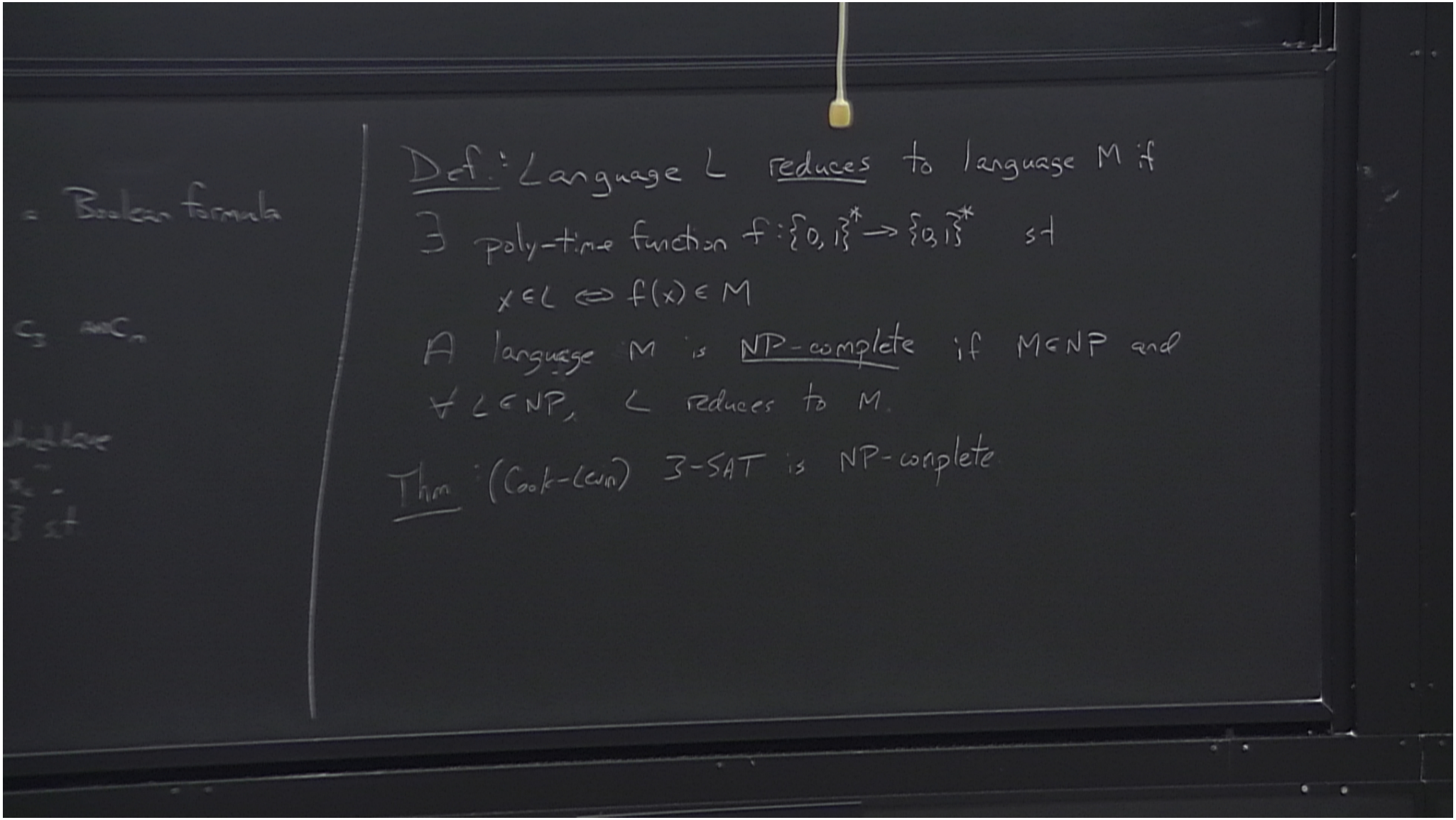
Title: Quantum Information Review-6

Date: Feb 24, 2015 11:30 AM

URL: http://pirsa.org/15020068

Abstract:


Boolean formula
Def: Language L reduces to language M if
∃ poly-time function f: {0,1}* → {0,1}* s.t.
x ∈ L ⇔ f(x) ∈ M
A language M is NP-complete if M ∈ NP and
∀ L ∈ NP, L reduces to M.
Thm: (Cook-Levin) 3-SAT is NP-complete

: NP is class of languages L

that $\exists$ "verifier" algorithm $V(x, w)$ s.t.

- $V(x,w)$ run in time $\text{poly}(|x|)$ when $|w| = \text{poly}(|x|)$
- $\forall x \in L$, $\exists w_x$ s.t. $V(x, w_x) = \text{yes}$, $|w_x| = \text{poly}(|x|)$
- $\forall x \notin L$, $\forall w$ $(|w| = \text{poly}(|x|))$, $V(x, w) = \text{no}$

is the witness for yes instance x

k-SAT: The instance is a Boolean formula

n variables $\{x_i\}$

Formula $f(x) = C_1$ AND C_2 AND C_3 AND C_m

m clauses C_i

Each C_i is OR of k atoms, which have the form either "x_a" or "NOT x_a".

$f(\{x_i\})$ is a yes instance if $\exists \{x_i\}$ s.t. $f(\{x_i\}) = \text{TRUE}$

$nk(\log n + 1)$

Def: Language L **reduces** to language M if

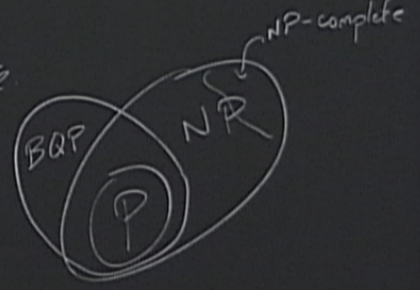
$\exists$ poly-time function $f: \{0,1\}^* \to \{0,1\}^*$ s.t.

$x \in L \Leftrightarrow f(x) \in M$

A language M is **NP-complete** if $M \in NP$ and

$\forall L \in NP$, L reduces to M.

Thm (Cook-Levin) 3-SAT is NP-complete



Oracle model:

Black box $O: \{0,1\}^n \to \{0,1\}$

Query to oracle $x \longmapsto O(x)$

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

Example: Promise $O: \mathbb{Z}_2^n \to \mathbb{Z}_2$ is either constant $O(x) = O(y) \quad \forall x, y$
or balanced $|\{x \mid O(x)=0\}| = |\{x \mid O(x)=1\}|$

Property: Say if the oracle is constant or balanced.

Oracle model:

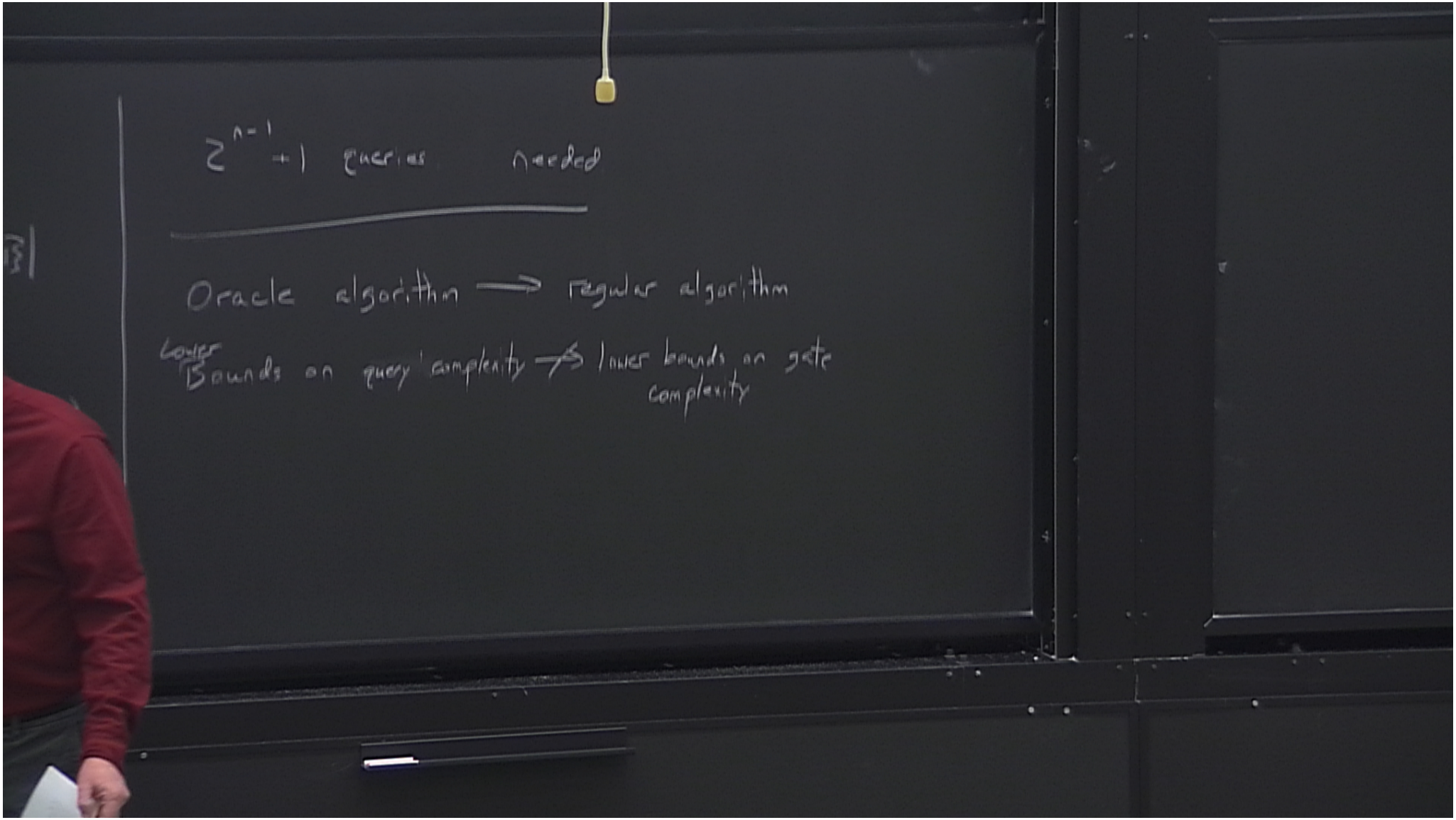
Black box $O: \{0,1\}^n \to \{0,1\}$

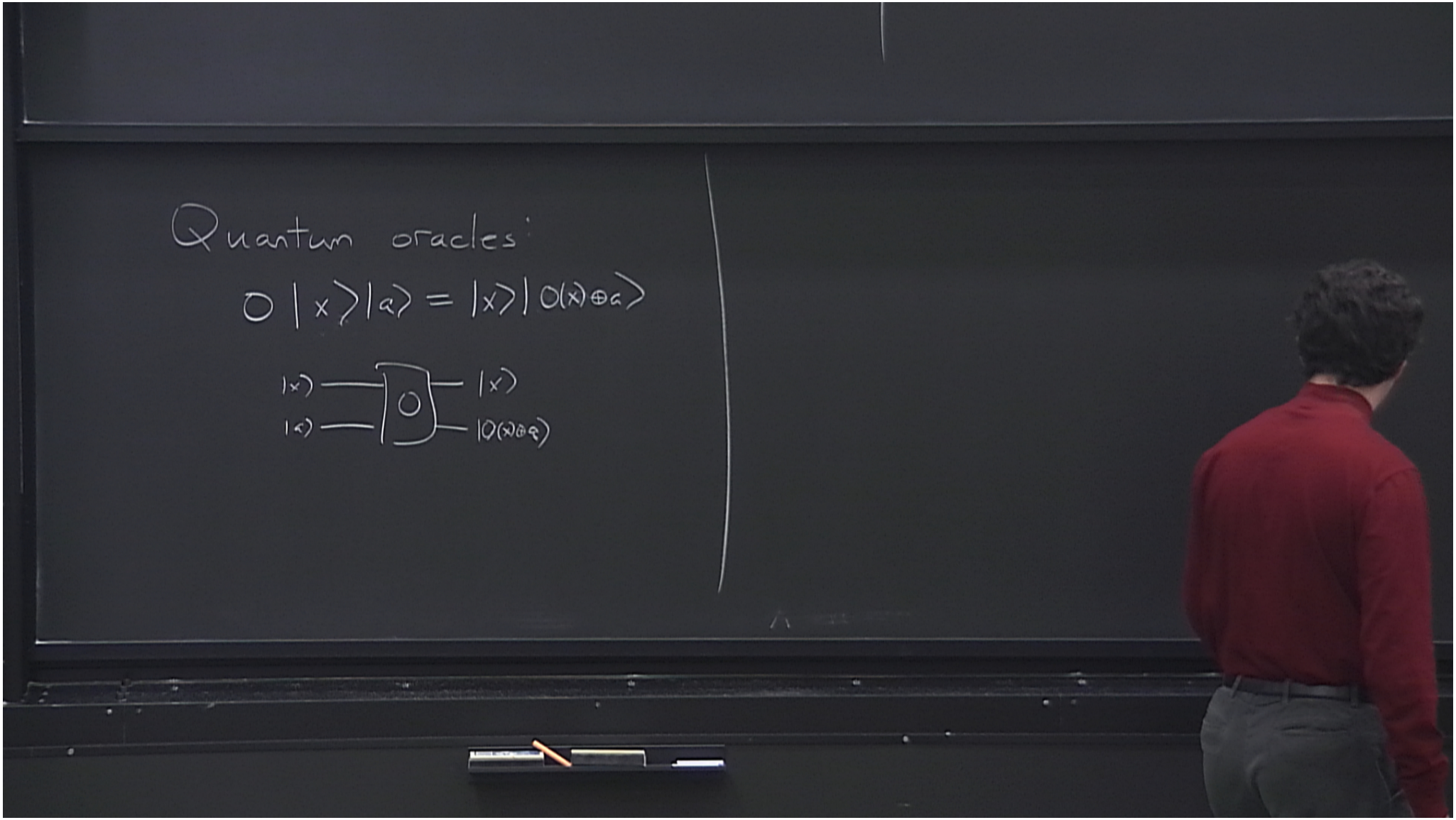
Query to oracle $x \longmapsto O(x)$

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

Example: Promise $O: \mathbb{Z}_2^n \to \mathbb{Z}_2$ is either constant $O(x) = O(y) \quad \forall x, y$
or balanced $|\{x \mid O(x)=0\}| = |\{x \mid O(x)=1\}|$

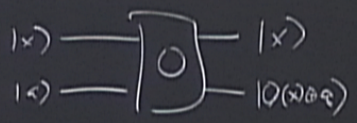
Property: Say if the oracle is constant or balanced w/ 100% certainty


$2^{n-1}+1$ queries needed
Oracle algorithm ⟹ regular algorithm
Lower Bounds on query complexity ⇏ lower bounds on gate complexity

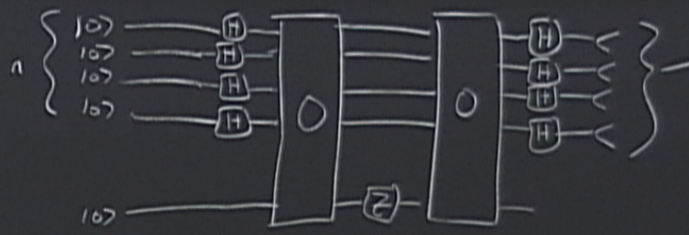

Quantum oracles:
O|x⟩|a⟩ = |x⟩|O(x)⊕a⟩
|x⟩
|a⟩
O
|x⟩
|O(x)⊕a⟩

Quantum oracles

$$O|x\rangle|a\rangle = |x\rangle|O(x)\oplus a\rangle$$



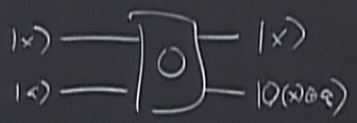
Deutsch-Jozsa algorithm



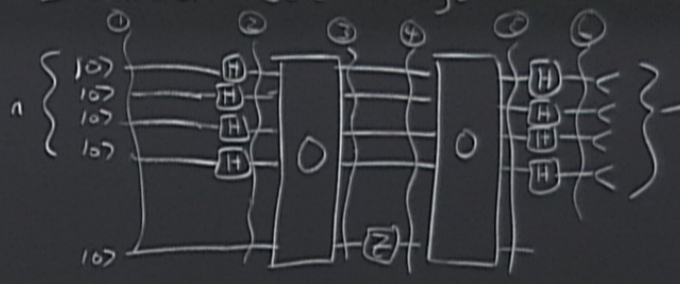
→ if O O, output "constant"
otherwise, output "balanced"

Quantum oracles

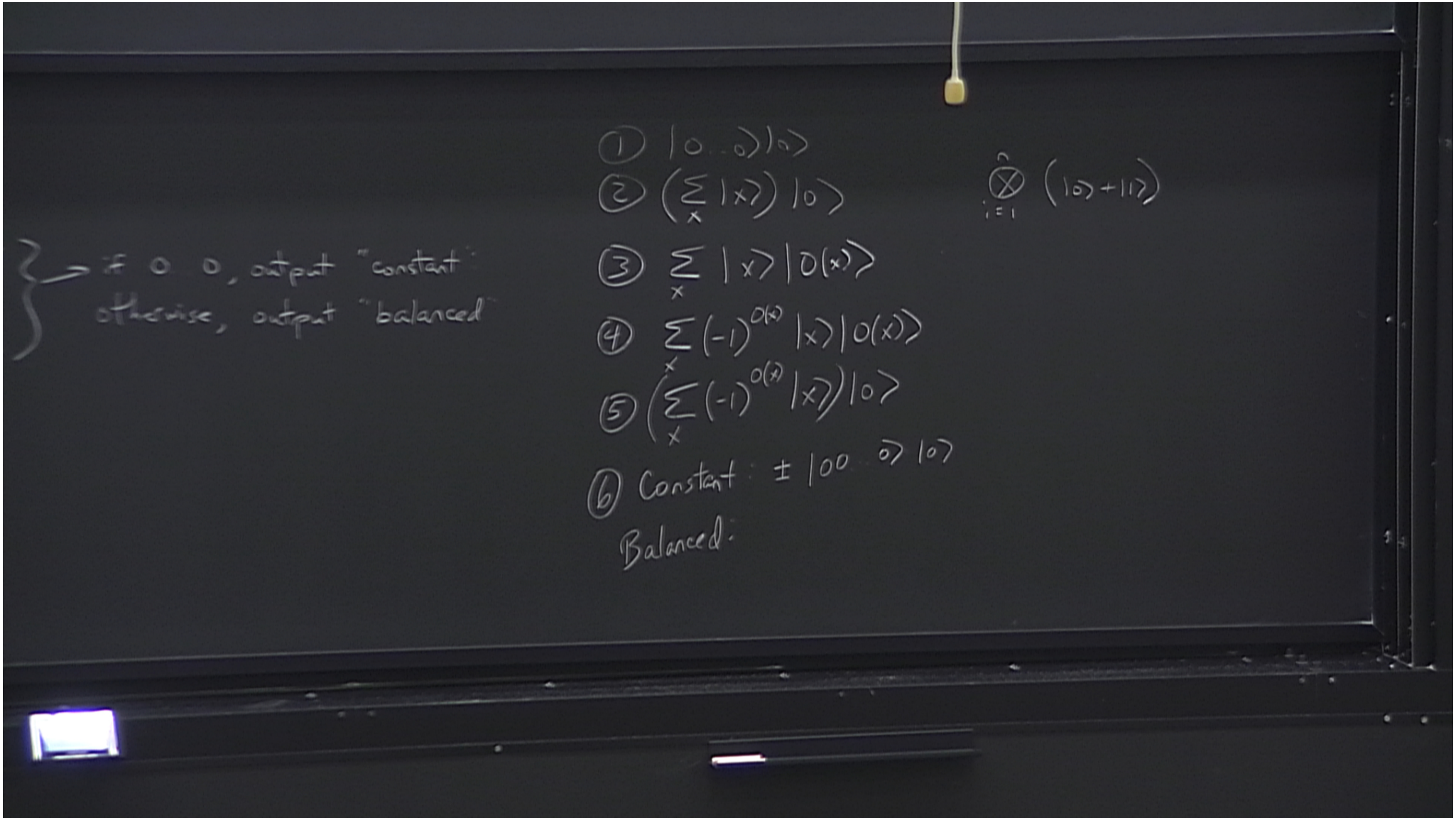
$$O|x\rangle|a\rangle = |x\rangle|O(x)\oplus a\rangle$$

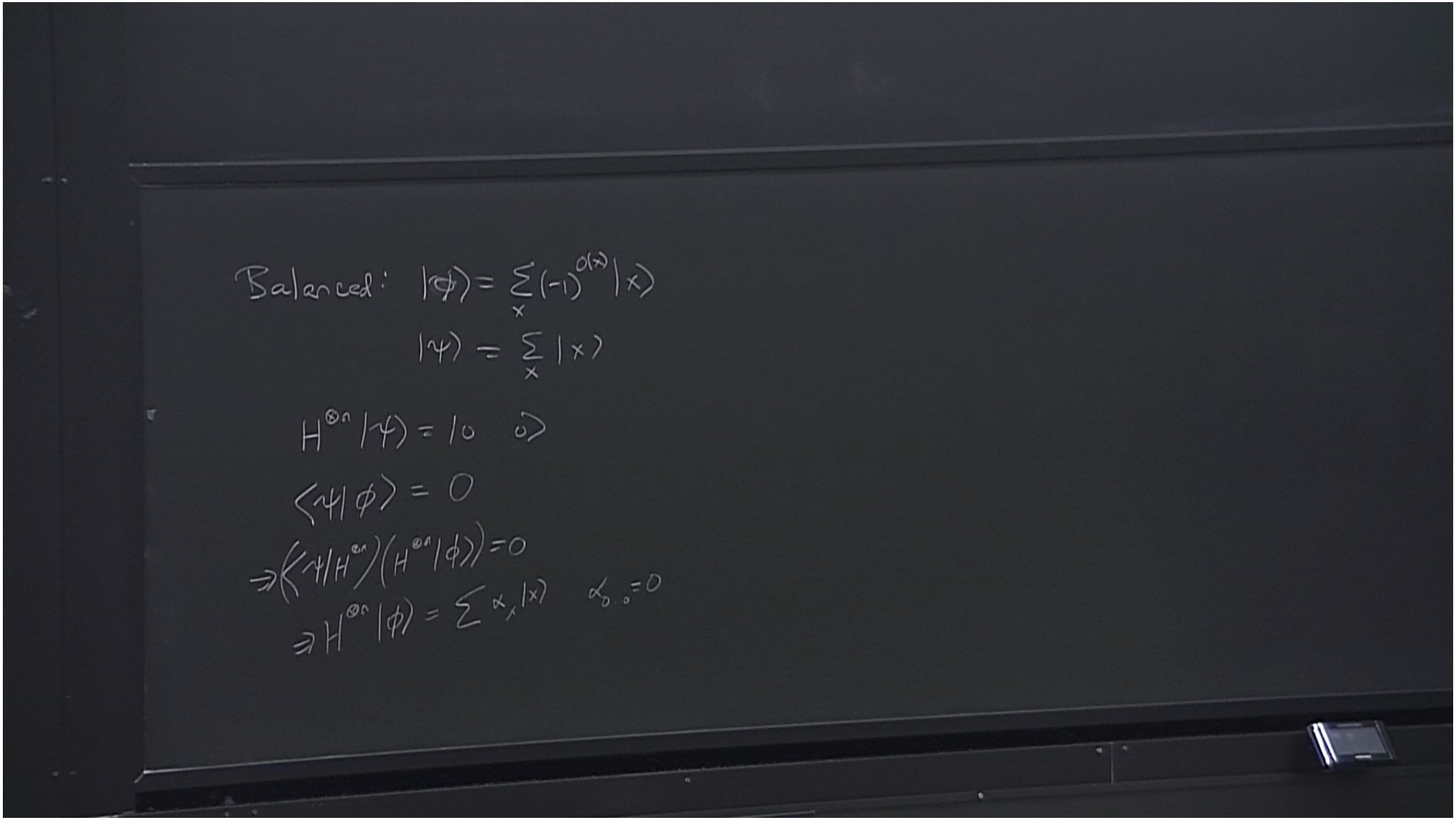


Deutsch-Jozsa algorithm



→ if 0 0, output "constant"
otherwise, output "balanced"


if 0 0, output "constant"
otherwise, output "balanced"
① |0...0⟩|0⟩
② (Σ_x |x⟩)|0⟩
③ Σ_x |x⟩|0(x)⟩
④ Σ_x (-1)^0(x) |x⟩|0(x)⟩
⑤ (Σ_x (-1)^0(x) |x⟩)|0⟩
⑥ Constant: ± |00...0⟩|0⟩
Balanced:
⊗ (|0⟩+|1⟩)


Balanced: $|\phi\rangle = \sum_x (-1)^{a(x)} |x\rangle$
$|\psi\rangle = \sum_x |x\rangle$
$H^{\otimes n} |\psi\rangle = |0 \quad 0\rangle$
$\langle\psi|\phi\rangle = 0$
$\Rightarrow (\langle\psi| H^{\otimes n})(H^{\otimes n}|\phi\rangle) = 0$
$\Rightarrow H^{\otimes n}|\phi\rangle = \sum \alpha_x |x\rangle \quad \alpha_{0\ldots0} = 0$