Setting an Exponential Separation between Quantum and Classical Computation

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

Table of Contents

Previously...

The Problem

Take a function $f : \{0, 1\} \to \{0, 1\}$

Either $f(0) = f(1)$ or $f(0) \neq f(1)$

Tell us whether the first or second case hold

Classically, need to run f twice. Quantumly, once is enough

Previously...

The Problem

Take a function $f : \{0,1\} \to \{0,1\}$

Either $f(0) = f(1)$ or $f(0) \neq f(1)$

Tell us whether the first or second case hold

Classically, need to run f twice. Quantumly, once is enough

Can we have more impressive differences in complexity?

Table of Contents

Global Phase Factor

Definition

Let $v, u \in \mathbb{C}^{2^n}$ be vectors. If $u = e^{i\theta} v$ we say that it is equal to v up to global phase factor $e^{i\theta}$

Theorem

$e^{i\theta} v$ and v are indistinguishable in the world of quantum mechanics

Proof sketch

Show that equality up to global phase is preserved by operators and normalisation + show that probability outcomes associated with v and $e^{i\theta} v$ are the same

Relative Phase Factor

Definition

We say that vectors $\sum_{x \in 2^n} \alpha_x |x\rangle$ and $\sum_{x \in 2^n} \beta_x |x\rangle$ differ by a relative phase factor if for all $x \in 2^n$

$$\alpha_x = e^{i\theta_x} \beta_x \qquad \text{(for some angle } \theta_x\text{)}$$

Example

Vectors $|0\rangle + |1\rangle$ and $|0\rangle - |1\rangle$ differ by a relative phase factor

Relative Phase Factor

Definition

We say that vectors $\sum_{x \in 2^n} \alpha_x |x\rangle$ and $\sum_{x \in 2^n} \beta_x |x\rangle$ differ by a relative phase factor if for all $x \in 2^n$

$$\alpha_x = e^{i\theta_x} \beta_x \qquad \text{(for some angle } \theta_x\text{)}$$

Example

Vectors $|0\rangle + |1\rangle$ and $|0\rangle - |1\rangle$ differ by a relative phase factor

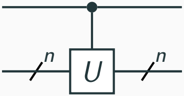
Vectors that differ by a relative phase factor are distinguishable

Table of Contents

The Phase Kickback Effect pt. I

Recall that every quantum operation 

gives rise to a controlled quantum operation, which is depicted below



Let v be an eigenvector of U (*i.e.* $Uv = e^{i\theta} v$) and calculate

$$\begin{aligned}
& cU\Big((\alpha\,|0\rangle + \beta\,|1\rangle) \otimes v\Big) \\
&= cU(\alpha\,|0\rangle \otimes v + \beta\,|1\rangle \otimes v) \\
&= \alpha\,|0\rangle \otimes v + \beta\,|1\rangle \otimes e^{i\theta} v \\
&= (\alpha\,|0\rangle + e^{i\theta}\beta\,|1\rangle) \otimes v
\end{aligned}$$

The Phase Kickback Effect pt. II

What just happened?

The Phase Kickback Effect pt. II

What just happened?

- Global phase $e^{i\theta}$ (introduced to v) was 'kickedback' as a relative phase in the control qubit

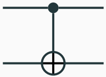
The Phase Kickback Effect pt. II

What just happened?

- Global phase $e^{i\theta}$ (introduced to v) was 'kickedback' as a relative phase in the control qubit
- Some information of U is now encoded in the control qubit

In general kickingback such phases causes interference patterns that give away information about U

Consider the controlled-not operation

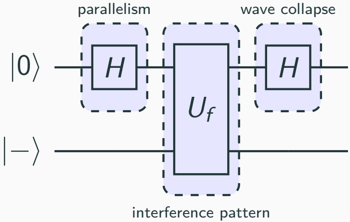


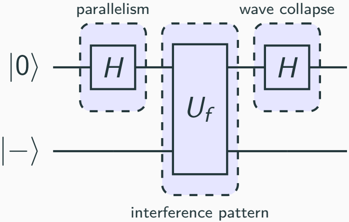
X has $|-\rangle$ as eigenvector with associated eigenstate -1. It thus yields the equation

$$cX\,|b\rangle\,|-\rangle = (-1)^b\,|b\rangle\,|-\rangle$$

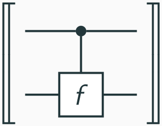
with $|b\rangle$ an element of the computational basis

Back to Deutsch's Problem



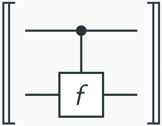


U_f can be seen as a generalised controlled not-operation



$$= |x\rangle\,|y\rangle \mapsto \begin{cases} |x\rangle\,|y\rangle & \text{if } f(x) = 0 \\ |x\rangle \neg |y\rangle & \text{if } f(x) = 1 \end{cases}$$

U_f can be seen as a generalised controlled not-operation



$$= |x\rangle\,|y\rangle \mapsto \begin{cases} |x\rangle\,|y\rangle & \text{if } f(x) = 0 \\ |y\rangle \neg\,|y\rangle & \text{if } f(x) = 1 \end{cases}$$

Recall that $|-\rangle$ is an eigenvector of X with eigenstate -1. Thus analogously to before we deduce

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

Back to Deutsch's Problem pt. III

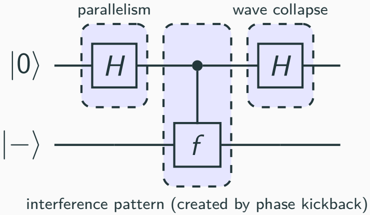


Table of Contents

Going Beyond the Current Separation

Albeit looking almost magical how we handled Deutsch's problem, the corresponding complexity difference between quantum and classical is unimpressive

Can we come up with a more impressive separation?

Setting the Stage

Lemma

For $a, b \in \{0, 1\}$ *the equation* $(-1)^a(-1)^b = (-1)^{a \oplus b}$ *holds*

Prook sketch

Build a truth table for each case and compare the corresponding contents

Definition

Given two bit-strings $x, y \in \{0, 1\}^n$ we define their product $x \cdot y \in \{0, 1\}$ as $x \cdot y = (x_1 \wedge y_1) \oplus \cdots \oplus (x_n \wedge y_n)$

Setting the Stage

Lemma

For any three binary strings $x, a, b \in \{0,1\}^n$ *the equation* $(x \cdot a) \oplus (x \cdot b) = x \cdot (a \oplus b)$ *holds*

Proof sketch

Follows from the fact that for any three bits $a, b, c \in \{0,1\}$ the equation $(a \wedge b) \oplus (a \wedge c) = a \wedge (b \oplus c)$ holds

Setting the Stage

Lemma

For any element $|b\rangle$ *in the computational basis of* $\mathbb{C}^2$ *we have* $H|b\rangle = \frac{1}{\sqrt{2}} \sum_{z \in 2} (-1)^{b \wedge z} |z\rangle$

Proof sketch

Build a truth table and compare the corresponding contents

Theorem

For any element $|b\rangle$ *in the computational basis of* $\mathbb{C}^{2^n}$ *we have* $H^{\otimes n}|b\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} (-1)^{b \cdot z} |z\rangle$

Proof sketch

Follows from induction on the size of n

Bernstein-Vazirani

The Problem

Take a function $f : \{0,1\}^n \to \{0,1\}$

You are promised that $f(x) = s \cdot x$ for some fixed bit-string s

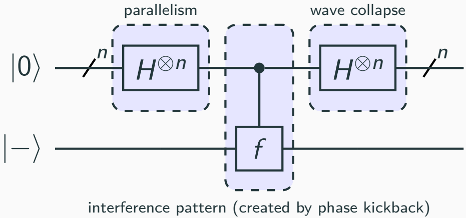
Find s

Classically, we run f n-times by computing

$$f(1\dots 0) = (s_1 \wedge 1) \oplus \cdots \oplus (s_n \wedge 0) = s_1$$
$$\vdots$$
$$f(0\dots 1) = (s_1 \wedge 0) \oplus \cdots \oplus (s_n \wedge 1) = s_n$$

Quantumly, we discover s by running f only once

The Circuit


parallelism
wave collapse
$|0\rangle$
n
$H^{\otimes n}$
$H^{\otimes n}$
n
$|-\rangle$
f
interference pattern (created by phase kickback)

The Computation

N.B. In order to not overburden notation we omit $|-\rangle$

$$H^{\otimes n}|0\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} |z\rangle \qquad \{\text{Theorem slide 18}\}$$
$$\overset{U_f}{\mapsto} \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} (-1)^{f(z)} |z\rangle \qquad \{\text{Definition slide 12}\}$$
$$\overset{H^{\otimes n}}{\mapsto} \frac{1}{2^n} \sum_{z \in 2^n} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big) \qquad \{\text{Theorem slide 18}\}$$
$$= \frac{1}{2^n} \sum_{z \in 2^n} \sum_{z' \in 2^n} (-1)^{(z \cdot s) \oplus (z \cdot z')} |z'\rangle \qquad \{\text{Lemma slide 16}\}$$
$$= \frac{1}{2^n} \sum_{z \in 2^n} \sum_{z' \in 2^n} (-1)^{z \cdot (s \oplus z')} |z'\rangle \qquad \{\text{Lemma slide 17}\}$$

The Computation pt. II

Probability of measuring s at the end given by

$$\left| \frac{1}{2^n} \sum_{z \in 2^n} (-1)^{z \cdot (s \oplus s)} |s\rangle \right|^2$$
$$= \left| \frac{1}{2^n} \sum_{z \in 2^n} (-1)^{z \cdot 0} |s\rangle \right|^2$$
$$= \left| \frac{1}{2^n} \sum_{z \in 2^n} 1 \, |s\rangle \right|^2$$
$$= \left| \frac{2^n}{2^n} \right|^2$$
$$= 1$$

This means that somehow all values yielding wrong answers were completely cancelled

T.P.C. Show exactly how all the wrong answers were cancelled

Going Even Further Beyond

We went from running f n times to running just once

Going Even Further Beyond

We went from running f n times to running just once

Still not very impressive (at least for the Computer Scientist :-))

Going Even Further Beyond

We went from running f n times to running just once

Still not very impressive (at least for the Computer Scientist :-))

Can we do even better?

Table of Contents

Deutsch-Josza

The Problem

Take a function $f : \{0,1\}^n \rightarrow \{0,1\}$

You are promised that f is either constant or balanced

Find out which case holds

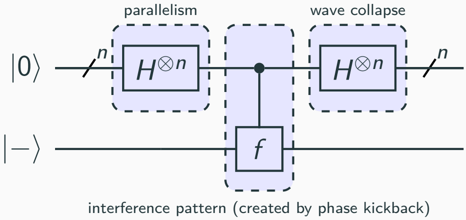
Classically, we evaluate half of the inputs ($\frac{2^n}{2} = 2^{n-1}$), evaluate one more and run the decision procedure,

- output always the same $\implies$ constant
- otherwise $\implies$ balanced

which requires running f $2^{n-1} + 1$ times

Quantumly, we know the answer by running f only once

The Circuit


parallelism
wave collapse
$|0\rangle$
n
$H^{\otimes n}$
$H^{\otimes n}$
n
$|-\rangle$
f
interference pattern (created by phase kickback)

The Computation

N.B. In order to not overburden notation we omit $|-\rangle$

$$H^{\otimes n}|0\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} |z\rangle \qquad \{\text{Theorem slide 18}\}$$
$$\overset{U_f}{\mapsto} \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} (-1)^{f(z)} |z\rangle \qquad \{\text{Definition slide 12}\}$$
$$\overset{H^{\otimes n}}{\mapsto} \frac{1}{2^n} \sum_{z \in 2^n} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big) \qquad \{\text{Theorem slide 18}\}$$

We then proceed by case distinction. Assume that f is constant

$$\frac{1}{2^n} \sum_{z \in 2^n} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$
$$= \frac{1}{2^n} (\pm 1) \sum_{z \in 2^n} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$

The Computation pt. II

Probability of measuring $|0\rangle$ at the end given by

$$\left|\frac{1}{2^n}(\pm 1)\sum_{z\in 2^n}(-1)^{z\cdot 0}\,|0\rangle\,\right|^2$$
$$= \left|\frac{1}{2^n}(\pm 1)\sum_{z\in 2^n} 1\,|0\rangle\,\right|^2$$
$$= \left|\frac{2^n}{2^n}\right|^2$$
$$= 1$$

So if f is constant we measure $|0\rangle$ with probability 1. Now if f is balanced...

The Computation pt. III

$$\frac{1}{2^n} \sum_{z \in 2^n} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$

$$= \frac{1}{2^n} \Bigg(\sum_{z \in 2^n, f(z)=0} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$

$$+ \sum_{z \in 2^n, f(z)=1} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big) \Bigg)$$

$$= \frac{1}{2^n} \Bigg(\sum_{z \in 2^n, f(z)=0} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$

$$+ \sum_{z \in 2^n, f(z)=1} (-1) \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big) \Bigg)$$

The Computation pt. IV

Probability of measuring $|0\rangle$ at the end given by

$$\left|\tfrac{1}{2^n}\Big(\textstyle\sum_{z\in 2^n, f(z)=0}(-1)^{z\cdot 0}\,|0\rangle + \sum_{z\in 2^n, f(z)=1}(-1)(-1)^{z\cdot 0}\,|0\rangle\Big)\right|^2$$
$$= \left|\tfrac{1}{2^n}\Big(\textstyle\sum_{z\in 2^n, f(z)=0}|0\rangle + \sum_{z\in 2^n, f(z)=1}(-1)\,|0\rangle\Big)\right|^2$$
$$= \left|\tfrac{1}{2^n}\Big(\textstyle\sum_{z\in 2^n, f(z)=0}|0\rangle - \sum_{z\in 2^n, f(z)=1}|0\rangle\Big)\right|^2$$
$$= 0$$

So if f is balanced we measure $|0\rangle$ with probability 0

Table of Contents

Revisiting Deutsch-Josza

The Problem

Take a function $f : \{0,1\}^n \to \{0,1\}$. The latter either constant or balanced

Find out which case holds

Classically, evaluate half of the inputs ($\frac{2^n}{2} = 2^{n-1}$), evaluate one more and run the decision procedure,

- output always the same $\implies$ constant
- otherwise $\implies$ balanced

Quantumly, we know the answer by running f only once

Revisiting Deutsch-Josza

The Problem

Take a function $f : \{0,1\}^n \to \{0,1\}$. The latter either constant or balanced

Find out which case holds

Classically, evaluate half of the inputs ($\frac{2^n}{2} = 2^{n-1}$), evaluate one more and run the decision procedure,

- output always the same $\implies$ constant
- otherwise $\implies$ balanced

Quantumly, we know the answer by running f only once

However ...

Tackling Deutsch-Josza with Probabilities

To solve the problem with some margin of error evaluate two arbitrary inputs x and y,

- $f(x) = f(y) \implies$ constant
- $f(x) \neq f(y) \implies$ balanced

Tackling Deutsch-Josza with Probabilities

To solve the problem with some margin of error evaluate two arbitrary inputs x and y,

- $f(x) = f(y) \implies$ constant
- $f(x) \neq f(y) \implies$ balanced

Probability of giving the right answer?

Tackling Deutsch-Josza with Probabilities

To solve the problem with some margin of error evaluate two arbitrary inputs x and y,

- $f(x) = f(y) \implies$ constant
- $f(x) \neq f(y) \implies$ balanced

Probability of giving the right answer?

- f is constant $\implies$ right answer with probability 1
- f is balanced $\implies$ right answer with probability $\frac{2^{n-1}}{2^n} = \frac{1}{2}$

Tackling Deutsch-Josza with Probabilities

To solve the problem with some margin of error evaluate two arbitrary inputs x and y,

- $f(x) = f(y) \implies$ constant
- $f(x) \neq f(y) \implies$ balanced

Probability of giving the right answer?

- f is constant $\implies$ right answer with probability 1
- f is balanced $\implies$ right answer with probability $\frac{2^{n-1}}{2^n} = \frac{1}{2}$

Can we do better?

Tackling Deutsch-Josza with Probabilities pt. II

To solve the problem with some margin of error evaluate k arbitrary inputs $x_1, \ldots, x_k$,

- output always the same $\implies$ constant
- otherwise $\implies$ balanced

Tackling Deutsch-Josza with Probabilities pt. II

To solve the problem with some margin of error evaluate k arbitrary inputs $x_1, \ldots, x_k$,

- output always the same $\Longrightarrow$ constant
- otherwise $\Longrightarrow$ balanced

Probability of giving the right answer?

Tackling Deutsch-Josza with Probabilities pt. II

To solve the problem with some margin of error evaluate k arbitrary inputs $x_1, \dots, x_k$,

- output always the same $\Longrightarrow$ constant
- otherwise $\Longrightarrow$ balanced

Probability of giving the right answer?

- f is constant $\Longrightarrow$ right answer with probability 1
- f is balanced $\Longrightarrow$ right answer with probability ...

$$1 - \left(\frac{2^{n-1}}{2^n}\right)^k = 1 - \frac{1}{2^k}$$

Probability of observing the same output in k tries

The Problem

Take a 2-1 function $f : \{0,1\}^n \rightarrow \{0,1\}^n$

There exists a string $s \in \{0,1\}^n$ s.t. $f(x) = f(y) \Rightarrow y = x \oplus s$

Find out s

Classically, evaluate inputs until collision is detected, *i.e.* $f(x) = f(y)$ for some x, y. Then compute $x \oplus y = x \oplus (x \oplus s) = s$

Since f is 2-1, after collecting 2^{n-1} evaluations with no collisions, next evaluation must cause a collision

So in the worst case we need $2^{n-1} + 1$ evaluations

Tackling Simon with Probabilities

How many evaluations do we need to have a collision with probability p?

Tackling Simon with Probabilities

How many evaluations do we need to have a collision with probability p?

To have a collision with probability $p = \frac{1}{k} \leq \frac{1}{2}$ we need

$$\approx \sqrt{(2 \cdot 2^n) \cdot p} = \sqrt{\frac{2}{k} \cdot 2^n} = \sqrt{\frac{2}{k}} \cdot 2^{\frac{n}{2}} \quad \text{evaluations}$$

See the Birthday's problem

Tackling Simon with Probabilities

How many evaluations do we need to have a collision with probability p?

To have a collision with probability $p = \frac{1}{k} \leq \frac{1}{2}$ we need

$$\approx \sqrt{(2 \cdot 2^n) \cdot p} = \sqrt{\frac{2}{k} \cdot 2^n} = \sqrt{\frac{2}{k}} \cdot 2^{\frac{n}{2}} \quad \text{evaluations}$$

See the Birthday's problem

But quantumly, we solve the problem in polynomial time with probability $\approx \frac{1}{4}$

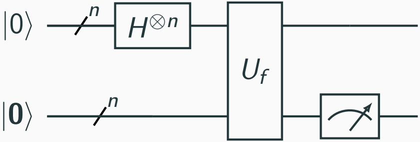
Simon's Algorithm: The Key Steps

1. Prepare superposition $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$ for some string x
2. Use interference to extract a string y s.t. $y \cdot s = 0$
3. Repeat previous steps $n - 1$ times to obtain system of equations s.t. $y_k \cdot s = 0$
4. Solve the system for s using Gaussian elimination

↓

Complexity n^3

Simon's Algorithm: Preparing the Superposition



N.B. $U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$

$$U_f(H^{\otimes n} \otimes I)\,|0\rangle\,|\mathbf{0}\rangle$$
$$= U_f\Big(\tfrac{1}{\sqrt{2^n}}\textstyle\sum_{x\in 2^n}|x\rangle\,|\mathbf{0}\rangle\Big)$$
$$= \tfrac{1}{\sqrt{2^n}}\textstyle\sum_{x\in 2^n}|x\rangle\,|f(x)\rangle$$

We then measure the n-bottom qubits to obtain a superposition

$$\tfrac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$$

Simon's Algorithm: Extracting the String

Simon's Algorithm: Extracting the String

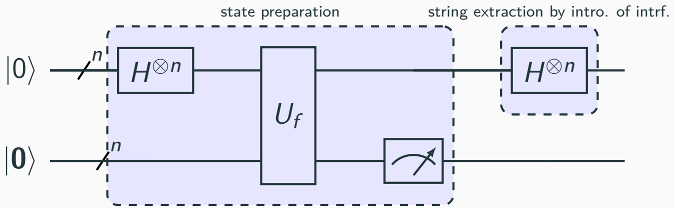
$$
\begin{aligned}
& H^{\otimes n} \tfrac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle) \\
&= \tfrac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y} |y\rangle + (-1)^{(x \oplus s)\cdot y} |y\rangle && \{\text{Theorem slide 18}\} \\
&= \tfrac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y} |y\rangle + (-1)^{x \cdot y \oplus s \cdot y} |y\rangle && \{\text{Lemma slide 17}\} \\
&= \tfrac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y} |y\rangle + (-1)^{x \cdot y}(-1)^{s \cdot y} |y\rangle && \{\text{Lemma slide 16}\} \\
&= \tfrac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y}(1 + (-1)^{s \cdot y}) |y\rangle
\end{aligned}
$$

Simon's Algorithm: Extracting the String

$$
\begin{aligned}
& H^{\otimes n}\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle) \\
&= \frac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y}\,|y\rangle + (-1)^{(x \oplus s)\cdot y}\,|y\rangle && \{\text{Theorem slide 18}\} \\
&= \frac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y}\,|y\rangle + (-1)^{x \cdot y \oplus s \cdot y}\,|y\rangle && \{\text{Lemma slide 17}\} \\
&= \frac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y}\,|y\rangle + (-1)^{x \cdot y}(-1)^{s \cdot y}\,|y\rangle && \{\text{Lemma slide 16}\} \\
&= \frac{1}{\sqrt{2^{n+1}}} \textstyle\sum_{y \in 2^n} (-1)^{x \cdot y}(1 + (-1)^{s \cdot y})\,|y\rangle
\end{aligned}
$$

Destructive interference when $s \cdot y = 1$. We only observe $|y\rangle$ s.t. $s \cdot y = 0$

The Circuit


state preparation
string extraction by intro. of intrf.
$|0\rangle$
$|\mathbf{0}\rangle$
n
n
$H^{\otimes n}$
U_f
$H^{\otimes n}$

Simon's Algorithm: Solving the System to Extract s

A system of $n-1$ linearly independent equations,

$$\begin{cases} y_1 \cdot s = 0 \\ \dots \\ y_{n-1} \cdot s = 0 \end{cases}$$

has two solutions. One is $s = 0$ but it violates the 2-1 promise. So only the other solution is of interest

Simon's Algorithm: Solving the System to Extract s

A system of $n-1$ linearly independent equations,

$$\begin{cases} y_1 \cdot s = 0 \\ \dots \\ y_{n-1} \cdot s = 0 \end{cases}$$

has two solutions. One is $s = 0$ but it violates the 2-1 promise. So only the other solution is of interest

Probability of obtaining such a system of equations by running the circuit $n-1$ times?

Simon's Algorithm: Probability of Success

Homework

If $s \neq 0$ then for half of the inputs y we have $y \cdot s = 0$ and for the other half $y \cdot s = 1$

#	Possibilities of failure at each step	Probability of failure
1	$\{0\}$	$\frac{2^0}{2^{n-1}}$
2	$\{0, y_1\}$	$\frac{2^1}{2^{n-1}}$
3	$\{0, y_1, y_2, y_1 \oplus y_2\}$	$\frac{2^2}{2^{n-1}}$
...	...	...
$n-1$	$\{0, y_1, y_2, y_3 \dots\}$	$\frac{2^{n-2}}{2^{n-1}}$

Simon's Algorithm: Probability of Success

#	Possibilities of failure at each step	Probability of failure
1	$\{0\}$	$\frac{2^0}{2^{n-1}}$
2	$\{0, y_1\}$	$\frac{2^1}{2^{n-1}}$
3	$\{0, y_1, y_2, y_1 \oplus y_2\}$	$\frac{2^2}{2^{n-1}}$
...	...	...
$n-1$	$\{0, y_1, y_2, y_3 \dots\}$	$\frac{2^{n-2}}{2^{n-1}}$

Table yields the sequence of probabilities of failure,

$$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots, \frac{1}{2^{n-1}} \qquad \text{(from bottom to top)}$$

Probability of failing in the first $n-2$ steps is thus

$$\frac{1}{4} + \frac{1}{8} + \dots = \frac{1}{4}\left(1 + \frac{1}{2} + \dots\right) \leq \frac{1}{4} \cdot \left(\sum_{i \in \mathbb{N}} \frac{1}{2^i}\right) = \frac{1}{2}$$

Geometric series whose sum is equal to two

Simon's Algorithm: Probability of Success

Probability of succeeding in the first $n-2$ steps at least $\frac{1}{2}$

Probability of succeeding in the $(n-1)$-th step is $\frac{1}{2}$

Thus probability of succeeding in all $n-1$ steps at least $\frac{1}{4}$

Simon's Algorithm: Probability of Success

Probability of succeeding in the first $n-2$ steps at least $\frac{1}{2}$

Probability of succeeding in the $(n-1)$-th step is $\frac{1}{2}$

Thus probability of succeeding in all $n-1$ steps at least $\frac{1}{4}$

More advanced maths tell that the probability is slightly higher (around $0.28878\ldots$)

Table of Contents

What Have We Learned?

Exponential separation between classical and quantum... even if probabilities are involved

What Have We Learned?

Exponential separation between classical and quantum... even if probabilities are involved

Always looking for a global property of f; not a local one

What Have We Learned?

Exponential separation between classical and quantum... even if probabilities are involved

Always looking for a global property of f; not a local one

Superposition and interference were instrumental

What Have We Learned?

Exponential separation between classical and quantum... even if probabilities are involved

Always looking for a global property of f; not a local one

Superposition and interference were instrumental

Problems solved were somewhat contrived. In the next lectures we will analyse problems with broader applications