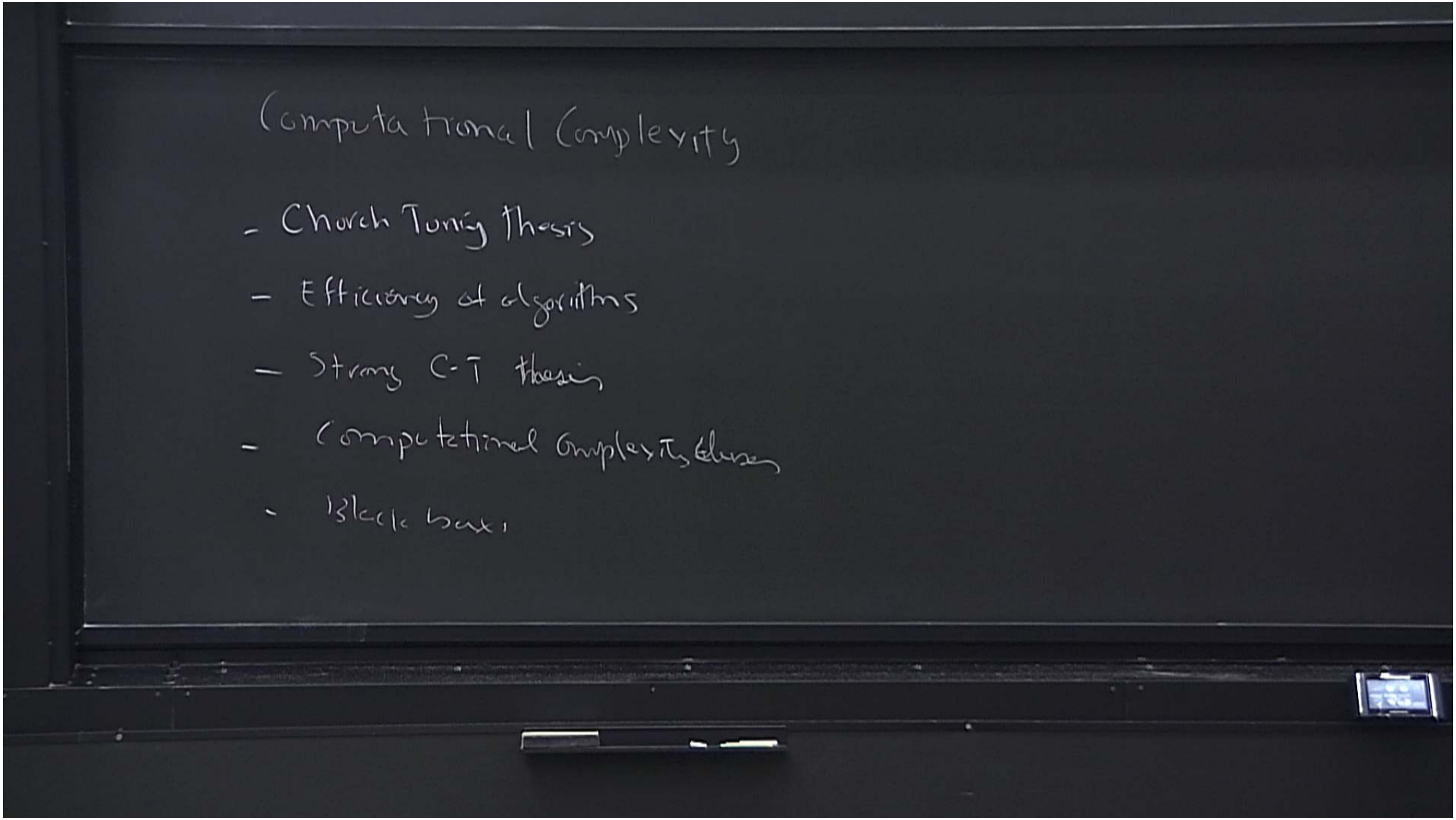
Title: PSI 2015/2016 Quantum Information - Lecture 8

Date: Mar 02, 2016 11:30 AM

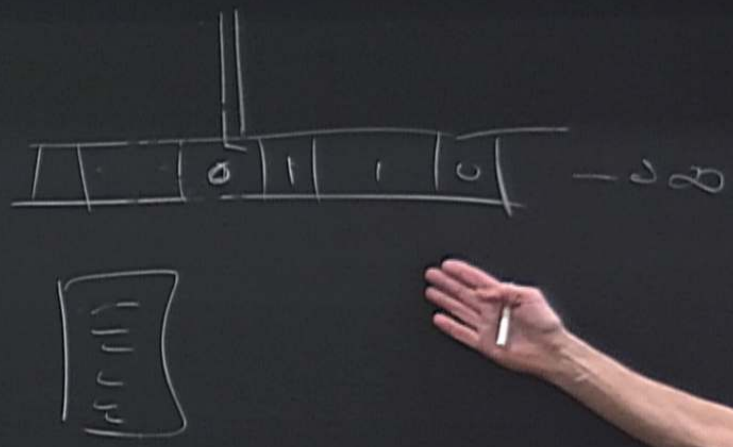
URL: http://pirsa.org/16030055

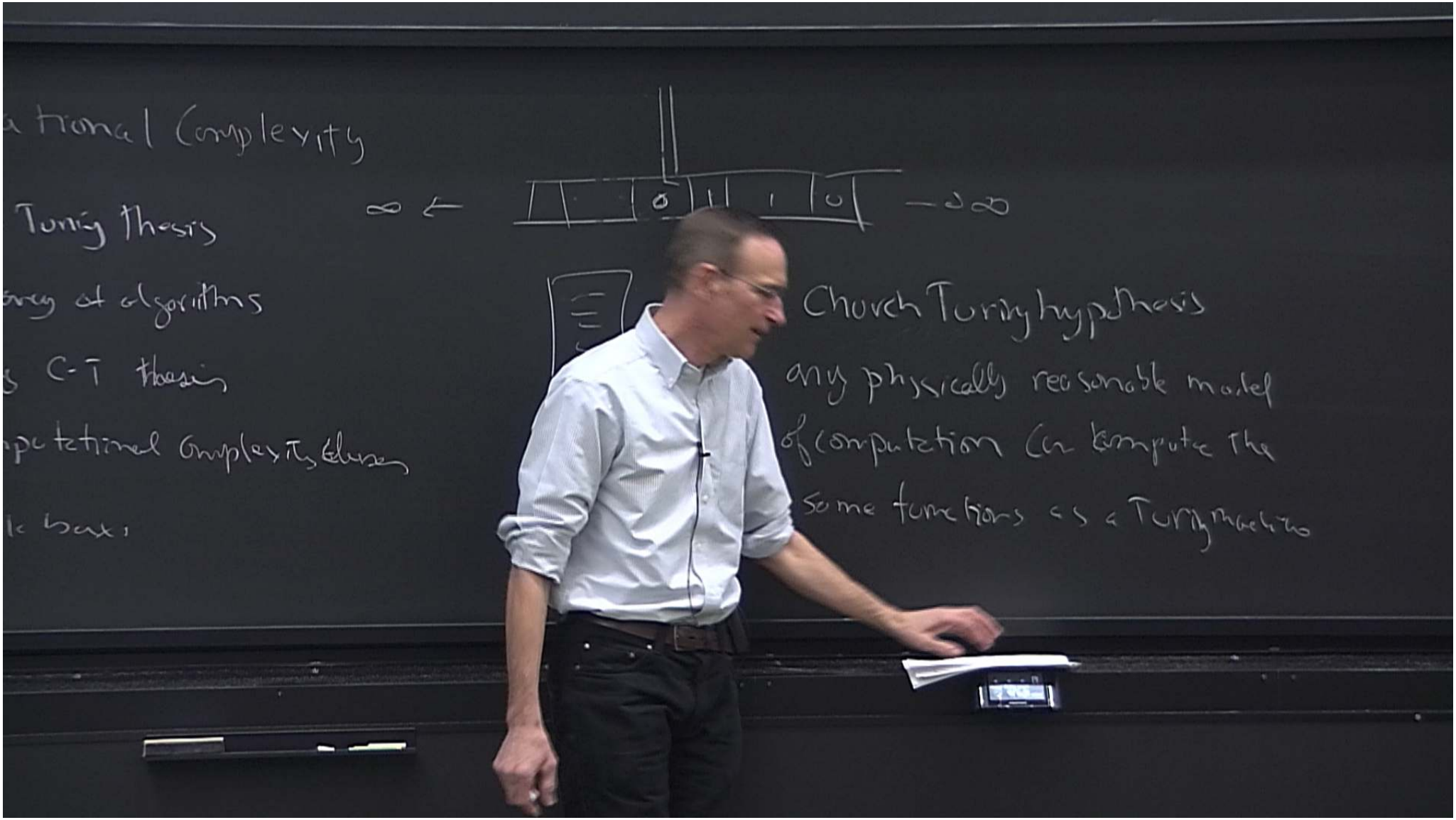
Abstract:

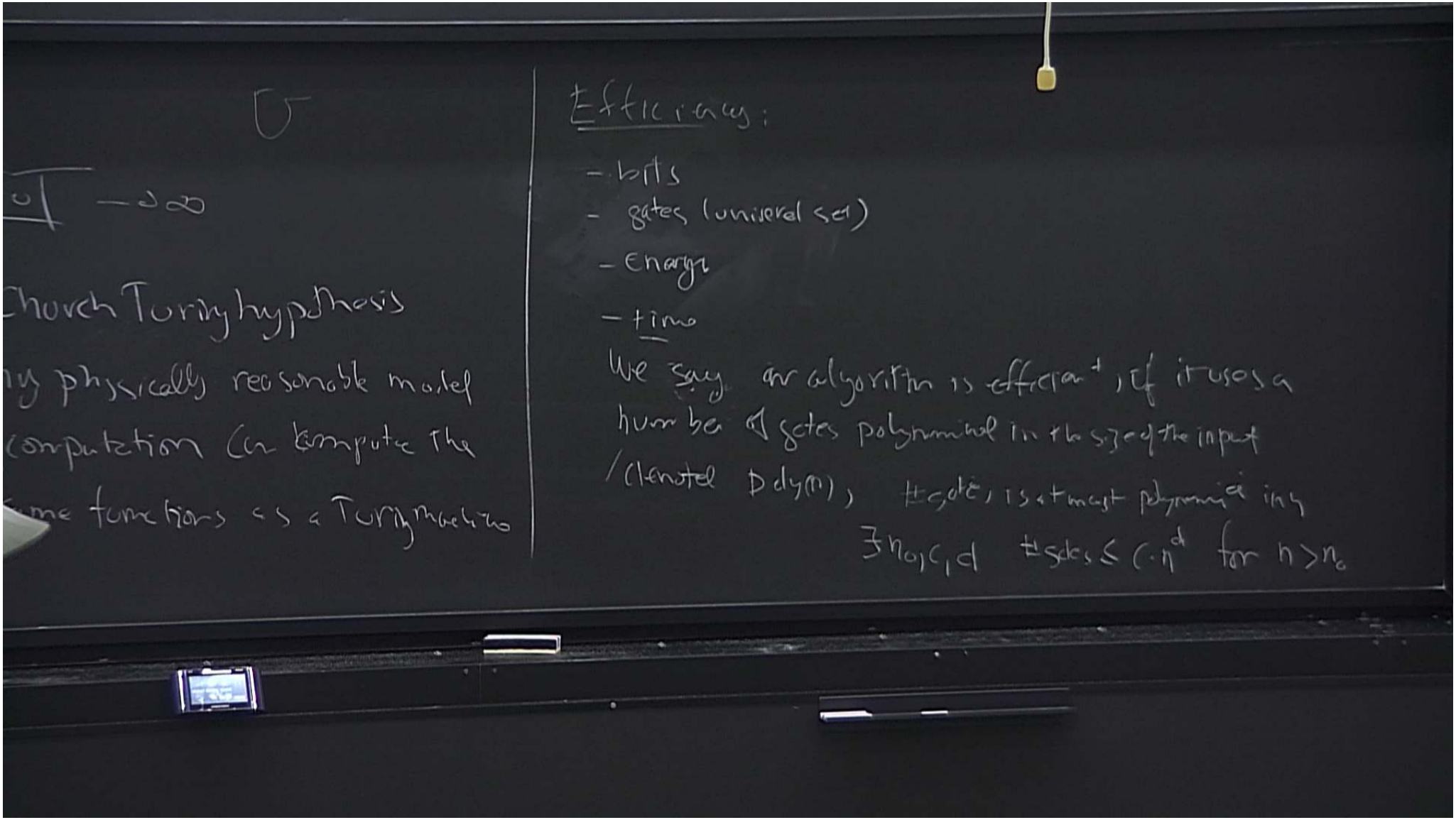

Computational Complexity
- Church Turing thesis
- Efficiency of algorithms
- Strong C-T thesis
- Computational Complexity Theory
- Black box

Computational Complexity

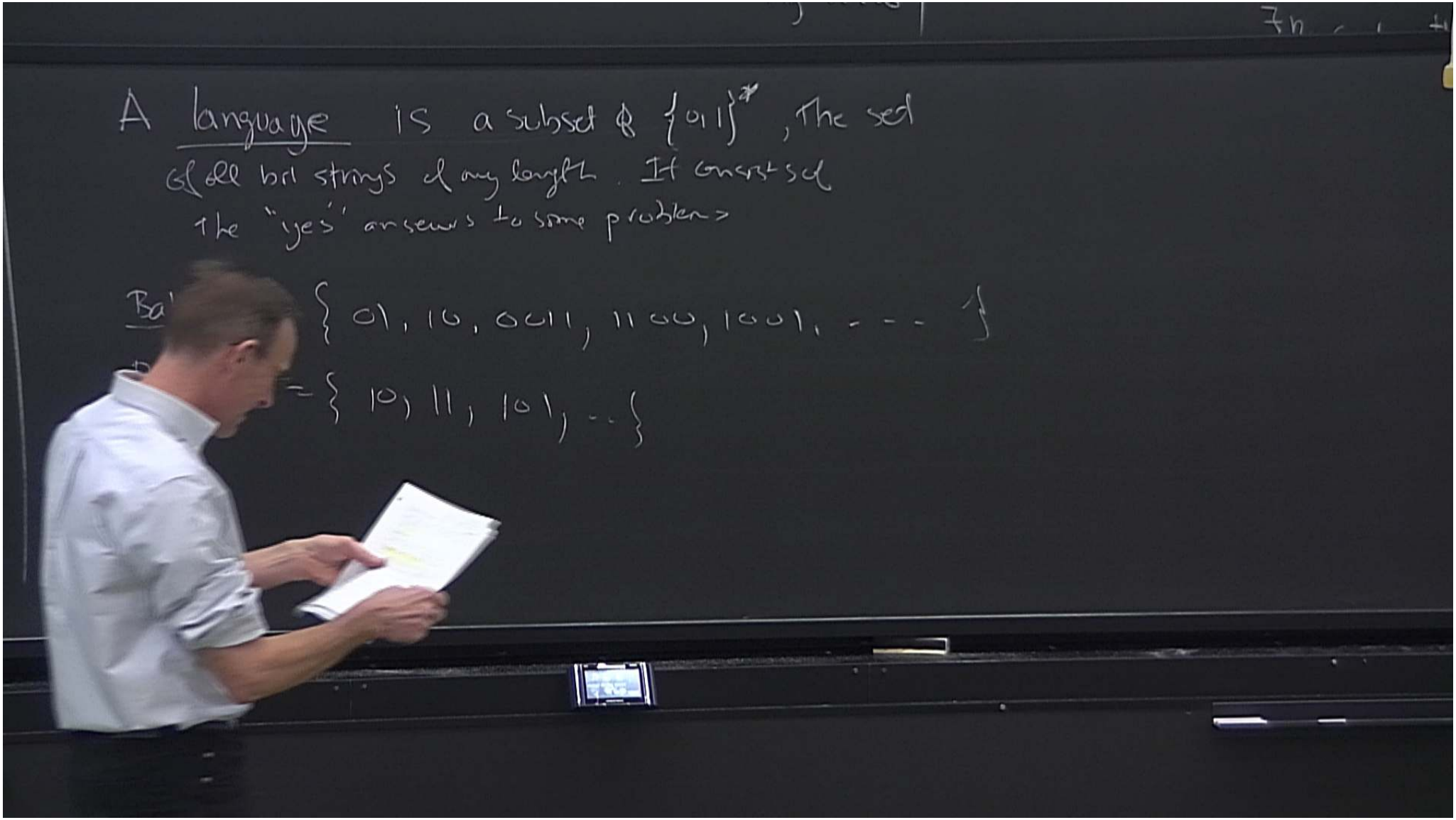
- Church Turing thesis
- Efficiency of algorithms
- Strong C-T thesis
- Computational Complexity theory
- Black box

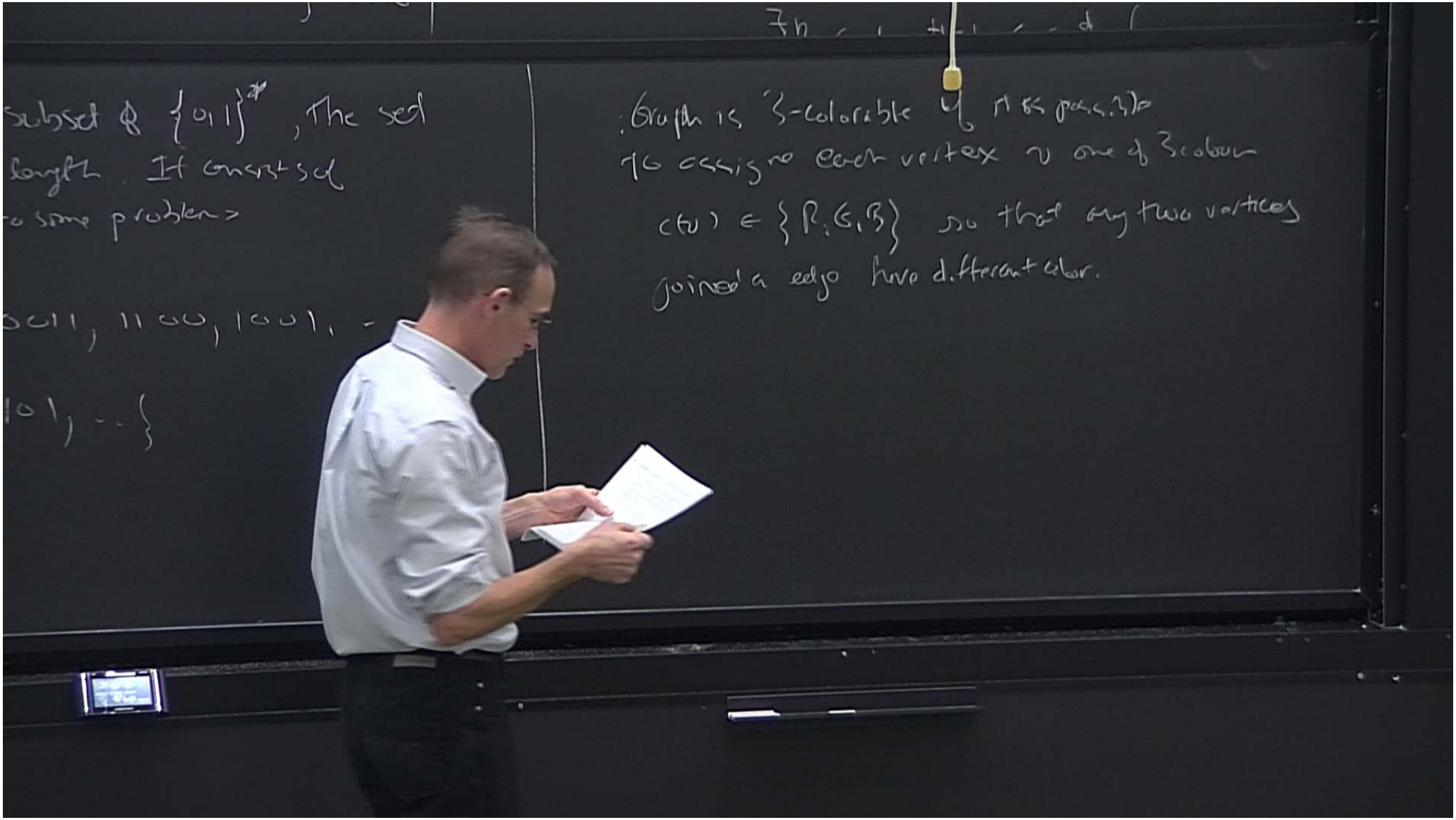



Turing Thesis
Church Turing hypothesis
any physically reasonable model
of computation can compute the
same functions as a Turing machine


Efficiency:
- bits
- gates (universal set)
- Energy
- time
We say an algorithm is efficient, if it uses a
number of gates polynomial in the size of the input
(denoted Poly(n)), #gates is at most polynomial in n
$\exists n_0, c, d$ #gates $\leq c \cdot n^d$ for $n > n_0$
Church Turing hypothesis
any physically reasonable model
computation can compute the
same functions as a Turing machine

A language is a subset of $\{0,1\}^*$, The set of all bit strings of any length. It consists of the "yes" answers to some problem.


A language is a subset of $\{0,1\}^*$, The set of all bit strings of any length. It consists of the "yes" answers to some problem
$\{01, 10, 0011, 1100, 1001, \ldots\}$
$= \{10, 11, 101, \ldots\}$

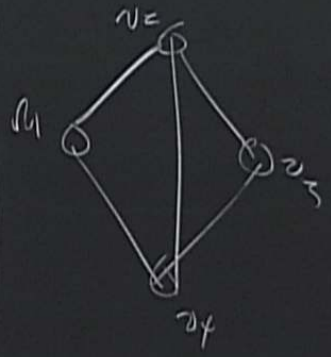

subset of {0,1}*, The set
length. It consists of
to some problem>
0011, 1100, 1001, ...
101, ...}
Graph is 3-colorable if it is possible
to assign each vertex v one of 3 colour
c(v) ∈ {R, G, B} so that any two vertices
joined a edge have different color.

subset of $\{0,1\}^*$, The set
length. It consists of
to some problem>

0011, 1100, 1001, - - - }

101, .. }

Graph is 3-colorable if it is possible
to assign each vertex v one of 3 colour
$c(v) \in \{R, G, B\}$ so that any two vertices
joined a edge have different color.



$e_1 = \{v_1 v_2\}$
$e_2 = \{v_1 v_3\}$
$e_3 = \{v_1 v_4\}$
$e_4 = \{v_2 v_3\}$
$e_5 = \{v_2 v_4\}$
$e_6 = \{v_3 v_4\}$

e_1	e_2	e_3	e_4	e_5	e_6
1	0	1	1	1	1

A complexity class is a set of languages

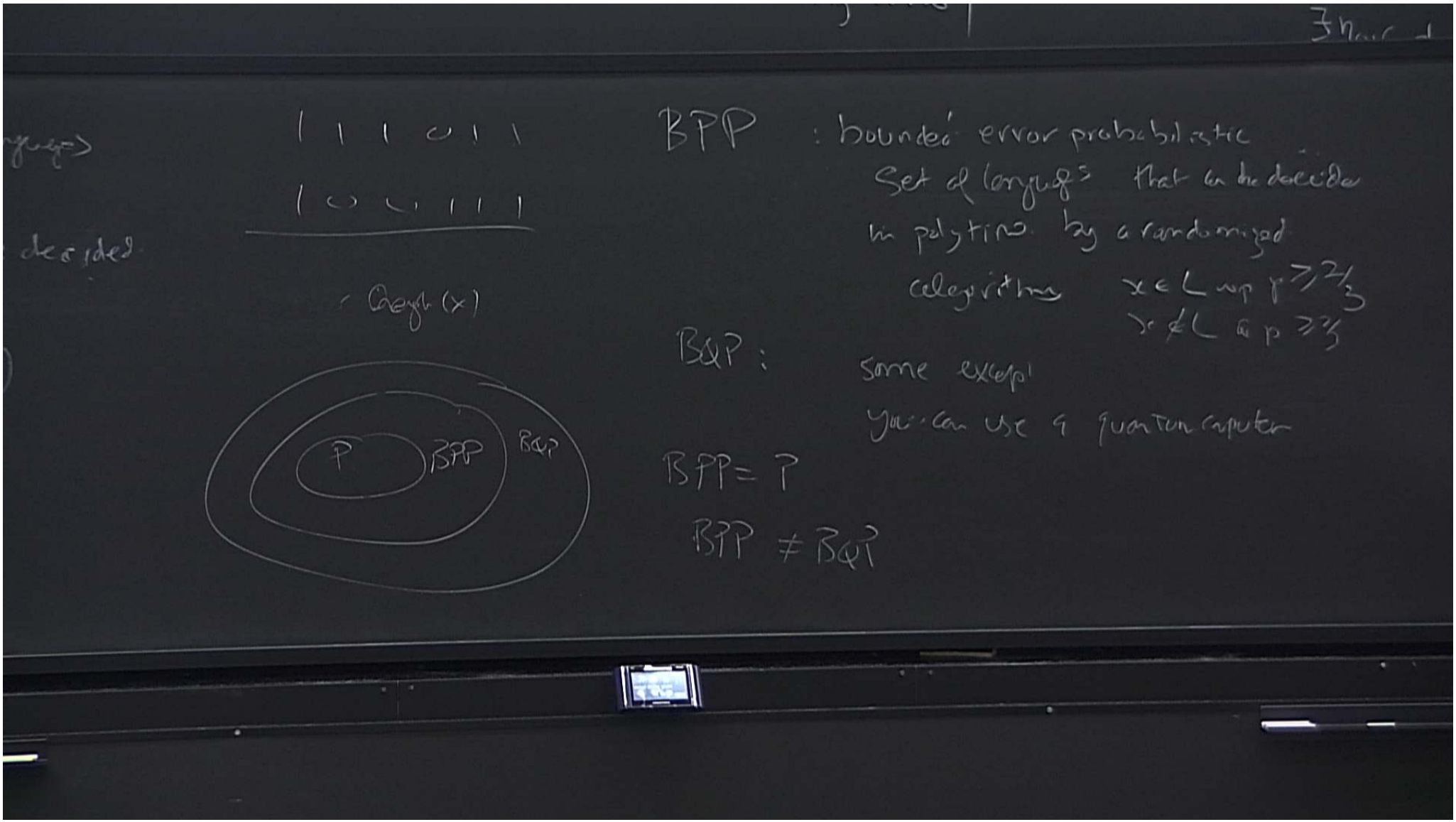
P: set of languages L that can be decided

in poly(time), on input x

poly(length(x))

accept: $x \in L$

reject: $x \in L'$


BPP : bounded error probabilistic
Set of languages that can be decided
in polytime by a randomized
algorithm x ∈ L w.p. ≥ 2/3
x ∉ L w.p. ≥ 2/3
BQP :
some except
you can use a quantum computer
BPP = P
BPP ≠ BQP
P
BPP
BQP
decided

A complexity class is a set of languages

P: set of languages L that can be decided in polynomial time, on input x

poly(length(x))

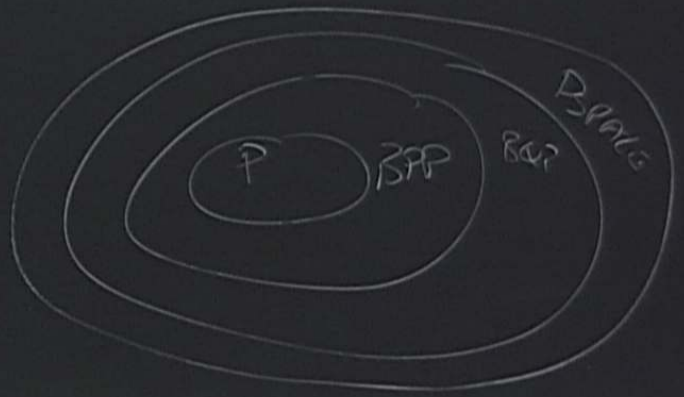
accept $x \in L$

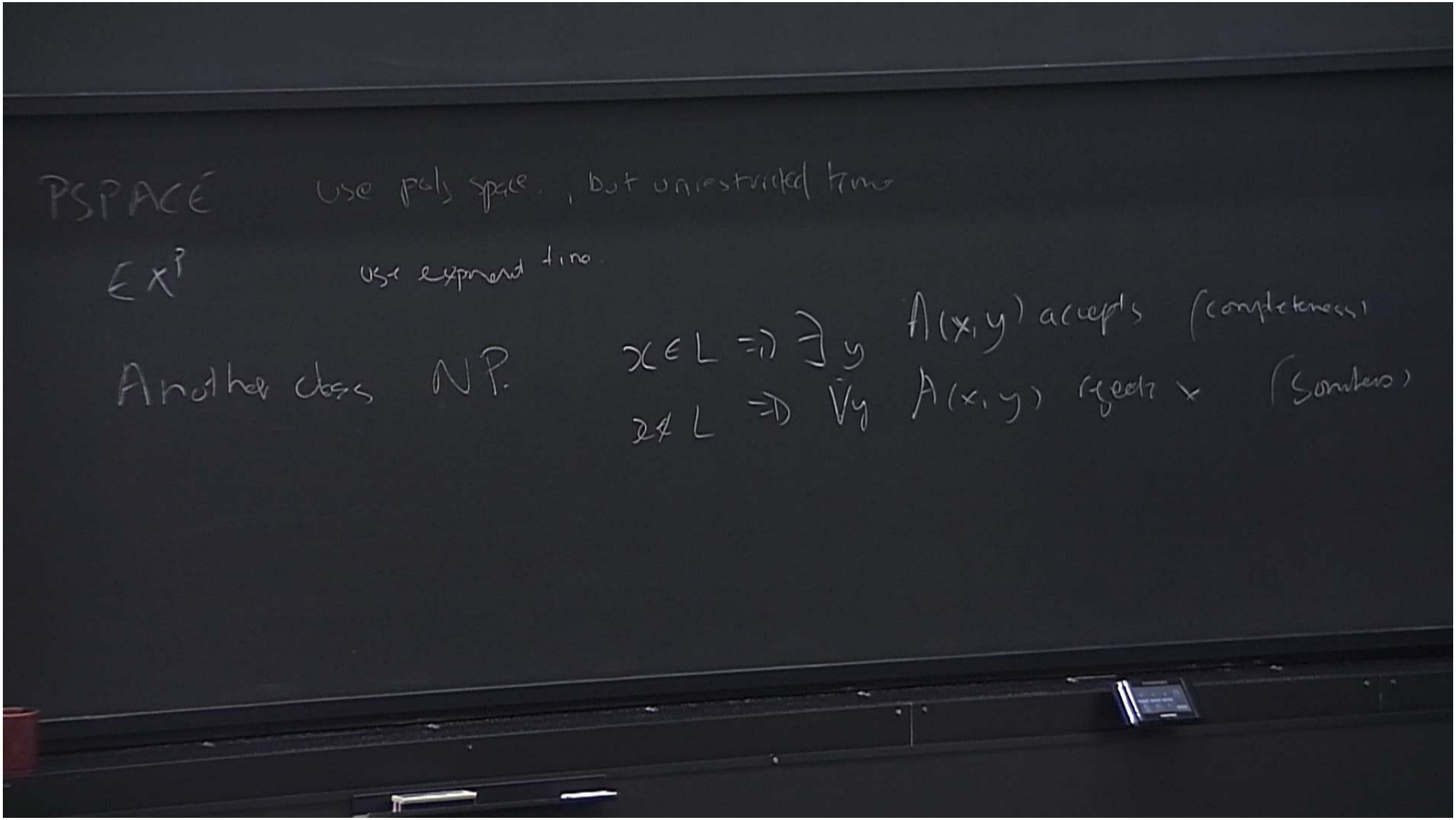
reject $x \notin L'$

BPP

length(x)

BQP:




PSPACE use poly space, but unrestricted time
EXP use exponential time
Another class NP.
$x \in L \Rightarrow \exists y$ $A(x,y)$ accepts (completeness)
$x \notin L \Rightarrow \forall y$ $A(x,y)$ rejects x (Soundness)