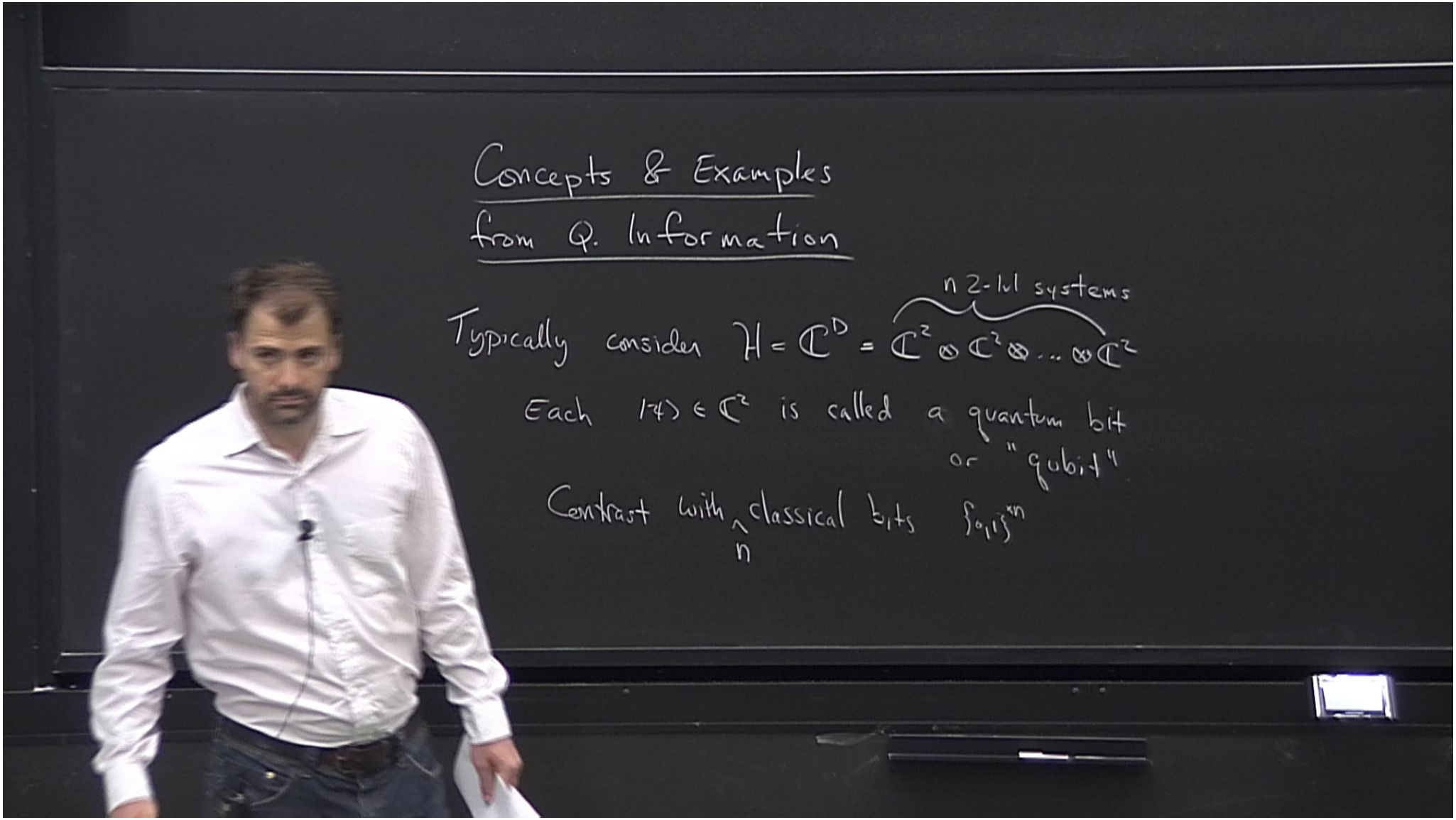
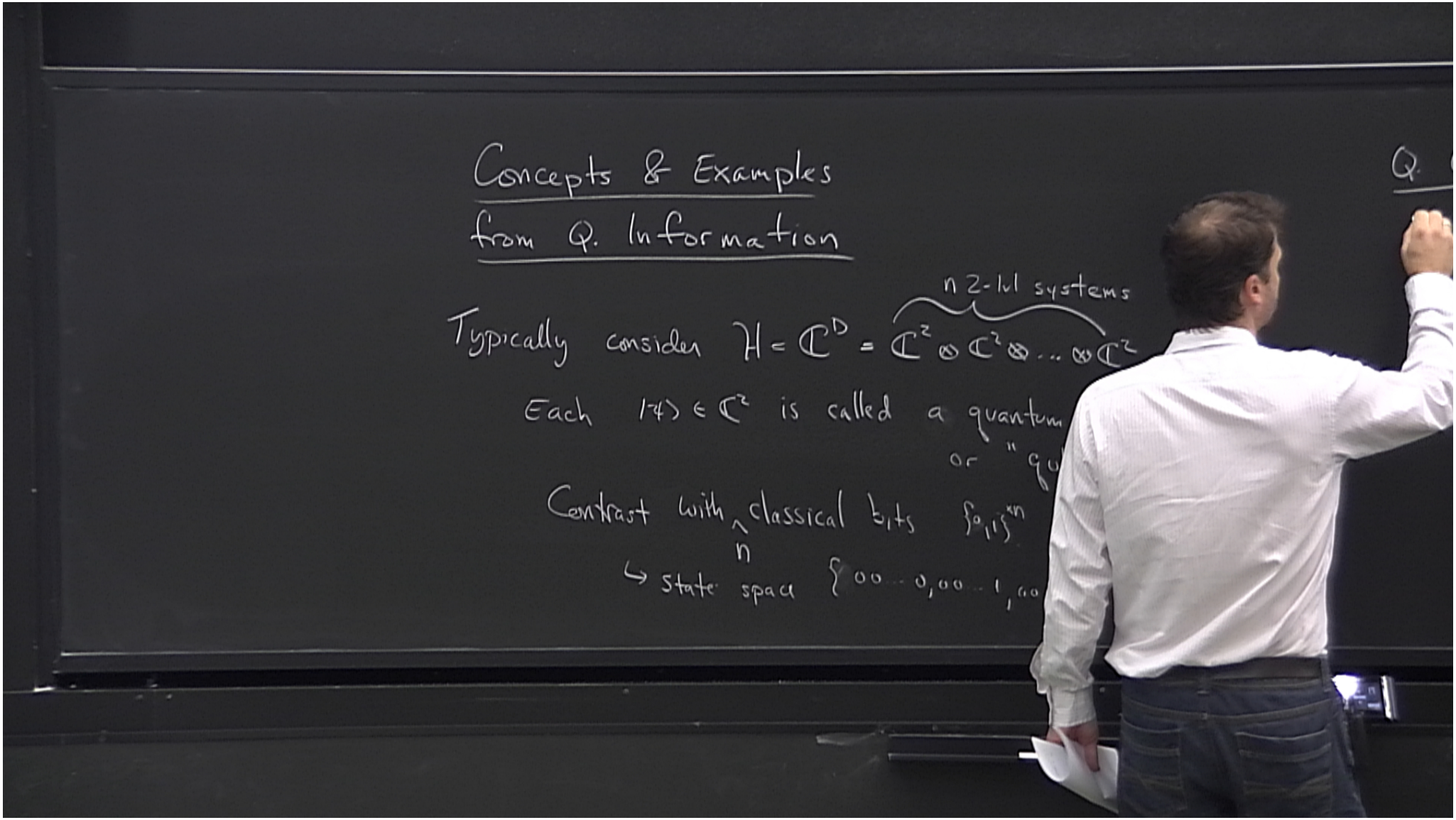
Title: Quantum Theory - Lecture 15

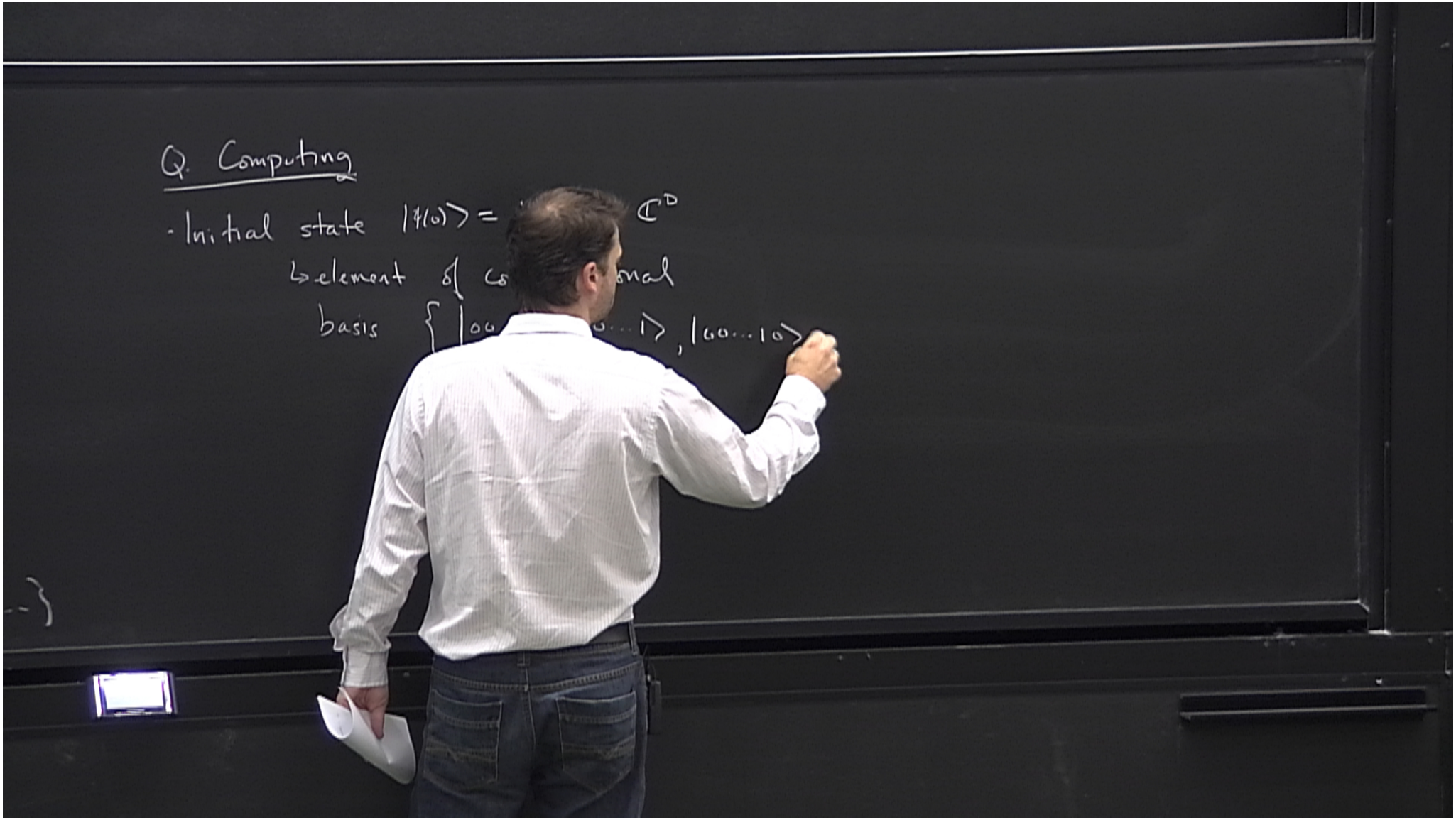
Date: Sep 28, 2012 09:00 AM

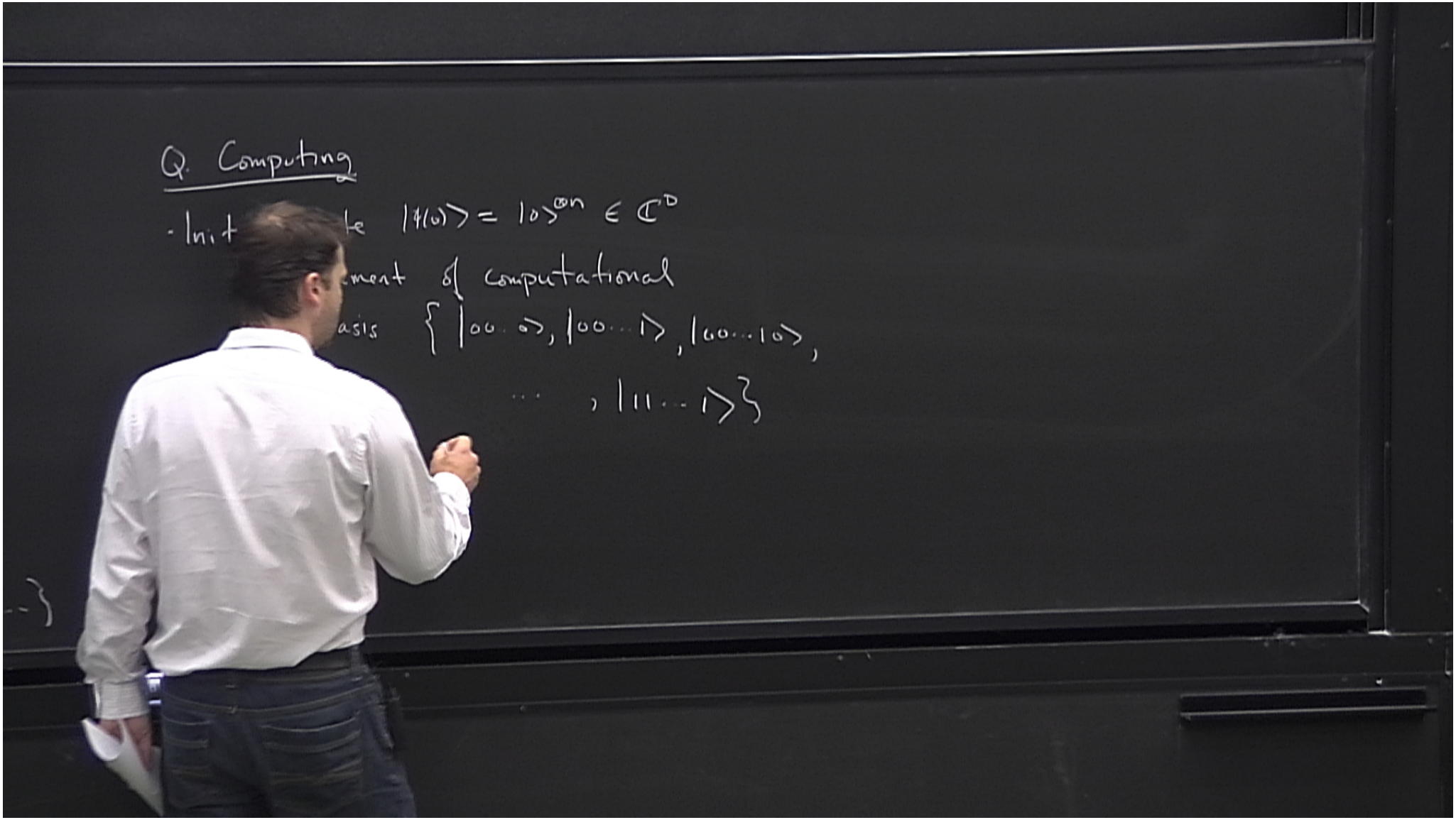
URL: http://pirsa.org/12090018

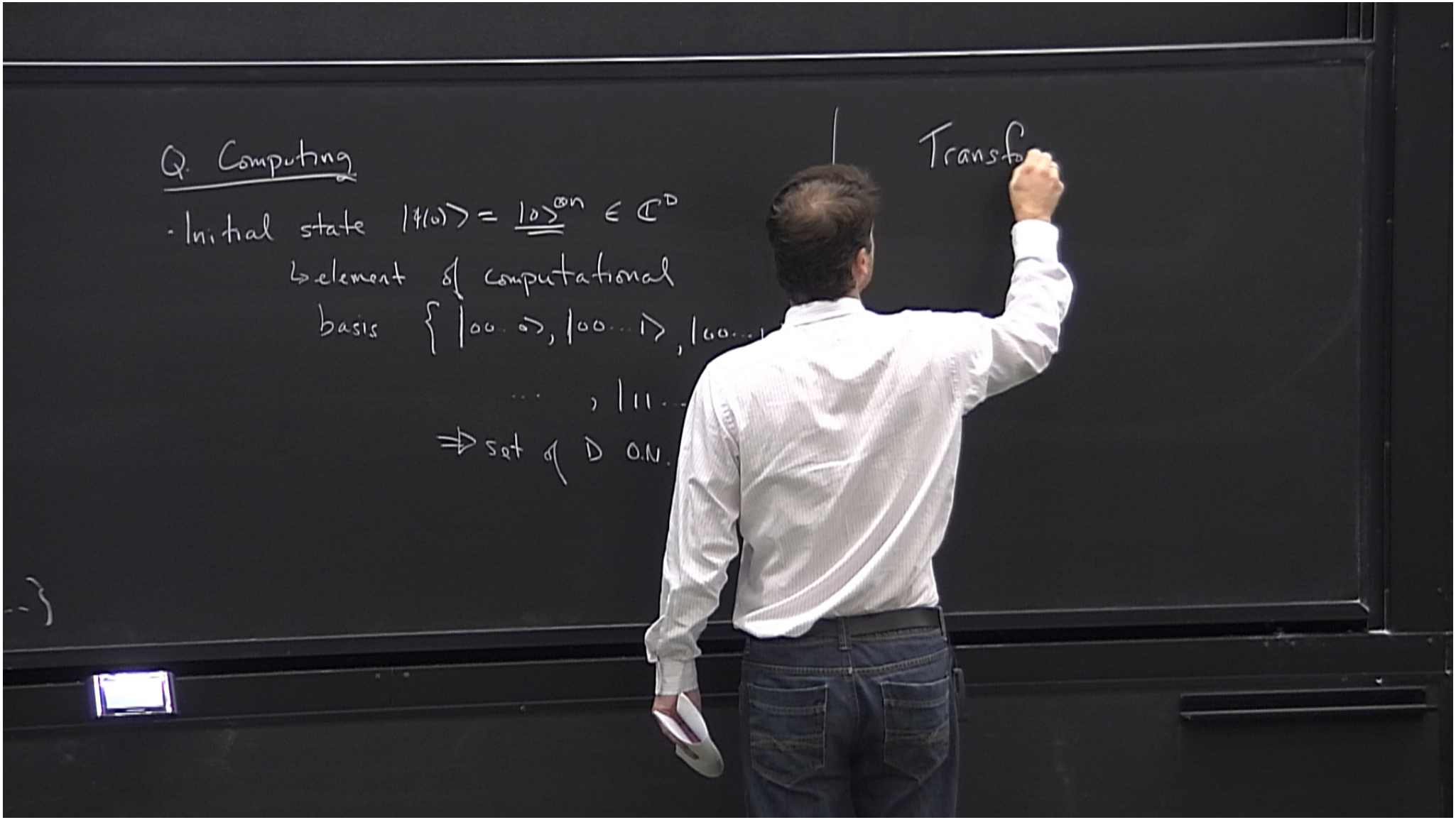
Abstract:

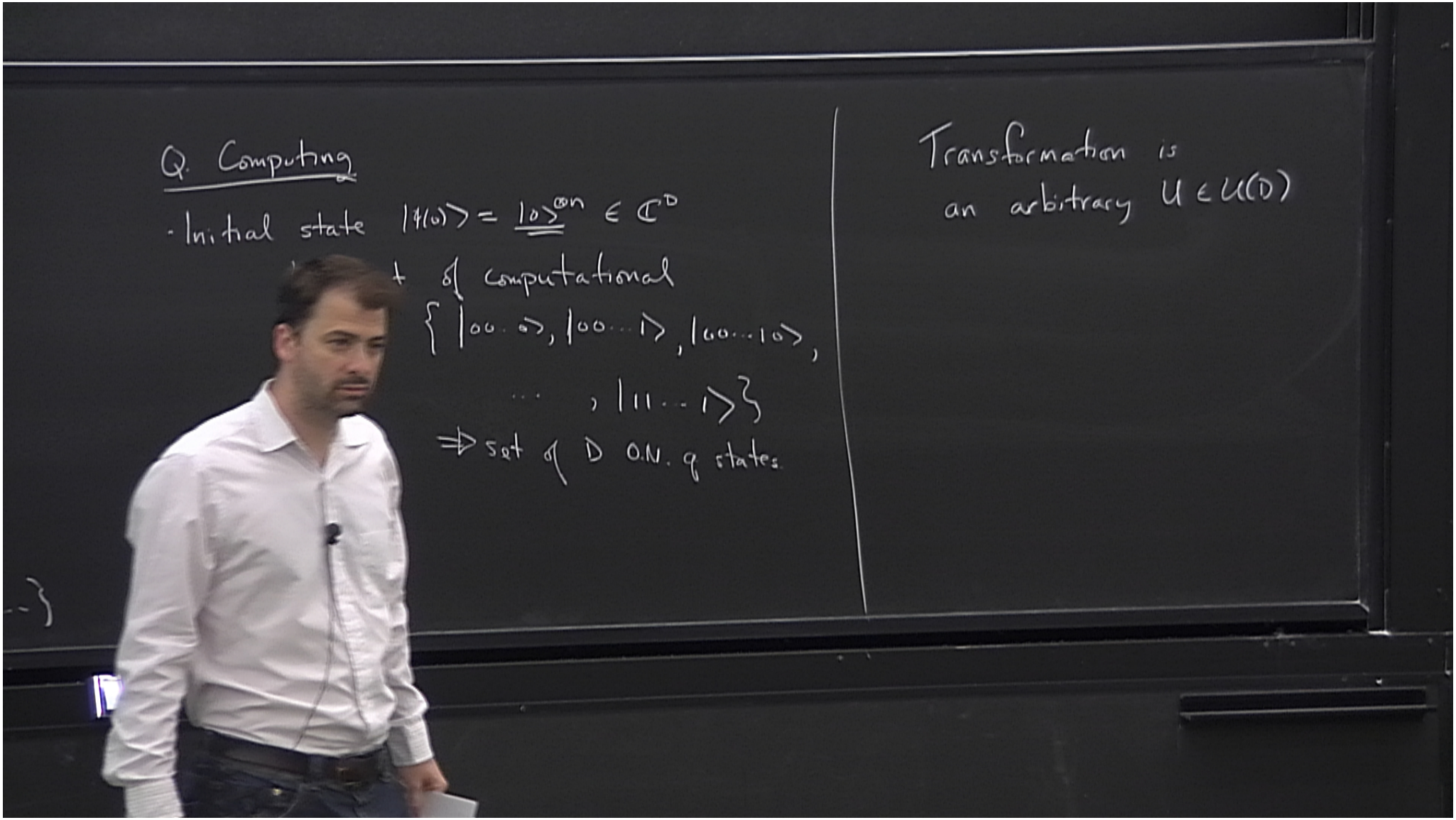

Concepts & Examples
from Q. Information
n 2-lvl systems
Typically consider $\mathcal{H} = \mathbb{C}^D = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$
Each $|\psi\rangle \in \mathbb{C}^2$ is called a quantum bit
or "qubit"
Contrast with $\uparrow_n$ classical bits $\{0,1\}^n$

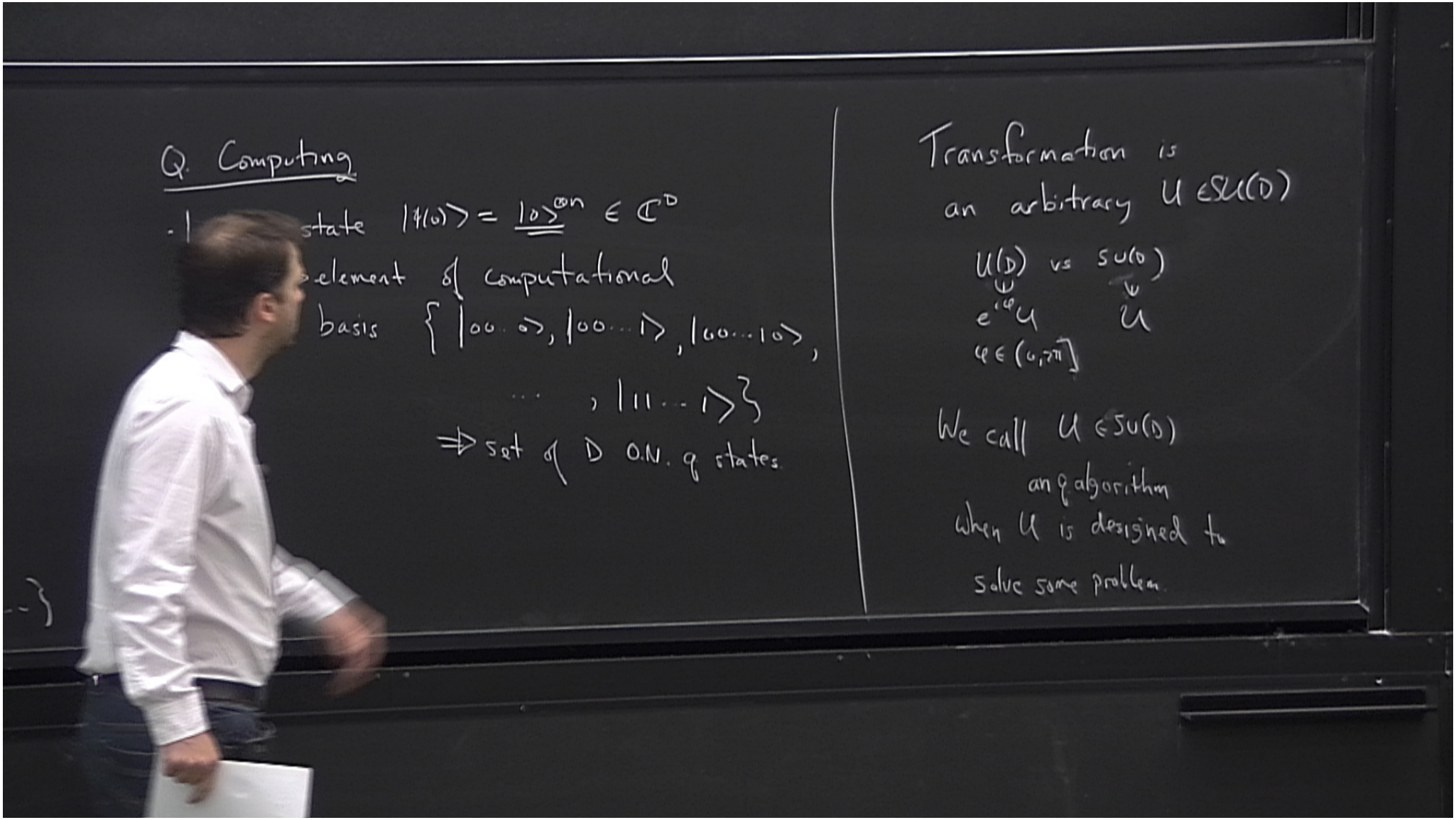

Concepts & Examples
from Q. Information
n 2-lvl systems
Typically consider $\mathcal{H} = \mathbb{C}^D = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$
Each $|\psi\rangle \in \mathbb{C}^2$ is called a quantum
Contrast with n classical bits $\{0,1\}^n$
↳ state space $\{00\dots0, 00\dots1, 00$

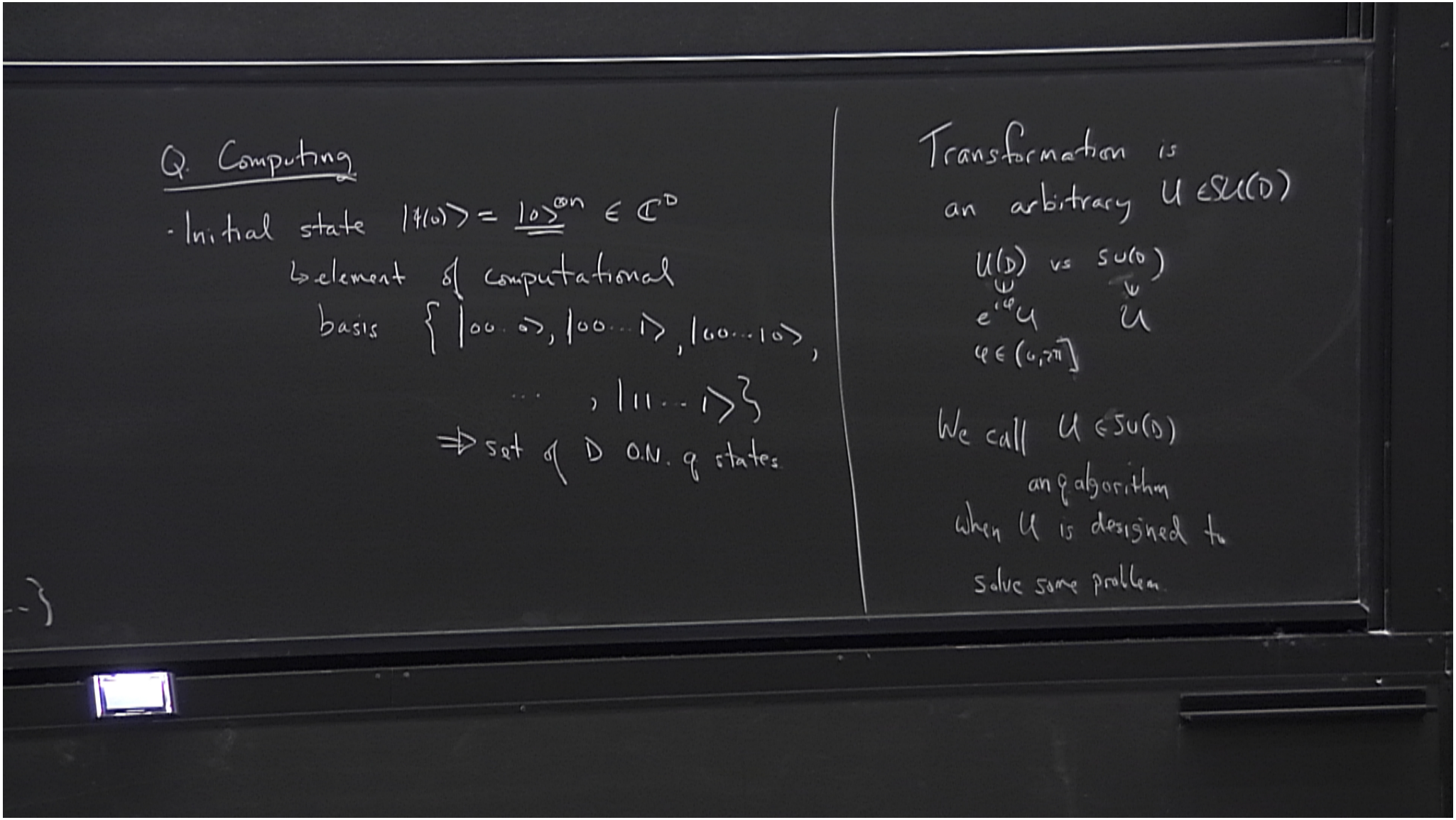

Q. Computing
- Initial state
basis


Q. Computing
- Init
te $|\psi(0)\rangle = |0\rangle^{\otimes n} \in \mathbb{C}^D$
ment of computational
asis $\{|00\ldots0\rangle, |00\ldots1\rangle, |00\ldots10\rangle,$
$\ldots, |11\ldots1\rangle\}$


Q. Computing
Transfo
· Initial state $|\psi(0)\rangle = |0\rangle^{\otimes n} \in \mathbb{C}^D$
↳ element of computational
basis $\{|00\ldots0\rangle, |00\ldots1\rangle, |00\ldots$
$\ldots, |11\ldots$
⇒ set of D O.N.


Q. Computing
· Initial state $|\psi(0)\rangle = |0\rangle^{\otimes n} \in \mathbb{C}^D$
+ of computational
$\{|00\ldots0\rangle, |00\ldots1\rangle, |00\ldots10\rangle,$
$\ldots, |11\ldots1\rangle\}$
⇒ set of D O.N. q states
Transformation is
an arbitrary $U \in U(D)$


Q. Computing
state $|\psi(0)\rangle = |0\rangle^{\otimes n} \in \mathbb{C}^D$
element of computational
basis $\{|00\ldots0\rangle, |00\ldots1\rangle, |00\ldots10\rangle,$
$\ldots, |11\ldots1\rangle\}$
$\Rightarrow$ set of D O.N. q states
Transformation is
an arbitrary $U \in SU(D)$
$U(D)$ vs $SU(D)$
$e^{i\varphi}U$ U
$\varphi \in (0, 2\pi]$
We call $U \in SU(D)$
an algorithm
when U is designed to
solve some problem


Q. Computing
- Initial state $|\psi(0)\rangle = |0\rangle^{\otimes n} \in \mathbb{C}^D$
b element of computational basis $\{|00\ldots0\rangle, |00\ldots1\rangle, |00\ldots10\rangle, \ldots, |11\ldots1\rangle\}$
⇒ set of D O.N. q states
Transformation is an arbitrary $U \in SU(D)$
$U(D)$ vs $SU(D)$
$e^{i\varphi}U$ U
$\varphi \in (0, 2\pi]$
We call $U \in SU(D)$ an algorithm when U is designed to solve some problem.

Q. Computing

- Initial state $|\psi(0)\rangle = |0\rangle^{\otimes n} \in \mathbb{C}^D$

  ↳ element of computational basis $\{|00\ldots0\rangle, |00\ldots1\rangle, |00\ldots10\rangle, \ldots, |11\ldots1\rangle\}$

  ⇒ set of D O.N. q states

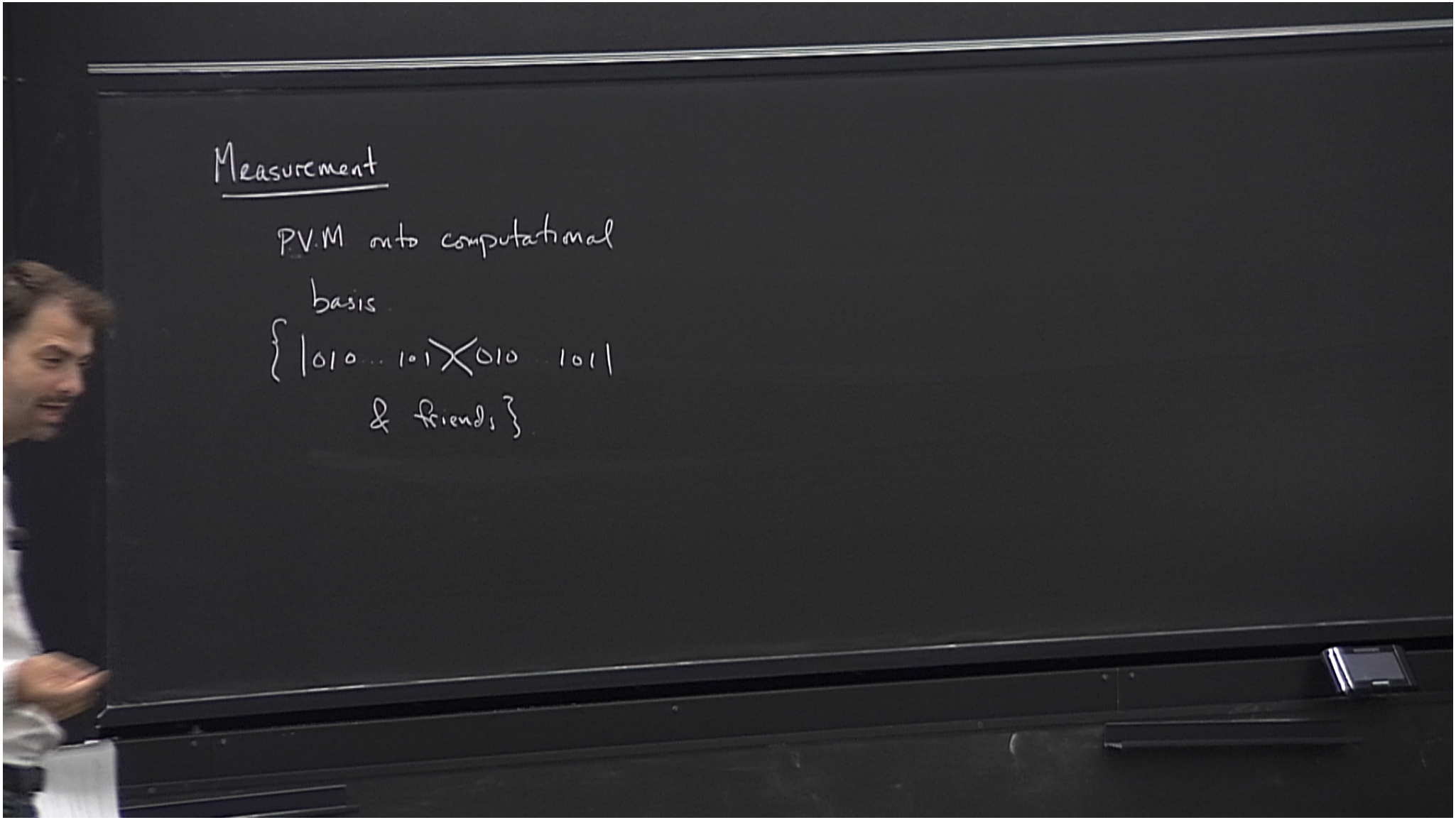
Transformation is an arbitrary $U \in SU(D)$

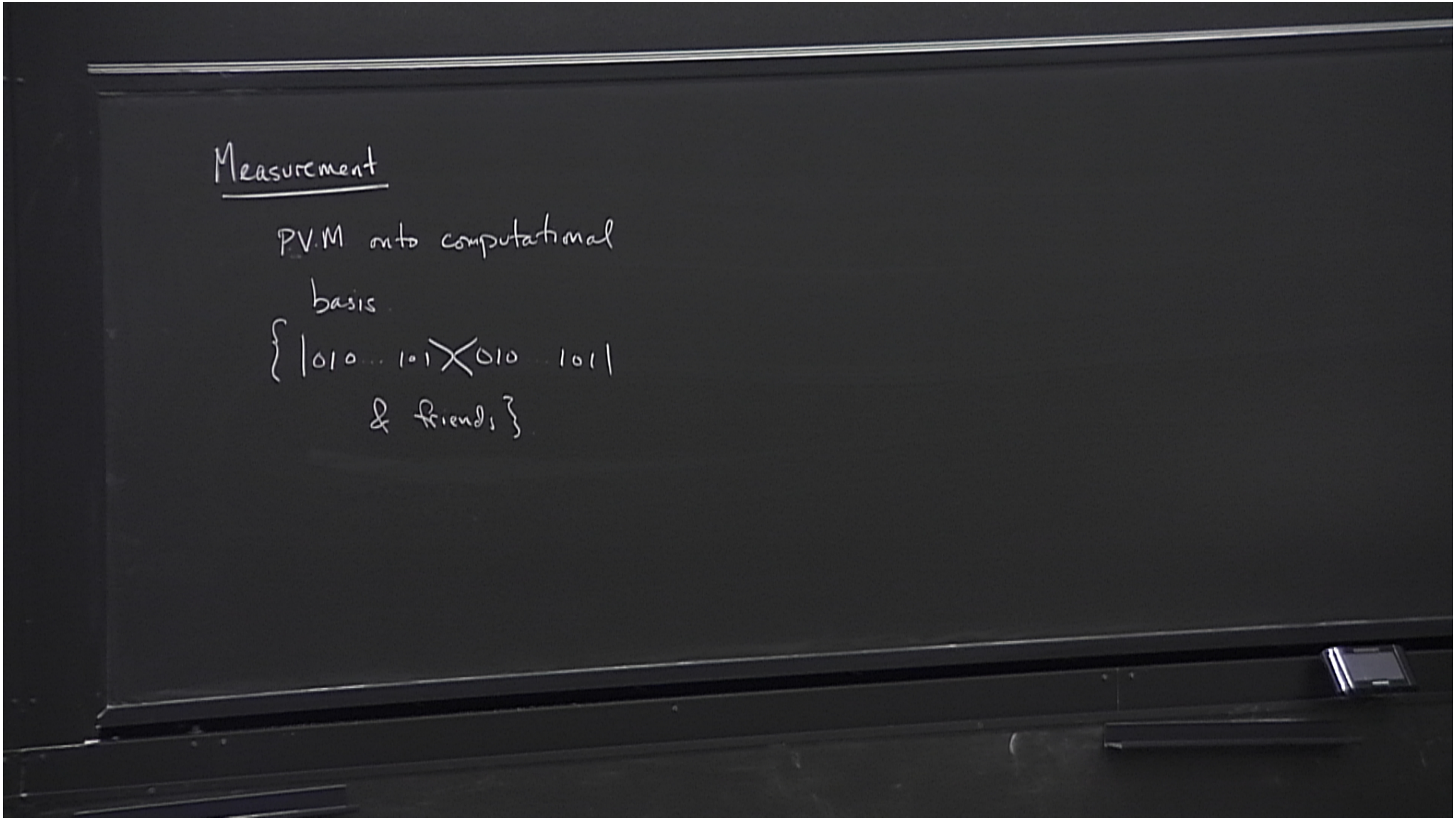
$U(D)$ vs $SU(D)$

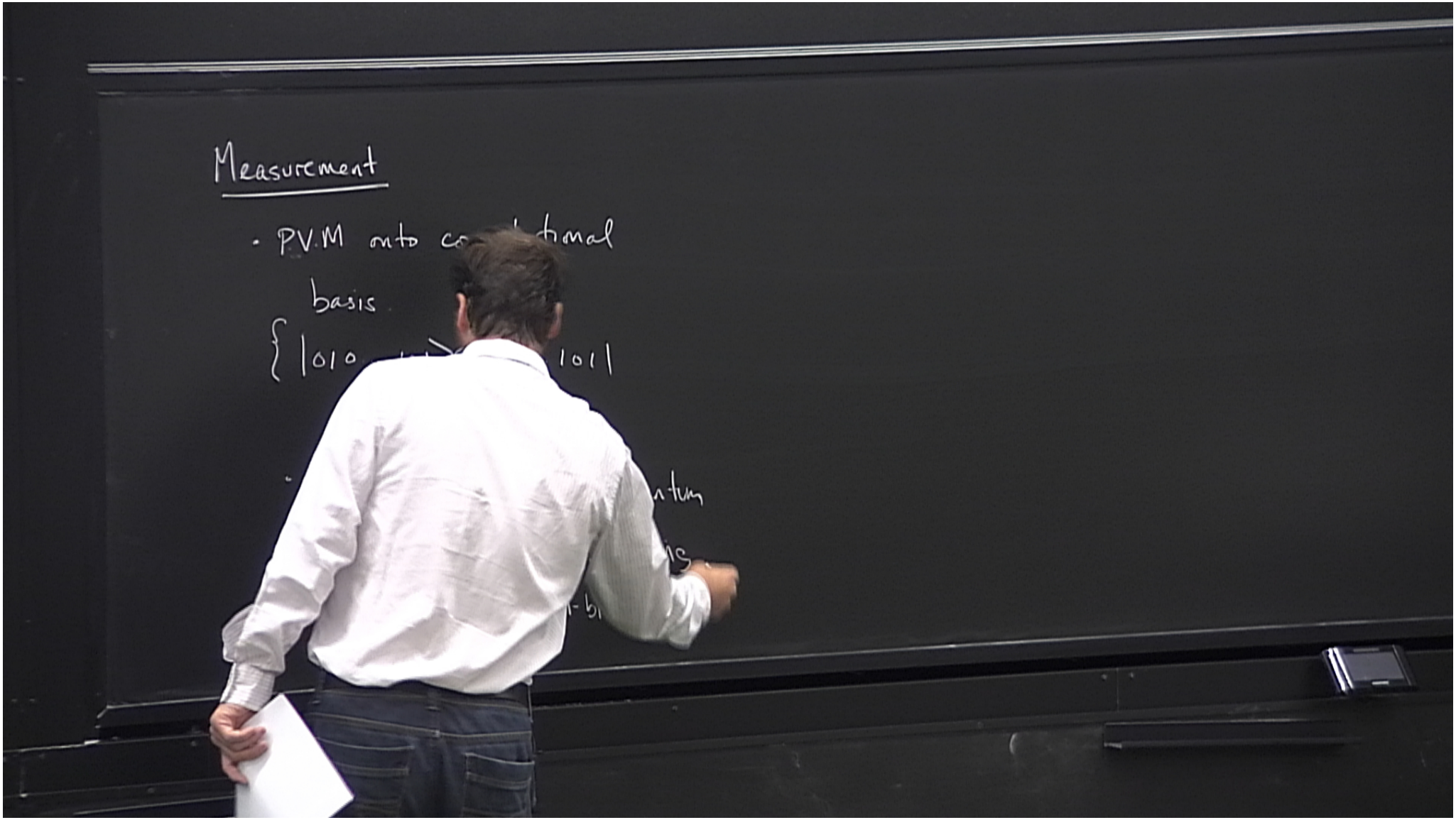
$e^{i\varphi}U$ $\quad$ U

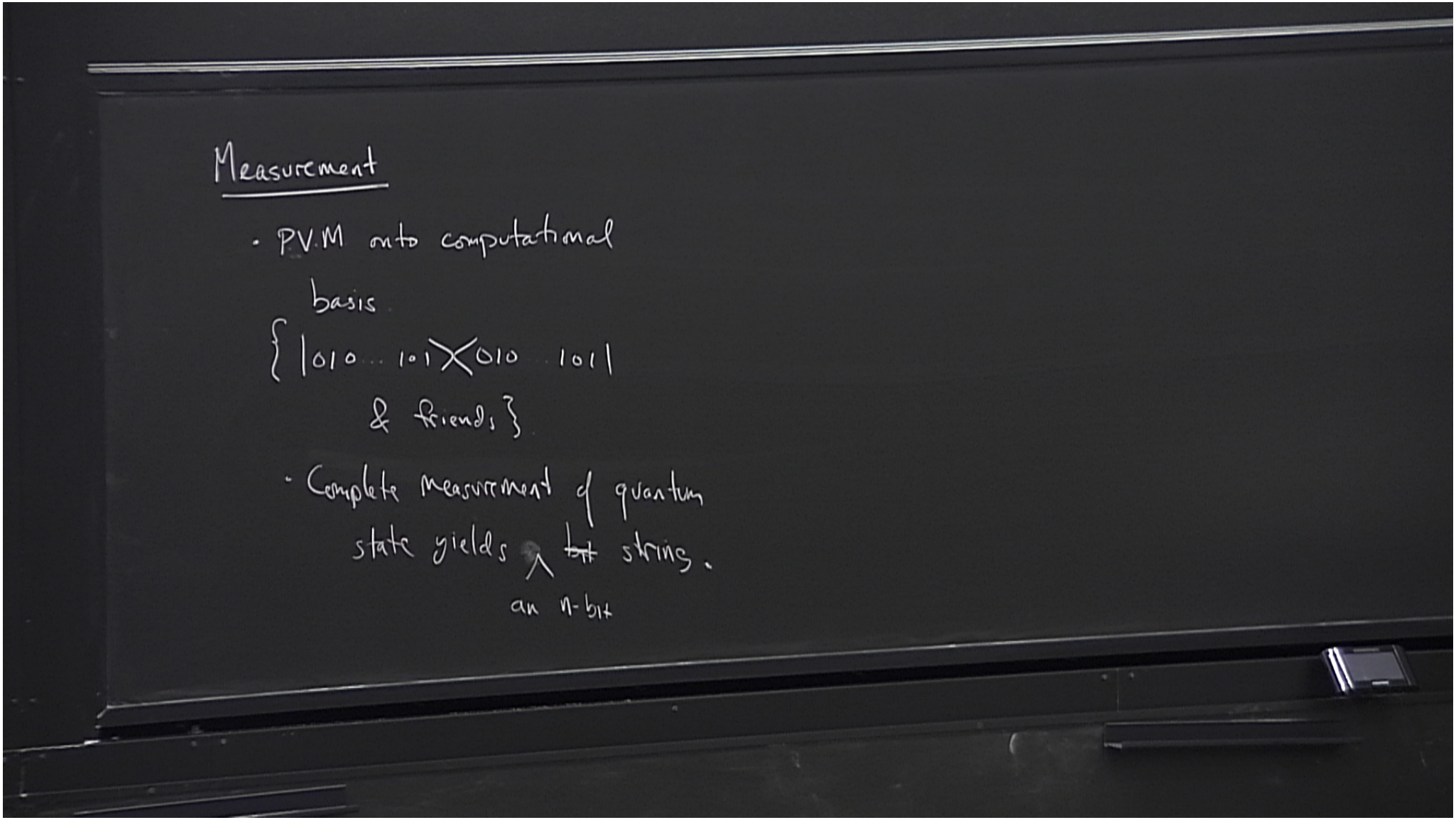
$\varphi \in (0, 2\pi]$

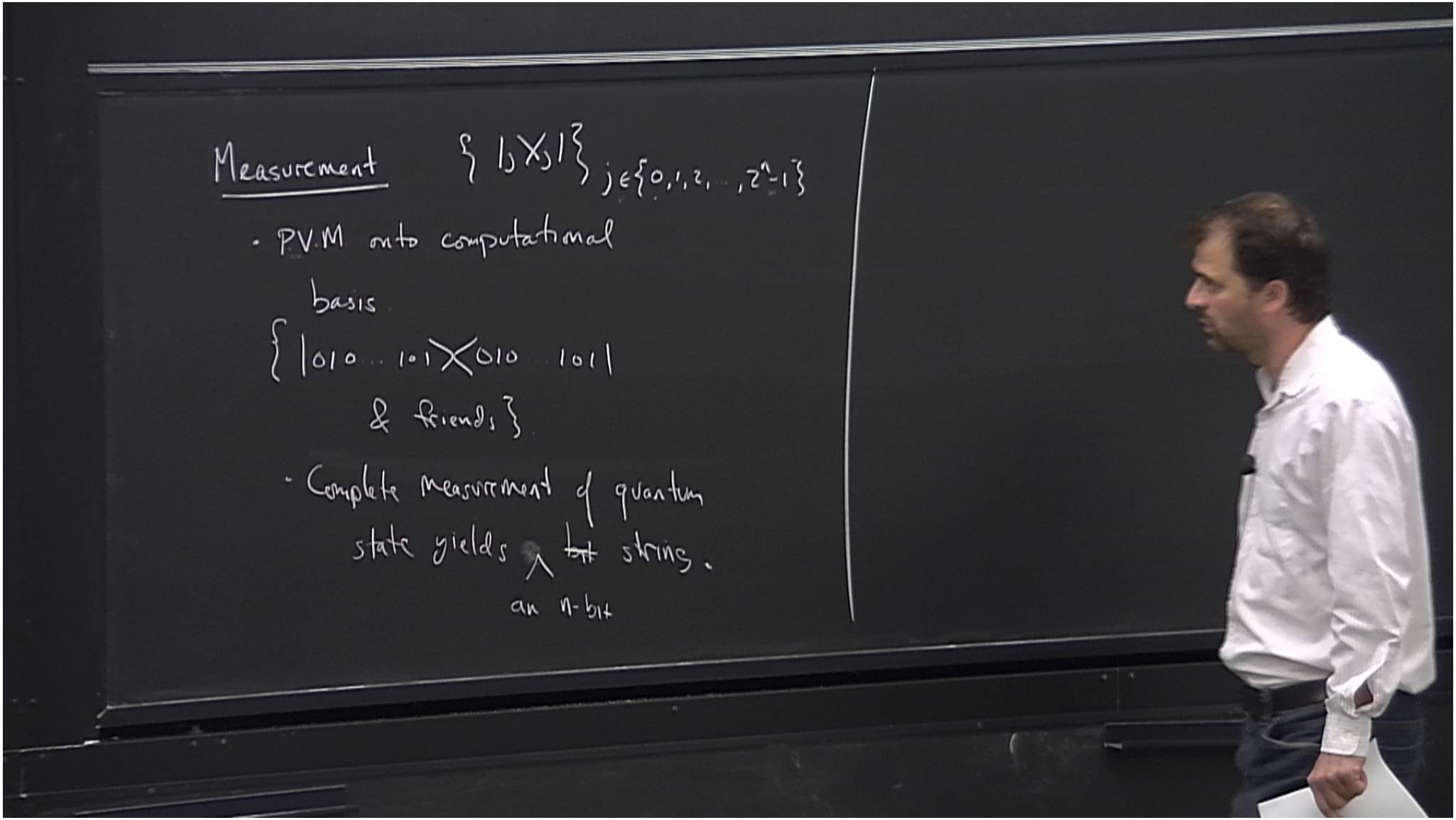
We call $U \in SU(D)$ an algorithm when U is designed to solve some problem.


Measurement
P.V.M onto computational
basis
{|010 .. 101 X 010 1011
& friends}


Measurement
P.V.M onto computational
basis
{|010 ... 101⟩⟨010 ... 101|
& friends}


Measurement
- PVM onto
basis
{|010
1011|


Measurement
• PVM onto computational basis
{|010⟩ |101⟩ |010⟩ |011⟩
& friends}
• Complete measurement of quantum state yields an n-bit string.


Measurement $\{|j\rangle\langle j|\}_{j \in \{0,1,2,\ldots,2^n-1\}}$
• PVM onto computational basis
$\{|010\ldots101\rangle\langle 010\ldots101|$ & friends$\}$
• Complete measurement of quantum state yields an n-bit string.

Measurement $\{|j\rangle\langle j|\}_{j \in \{0,1,2,\ldots,2^n-1\}}$

- PVM onto computational basis

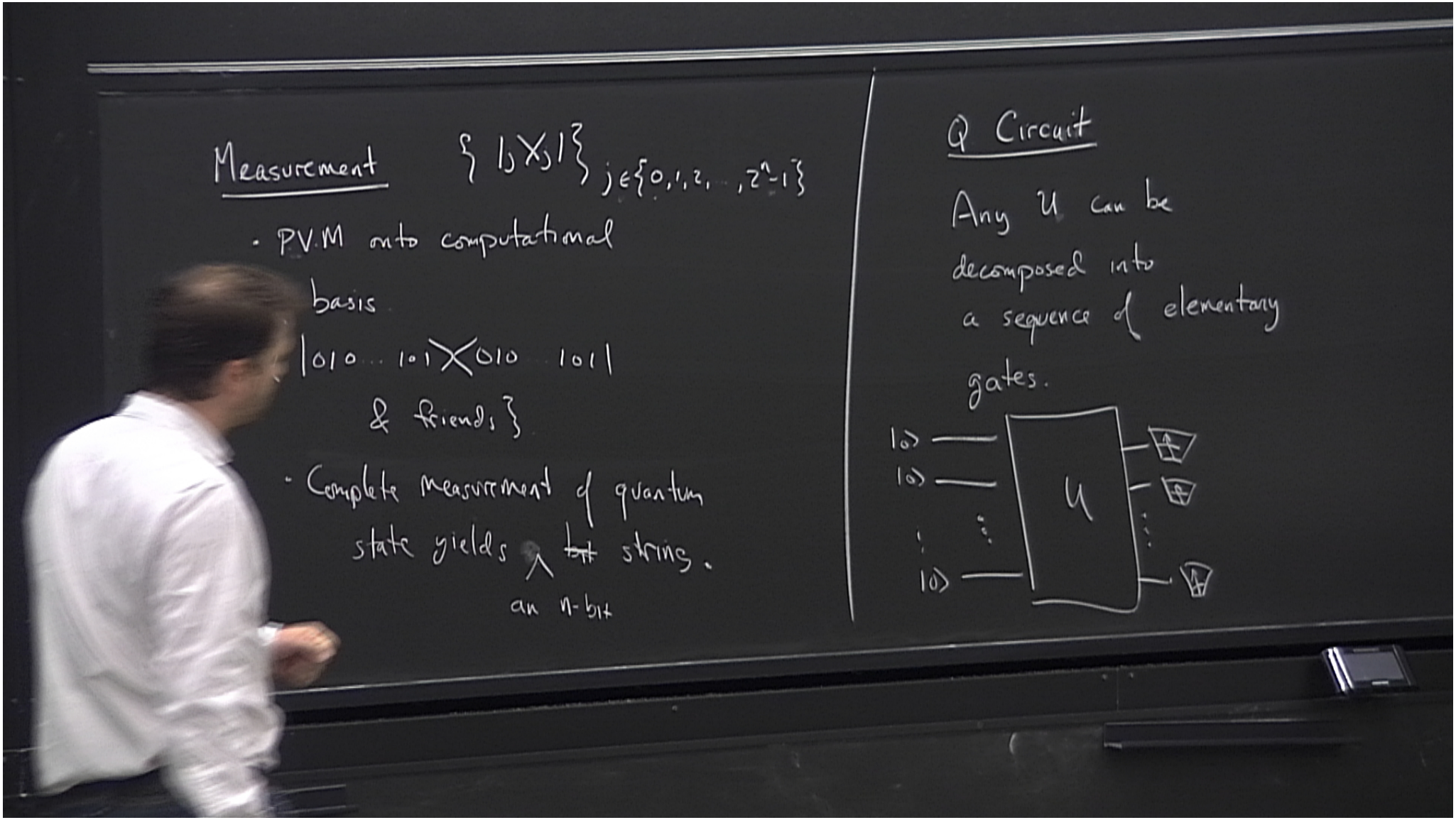
$\{|010\ldots101\rangle\langle 010\ldots101|$ & friends$\}$

- Complete measurement of quantum state yields ~~bit~~ string.

an n-bit

Q Circuit

Any U can be decomposed into a sequence of elementary gates.


Measurement
$\{|j\rangle\langle j|\}_{j\in\{0,1,2,\ldots,2^n-1\}}$
• P.V.M onto computational basis
$|010\ldots101\rangle\langle 010\ldots101|$
& friends }
• Complete measurement of quantum state yields ~~bit~~ string.
an n-bit
Q Circuit
Any U can be decomposed into a sequence of elementary gates.
$|0\rangle$
$|0\rangle$
$|0\rangle$
U

Measurement $\{|b\rangle\langle b|\}_{j \in \{0,1,2,\ldots,2^n-1\}}$

- PVM onto computational basis

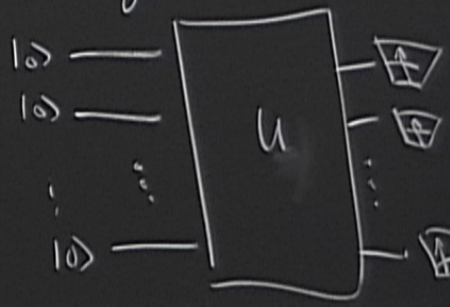
$\{|010\ldots101\rangle\langle 010\ldots101|$ & friends $\}$

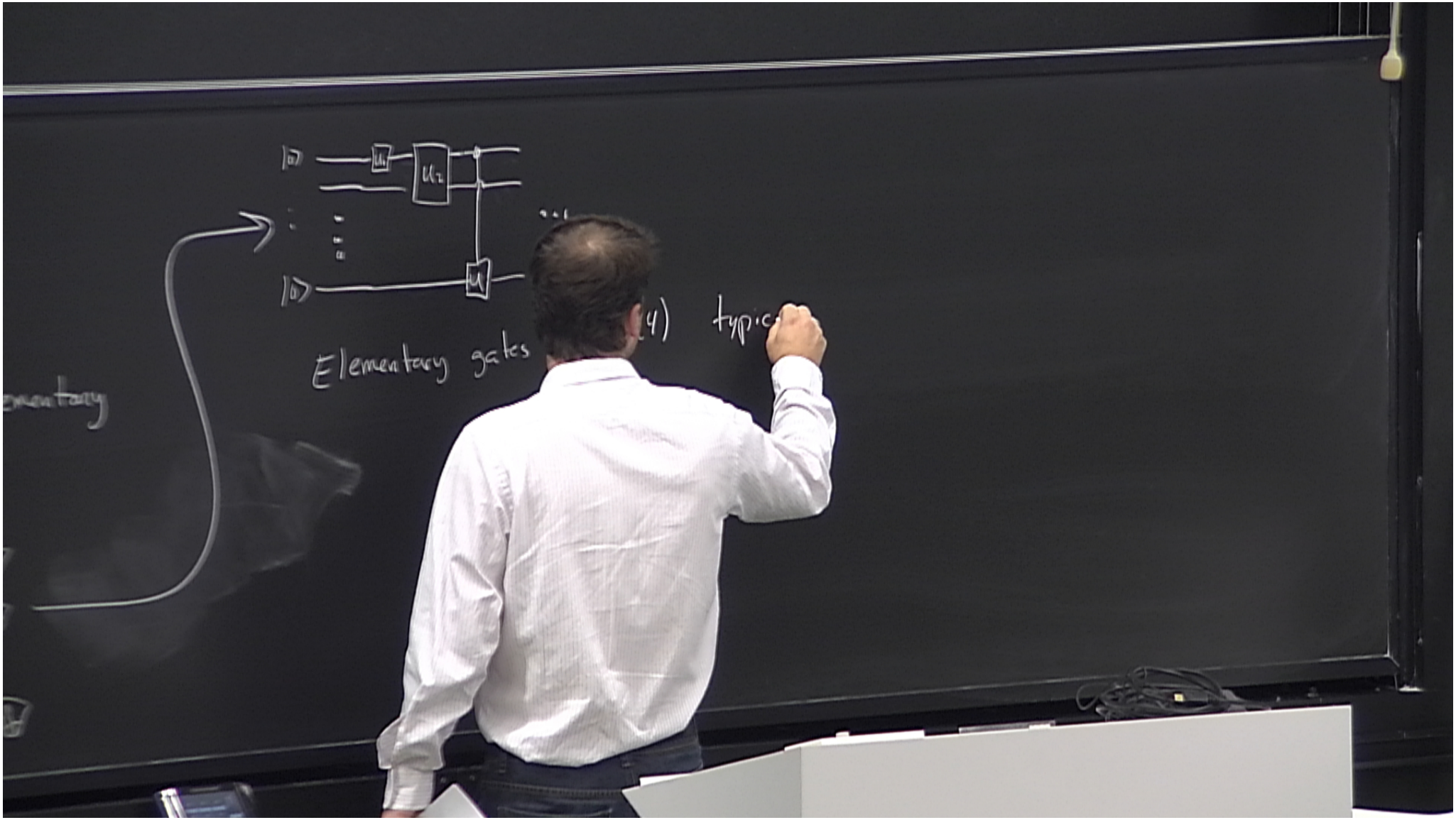
- Complete measurement of quantum state yields ~~bit~~ string.

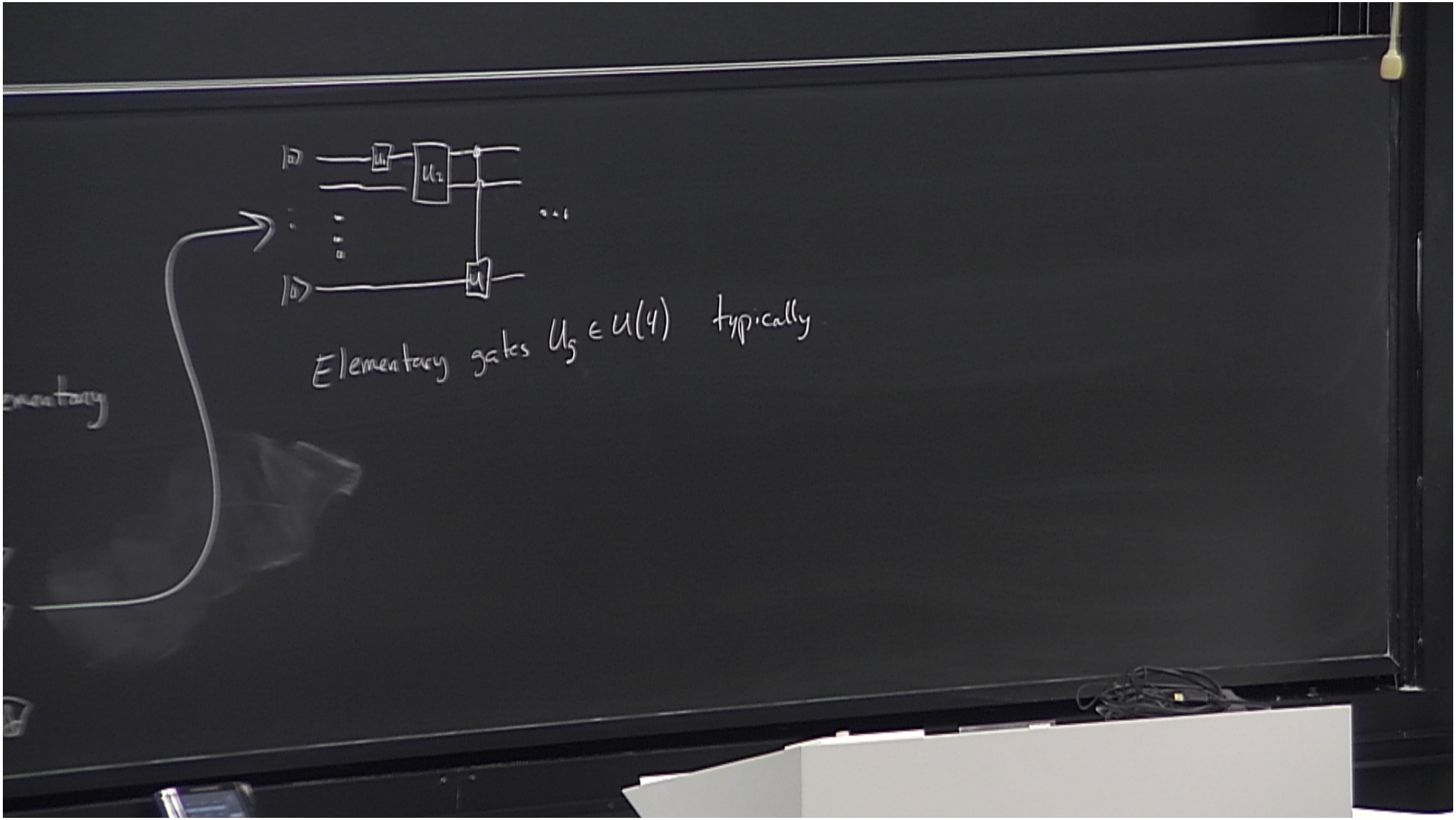
an n-bit

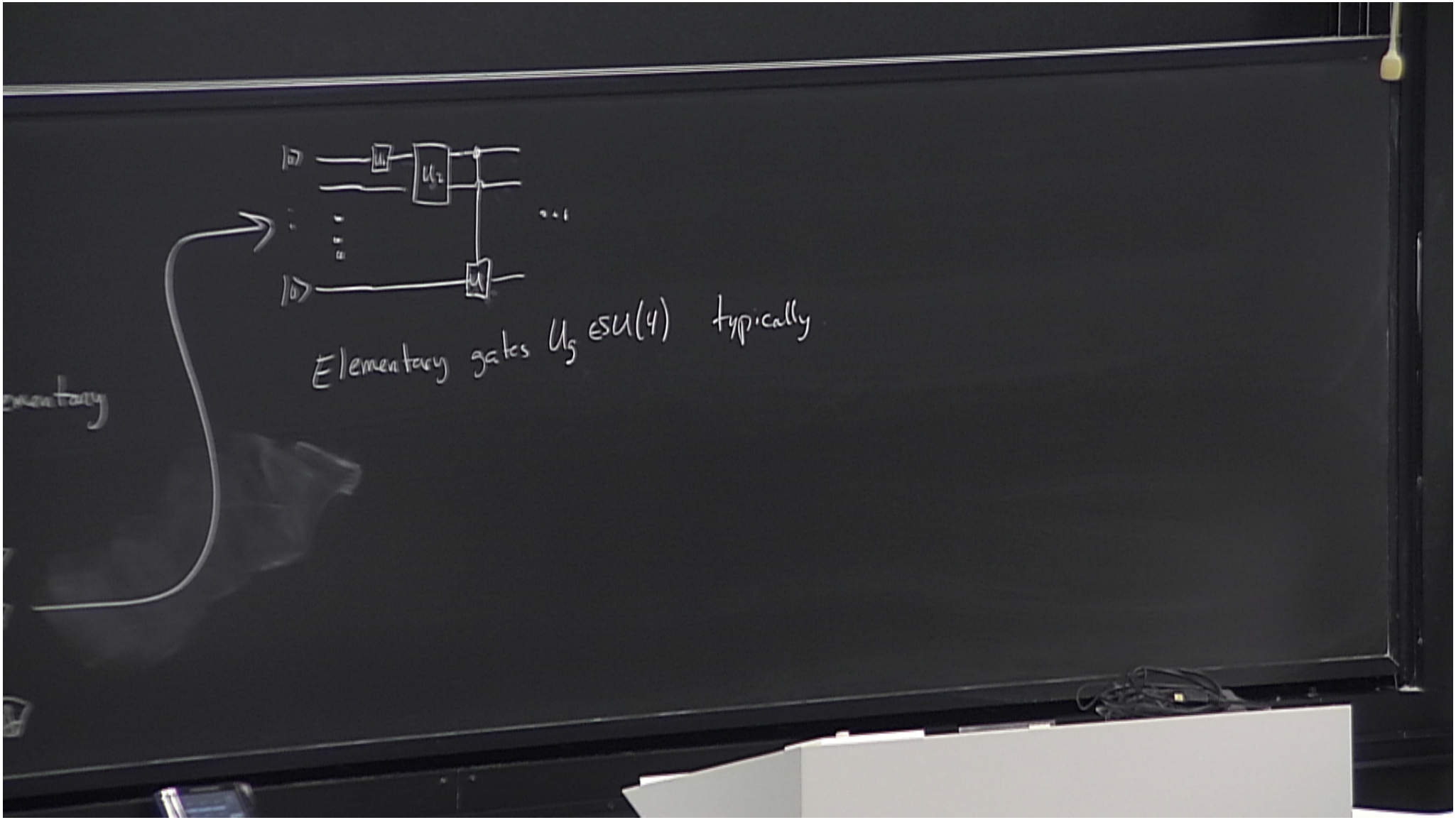
Q Circuit

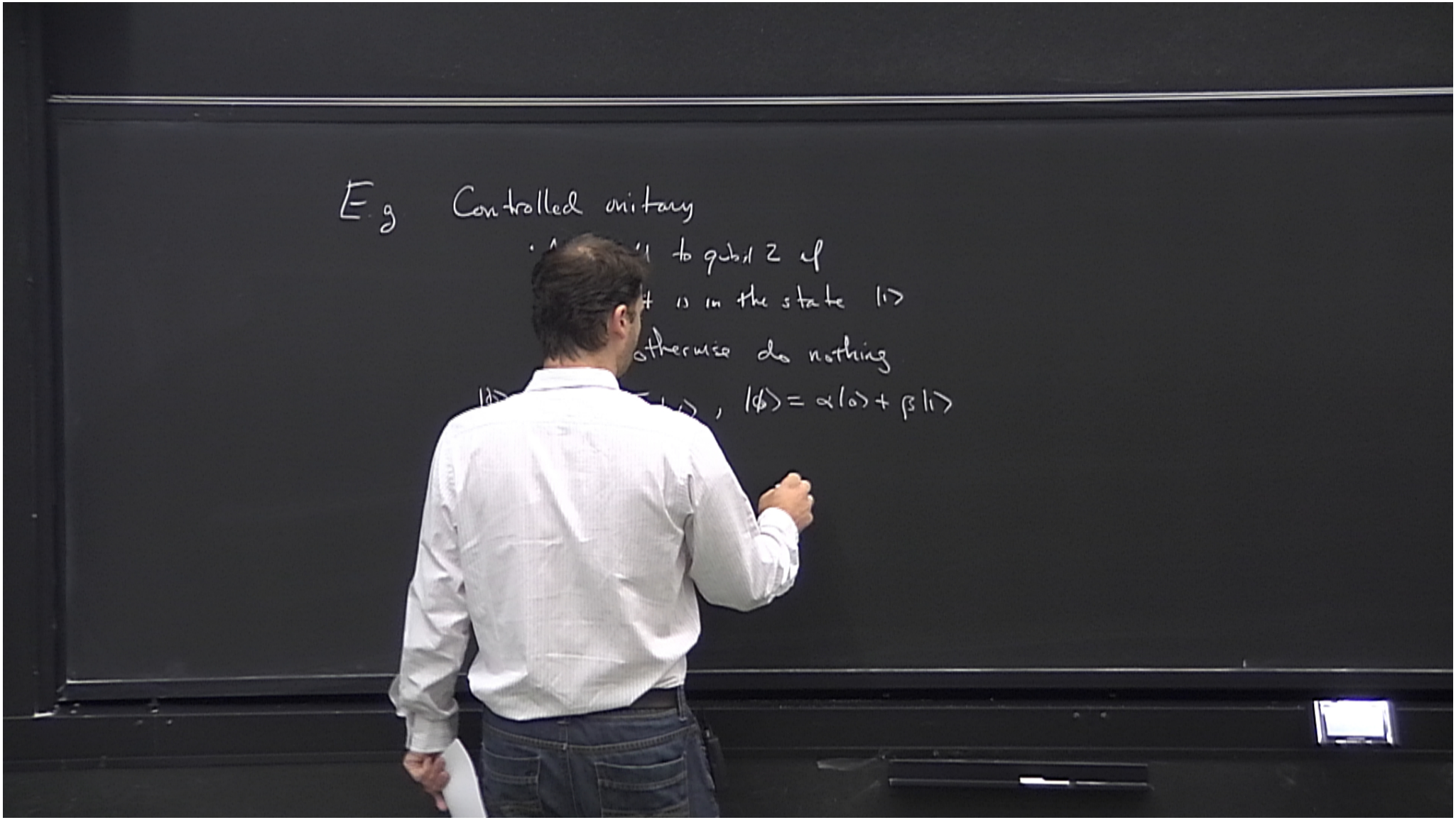
Any U can be decomposed into a sequence of elementary gates.




Elementary gates
typic

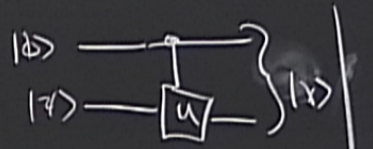

Elementary gates $U_S \in U(4)$ typically


Elementary gates $U_j \in SU(4)$ typically


Eg Controlled unitary
to qubit 2 of
is in the state |1>
otherwise do nothing
, |φ> = α|0> + β|1>

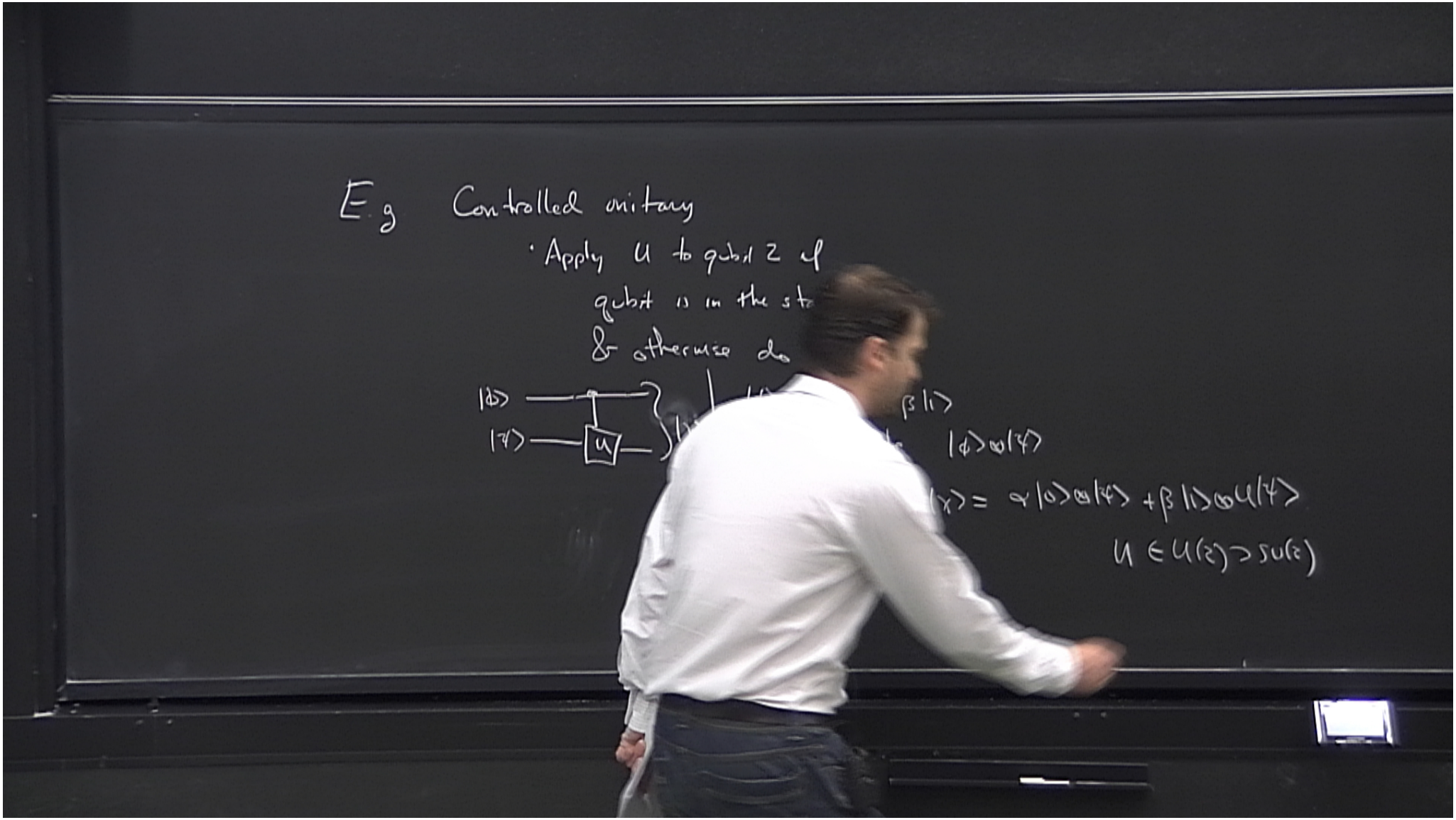
Eg Controlled unitary

· Apply U to qubit 2 if qubit 1 is in the state $|1\rangle$ & otherwise do nothing



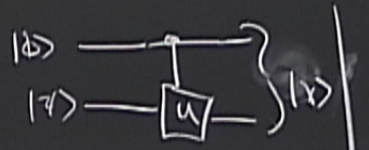
$|\phi\rangle = \alpha|$

$+\beta|1\rangle\otimes U|$


Eg Controlled unitary
· Apply U to qubit 2 if
qubit is in the st
& otherwise do
|ϕ⟩
|ψ⟩
U
β|1⟩
|ϕ⟩⊗|ψ⟩
= α|0⟩⊗|ψ⟩ +β|1⟩⊗U|ψ⟩
U ∈ U(2) ⊃ SU(2)

Eg Controlled unitary

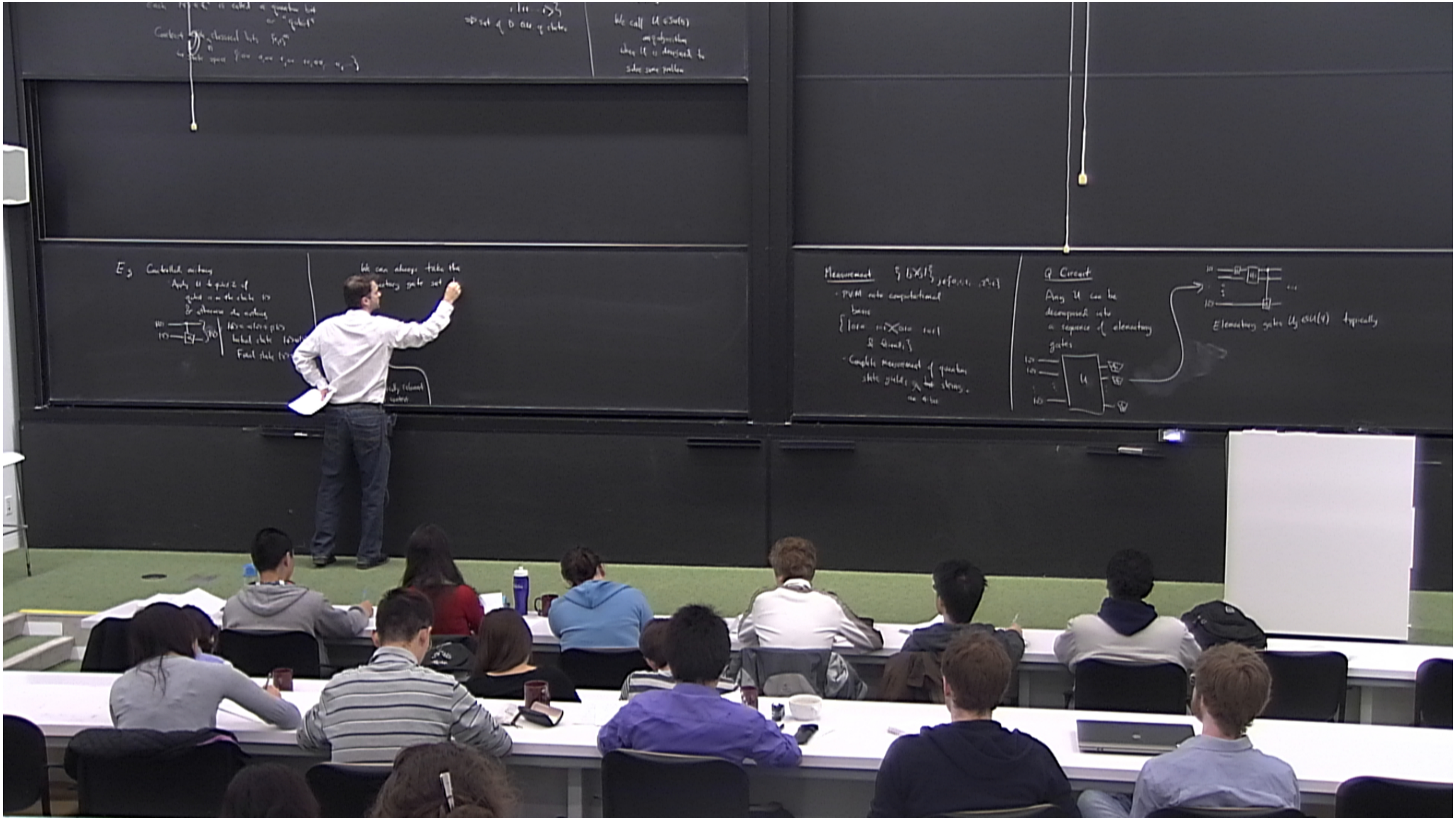
· Apply U to qubit 2 if qubit is in the state $|1\rangle$ & otherwise do nothing



$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

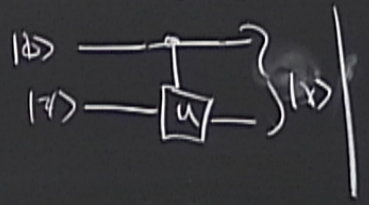
Initial state $|\phi\rangle \otimes |\psi\rangle$

Final state $|x\rangle =$


Measurement
Q Circuit
Elementary gates

Eg Controlled unitary

· Apply U to qubit 2 of qubit is in the state $|1\rangle$ & otherwise do nothing



$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

Initial state

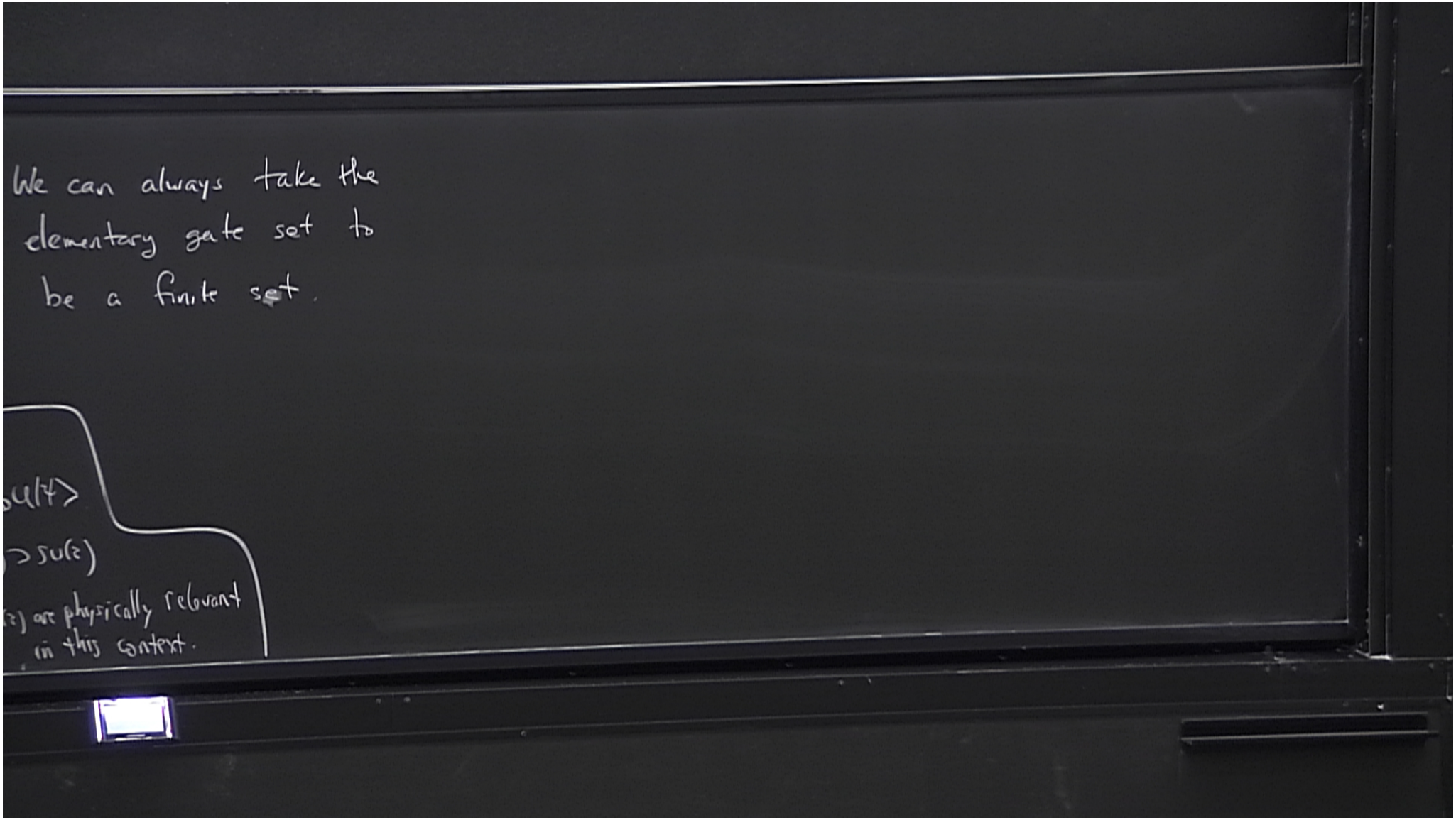
Final stat

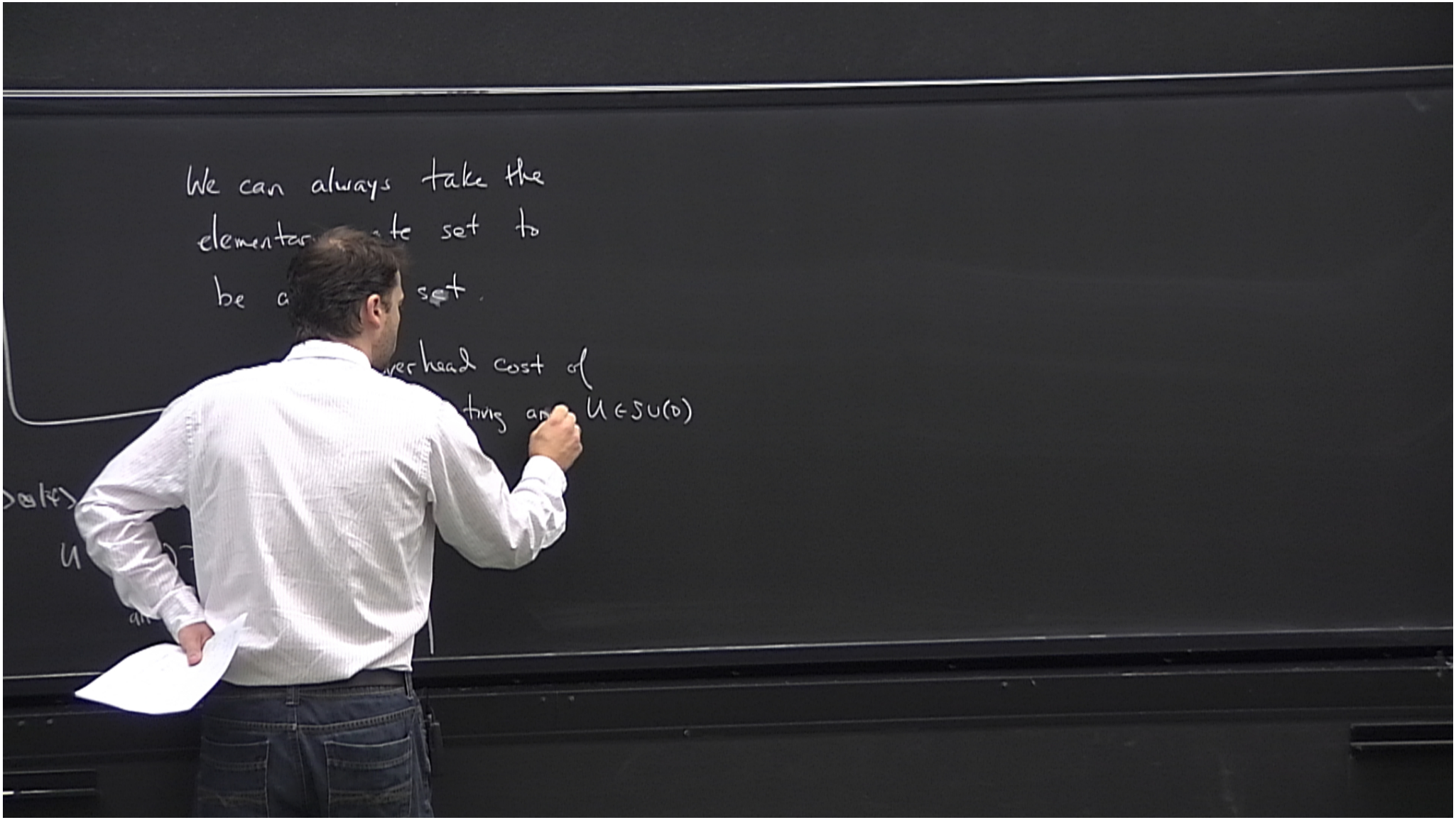
We can always
elementary ga
be a

$|\psi\rangle$

SU(2)

are physically relevant
in this context.


We can always take the
elementary gate set to
be a finite set.
su(4)
⊃ su(2)
(2) are physically relevant
in this context.


We can always take the
elementar te set to
be a set.
erhead cost of(
ting an U∈SU(D)

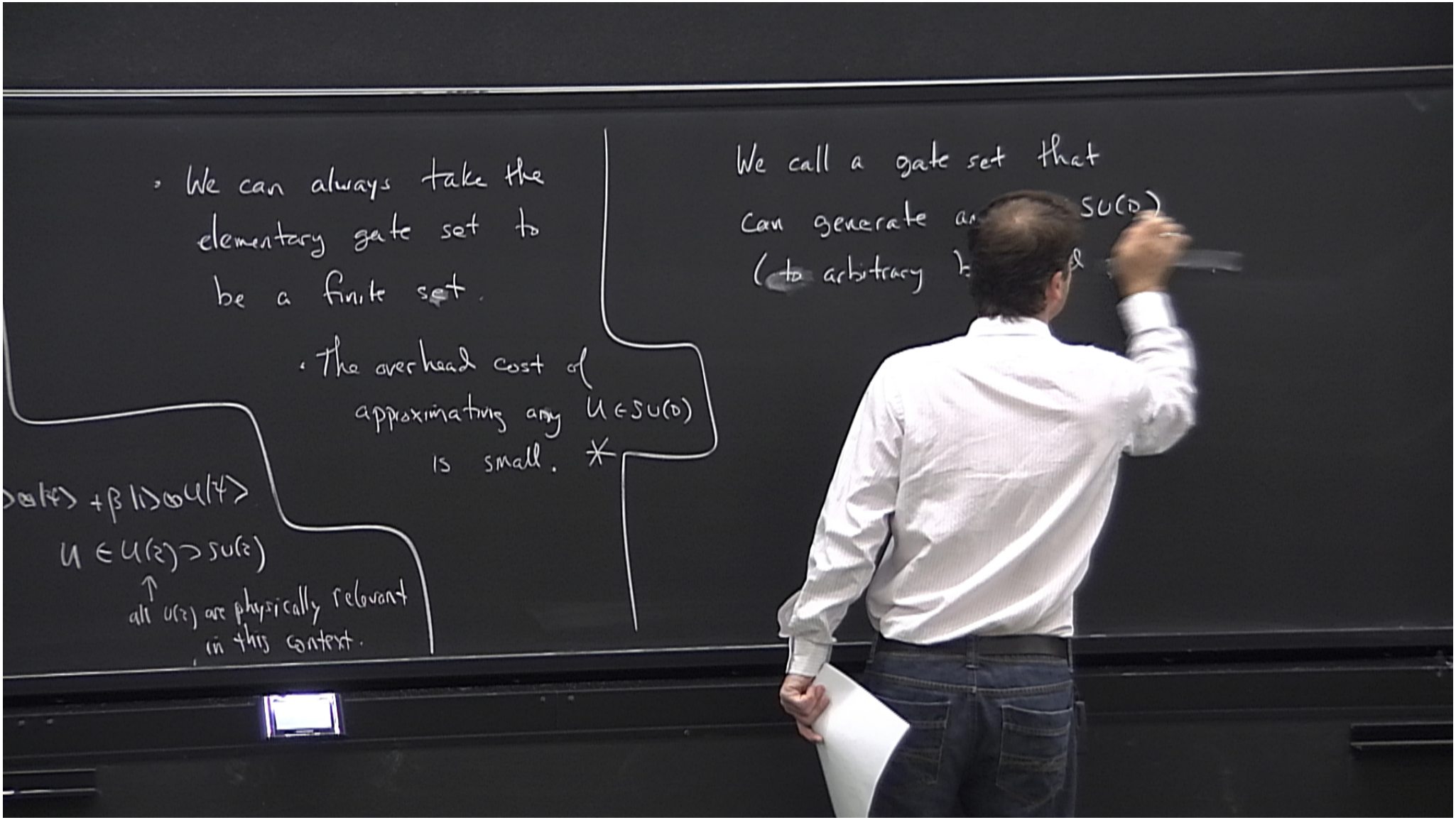
- We can always take the elementary gate set to be a finite set.

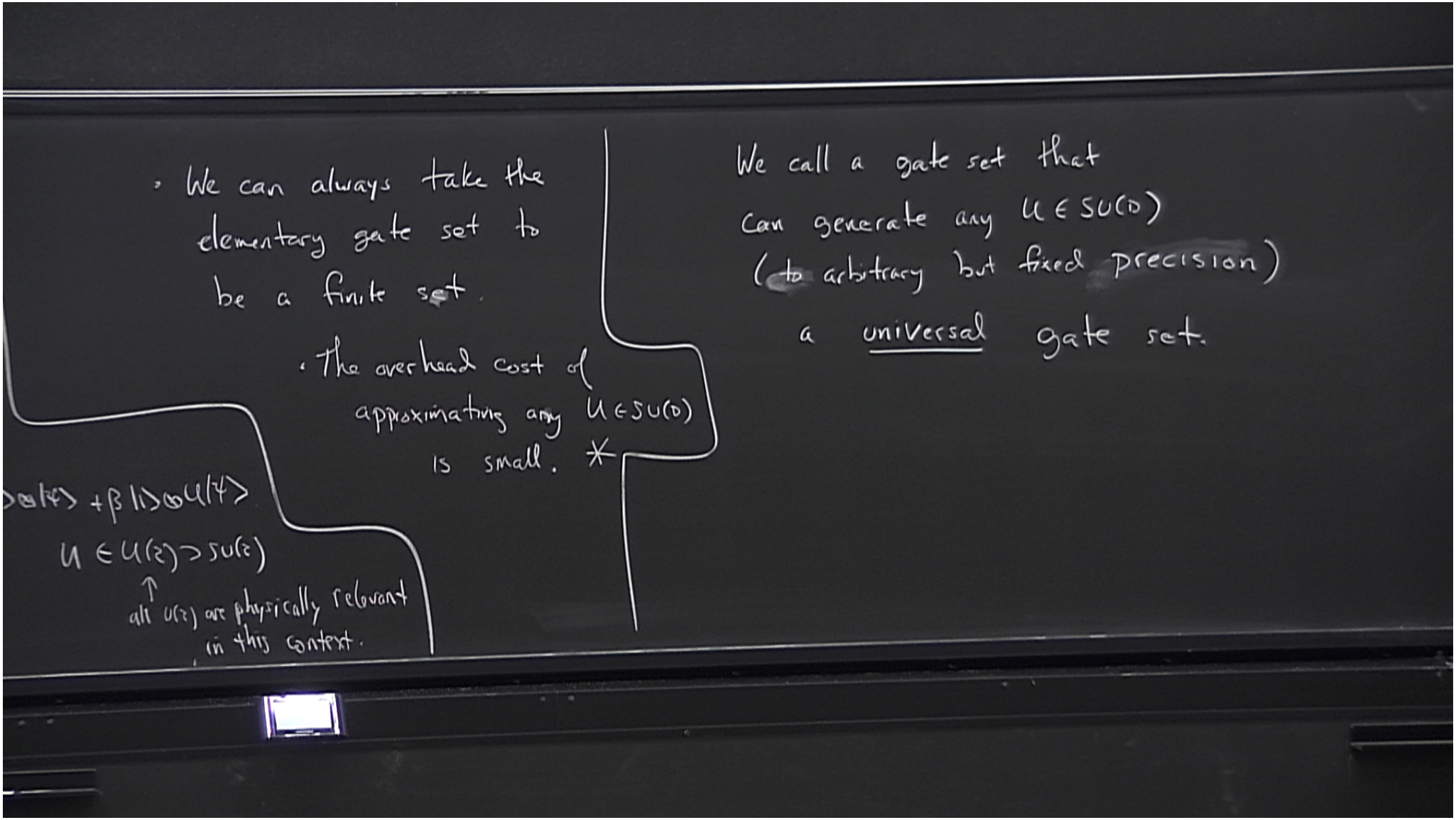
- The overhead cost of approximating any $U \in SU(D)$ is small

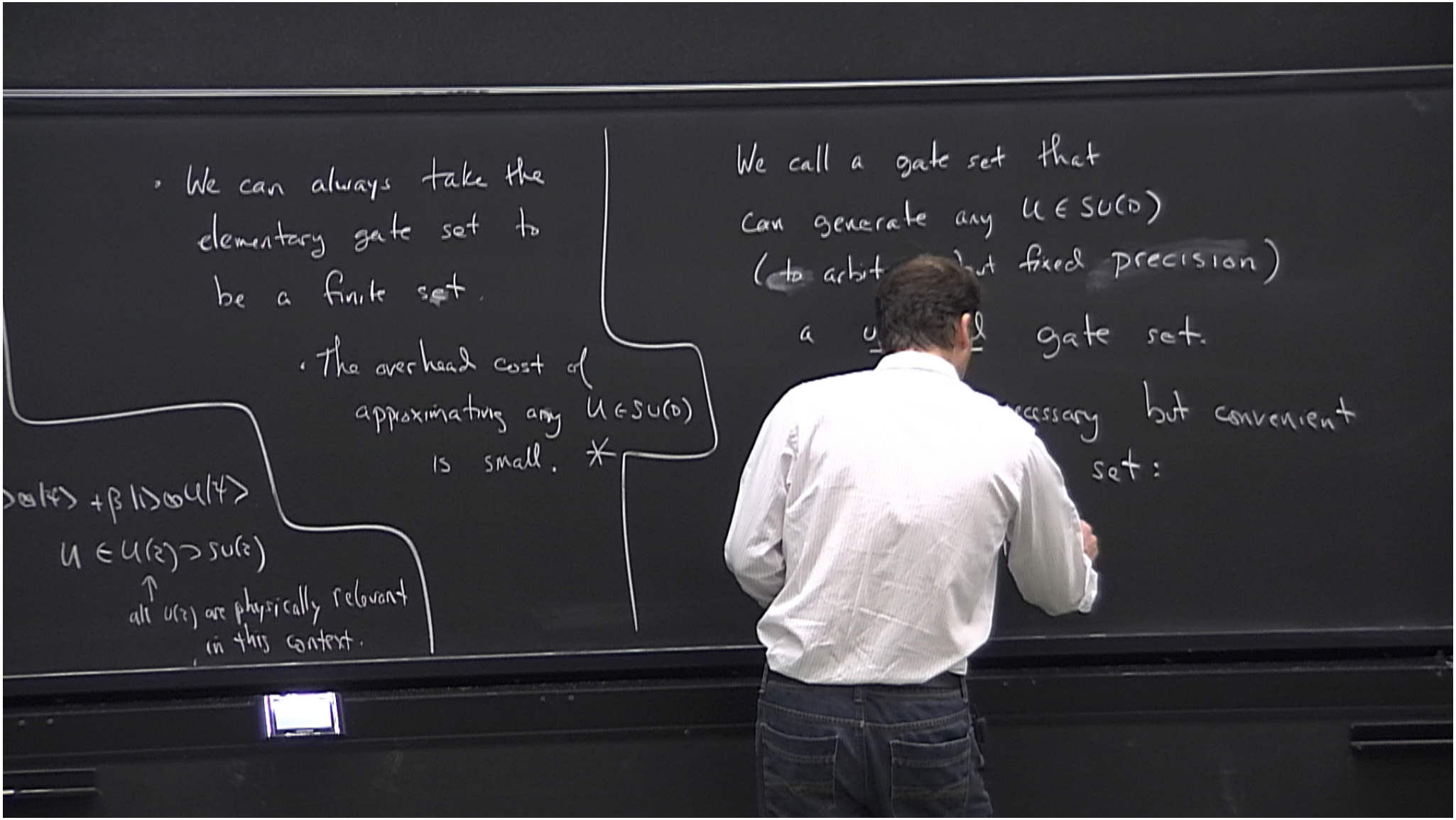
$\alpha|\psi\rangle + \beta|1\rangle \otimes U|\psi\rangle$

$U \in U(2) \supset SU(2)$

↑ all $U(2)$ are physically relevant in this context.


• We can always take the elementary gate set to be a finite set.
• The overhead cost of approximating any U∈SU(D) is small. *
We call a gate set that
Can generate
(to arbitrary
+β|1⟩⊗U|ψ⟩
U∈U(2)⊃SU(2)
all U(2) are physically relevant in this context.


• We can always take the elementary gate set to be a finite set.
• The overhead cost of approximating any $U \in SU(D)$ is small. *
We call a gate set that can generate any $U \in SU(D)$ (to arbitrary but fixed precision) a universal gate set.
$\alpha|\psi\rangle + \beta|\perp\rangle \otimes U|\psi\rangle$
$U \in U(z) \supset SU(z)$
all $U(z)$ are physically relevant in this context.


• We can always take the elementary gate set to be a finite set.
• The overhead cost of approximating any U∈SU(D) is small. *
We call a gate set that
Can generate any U ∈ SU(D)
(to arbit
fixed precision)
a
gate set.
but convenient
set:
+β|1⟩⊗U|ψ⟩
U ∈ U(2) ⊃ SU(2)
all U(2) are physically relevant in this context.

- We can always take the elementary gate set to be a finite set.

- The overhead cost of approximating any $U \in SU(D)$ is small. *

We call a gate set that can generate any $U \in SU(D)$ (to arbitrary but fixed precision) a universal gate set.

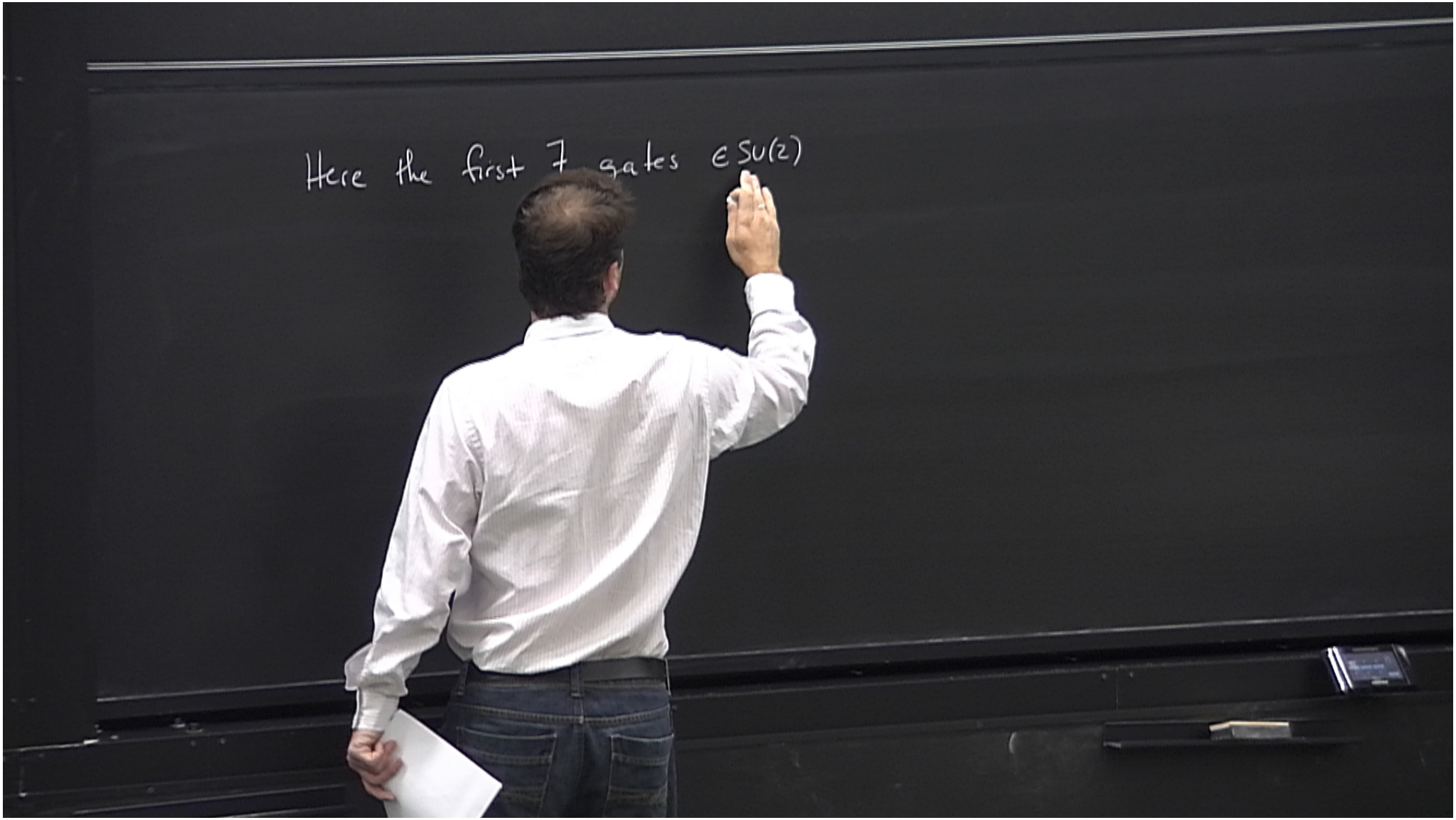
A larger than necessary but convenient universal gate set:

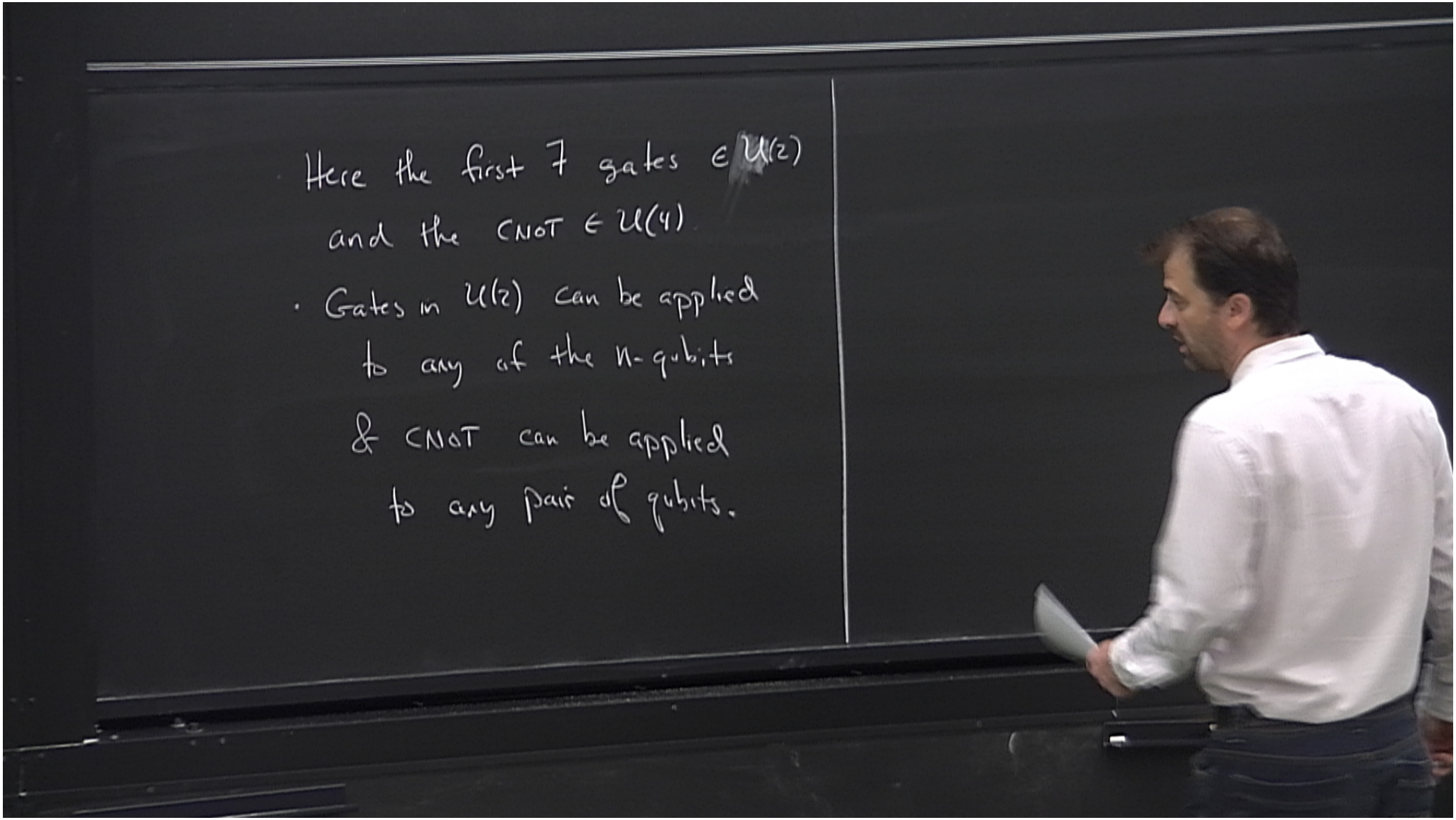
$$\{\mathbb{1}, X, Y, Z, H, S, T, CNOT\}$$

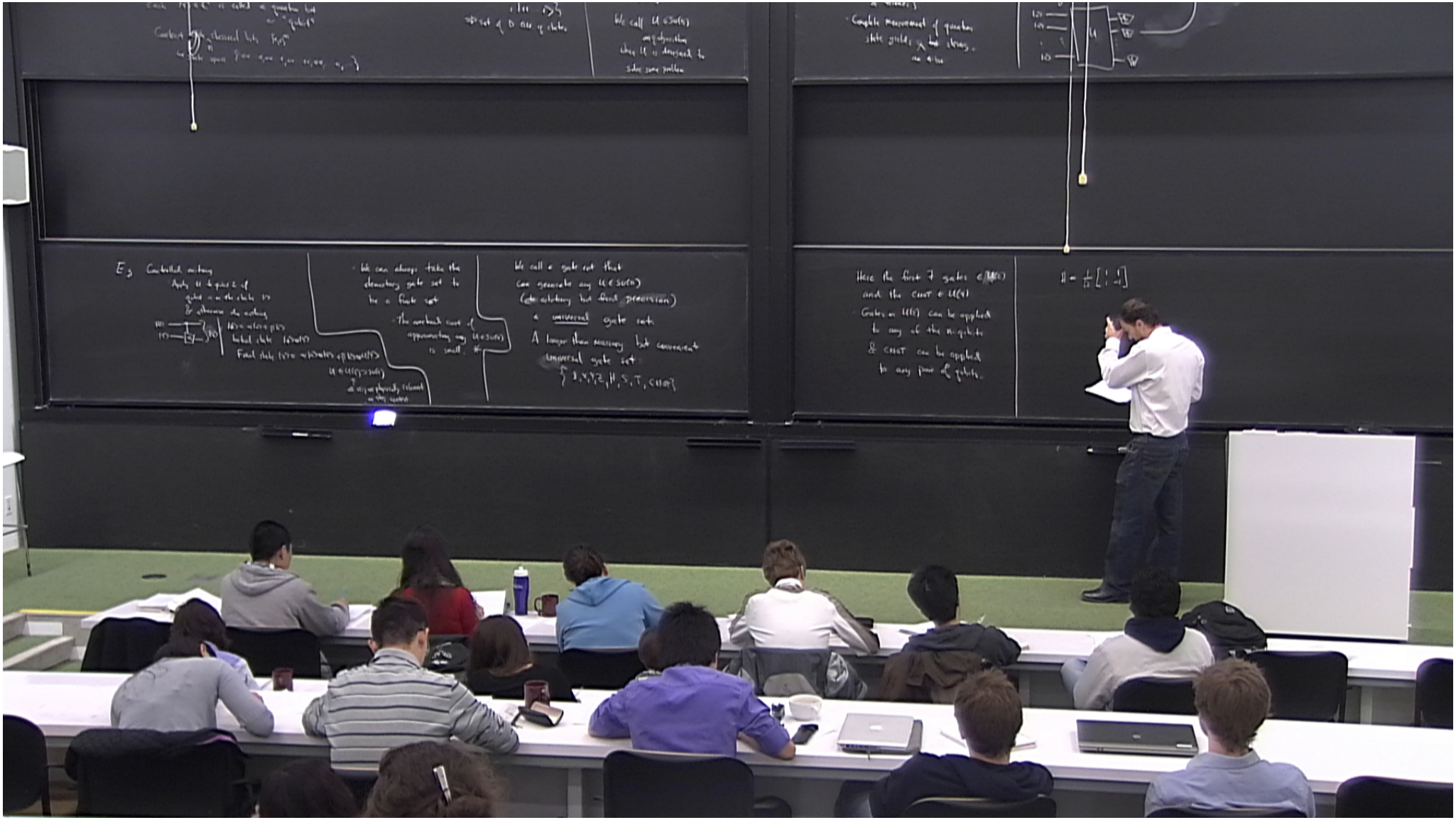
$\alpha|\psi\rangle + \beta|1\rangle \otimes U|\psi\rangle$

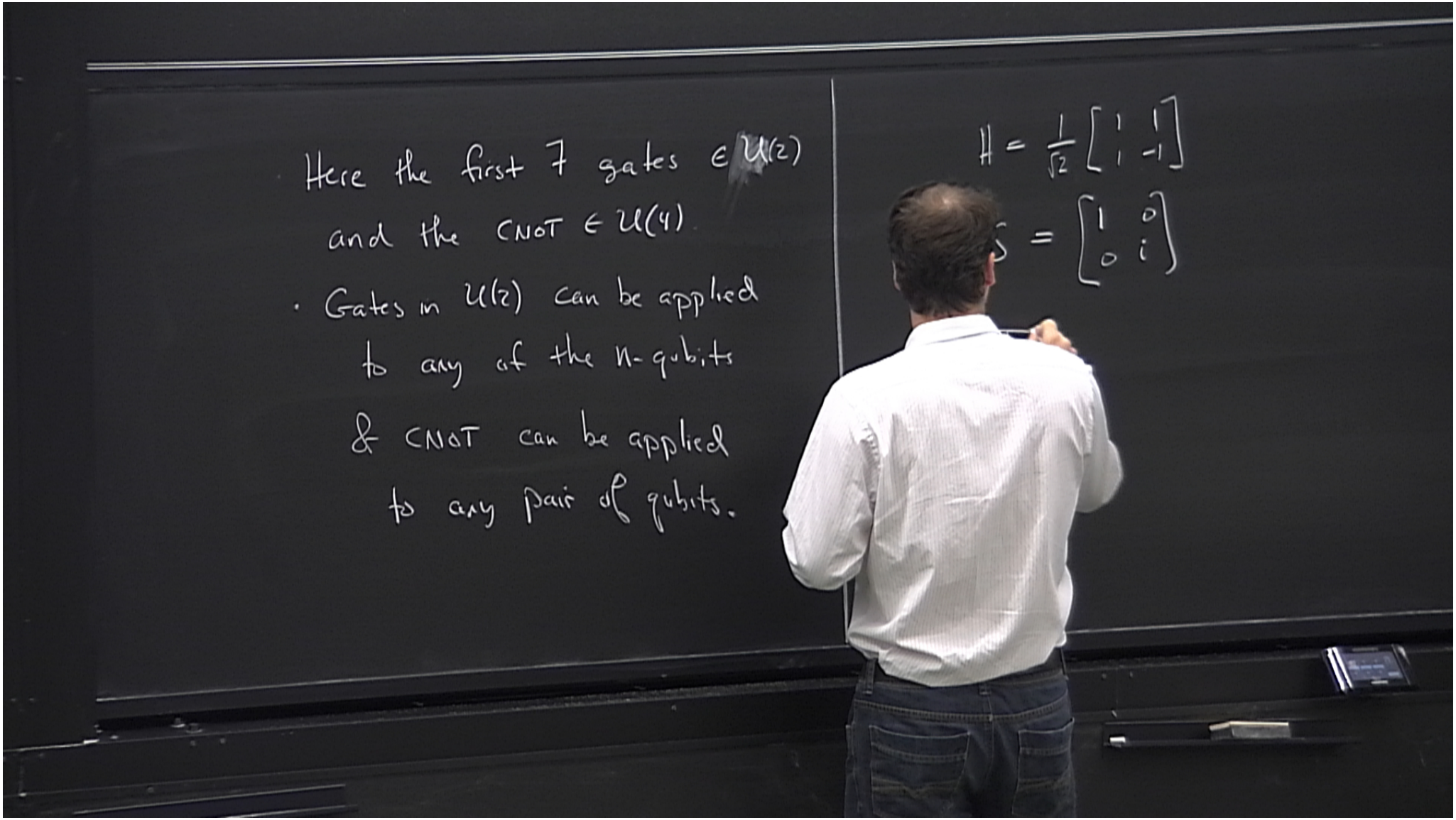
$U \in U(2) \supset SU(2)$

↑ all $U(2)$ are physically relevant in this context.


Here the first 7 gates $\in SU(2)$


Here the first 7 gates $\in \mathcal{U}(2)$
and the CNOT $\in \mathcal{U}(4)$
• Gates in $\mathcal{U}(2)$ can be applied
to any of the n-qubits
& CNOT can be applied
to any pair of qubits.


Ex: Controlled unitary
We call a gate set that
can approximate any U ∈ SU(n)
a universal gate set
Here the first 7 gates ∈ U(8)
and the CNOT ∈ U(4)
H = 1/√2 [1 1; 1 -1]


Here the first 7 gates ∈ U(2)
and the CNOT ∈ U(4)
• Gates in U(2) can be applied
to any of the n-qubits
& CNOT can be applied
to any pair of qubits.
H = 1/√2 [1 1; 1 -1]
S = [1 0; 0 i]

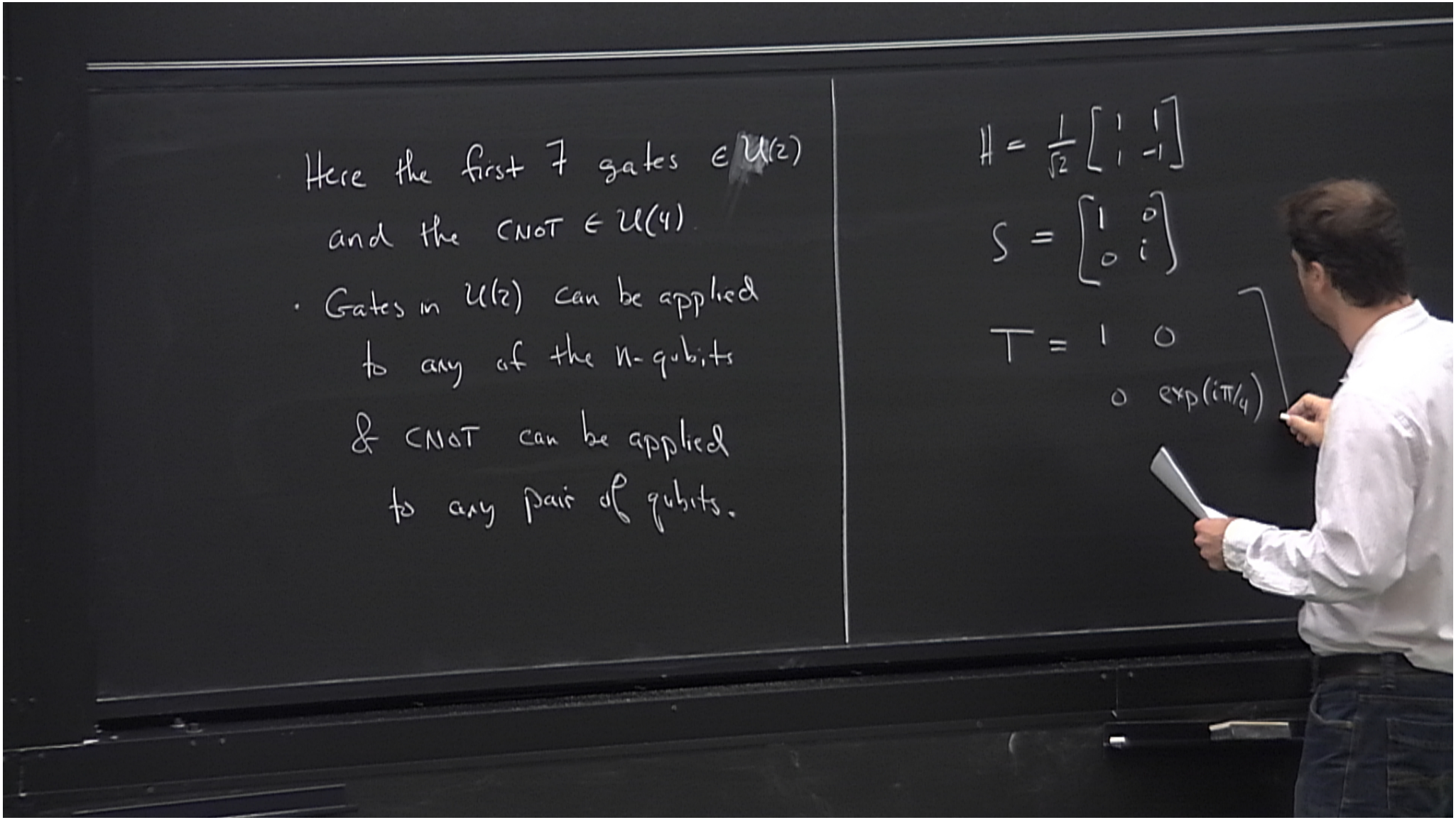
Here the first 7 gates $\in \mathcal{U}(2)$ and the CNOT $\in \mathcal{U}(4)$

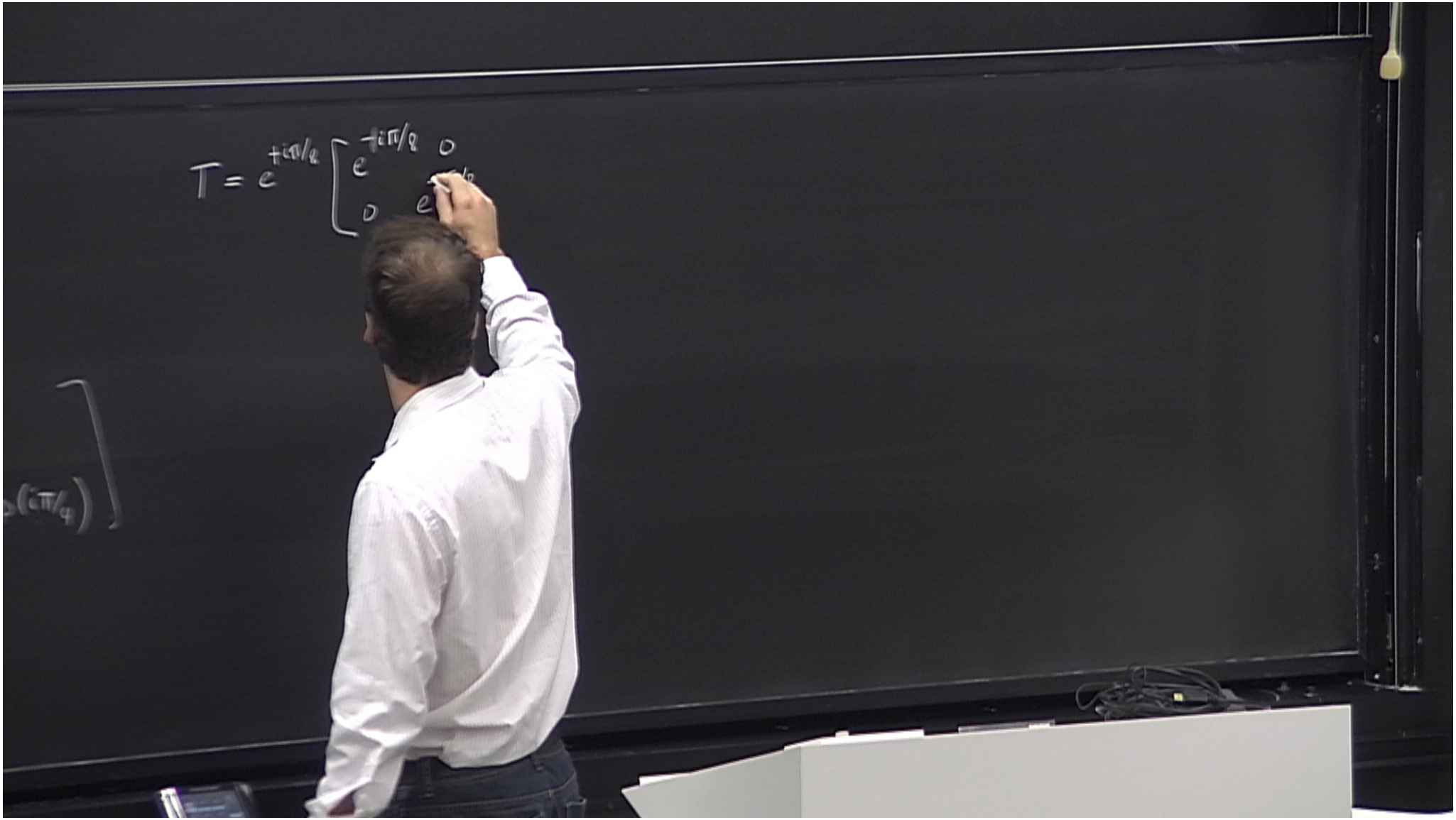
- Gates in $\mathcal{U}(2)$ can be applied to any of the n-qubits & CNOT can be applied to any pair of qubits.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

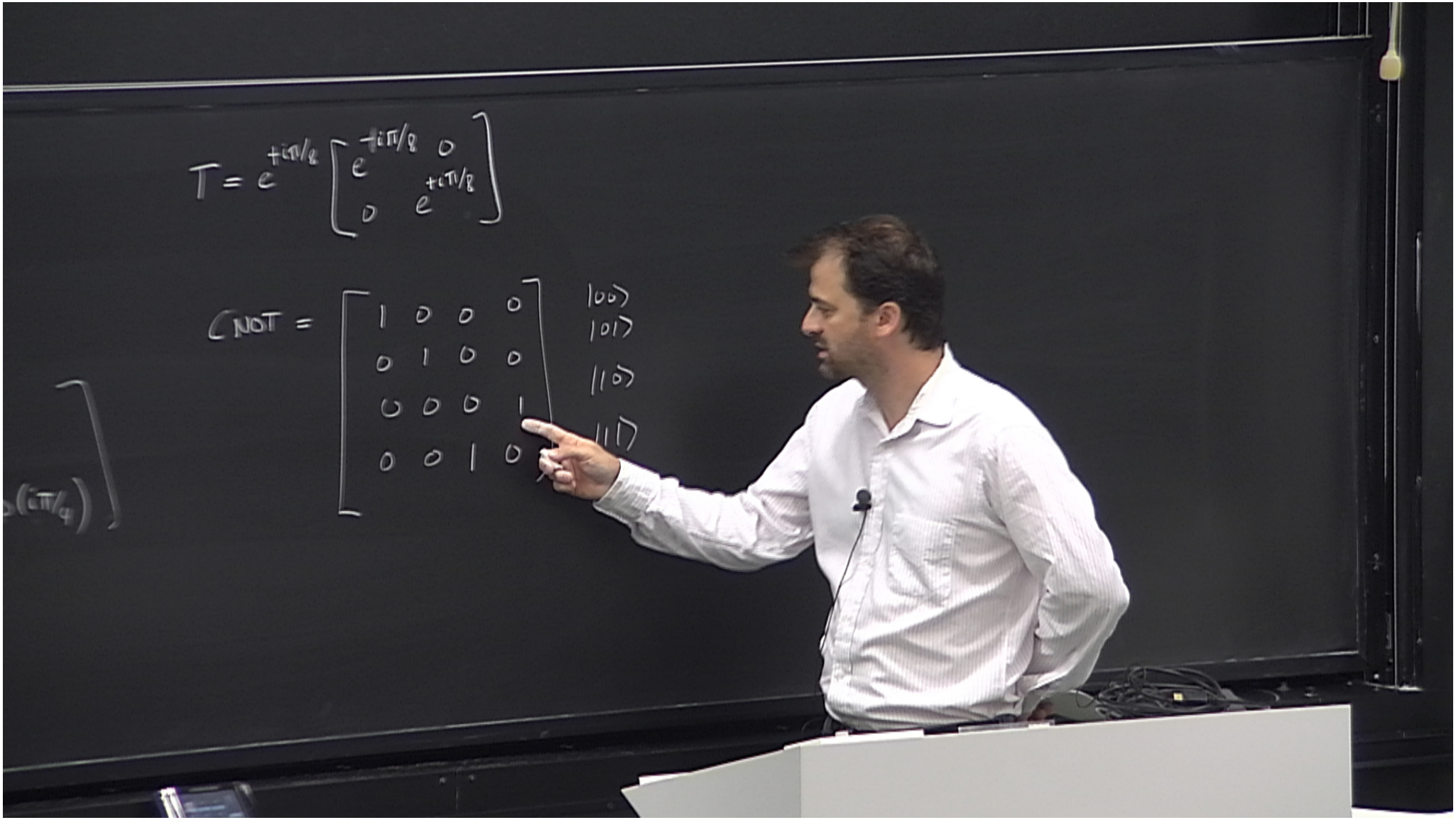
$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

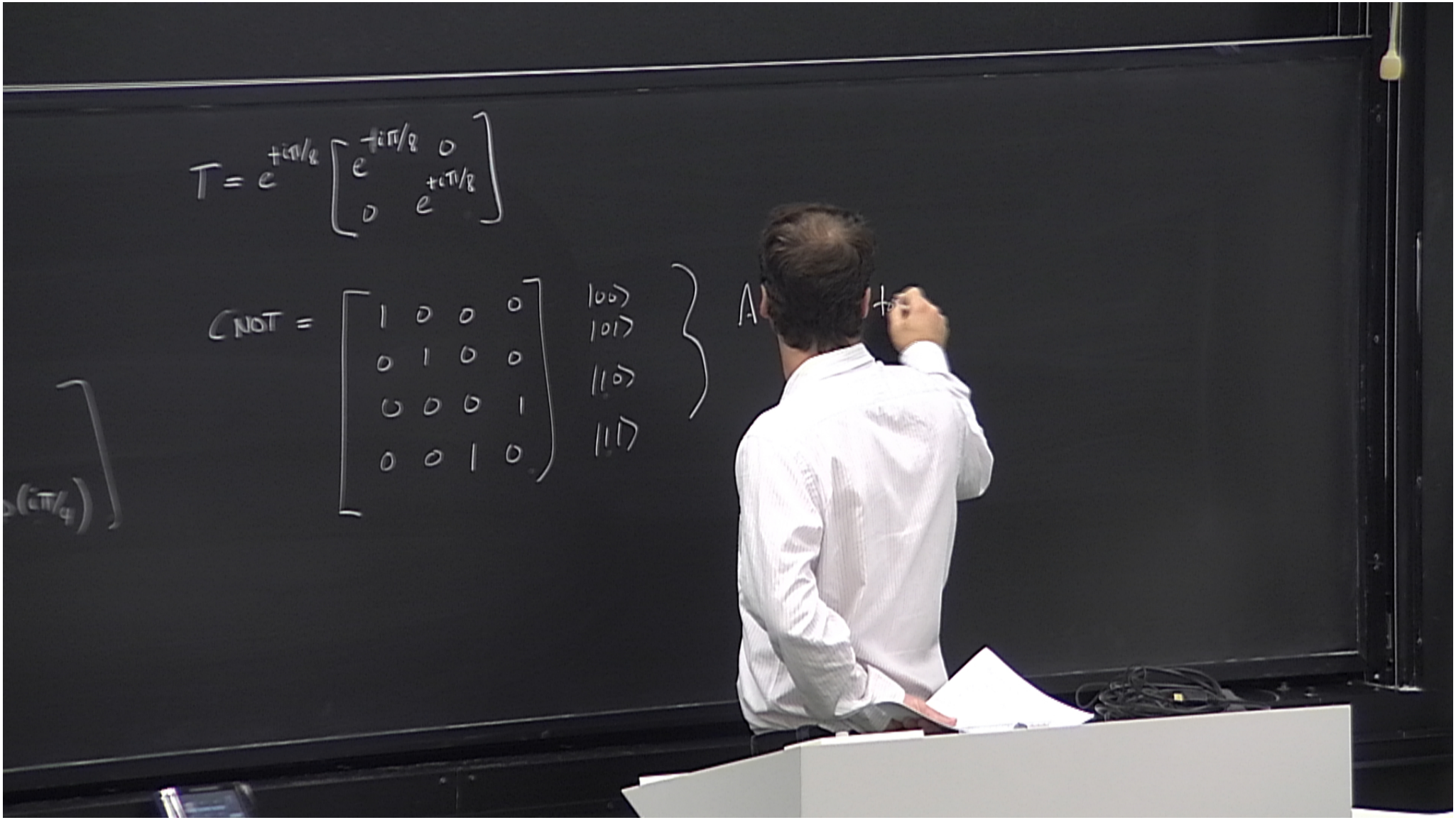
$$T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

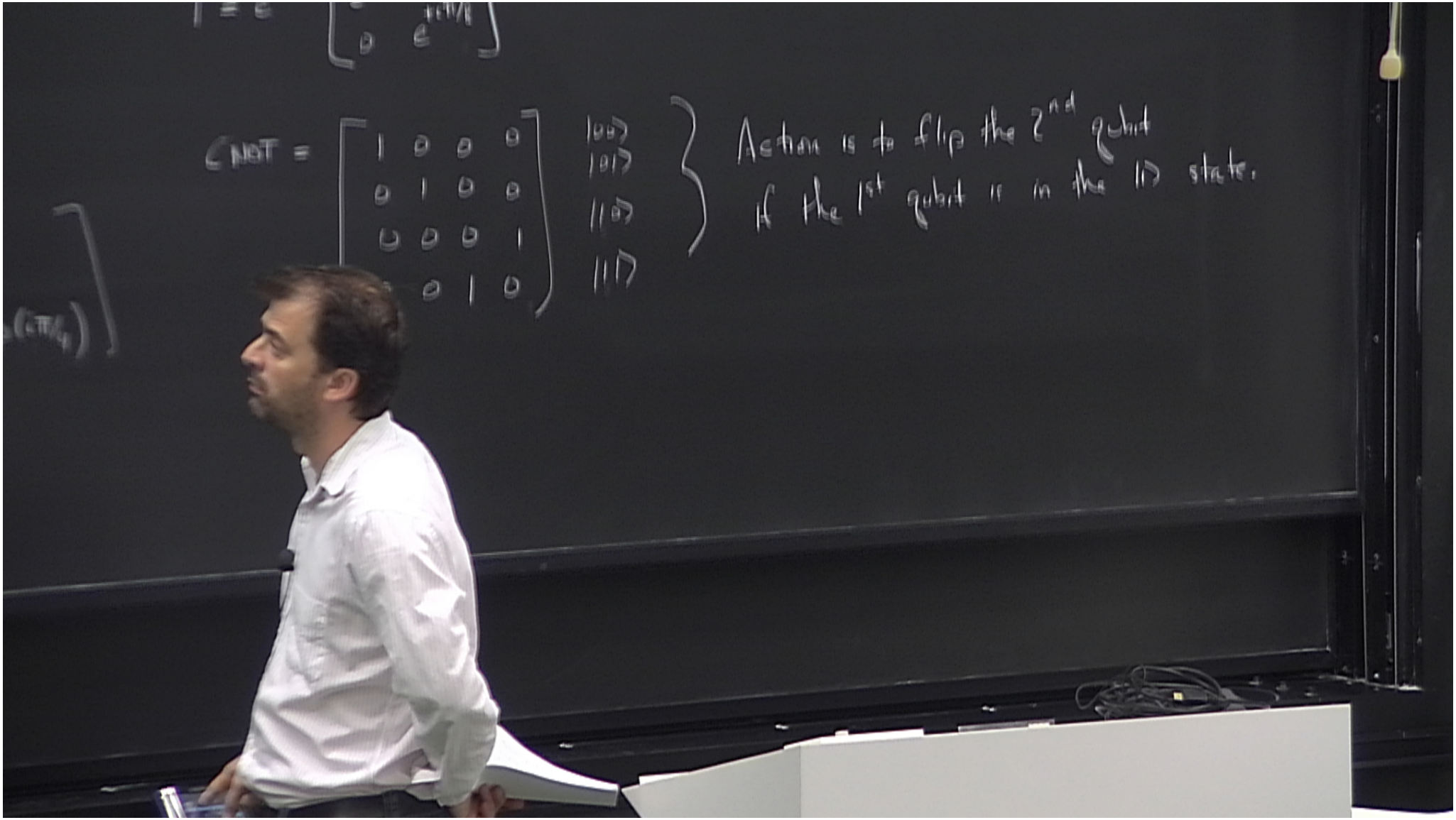


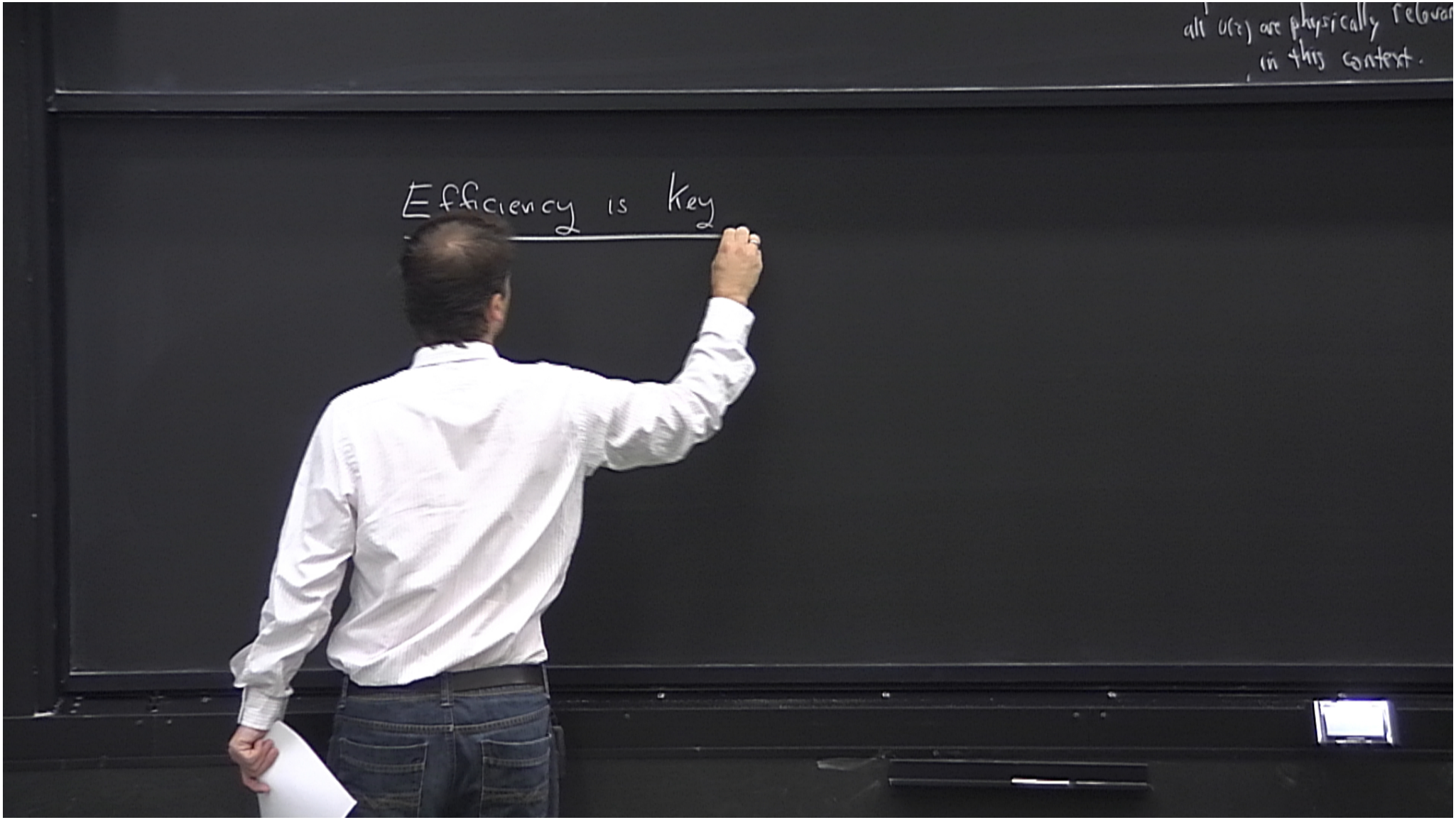

$T = e^{\pm i\pi/4} \begin{bmatrix} e^{\mp i\pi/8} & 0 \\ 0 & e^{\pm i\pi/8} \end{bmatrix}$


$T = e^{\pm i\pi/8} \begin{bmatrix} e^{\mp i\pi/8} & 0 \\ 0 & e^{\pm i\pi/8} \end{bmatrix}$


$T = e^{+i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{+i\pi/8} \end{bmatrix}$
$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
$|00\rangle$
$|01\rangle$
$|10\rangle$
$|11\rangle$


T = e^{+iπ/8} [e^{-iπ/8} 0 ; 0 e^{+iπ/8}]
CNOT = [1 0 0 0 ; 0 1 0 0 ; 0 0 0 1 ; 0 0 1 0]
|00⟩
|01⟩
|10⟩
|11⟩

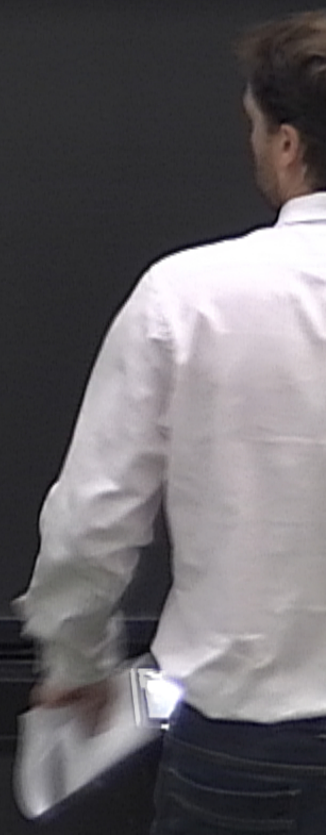

CNOT =
Action is to flip the 2nd qubit
if the 1st qubit is in the |1⟩ state.

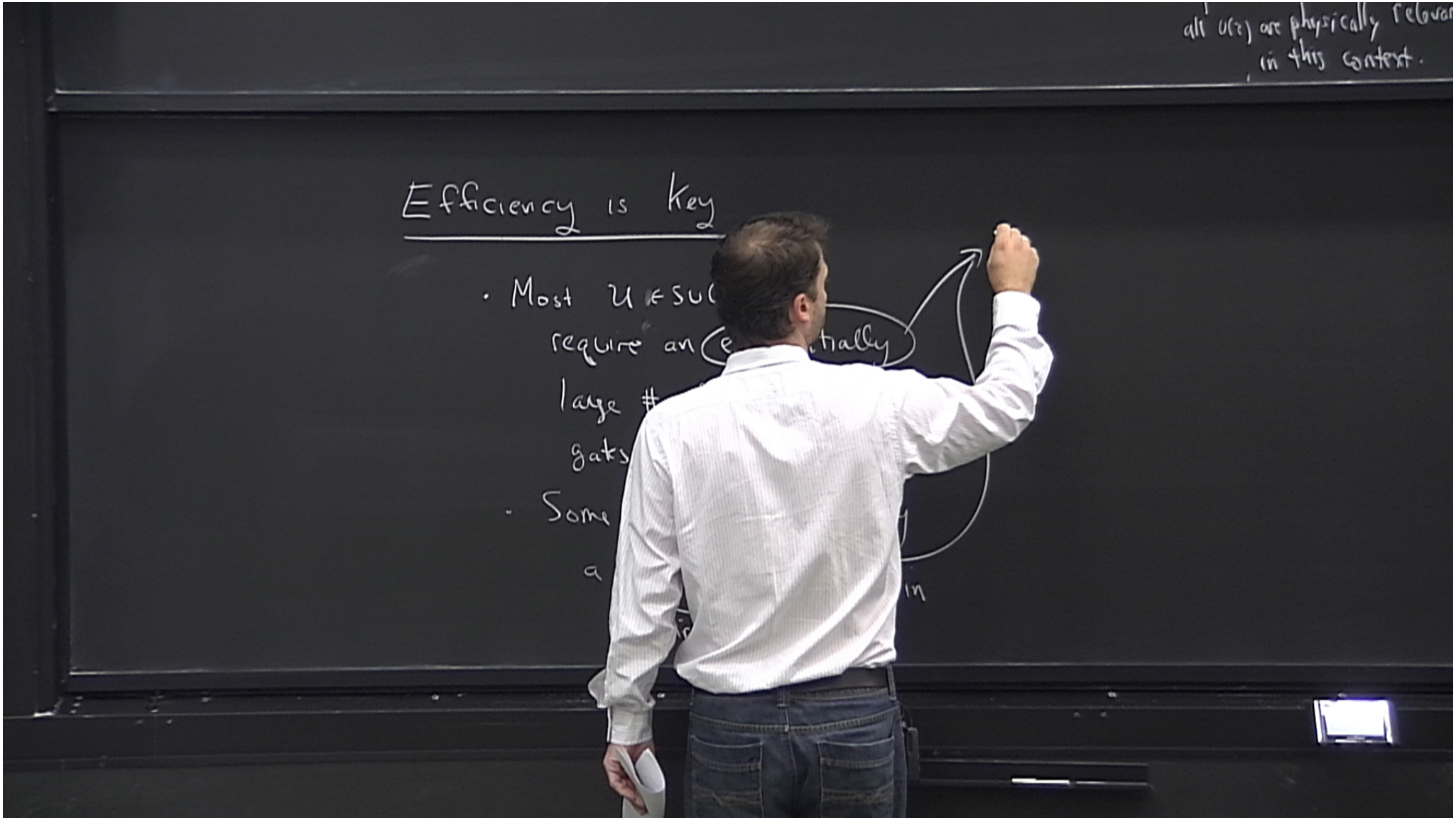

all U(z) are physically relevan
in this context.
Efficiency is key

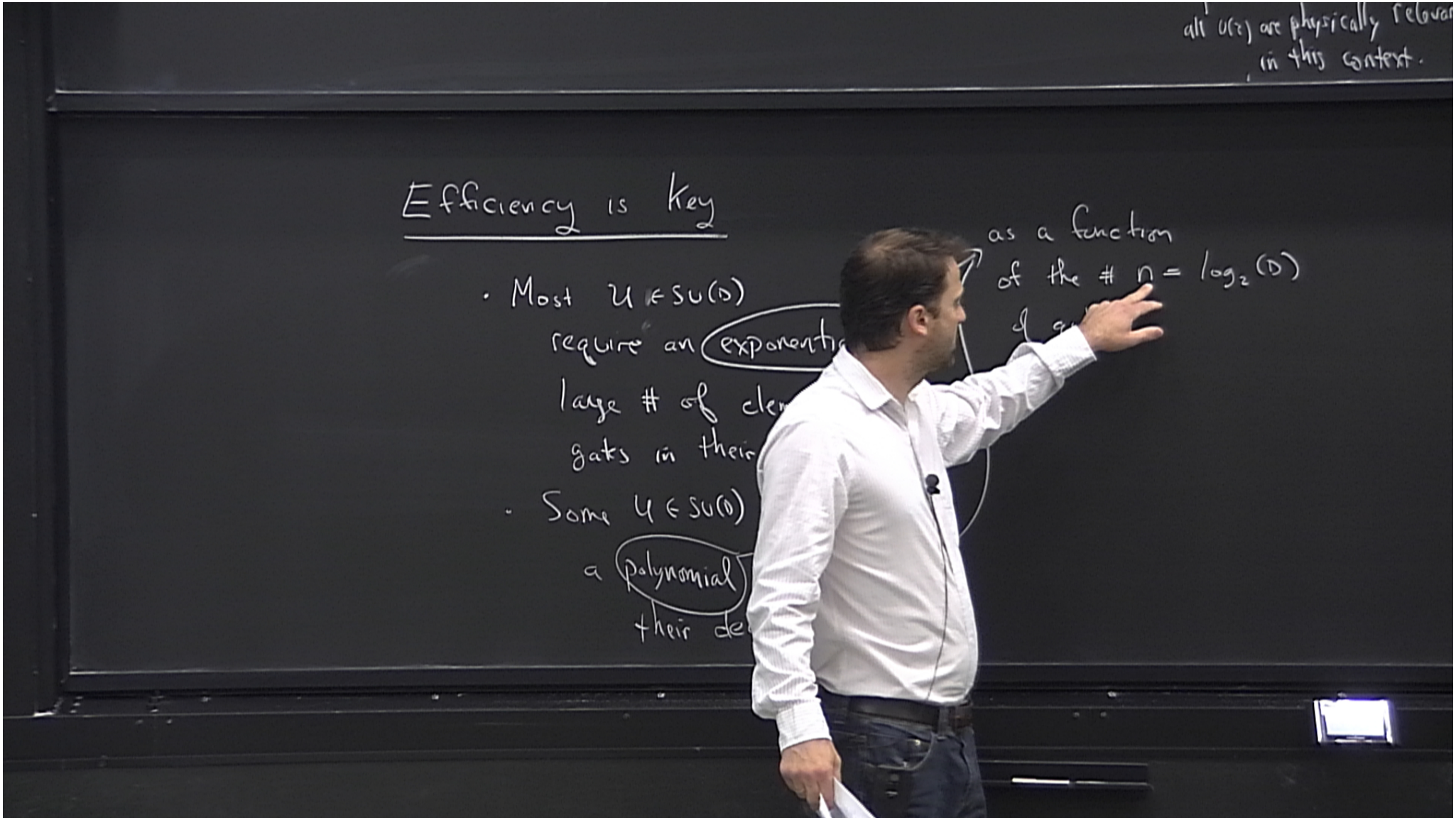
all $U(2)$ are physically relevant in this context.

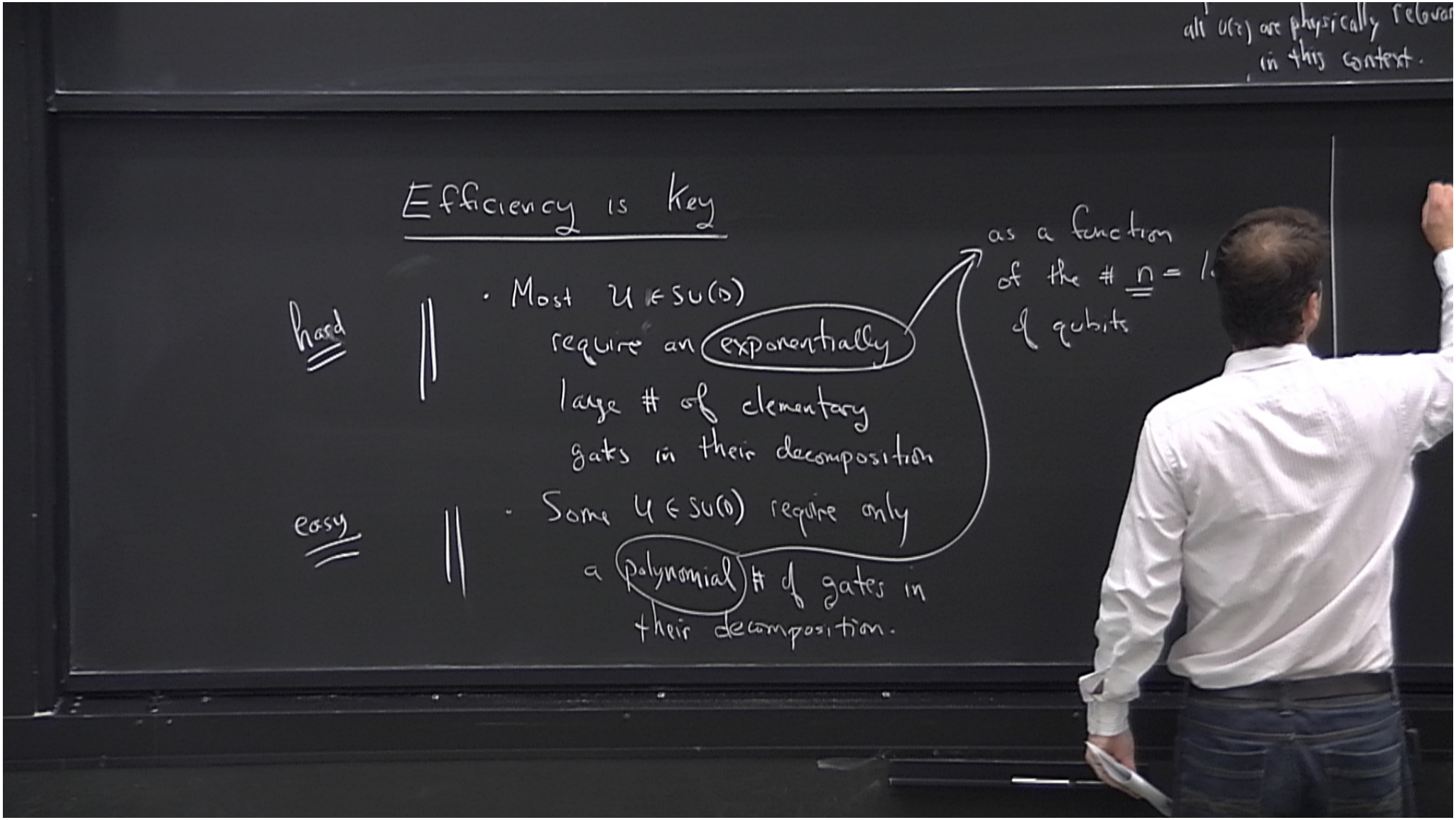
Efficiency is key

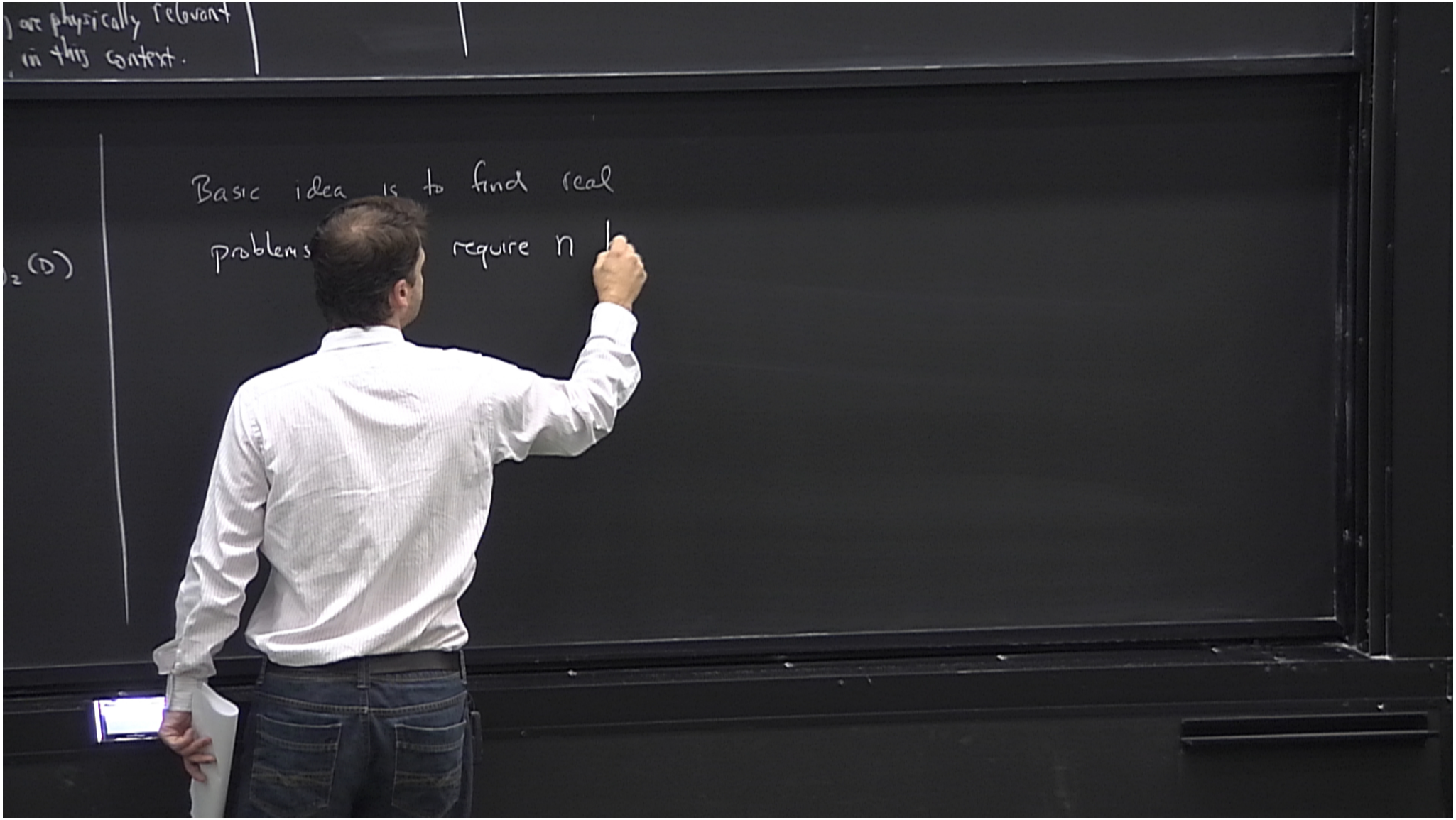
- Most $U \in SU(D)$ require an exponentially large # of elementary gates in their decomposition
- Some $U \in SU(D)$ require only a polynomial # of gates in their decomposition.

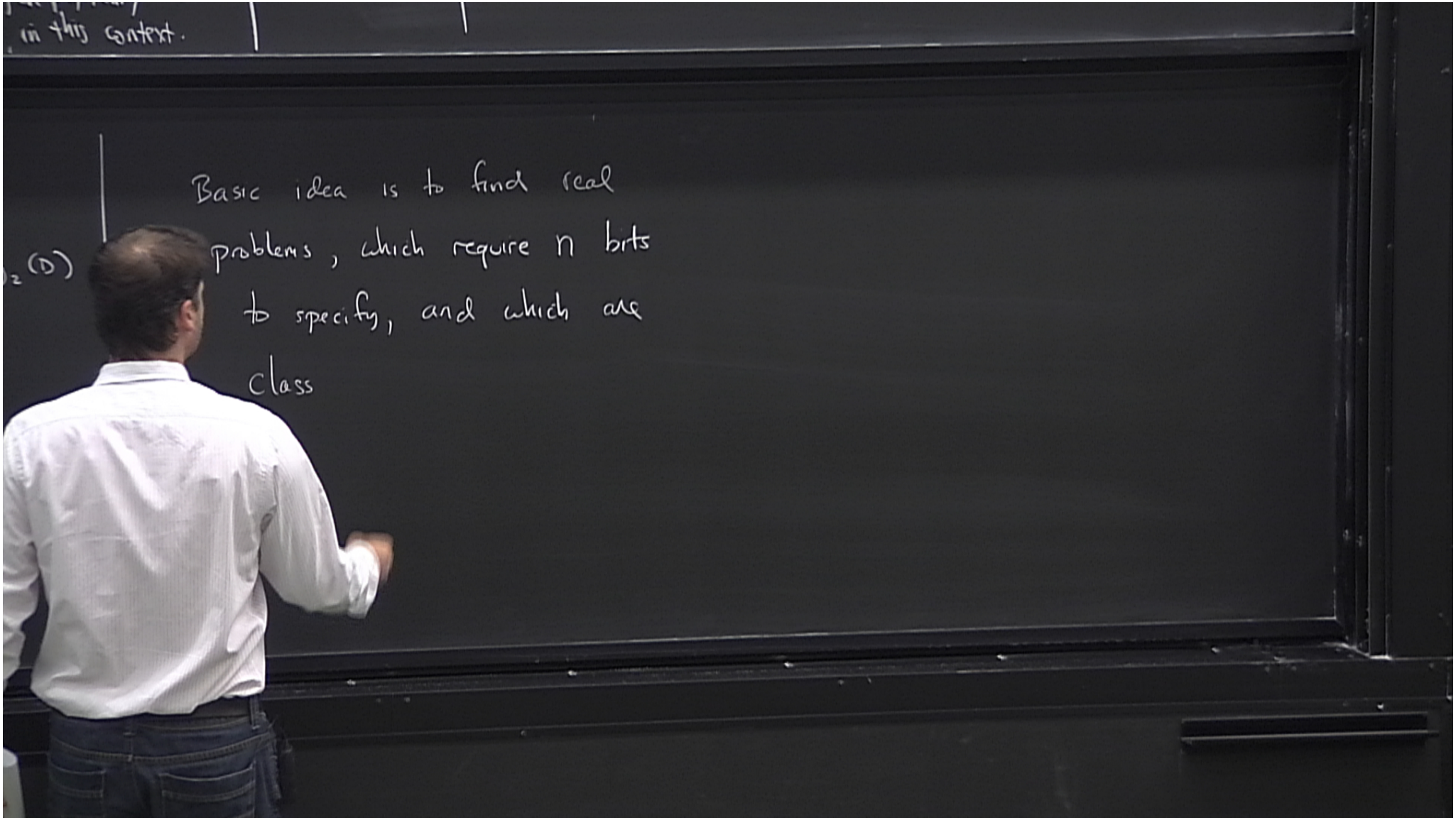


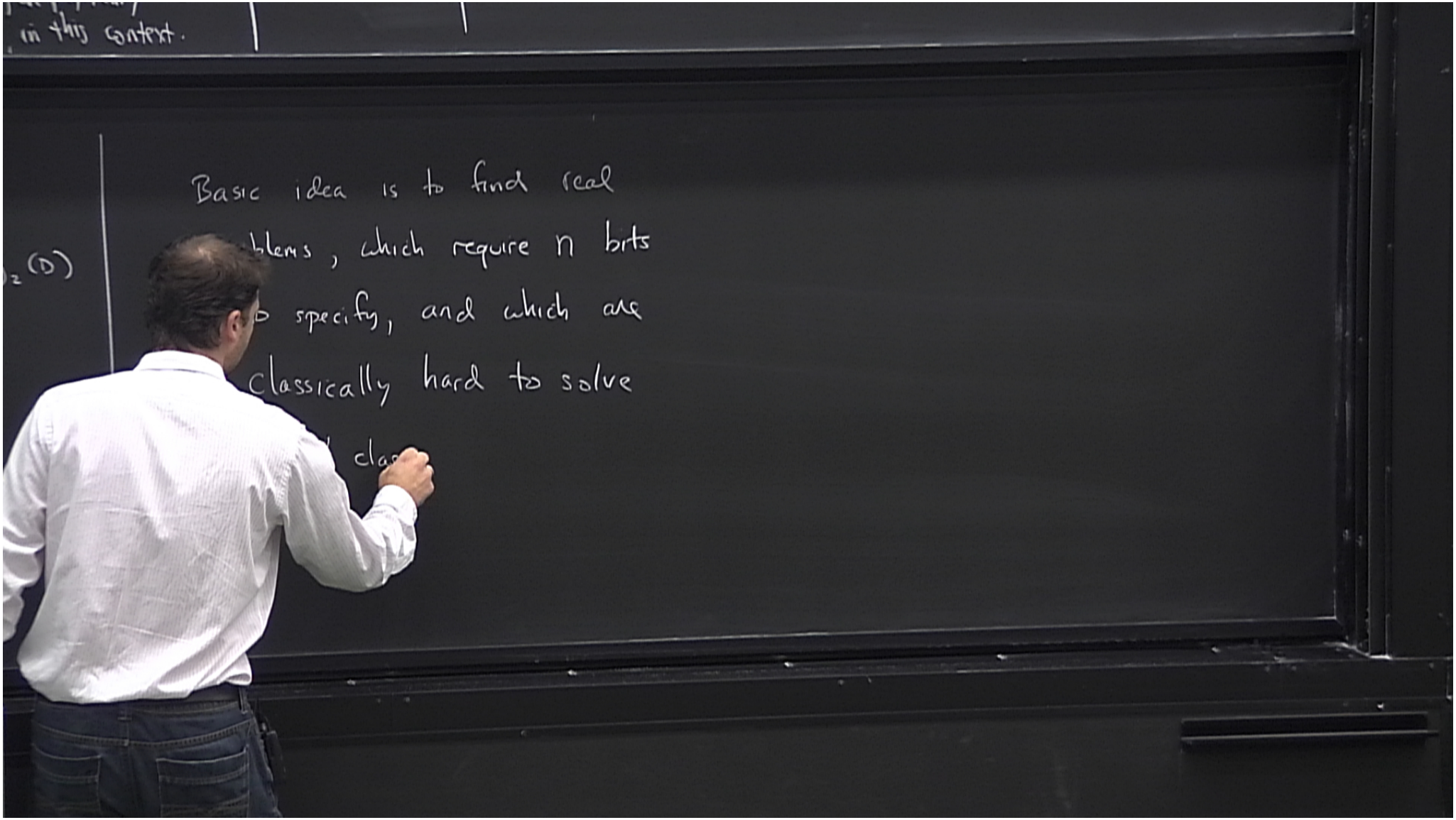

all U(z) are physically relevan
in this context.
Efficiency is key
· Most U
require an
large #
gate
· Some
a
in


all U(2) are physically relevan
in this context.
Efficiency is key
as a function
of the # n = log2(D)
Most U ∈ SU(D)
require an exponentia
large # of cle
gates in their
Some U ∈ SU(D)
a polynomial
their de


all U(2) are physically relevant
in this context.
Efficiency is key
hard
easy
· Most U ∈ SU(D)
require an exponentially
large # of elementary
gates in their decomposition
· Some U ∈ SU(D) require only
a polynomial # of gates in
their decomposition.
as a function
of the # n = log D
of qubits


are physically relevant
in this context.
Basic idea is to find real
problems require n


in this context.
Basic idea is to find real
problems, which require n bits
to specify, and which are
class

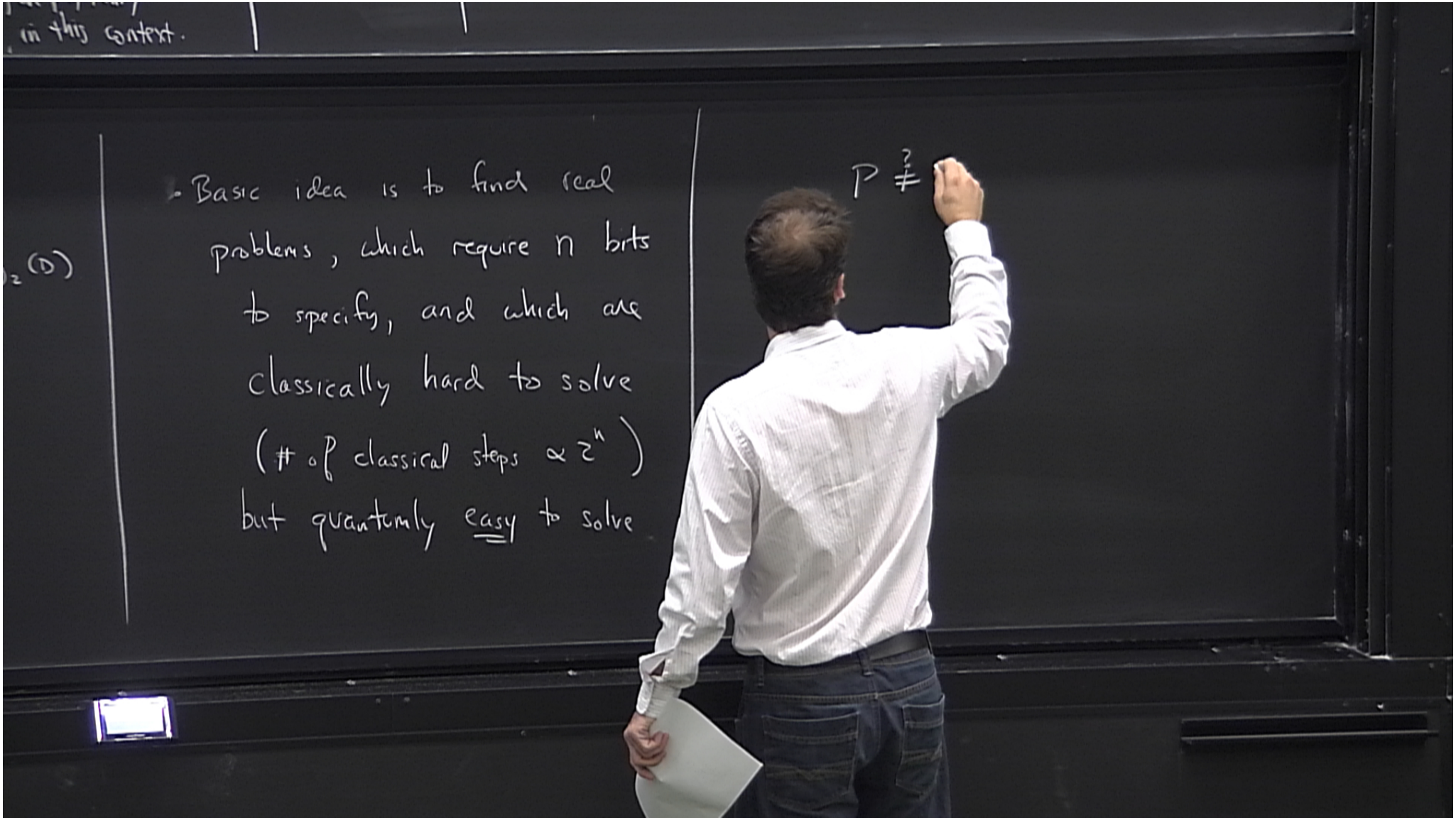

in this context.
Basic idea is to find real
blems, which require n bits
specify, and which are
classically hard to solve

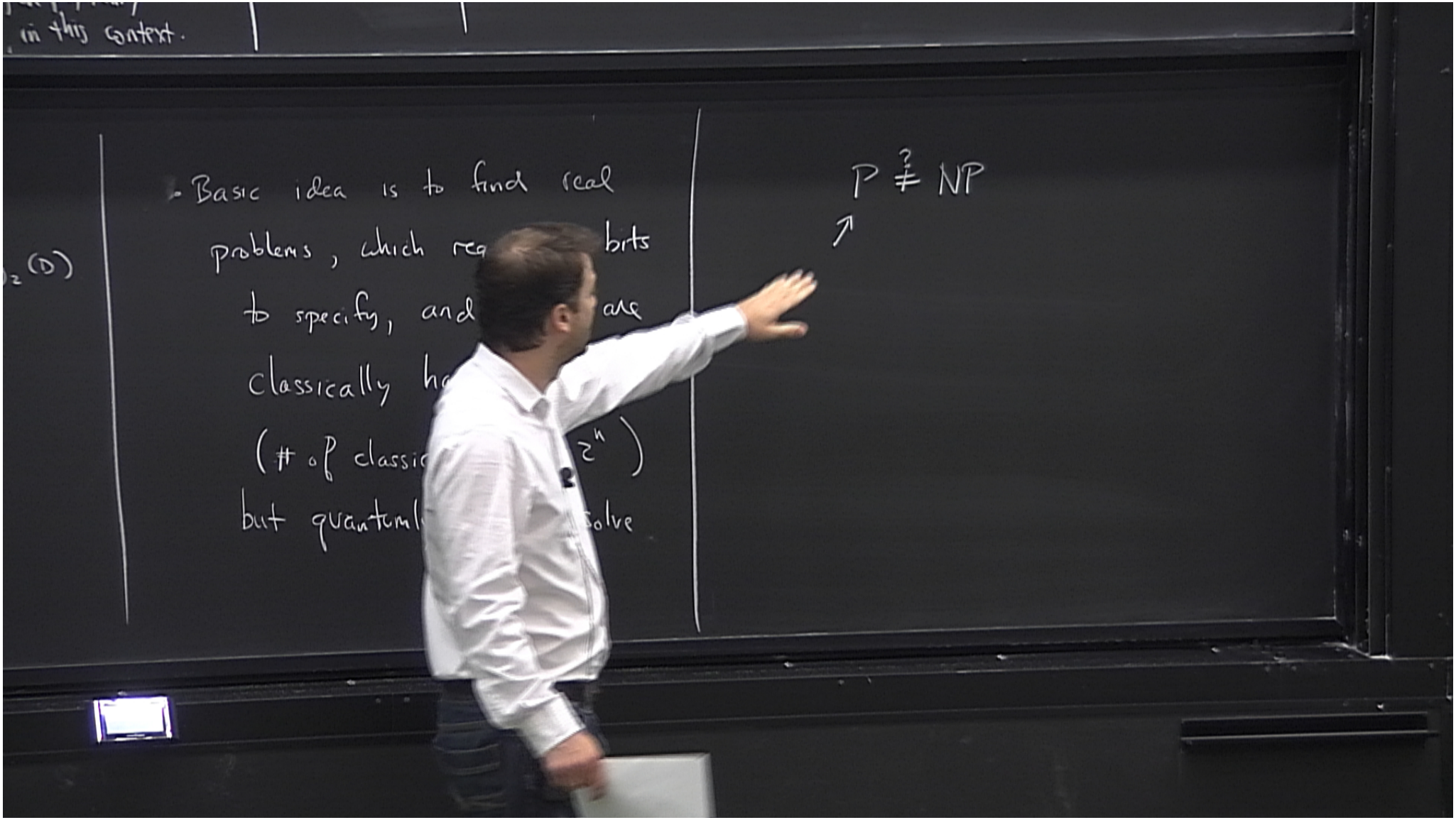
in this context.

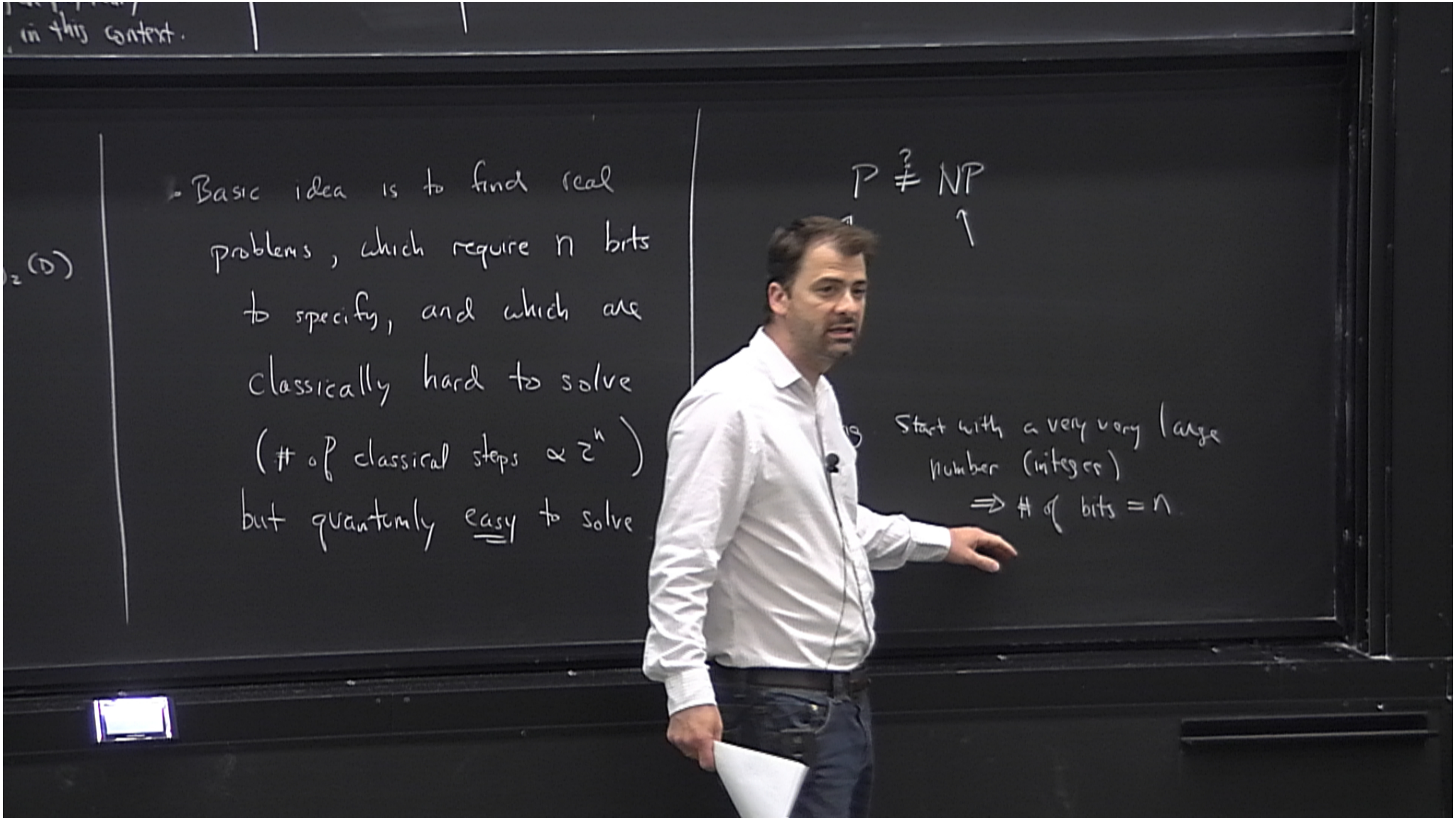
Basic idea is to find real problems, which require n bits to specify, and which are classically hard to solve ($\#$ of classical steps $\propto 2^n$) but quantumly easy to solve

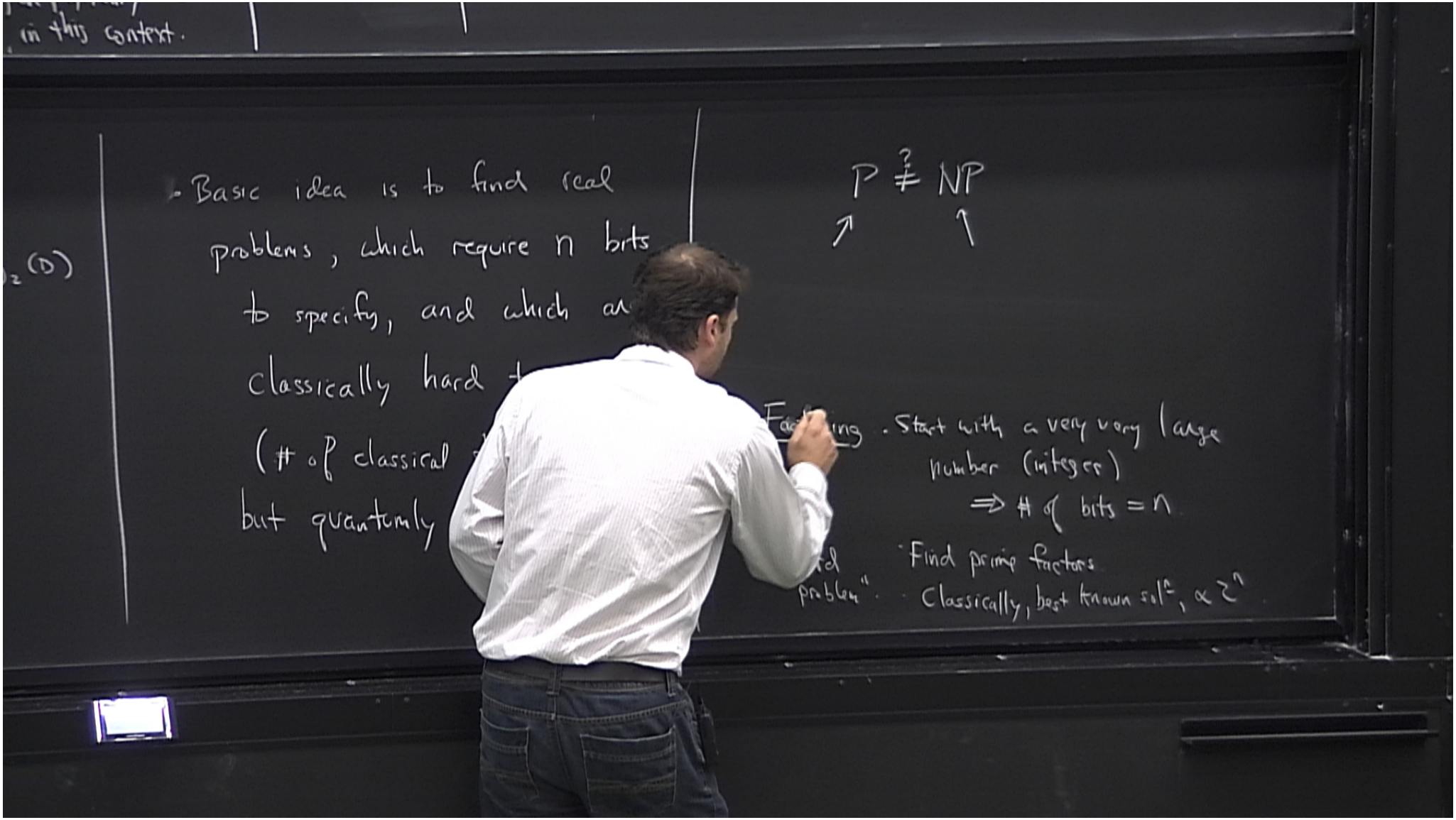
in this context.

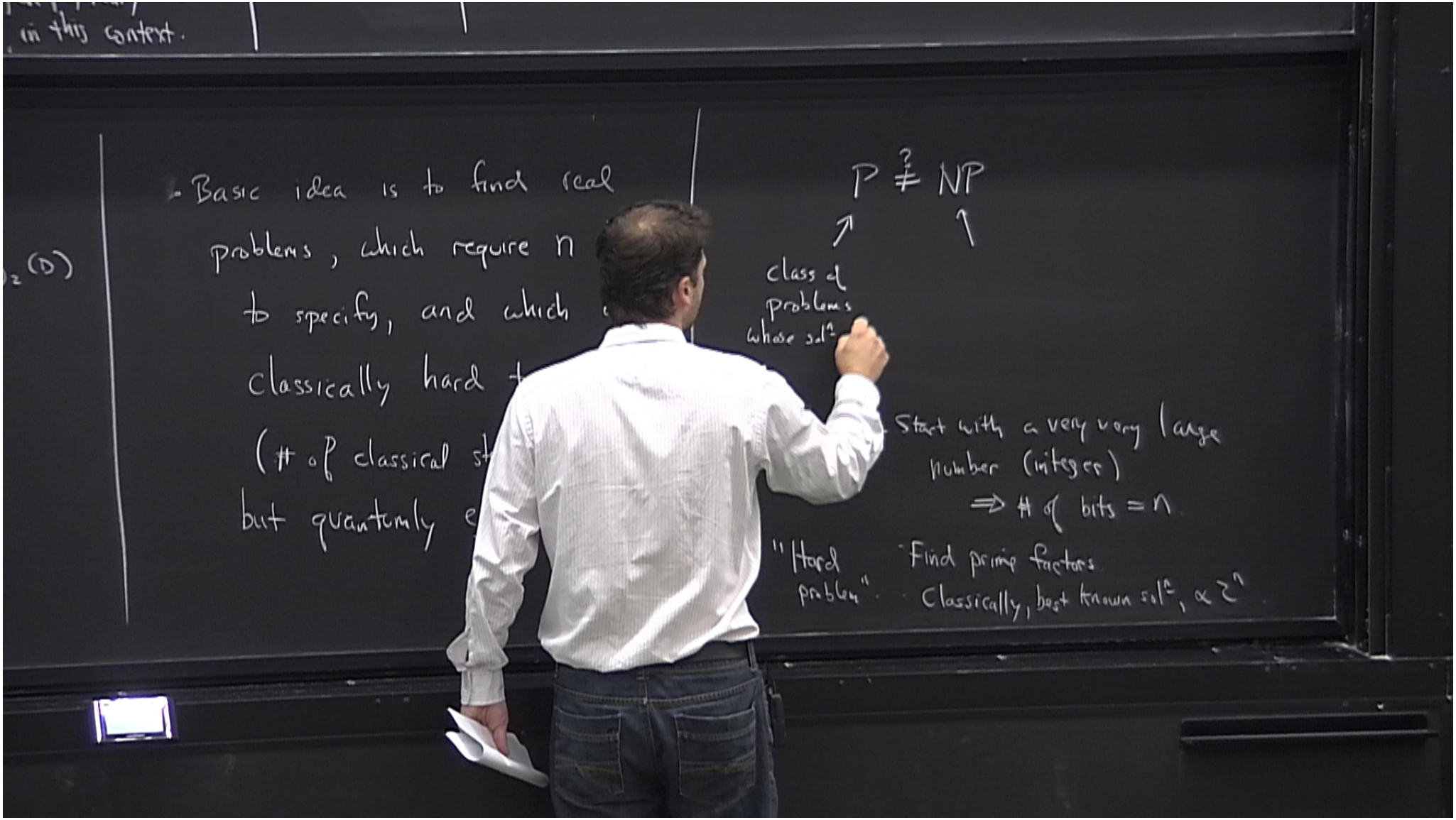
Basic idea is to find real problems, which require n bits to specify, and which are classically hard to solve ($\#$ of classical steps $\propto 2^n$) but quantumly easy to solve

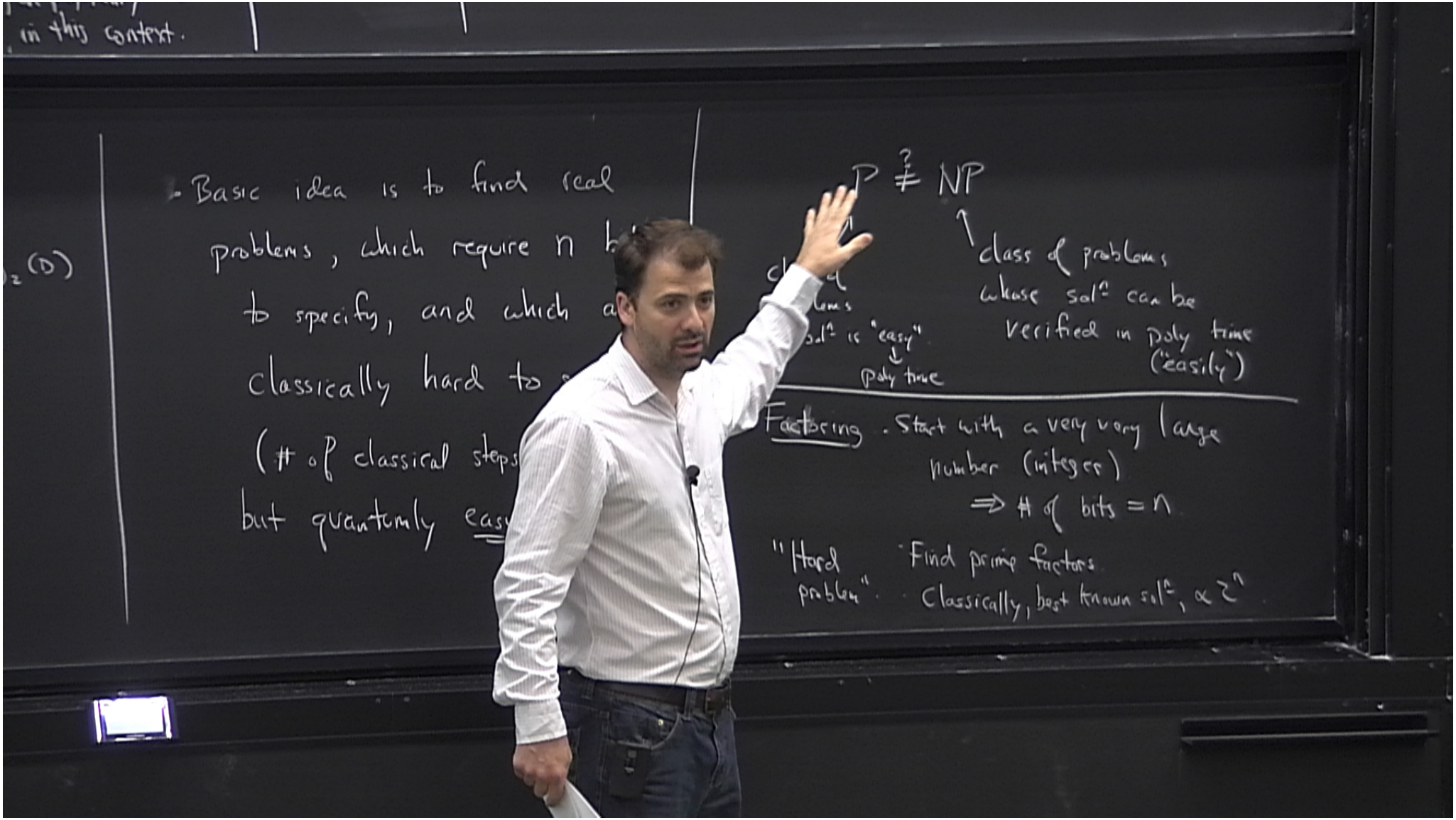

in this context.
• Basic idea is to find real problems, which require n bits to specify, and which are classically hard to solve (# of classical steps $\propto 2^n$) but quantumly easy to solve
$P \stackrel{?}{\neq}$


in this context.
- Basic idea is to find real
problems, which rea bits
to specify, and are
classically ha
(# of classic 2^n)
but quantuml solve
$P \stackrel{?}{\neq} NP$


in this context.
- Basic idea is to find real problems, which require n bits to specify, and which are classically hard to solve (# of classical steps $\propto 2^n$) but quantumly easy to solve
$P \overset{?}{\neq} NP$
Start with a very very large number (integer)
$\Rightarrow$ # of bits = n


in this context.
Basic idea is to find real
problems, which require n bits
to specify, and which ar
classically hard
(# of classical
but quantumly
$P \overset{?}{\neq} NP$
Factoring
Start with a very very large number (integer)
$\Rightarrow$ # of bits = n
Find prime factors
Classically, best known sol^{n}, $\propto 2^{n}$


in this context.
Basic idea is to find real
problems, which require n
to specify, and which
classically hard
(# of classical
but quantumly
P ≟ NP
Class of
problems
whose
Start with a very very large
number (integer)
⇒ # of bits = n
"Hard
problem"
Find prime factors.
Classically, best known


in this context.
Basic idea is to find real
problems, which require n
to specify, and which
classically hard to
(# of classical steps
but quantumly
P ? ≠ NP
class of problems
whose sol^n can be
verified in poly time
("easily")
sol^n is "easy"
poly time
Factoring. Start with a very very large
number (integer)
⇒ # of bits = n
"Hard
problem"
Find prime factors.
Classically, best known sol^n, ∝ 2^n

in this context.

- Basic idea is to find real problems, which require n bits to specify, and which are classically hard to solve ($\#$ of classical steps $\propto 2^n$) but quantumly easy to solve

$P \overset{?}{\neq} NP$

Class of problems whose sol^n is "easy" (poly time)

Class of problems whose sol^n can be verified in poly time ("easily")

Factoring. Start with a very very large number (integer) $\Rightarrow$ # of bits $= n$

"Hard problem"

- Find prime factors.
- Classically, best known sol^n, $\propto 2^n$

in this context.

Efficiency is key

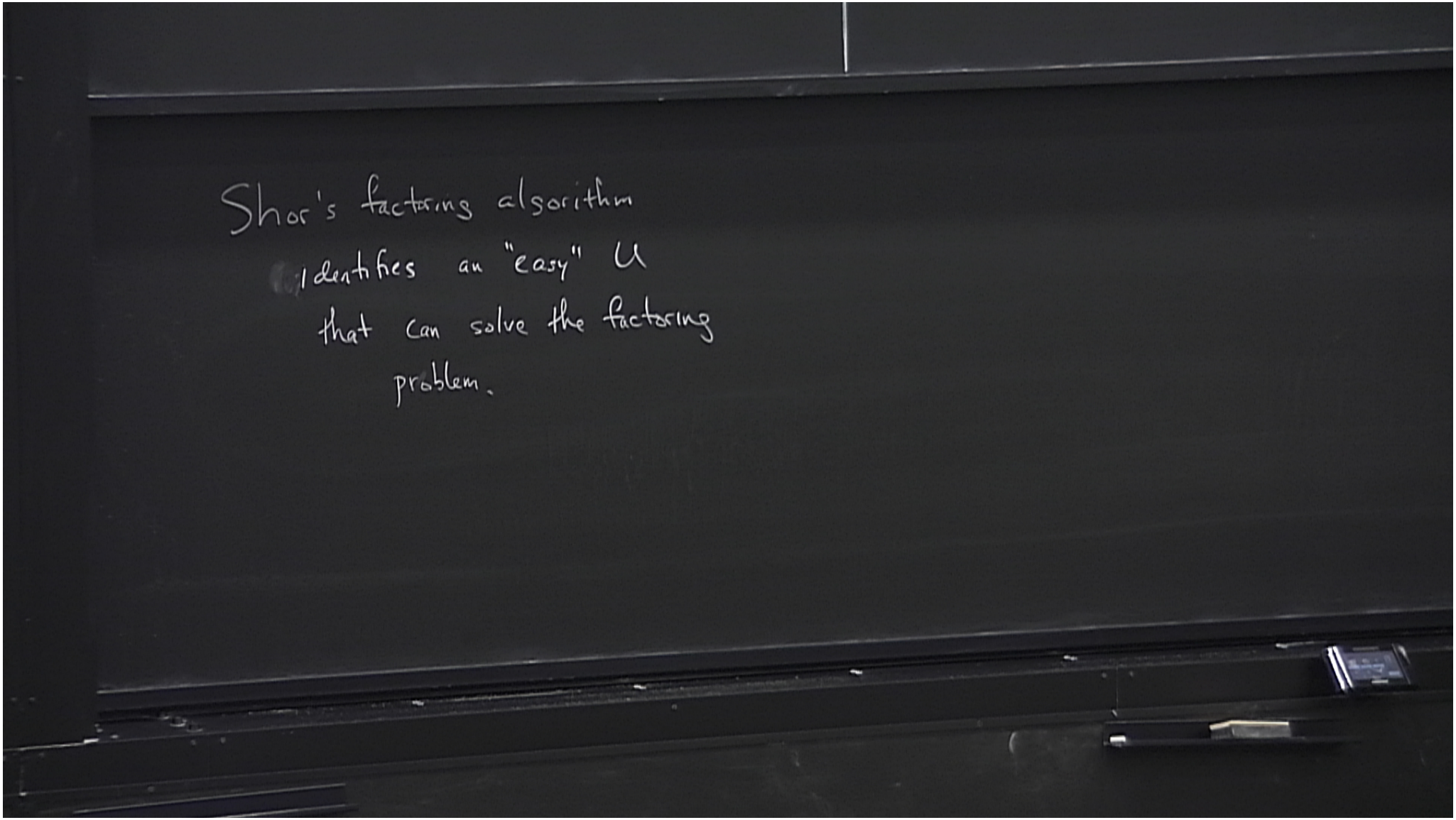
hard ||

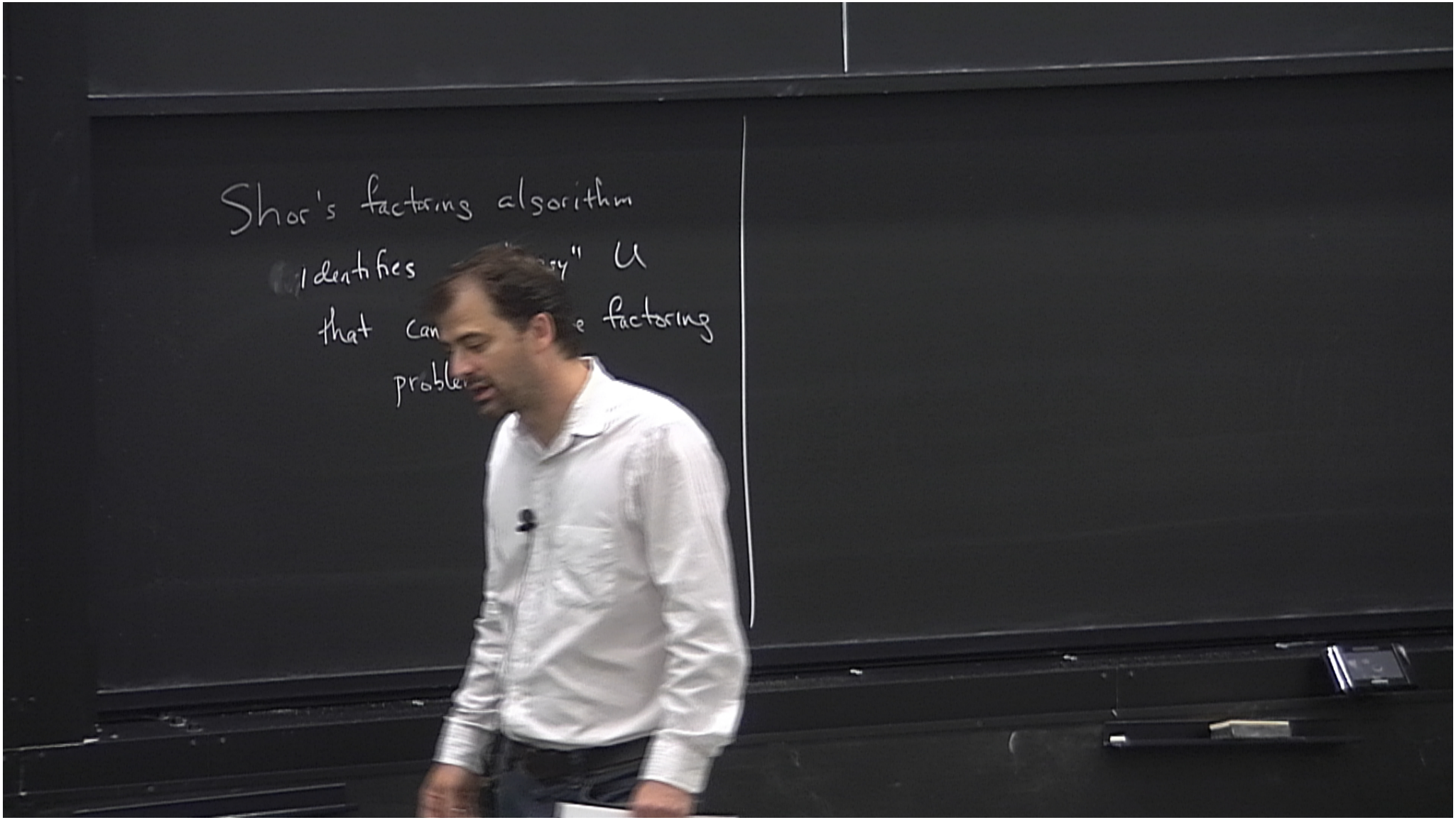
- Most $U \in SU(D)$ require an (exponentially) large # of elementary gates in their decomposition

easy ||

- Some $U \in SU(D)$ require only a (polynomial) # of gates in their decomposition.

as a function of the # $n = \log_2(D)$ of qubits


Shor's factoring algorithm
identifies an "easy" U
that can solve the factoring
problem.


Shor's factoring algorithm
identifies
that
factoring
proble

in this context.

(D)

- Basic idea is to find real problems, which require n bits to specify, and which are classically hard to solve ($\#$ of classical steps $\propto 2^n$) but quantumly easy to solve

$P \overset{?}{\neq} NP$

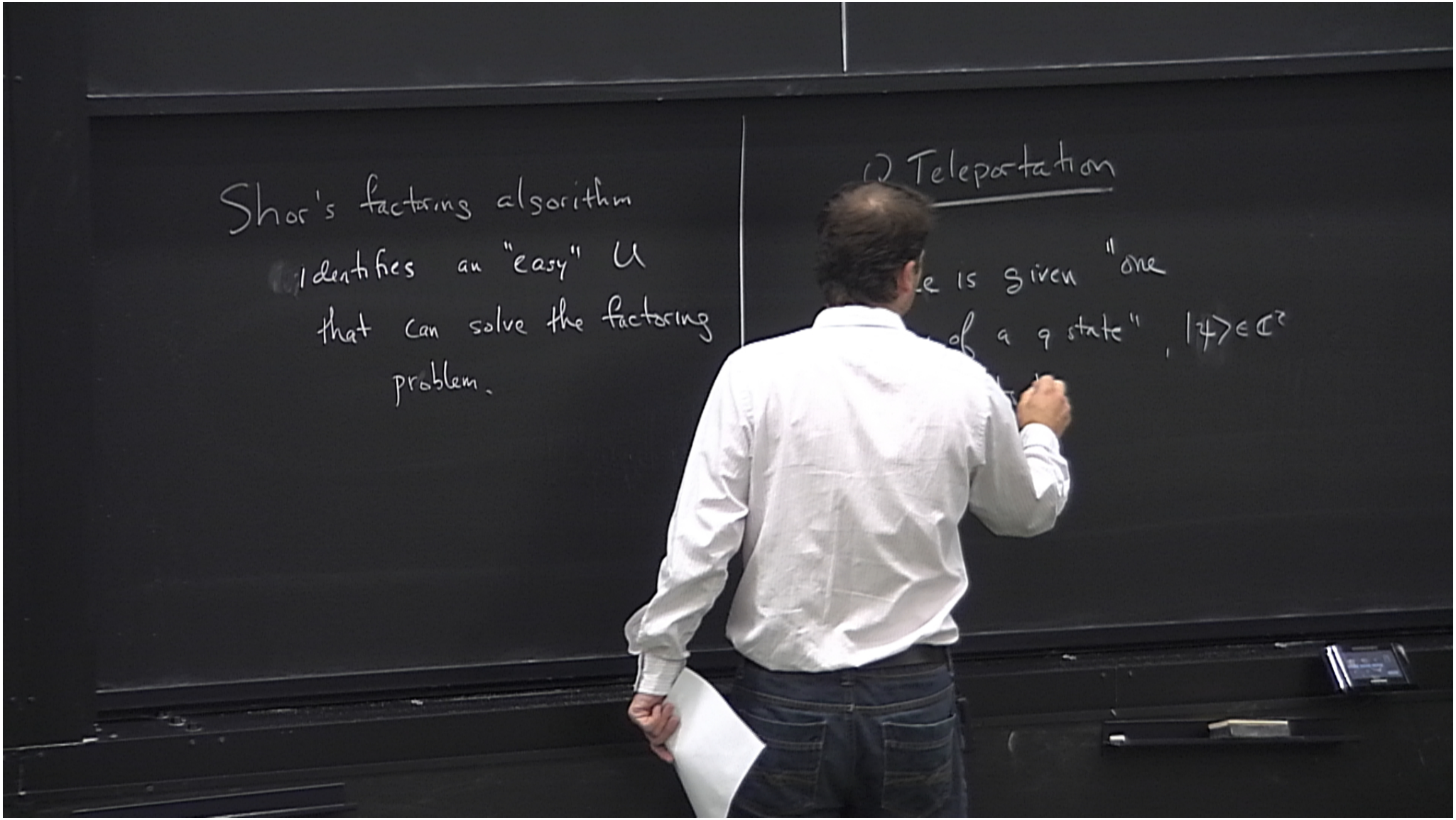
↗ Class of problems whose sol^n is "easy" ↓ poly time

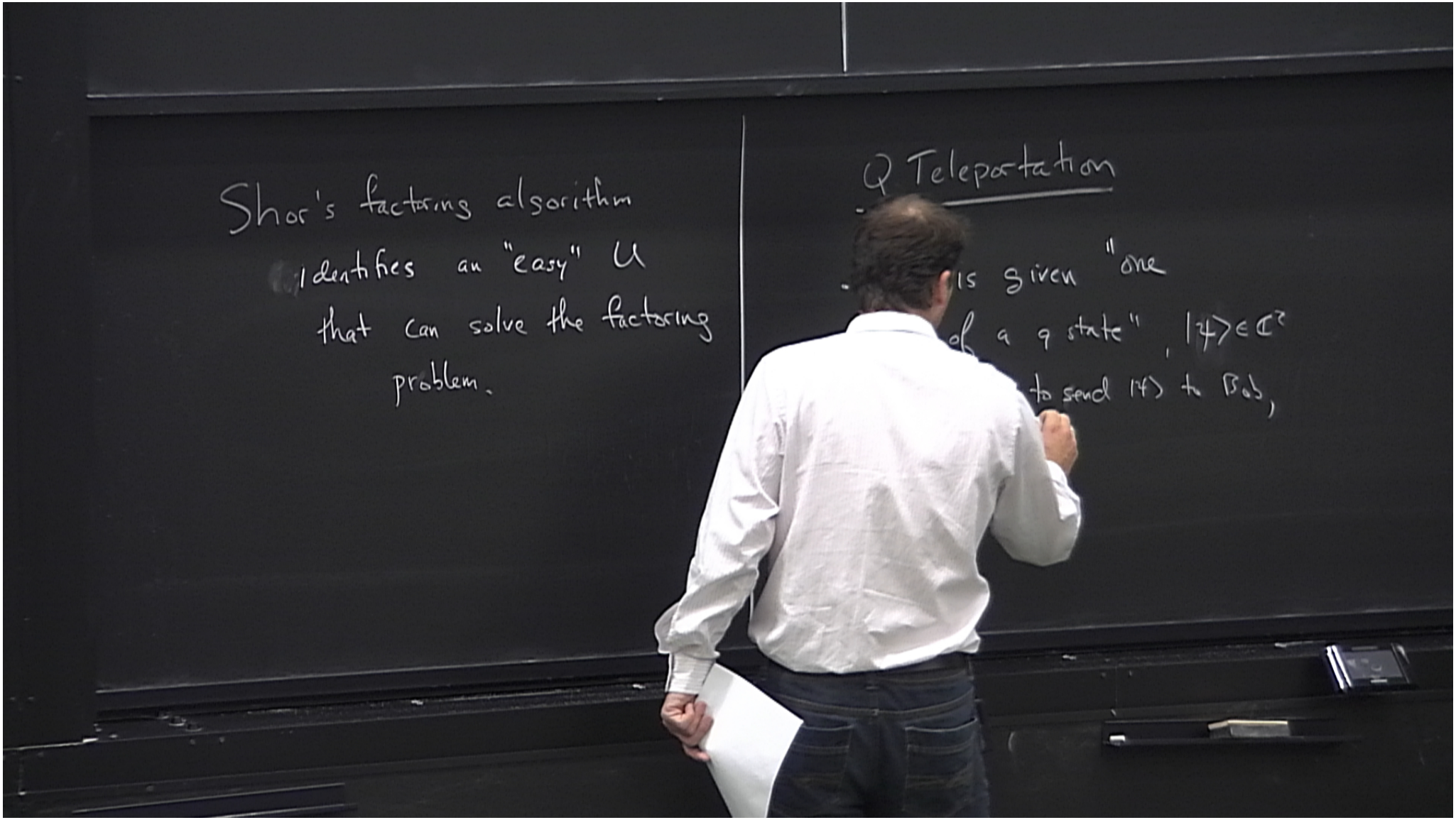
↖ class of problems whose sol^n can be verified in poly time ("easily")

Factoring. Start with a very very large number (integer) $\Rightarrow$ # of bits $= n$

"Hard problem"

- Find prime factors
- Classically, best known sol^n, $\propto 2^n$


Shor's factoring algorithm
identifies an "easy" U
that can solve the factoring
problem.
2) Teleportation
is given "one
of a q state" $|\psi\rangle \in \mathbb{C}^2$

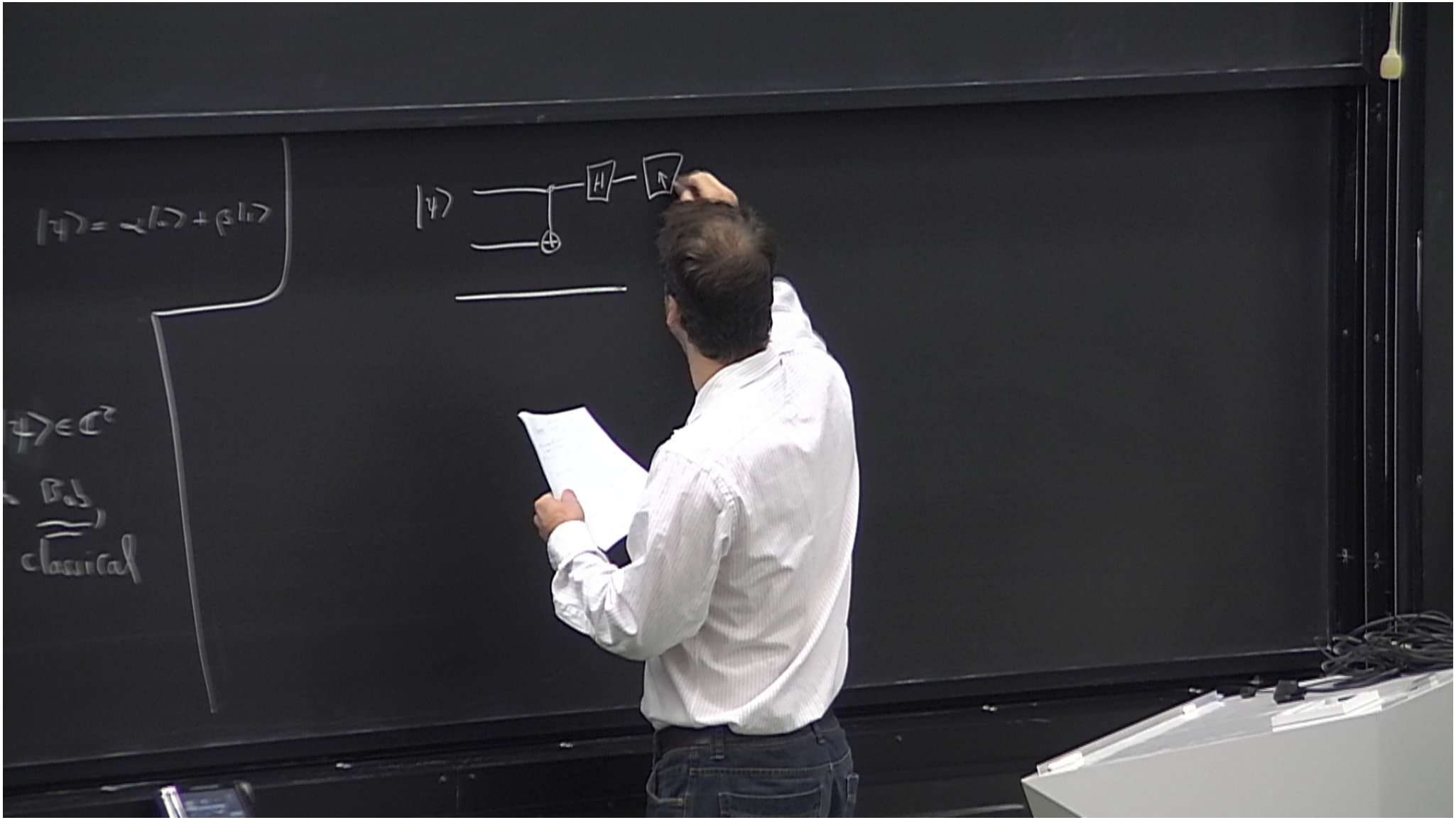

Shor's factoring algorithm
identifies an "easy" U
that can solve the factoring
problem.
Q Teleportation
is given "one
of a q state" $|\psi\rangle \in \mathbb{C}^2$
to send $|\psi\rangle$ to Bob,

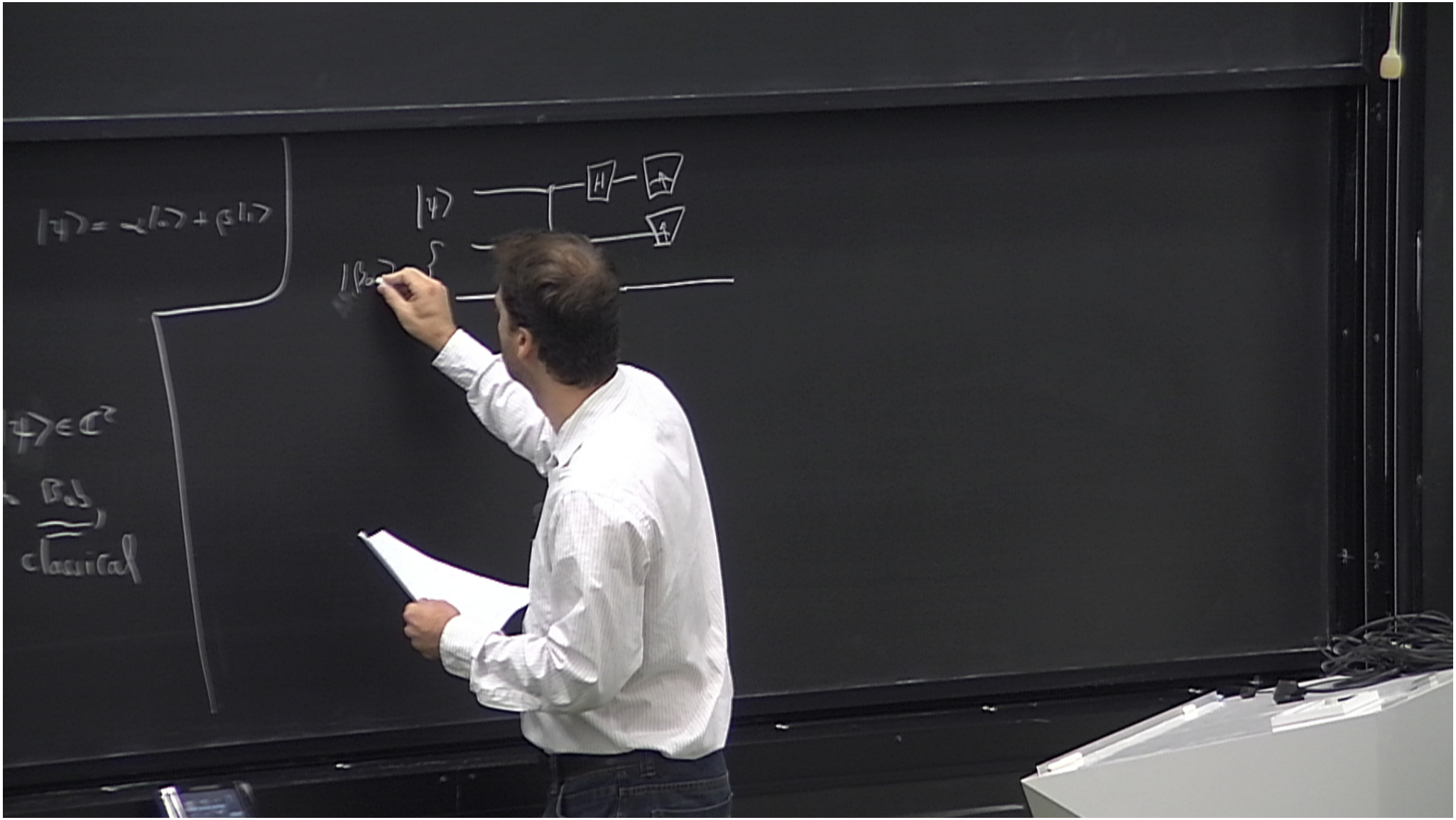
Shor's factoring algorithm identifies an "easy" U that can solve the factoring problem.

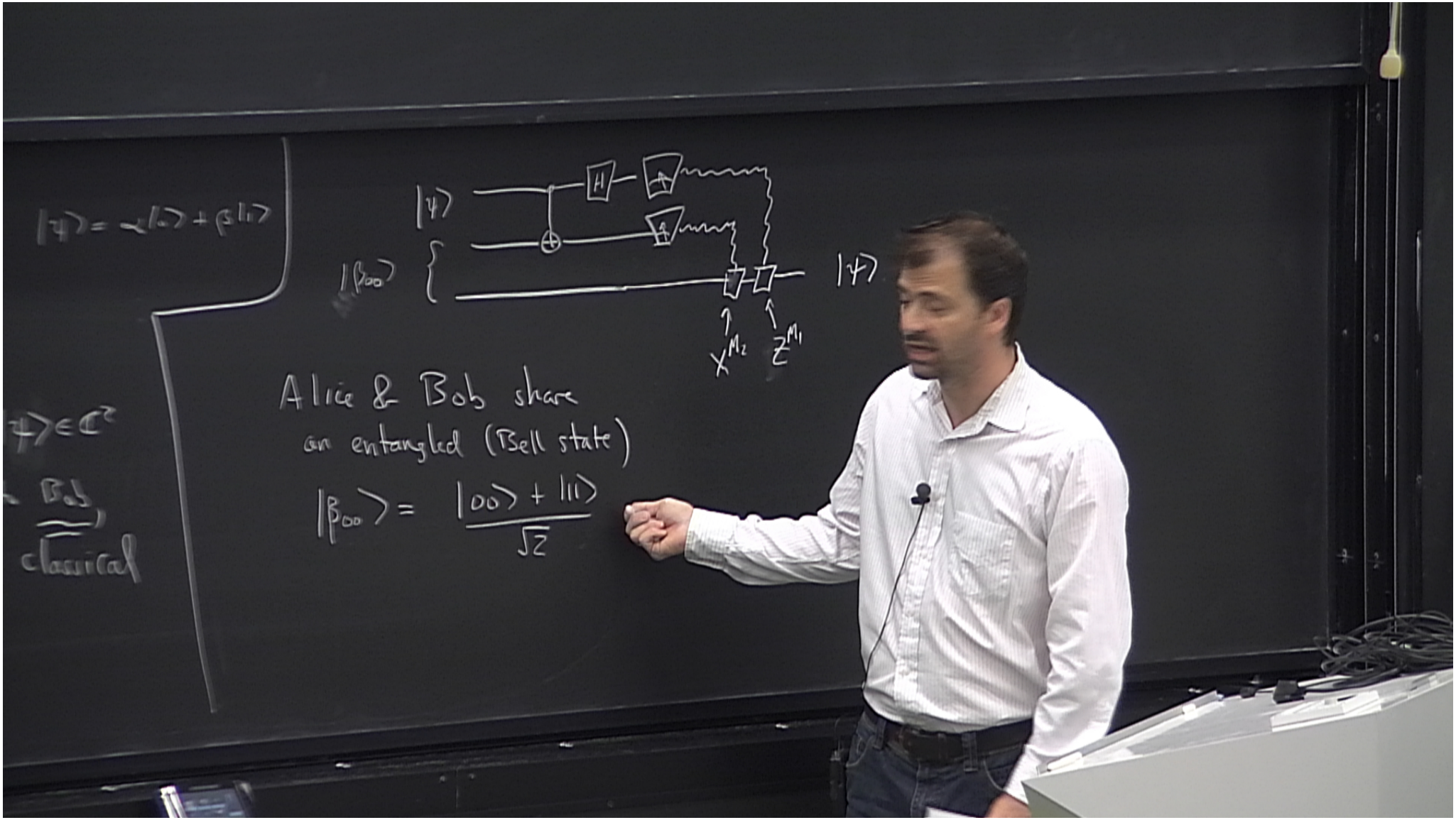
Q Teleportation

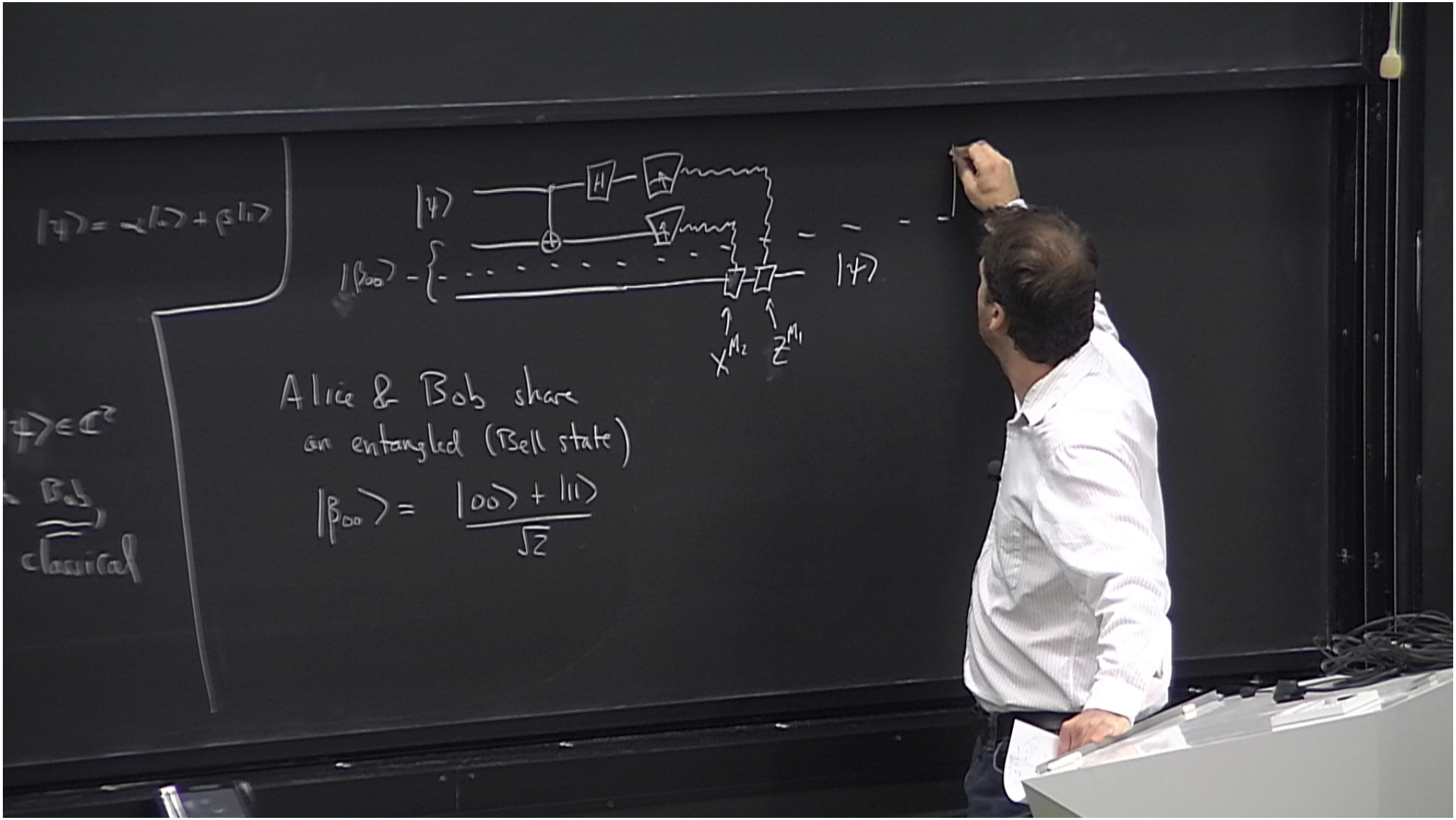
- Alice is given "one copy of a q state", $|\psi\rangle \in \mathbb{C}^2$
- Alice wants to send $|\psi\rangle$ to Bob, but only has access to classical communication.

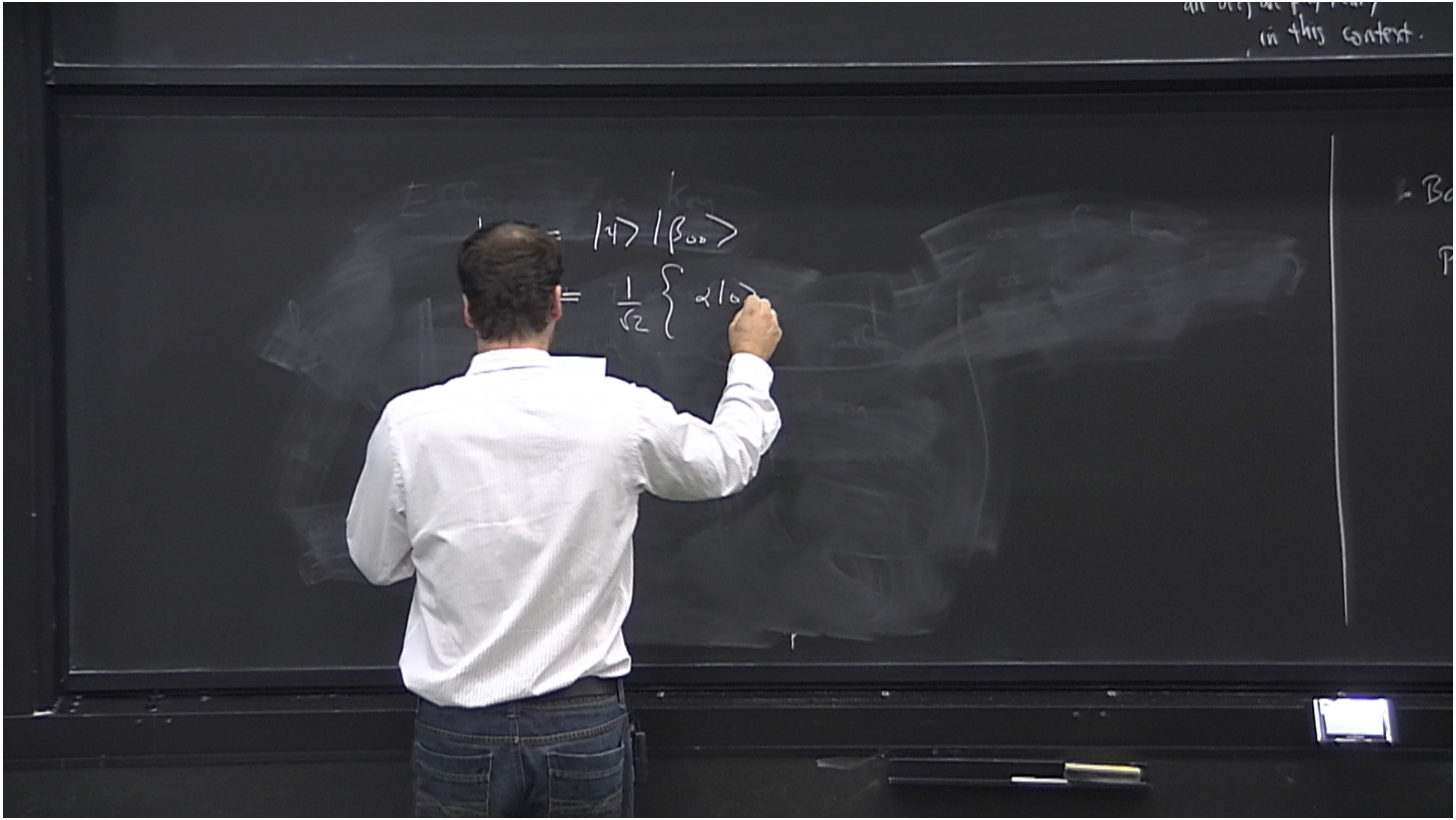

Efficiency is key
Here the first 7 gates
and the CNOT
Shor's factoring algorithm
Q Teleportation

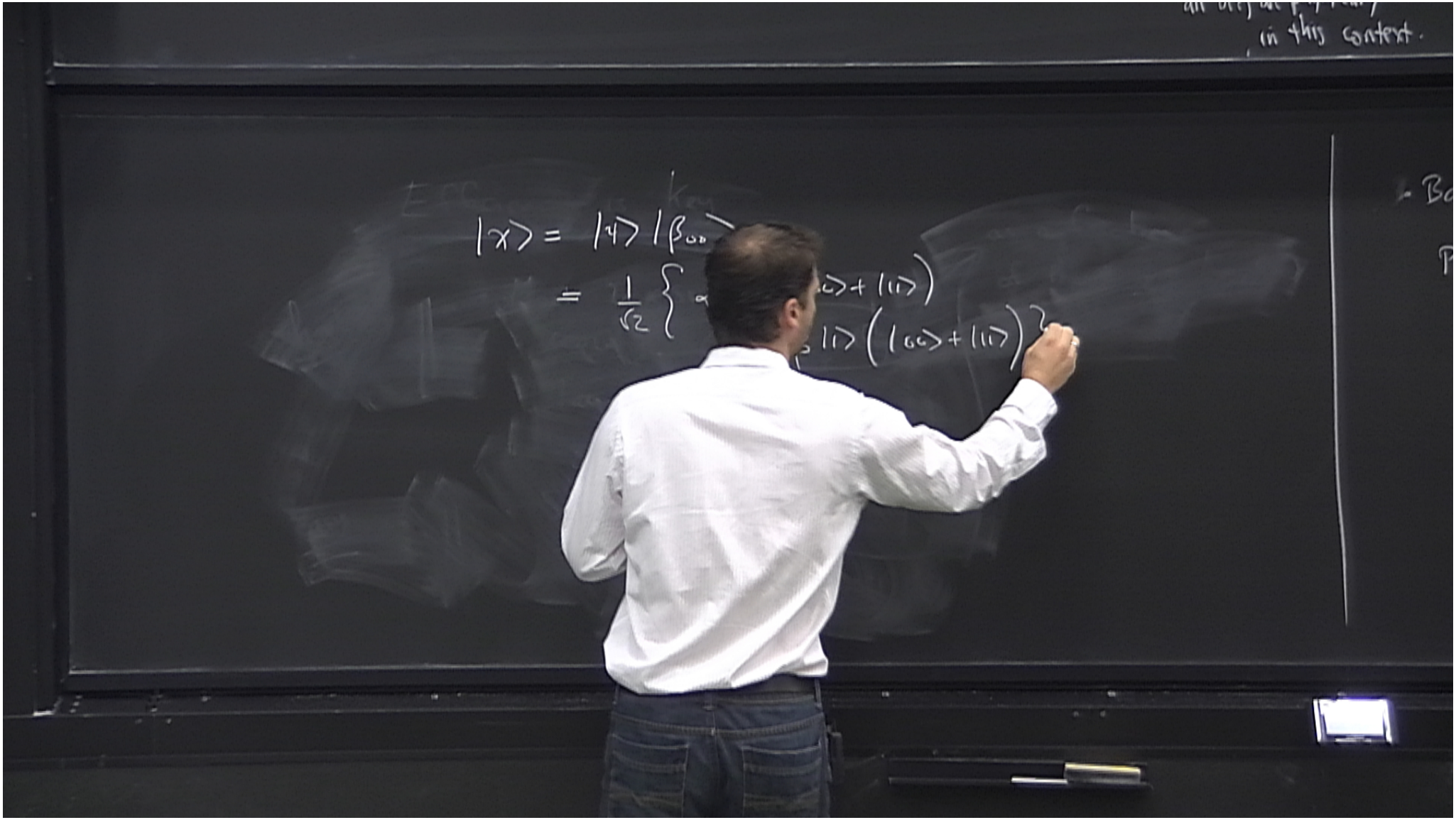

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
$|\psi\rangle$
H
$|\psi\rangle \in \mathbb{C}^2$
By
classical

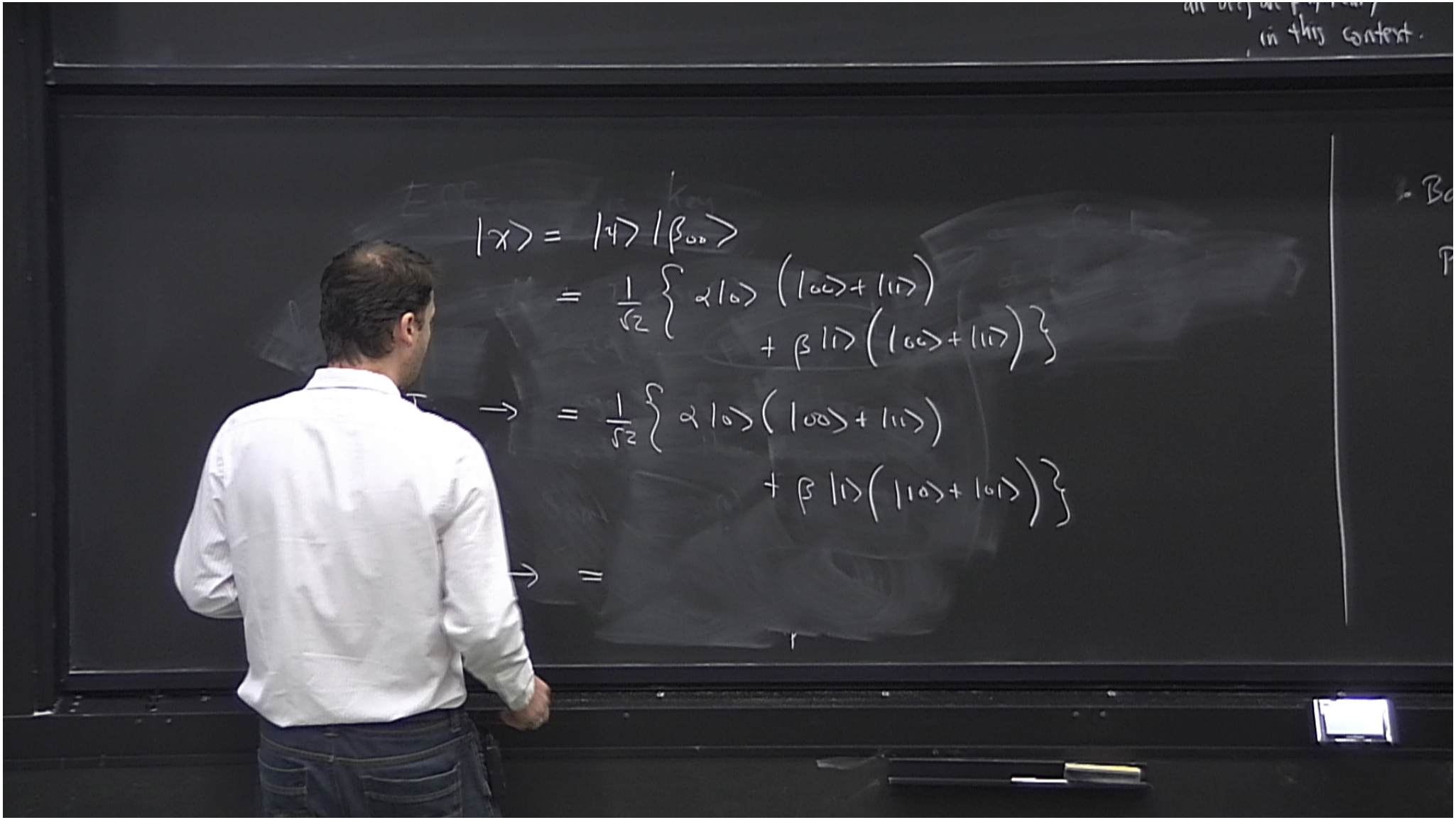

classical

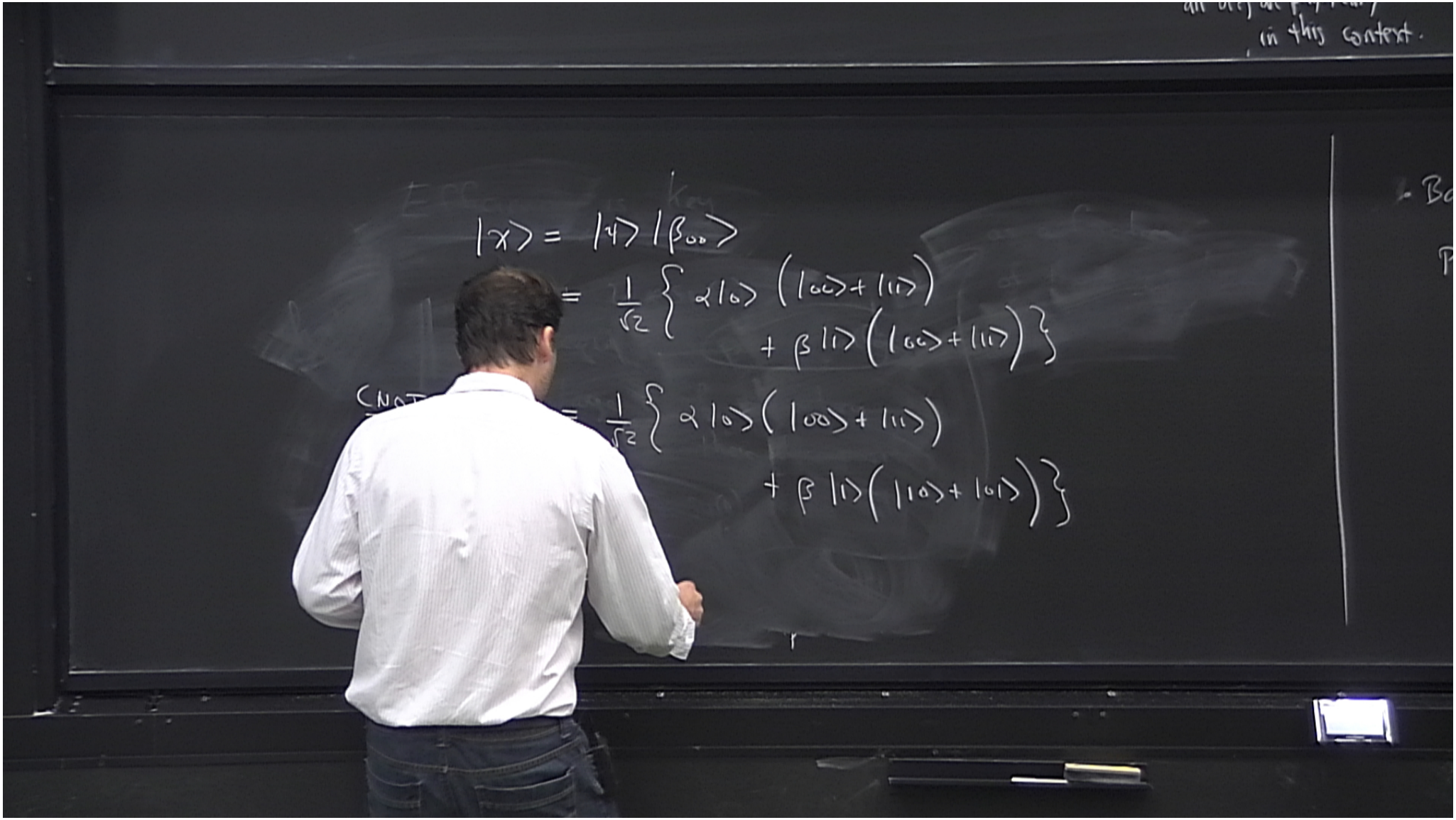

Alice & Bob share
an entangled (Bell state)
$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
$|\psi\rangle$
$|\beta_{00}\rangle$
X^{M_2}
Z^{M_1}
$|\psi\rangle$
classical

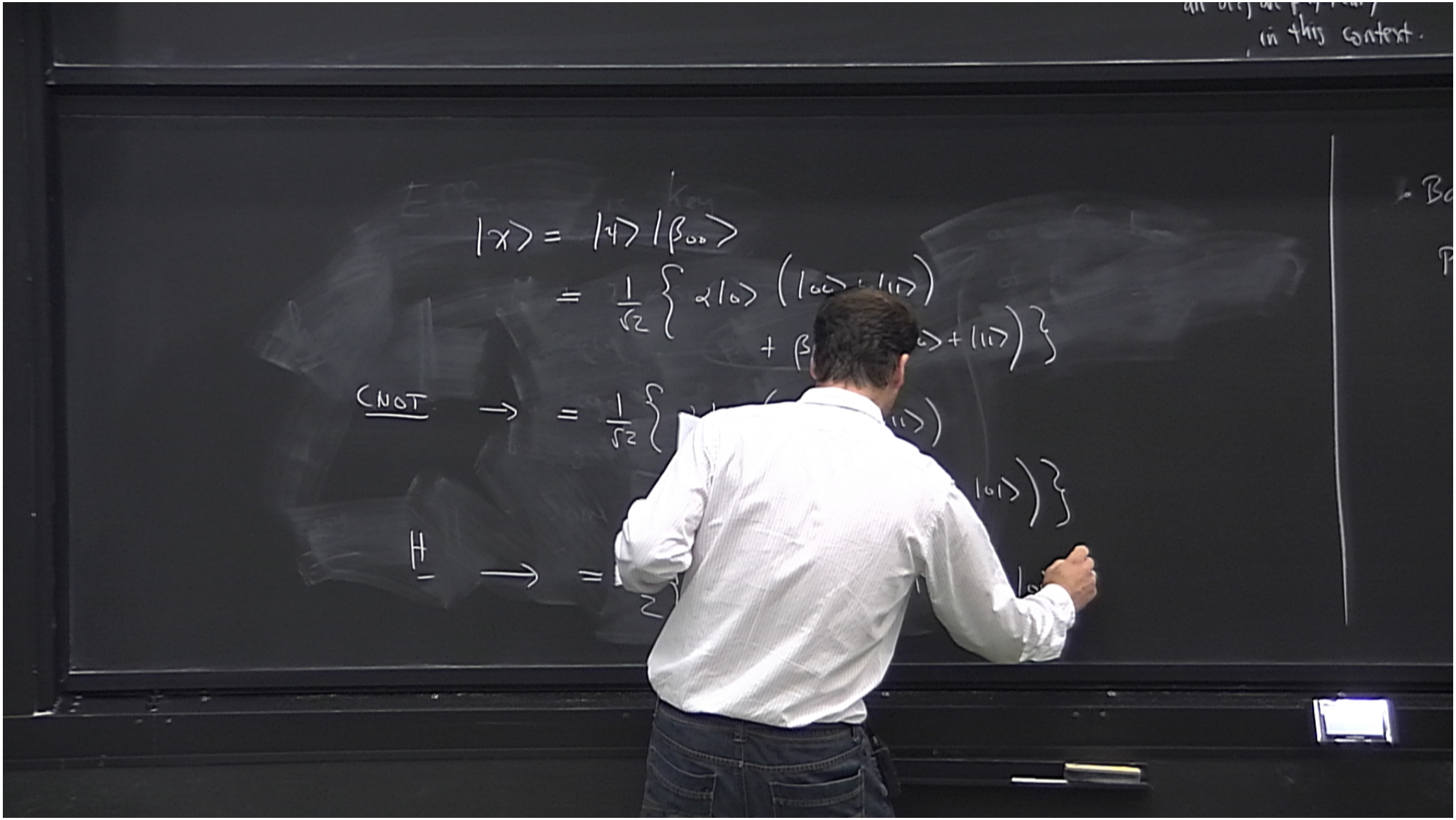

Alice & Bob share
an entangled (Bell state)
$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
$|\psi\rangle$
$|\beta_{00}\rangle$
H
X^{M_2}
Z^{M_1}
$|\psi\rangle$

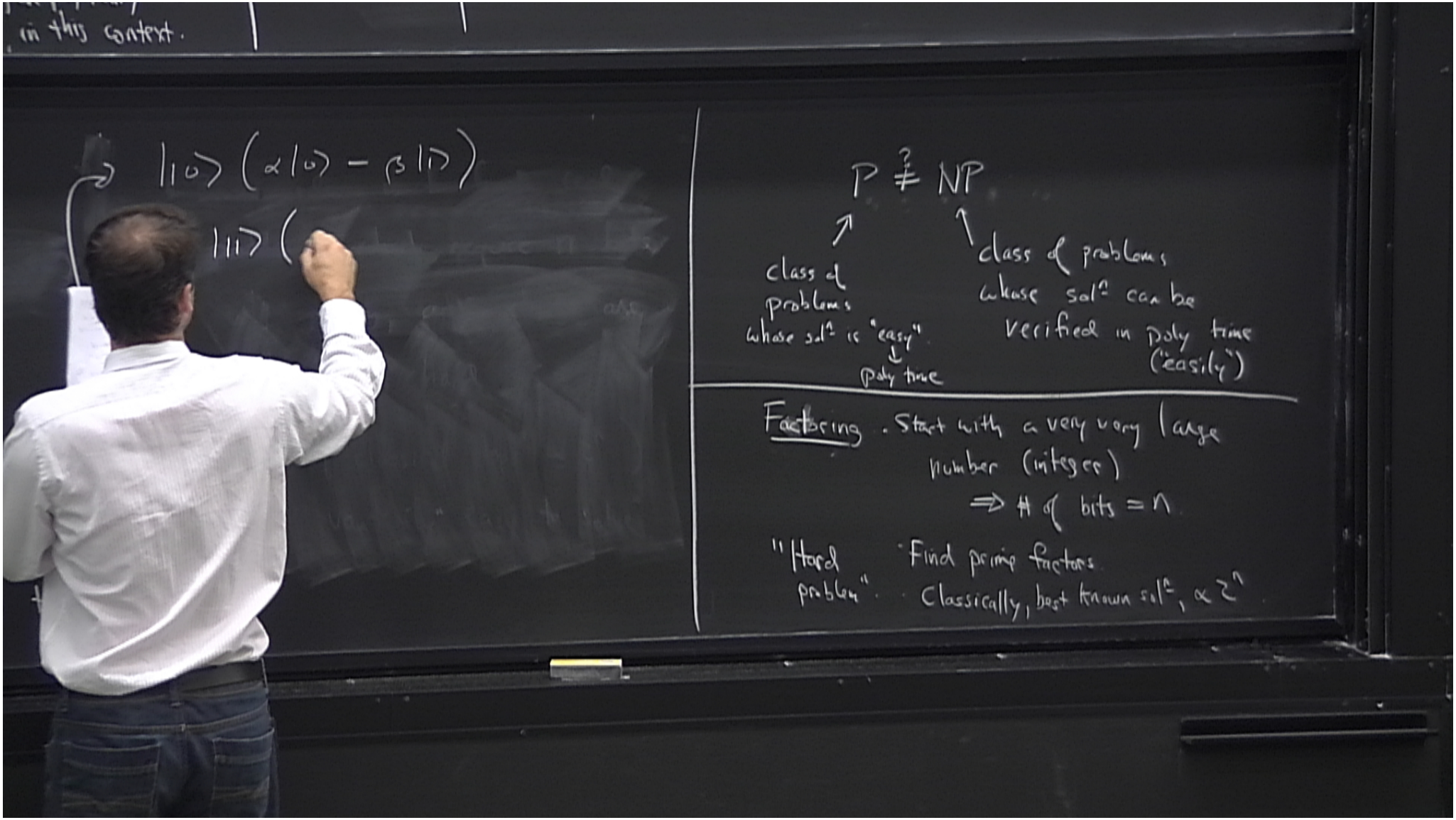

in this context.
$|\psi\rangle = |+\rangle\,|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle$

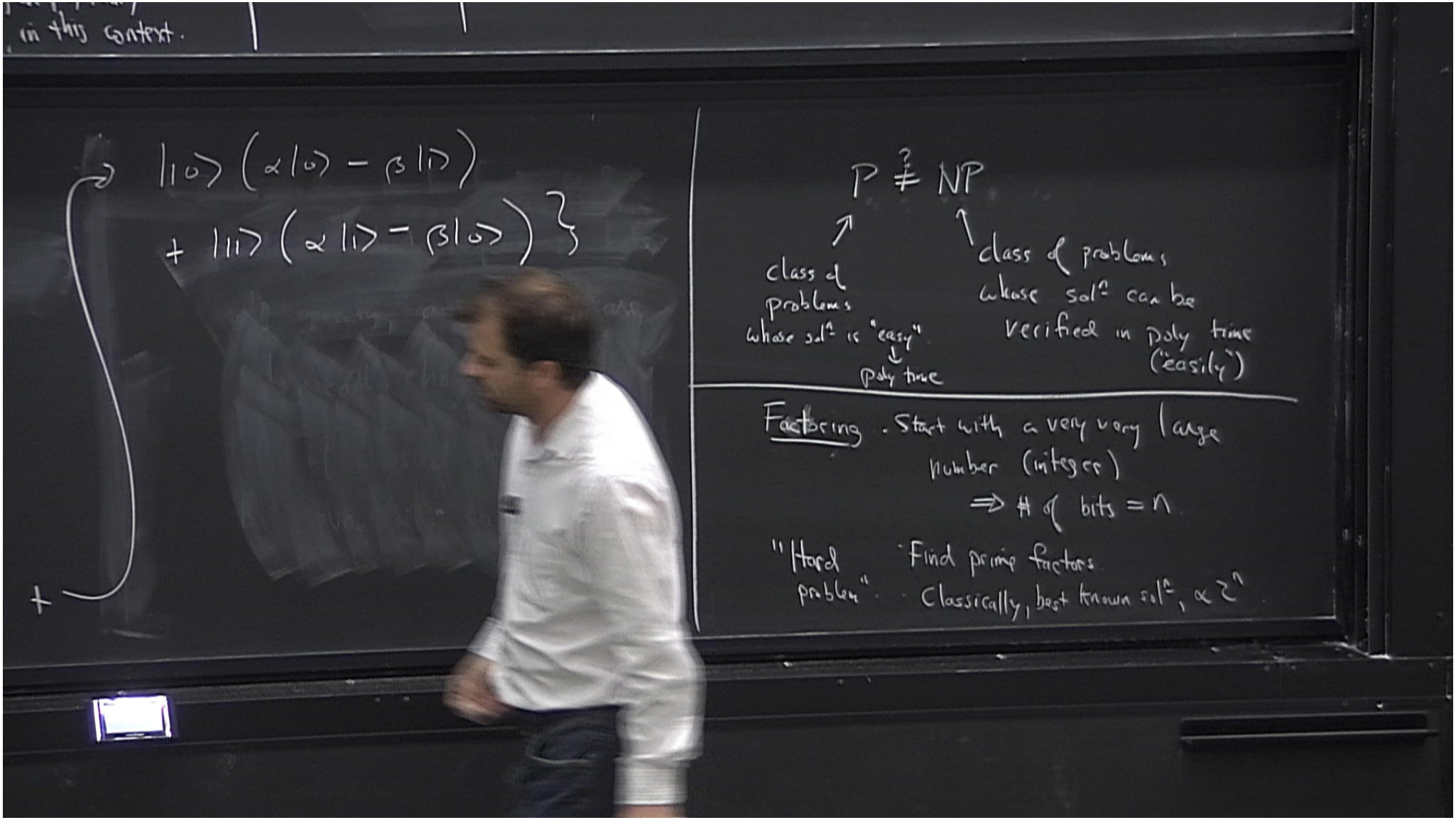

in this context.
$|\chi\rangle = |+\rangle|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{$
$|0\rangle + |1\rangle)$
$|1\rangle(|0\rangle + |1\rangle)\}$

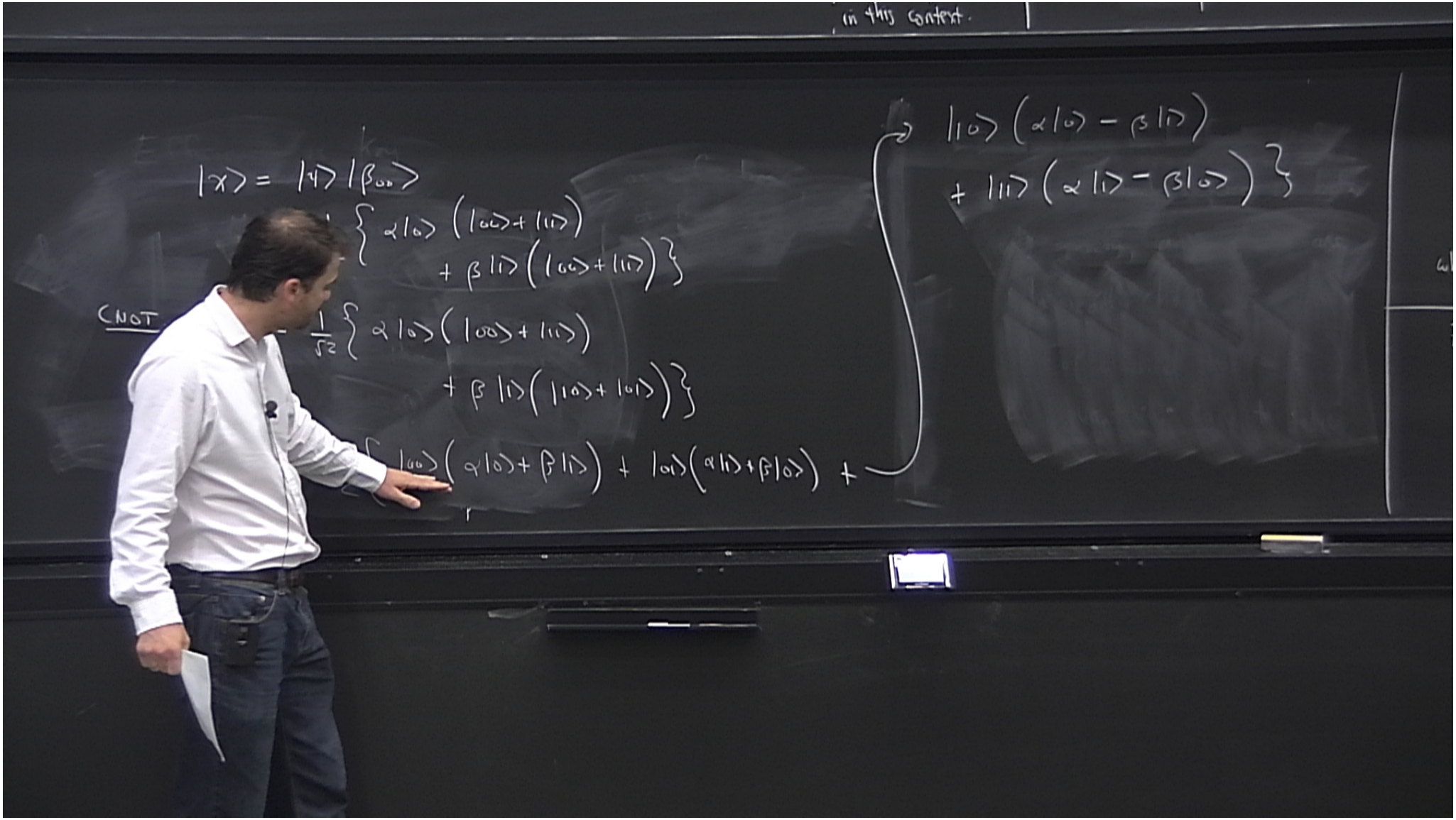

in this context.
$|\chi\rangle = |+\rangle|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)\}$
$\rightarrow = \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\}$
$\rightarrow =$


in this context.
$|\chi\rangle = |+\rangle|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)\}$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\}$

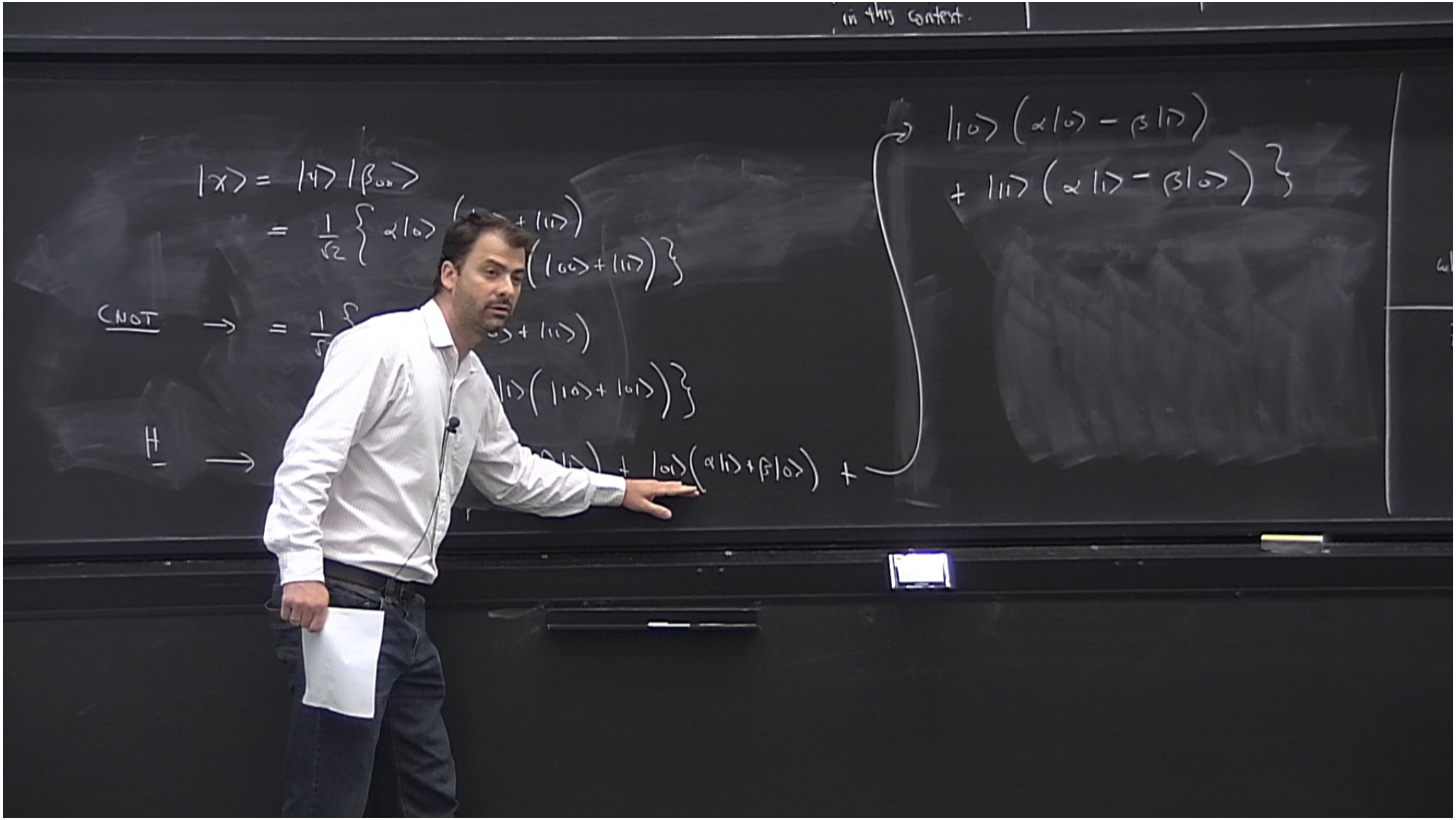

in this context.
$|x\rangle = |+\rangle|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle + |11\rangle)$
$+ \beta$ $\rangle + |11\rangle)\}$
CNOT $\rightarrow$ $= \frac{1}{\sqrt{2}}\{$ $|11\rangle)$
$|01\rangle)\}$
H $\rightarrow$ $=$

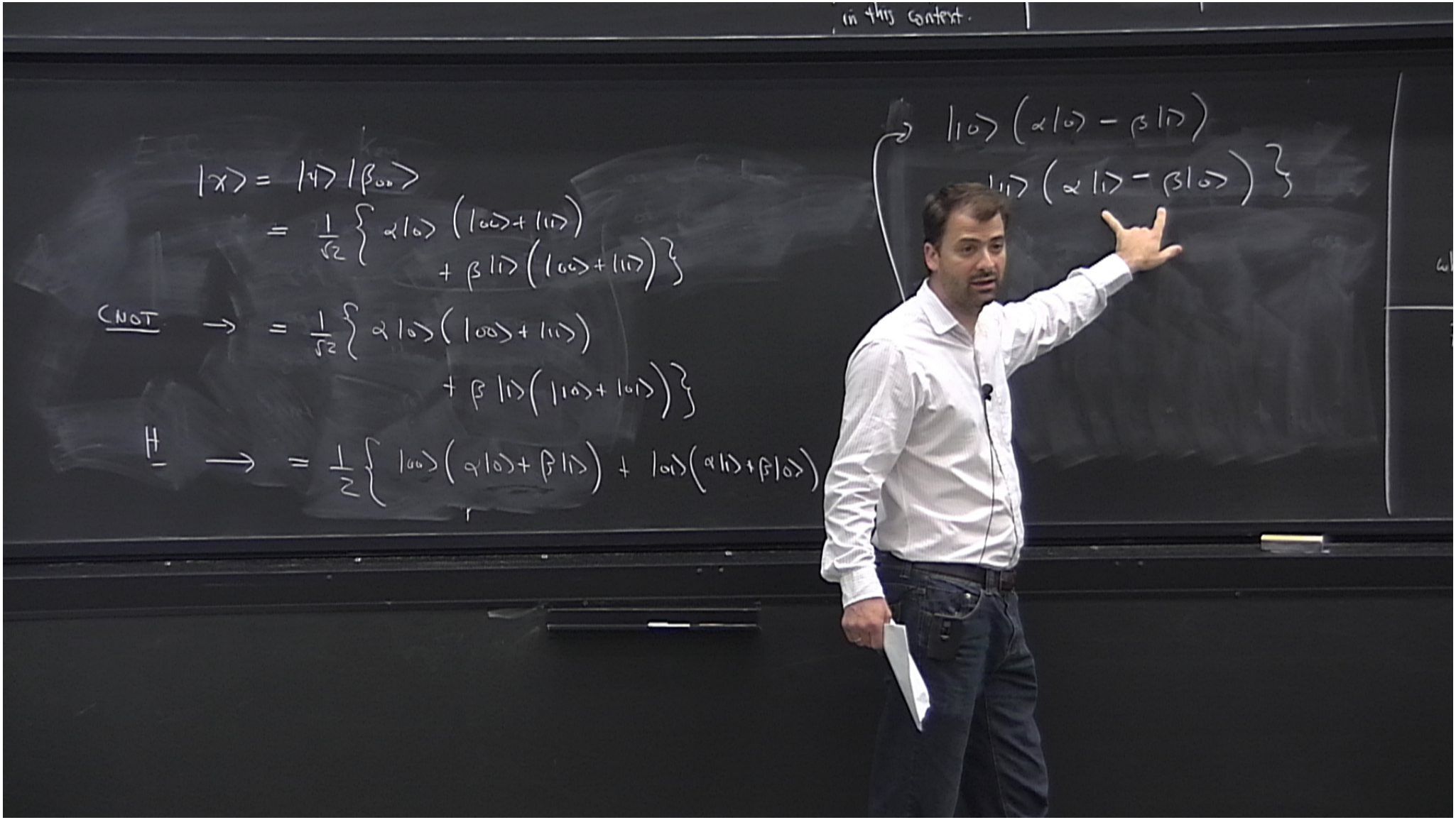

in this context.
$|1\rangle(\alpha|0\rangle - \beta|1\rangle)$
$|1\rangle($
$P \stackrel{?}{\neq} NP$
Class of problems whose sol^n is "easy"
poly time
Class of problems whose sol^n can be verified in poly time ("easily")
Factoring . Start with a very very large number (integer)
$\Rightarrow$ # of bits $= n$
"Hard problem"
. Find prime factors.
. Classically, best known sol^n, $\propto 2^n$


in this context.
$|1\rangle(\alpha|0\rangle - \beta|1\rangle)$
$+ |1\rangle(\alpha|1\rangle - \beta|0\rangle)\}$
$P \stackrel{?}{\neq} NP$
Class of problems whose sol^n is "easy"
poly time
Class of problems whose sol^n can be verified in poly time ("easily")
Factoring . Start with a very very large number (integer)
$\Rightarrow$ # of bits $= n$
"Hard problem"
Find prime factors.
Classically, best known sol^n, $\propto 2^n$


in this context.
$|\chi\rangle = |+\rangle|\beta_{00}\rangle$
$\frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)\}$
CNOT
$\frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\}$
$|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) +$
$|10\rangle(\alpha|0\rangle-\beta|1\rangle)$
$+ |11\rangle(\alpha|1\rangle-\beta|0\rangle)\}$


in this context.
$|x\rangle = |+\rangle|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\}$
CNOT $\rightarrow$ $= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\}$
H $\rightarrow$ $= \frac{1}{2}\{|0\rangle(\alpha|0\rangle+\beta|1\rangle) + |1\rangle(\alpha|1\rangle+\beta|0\rangle) + |0\rangle(\alpha|0\rangle-\beta|1\rangle) + |1\rangle(\alpha|1\rangle-\beta|0\rangle)\}$


in this context.
$|x\rangle = |+\rangle|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle)$
$(|00\rangle+|11\rangle)\}$
CNOT $\rightarrow$ $= \frac{1}{\sqrt{2}}\{$
$+|11\rangle)$
$|1\rangle(|10\rangle+|01\rangle)\}$
H $\rightarrow$
$+|0\rangle(\alpha|1\rangle+\beta|0\rangle)+$
$|1\rangle(\alpha|0\rangle-\beta|1\rangle)$
$+|1\rangle(\alpha|1\rangle-\beta|0\rangle)\}$


in this context.
$|\psi\rangle = |+\rangle|\beta_{00}\rangle$
$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)\}$
CNOT $\rightarrow = \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\}$
H $\rightarrow = \frac{1}{2}\{|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle)$
$|10\rangle(\alpha|0\rangle-\beta|1\rangle)$
$|11\rangle(\alpha|1\rangle-\beta|0\rangle)\}$

in this context.

$$|\chi\rangle = |\psi\rangle|\beta_{00}\rangle$$

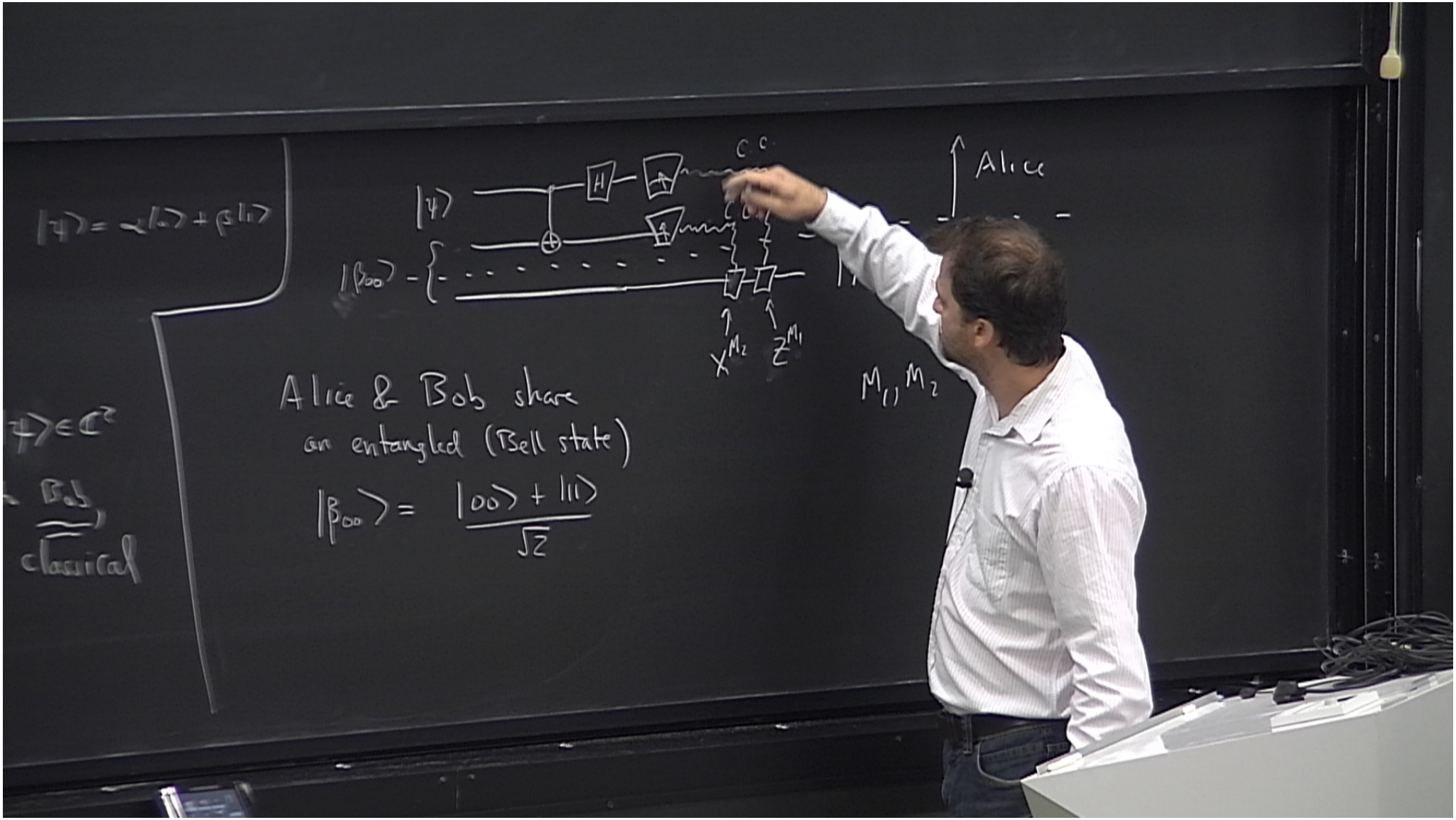
$$= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)\}$$

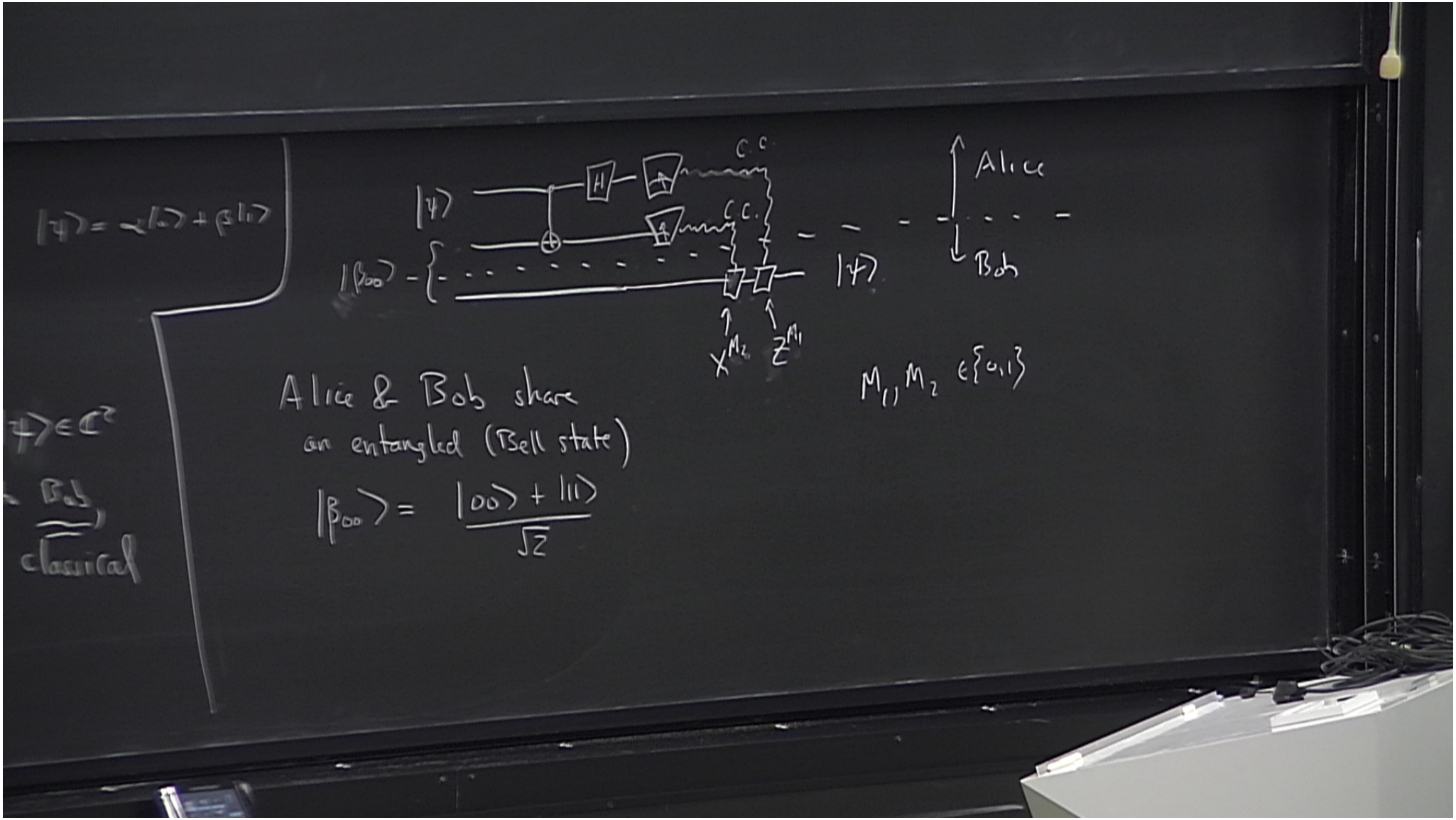
CNOT $\rightarrow$ $= \frac{1}{\sqrt{2}}\{\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\}$

$H_1 \rightarrow$ $= \frac{1}{2}\{|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) +$

$|10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\}$


Alice & Bob share
an entangled (Bell state)
$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
Alice
X^{M_2}
Z^{M_1}
$M_1, M_2 \in$
classical


Alice
Alice & Bob share
an entangled (Bell state)
$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
M_1, M_2
classical


Alice
Bob
Alice & Bob share
an entangled (Bell state)
$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
$M_1, M_2 \in \{0,1\}$
classical

in this context.

$|1\rangle(\alpha|0\rangle - \beta|1\rangle)$

$+ |1\rangle(\alpha|1\rangle - \beta|0\rangle)\}$

$\Rightarrow$ Hence 1 EPR pair & 2 bits of c.c. $\equiv$ 1 qubit of communication

$P \stackrel{?}{\neq} NP$

Class of problems whose sol^n is "easy" (poly time)

Class of problems whose sol^n can be verified in poly time ("easily")

Factoring. Start with a very very large number (integer) $\Rightarrow$ # of bits $= n$

"Hard problem". Find prime factors. Classically, best known sol^n, $\propto 2^n$

in this context.

$|1\rangle(\alpha|0\rangle - \beta|1\rangle)$

$+ |1\rangle(\alpha|1\rangle - \beta|0\rangle)\}$

$\Rightarrow$ Hence 1 EPR pair & 2 bits of cc.

$\equiv$ 1 qubit of communication

$P \overset{?}{\neq} NP$

Class of problems whose sol^n is "easy" (poly time)

Class of problems whose sol^n can be verified in poly time ("easily")

Factoring. Start with a very very large number (integer)

$\Rightarrow$ # of bits $= n$

"Hard problem"

Find prime factors.

Classically, best known sol^n, $\propto 2^n$