BRICS Mini-course on Quantum Computation

A Berthiaume
C.W.I.

Session III: Complexity (II)

Complexity Classes:

BPP $\equiv$ decision problems for which $\exists\ \varepsilon \in \,]0, 1/2]$ and $\exists$ PTM M such that

$$\forall x \ \ \mathrm{Prob}[M(x) \text{ correct}] > 1/2 + \varepsilon$$

ZQP $\equiv$ decision problem Solvable on a QC in expected Poly-Time.

N.B. : the answer must be correct

Simon's Problem:

Def: $f : \{0,1\}^n \to \{0,1\}^m$ with $m \geq n$
is said to be s-invariant
if $\exists\, s \in \{0,1\}^n$, $s \neq 0^n$ s.t.
$\forall\, x \neq x'$ $\quad f(x) = f(x') \iff x' = x \oplus s$

Problem: Given a function f with the promise that either

1) f is 1-to-1

or 2) f is s-invariant,

you must decide which (and if 2, also produce s)

Simon's Problem is hard:

Consider a PTM M that queries f on k values and gets

$$A = f(x_1), \ldots, f(x_k)$$

Case 1: A contains no pairs

→ no info, flip coin...

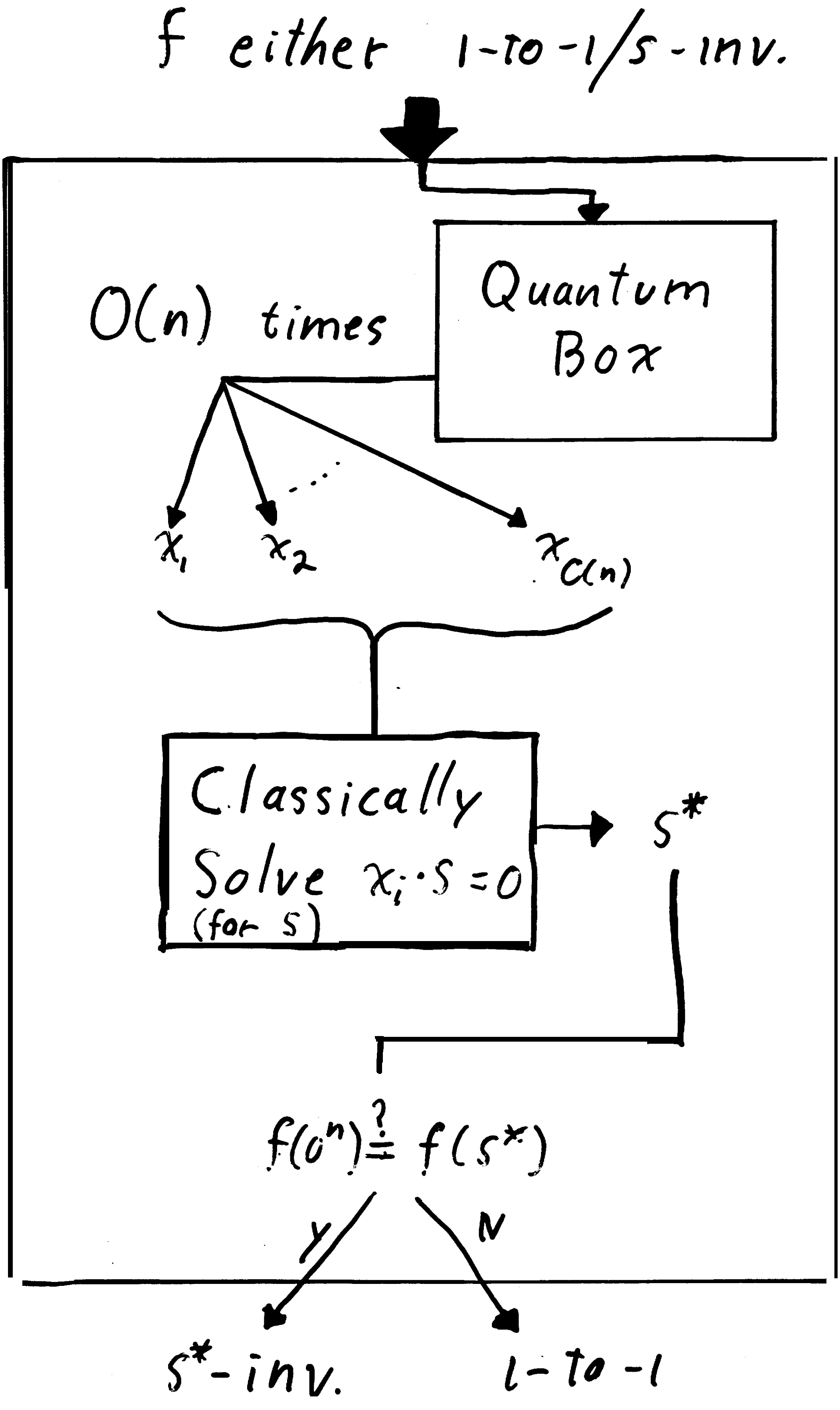
Case 2: A contains >1 pair

→ we know s, but...

➜ Only $< k^2/2^n$ different s can be "discovered" with these specific $x_1, \ldots x_k$

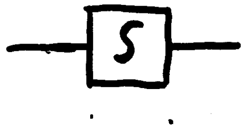
→ if $k = 2^{n/4}$, this is only $1/2^{n/2}$!

Diagram:

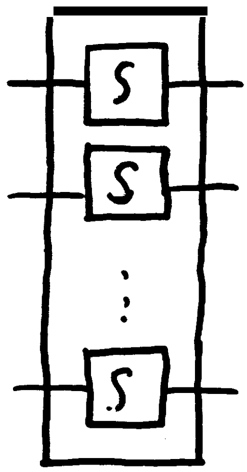

f either 1-to-1/s-inv.
Quantum Box
O(n) times
x1 x2 xO(n)
Classically Solve xi·s = 0 (for s)
s*
f(0^n) ?= f(s*)
Y
N
s*-inv.
1-to-1

Quamtum Solution:

Def: $S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$



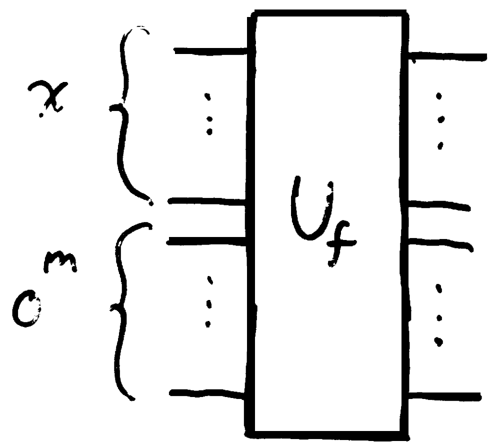
$$S_n = \bigotimes_n S$$



S_n

Recall: f computable $\Rightarrow \exists\, U_f$

s.t.



$$U_f |x, 0\rangle = |x, f(x)\rangle$$

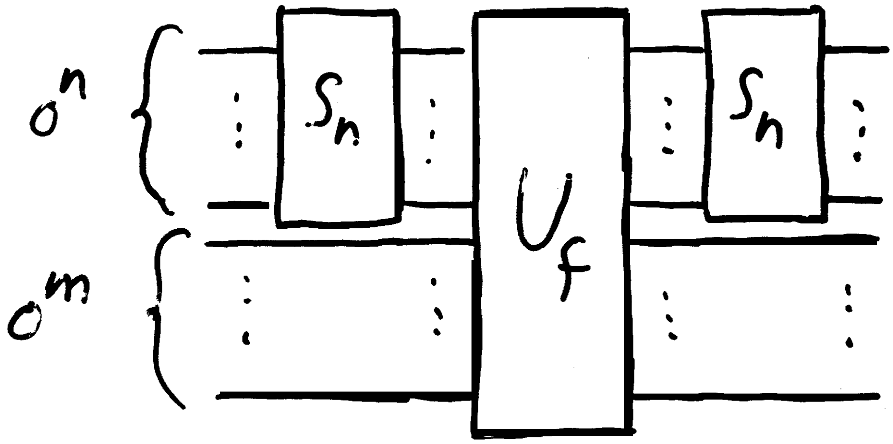
Remark about S_n:

For $a, b \in \{0,1\}^n$, $a \cdot b$ is the XOR of the bitwise product (AND, $\wedge$) of a and b.

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

$$\frac{1}{\sqrt{2^n}}\begin{array}{cc} \begin{array}{ccc} & i & \end{array} & \\ \begin{pmatrix} 1 & & \\ 1 & \vdots & \\ 1 & \vdots & \\ \vdots & (-1)^{w\cdot i} & \cdots \\ \vdots & & \\ 1 & & \end{pmatrix} & \begin{array}{c} \\ \\ \\ w \\ \\ \\ \end{array} \end{array}$$

Quantum Solution:



$$|0,0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_i |i, 0\rangle$$

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_i |i, f(i)\rangle$$

$$\rightarrow \frac{1}{2^n} \sum_i \sum_j (-1)^{i \cdot j} |j, f(i)\rangle$$

then, we observe (standard basis)

$$\rightarrow |x, f(y)\rangle$$

Quantum Solution (cont.):

Repeat k times (with same f !)

$|x_1, f(y_1)\rangle$, ... , $|x_k, f(y_k)\rangle$

Case 1: If f is 1-TO-1

→ the $|x_i, f(y_i)\rangle$ are selected uniformely from all possible $|a, f(b)\rangle$

Quantum Solution (cont.):

Case 2: f is s-invariant

$\forall\, x, y$ $\quad |x, f(y)\rangle$ identical to $|x, f(y \oplus s)\rangle$

its amplitude: $\frac{1}{2^n}\left((-1)^{y \cdot x} + (-1)^{(y \oplus s)\cdot x}\right)$

but: this is

$\pm\, \frac{1}{2^{n-1}}$ if $x \cdot s = 0$

0 otherwise

So: the $|x_i, f(y_i)\rangle$ are uniformly selected from

$$\{\, |x, f(y)\rangle \mid x \cdot s = 0 \,\}$$

Quantum Solution (cont.):

To determine whether f is 1-to-1 or s-invariant:

1) Solve for s the system

$$\left.\begin{array}{l} x_1 \cdot s = 0 \\ x_2 \cdot s = 0 \\ \vdots \\ x_k \cdot s = 0 \end{array}\right\} \quad s^*$$

Where $k \in O(n)$

2) test $f(0^n) \stackrel{?}{=} f(s^*)$

yes? $\to$ f is s^*-invariant

No? $\to$ f is 1-to-1

➜ If <u>expected</u> $O(n)$ running time, this works.

Oracle Result:

thm: $\exists\ X \in \{0,1\}^*$ such that

$$ZQP^X \not\subseteq BPP^X$$

Proof: Immediate with X constructed as follow

$\forall n$: Flip a fair coin.

H: $X_{[n]} \leftarrow$ Random 1-to-1 f

T: $X_{[n]} \leftarrow$ Random s-inv. f