Title: Lecture - Quantum Information, PHYS 635

Speakers: Alex May

Collection/Series: Quantum Information (Elective), PHYS 635, February 24 - March 28, 2025

Subject: Quantum Information

Date: March 24, 2025 - 11:30 AM

URL: https://pirsa.org/25030022

Lecture 11 - Complexity theory

Recall: TM model, complexity

"Complexity class

P = prob

EXP = "

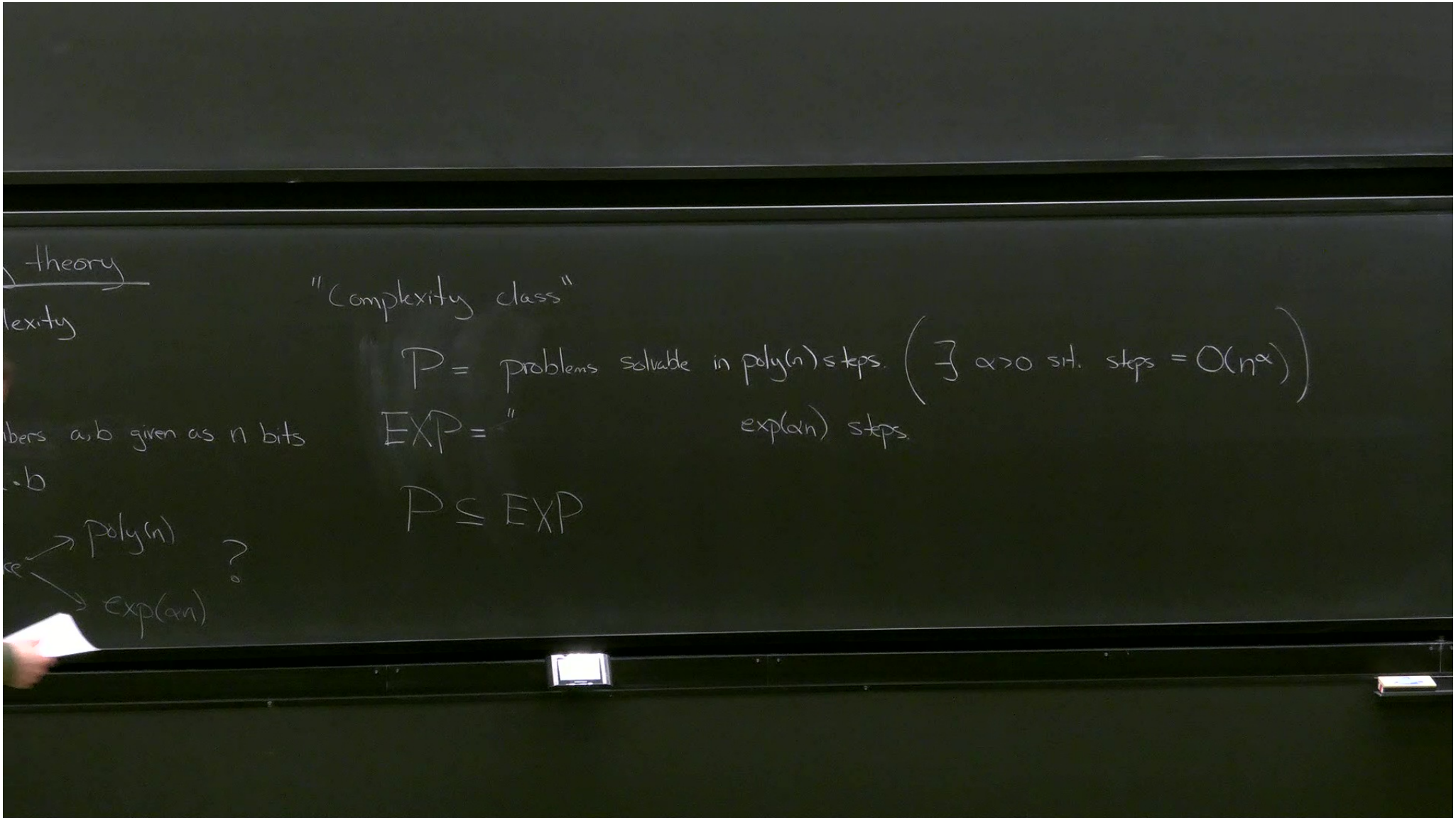
Multiply:

Input: numbers a, b given as n bits

Output: $a \cdot b$

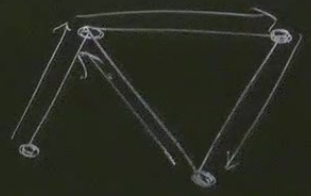
Does this take → $poly(n)$?

→ $exp(an)$


theory
lexity
"Complexity class"
P = problems solvable in poly(n) steps. (∃ α>0 s.t. steps = O(n^α))
EXP = " exp(αn) steps.
P ⊆ EXP
bers a, b given as n bits
.b
poly(n)
exp(αn)
?

$\exp(an)$

The class P

$G =$ 

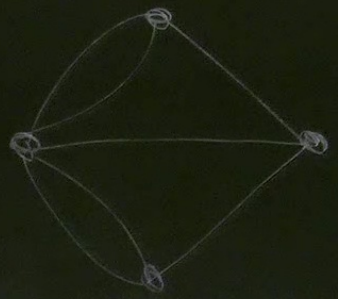
Def! "Eulerian cycle" = path through G that visits each edge exactly once, and returns to starting point

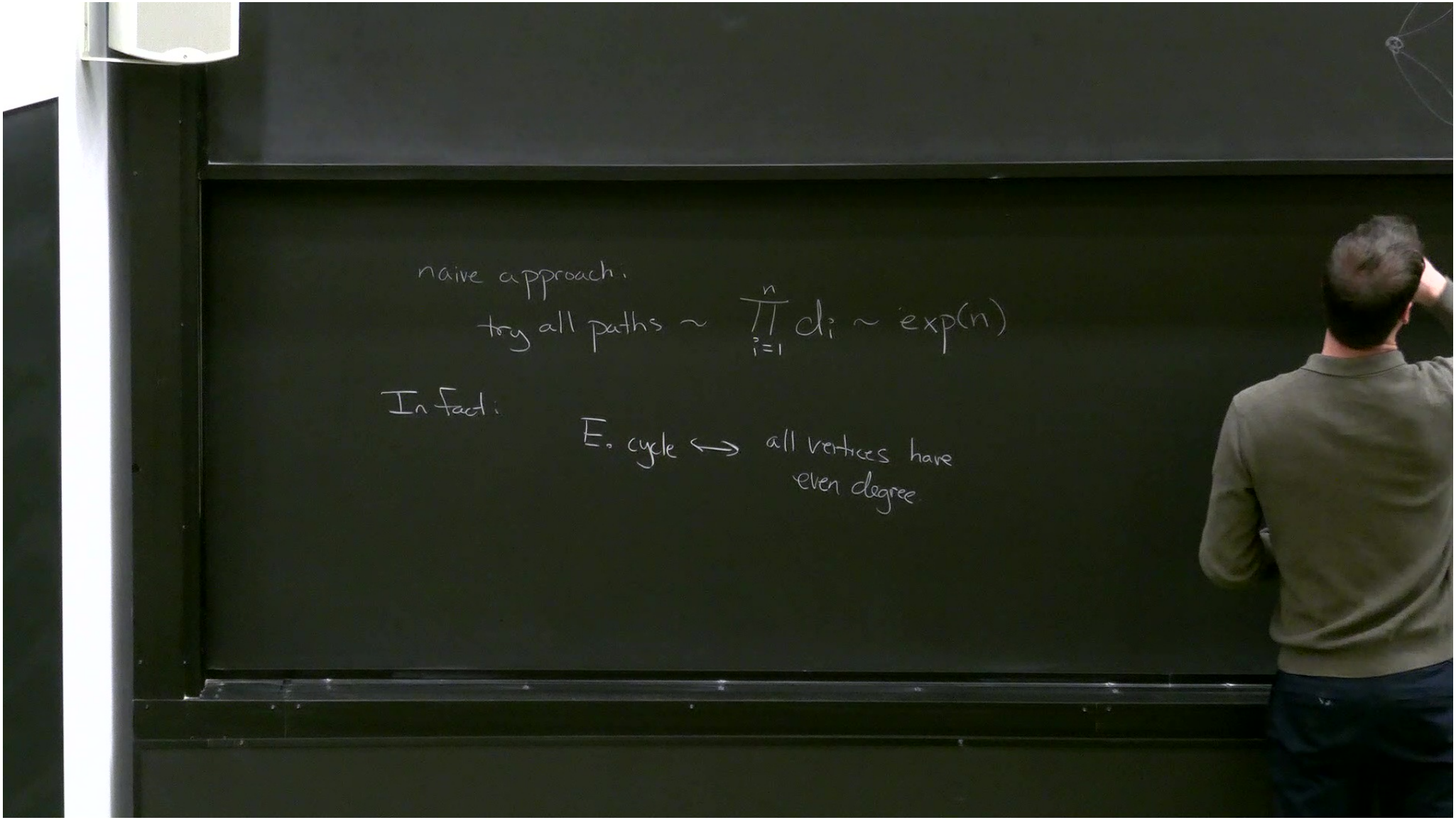
Eulerian Cycles

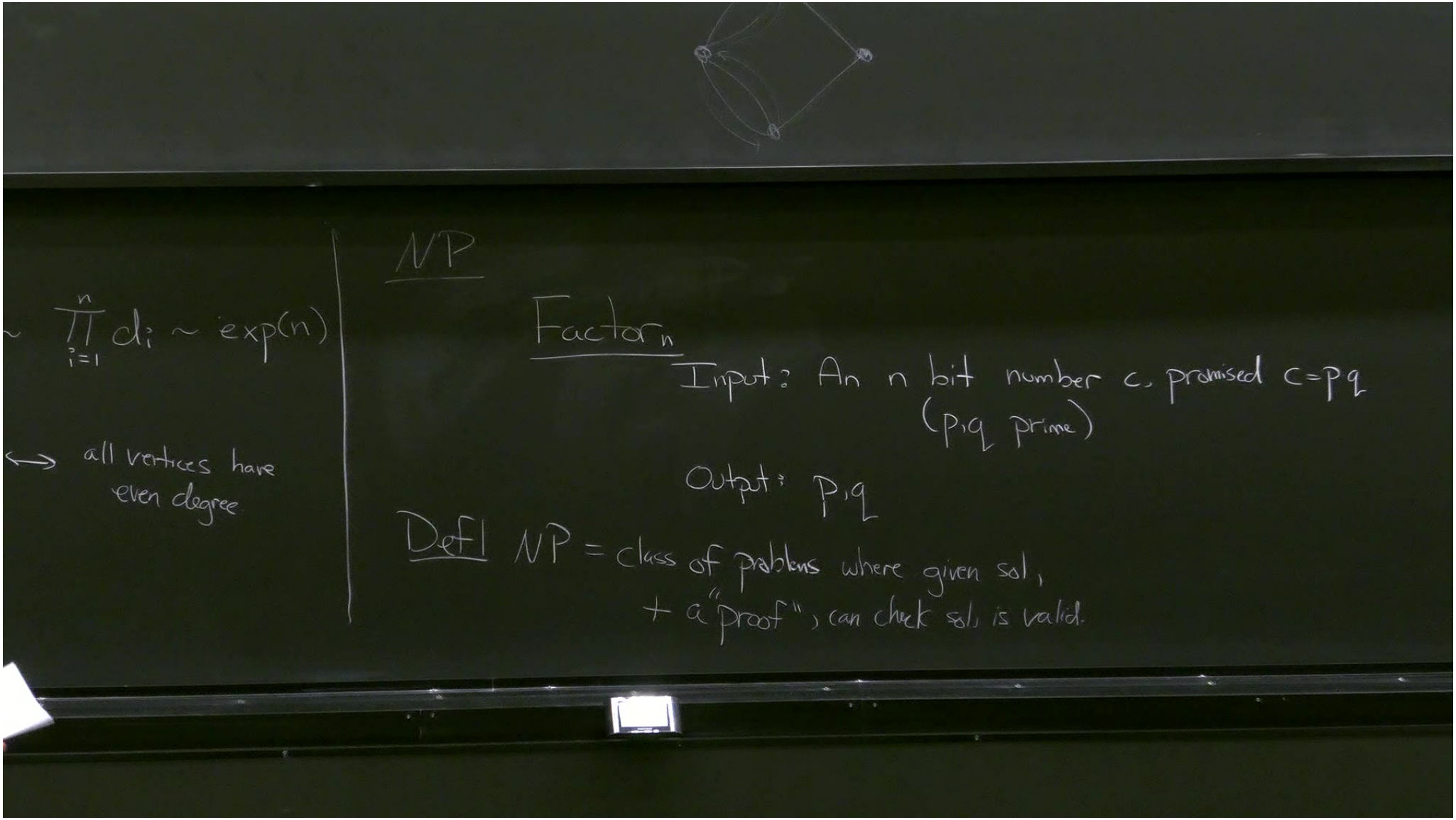
Input: A graph G with n vertices.

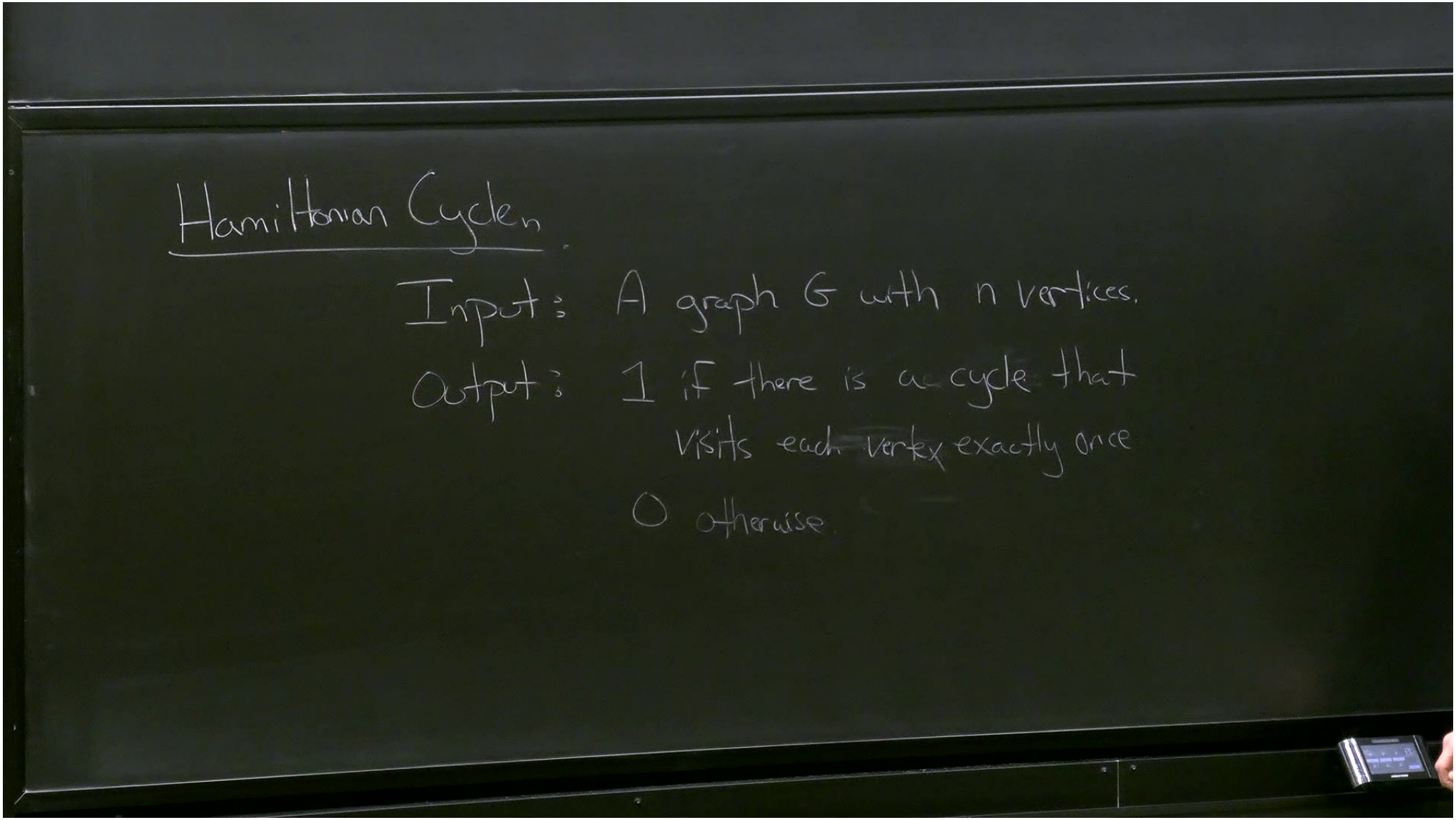
Output: 1 if $\exists$ Eulerian cycle.

0 otherwise.




naive approach:
try all paths ~ $\prod_{i=1}^{n} d_i \sim \exp(n)$
In fact:
E. cycle ⟺ all vertices have even degree


$\sim \prod_{i=1}^{n} d_i \sim \exp(n)$
$\leftrightarrow$ all vertices have even degree
NP
Factor$_n$
Input: An n bit number c, promised c=pq (p,q prime)
Output: p,q
Def! NP = class of problems where given sol, + a "proof", can check sol. is valid.


Hamiltonian Cycle
Input: A graph G with n vertices.
Output: 1 if there is a cycle that visits each vertex exactly once
0 otherwise.

BPP: class of problems where ∃ probabilistic poly time TM s.t.

1) On "yes" instances, accepts with $p > 2/3$
2) "no" reject $p > 2/3$

$p > \frac{1}{2} + \delta$

$p > \frac{1}{2} + \frac{1}{2^n}$

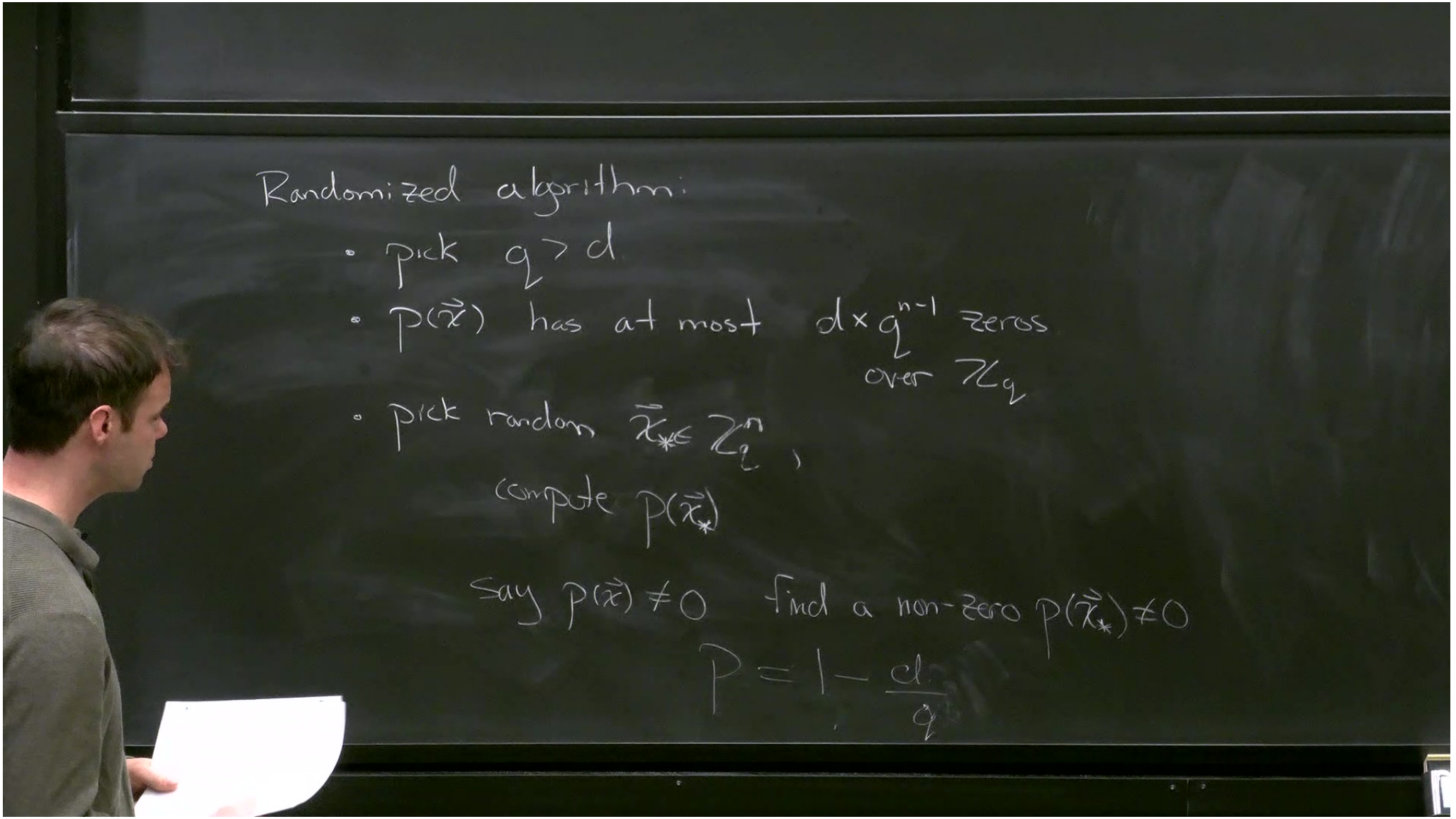
Polynomial identity testing

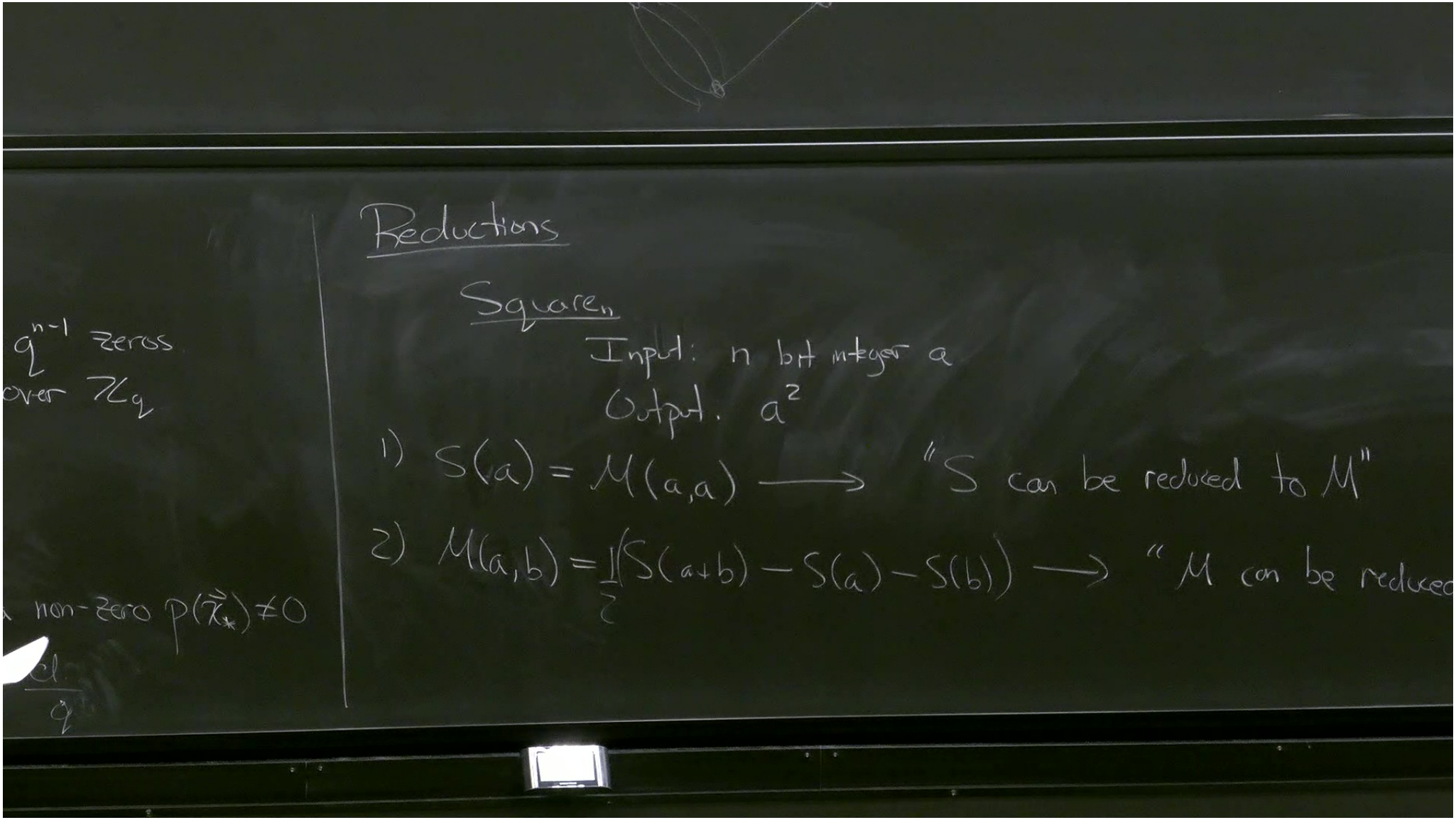
Input. A polynomial $p(x_1, \ldots x_n)$, degree poly(n).

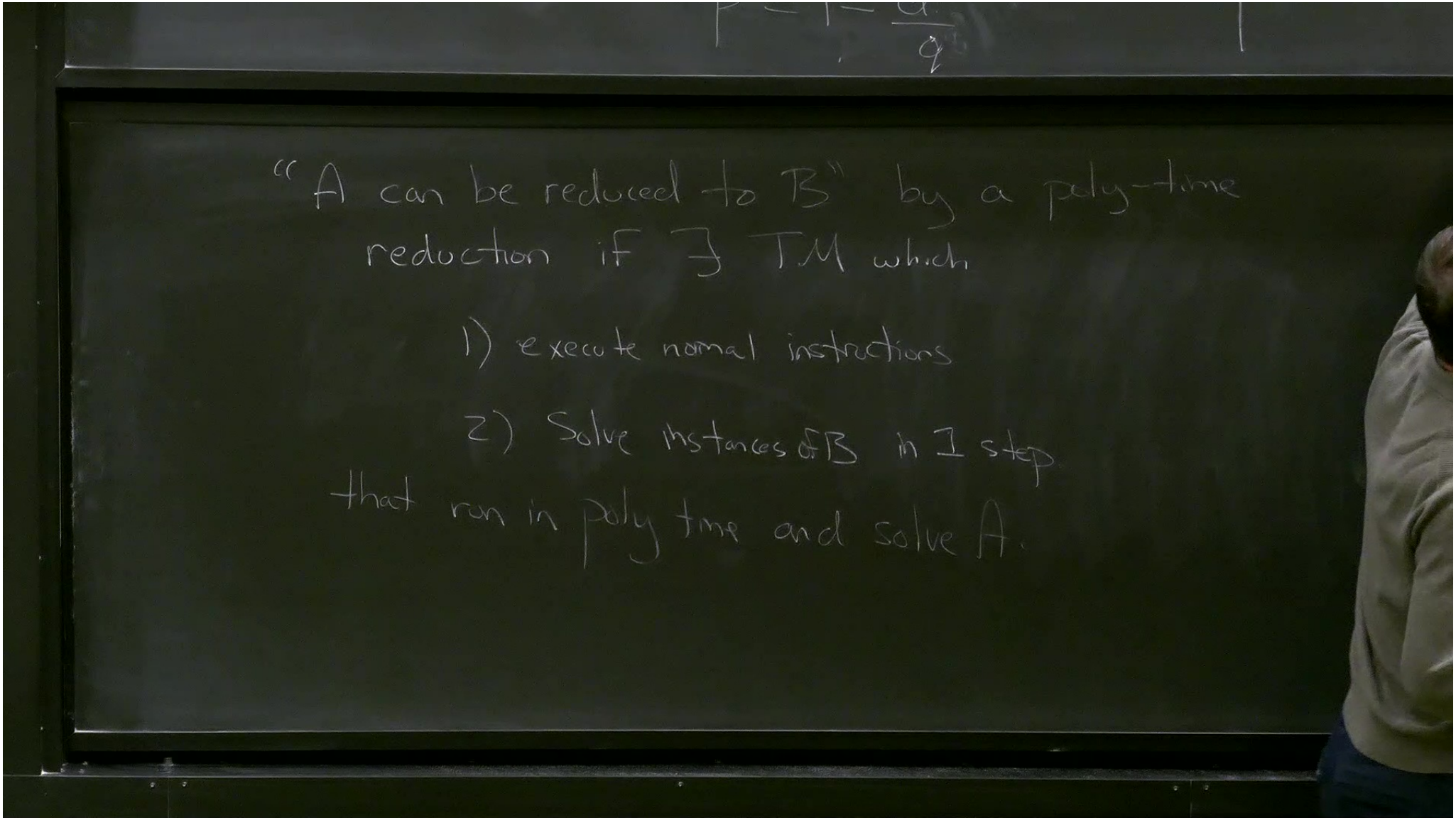
Output: 1 if $p(x_1, \ldots, x_n) = 0$

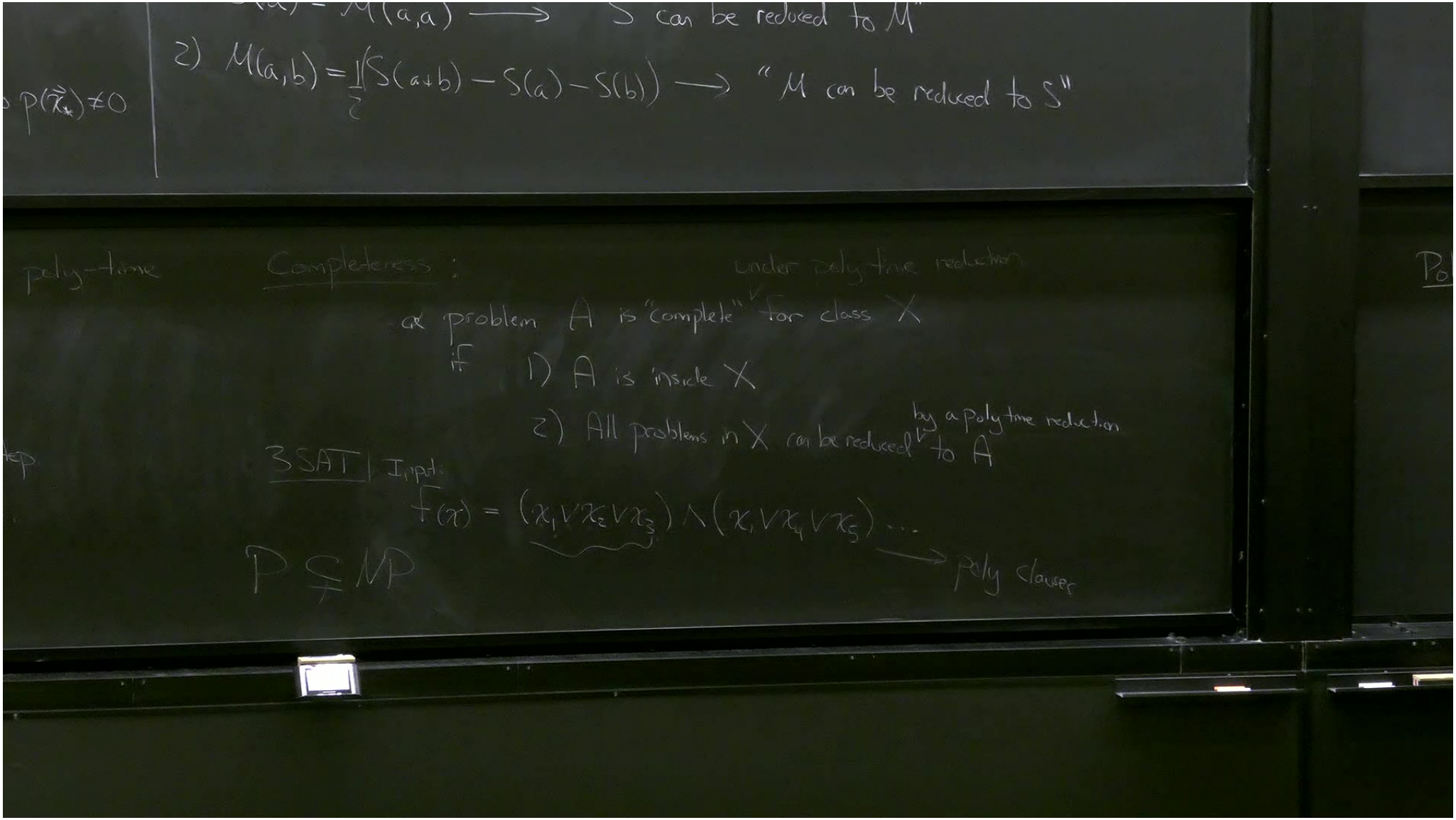
0 otherwise.

$p(x) = (x^2 - 1) - (x-1)(x+1)$


Randomized algorithm:
• pick $q > d$
• $p(\vec{x})$ has at most $d \times q^{n-1}$ zeros over $\mathbb{Z}_q$
• pick random $\vec{x}_* \in \mathbb{Z}_q^n$, compute $p(\vec{x}_*)$
Say $p(\vec{x}) \neq 0$ find a non-zero $p(\vec{x}_*) \neq 0$
$P = 1 - \frac{d}{q}$


Reductions
Squaren
Input: n bit integer a
Output. a^2
1) $S(a) = M(a,a)$ ⟶ "S can be reduced to M"
2) $M(a,b) = \frac{1}{2}(S(a+b) - S(a) - S(b))$ ⟶ "M can be reduced
q^{n-1} zeros
over $\mathbb{Z}_q$
non-zero $p(\vec{x}_*) \neq 0$


"A can be reduced to B" by a poly-time
reduction if ∃ TM which
1) execute normal instructions
2) Solve instances of B in 1 step
that run in poly time and solve A.


S can be reduced to M"
2) M(a,b) = 1/2 (S(a+b) − S(a) − S(b)) ⟶ "M can be reduced to S"
p(x⃗*) ≠ 0
poly-time
Completeness:
under poly-time reduction
a problem A is "complete" for class X
if 1) A is inside X
2) All problems in X can be reduced by a poly-time reduction to A
3SAT | Input:
f(x) = (x1 ∨ x2 ∨ x3) ∧ (x1 ∨ x4 ∨ x5) ...
Poly clauses
P ⊆ NP