Title: PSI 2015/2016 Quantum Information - Lecture 8

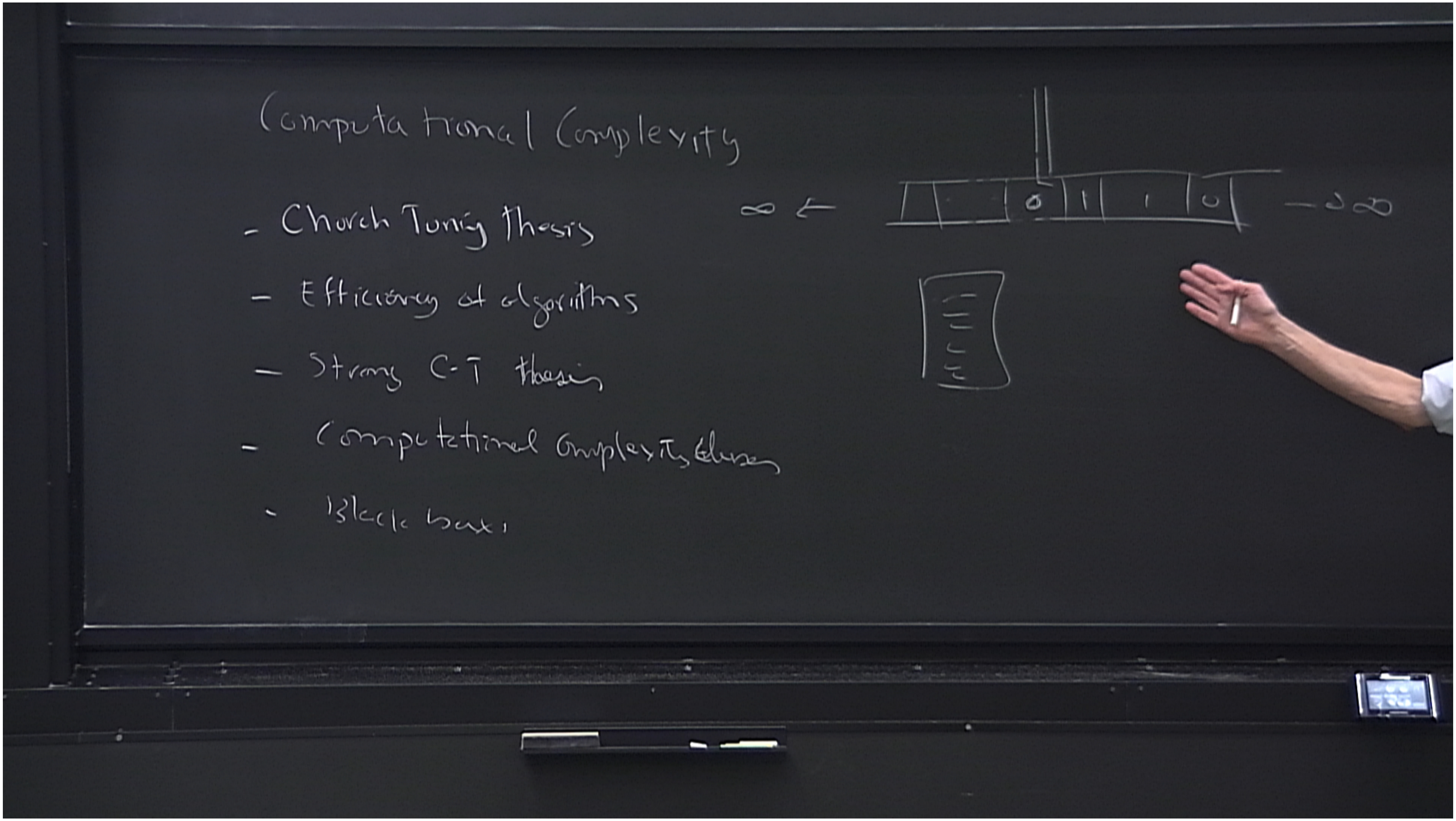
Date: Mar 02, 2016 11:30 AM

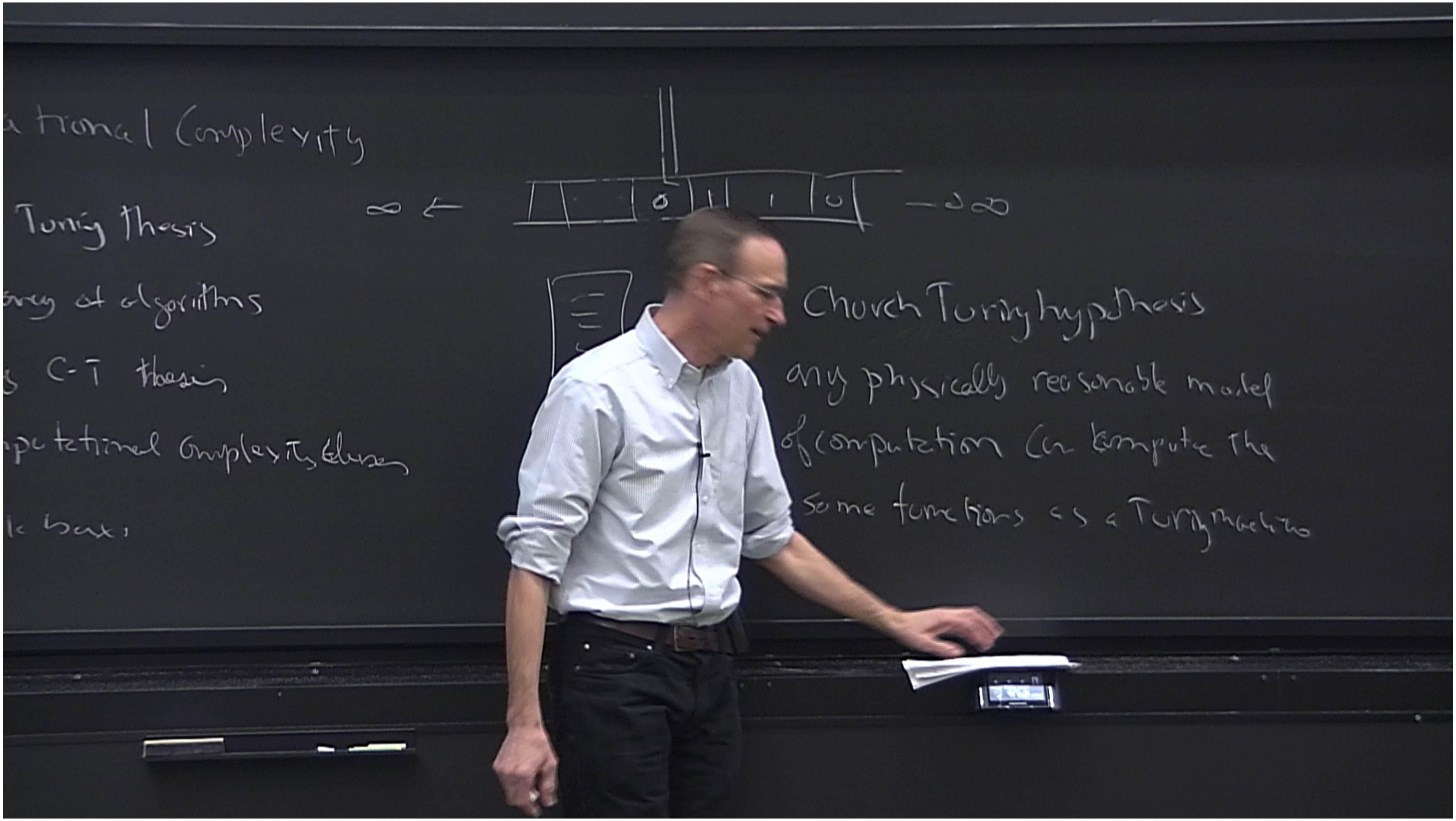
URL: http://pirsa.org/16030055

Abstract:

Computational Complexity

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


Computational Complexity
- Church Turing thesis
- Efficiency of algorithms
- Strong C-T thesis
- Computational Complexity Classes
- Black box
∞ ←
0
1
1
0
→ ∞


ational Complexity
Turing thesis
ory of algorithms
C-T thesis
Church Turing hypothesis
any physically reasonable model
of computation can compute the
same functions as a Turing machine

U

UT — ∞

Church Turing hypothesis

...ny physically reasonable model
computation can compute the
...me functions as a Turing machine

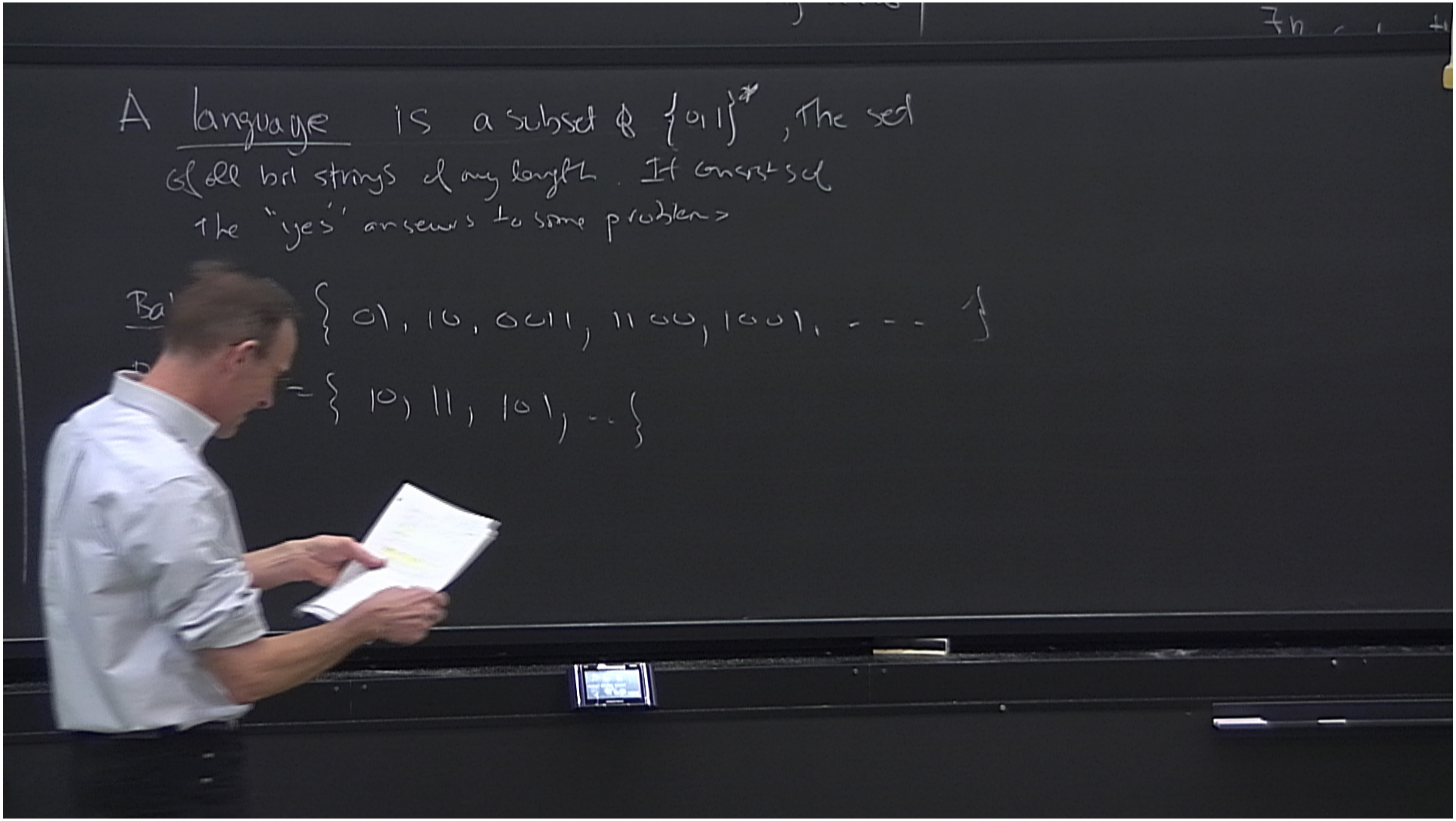
Efficiency:

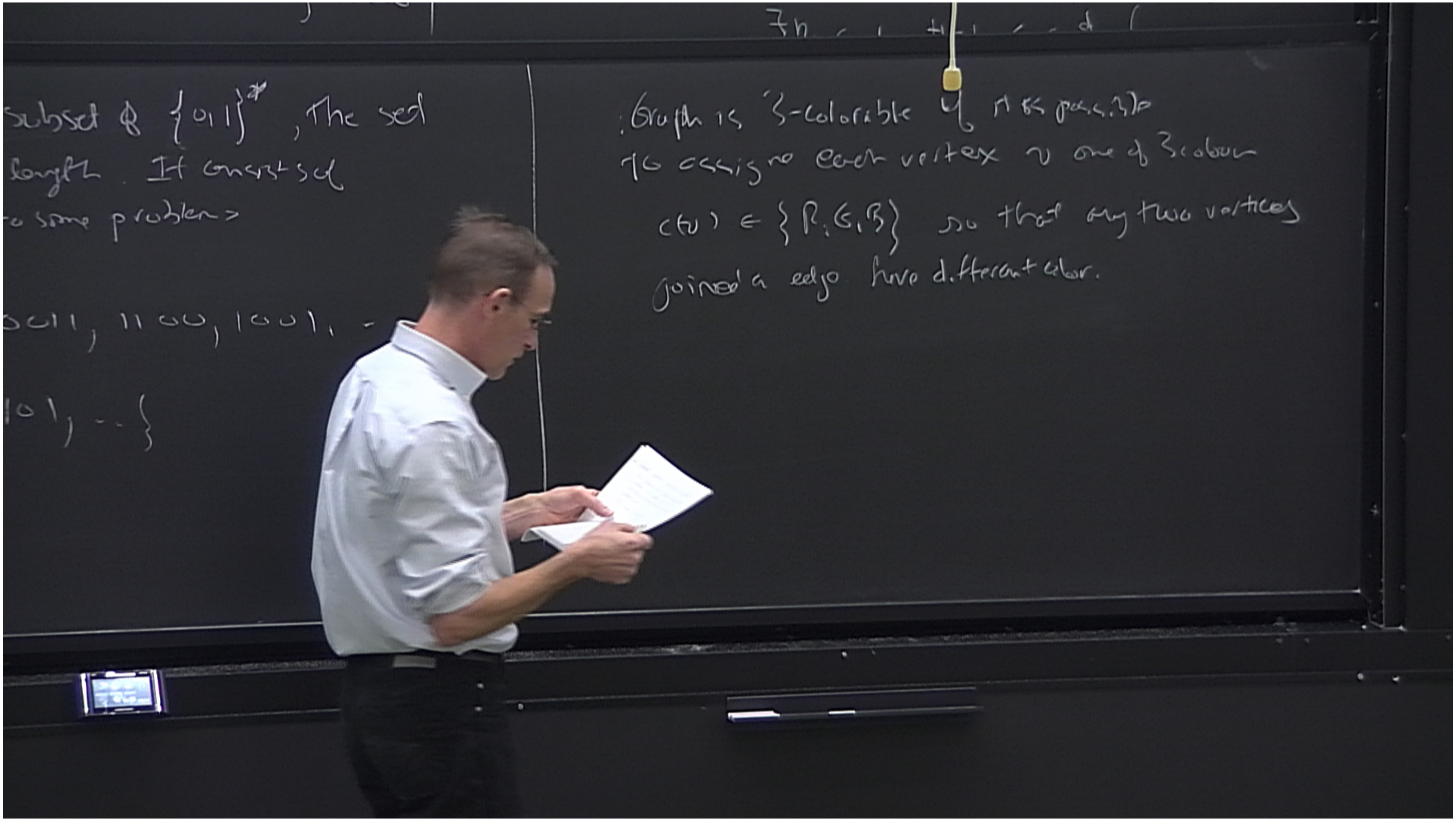
- bits
- gates (universal set)
- energy
- time

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

$\exists\, n_0, c, d \quad \#\text{gates} \leq c \cdot n^d$ for $n > n_0$

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 problems
{01, 10, 0011, 1100, 1001, ...}
= {10, 11, 101, ...}

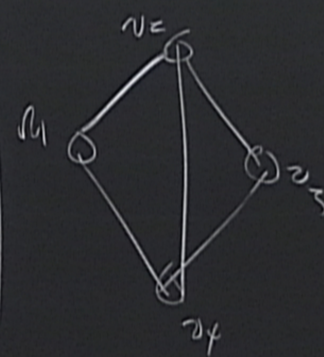

subset of $\{0,1\}^*$, The set
length. If consists of
to some problem
0011, 1100, 1001, ...
101, ...}
Graph is 3-colorable if it is possible
to assign to each vertex v one of 3 colors
$c(v) \in \{R, G, B\}$ so that any two vertices
joined a edge have different color.

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

$\ldots 011, 1100, 1001, \ldots \}$

$101, \ldots \}$

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



$e_1 = \{v_1, v_2\}$

$e_2 = \{v_1, v_2\}$

$e_3 = \{v_1, v_4\}$

$e_4 = \{v_2\ v_3\}$

$e_5 = \{v_2\ v_4\}$

$e_6 = \{v_3\ v_4\}$

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

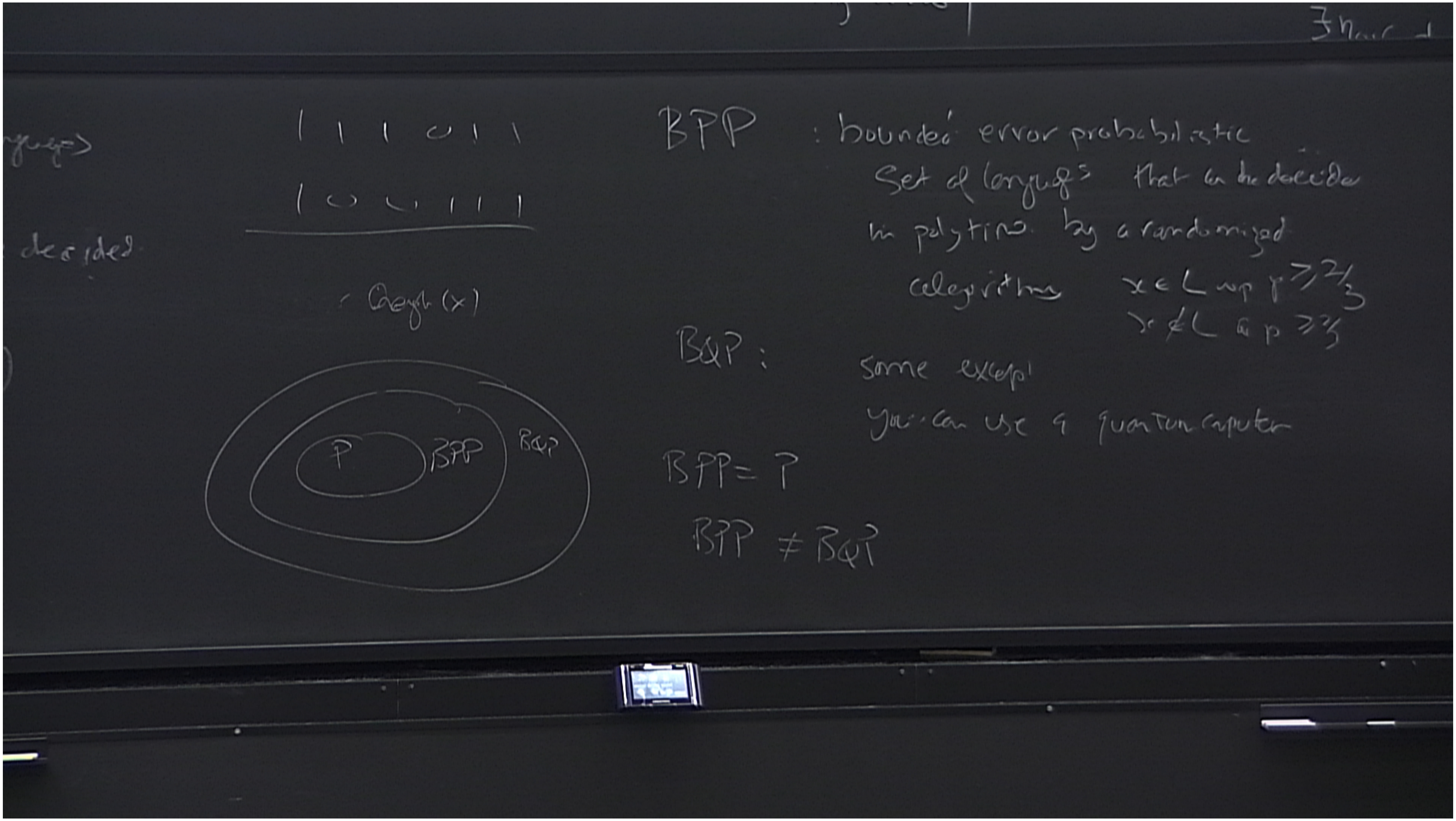
P: set of languages L that can be decided

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
BQP :
You can use a quantum computer
BPP = P
BPP ≠ BQP
P
BPP
BQP
length(x)
decided

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 $x \in L'$

1 1 1 0 1 1 1

1 0 0 0 1 1 1

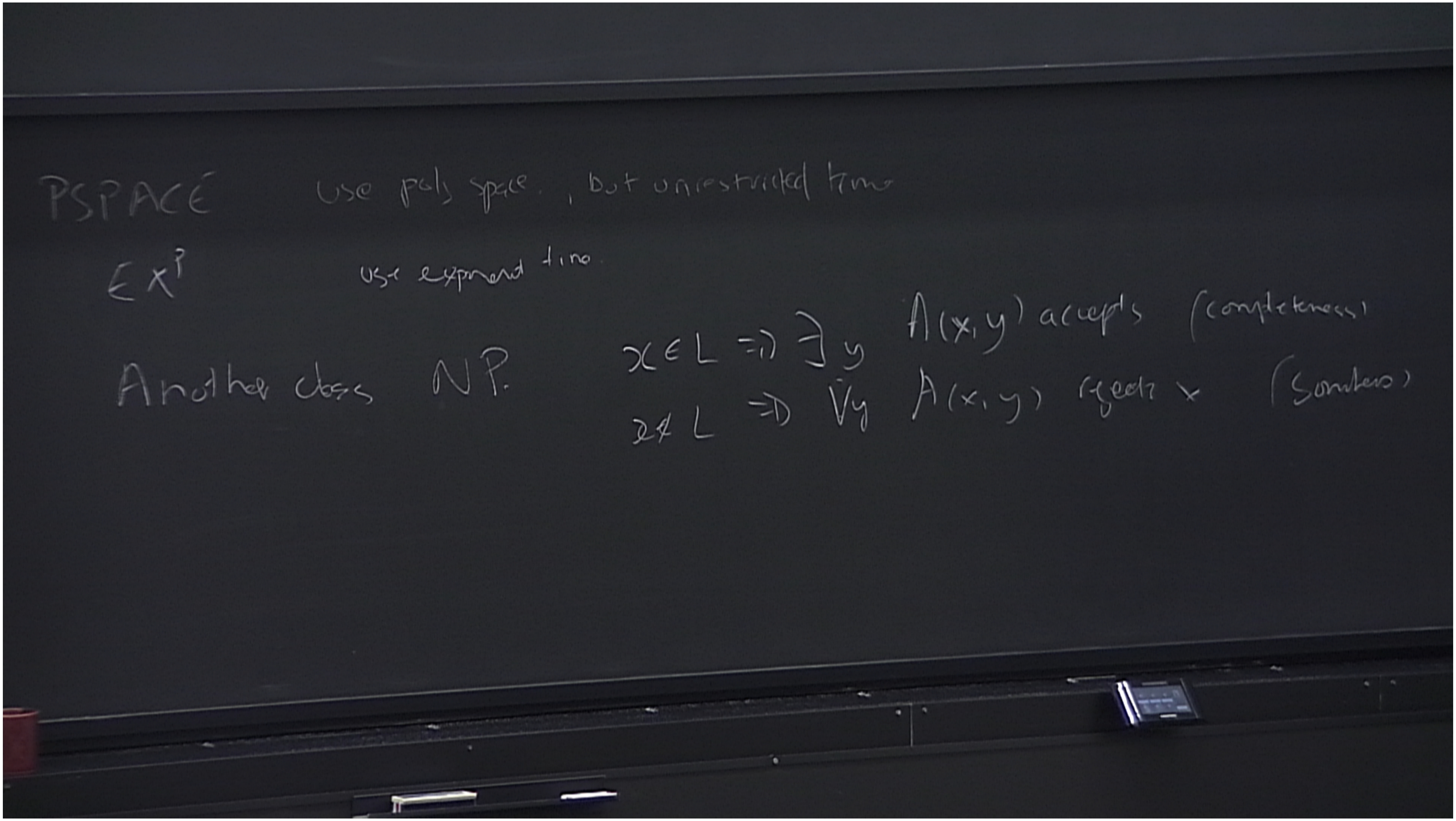
~ length(x)

BPP

BQP :

BPP = P

BPP ≠


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)