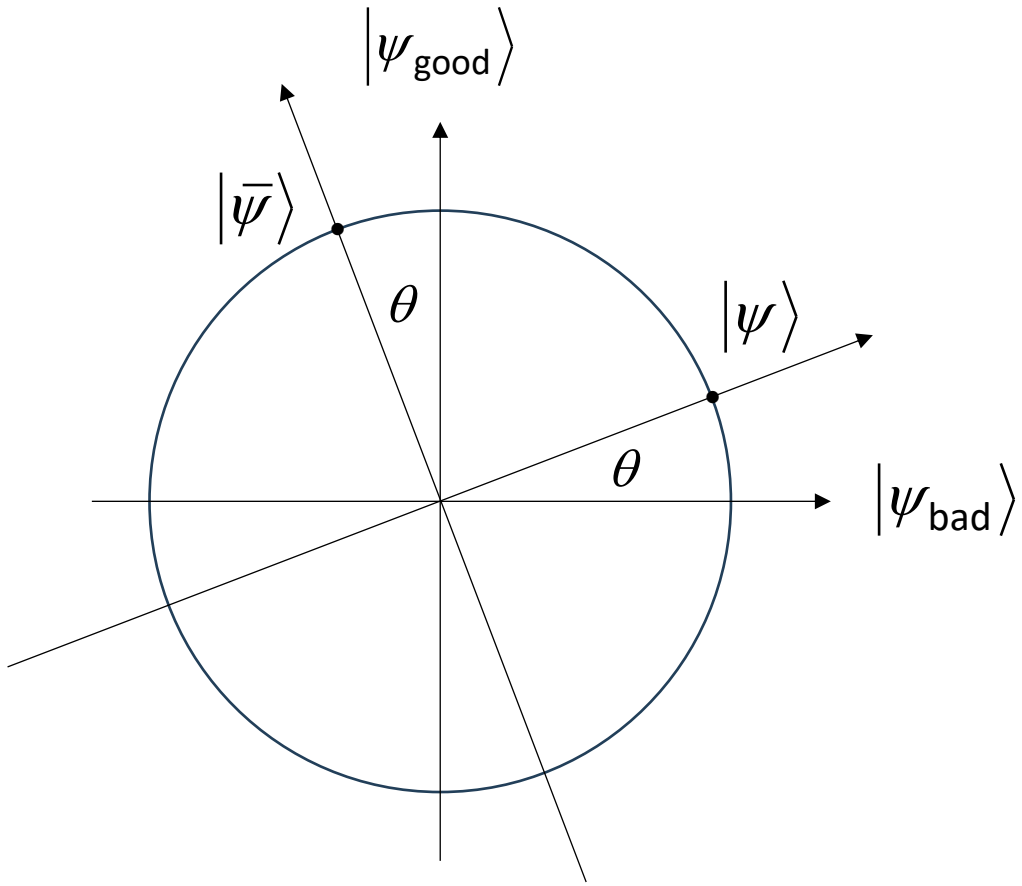
  or more generally

$$|\psi\rangle = A|00\ldots0\rangle = \sum_x \alpha_x |x\rangle|\text{junk}(x)\rangle$$

  have only real amplitudes, and the Grover iteration does not introduce any complex phases, then the amplitudes always remain real

- This allows us to represent the Grover's algorithm, as done in the next Figures

Geometric Interpretation of the Grover's Algorithm



$$|\psi\rangle = \sin\theta|\psi_{good}\rangle + \cos\theta|\psi_{bad}\rangle$$
$$|\bar{\psi}\rangle = \cos\theta|\psi_{good}\rangle - \sin\theta|\psi_{bad}\rangle$$

[25]

$$|\psi_{good}\rangle = \sin\theta|\psi\rangle + \cos\theta|\bar{\psi}\rangle$$
$$|\psi_{bad}\rangle = \cos\theta|\psi\rangle - \sin\theta|\bar{\psi}\rangle$$

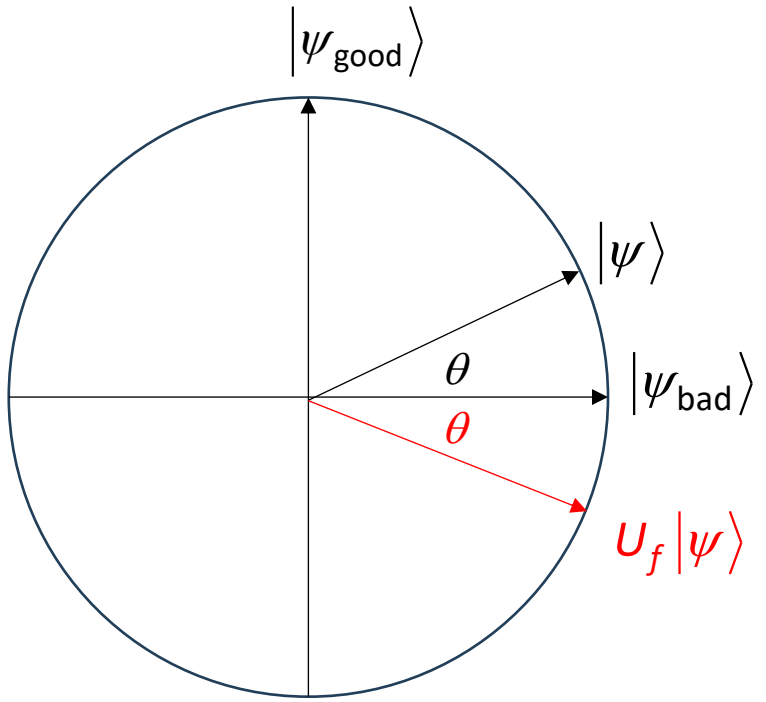
Geometric Interpretation of the Grover's Algorithm

- Note that U_f will map

$$|\psi\rangle = \sin\theta|\psi_{\text{good}}\rangle + \cos\theta|\psi_{\text{bad}}\rangle \xrightarrow{U_f} U_f|\psi\rangle = -\sin\theta|\psi_{\text{good}}\rangle + \cos\theta|\psi_{\text{bad}}\rangle \qquad [26]$$

as illustrated in the Figure

$$U_f|\psi_{\text{good}}\rangle = -|\psi_{\text{good}}\rangle$$
$$U_f|\psi_{\text{bad}}\rangle = |\psi_{\text{bad}}\rangle$$



Geometric Interpretation of the Grover's Algorithm

$$U_f|\psi\rangle = -\sin\theta|\psi_{\text{good}}\rangle + \cos\theta|\psi_{\text{bad}}\rangle$$

- The action of $U_{\psi^\perp}$ is most easily seen in the basis $\{|\psi\rangle, |\bar{\psi}\rangle\}$

- Substituting [25] into [26] produces

$$\begin{aligned} U_f|\psi\rangle &= -\sin\theta\left(\sin\theta|\psi\rangle + \cos\theta|\bar{\psi}\rangle\right) + \cos\theta\left(\cos\theta|\psi\rangle - \sin\theta|\bar{\psi}\rangle\right) \\ &= -\sin^2\theta|\psi\rangle - \sin\theta\cos\theta|\bar{\psi}\rangle + \cos^2\theta|\psi\rangle - \cos\theta\sin\theta|\bar{\psi}\rangle \\ &= \underbrace{\cos^2\theta - \sin^2\theta}_{\cos 2\theta}|\psi\rangle - \underbrace{2\sin\theta\cos\theta}_{\sin 2\theta}|\bar{\psi}\rangle \end{aligned}$$

- Thus

$$U_f|\psi\rangle = \cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle \qquad [27]$$

$$|\psi_{\text{good}}\rangle = \sin\theta|\psi\rangle + \cos\theta|\bar{\psi}\rangle$$
$$|\psi_{\text{bad}}\rangle = \cos\theta|\psi\rangle - \sin\theta|\bar{\psi}\rangle$$

Geometric Interpretation of the Grover's Algorithm

- Therefore

$$U_f|\psi\rangle = -\sin\theta|\psi_{\text{good}}\rangle + \cos\theta|\psi_{\text{bad}}\rangle$$
$$= \cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle$$

[27]

Geometric Interpretation of the Grover's Algorithm

- Now, by applying $U_{\psi^\perp}$ to [27] we get

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right)=\cos 2\theta\left(U_{\psi^\perp}|\psi\rangle\right)-\sin 2\theta\left(U_{\psi^\perp}|\bar{\psi}\rangle\right) \qquad [28]$$

- Let's now calculate separately $U_{\psi^\perp}|\psi\rangle$ and $U_{\psi^\perp}|\bar{\psi}\rangle$, where $U_{\psi^\perp}=2|\psi\rangle\langle\psi|-I$

$$U_{\psi^\perp}|\psi\rangle=\left(2|\psi\rangle\langle\psi|-I\right)|\psi\rangle=2|\psi\rangle\underbrace{\langle\psi|\psi\rangle}_{=1}-|\psi\rangle=|\psi\rangle \qquad [29]$$

$$U_{\psi^\perp}|\bar{\psi}\rangle=\left(2|\psi\rangle\langle\psi|-I\right)|\bar{\psi}\rangle=2|\psi\rangle\underbrace{\langle\psi|\bar{\psi}\rangle}_{=0}-|\bar{\psi}\rangle=-|\bar{\psi}\rangle \qquad [30]$$

Geometric Interpretation of the Grover's Algorithm

- By substituting [29] and [30] into [28] we get:

$$U_{\psi^{\perp}}\left(U_f\left|\psi\right\rangle\right) = \cos 2\theta \left|\psi\right\rangle + \sin 2\theta \left|\bar{\psi}\right\rangle \qquad [31]$$

Geometric Interpretation of the Grover's Algorithm

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right)=\cos 2\theta|\psi\rangle+\sin 2\theta|\bar{\psi}\rangle$$

- Now, by substituting [24] into [31] we get

$$\begin{aligned}U_{\psi^\perp}\left(U_f|\psi\rangle\right)&=\cos 2\theta\left(\sin\theta|\psi_{\text{good}}\rangle+\cos\theta|\psi_{\text{bad}}\rangle\right)+\sin 2\theta\left(\cos\theta|\psi_{\text{good}}\rangle-\sin\theta|\psi_{\text{bad}}\rangle\right)\\&=\underbrace{\left(\cos 2\theta\sin\theta+\sin 2\theta\cos\theta\right)}_{\sin 3\theta}|\psi_{\text{good}}\rangle+\underbrace{\left(\cos 2\theta\cos\theta-\sin 2\theta\sin\theta\right)}_{\cos 3\theta}|\psi_{\text{bad}}\rangle\\&=\sin 3\theta|\psi_{\text{good}}\rangle+\cos 3\theta|\psi_{\text{bad}}\rangle\end{aligned}$$

- Thus

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right)=\sin 3\theta|\psi_{\text{good}}\rangle+\cos 3\theta|\psi_{\text{bad}}\rangle$$

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right)=\cos 2\theta|\psi\rangle+\sin 2\theta|\bar{\psi}\rangle$$

Geometric Interpretation of the Grover's Algorithm

$$U_{\psi^\perp}\left(U_f|\psi\rangle\right)=\cos 2\theta|\psi\rangle+\sin 2\theta|\bar{\psi}\rangle$$

- Since:

$$G=U_{\psi^\perp}U_f$$

the above calculation boils down to

$G\|\psi\rangle=\cos 2\theta\|\psi\rangle+\sin 2\theta\|\bar{\psi}\rangle$	along the basis $\{\|\psi\rangle,\|\bar{\psi}\rangle\}$
$G\|\psi\rangle=\sin 3\theta\|\psi_{\text{good}}\rangle+\cos 3\theta\|\psi_{\text{bad}}\rangle$	along the basis $\{\|\psi_{\text{good}}\rangle,\|\psi_{\text{bad}}\rangle\}$

[32]

Geometric Interpretation of the Grover's Algorithm

$$U_{\psi^\perp}\left(U_f\left|\psi\right\rangle\right)=\cos 2\theta\left|\psi\right\rangle+\sin 2\theta\left|\bar{\psi}\right\rangle$$

- Likewise, for the orthogonal state $\left|\bar{\psi}\right\rangle$, we have:

$$G\left|\bar{\psi}\right\rangle=U_{\psi^\perp}\left(U_f\left|\bar{\psi}\right\rangle\right)=U_{\psi^\perp}U_f\left(\cos\theta\left|\psi_{\text{good}}\right\rangle-\sin\theta\left|\psi_{\text{bad}}\right\rangle\right)=U_{\psi^\perp}\left(-\cos\theta\left|\psi_{\text{good}}\right\rangle-\sin\theta\left|\psi_{\text{bad}}\right\rangle\right)$$

$$=-\sin 2\theta\left|\psi\right\rangle+\cos 2\theta\left|\bar{\psi}\right\rangle=-\sin 3\theta\left|\psi_{\text{good}}\right\rangle+\cos 3\theta\left|\psi_{\text{bad}}\right\rangle$$

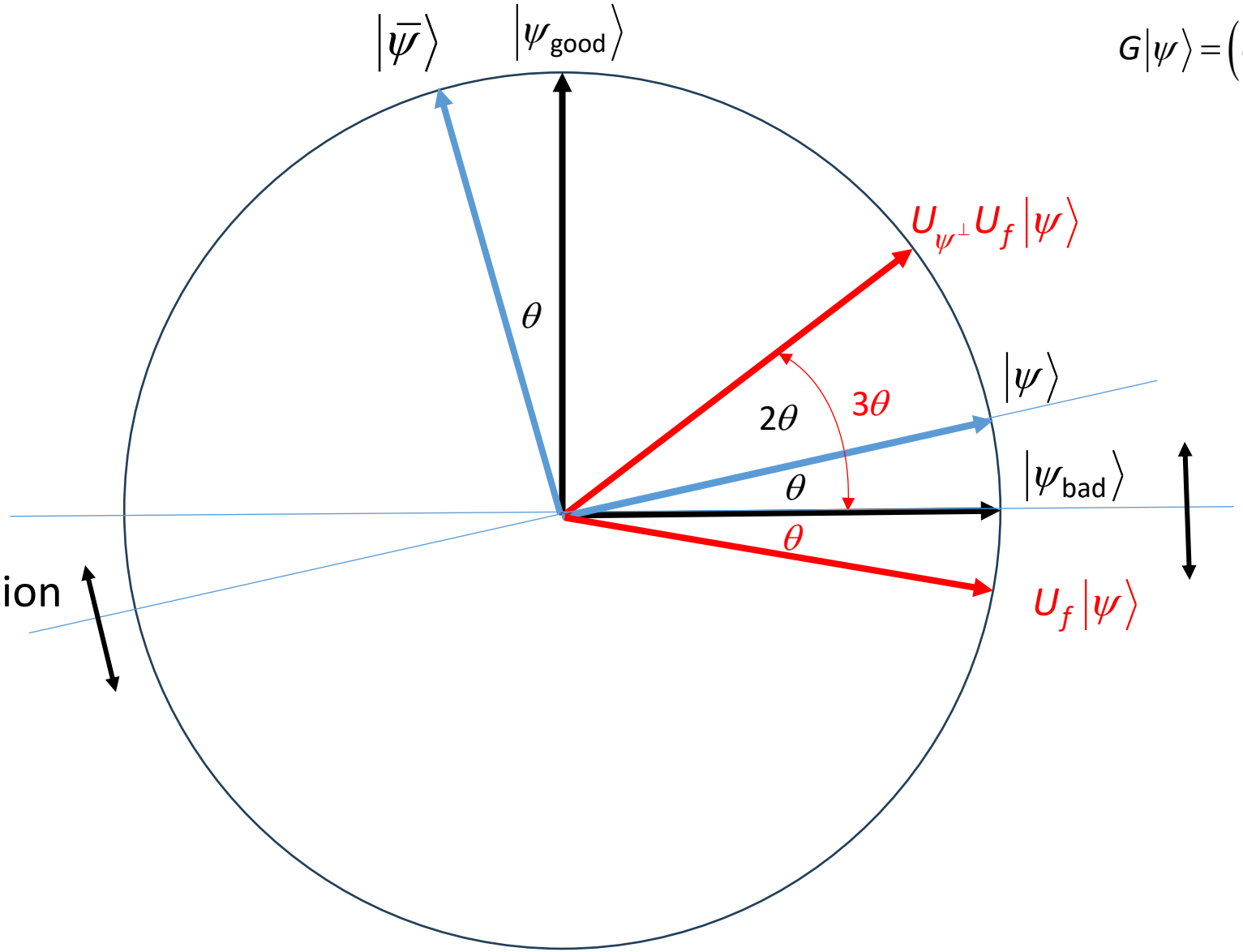
- To sum up, we can conclude that

$G\left\|\bar{\psi}\right\rangle=-\sin 2\theta\left\|\psi\right\rangle+\cos 2\theta\left\|\bar{\psi}\right\rangle$	along the basis $\left\{\left\|\psi\right\rangle,\left\|\bar{\psi}\right\rangle\right\}$
$G\left\|\bar{\psi}\right\rangle=-\sin 3\theta\left\|\psi_{\text{bad}}\right\rangle+\cos 3\theta\left\|\psi_{\text{good}}\right\rangle$	along the basis $\left\{\left\|\psi_{\text{good}}\right\rangle,\left\|\psi_{\text{bad}}\right\rangle\right\}$

[33]

$$G|\psi\rangle = \left(U_{\psi^\perp} U_f\right)|\psi\rangle = \sin 3\theta\,|\psi_{\text{good}}\rangle + \cos 3\theta\,|\psi_{\text{bad}}\rangle$$

$$G|\psi\rangle = \left(U_{\psi^\perp} U_f\right)|\psi\rangle = \cos 2\theta\,|\psi\rangle + \sin 2\theta\,|\bar{\psi}\rangle$$



$U_{\psi^\perp}$ reflection about $|\psi\rangle$

U_f: reflection about $|\psi_{\text{bad}}\rangle$

Geometric Interpretation of the Grover's Algorithm

- Notice that more generally for any real number ϕ, the operation U_f does the following

$$U_f\left(\sin\phi\left|\psi_{\text{good}}\right\rangle+\cos\phi\left|\psi_{\text{bad}}\right\rangle\right)=-\sin\phi\left|\psi_{\text{good}}\right\rangle+\cos\phi\left|\psi_{\text{bad}}\right\rangle$$

  and so U_f performs a **reflection** about the axis defined by the vector $\left|\psi_{\text{bad}}\right\rangle$

- Similarly, the operation $U_{\psi^\perp}$ does the following in general:

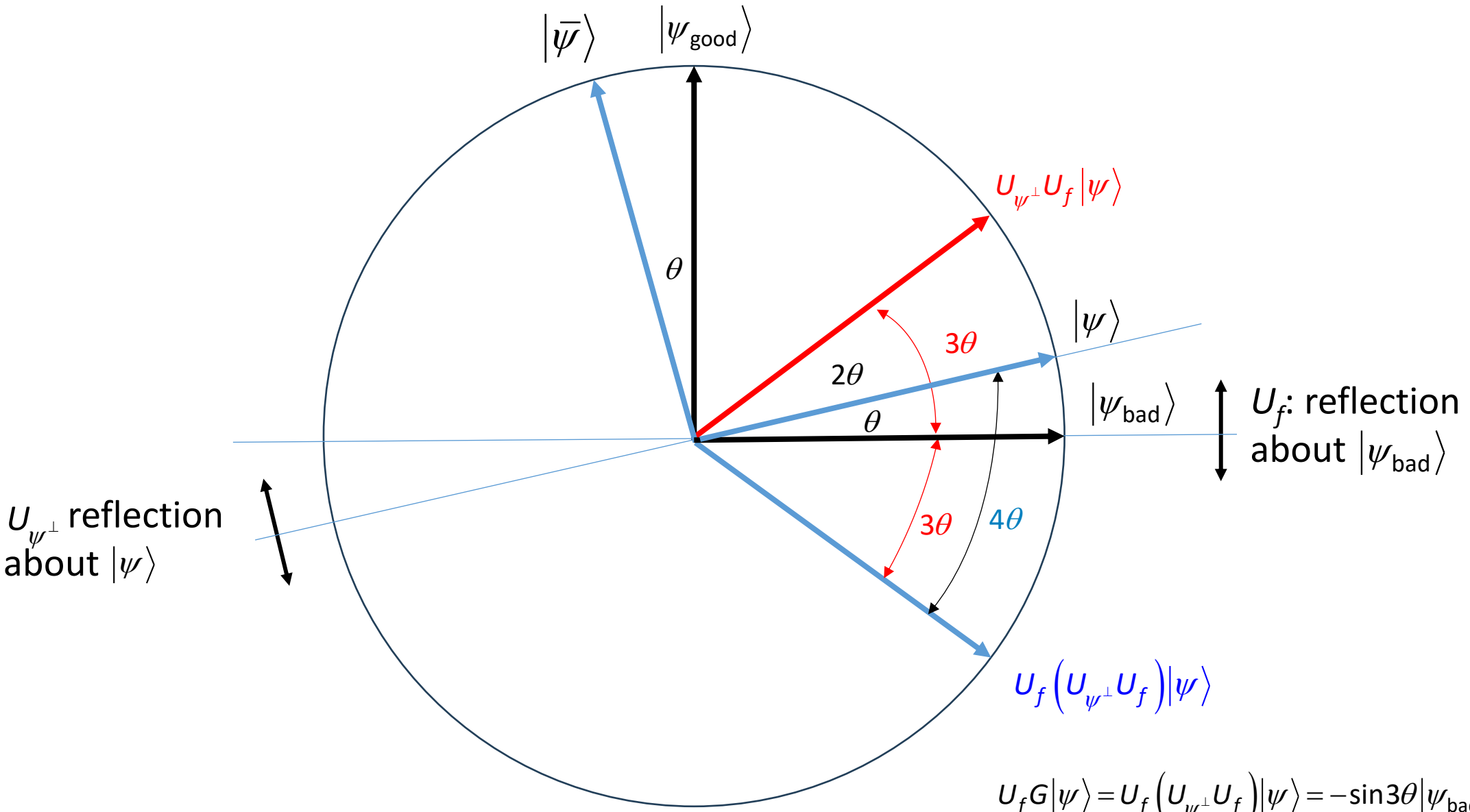
$$U_{\psi^\perp}\left(\sin\phi\left|\psi\right\rangle+\cos\phi\left|\bar{\psi}\right\rangle\right)=\sin\phi\left|\psi\right\rangle-\cos\phi\left|\bar{\psi}\right\rangle$$

  and so $U_{\psi^\perp}$ performs a **reflection** about the axis defined by the vector $\left|\psi\right\rangle$

Geometric Interpretation of the Grover's Algorithm

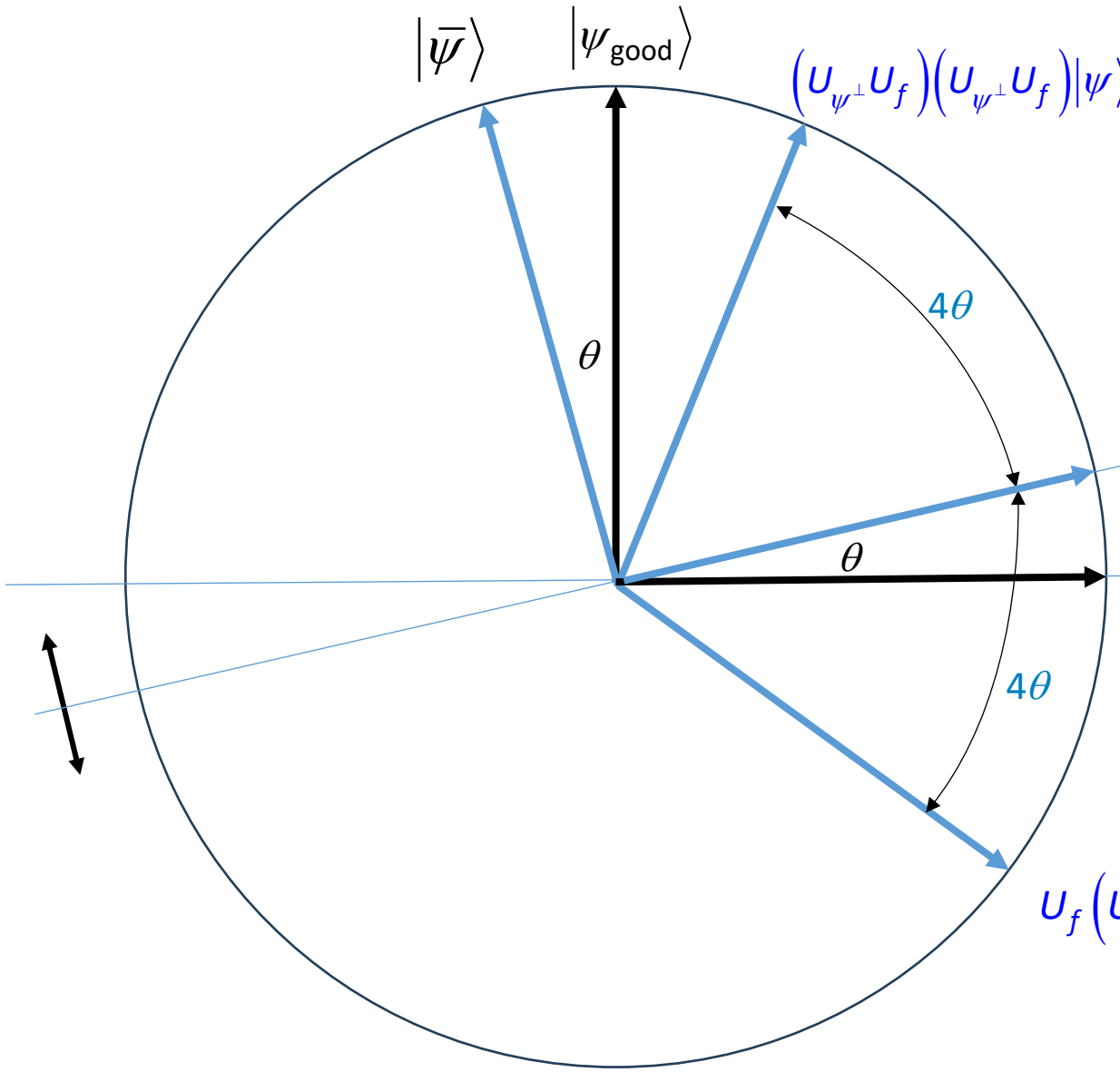
- Two such reflections correspond to a rotation through an angle 2θ in the 2-dimensional subspace $\{|\psi\rangle, |\bar{\psi}\rangle\}$

- Four such reflections correspond to a rotation through an angle 4θ in the 2-dimensional subspace $\{|\psi\rangle, |\bar{\psi}\rangle\}$



$$U_f G|\psi\rangle = U_f\left(U_{\psi^\perp}U_f\right)|\psi\rangle = -\sin 3\theta|\psi_{\text{bad}}\rangle + \cos 3\theta|\psi_{\text{good}}\rangle$$

$$U_f G|\psi\rangle = U_f\left(U_{\psi^\perp}U_f\right)|\psi\rangle = -\sin 4\theta|\psi\rangle + \cos 4\theta|\bar{\psi}\rangle$$



$\left(U_{\psi^\perp}U_f\right)\left(U_{\psi^\perp}U_f\right)|\psi\rangle=\left(U_{\psi^\perp}U_f\right)^2|\psi\rangle$

$\left(U_{\psi^\perp}U_f\right)\left(U_{\psi^\perp}U_f\right)|\psi\rangle=\sin 5\theta|\psi_{\text{good}}\rangle+\cos 5\theta|\psi_{\text{bad}}\rangle$

$\left(U_{\psi^\perp}U_f\right)\left(U_{\psi^\perp}U_f\right)|\psi\rangle=\cos 4\theta|\psi\rangle+\sin 4\theta|\bar{\psi}\rangle$

U_f: reflection about $|\psi_{\text{bad}}\rangle$

$U_{\psi^\perp}$ reflection about $|\psi\rangle$

$U_f\left(U_{\psi^\perp}U_f\right)|\psi\rangle$

$U_f\left(U_{\psi^\perp}U_f\right)|\psi\rangle=-\sin 3\theta|\psi_{\text{bad}}\rangle+\cos 3\theta|\psi_{\text{good}}\rangle$

$U_f\left(U_{\psi^\perp}U_f\right)|\psi\rangle=-\sin 4\theta|\psi\rangle+\cos 4\theta|\bar{\psi}\rangle$

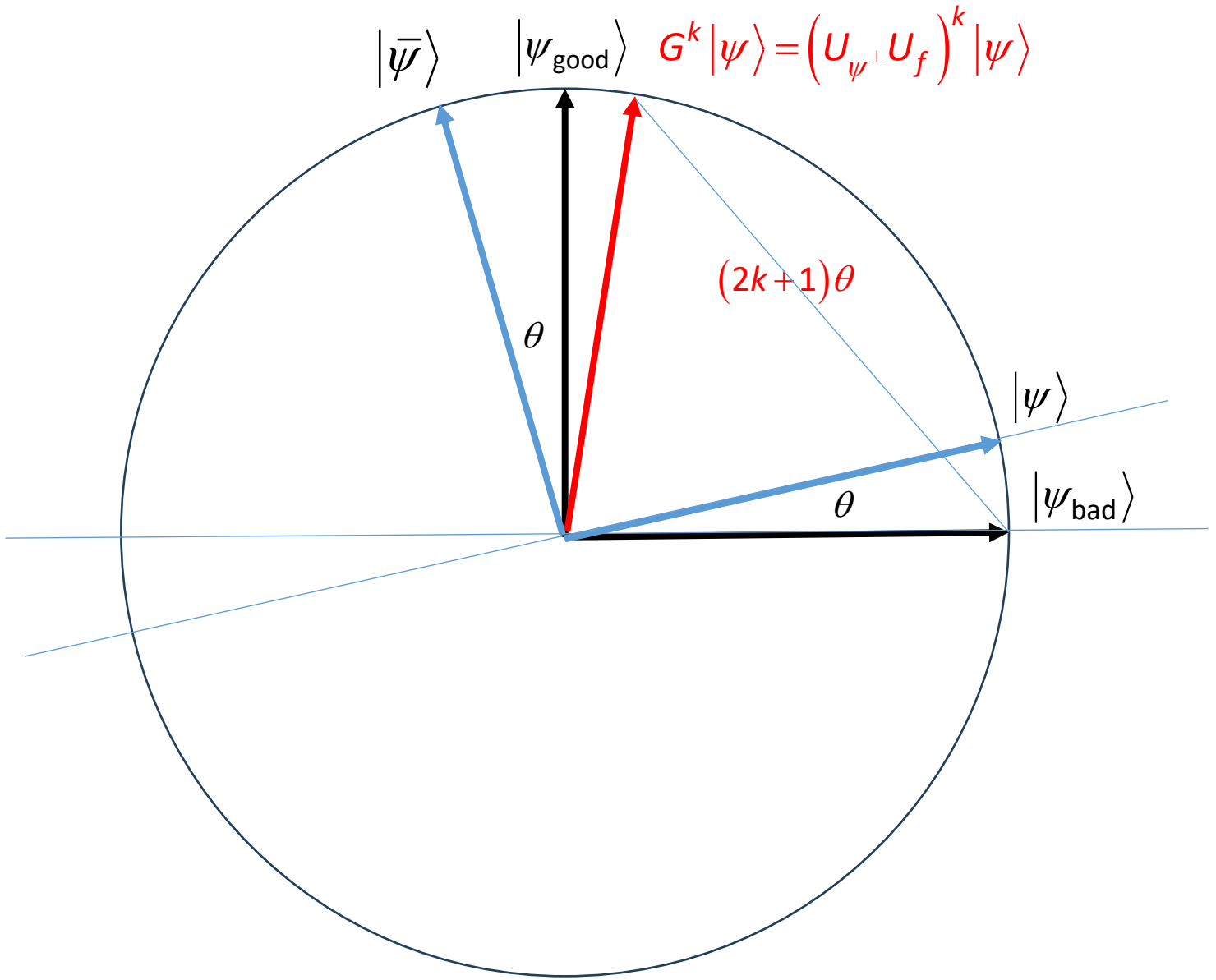
Geometric Interpretation of the Grover's Algorithm

- Thus, repeatedly applying the operation $G = U_{\psi^\perp} U_f$ a total of k times rotates the initial state $|\psi\rangle$ to

$$G^k |\psi\rangle = \cos\big((2k+1)\theta\big)|\psi_{\text{bad}}\rangle + \sin\big((2k+1)\theta\big)|\psi_{\text{good}}\rangle$$

$$G^k |\psi\rangle = \cos(2k\theta)|\psi\rangle + \sin(2k\theta)|\bar{\psi}\rangle$$

  as illustrated in the next slide


$|\bar{\psi}\rangle$
$|\psi_{\text{good}}\rangle$
$G^k|\psi\rangle = \left(U_{\psi^\perp} U_f\right)^k |\psi\rangle$
$(2k+1)\theta$
θ
$|\psi\rangle$
θ
$|\psi_{\text{bad}}\rangle$

Geometric Interpretation of the Grover's Algorithm

- Searching by amplitude amplification works by applying *G* an appropriate number of times until the state is such that a measurement will yield an element of the subspace spanned by $\left|\psi_{\text{good}}\right\rangle$ with high probability

- It remains to analyze how many iterations of *G* are needed
- To get a high probability of measuring a good value, the smallest positive *k* we can choose is such that

$$\left(2k+1\right)\theta = \frac{\pi}{2} \quad \rightarrow \quad k = \frac{\pi}{4\theta} - \frac{1}{2}$$

Geometric Interpretation of the Grover's Algorithm

- Note that for small θ, $\sin\theta \approx \theta$ and if $\sin\theta = \frac{1}{\sqrt{N}} \rightarrow \quad \theta \approx \frac{1}{\sqrt{N}}$

- By substituting this expression for θ into

$$k = \frac{\pi}{4\theta} - \frac{1}{2}$$

we get

$$k \sim \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \sim \frac{\pi}{4}\sqrt{N} \quad \text{for} \quad N \gg 1$$

- Therefore, searching via amplitude amplification uses only $O\left(\sqrt{N}\right)$ queries to *Grover* iteration, which is a *quadratic speedup* over the classical computer's $O(N)$

Geometric Interpretation of the Grover's Algorithm

- Note that for small θ, $\sin\theta \approx \theta$ and since $\sin\theta = \sqrt{p_{\text{good}}}$ searching via amplitude amplification uses only

$$k = \frac{\pi}{4\theta} - \frac{1}{2} = \frac{\pi}{4\sqrt{p_{\text{good}}}} - \frac{1}{2} = O\left(\sqrt{\frac{1}{p_{\text{good}}}}\right)$$

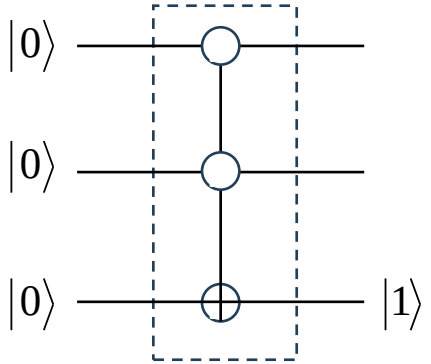
queries to U_f

Geometric Interpretation of the Grover's Algorithm

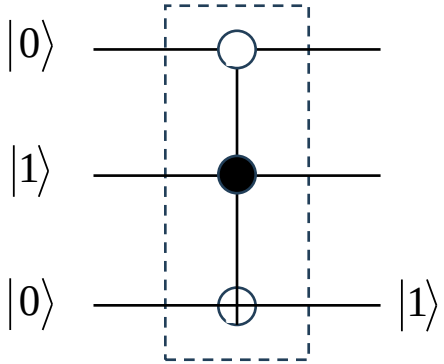
- The angle of the final state may not be exactly $\pi/2$, so the success probability may not be exactly 1
- This is not an issue, however, for a couple of reasons:
  - first, for large *N*, the angle ϑ is small and so, the final state may only miss $|w\rangle$ by a small amount;
  - second, there are ways to adjust this algorithm so that the last step rotates by a different angle, causing the final state to be exactly aligned with $|w\rangle$
- This is beyond the scope of this course

Exercise: Search Space of *N*=4 $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

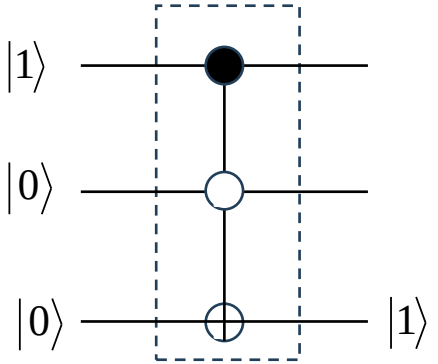
- Here is an explicit example illustrating how the quantum search algorithm works on a search space of size *N* = 4, i.e., *n*=2 ($N = 2^n$)
- The oracle (dotted box), for which $f(x) = 0$ for all *x* except $x = w$, in which case $f(w) = 1$ can be taken to be one of the four circuits



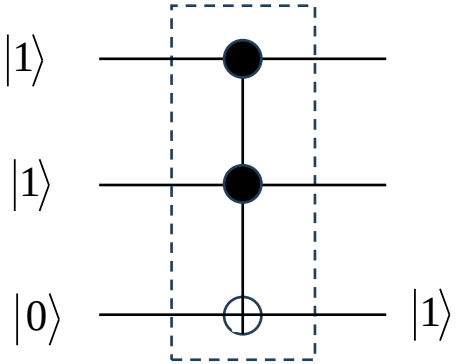
$w = 0 \ \ (00)$



$w = 1 \ \ (01)$

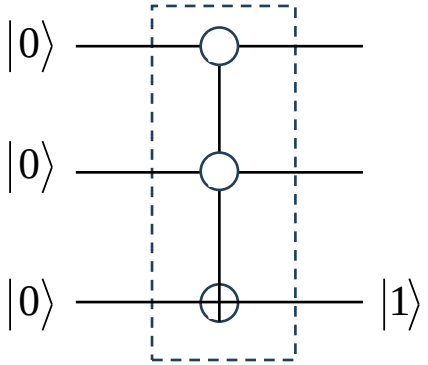


$w = 2 \ \ (10)$

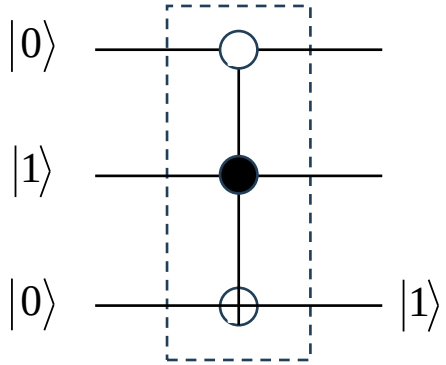


$w = 3 \ \ (11)$

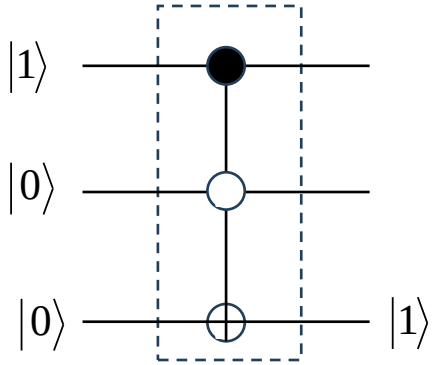
Search Space of *N*=4



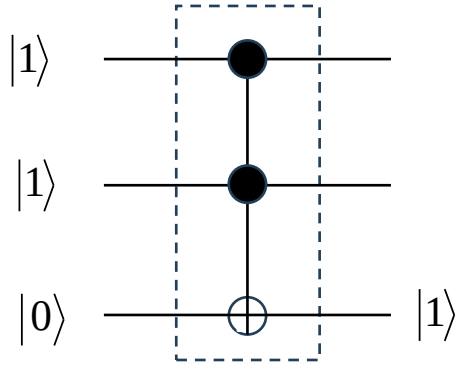
$w = 0 \ \ (00)$



$w = 1 \ \ (01)$



$w = 2 \ \ (10)$

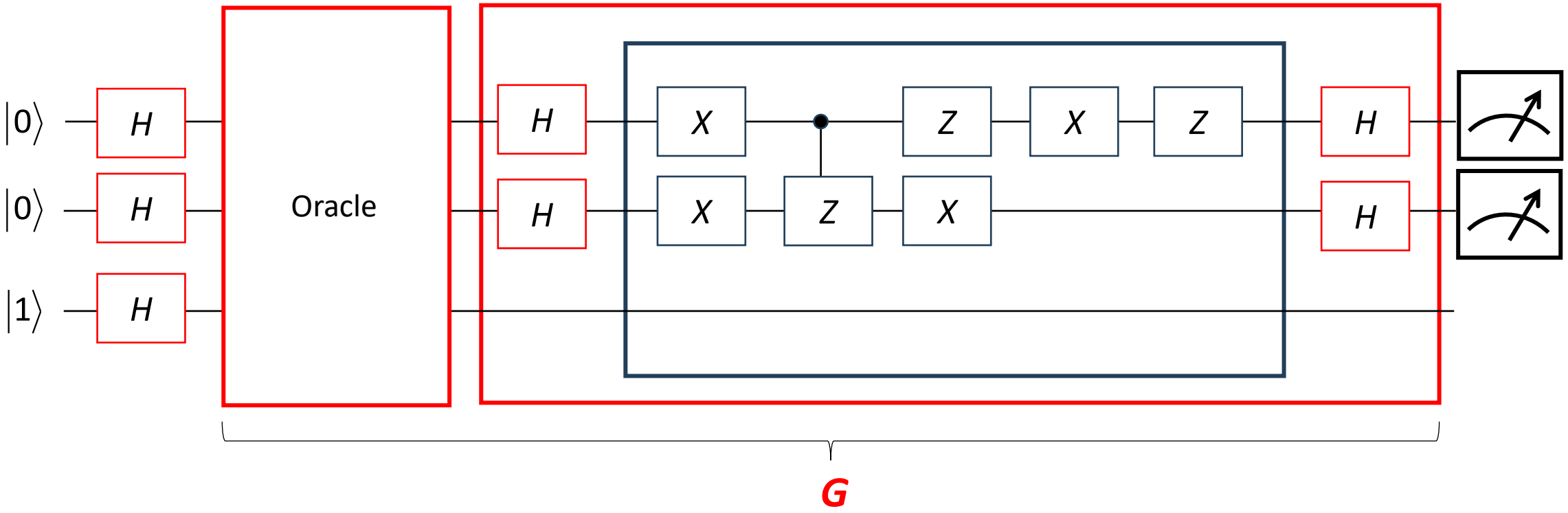


$w = 3 \ \ (11)$

- The top two qubits carry the query *x*, and the bottom qubit carries the oracle's response

Search Space of N=4

- The quantum circuit which performs the initial Hadamard transforms and a single Grover iteration *G*



Search Space of N=4

- Initially, the top two qubits are prepared in the state $|0\rangle$, and the bottom one is prepared in the state $|1\rangle$

Search Space of *N*=4

- How many times must we repeat *G* to obtain *w*?
- Since *N*=4

$$\sin\theta = \frac{1}{\sqrt{4}} = \frac{1}{2} \quad \rightarrow \quad \theta = \frac{\pi}{6} \quad \rightarrow \quad 30^0$$

- It turns out that *only exactly one iteration* is required, to perfectly obtain *w*, in this special case

$$k = \frac{\pi}{4\theta} - \frac{1}{2} = \frac{\pi}{4}\frac{6}{\pi} - \frac{1}{2} = 1$$

Search Space of *N*=4

- To confirm that, let's look at the expression:

$$G^k\left|\psi\right\rangle = \cos\left(\left(2k+1\right)\theta\right)\left|\psi_{\text{bad}}\right\rangle + \sin\left(\left(2k+1\right)\theta\right)\left|\psi_{\text{good}}\right\rangle$$

- For k=1, $\theta = 30^0 = \frac{\pi}{6}$

$$G^1\left|\psi\right\rangle = \cos\left(3\theta\right)\left|\psi_{\text{bad}}\right\rangle + \sin\left(3\theta\right)\left|\psi_{\text{good}}\right\rangle = \cos\left(3\frac{\pi}{6}\right)\left|\psi_{\text{bad}}\right\rangle + \sin\left(3\frac{\pi}{6}\right)\left|\psi_{\text{good}}\right\rangle$$

$$= \cos\left(\frac{\pi}{2}\right)\left|\psi_{\text{bad}}\right\rangle + \sin\left(\frac{\pi}{2}\right)\left|\psi_{\text{good}}\right\rangle = \left|\psi_{\text{good}}\right\rangle$$

Search Space of *N*=4

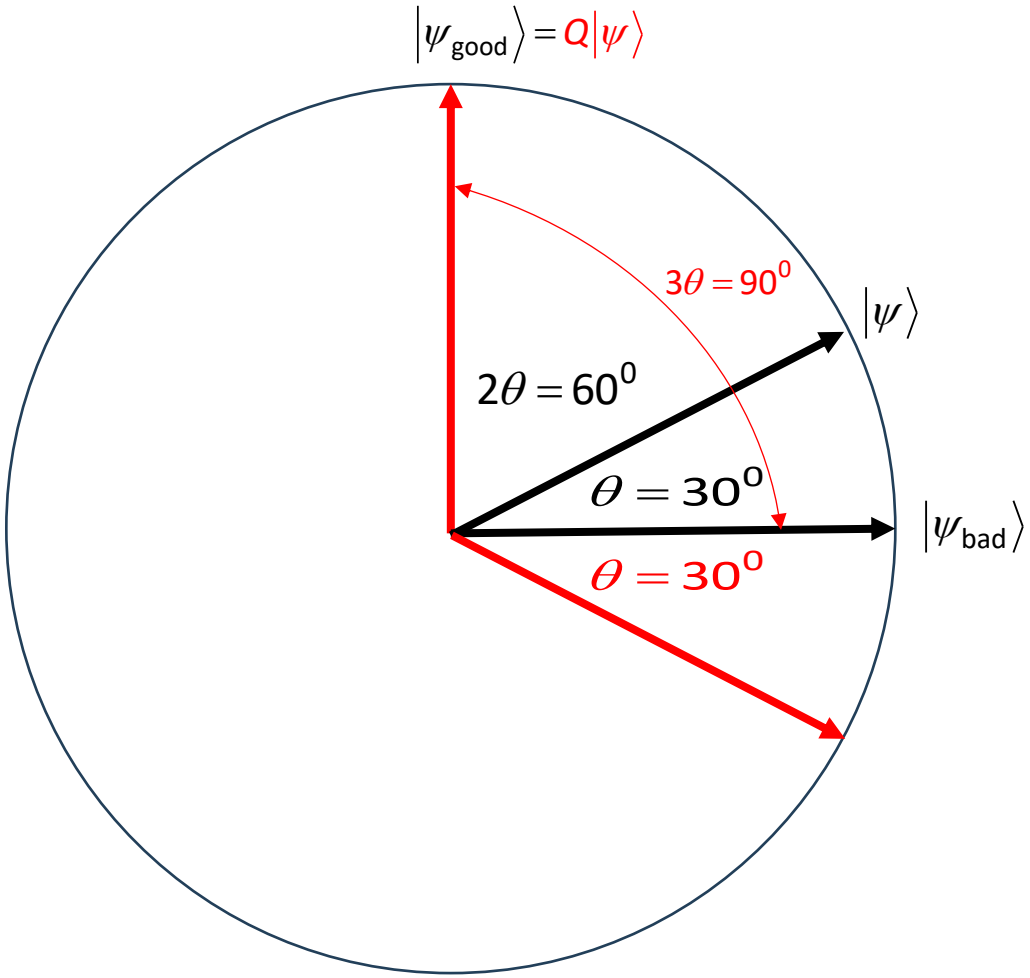
In the geometric picture, our initial state

$$|\psi\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

is $\vartheta = 30^0$ from $|\psi_{\text{bad}}\rangle$, and a single rotation by $\theta = 60^0$ moves $|\psi\rangle$ to $|\psi_{\text{good}}\rangle$

Note that

$$\sin\vartheta = \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{4}} = \frac{1}{2} \quad \rightarrow \quad \vartheta = 30^0$$



Quantum Amplitude Estimation and Quantum Counting

- You may have noticed that to apply this algorithm we have to know ahead of time how many times to apply *G*

- In the case that *A* uniformly samples the input, this requires knowing the number of solutions to the search problem

- For more general *A* it requires knowing the probability with which *A* guesses a solution to $f(x) = 1$, that is, $\sin^2(\theta)$

Quantum Amplitude Estimation and Quantum Counting

- Suppose instead of being interested in finding a solution to a search problem we are interested in counting how many solutions exist
- That is, given a search space with N elements, indexed by $\{0,1,2,\ldots,N-1\}$, $\boldsymbol{t}$ of which are solutions to $f(x) = 1$, we want to determine t
- This is the **counting problem** associated with f
- We will also consider the easier problem of approximately counting $\boldsymbol{t}$

Quantum Amplitude Estimation and Quantum Counting

- As we did earlier, let X_{bad} be the set of x that **are not solutions** to the search problem, and let X_{good} be the set of x that **are solutions** to the search problem
- We again define $|\psi_{good}\rangle$ and $|\psi_{bad}\rangle$ as before

$$|\psi_{good}\rangle = \frac{1}{\sqrt{t}} \sum_{j \in X_{good}} |j\rangle \qquad |\psi_{bad}\rangle = \frac{1}{\sqrt{N-t}} \sum_{j \in X_{bad}} |j\rangle$$

where $0 < t < N$

Quantum Amplitude Estimation and Quantum Counting

$$\rightarrow |\psi\rangle = H|00\ldots0\rangle = \frac{1}{\sqrt{N}} \sum_{j \in X_{good}} |j\rangle + \frac{1}{\sqrt{N}} \sum_{j \in X_{bad}} |j\rangle = \sqrt{\frac{t}{N}} \underbrace{\frac{1}{\sqrt{t}} \sum_{j \in X_{good}} |j\rangle}_{|\psi_{good}\rangle} + \sqrt{\frac{N-t}{N}} \underbrace{\frac{1}{\sqrt{N-t}} \sum_{j \in X_{bad}} |j\rangle}_{|\psi_{bad}\rangle}$$

- Therefore

$$|\psi\rangle = H|00\ldots0\rangle = \sqrt{\frac{t}{N}} |\psi_{good}\rangle + \sqrt{\frac{N-t}{N}} |\psi_{bad}\rangle$$

- If we put

$$\sin\vartheta = \sqrt{\frac{t}{N}} \quad \rightarrow \quad |\psi\rangle = \sin\vartheta |\psi_{good}\rangle + \cos\theta |\psi_{bad}\rangle$$

Quantum Amplitude Estimation and Quantum Counting

- Thus, we have

$$\sin^2(\theta) = \frac{t}{N}$$

and therefore, an estimation of $\sin^2(\theta)$ gives us an estimation of *t*

- We can now re-interpret the objective of Grover's algorithm as being to take an equally weighted superposition of all possible indices, $|\psi\rangle$, into $|\psi_{\text{good}}\rangle$, and then measure this state to reveal one of the index values *x* that solves $f(x) = 1$

Quantum Amplitude Estimation and Quantum Counting

- By the above construction, the probability of finding a solution (naively) simply by measuring the equal superposition state, $|\psi\rangle$, is t/N , which is exactly what one expects classically by a random generate-and-test approach
- However, if we amplitude amplify the equal superposition state before making our final measurement then we can boost our chances of success considerably
- For this we need the *t*-solutions analog of the **amplitude amplification operator**, *G*, which we built for the single-solution case

Quantum Amplitude Estimation and Quantum Counting

- Recall that in non-trivial cases the amplitude amplification *G* is a rotation in the space spanned by $\left\{\left|\psi_{\text{good}}\right\rangle,\left|\psi_{\text{bad}}\right\rangle\right\}$ through an angle 2θ

- As we saw earlier, In the subspace spanned by $\left\{\left|\psi_{\text{good}}\right\rangle,\left|\psi_{\text{bad}}\right\rangle\right\}$, *G* is described by the rotation matrix

$$G=\begin{bmatrix}\cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta\end{bmatrix}$$

where now $\sin\theta=\sqrt{t/N}$

Quantum Amplitude Estimation and Quantum Counting

- To predict the effect of *k* successive applications of *G*, we compute:

$$G^k = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix}^k = \begin{bmatrix} \cos 2k\theta & \sin 2k\theta \\ -\sin 2k\theta & \cos 2k\theta \end{bmatrix}$$

- Hence, when applied to the initial state $|\psi\rangle = \sin\vartheta |\psi_{good}\rangle + \cos\theta |\psi_{bad}\rangle$ we obtain:

$$G^k |\psi\rangle = Q^k \left(\sin\vartheta |\psi_{good}\rangle + \cos\theta |\psi_{bad}\rangle \right) = \begin{bmatrix} \cos 2k\theta & \sin 2k\theta \\ -\sin 2k\theta & \cos 2k\theta \end{bmatrix} \begin{bmatrix} \sin\vartheta \\ \cos\theta \end{bmatrix} = \begin{bmatrix} \sin(2k+1)\theta \\ \cos(2k+1)\theta \end{bmatrix} \longrightarrow$$

$$G^k |\psi\rangle = \sin\left((2k+1)\theta\right) |\psi_{good}\rangle + \cos\left((2k+1)\theta\right) |\psi_{bad}\rangle$$

Quantum Amplitude Estimation and Quantum Counting

- Consequently, to obtain a solution to $f(x) = 1$ by first amplitude amplifying $|\psi\rangle$ a number of times k, and then measuring the resulting state, we will obtain a success probability of $O(1)$ provided we pick the smallest integer k such that $(2k+1)\theta \approx \pi/2$
- As $\theta = \sqrt{\frac{t}{N}}$, this implies $k = \frac{\pi}{4}\sqrt{\frac{N}{t}} - \frac{1}{2}$, i.e., $O\left(\sqrt{\frac{N}{t}}\right)$
- Thus, classically a solution can be found in $O(N/t)$ trials, whereas quantumly one can be found in $O\left(\sqrt{N/t}\right)$ trials
- As in the case of a single solution, we again see a square root speedup for the case when there are t solutions out of $N = 2^n$ candidates

Quantum Counting

- If the number of solutions ***t*** to a multi-solution quantum search problem is not known in advance, then the quantum search can be combined with another quantum algorithm - called **quantum counting** - to efficiently count the number of solutions before running the quantum search algorithm.

Quantum Counting

- Specifically, the quantum counting algorithm returns an estimate for the number of index values, *x*, for which the function $f\ x\ :\ 0,1,2,\ldots,N-1\ \rightarrow\ 0,1$ returns the value 1
- The **quantum counting algorithm** exploits the fact that the **eigenvalues** of the Grover operator,

$$G=\begin{bmatrix}\cos 2\theta & \sin 2\theta\\ -\sin 2\theta & \cos 2\theta\end{bmatrix}$$

  are related to the number of solutions, ***t***, to the search problem
- Thus, by estimating the eigenvalues of *G* using the quantum eigenvalue estimation algorithm, one infer *t*

Quantum Amplitude Estimation and Quantum Counting

- **Eigenvalues** calculation

$$\begin{vmatrix} \cos 2\theta - \lambda & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta - \lambda \end{vmatrix} = 0 \quad \rightarrow \quad (\cos 2\theta - \lambda)^2 + \sin^2 2\theta = 0$$

- Now, let's make some calculations

$$\cos^2 2\theta + \lambda^2 - 2\lambda \cos 2\theta + \sin^2 2\theta = 0 \quad \rightarrow \quad \lambda^2 - 2\lambda \cos 2\theta + 1 = 0$$

- Thus

$$\lambda = \cos 2\theta \pm \sqrt{\cos^2 2\theta - 1} = \cos 2\theta \pm \sqrt{-\sin^2 2\theta} = \cos 2\theta \pm i \sin 2\theta = e^{\pm i 2\theta} \quad \rightarrow$$

$$\lambda = e^{\pm i 2\theta}$$

Quantum Amplitude Estimation and Quantum Counting

- **Eigenvector** associated to $\lambda = e^{+i2\theta}$

$$\begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = e^{+i2\theta} \begin{bmatrix} x \\ y \end{bmatrix} \quad \rightarrow \quad \begin{cases} x\cos 2\theta + y\sin 2\theta = xe^{i2\theta} \\ -x\sin 2\theta + y\cos 2\theta = ye^{i2\theta} \end{cases}$$

$$\begin{cases} x\left(\cos 2\theta - e^{i2\theta}\right) = -y\sin 2\theta \\ x\sin 2\theta = y\left(\cos 2\theta - e^{i2\theta}\right) \end{cases} \qquad \begin{cases} x\left(\cos 2\theta - \cos 2\theta - i\sin 2\theta\right) = -y\sin 2\theta \\ x\sin 2\theta = y\left(\cos 2\theta - \cos 2\theta - i\sin 2\theta\right) \end{cases}$$

$$\begin{cases} x\left(-i\sin 2\theta\right) = -y\sin 2\theta \\ x\sin 2\theta = y\left(-i\sin 2\theta\right) \end{cases} \qquad \begin{cases} ix = y \\ x = -iy \end{cases}$$

Quantum Amplitude Estimation and Quantum Counting

- If we take $x = -iy$, since $x^2 + y^2 = 1 \rightarrow x = -\frac{i}{\sqrt{2}}, \; y = \frac{1}{\sqrt{2}}$
- Denoting by $|\psi_+\rangle$ the eigenvector of *G* associated with the eigenvalue $\lambda = e^{+i2\theta}$ we have

$$G|\psi_+\rangle = e^{+i2\theta}|\psi_+\rangle$$

$$|\psi_+\rangle = \begin{bmatrix} -i/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = -\frac{i}{\sqrt{2}}|\psi_{\text{good}}\rangle + \frac{1}{\sqrt{2}}|\psi_{\text{bad}}\rangle$$

Quantum Amplitude Estimation and Quantum Counting

- **Eigenvector** associated to $\lambda = e^{-i2\theta}$

$$\begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = e^{-i2\theta} \begin{bmatrix} x \\ y \end{bmatrix} \quad \rightarrow \quad \begin{cases} x\cos 2\theta + y\sin 2\theta = xe^{-i2\theta} \\ -x\sin 2\theta + y\cos 2\theta = ye^{-i2\theta} \end{cases}$$

$$\begin{cases} x\left(\cos 2\theta - e^{-i2\theta}\right) = -y\sin 2\theta \\ x\sin 2\theta = y\left(\cos 2\theta - e^{-i2\theta}\right) \end{cases} \qquad \begin{cases} x\left(\cos 2\theta - \cos 2\theta + i\sin 2\theta\right) = -y\sin 2\theta \\ x\sin 2\theta = y\left(\cos 2\theta - \cos 2\theta + i\sin 2\theta\right) \end{cases}$$

$$\begin{cases} x\left(i\sin 2\theta\right) = -y\sin 2\theta \\ x\sin 2\theta = y\left(i\sin 2\theta\right) \end{cases} \qquad \begin{cases} ix = -y \\ x = iy \end{cases}$$

Quantum Amplitude Estimation and Quantum Counting

- Let's take $y = -ix$. Since $x^2 + y^2 = 1 \rightarrow x = \frac{i}{\sqrt{2}}, \; y = \frac{1}{\sqrt{2}}$
- Denoting by $|\psi_-\rangle$ the eigenvector of *G* associated with the eigenvalue $\lambda = e^{-i2\theta}$ we have

$$G|\psi_-\rangle = e^{-i2\theta}|\psi_-\rangle$$

$$|\psi_-\rangle = \begin{bmatrix} i/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = \frac{i}{\sqrt{2}}|\psi_{\text{good}}\rangle + \frac{1}{\sqrt{2}}|\psi_{\text{bad}}\rangle$$

- Thus, the eigenvalues depend on θ, and θ depends on *t*

Quantum Amplitude Estimation and Quantum Counting

- Hence, if we can find the eigenvalue $e^{-i2\theta}$ given knowledge of $|\psi_-\rangle$, or if we can find $e^{+i2\theta}$ given knowledge of $|\psi_+\rangle$, we will be able to compute θ and hence $t = N\sin^2\theta \approx N\theta^2$ for small θ
- Unfortunately, there is a problem: we do not know $|\psi_-\rangle$, and $|\psi_+\rangle$ because we do not know the two states from which they are built, i.e., $|\psi_{\text{good}}\rangle$ and $|\psi_{\text{bad}}\rangle$
- Luckily, though, we can write a state that is easy to make - the equally weighted superposition state - as a sum of $|\psi_+\rangle$ and $|\psi_-\rangle$

Quantum Amplitude Estimation and Quantum Counting

- Specifically, we have:

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \sin\theta|\psi_{\text{good}}\rangle + \cos\theta|\psi_{\text{bad}}\rangle$$

$$= \left(\frac{ie^{-i\theta} - ie^{+i\theta}}{2}\right)|\psi_{\text{good}}\rangle + \left(\frac{e^{-i\theta} + e^{+i\theta}}{2}\right)|\psi_{\text{bad}}\rangle$$

$$= \frac{e^{+i\theta}}{\sqrt{2}}\left(-\frac{i}{\sqrt{2}}|\psi_{\text{good}}\rangle + \frac{1}{\sqrt{2}}|\psi_{\text{bad}}\rangle\right) + \frac{e^{-i\theta}}{\sqrt{2}}\left(\frac{i}{\sqrt{2}}|\psi_{\text{good}}\rangle + \frac{1}{\sqrt{2}}|\psi_{\text{bad}}\rangle\right)$$

$$= \frac{e^{+i\theta}}{\sqrt{2}}|\psi_{+}\rangle + \frac{e^{-i\theta}}{\sqrt{2}}|\psi_{-}\rangle$$

Quantum Amplitude Estimation and Quantum Counting

- Now we can use this state

$$|\psi\rangle = \frac{e^{+i\theta}}{\sqrt{2}}|\psi_+\rangle + \frac{e^{-i\theta}}{\sqrt{2}}|\psi_-\rangle$$

as the known input to the **eigenvalue estimation algorithm**

Multiple Eigenstates (From Unit 14)

- Assume we have two eigenstates of *U*, which we call $|\nu_1\rangle$ and $|\nu_2\rangle$, with corresponding eigenvalues $e^{2\pi i\lambda_1}$ and $e^{2\pi i\lambda_2}$
- Say we are using the previous phase estimation algorithm but **prepare the eigenstate register** in the following **superposition** of $|\nu_1\rangle$ and $|\nu_2\rangle$

$$\frac{\sqrt{3}}{2}|\nu_1\rangle+\frac{1}{2}|\nu_2\rangle$$

- We also have the *m* qubits that each start in the state $|0\rangle$, so the initial state of the phase estimation circuit is

$$|0\ldots000\rangle\left(\frac{\sqrt{3}}{2}|\nu_1\rangle+\frac{1}{2}|\nu_2\rangle\right)=\frac{\sqrt{3}}{2}|0\ldots000\rangle|\nu_1\rangle+\frac{1}{2}|0\ldots000\rangle|\nu_2\rangle$$

Multiple Eigenstates (From Unit 14)

- Following the same calculation as the previous section, the final state of the phase estimation circuit

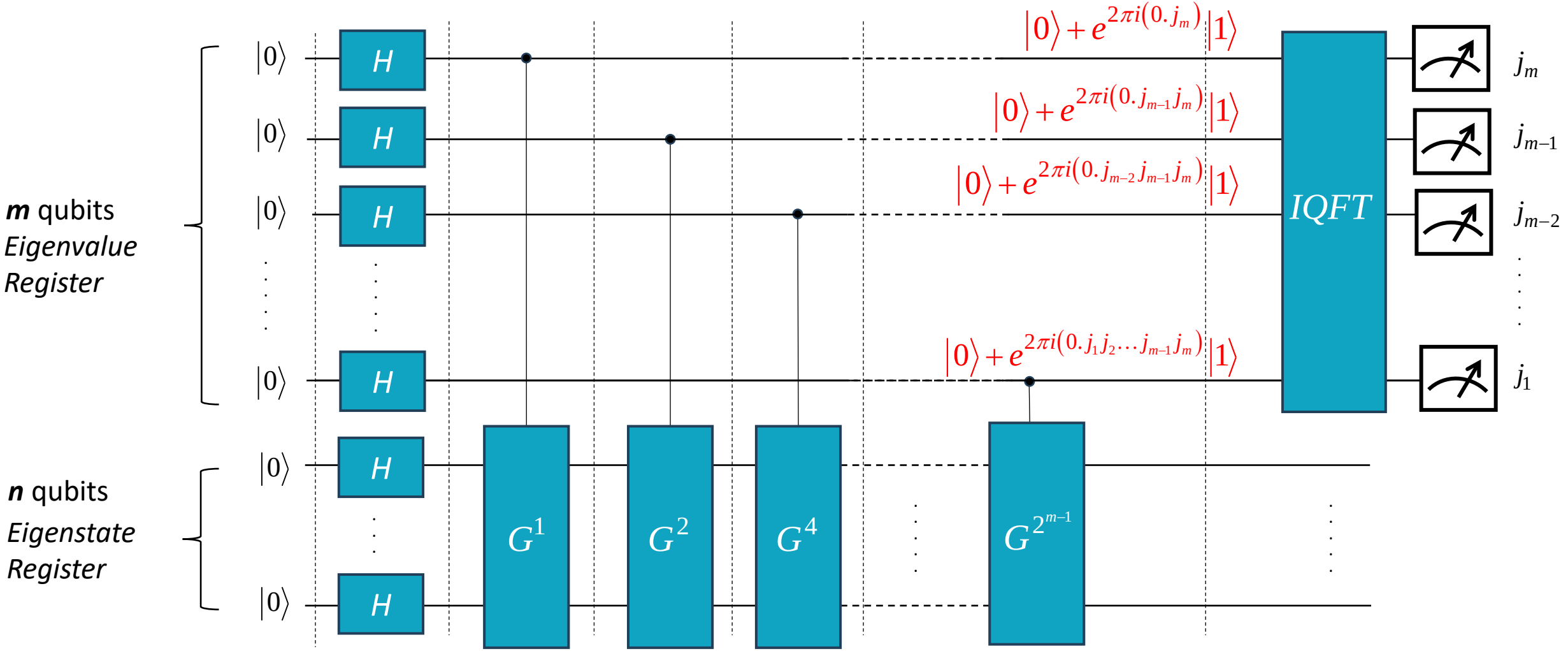
$$\frac{\sqrt{3}}{2}\left|j_1 j_2 \ldots j_m\right\rangle\left|\nu_1\right\rangle+\frac{1}{2}\left|j_1' j_2' \ldots j_m'\right\rangle\left|\nu_2\right\rangle \qquad [11]$$

  where $0.j_1 j_2 \ldots j_m$ is an m-bit approximation of λ_1 and $0.j_1' j_2' \ldots j_m'$

  is an m-bit approximation of λ_2

- Then, when we measure the qubits at the end of the circuit, we get an approximation of λ_1 with probability 3/4 or an approximation of λ_2 with probability of 1/4

Quantum Amplitude Estimation and Quantum Counting



Quantum Amplitude Estimation and Quantum Counting

- The picture reported in the previous slide illustrates the quantum circuit for **quantum counting** the number of solutions to a search problem with amplitude amplification operator *G*

- Note that the Hadamard gates acting on the bottom set of qubits create the uniform superposition

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} |x\rangle$$

Quantum Amplitude Estimation and Quantum Counting

- However, this state may also be interpreted as a superposition of the two (unknown) eigenvectors of *G*, i.e., $|\psi_+\rangle$ and $|\psi_-\rangle$
- Specifically, we have

$$|\psi\rangle = \frac{e^{+i\theta}}{\sqrt{2}}|\psi_-\rangle + \frac{e^{-i\theta}}{\sqrt{2}}|\psi_+\rangle$$

- So, the output from the top set of qubits are the sequence of bits in the binary fraction expansion of 2θ or -2θ of the eigenvalues of *G,* from which we can compute an estimate of

$$t = 2^n \sin^2(\pi j) = \sin^2(-\pi j) \quad \text{where} \quad j = 0.j_1 j_2 \ldots j_m = \frac{j_1}{2} + \frac{j_2}{2^2} + \cdots + \frac{j_m}{2^m}$$

Appendix

Quantum Amplitude Estimation and Quantum Counting

Exercise: In the subspace spanned by $\left\{\left|\psi_{\text{good}}\right\rangle,\left|\psi_{\text{bad}}\right\rangle\right\}$, prove that *G* is described by a rotation through an angle 2θ, i.e.,

$$G=\begin{bmatrix}\cos 2\theta & \sin 2\theta\\ -\sin 2\theta & \cos 2\theta\end{bmatrix}$$

Proof

- Bring back to mind the four results that were obtained earlier

$G=U_{\psi^{\perp}}U_f$

$U_{\psi^{\perp}}=2\left|\psi\right\rangle\left\langle\psi\right|-I$

$\left|\psi\right\rangle=\sin\theta\left|\psi_{\text{good}}\right\rangle+\cos\theta\left|\psi_{\text{bad}}\right\rangle$

$U_f=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$

and first derive $U_{\psi^{\perp}}=2\left|\psi\right\rangle\left\langle\psi\right|-I$

Quantum Amplitude Estimation and Quantum Counting

$$U_{\psi^\perp} = 2|\psi\rangle\langle\psi| - I = 2\left(\sin\theta|\psi_{\text{good}}\rangle + \cos\theta|\psi_{\text{bad}}\rangle\right)\left(\sin\theta\langle\psi_{\text{good}}| + \cos\theta\langle\psi_{\text{bad}}|\right) - I$$

$$= 2\left(\sin^2\theta|\psi_{\text{good}}\rangle\langle\psi_{\text{good}}| + \sin\theta\cos\theta|\psi_{\text{good}}\rangle\langle\psi_{\text{bad}}| + \cos\theta\sin\theta|\psi_{\text{bad}}\rangle\langle\psi_{\text{good}}| + \cos^2\theta|\psi_{\text{bad}}\rangle\langle\psi_{\text{bad}}|\right) - I$$

$$= 2\begin{bmatrix} \sin^2\theta & \cos\theta\sin\theta \\ \sin\theta\cos\theta & \cos^2\theta \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2\sin^2\theta - 1 & 2\cos\theta\sin\theta \\ 2\sin\theta\cos\theta & 2\cos^2\theta - 1 \end{bmatrix} = \begin{bmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}$$

where

$$\begin{array}{c} \\ |\psi_{\text{good}}\rangle \\ |\psi_{\text{bad}}\rangle \end{array} \begin{array}{c} \langle\psi_{\text{good}}| \quad\quad \langle\psi_{\text{bad}}| \\ \begin{bmatrix} \sin^2\theta & \cos\theta\sin\theta \\ \sin\theta\cos\theta & \cos^2\theta \end{bmatrix} \end{array}$$

Quantum Amplitude Estimation and Quantum Counting

Since $G = U_{\psi^\perp} U_f$, where $U_f = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ $\rightarrow$

$$G = \begin{bmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix}$$

□