Grover's algorithm

and

applications

by

Alain Tapp

DIRO
Université de Montréal
email: tappa@iro.umontreal.ca http://www.iro.umontreal.ca/~tappa/

Plan

1. P and NP

2. Grover's iteration

3. Search algorithm

4. Applications

5. Heuristics

6. Approximate counting

7. Applications

P

Definition: The class **P** is the class of problems that can be solved by an algorithm running in polynomial time.

The running time of an algorithm is a function of the input size.

Computer scientists like polynomials.

$$p(n) + q(n) = r(n)$$

$$p(n)q(n) = s(n)$$

$$p(q(n)) = t(n)$$

Where p, q, r, s and t are polynomials.

P is more or less the class of problems that we can hope to solve for a reasonably sized input.

In computer science, complexity classes are defined as languages. Formally, the above class is **FP**.

NP

A set S is in **NP** if there is a polynomial time algorithm F such that

$$\forall w \in S, \exists x, F(w,x) = 1$$

$$\forall w \notin S, \forall x, F(w,x) = 0$$

Problems in **NP** can be called puzzles for obvious reasons.

Examples of NP problems

Scheduling:
Given a set of constraints C find a schedule s without conflicts. Thus $F(C, s) = 1$ iff s is a schedule without conflicts in C.

Travelling salesman:
Given a fixed budget c and the cost to travel between a list of cities C, give a tour t with cost less than the budget c. Thus $F((C, c), t) = 1$ iff t is an appropriate tour.

Knapsack:
Given a list of objects L with their weights and values, is it possible to find a subset with value at least v and with a total weight of w. Thus $F((L, v, w), s) = 1$ iff s is appropriate.

Satisfiability:
Given a Boolean expression E, give an assignment to the Boolean variables x_i such that $E(x_1, \ldots, x_n) = 1$. Thus $F(E, x) = 1$ iff $E(x) = 1$.

NP-Complete problems

A set is **NP**-Complete if it is in **NP** and every set in **NP** reduces to it in polynomial time.

If you can solve an NP-Complete problem in polynomial time, then you can solve **ALL** problems in **NP** in polynomial time.

If this is the case we have that **P=NP**.

All the **NP** examples that I gave are actually **NP**-Complete.

There are several hundred problems that are known to be **NP**-Complete.

P=NP? is the most important open question in computer science.

There is a prize of 1000000$ for a solution.

Search Problem

Searching a database

Given a table T and an entry y,
find i such that $T[i] = y$.

Searching under computable constraints

Given a boolean function $F : X \to \{0, 1\}$
find x such that $F(x) = 1$.

Note: It clearly relates to **NP** problems.

Quantum circuits for f

To any function $f : X \to Y$ we can associate a unitary transformation

$$F\left|x\right\rangle\left|y\right\rangle := \left|x\right\rangle\left|y \oplus f(x)\right\rangle.$$

Clearly $F = F^\dagger$, $FF^\dagger = FF = I$. Also

$$F\left|x\right\rangle\left|0\right\rangle := \left|x\right\rangle\left|f(x)\right\rangle$$

The quantum circuit that computes F has roughly twice the number of gates than the classical circuit computing f.

If f is a binary function, we can also define

$$F'\left|x\right\rangle := (-1)^{f(x)}\left|x\right\rangle$$

again $F' = F'^\dagger$ and $F'F'^\dagger = F'F' = I$.

Quantum circuit for f (2)

$$F\,|x\rangle\,|y\rangle := |x\rangle\,|y \oplus f(x)\rangle$$

$$F'\,|x\rangle := (-1)^{f(x)}\,|x\rangle$$

From F, we can construct F' by choosing

$$|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Quantum circuit for f (3)

If $f(x) = 0$...

$$\begin{aligned}
F\left|x\right\rangle \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) &= \frac{1}{\sqrt{2}}(F\left|x\right\rangle\left|0\right\rangle - F\left|x\right\rangle\left|1\right\rangle) \\
&= \frac{1}{\sqrt{2}}(\left|x\right\rangle\left|0\right\rangle - \left|x\right\rangle\left|1\right\rangle) \\
&= \left|x\right\rangle \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \\
&= (-1)^{f(x)}\left|x\right\rangle \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \\
&= (F'\left|x\right\rangle)\ \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)
\end{aligned}$$

Quantum circuit for f (4)

If $f(x) = 1\ldots$

$$\begin{aligned}
F\left|x\right\rangle \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) &= \frac{1}{\sqrt{2}}(F\left|x\right\rangle\left|0\right\rangle - F\left|x\right\rangle\left|1\right\rangle) \\
&= \frac{1}{\sqrt{2}}(\left|x\right\rangle\left|1\right\rangle - \left|x\right\rangle\left|0\right\rangle) \\
&= \left|x\right\rangle \frac{1}{\sqrt{2}}(\left|1\right\rangle - \left|0\right\rangle) \\
&= -\left|x\right\rangle \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \\
&= (-1)^{f(x)}\left|x\right\rangle \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \\
&= (F'\left|x\right\rangle)\ \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)
\end{aligned}$$

Grover's algorithm for $N=4$

Let $f : \{0,1\}^2 \to \{0,1\}$ with the promise that there exists exactly one x_0 such that $f(x_0) = 1$.

We assume that the computation of f takes one day!

Let's define the unitary transformation U by

$$\begin{aligned}
U|00\rangle &= \frac{1}{2}(-|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\
U|01\rangle &= \frac{1}{2}(+|00\rangle - |01\rangle + |10\rangle + |11\rangle) \\
U|10\rangle &= \frac{1}{2}(+|00\rangle + |01\rangle - |10\rangle + |11\rangle) \\
U|11\rangle &= \frac{1}{2}(+|00\rangle + |01\rangle + |10\rangle - |11\rangle)
\end{aligned}$$

Clearly this is unitary since the 4 states on the right are orthonormal.

Grover's algorithm for N=4

The computation of F' takes two days.

Grover(f)

- $|\psi\rangle = U^{\dagger} F' H^{\otimes 2} |00\rangle$
- $m =$ Measure($|\psi\rangle$)
- return m

Grover's algorithm for N=4

If, for example, we have $x_0 = 10 (= 2)$, we get

$$
\begin{aligned}
|\psi\rangle &= U^\dagger F' H^{\otimes 2} |00\rangle \\
|\psi\rangle &= U^\dagger F' \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\
|\psi\rangle &= U^\dagger \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle) \\
|\psi\rangle &= |10\rangle
\end{aligned}
$$

In two days, any classical algorithm will have probability $1/2$ of failure.

The quantum algorithm succeeds with certainty.

Grover's Algorithm

Grover(f, m)

$|\Psi\rangle \leftarrow H\,|0\rangle$

Do m times

$$|\Psi\rangle \leftarrow G_f\,|\Psi\rangle$$

Measure $|\Psi\rangle$ and output its value.

$$G_f = -HSHF'$$

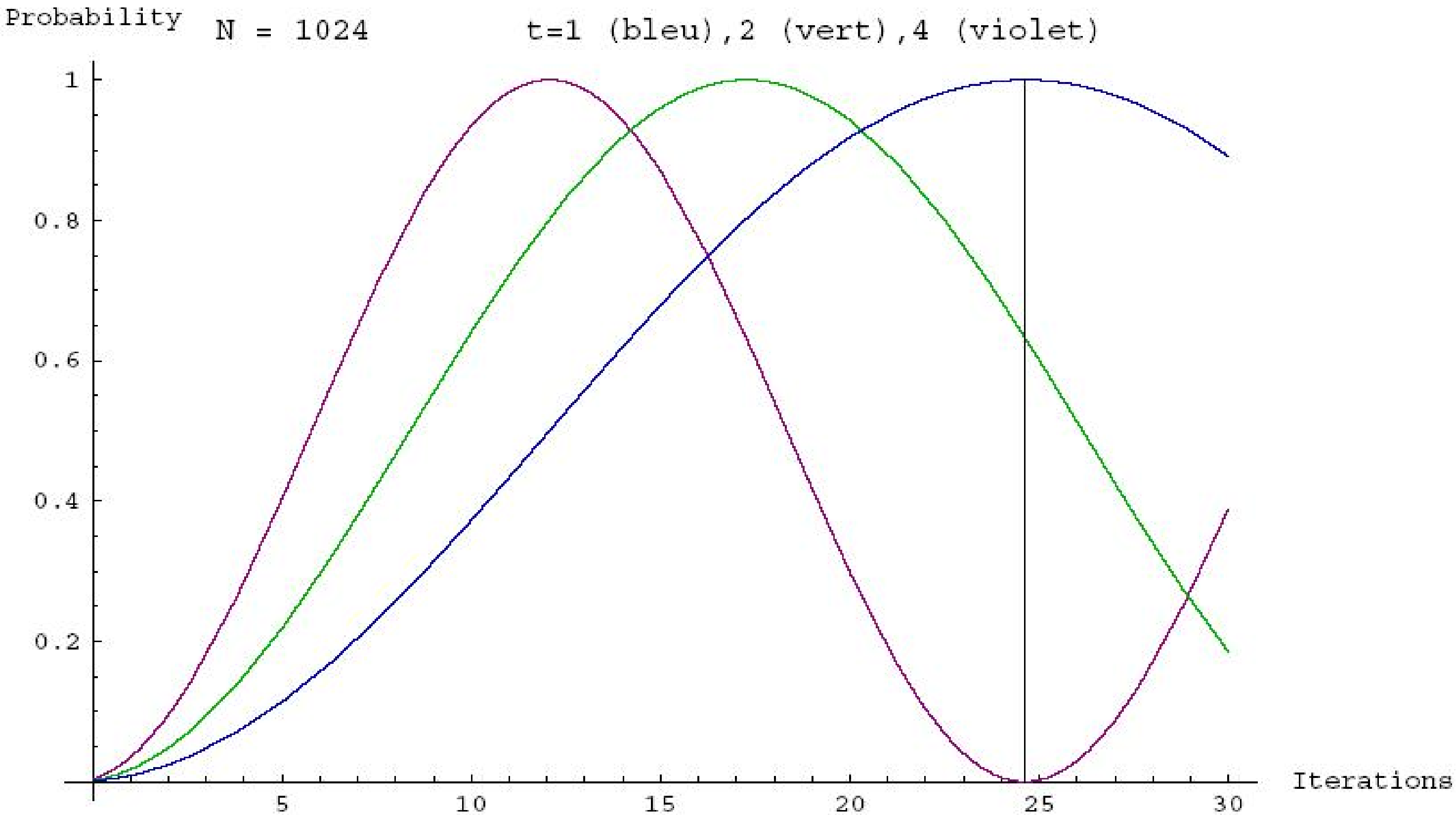
$$S|i\rangle = \begin{array}{rl} -|i\rangle & \text{if } i = 0 \\ |i\rangle & \text{otherwise.} \end{array}$$

$$F'|i\rangle = \begin{array}{rl} -|i\rangle & \text{if } f(i) = 1 \\ |i\rangle & \text{otherwise.} \end{array}$$

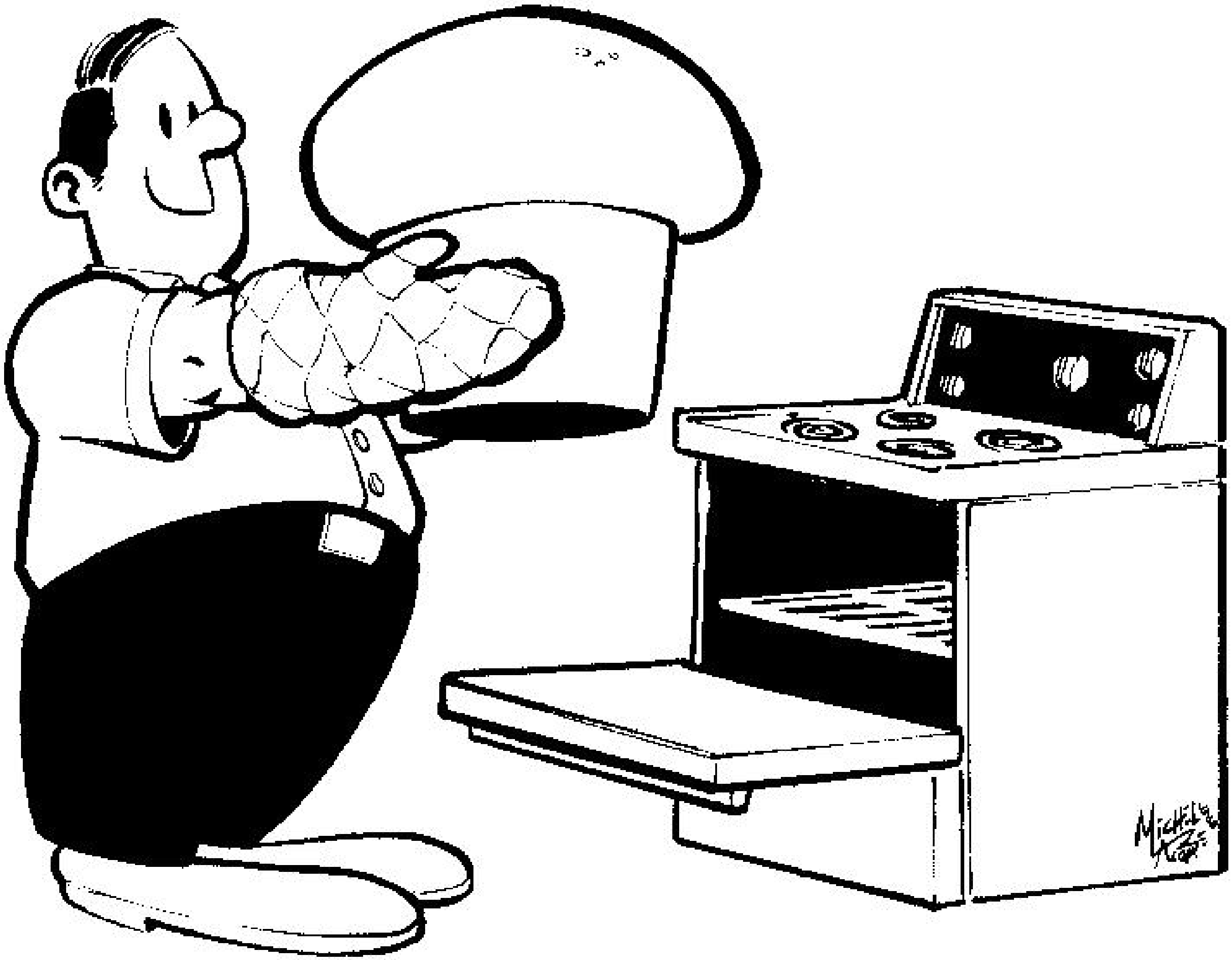
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{i \cdot j} |i\rangle$$

Success probability



Soufflé



Intuition

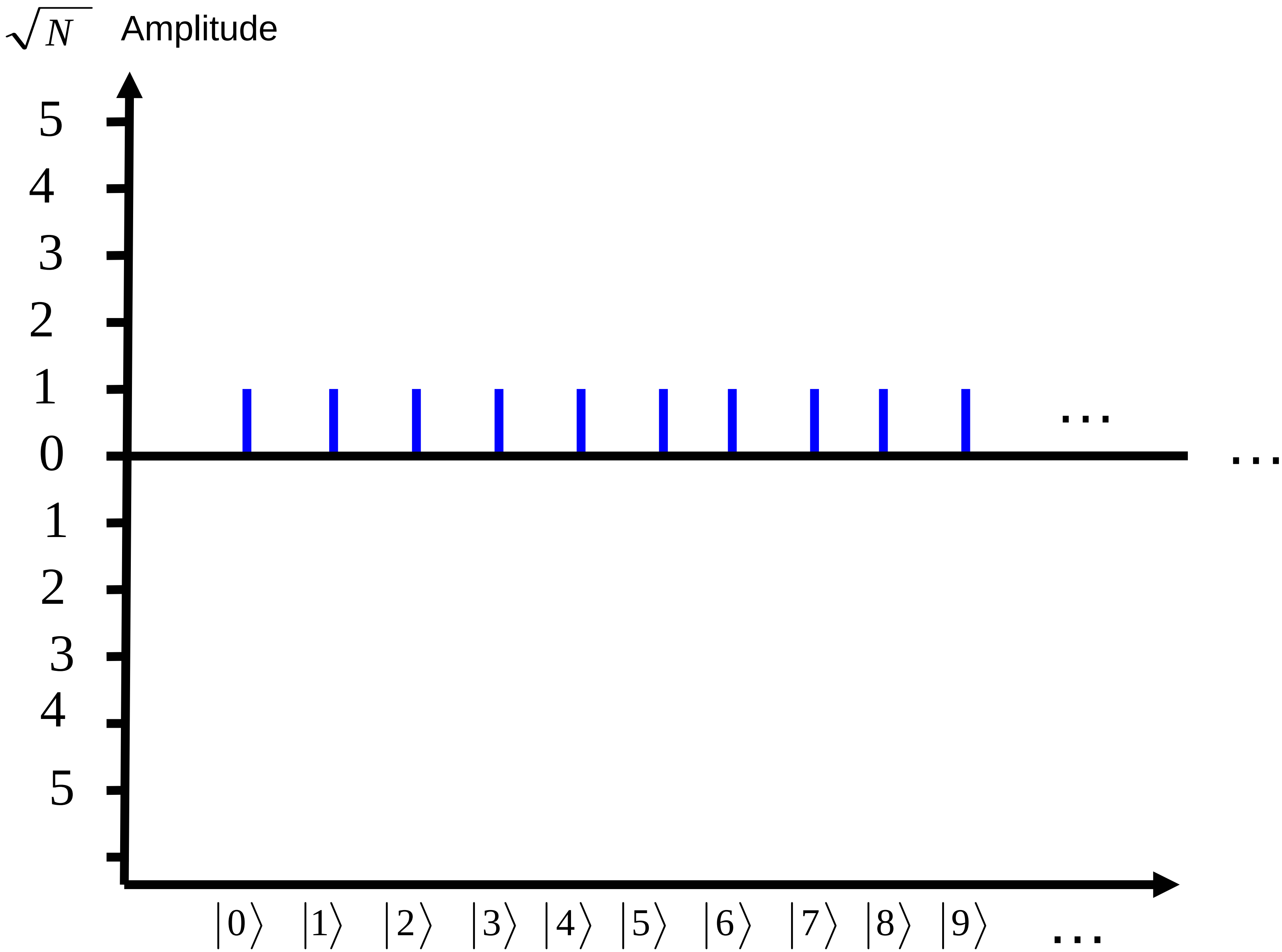
The algorithm is composed of two parts.

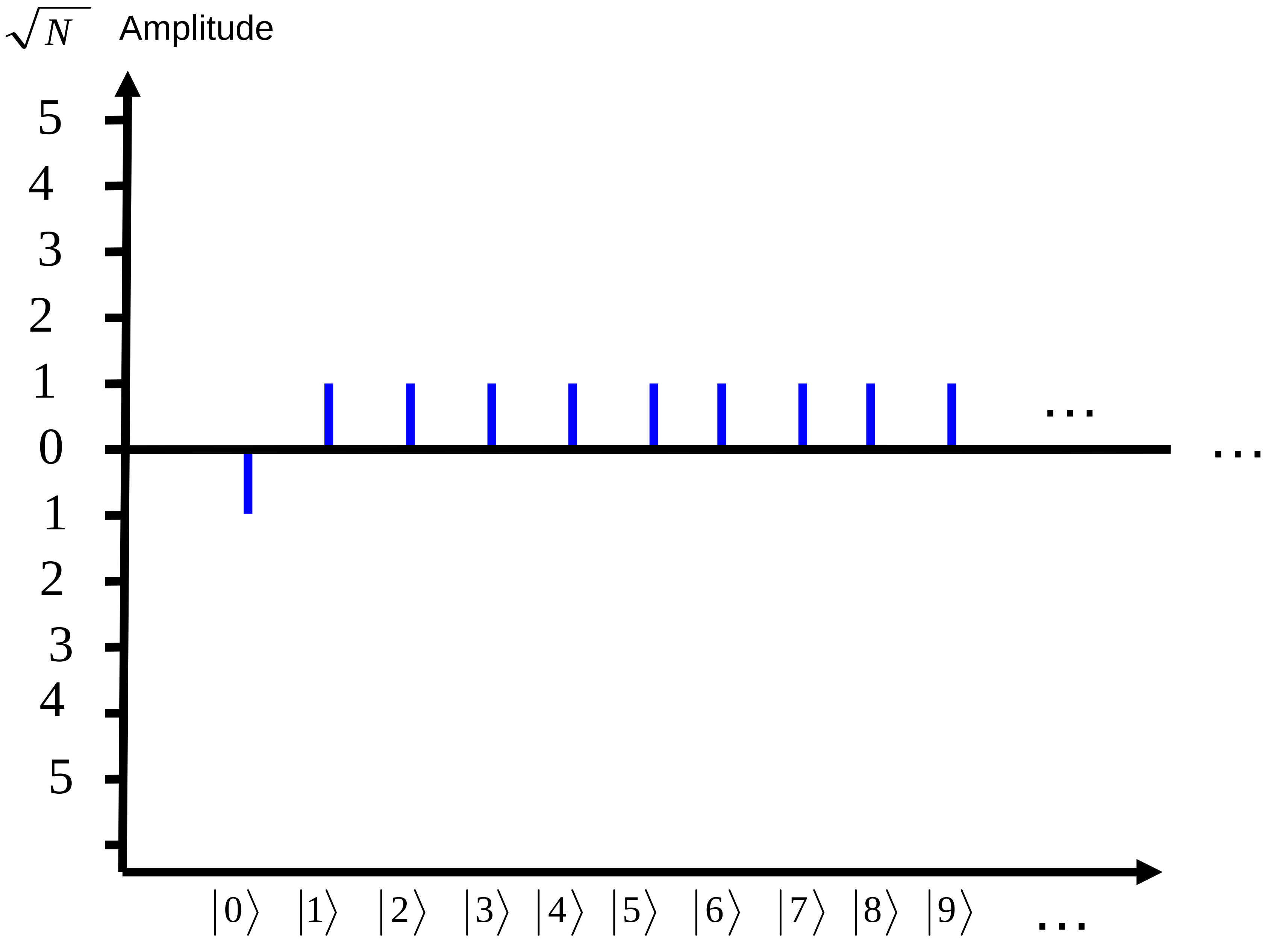
$$F'$$

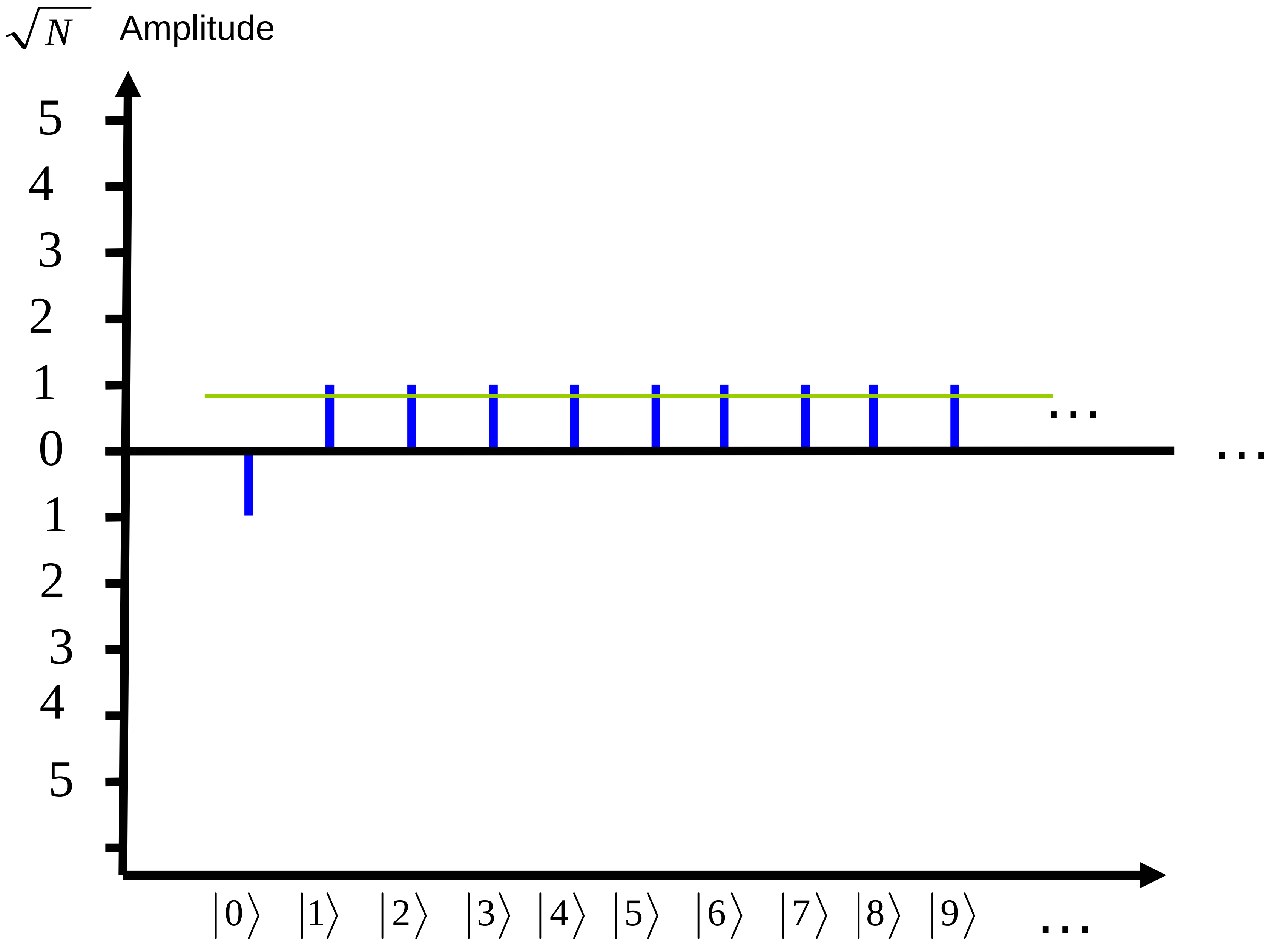
This is going to flip the sign of the solution and

$$-(HSH)$$

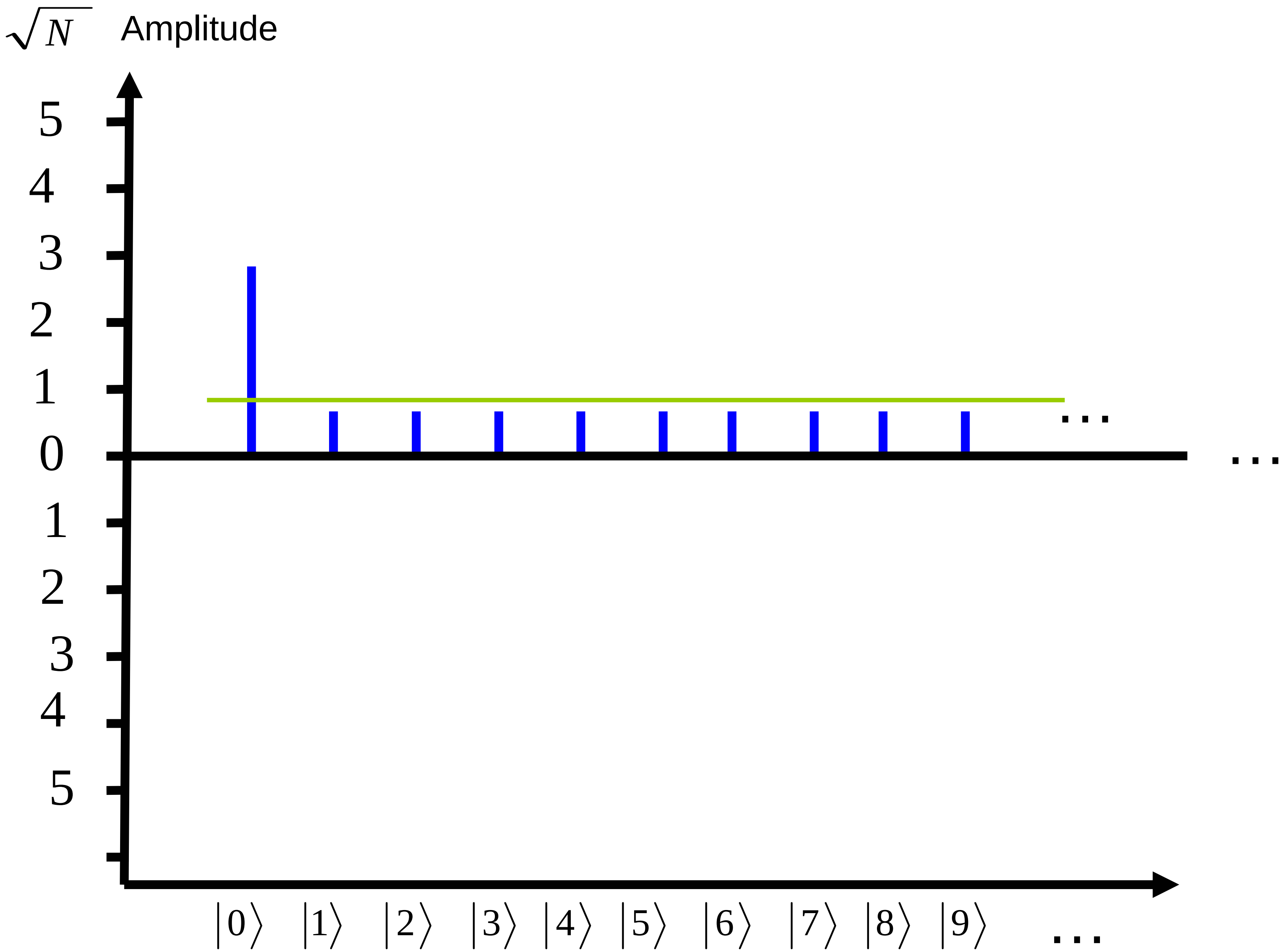
This is going to flip all amplitudes (exactly) over the line defined by the average of all amplitudes.


$\sqrt{N}$ Amplitude
5
4
3
2
1
0
1
2
3
4
5
...
...
$|0\rangle$ $|1\rangle$ $|2\rangle$ $|3\rangle$ $|4\rangle$ $|5\rangle$ $|6\rangle$ $|7\rangle$ $|8\rangle$ $|9\rangle$ ...

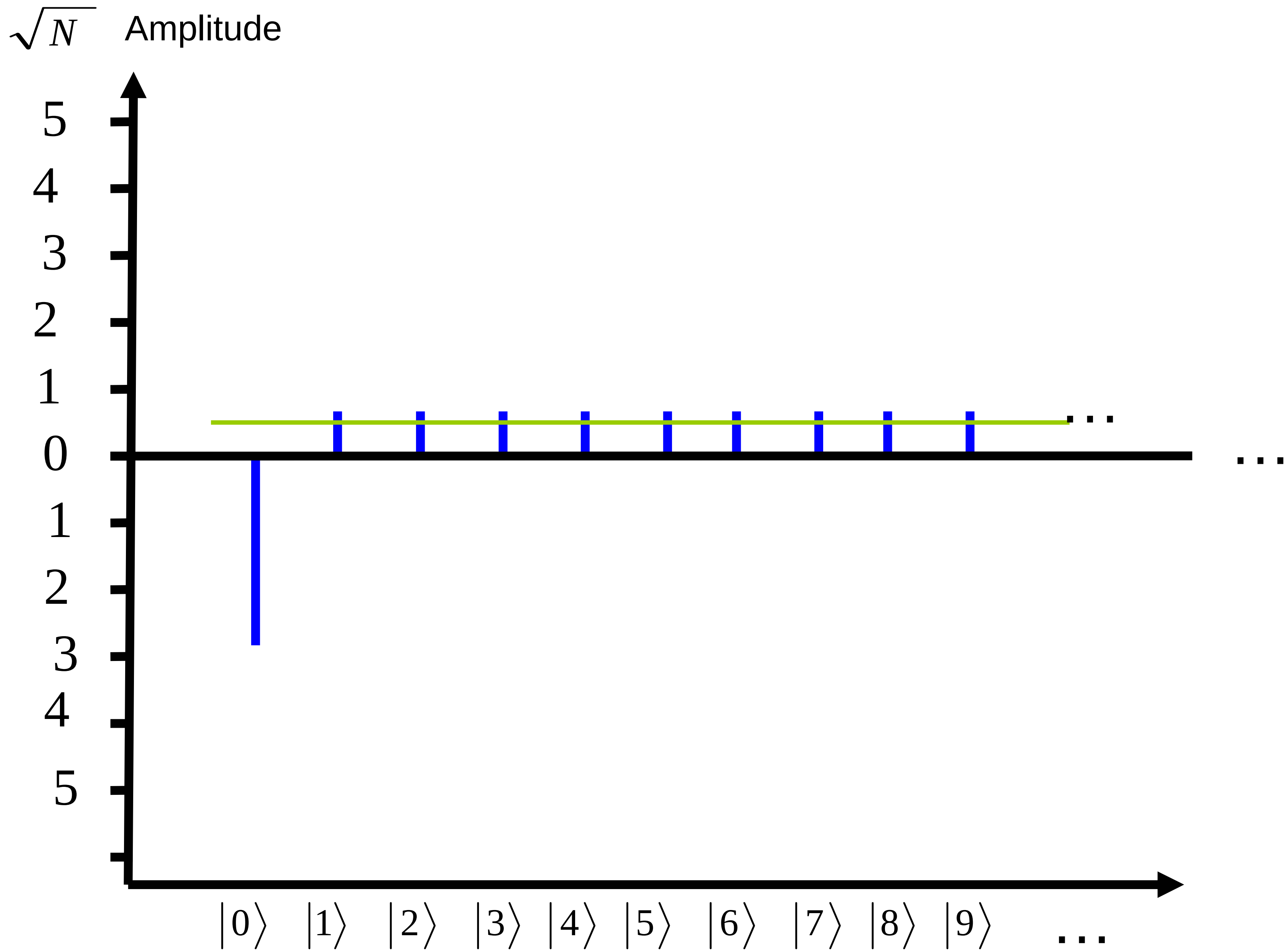

$\sqrt{N}$ Amplitude
5
4
3
2
1
0
1
2
3
4
5
...
...
$|0\rangle$ $|1\rangle$ $|2\rangle$ $|3\rangle$ $|4\rangle$ $|5\rangle$ $|6\rangle$ $|7\rangle$ $|8\rangle$ $|9\rangle$ ...



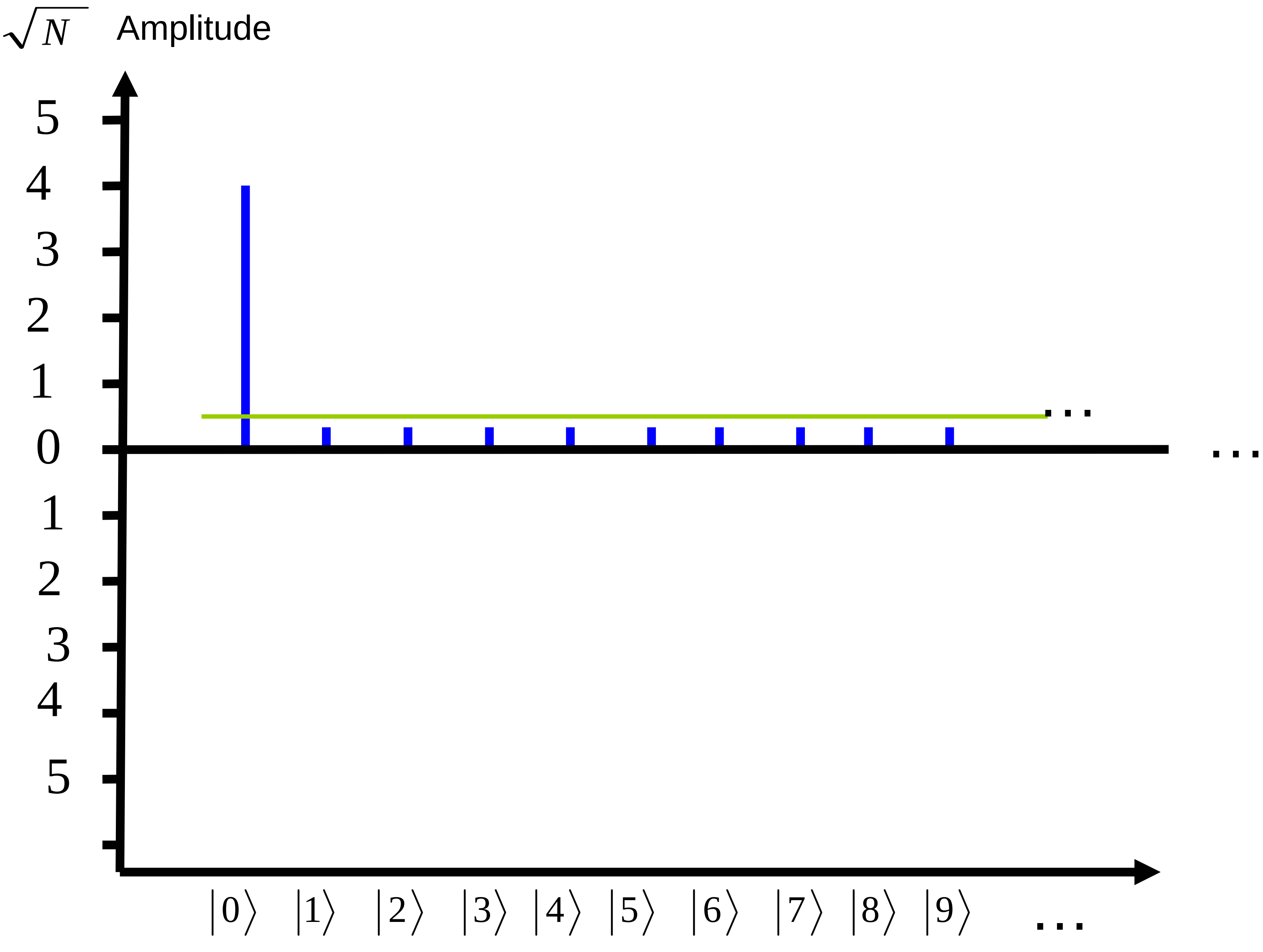
$\sqrt{N}$ Amplitude
5
4
3
2
1
0
1
2
3
4
5
...
...
$|0\rangle$ $|1\rangle$ $|2\rangle$ $|3\rangle$ $|4\rangle$ $|5\rangle$ $|6\rangle$ $|7\rangle$ $|8\rangle$ $|9\rangle$ ...



$\sqrt{N}$ Amplitude
5
4
3
2
1
0
1
2
3
4
5
...
...
$|0\rangle$ $|1\rangle$ $|2\rangle$ $|3\rangle$ $|4\rangle$ $|5\rangle$ $|6\rangle$ $|7\rangle$ $|8\rangle$ $|9\rangle$ ...



$\sqrt{N}$ Amplitude
5
4
3
2
1
0
1
2
3
4
5
$|0\rangle$ $|1\rangle$ $|2\rangle$ $|3\rangle$ $|4\rangle$ $|5\rangle$ $|6\rangle$ $|7\rangle$ $|8\rangle$ $|9\rangle$ ...


$\sqrt{N}$ Amplitude
5
4
3
2
1
0
1
2
3
4
5
...
...
$|0\rangle$ $|1\rangle$ $|2\rangle$ $|3\rangle$ $|4\rangle$ $|5\rangle$ $|6\rangle$ $|7\rangle$ $|8\rangle$ $|9\rangle$ ...

Intuition

If N is very large, at the first iteration, the amplitude of the good state will go from

$$\frac{1}{\sqrt{N}} \Rightarrow \frac{3}{\sqrt{N}}.$$

In the second iteration, it will move from

$$\frac{3}{\sqrt{N}} \Rightarrow \frac{5}{\sqrt{N}}.$$

If each iteration behaved in the same way, $\frac{\sqrt{N}}{2}$ iterations would be enough to increase the amplitude close to one.

Intuition

Unfortunately, when the amplitude of the good state grows, the amplitude of the bad state decreases and so after some number of iterations we will not have a full $2/\sqrt{N}$ increase in the amplitude.

Although incorrect, this intuitive argument gives a number of iteration that is close to the correct one.

Let's do the math!

Iteration analysis

$$N = |X| \qquad t = |\{x \in X | f(x) = 1\}|$$

$$|A\rangle = \sum_{f(x)=1} |x\rangle \qquad |B\rangle = \sum_{f(x)=0} |x\rangle$$

$$|A\rangle + |B\rangle = \sum_{x \in X} |x\rangle$$

$$\langle A|A\rangle = t \qquad \langle B|B\rangle = N - t$$

$$H|0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in X} |x\rangle = \frac{1}{\sqrt{N}} |A\rangle + \frac{1}{\sqrt{N}} |B\rangle$$

$$S = I - 2|0\rangle\langle 0|$$

Iteration analysis

The initial state before the first iteration is

$$H|0\rangle \;=\; \frac{1}{\sqrt{N}}\sum_{x\in X}|x\rangle \;=\; \frac{1}{\sqrt{N}}|A\rangle + \frac{1}{\sqrt{N}}|B\rangle$$

Solve:

$$G_f^m(H|0\rangle) = k_m|A\rangle + \ell_m|B\rangle$$

Iteration analysis (2)

$$
\begin{aligned}
G_f |\Psi\rangle &= -HSHF' \;\; (k|A\rangle + \ell|B\rangle) \\
&= HSH \;\; (k|A\rangle - \ell|B\rangle) \\
&= H(I - 2|0\rangle\langle 0|)H \;\; (k|A\rangle - \ell|B\rangle) \\
&= (I - \frac{2}{N}(|A\rangle + |B\rangle)(\langle A| + \langle B|)) \;\; (k|A\rangle - \ell|B\rangle) \\
&= k|A\rangle - \ell|B\rangle + \left(-\frac{2t}{N}k + 2\frac{N-t}{N}\ell\right)(|A\rangle + |B\rangle) \\
&= \left(\frac{N-2t}{N}k + \frac{2(N-t)}{N}\ell\right)|A\rangle \\
&\quad + \left(\frac{-2t}{N}k + \frac{N-2t}{N}\ell\right)|B\rangle
\end{aligned}
$$

Theorem:

Let

$$\sin^2\theta = t/N$$

then

$$(G_f)^m(H\,|0\rangle) \;=\; k_m \sum_{f(x)=1} |x\rangle + \ell_m \sum_{f(x)=0} |x\rangle$$

where

$$k_m \;=\; \frac{\sin((2m+1)\theta)}{\sqrt{t}}$$

$$\ell_m \;=\; \frac{\cos((2m+1)\theta)}{\sqrt{N-t}}$$

Proof:

By induction...

When $t = N/4$

$$\sin(\theta)^2 \;=\; \frac{t}{N} = \frac{1}{4}$$

Thus

$$\theta \;=\; \frac{\pi}{6}$$

and

$$k_1 \;=\; \frac{\sin((2m+1)\theta)}{\sqrt{t}} \;=\; \frac{\sin(\pi/2)}{\sqrt{N/4}} \;=\; \frac{1}{\sqrt{N/4}}$$

therefore the success probability after one iteration is

$$t\;|k_1|^2 \;=\; (N/4)\frac{1}{N/4} \;=\; 1$$

When t is known

Theorem:
When

$$m \;=\; \lfloor \frac{\pi}{\text{arcsin}\left(\sqrt{t/N}\right)} \rfloor \in O(\sqrt{N/t})$$

Grover(f, m) outputs x such that $f(x) = 1$ with probability at least $\frac{N-t}{N}$.

Proof:
From the previous theorem, the success probability is maximal when $\tilde{m} = (\pi - 2\theta)/4\theta$. Let $m = \lfloor \frac{\pi}{4\theta} \rfloor$ then $|m - \tilde{m}| \leq 1/2$ and $|(2m+1)\theta - (2\tilde{m}+1)\theta| \leq \theta$ and so $|\cos((2m+1)\theta)| \leq |\sin(\theta)|$.
Finally $(N-t)l_m^2 = \cos((2m+1)\theta)^2 \leq \sin(\theta)^2 = t/N$.

When t is unknown

Theorem:
There exists a quantum algorithm **Search** that given f with $t > 0$ finds x such that $f(x) = 1$ with expected time in $O(\sqrt{N/t})$.

Search(f)

1. $m = 1, \lambda = 8/7$
2. $j \in_R \{0, \ldots, m-1\}$
3. $x =$**Grover**(f, j)
4. If $f(x) = 1$ then output x and stop
5. $m = min(\lambda m, \sqrt{N})$
6. goto step 2.

Note: we can add a threshold of $O(\sqrt{N})$ if we are not sure that there is a solution.

Minimum

Theorem:
There exists an algorithm **Minimum** that finds x_0 such that $\forall x,\ T(x) \geq T(x_0)$, with probability 1/2, with an expected $O(\sqrt{N})$ calls to T.

Minimum(T)

1. $x_0 \in_R \{0, \ldots, N-1\}$
2. Define F such that $F(x) = 1 \Leftrightarrow T(x) < T(x_0)$
3. $x_1 =$ **Search**(F)
4. If $T(x_1) < T(x_0)$ then $x_0 \leftarrow x_1$
5. If the cumulative number of calls to T is less than $25\sqrt{N}$ goto step 2
6. Output x_0.

Collision

Theorem:
Given $G : X \to Y$ a two-to-one function with $|X| = N$, the algorithm **Collision** finds (x_0, x_1) such that $G(x_0) = G(x_1)$ in time and space $O(\sqrt[3]{N})$.

Collision(G)

1. For i from 1 to $\sqrt[3]{N}$ set T[i]=(i,G(i)).
2. Sort T and look for a collision in T
3. Define $F(x) = 1 \Leftrightarrow (x \geq \sqrt[3]{N}$ and $G(x) \in T)$
4. Set x_0 =**Search**(F) and x_1 such that $G(x_1) = G(x_0)$
5. Output (x_0, x_1).

Examples of heuristics

Hill-Climbing: local variations that increase an objective function. Often very efficient!

Example: 3-Satisfiability, find assignment to $\{x_1, x_2, x_3, x_4\}$ that satisfies

$(\bar{x_1} \vee \bar{x_4} \vee \bar{x_2})(\bar{x_1} \vee x_2 \vee \bar{x_3})(\bar{x_2} \vee \bar{x_4} \vee x_3)$
$(x_1 \vee \bar{x_1} \vee x_4)(x_4 \vee x_3 \vee x_3)(\bar{x_3} \vee \bar{x_4} \vee \bar{x_2})$

Random assignment:
$x_1 = 1,\ x_2 = 1,\ x_3 = 1$ and $x_4 = 1$
satisfies 4 clauses
local variation $x_1 = 0$
satisfies 5 clauses
local variation $x_2 = 0$
satisfies all 6 clauses!

Heuristics

Let $\mathcal{F}$ be a family of functions of the form
$F : X \rightarrow \{0, 1\}$ and $\mathcal{D}$ a probability distribution over this family.

A **heuristic** is a function
$G : \mathcal{F} \times R \rightarrow X$.

Let $t_F = |\{x|F(x) = 1\}|$
and $h_F = |\{r|F(G(F, r)) = 1\}|$

A *good* heuristic is such that

$$E_{\mathcal{F}}\left(\frac{h_F}{|R|}\right) > E_{\mathcal{F}}\left(\frac{t_F}{|N|}\right)$$

Heuristics

Let $G'_F(r) = F(G(r, F))$

Algorithm:
Output $G(F,$ **Search**$(G'_F))$

Analysis:
Warning! In general

$$\left(\sum x_i\right)^{1/2} \leq \sum \sqrt{x_i}$$

but

$$\sum_{F \in \mathcal{F}} \sqrt{\frac{R}{t_F} P_F} = \sum_{F \in \mathcal{F}} \sqrt{\frac{R}{t_F} P_F} \sqrt{P_F} \leq$$

$$\left(\sum_{F \in \mathcal{F}} \frac{R}{t_F} P_F\right)^{1/2} \left(\sum_{F \in \mathcal{F}} P_F\right)^{1/2} = \left(\sum_{F \in \mathcal{F}} \frac{R}{t_F} P_F\right)^{1/2}$$

Counting

The amplitude is a periodic function.
The period is related to t.

When m varies from 0 to $P-1$
k_m draws r periods of a sine function.

$$k_m = \frac{\sin((2m+1)\theta)}{\sqrt{t}}$$

$$r = P\theta/\pi$$

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

Use Fourier analysis to evaluate r.

Basic Tools

Parameterize Grover's iteration

$$GI_F \;:\; |m\rangle \otimes |\Psi\rangle \rightarrow |m\rangle \otimes (G_F)^m\, |\Psi\rangle$$

Quantum Fourier Transform

$$QFT_P \;:\; |k\rangle \rightarrow \frac{1}{\sqrt{P}} \sum_{l=0}^{P-1} e^{2\pi i \frac{kl}{P}}\, |l\rangle \quad k \in Z_P$$

Note that:

$$QFT_P\, |0\rangle \;=\; \frac{1}{\sqrt{P}} \sum_{l=0}^{P-1} |l\rangle$$

Algorithm

Count(F, P)

1. $|\Psi_0\rangle \leftarrow |\mathbf{0}\rangle H^{\otimes n} |\mathbf{0}\rangle$
2. $|\Psi_1\rangle \leftarrow QFT_P \otimes I^{\otimes n} |\Psi_0\rangle$
3. $|\Psi_2\rangle \leftarrow GI_F |\Psi_1\rangle$
4. $|\Psi_3\rangle \leftarrow QFT_P^{-1} \otimes I^{\otimes n} |\Psi_2\rangle$
5. $\tilde{r} \leftarrow$ measure first register of $|\Psi_3\rangle$
6. Output: $\tilde{t} = N \sin^2 \frac{\tilde{r}\pi}{P}$ (and $\tilde{r}$ if needed)

$$
\begin{aligned}
|\Psi_0\rangle &= |\mathbf{0}\rangle\,|\mathbf{0}\rangle \\
|\Psi_1\rangle &= \left(\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}|y\rangle\right)\otimes\left(\frac{1}{\sqrt{N}}\sum_{x=X}|x\rangle\right) \\
&= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}|y\rangle\left(\frac{1}{\sqrt{t}}\sum_{F(x)=1}|x\rangle+\frac{1}{\sqrt{N-t}}\sum_{F(x)=0}|x\rangle\right) \\
|\Psi_2\rangle &= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}|y\rangle\left(k_m\sum_{F(x)=1}|x\rangle+\ell_m\sum_{F(x)=0}|x\rangle\right) \\
&\ \text{We observe } x \text{ such that } F(x)=1 \\
|\Psi_3\rangle &= \alpha\sum_{y=0}^{2^m-1}\sin((2y+1)\theta)\,|y\rangle \\
|\Psi_4\rangle &= a\,|f\rangle + b\,|2^m-f\rangle + c\,|R\rangle
\end{aligned}
$$

$$
\sin^2(\theta)=\frac{t}{N} \qquad f\simeq 2^m\theta/\pi \qquad t\simeq N\sin^2\left(\frac{f\pi}{2^m}\right)
$$

$$
\begin{aligned}
|\Psi_0\rangle &= |\mathbf{0}\rangle\,|\mathbf{0}\rangle \\
|\Psi_1\rangle &= \left(\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}|y\rangle\right)\otimes\left(\frac{1}{\sqrt{N}}\sum_{x=X}|x\rangle\right) \\
&= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}|y\rangle\left(\frac{1}{\sqrt{t}}\sum_{F(x)=1}|x\rangle+\frac{1}{\sqrt{N-t}}\sum_{F(x)=0}|x\rangle\right) \\
|\Psi_2\rangle &= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}|y\rangle\left(k_m\sum_{F(x)=1}|x\rangle+\ell_m\sum_{F(x)=0}|x\rangle\right) \\
&\quad \text{We observe } x \text{ such that } F(x)=0 \\
|\Psi_3\rangle &= \alpha\sum_{y=0}^{2^m-1}\cos((2y+1)\theta)\,|y\rangle \\
|\Psi_4\rangle &= a\,|f\rangle+b\,|2^m-f\rangle+c\,|R\rangle
\end{aligned}
$$

$$\sin^2(\theta)=\frac{t}{N} \qquad f\simeq 2^m\theta/\pi \qquad t\simeq N\sin^2\left(\frac{f\pi}{2^m}\right)$$

Counting
Main Theorem

Theorem (Counting):
For $\tilde{t} = \textbf{Count}(F, P)$ then

$$|t - \tilde{t}| < \frac{2\pi}{P}\sqrt{t(N-t)} + \frac{\pi^2}{P^2}N$$

with probability at least $\frac{8}{\pi^2}$.

Approximate Counting

Counting Problem: given $F : X \to \{0, 1\}$ with $|X| = N$ find $\tilde{t}$ a good estimate of $t = \{x|F(x) = 1\}$.

$\vert t - \tilde{t}\vert$	Quantum	Classical
$O(\sqrt{t})$	$O(\sqrt{N})$	$\Omega(N)$
ϵt	$O\left(\frac{1}{\epsilon}\sqrt{\frac{N}{t}}\right)$	$\Omega\left(\frac{N}{\epsilon^2 t}\right)$
< 1	$O(\sqrt{t(N-t)})$	$\Omega(N)$

Other Applications (Sum)

Corollary 4:
Let $F : X \to Y$ with $|X| = N$ and Y an ordered set of n-bit numbers between 0 and 1 and let

$$S = \sum_{i \in X} F(i).$$

There exists an algorithm **Sum** that output $\tilde{S}$ such that

$$|\tilde{S} - S| < \sqrt{S}$$

which runs in time $O(n^2\sqrt{N})$.

Other Applications (Sum)

Proof:
Let $F(i)_j$ be the jth bit of $F(i)$.

Sum(F, N, n) (Christoph Dürr 97)

1. $S \leftarrow 0$

2. For j ranging from 1 to n

   $S \leftarrow S + 2^j \textbf{Count}^n(F_j, \sqrt{N})$

3. Output S.

Other Applications (Selection)

Approximate Selection Problem:
Given $F : X \rightarrow Y$ with $|X| = N$ and k, find x_0 such that if $k' = |\{x|F(x) < F(x_0)\}|$ then $|k - k'| < 2\pi\sqrt{k} + \pi^2$.

Use binary search in combination with counting.

Can be solved in time $O(\log(N)^2\sqrt{N})$

References

Lov K. Grover, A fast quantum mechanical algorithm for database search, Proceedings of 28th Annual ACM Symposium on Theory of Computing, May 1996, pp. 212−219.
(quant-ph/9605043)

Michel Boyer, Gilles Brassard, Peter Høyer and Alain Tapp, Tight Bounds on Quantum Searching, Fortschritte der Physik, vol.46(4-5), 1998, pp. 493-505.
(quant-ph/9605034)

Gilles Brassard, Peter Høyer and Alain Tapp, Cryptology Column — Quantum Algorithm for the Collision Problem, ACM SIGACT News, Vol. 28, June 1997, pp. 14-19. Presented at LATIN'98.
(quant-ph/9705002)

References

Christoph Dürr and Peter Høyer, A Quantum Algorithm for Finding the Minimum
(quant-ph/9607014)

Gilles Brassard, Peter Høyer and Alain Tapp, Quantum Counting, 25th International Colloquium, ICALP'98, LNCS vol. 1443, Springer, pp.820-831,1998.
(quant-ph/9805082)

Gilles Brassard, Peter Høyer, Michele Mosca and Alain Tapp, Quantum Amplitude Amplification and Estimation, in Quantum Computation & Quantum Information Science, AMS Contemporary Math Series.
(quant-ph/0005055)