3: Entanglement and Grover's algorithm.

- Basis
- Bell basis.
- CHSH game.
- Grover's algorithm.

Basis:

What is a basis? Well, we can't talk about a basis without talking about a vector space first!

Def/ Vector space:

A set V is a vector space if:

1. addition is well-defined: i.e. $\exists f$ s.t. $\forall u, v \in V$, $f(u,v) = u+v$ and $u+v \in V$.
2. scalar multiplication is well-defined: i.e. $\exists f$ s.t. $\forall u \in V$ and any scalar λ, $f(u) = \lambda u$ and $\lambda u \in V$.

Def/ Basis of a vector space:

A basis B of a vector space V is a list of vectors in V that is linearly independent and spans V (i.e. cannot write one vector as a sum of the other, but can write any vector in V as a sum of vectors in B).

Hilbert space: a (complex) vector space w/ an inner product.

inner product:

$$\langle x|y\rangle = \sum_i x_i^* y_i$$

So, an arbitrary (pure) quantum state is just a vector in a Hilbert space!

examples of bases:

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$ "standard" or "Z"

show that this is a basis:

$$\left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \right\}$$

linearly independent ✓

span $\mathbb{C}^{2^2} = \mathbb{C}^4$ ✓:

for $\alpha, \beta, \gamma, \eta \in \mathbb{C}$: $\begin{pmatrix}\alpha\\\beta\\\gamma\\\eta\end{pmatrix} = \alpha\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \gamma\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \eta\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

$|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle$, "Hadamard" or "X"

$|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle$, "Bell"

– these are all orthonormal: $\langle\psi|\phi\rangle = 1$ if $|\psi\rangle \equiv |\phi\rangle$

$\langle\psi|\phi\rangle = 0$ if $|\psi\rangle \not\equiv |\phi\rangle$

Bell Basis:

- separability:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|00\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \left(|1\rangle + |0\rangle\right)\right)$$

we call such a state "separable": it factors via the tensor product.

- entanglement: not separable!

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

– there is no way to write this as a factor of tensor products! we call such a state entangled.

other examples:

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

in terms of vectors:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$ "Bell state"

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$$

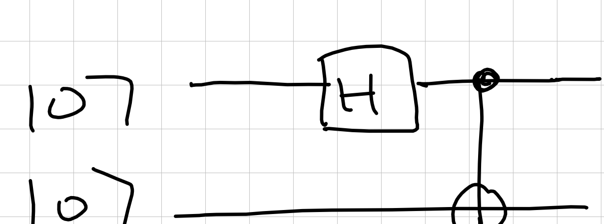
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$$

Note that, none of these Bell states are separable!

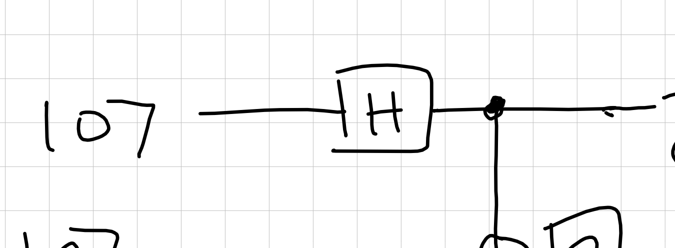
Preparing a Bell state:

$|\beta_{00}\rangle$:



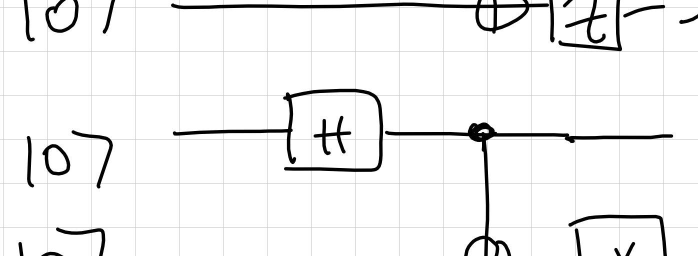
$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$|\beta_{01}\rangle$:



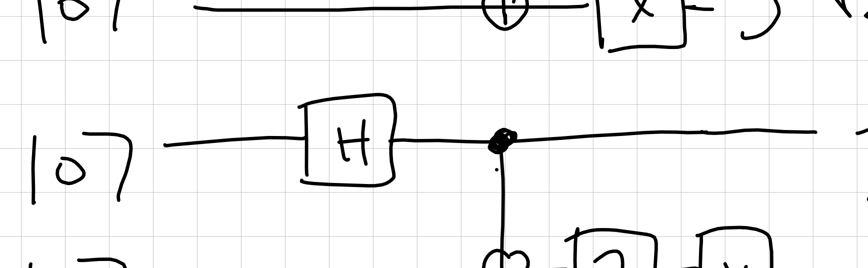
$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$

$|\beta_{10}\rangle$:



$\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$

$|\beta_{11}\rangle$:



$\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

- todo: Bell basis measurement, CHSH game, Grover's algorithm.

CHSH game:

- Clauser, Horne, Shimony, Holt.
- A bit on the history of the foundations of QM:

EPR paradox: (Einstein, Podolsky, Rosen):

If we prepare an EPR pair:

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

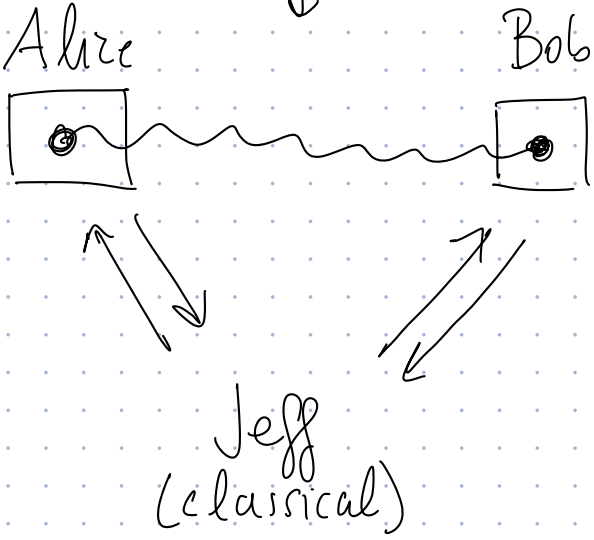
Then measuring qubit 1 allows us to predict, with certainty, the value of qubit 2 (in some fixed basis). This is possible even though no actual information was transferred between the two particles.

EPR argued that this must imply that there is some type of local hidden variable that deterministically leads to the value of the measurement outcomes, and so the correlation in outcomes is the result of purely classical correlations.

Then Bell (and CHSH) actually demonstrated the opposite: such a local hidden variable theory cannot exist.

CHSH game setup:

separated by a large distance, so cannot communicate.



Game:

1. Verifier chooses bits x, y uniformly at random and sends x to Alice and y to Bob.
2. Alice responds with $r_A \in \{0,1\}$ and Bob responds with $r_B \in \{0,1\}$.
3. Jeff checks whether

$$s_A \cdot s_B = r_A \oplus r_B$$

↓ mult. ↓ XOR:

r_A	r_B	$r_A \oplus r_B$
0	0	0
0	1	1
1	0	1
1	1	0

Alice + Bob win the game iff $s_A \cdot s_B = r_A \oplus r_B$.

Question: what is the strategy for Alice + Bob such that they win the game w/ high prob.?

Let's say that A+B have a purely classical strategy. What is their maximal winning probability?

Classical strategy: assign a response conditioned on the input.

Possible winning conditions:

x	y	$x \cdot y$	$= r_{A,x} \oplus r_{B,y}$
0	0	0	$= r_{A,0} \oplus r_{B,0}$
0	1	0	$= r_{A,0} \oplus r_{B,1}$
1	0	0	$= r_{A,1} \oplus r_{B,0}$
1	1	1	$= r_{A,1} \oplus r_{B,1}$

To find a winning strategy that works w/ 100% probability, would need to find

$r_{A,0}$; $r_{B,0}$; $r_{A,1}$; $r_{B,1}$

such that all of the above equations are satisfied.

BUT: the LHS : $0 \oplus 0 \oplus 0 \oplus 1 = 1$

RHS: $(r_{A,0} \oplus r_{B,0}) \oplus (r_{A,0} \oplus r_{B,1}) \oplus (r_{A,1} \oplus r_{B,0}) \oplus (r_{A,1} \oplus r_{B,1})$

$= (r_{B,0} \oplus r_{A,0}) \oplus (r_{A,0} \oplus r_{B,1}) \oplus (r_{A,1} \oplus r_{B,0}) \oplus (r_{A,1} \oplus r_{B,1})$

(associative and commutative and self-inverse).

$= 0$

So, not all equations can be satisfied.

At most 3 of them can, and therefore the best classical strategy is w/ 75% probability.

What about a quantum strategy?

Idea: Alice and Bob share an EPR pair:

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}} |0_A 0_B\rangle + |1_A 1_B\rangle$$

In this case, choosing a strategy involves choosing a mapping between input bit from

Jeff and a measurement basis.

How do we find the optimal strategy?

CHSH inequality: metric of correlation strength for classical systems. This equals 2.

To find optimal strategy, want to find measurements that maximize the CHSH inequality.

$$E(a,b) - E(a,b') + E(a',b') + E(a',b) \leq 2$$

"CHSH inequality": a, a', b, b' are detector settings and $E(\cdot)$ is the correlation between measurement outcomes.

Turns out, the optimal strategy is:

Alice measures:

If $x=0$: Z basis

If $x=1$: X basis

Bob measures:

If $x=0$: $\frac{X+Z}{\sqrt{2}}$ basis

If $x=1$: $\frac{Z-X}{\sqrt{2}}$ basis

Winning probability is: $\cos^2\left(\frac{\pi}{8}\right)$ (Tsirelson bound).

$\approx 85\%$

intuition: there are unique correlations that exist due to entanglement which can increase the winning probability.

See github for original CHSH paper.

Grover's algorithm notes by: Francisca Vasconcelos and Amir Karamlou

1 Grover's Algorithm

Following Shor's algorithm, in 1995, Lov Grover proposed the quantum search algorithm now known as Grover's algorithm. Although Grover's algorithm did not provide as spectacular of a speedup (exponential) as Shor's algorithm, the widespread applicability of search-based methodologies created considerable interest in it.

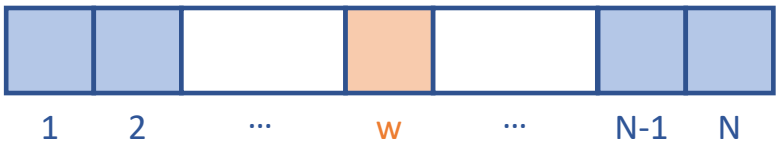
As we will see, classical linear search requires $O(N)$ operations, while quantum search requires $O(\sqrt{N})$ operations. Note that while faster classical search algorithms exist (i.e. binary search is $O(\log(n)) < O(\sqrt{N})$), but these algorithms require a *sorted* list of input. If the sorting time is considered, the classical search is overall less efficient.

1.1 Problem Statement

Grover's algorithm aims to solve the following problem:

Given a search space of size N, and no prior knowledge about the structure of information in it (i.e. unstructured), find an element of that search space satisfying a known property.

Given: a list of N items



Goal: identify the winner state (w)

1.2 Mapping to the Quantum Domain

Q: How will the list be defined in our quantum computer?
A: With an oracle.

In this case, the oracle is a "black-box" function which returns 0 for unmarked input and 1 for the winner input

$$f(x) = \begin{cases} 1, & \text{if } x = w \\ 0, & \text{if } x \neq w \end{cases}$$

In the quantum computer the oracle will be encoded as a *unitary matrix* and the list of items will be provided as a *superposition* of states. In order to represent the list items with qubits, we must choose a binary encoding $x, w \in 0, 1^n$ such that $N = 2^n$ (where n is the number of list items).

Example: Suppose we have a list of length $N = 8$, we need 3-bit binary encodings ($8{=}2^3$).

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$$

Important Note: You may be wondering what the point of the oracle is at this point...It seems as though the oracle already knows the answer to the search problem?! However, a distinction should be made. You can *recognize* the solution to a search problem without actually *knowing* the solution. The power of the quantum computer lies in out ability to apply this recognition function to *all* N items at once (with superposition), rather than testing each item individually, as is done classically.

We define the Grover oracle as unitary matrix U_f, which acts on any of the standard basis states $|x\rangle$ by,

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

If x is unmarked, the oracle does nothing to the state. If x is a winner state, then $U_f|x\rangle = U_f|w\rangle = -|w\rangle$.

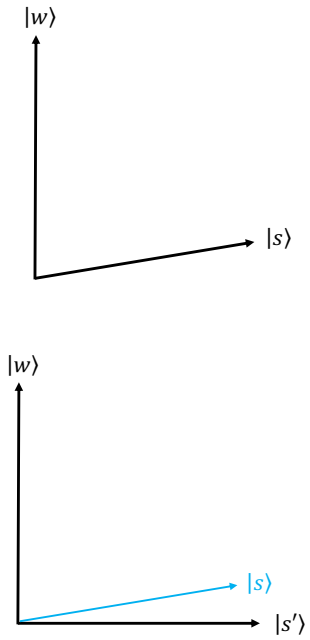
Now, all that is left is to define the input state to our system. Before looking at our list of items, we have no idea where the winner state is. Any guess of its location is as good as any other, meaning our input should be a *uniform* superposition state,

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

If we were to stop here and measure our state, the superposition would collapse to any one of the basis states with the *same* probability, $\frac{1}{N} = \frac{1}{2^n}$.

1.3 Geometric Picture

Grover's algorithm uses a procedure called *amplitude amplification* to significantly enhance the probability of measuring the winner state. Geometrically, we can picture the 2 special states (winner $|w\rangle$ and $|s\rangle$) as 2 vectors spanning $\mathbb{C}^N$.
However, since $|s\rangle$, is a superposition over all possible states (including $|w\rangle$), it is not



perpendicular to $|s\rangle$. Thus, we introduce orthogonal state $|s'\rangle$. $|s'\rangle$ is obtained from $|s\rangle$ by removing $|w\rangle$ and rescaling (as in the Gram-Schmidt process).

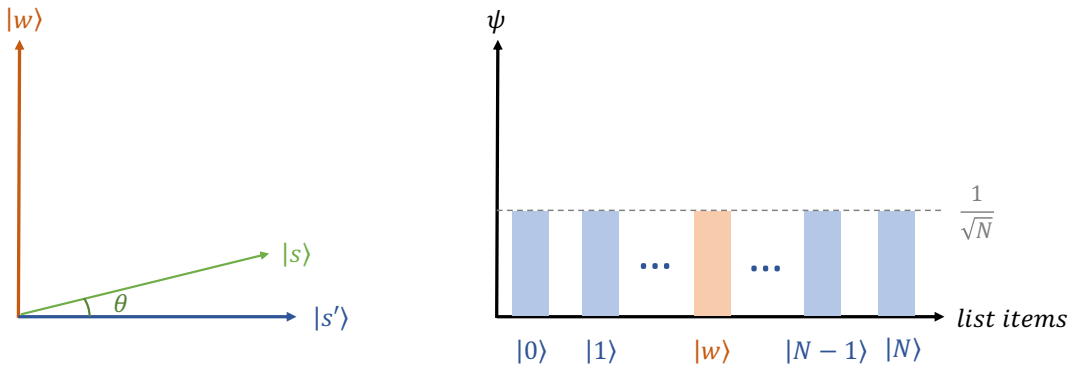
1.4 Amplitude Amplification Procedure

We now have everything we need to describe the procedure of Grover's algorithm!

Step 0: Initialization
Initialize to superposition state, at $t = 0$,

$$|\Psi_0\rangle = |s\rangle = H^{\otimes n}|0\rangle^n \qquad \left(= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \right)$$

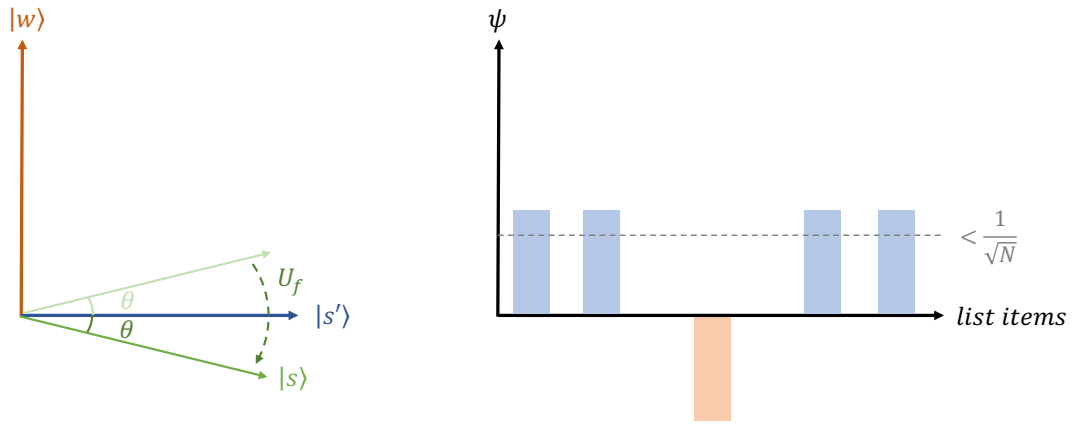
The average amplitude of N states is $\frac{1}{\sqrt{N}}$.



Step 1: Apply Oracle
Apply the oracle, U_f,

$$|\Psi_{t'}\rangle = U_f|\Psi_0\rangle.$$

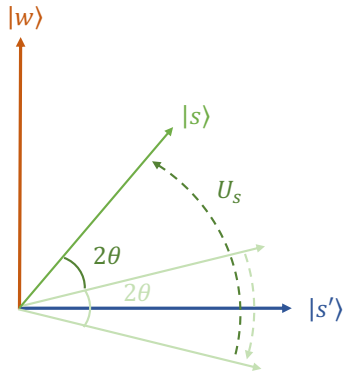
Geometrically, U_f corresponds to a reflection of state $|\Psi_0\rangle$ about $|s'\rangle$. Thus, the amplitude of the $|w\rangle$ state becomes negative and the overall average amplitude is lowered $\left(< \frac{1}{\sqrt{N}}\right)$.

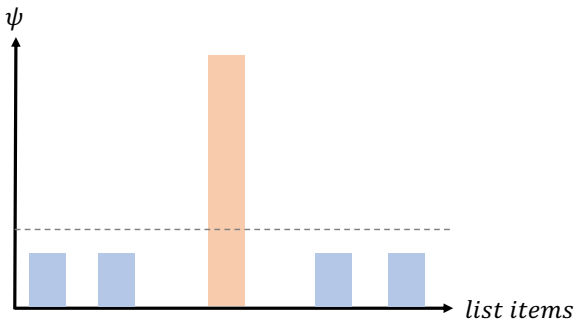


Step 2: Amplitude Amplification
Apply $U_s = 2|s\rangle\langle s| - \mathbb{I}$,

$$|\Psi_t\rangle = U_s|\Psi_{t'}\rangle = U_sU_f|\Psi_0\rangle.$$

Geometrically, U_s corresponds to a reflection of state $|\Psi_{t'}\rangle$ about $|s\rangle$. From the perspective our measurement amplitudes, this corresponds to a reflection about the average amplitude. We can verify this mathematically by applying the operation $(2|s\rangle\langle s| - \mathbb{I})$, with $|s\rangle =$





$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$, to a general state, $\sum_{k=0}^{N-1}\alpha_k|k\rangle$, with average $\langle\alpha\rangle = \sum_k \alpha_k|\langle s|k\rangle|^2$,

$$
\begin{aligned}
(2|s\rangle\langle s| - \mathbb{I})\sum_k \alpha_k|k\rangle &= \sum_k 2\alpha_k|s\rangle\langle s|k\rangle - \alpha_k|k\rangle \\
&= \sum_k 2\alpha_k|s\rangle\left(\tfrac{1}{\sqrt{N}}\sum_x\langle x|k\rangle\right) - \alpha_k|k\rangle \\
&= \sum_k 2\alpha_k|s\rangle\left(\tfrac{1}{\sqrt{N}}\sum_x \delta_{xk}\right) - \alpha_k|k\rangle \\
&= \sum_k \tfrac{2\alpha_k}{\sqrt{N}}|s\rangle - \alpha_k|k\rangle \\
&= \sum_k \tfrac{2\alpha_k}{\sqrt{N}}\left(\tfrac{1}{\sqrt{N}}\sum_x|x\rangle\right) - \alpha_k|k\rangle \\
&= 2\sum_k\sum_x \tfrac{\alpha_k}{N}|x\rangle - \sum_k \alpha_k|k\rangle \\
&= 2\sum_x\left(\sum_k \alpha_k|\langle s|k\rangle|^2\right)|x\rangle - \sum_k \alpha_k|k\rangle \\
&= \sum_x 2\langle\alpha\rangle|x\rangle - \sum_k \alpha_k|k\rangle \\
&= \sum_k \left(2\langle\alpha\rangle - \alpha_k\right)|k\rangle \quad \square
\end{aligned}
$$

Step 3: Repeat

Repeat Steps 1 and 2 several times in order to rotate $|s\rangle$ closer to $|w\rangle$ and away from $|s'\rangle$. After t rotations, the state becomes,

$$|\Psi_t\rangle = (U_s U_f)^t|\Psi_0\rangle$$

As it turns out, $\sqrt{N}$ rotations are necessary, since the amplitude of $|w\rangle$ grows linearly with the number of applications (grows as $\sim t\sqrt{N}$, where $t = \sqrt{N}$ such that $\langle w|s\rangle \approx 1$).

1.5 Pseudocode

1) create superposition of n qubits

2) apply oracle O
3) apply Hadamard transformation $H^{\otimes n}$
4) perform a conditional phase shift on the computer, with every computational basis state except $|0\rangle$ receiving a phase shift of -1

$$|x\rangle \rightarrow -(-1)^{\delta_{x,0}}|x\rangle$$

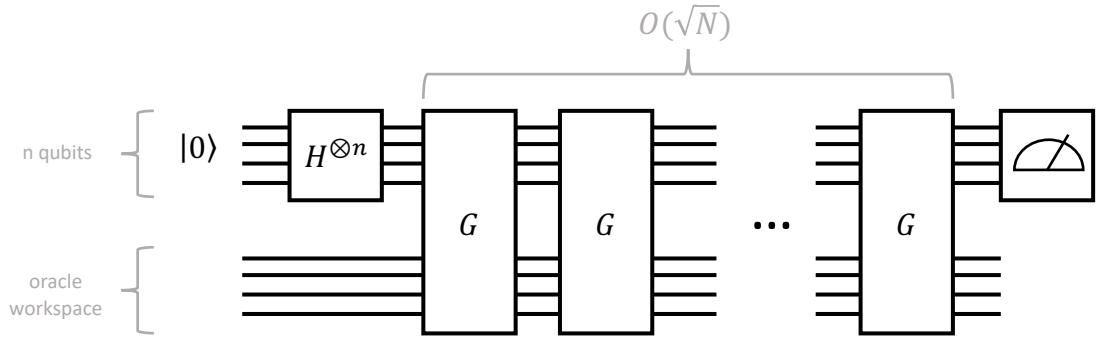
can be done with operator $2|0\rangle\langle 0| - \mathbb{I}$

5) apply Hadamard transformation $H^{\otimes n}$

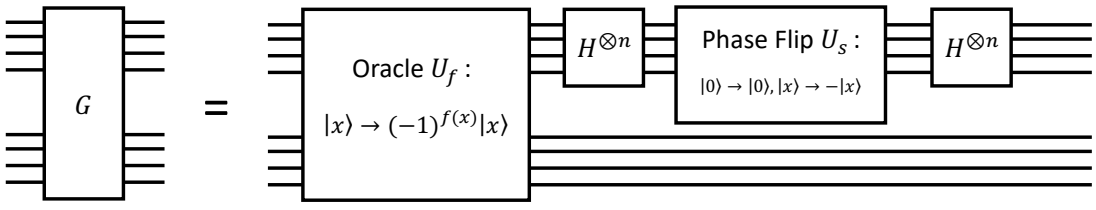
} Grover Iteration

6) repeat steps 2-5 (Grover Iteration) $O(\sqrt{N})$ times

1.6 General Quantum Circuit

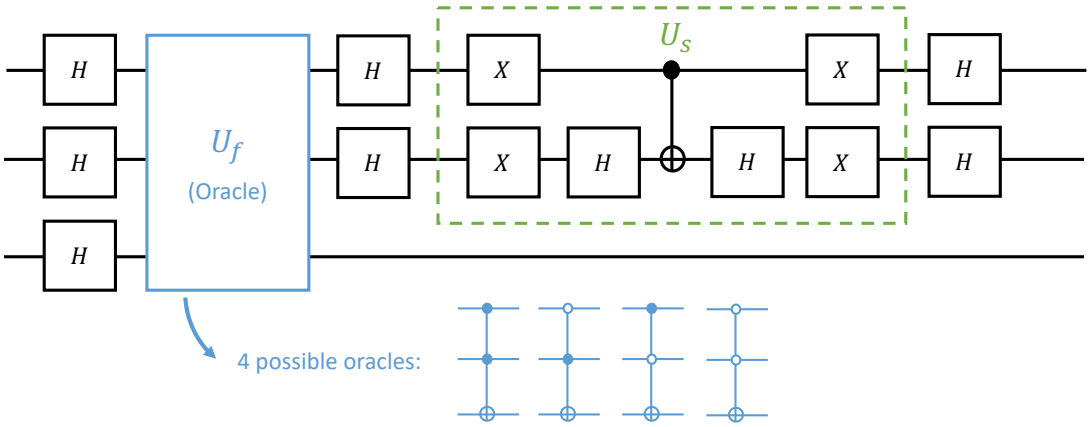


Grover search algorithm implementation, where each "G" gate corresponds to a single Grover iteration.



1.7 $N = 4$ (2-bit) Implementation Example

We now provide an example of the exact gates necessary to implement Grover's algorithm to search in a list of 4 items ($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$).



As you can see, there are four different possible oracles, corresponding to the state we are searching for. On your pset you will be tasked with verifying that each of these oracles result in a different output states.

1.8 Further Reading

To see how the algorithm can be implemeted in a hybrid system (i.e. one with classical memory) and how the algorithm acts when there are multiple winner states in the list of items, read chapter 6 of *Quantum Computation and Quantum Information*, by Nielsen and Chuang.