Title: PSI 2018/2019 - Quantum Information Review - Lecture 7

Speakers: Daniel Gottesman

Collection: PSI 2018/2019 - Quantum Information Review (Gottesman)

Date: March 12, 2019 - 11:30 AM

URL: http://pirsa.org/19030044

Def: A language L reduces to language M if $\exists$ poly-time computable $f:\{0,1\}^* \to \{0,1\}^*$ s.t. $x \in L \iff f(x) \in M$. A language $M \in NP$ is NP-complete if $\forall L \in NP$, L reduces to M.

Def: A language L reduces to language M
if $\exists$ poly-time computable $f : \{0,1\}^* \to \{0,1\}^*$
s.t. $x \in L \Leftrightarrow f(x) \in M$. A language $M \in NP$
is NP-complete if $\forall L \in NP$, L reduces to M.

Thm: k-SAT is NP-complete for $k \geq 3$.
(Cook-Levin thm).

Def: BQP is the set of languages L for which there exists a quantum algorithm $A_L(x)$ s.t.

1. $A_L(x)$ runs in time polynomial in $|x|$
2. If $x \in L$, then $A_L(x) = \text{yes}$ w/ probability $\geq 2/3$.
3. If $x \notin L$, then $A_L(x) = \text{no}$ w/ probability $\geq 2/3$.

M

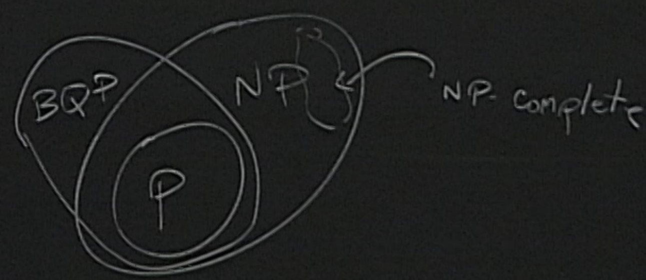
$\{0,1\}^*$

$M \in NP$

M.

Def: BQP is the set of languages L for which there exists a quantum algorithm $A_L(x)$ s.t.

1. $A_L(x)$ runs in time polynomial in $|x|$
2. If $x \in L$, then $A_L(x) = \text{yes}$ w/ probability $\geq 2/3$.
3. If $x \notin L$, then $A_L(x) = \text{no}$ w/ probability $\geq 2/3$.



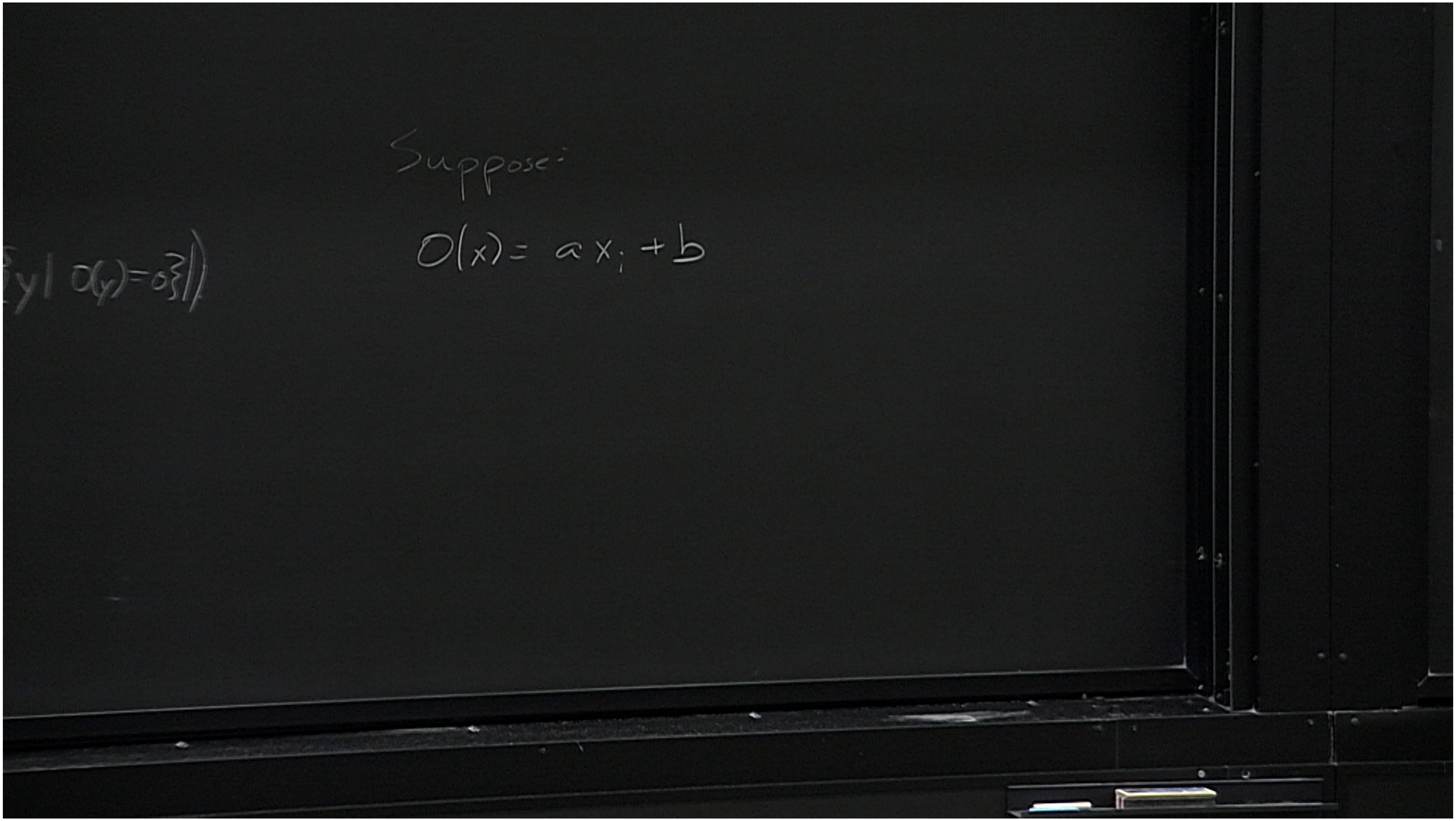
$O : \mathbb{Z}_2^n \to \mathbb{Z}_2$ oracle

Def: Let $f(O)$ be a property of oracles. The query complexity of f is the minimum number of queries to O needed to calculate $f(O)$.

Example: This is a promise problem. The promise is that O is either constant ($O(x) = O(y)\ \forall x, y$) or balanced ($|\{x \mid O(x) = 1\}| = |\{y \mid O(y) = 0\}|$).

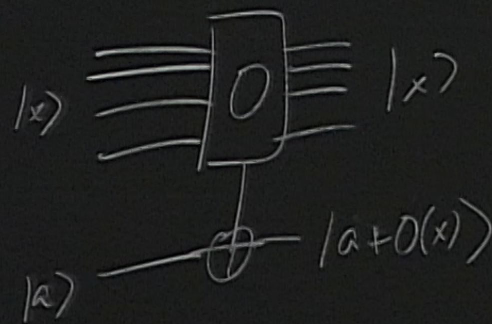
Determine if O is constant or balanced w/ 100% probability.

Needs $2^{n-1}+1$ queries.

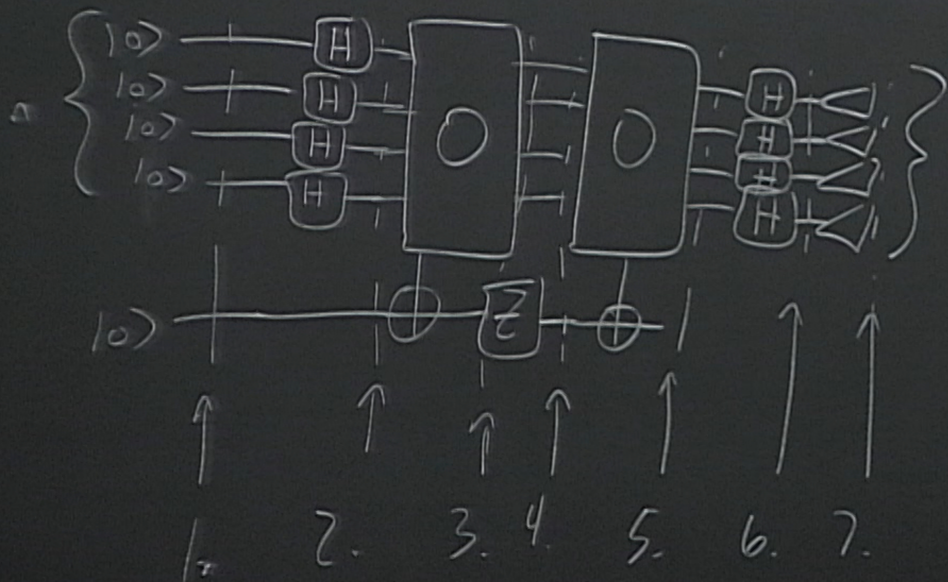

{y| O(y)=0}|)
Suppose:
O(x) = a x_i + b

Quantum Oracles

$$O\,\underbrace{|x\rangle}_{n\text{ qubits}}\underbrace{|a\rangle}_{1\text{ qubit}} = |x\rangle\,|a+O(x)\rangle$$



Deutsch-Jozsa algorithm:



if all 0 ⇒ output "constant"

if not ⇒ output "balanced"

8.

1. $|0 \ldots 0\rangle|0\rangle$

2. $\sum_x |x\rangle|0\rangle$

3. $\sum_x |x\rangle|O(x)\rangle$

4. $\sum_x (-1)^{O(x)}|x\rangle|O(x)\rangle$

5. $\sum_x (-1)^{O(x)}|x\rangle|0\rangle$

Constant:

1. $|0\ldots0\rangle|0\rangle$

2. $\sum_x |x\rangle|0\rangle$

3. $\sum_x |x\rangle|O(x)\rangle$

4. $\sum_x (-1)^{O(x)}|x\rangle|O(x)\rangle$

5. $\sum_x (-1)^{O(x)}|x\rangle|0\rangle$

Constant:

5. $\pm\left(\sum_x |x\rangle\right)|0\rangle$

6. $\pm|0\ldots0\rangle|0\rangle$

7. $0\,0\,0\ldots0$

8. constant ✓

Balanced:

5. $|\phi\rangle = \sum_x (-1)^{f(x)} |x\rangle$

6. $\left(H^{\otimes n}|\phi\rangle\right)|0\rangle$

7. $y_1, \dots y_n \neq 0 \dots 0.$

8. balanced ✓

$|\psi\rangle = \sum_x |x\rangle$

$\langle\psi|\phi\rangle = 0$

$\langle\psi|H^{\otimes n} H^{\otimes n}|\phi\rangle = \langle\psi|\phi\rangle = 0$

$\langle 0\dots0|\left(H^{\otimes n}|\phi\rangle\right) = 0.$

...nstant :

$= \left(\sum_x |x\rangle\right)|0\rangle$

$= |0 \ldots 0\rangle|0\rangle$

$00 \ldots 0$

...nstant ✓

Balanced:

5. $|\phi\rangle = \sum_x (-1)^{f(x)} |x\rangle$

6. $\left(H^{\otimes n}|\phi\rangle\right)|0\rangle$

7. $y_1 \ldots y_n \neq 0 \ldots 0.$

8. balanced ✓

$|\psi\rangle = \sum_x |x\rangle$

$\langle\psi|\phi\rangle = 0$

$\left(\underbrace{\langle\psi|H^{\otimes n}}\right)\left(H^{\otimes n}|\phi\rangle\right) = \langle\psi|\phi\rangle = 0$

$\langle 0 \ldots 0|\left(H^{\otimes n}|\phi\rangle\right) = 0.$