Universal set of quantum gates

A set of quantum gates that allows us to approximate any quantum gate to any desired precision is called a universal gate set.

(*Exactly) universal*: all gates of one and two quits.

(Approximately universal): We say that a circuit with gates $U_1 U_2 \dots U_t$ approximates U with precision ϵ if[1]

$$\|U - U_t \dots U_2 U_1\| \leq \epsilon$$

with some appropriate matrix norm. For instance, the spectral norm

$$\|A\| := \max_{|\psi\rangle} \frac{\|A|\psi\rangle\|}{\||\psi\rangle\|}$$

i.e., the largest *singular value* of A.

[1]A. M. Childs, Lecture Notes on Quantum Algorithms, http://www.cs.umd.edu/~amchilds/qa/.

Some examples of universal gate sets are:

- {CNOT, all single-qubit gates}[1]
- {CNOT, H, T}[2]
- {CNOT, $R_y(\pi/4)$, S}[3]
- {Toffoli, H}[4] - reversible classical gate + 1 quantum gate!

Properties of a set of quantum gates to be universal:

- Superposition;
- Entanglement;
- Complex amplitudes;
- Contain more than the *Clifford group* {CNOT, H, S}.

[1]A. Barenco, et al., *Phys. Rev. A* **52**, 3457 (1995).
[2]P. O. Boykin, et al. *Inf. Proc. Lett.* **75**, 101 (2000).
[3]A. Y. Kitaev, *RMS: Russian Mathematical Surveys* **52**, 1191 (1997).
[4]Y. Shi, arXiv:quant-ph/0205115 (2002).

The *Clifford group* is the set of gates $\{\mathrm{CNOT}, H, S\}$.

Although this set contains the properties described previously, the *Gottesman-Knill theorem*[1] says that a quantum circuit containing only these gates is efficiently simulated by a classical computer.

Theorem: A quantum circuit using only the following elements can be simulated efficiently on a classical computer:

1. Preparation of qubits in state $|0\rangle^{\otimes n}$,
2. Clifford gates,
3. Measurements in the computational basis.

This theorem shows that even some *highly entangled states* can be simulated efficiently.

[1] D. Gottesman, arXiv:quant-ph/9807006v1, (1998).

Solovay-Kitaev Theorem

Theorem[1]: Fix two universal gate sets that are closed under inverses. Then any t-gate circuit using one gate set can be implemented to precision ϵ using a circuit of $t\,\mathrm{poly}\log(t/\epsilon)$ gates from other set (indeed, there is a classical algorithm for finding this circuit in time $t\,\mathrm{poly}\log(t/\epsilon)$.

Meaning:

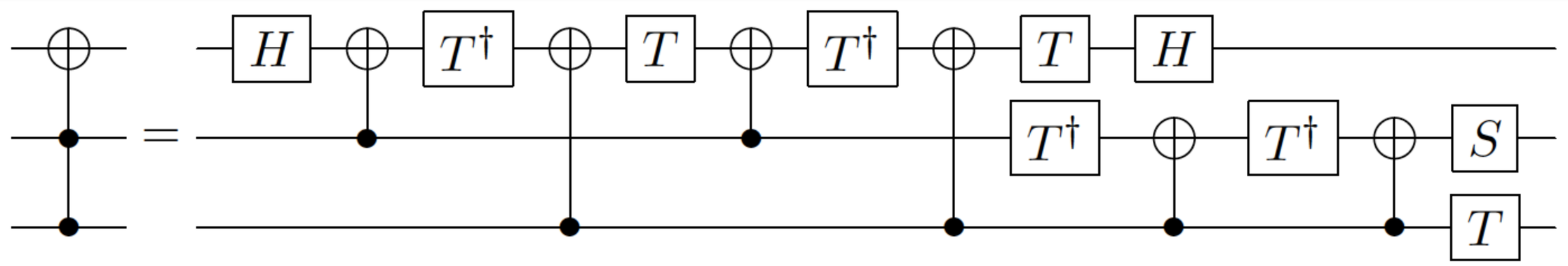
- The running time of an algorithm using one gate set is the same as that using the other gate set up to logarithmic factors;
- This means that even polynomial quantum speedups are robust with respect to the choice of gate set;
- Quantum computers need only implement a finite number of gates to gain the full power of quantum computation.

[1]A. M. Childs, Lecture Notes on Quantum Algorithms, http://www.cs.umd.edu/~amchilds/qa/.

Circuit complexity

It is the least number of quantum gates required to implement a given quantum circuit, relative to some universal set of quantum gates.

Example: Toffoli gate decomposed into 16 one and two qubits gates.



Efficient quantum algorithms have at most *polynomial* circuit complexity $\mathrm{poly}(n)$, in which n is the number of input qubits .

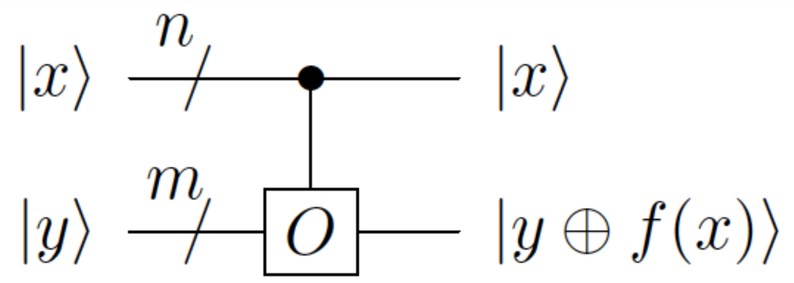
Circuit complexity is generally hard to find!

Quantum Oracles

In this model, we assume we have access to an *oracle*, or *black box*, to which we can pass queries, and which returns answers to our queries. Our *goal* is to determine some property of the oracle using the *minimal number of queries*[1].

XOR Oracle[2]

The XOR quantum oracle O is a unitary operator that implements the *boolean function* $f : \{0,1\}^n \to \{0,1\}^m$:



$|x\rangle$ is the input state

$|y\rangle$ is the *target* or *answer* state

[1]A. Montanaro, Quantum computation - Lecture notes, https://people.maths.bris.ac.uk/~csxam/teaching/qc2020/.

[2]G. G. Pollachini, (2018). http://gcq.ufsc.br/doku.php?id=trabalhos_desenvolvidos. In portuguese.

$y \oplus f(x)$ is the *bitwise* XOR operation,

$$y \oplus f(x) = y_1 \oplus f_1(x) \ldots y_m \oplus f_m(x) = \text{string of length } m$$

Notice that if $|y\rangle = |0\rangle^{\otimes m}$, then the output state is $|y \oplus f(x)\rangle = |f(x)\rangle$.

Phase Oracle[1]

Lets consider only one target qubit to illustrate the idea. Our first goal is to prepare the state $|y\rangle = |-\rangle$

$$|x\rangle|0\rangle \xrightarrow{I\otimes X} |x\rangle|1\rangle \xrightarrow{I\otimes H} |x\rangle|-\rangle$$

[1]G. G. Pollachini, TCC, (2018). In portuguese.

Then, querying the oracle, we get

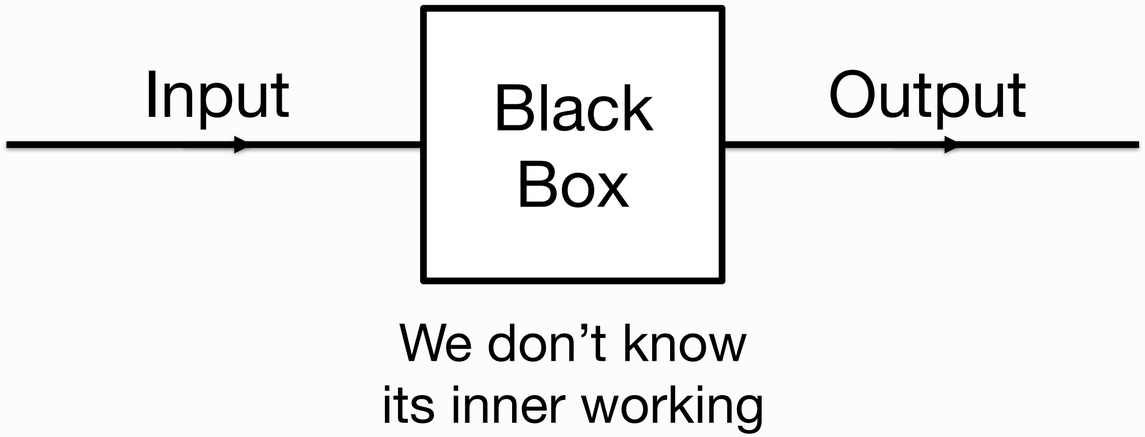
$$
\begin{aligned}
|x\rangle|-\rangle &= |x\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \\
&\underset{O}{=} \frac{1}{\sqrt{2}}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) \\
&\longrightarrow \frac{1}{\sqrt{2}}\left(|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\right) \\
&= \begin{cases} \frac{1}{\sqrt{2}}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right), & f(x) = 0 \\ \frac{1}{\sqrt{2}}\left(|x\rangle|1\rangle - |x\rangle|0\rangle\right), & f(x) = 1 \end{cases} \\
&= \begin{cases} |x\rangle|-\rangle, & f(x) = 0 \\ -|x\rangle|-\rangle, & f(x) = 1 \end{cases} \\
&= (-1)^{f(x)}|x\rangle|-\rangle .
\end{aligned}
$$

Therefore, the action of a phase oracle O_P can be summarized as

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

Query complexity

It is the number of calls to a function, or queries to an oracle (or black box) needed to solve the problem.



Example: In the Grover's search algorithm, the classical solution takes $O(N)$ queries, while in the quantum case it takes only $O(\sqrt{N})$.

We call *oracle separation* the speedup in the number of oracle queries.

Oracular quantum algorithms

Deutsch problem[1]

Problem: Let $f(x)$ be a boolean function $f : \{0,1\} \rightarrow \{0,1\}$, which is promised to be *constant* ($f(0) = f(1)$) or *balanced* ($f(0) \neq f(1)$). The problem is to determine if the function is balanced or constant.

Classical solution

In the classical scenario, we must calculate $f(0)$ and $f(1)$ and compare them.

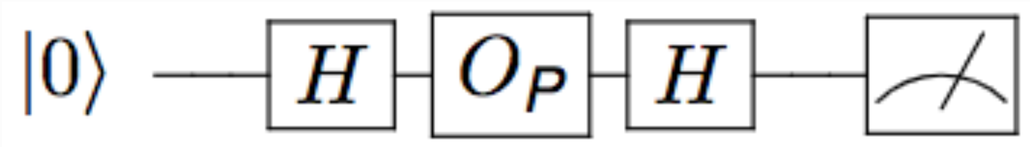
Two bits of information are required!

[1]D. Deutsch, *Proc. R. Soc. A* **400**, 7 (1985).

Oracular quantum algorithms

Deutsch problem[1]

Problem: Let $f(x)$ be a boolean function $f:\{0,1\}\rightarrow\{0,1\}$, which is promised to be *constant* ($f(0)=f(1)$) or *balanced* ($f(0)\neq f(1)$). The problem is to determine if the function is balanced or constant.



$$|0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} \rightarrow \frac{(-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle}{\sqrt{2}} \rightarrow \left[\frac{(-1)^{f(0)}+(-1)^{f(1)}}{2}\right]|0\rangle+\left[\frac{(-1)^{f(0)}-(-1)^{f(1)}}{2}\right]|1\rangle$$

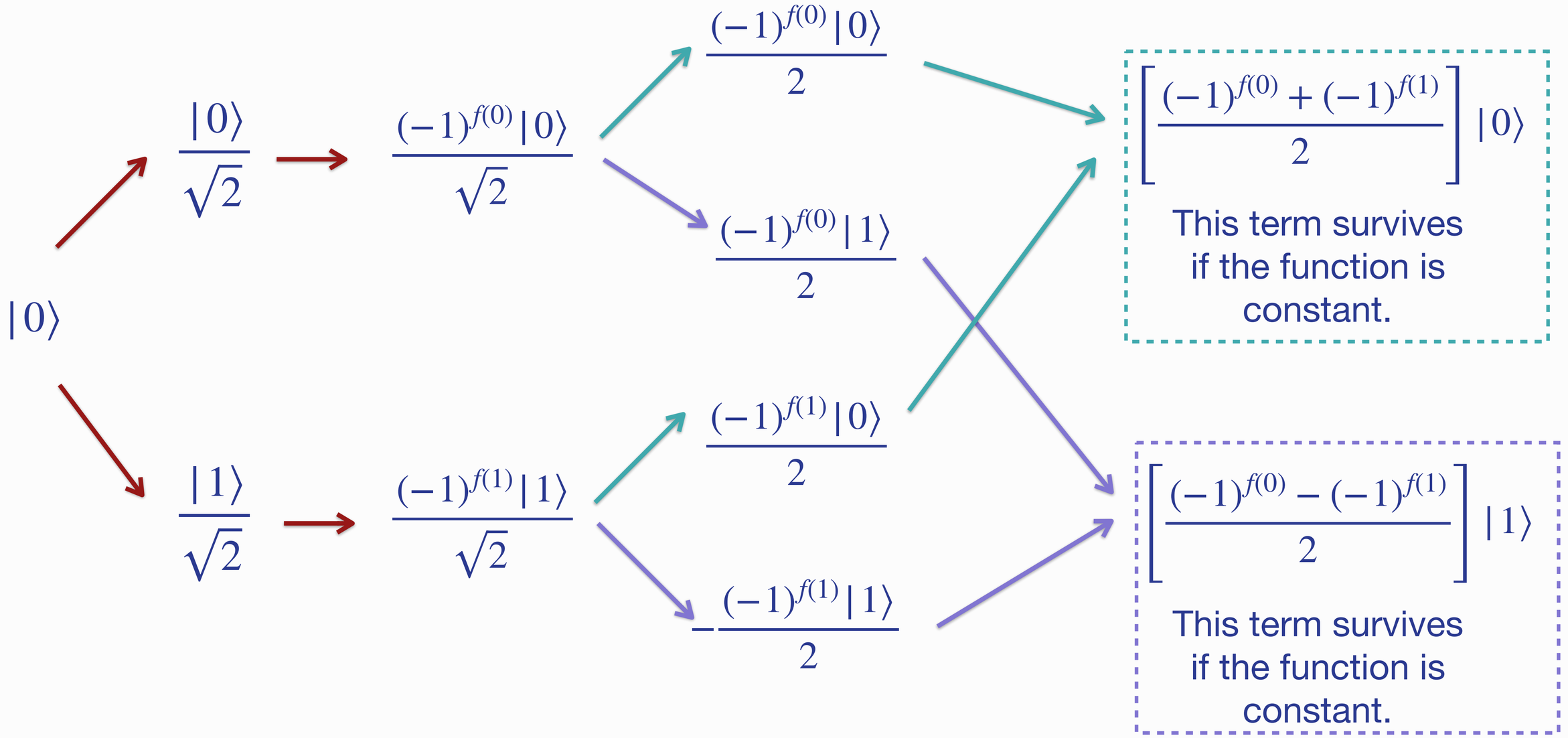
If $f(x)$ is constant, then we measure the state $|0\rangle$;
If $f(x)$ is balanced, then we measure the state $|1\rangle$.

Just one qubit of information![2]

[1]D. Deutsch, *Proc. R. Soc. A* **400**, 7 (1985).
[2]D. Collins, K. W. Kim, and W. C. Holton Phys. Rev. A **58**, R1633(R) (1998).

The power of quantum interference

Lets interpret the algorithm as an interference process:



Deutsch-Jozsa algorithm[1]

Problem: Let $f(x)$ be a boolean function $f : \{0,1\}^n \to \{0,1\}$, which is promised to be *constant* or *balanced*. The problem is to determine if the function is balanced or constant.

Deterministic classical solution

There are 2^n functions $\{f(0), f(1), f(2), f(3), \ldots, f(2^n - 1)\}$

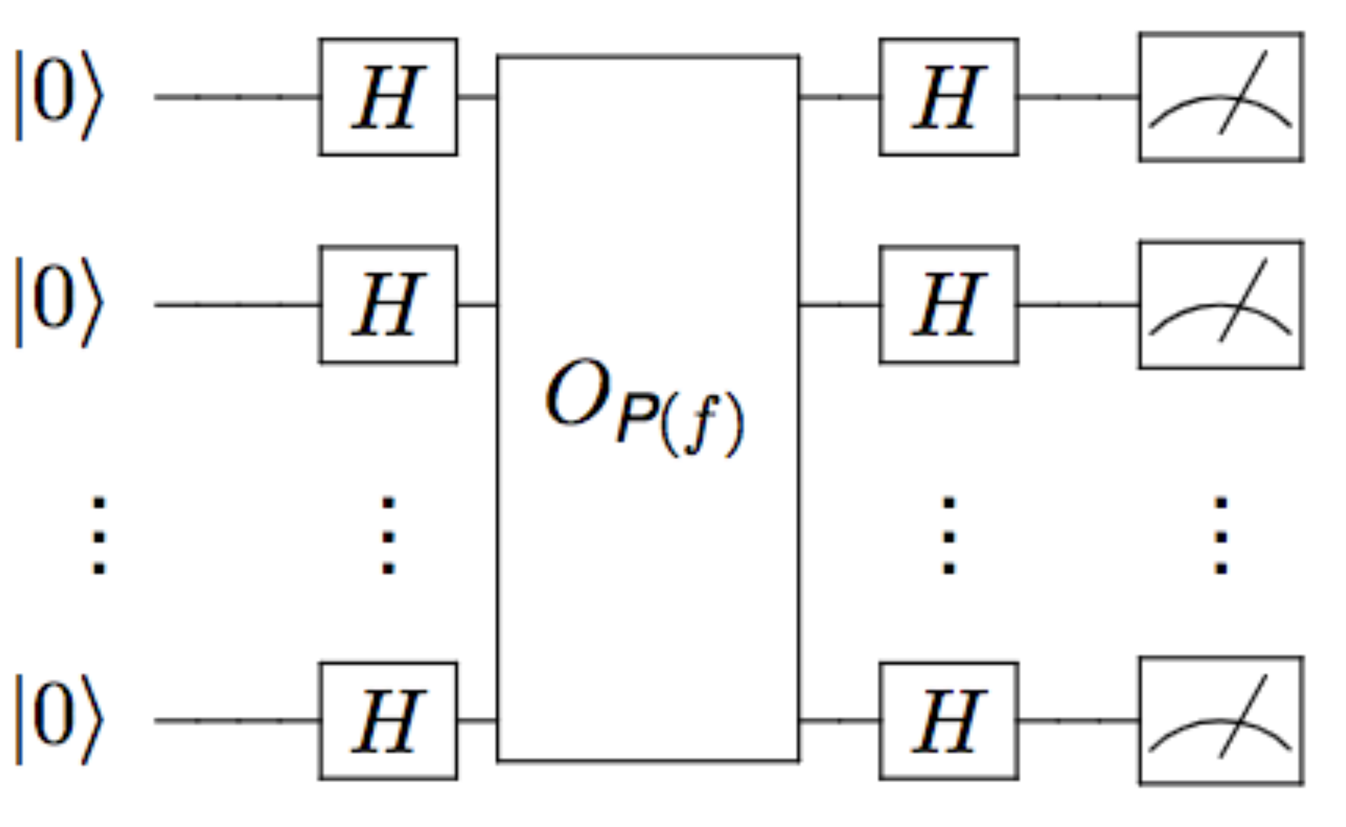
In the worst case it is necessary to evaluate $2^{n-1} + 1$ functions to decide if f is constant or balanced.

Exponential number of queries to the classical oracle.

[1]D. Deutsch, R. Jozsa, *Proc. R. Soc. London A*. **439**, 553 (1992).

Quantum solution

Optimized version of the circuit used to solve the Deutsch-Jozsa problem[1].



[1]D. Collins, K. W. Kim, and W. C. Holton Phys. Rev. A **58**, R1633(R) (1998).

Step 0 - Initial state: $|0\rangle^{\otimes n}$

Step 1 - Uniforme superposition state:

$$
\begin{aligned}
|\psi_1\rangle &= H^{\otimes n}\,|0\rangle^{\otimes n} \\
&= |+\rangle^{\otimes n} \\
&= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \cdots \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{B}_n} |x\rangle \ ,
\end{aligned}
$$

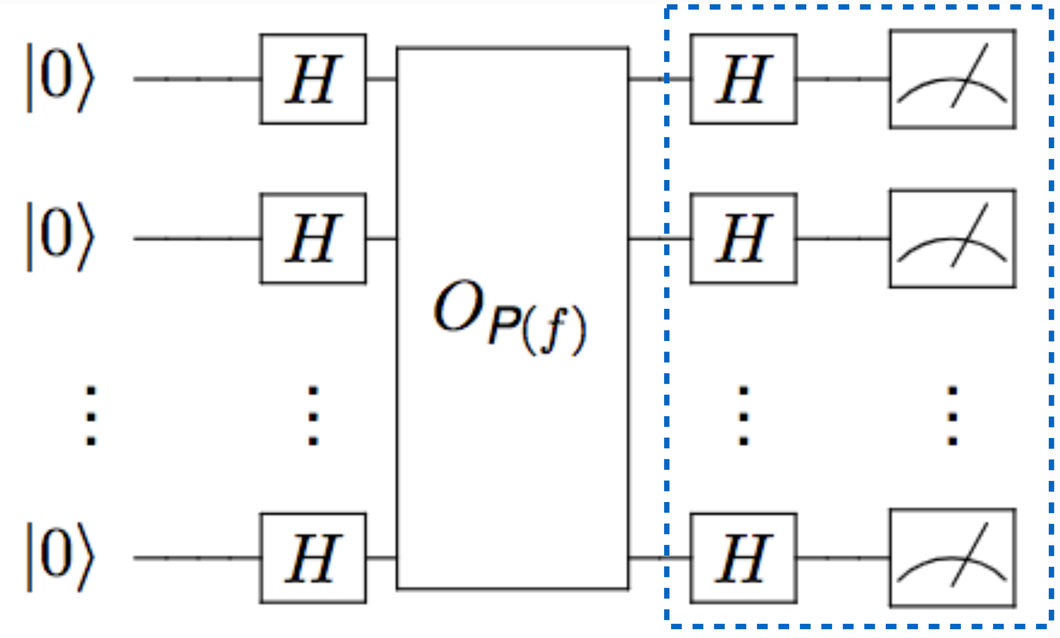
2^n possible combinations of n qubits

$$
\begin{aligned}
\mathbb{B}_n &= \{0\ldots00\,,\ 0\ldots01\,,\ 0\ldots10\,,\ 0\ldots11\,,\ \ldots\,,\ 1\ldots11\} \\
&= \{0, 1, 2, 3, \ldots, 2^n - 1\} \ .
\end{aligned}
$$

Step 2 - Oracle query:

$$
\begin{aligned}
|\psi_2\rangle &= O_P \ |\psi_1\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{B}_n} O_P |x\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{B}_n} (-1)^{f(x)} \ |x\rangle
\end{aligned}
$$

Step 3 - Measurement (rotated basis) $\{|+\rangle, |-\rangle\}$:



$$H|0\rangle = |+\rangle$$

$$H|1\rangle = |-\rangle$$

Density of probability of finding the system in the final state $|+\rangle^{\otimes n}$:

$$\langle +|^{\otimes n}|\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{B}_n}\langle y|\right)\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{B}_n}(-1)^{f(x)}|x\rangle$$

$$= \frac{1}{2^n}\sum_{x\in\mathbb{B}_n}\sum_{y\in\mathbb{B}_n}(-1)^{f(x)}\langle y|x\rangle$$

$$= \frac{1}{2^n}\sum_{x\in\mathbb{B}_n}\sum_{y\in\mathbb{B}_n}(-1)^{f(x)}\delta_{x,y}$$

$$= \frac{1}{2^n}\sum_{x\in\mathbb{B}_n}(-1)^{f(x)}\ .$$

$\langle + | = \langle 0 | H$

$\langle - | = \langle 1 | H$

± 1 – for constant function

0 – for balanced function

Therefore, if the result of the measurement is $|0\rangle^{\otimes n}$, the function is constant, otherwise it is balanced.

Only one oracle query in the quantum case.

Exponential speedup.

But, it is not all roses

Efficient probabilistic classical solution to the Deutsch-Jozsa problem.

Exercise: Given that f is a balanced function of n qubits. Show that the probability of a wrong guess that the function is constant is

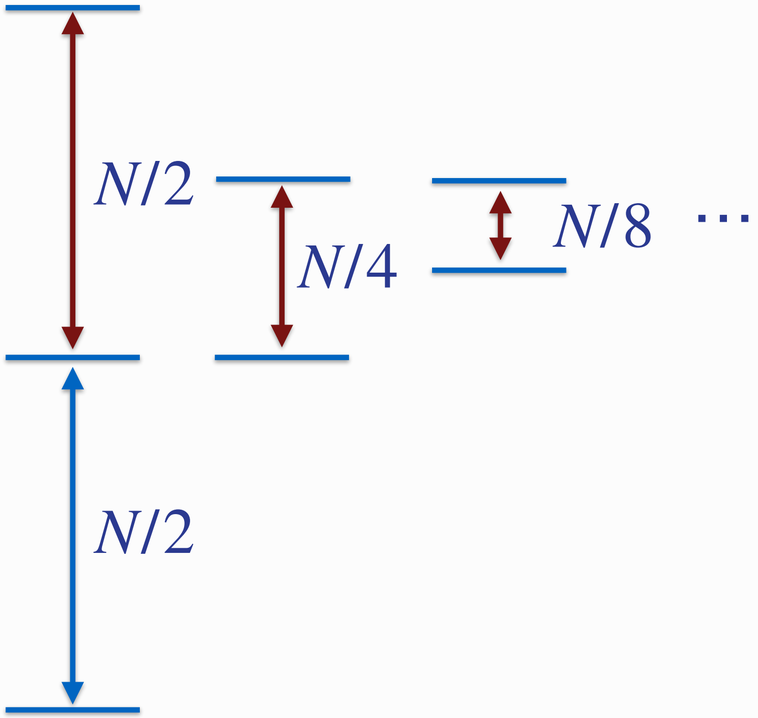
$$p_{error} = \frac{1}{2^k}$$

For k measurements s.t. $2^n \gg k$.

Looking for names and phone numbers in a telephone book

Looking for *names* is easy!

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



Binary search algorithm:

$$\frac{\#\text{ of names}}{2^{\{\#\text{ of steps}\}}} = \frac{N}{2^k} = 1$$

Number of steps in average

$O(\log_2 N)$

Whats is the number of steps to find a given phone number?

Grover's problem[1]

The goal of the Grover's algorithm is to find an element in an unstructured list of $N = 2^n$ elements.

Problem: Find the only entry $x_0 \in \{0,1\}^n$ such that

$$f(x) = \begin{cases} 1, & x = x_0, \\ 0, & x \neq x_0 \, . \end{cases}$$

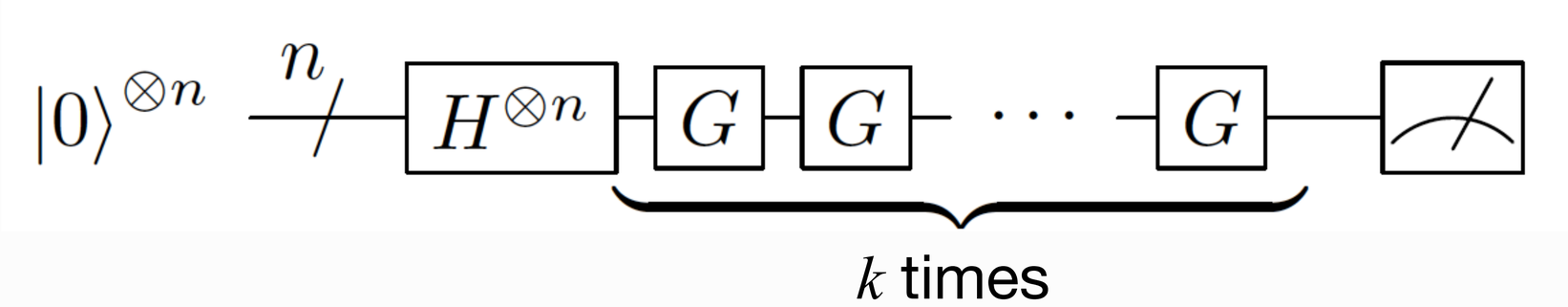
Classical solution: It is necessary looking for $\Theta(N)$ elements.

PS: The primary use of Grover's algorithm (at least initially) is likely not to be searching physical databases, but instead searching for solutions to computational problems.

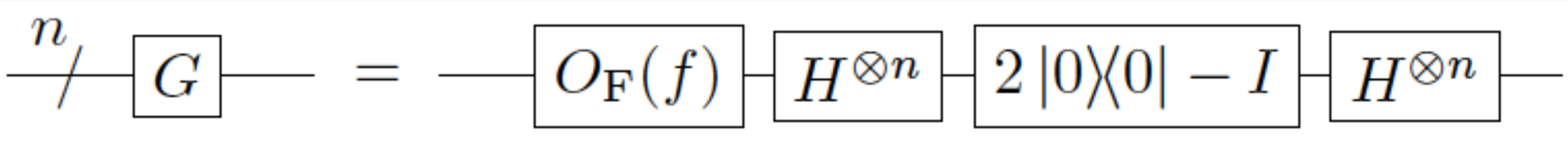
[1]L. K. Grover, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 212 (1996).

Grover's algorithm

The compact notation of the quantum circuit is[1]



in which



is the Grover's operator.

[1]G. G. Pollachini, (2018). http://gcq.ufsc.br/doku.php?id=trabalhos_desenvolvidos. In portuguese.

Step 0 - Initial state: $|0\rangle^{\otimes n}$

Step 1 - Uniforme superposition state:

Lets first define the following states

2D space

Target state

$$|\beta\rangle := |x_0\rangle$$

Complementary state

$$|\alpha\rangle := \sum_{\substack{x \in \mathbb{B}_n \\ x \neq x_0}} \frac{|x\rangle}{\sqrt{N-1}}$$

$$\begin{aligned}
|\psi\rangle &= |+\rangle^{\otimes n} \\
&= \sum_{x \in \mathbb{B}_n} \frac{|x\rangle}{\sqrt{N}} \\
&= \frac{\sqrt{N-1}}{\sqrt{N}} \sum_{\substack{x \in \mathbb{B}_n \\ x \neq x_0}} \frac{|x\rangle}{\sqrt{N-1}} + \frac{|x_0\rangle}{\sqrt{N}} \\
&= \frac{\sqrt{N-1}}{\sqrt{N}} |\alpha\rangle + \frac{1}{\sqrt{N}} |\beta\rangle
\end{aligned}$$

Step 3 - Grover's operator

Oracle's effect:

$$O_F|x\rangle = (-1)^{f(x)}|x\rangle \rightarrow = \begin{cases} O_F|x\rangle = -|x\rangle, & x = x_0, \\ O_F|x\rangle = |x\rangle, & x \neq x_0 . \end{cases}$$

$$\begin{aligned} O_{\mathrm{F}}|\alpha\rangle &= O_{\mathrm{F}} \sum_{\substack{x \in \mathbb{B}_n \\ x \neq x_0}} \frac{|x\rangle}{\sqrt{N-1}} \\ &= \sum_{\substack{x \in \mathbb{B}_n \\ x \neq x_0}} \frac{1}{\sqrt{N-1}} O_{\mathrm{F}}|x\rangle \\ &= \sum_{\substack{x \in \mathbb{B}_n \\ x \neq x_0}} \frac{1}{\sqrt{N-1}}|x\rangle \\ &= |\alpha\rangle \ , \end{aligned}$$

and

$$\begin{aligned} O_{\mathrm{F}}|\beta\rangle &= O_{\mathrm{F}}|x_0\rangle \\ &= -|x_0\rangle \\ &= -|\beta\rangle \ . \end{aligned}$$

Rewriting the G operator

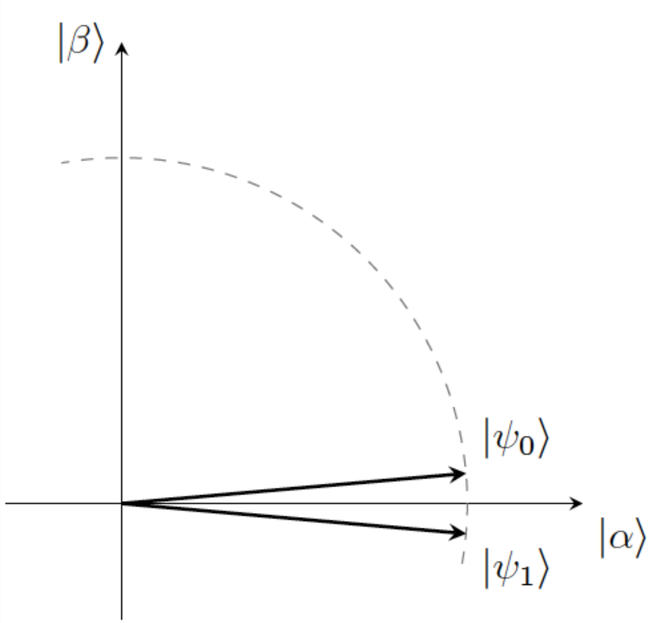
$$
\begin{aligned}
G &= H^{\otimes n}(2\left|0\right\rangle\!\left\langle 0\right| - I)H^{\otimes n}O_{\mathrm{F}} \\
&= \left(2H^{\otimes n}\left|0\right\rangle\!\left\langle 0\right|H^{\otimes n} - H^{\otimes n}IH^{\otimes n}\right)O_{\mathrm{F}} \\
&= \left(2H^{\otimes n}\left|0\right\rangle\!\left\langle 0\right|(H^{\otimes n})^{\dagger} - H^{\otimes n}H^{\otimes n}\right)O_{\mathrm{F}} \\
&= (2\left|\psi\right\rangle\!\left\langle\psi\right| - I)O_{\mathrm{F}}
\end{aligned}
$$

$$|\psi\rangle = |+\rangle^{\otimes n}$$

Don’t forget!

Application of the quantum oracle:

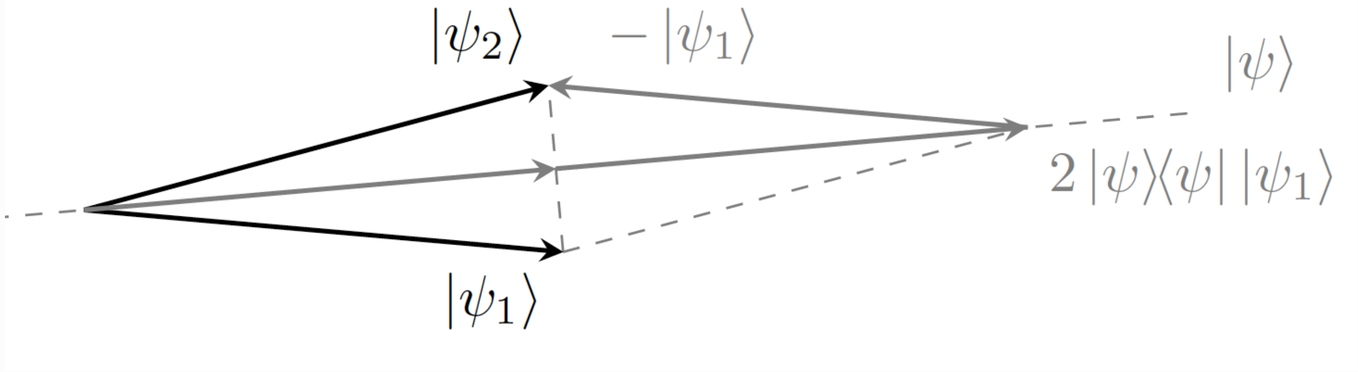
$$
\begin{aligned}
|\psi_1\rangle &= O_{\mathrm{F}}\left|\psi_0\right\rangle \\
&= O_{\mathrm{F}}\left(\frac{\sqrt{N-1}}{\sqrt{N}}\left|\alpha\right\rangle + \frac{1}{\sqrt{N}}\left|\beta\right\rangle\right) \\
&= \frac{\sqrt{N-1}}{\sqrt{N}}\left|\alpha\right\rangle - \frac{1}{\sqrt{N}}\left|\beta\right\rangle
\end{aligned}
$$



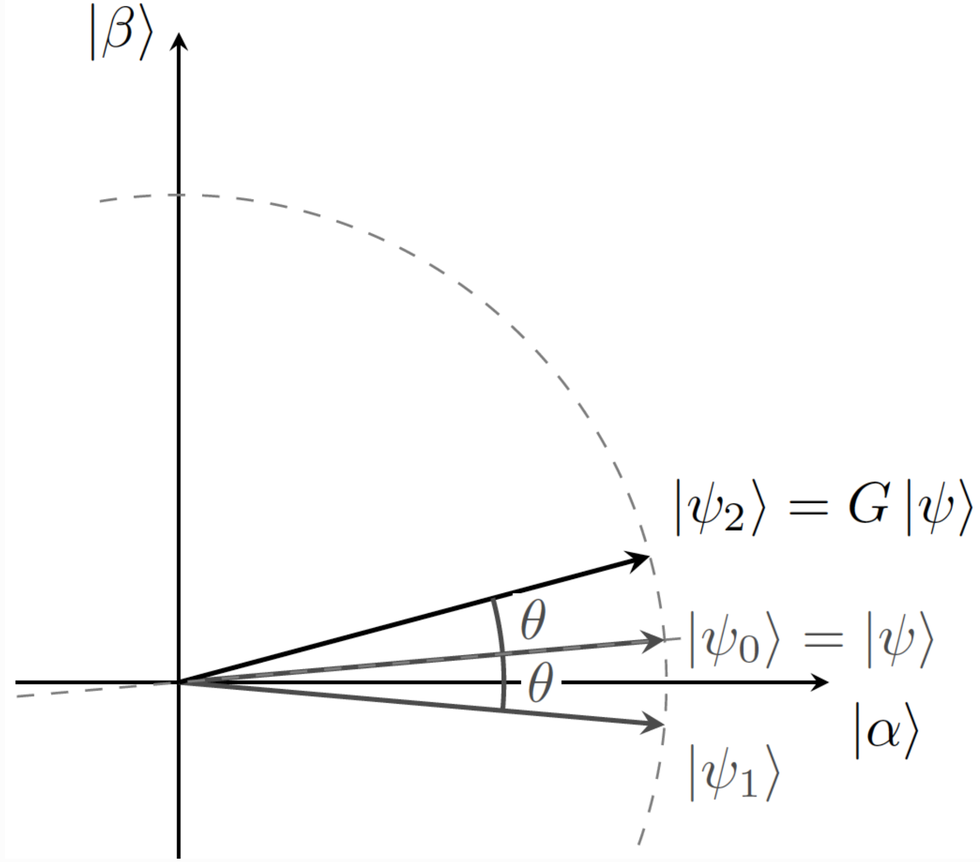
Reflection with respect to the axis

...

$$|\psi_2\rangle = (2\,|\psi\rangle\langle\psi| - I)\,|\psi_1\rangle$$
$$= 2\,|\psi\rangle\langle\psi|\,|\psi_1\rangle - |\psi_1\rangle$$



Reflexion with respect to the axis determined by the vector $|\psi\rangle$



State of the system after the first application of the Grover's operator

$$\cos\frac{\theta}{2} = \langle\alpha\,|\,\psi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}$$

Interpreting the Grover's operator

$$G = (2\,|\psi\rangle\langle\psi| - I)O_F$$

O_F mark the target state with a phase (-1).

Decomposing the identity operator as $I = |\psi\rangle\langle\psi| + |\psi_\perp\rangle\langle\psi_\perp|$, we have

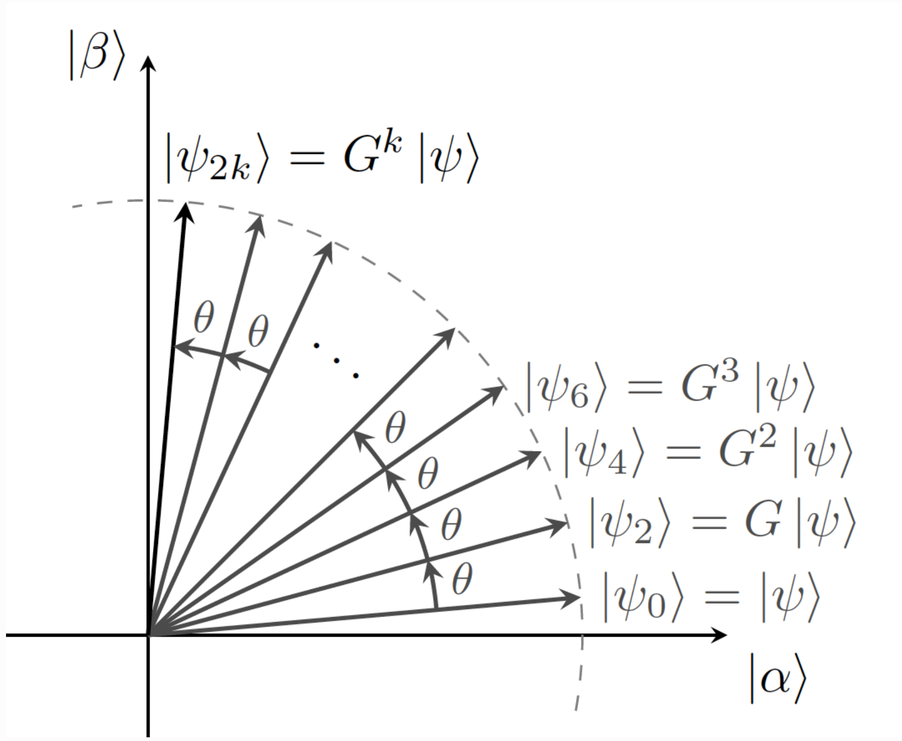
$$-(2\,|\psi\rangle\langle\psi| - I) = -\,|\psi\rangle\langle\psi| + |\psi_\perp\rangle\langle\psi_\perp| = -\,|\psi\rangle\langle\psi| + |\psi_\perp\rangle\langle\psi_\perp| = O_\psi$$

O_F mark the initial state with a phase (-1).

Therefore,

$$G = -\,O_\psi O_F$$

After successive applications of the Grover's operator, we have



To achieve the target state after k steps, we impose

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2} \implies k = \frac{\pi - \theta}{2\theta}$$

Different expressions of θ will be useful to obtain k.

$$\cos\frac{\theta}{2} = \frac{\sqrt{N-1}}{\sqrt{N}} \Rightarrow \sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \Rightarrow \theta = 2\arcsin\frac{1}{\sqrt{N}}$$

For large $N \Rightarrow \theta \ll 1$, we obtain

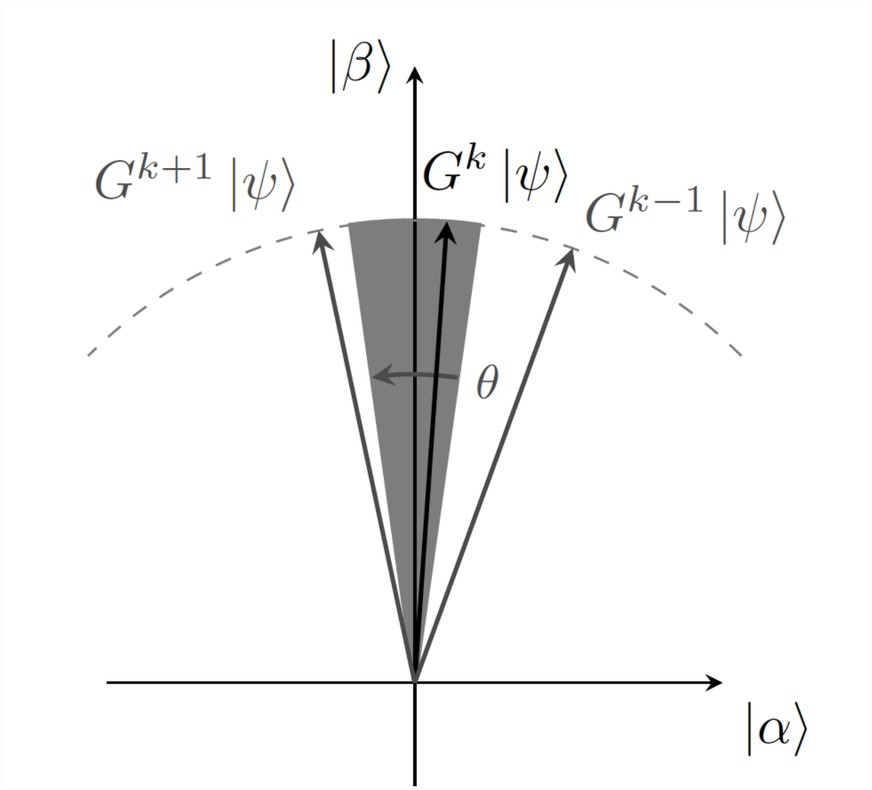
$$\theta \approx \frac{2}{\sqrt{N}} + O(N^{-3/2})$$

Then, the number of oracle queries is $k = \frac{\pi}{4}\sqrt{N}$

The success probability of achieving $|\beta\rangle = |x_0\rangle$ after $O(\sqrt{N})$ steps is

$$
\begin{aligned}
P_a &= \left\| |x_0\rangle\langle x_0| \, G^k \, |\psi\rangle \right\|^2 \\
&= \left| \langle x_0 | G^k \, |\psi\rangle \rangle \right|^2 \\
&= \left| \cos\theta \left(\, |x_0\rangle \, , G^k \, |\psi\rangle \, \right) \right|^2 \\
&> \left| \cos\theta/2 \right|^2 \\
&= \left(\frac{\sqrt{N-1}}{\sqrt{N}} \right)^2 \\
&= \frac{N-1}{N} \, , \quad N = 2^n \, .
\end{aligned}
$$

Very close to 1 for large N.



If we give more or less steps than k, the projection of the final state on the desired state becomes smaller.

Grover's algorithm is optimal.