Title: A Device Independent Protocol for a Private Randomness Expansion

Date: Aug 10, 2011 01:00 PM

URL: http://pirsa.org/11080074

Abstract:

P_{AB} $(a,b) \to (x,y)$ $\}$ $P_{XY|AB}$

$E: z, p^z$ $\hookrightarrow = \sum p^z P^z_{XY|AB}$ ⇐ quantum.

induced behavior

$$P_{guess} = \sum_z p^z \max_{(x,y)} P^z_{XY|A=a,B=b}$$

ρ, E

$\} \to (x,y) \} P_{xy1AB}$

$\hookrightarrow = \sum_z p^z P^z_{xy1AB}$ ⟸ quantum. $\rho, \{M_a^x, M_b^y\}$

$P^z_{xy1AB} = \mathrm{tr}(M_a^x \otimes M_b^y \rho)$

induced behavior

$\sum_z p^z \max_{(x,y)} P^z_{xy1A=a,B=b}$ ρ, E

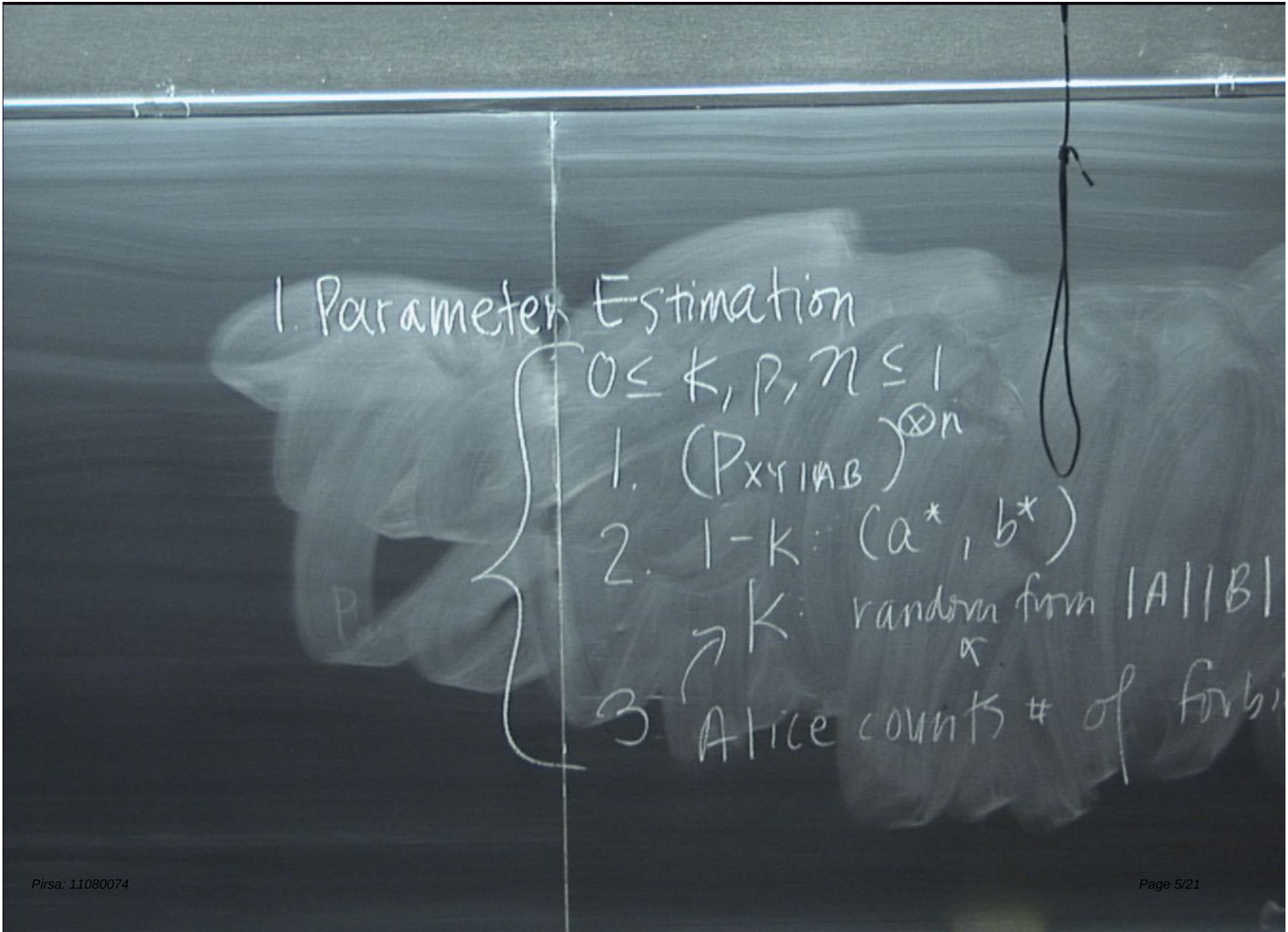
SDP: first level

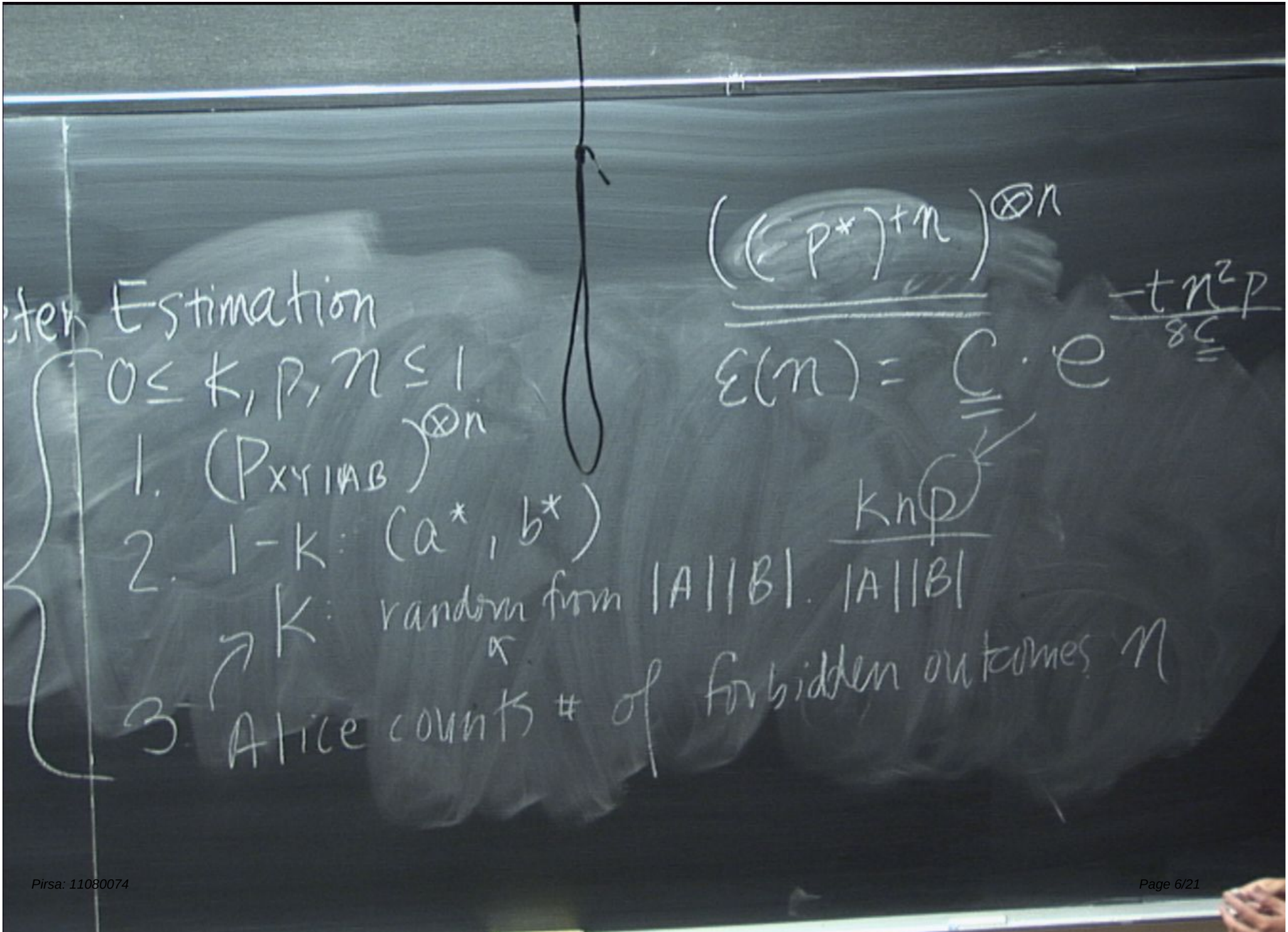
$\begin{pmatrix} Q & P \\ P^\dagger & R \end{pmatrix} \geq 0$

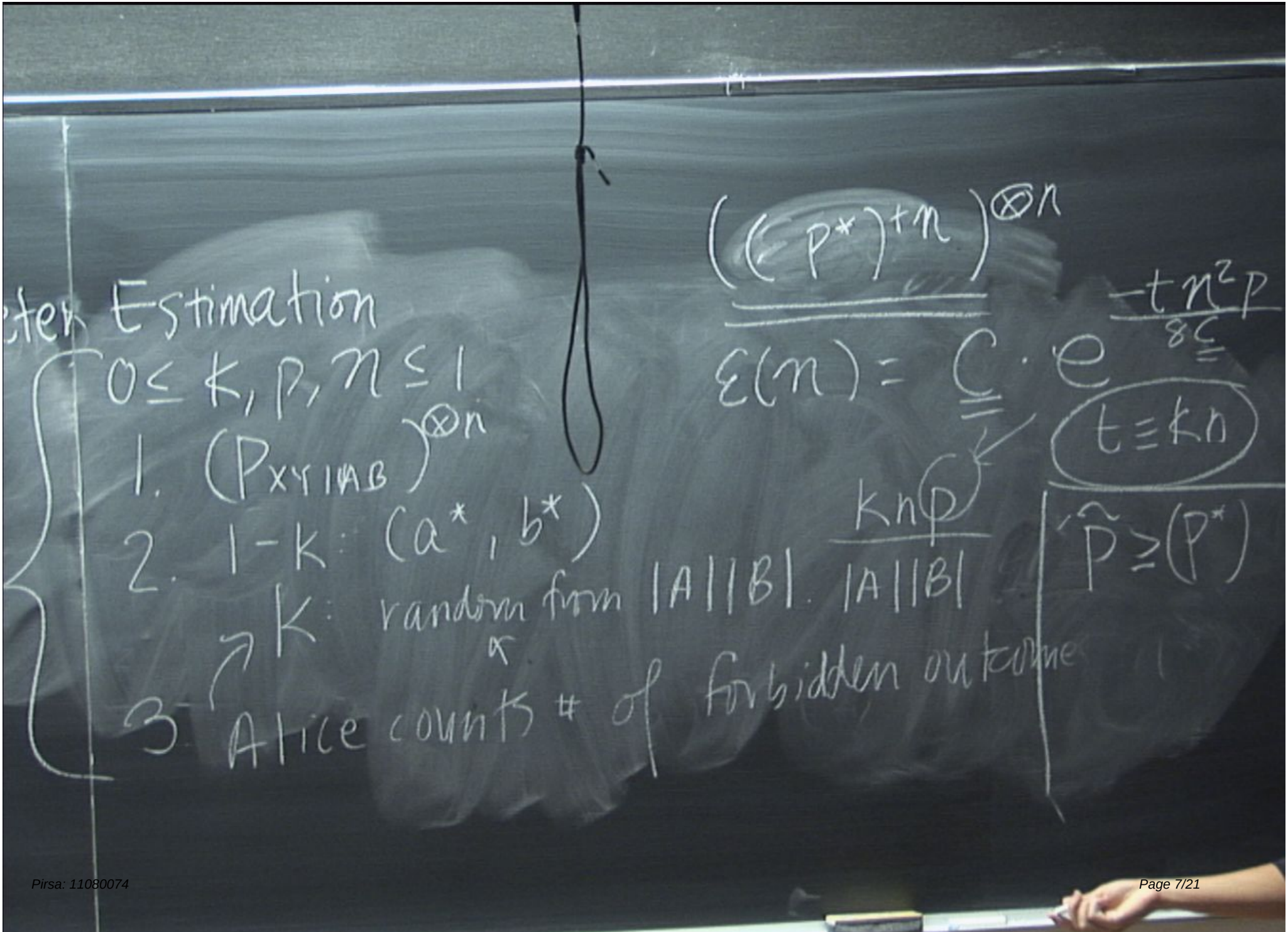
$$\left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right]^{\otimes 2}$$

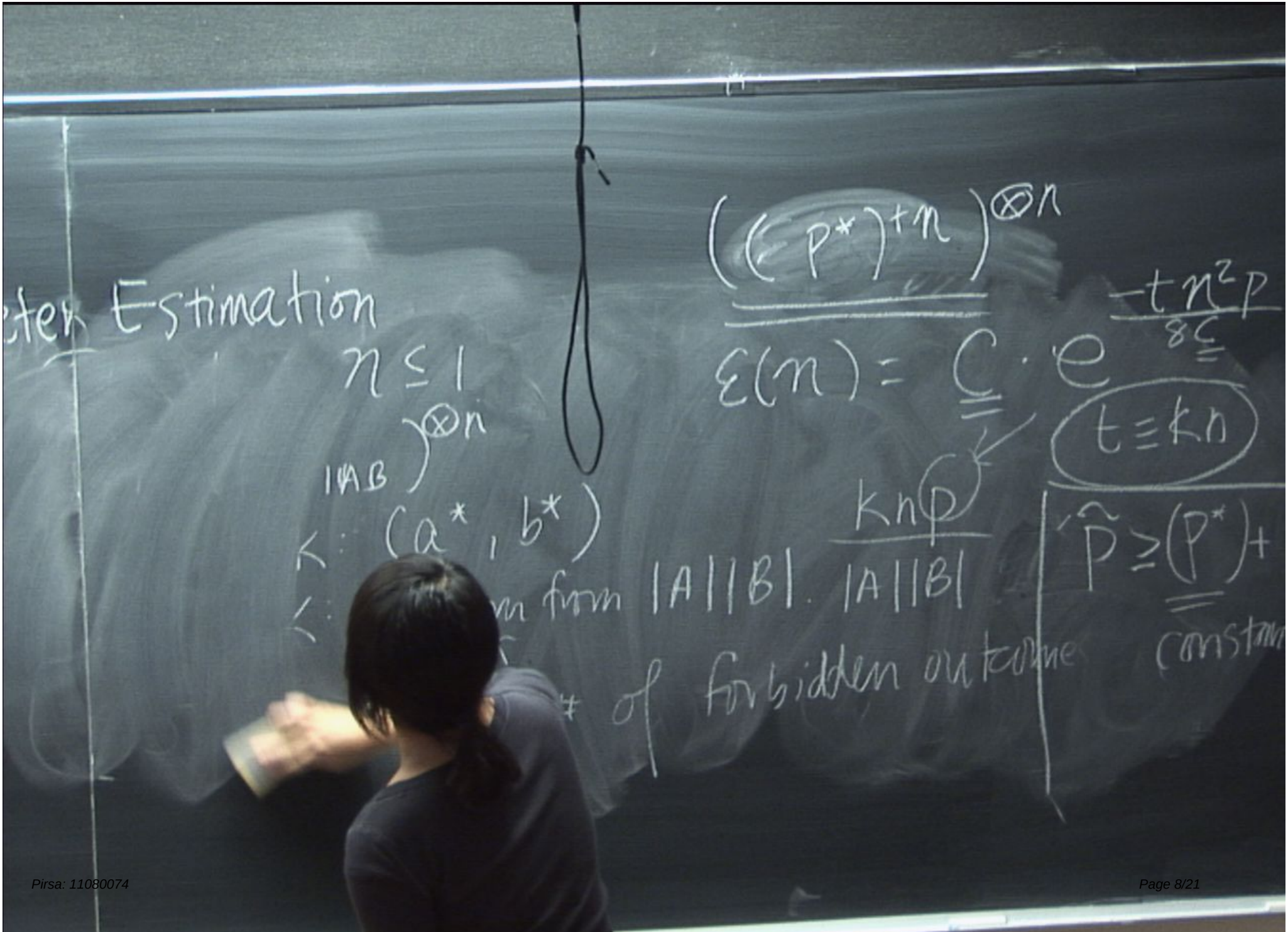
grid

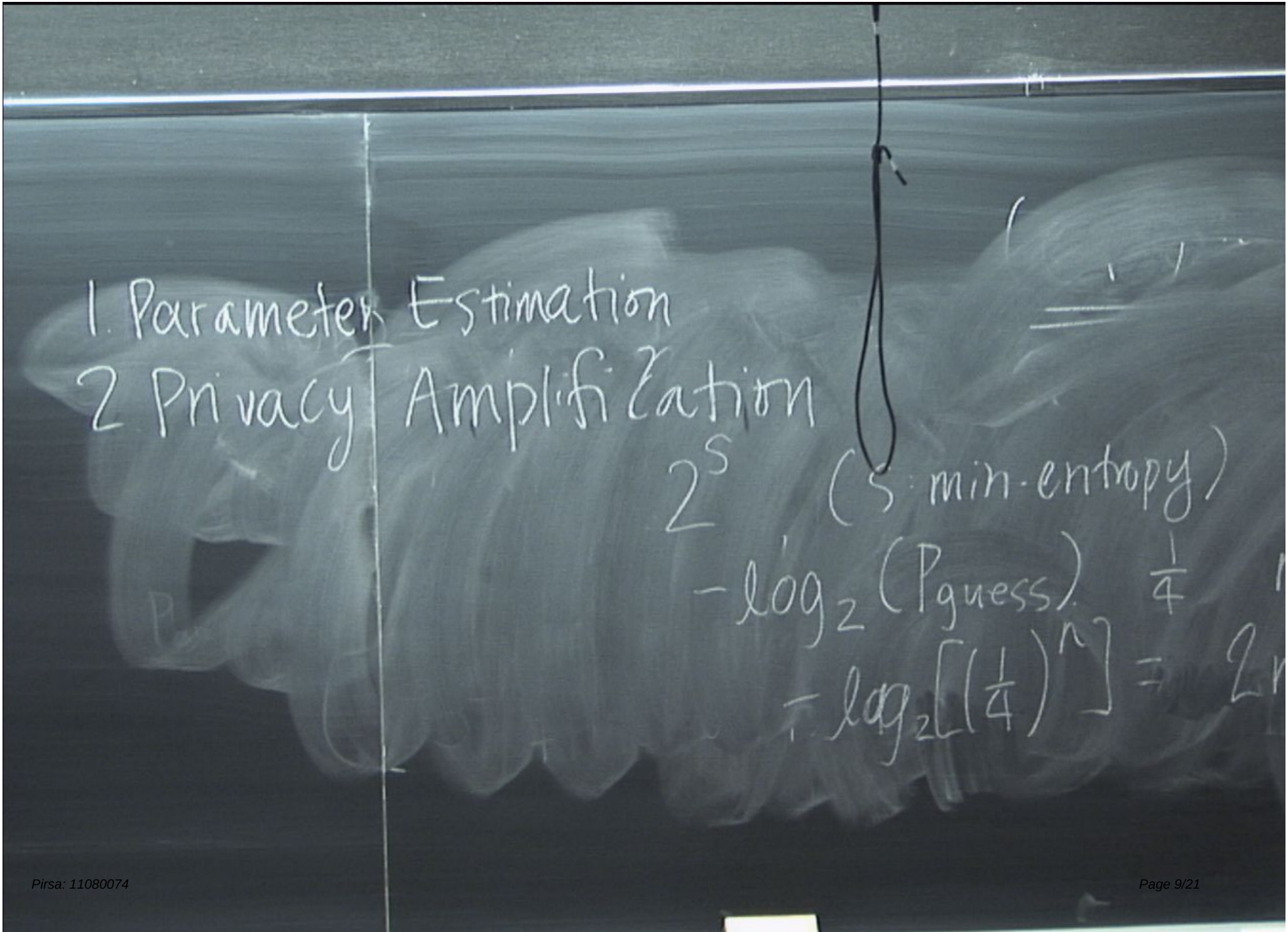
(a,b) $(2,3)$

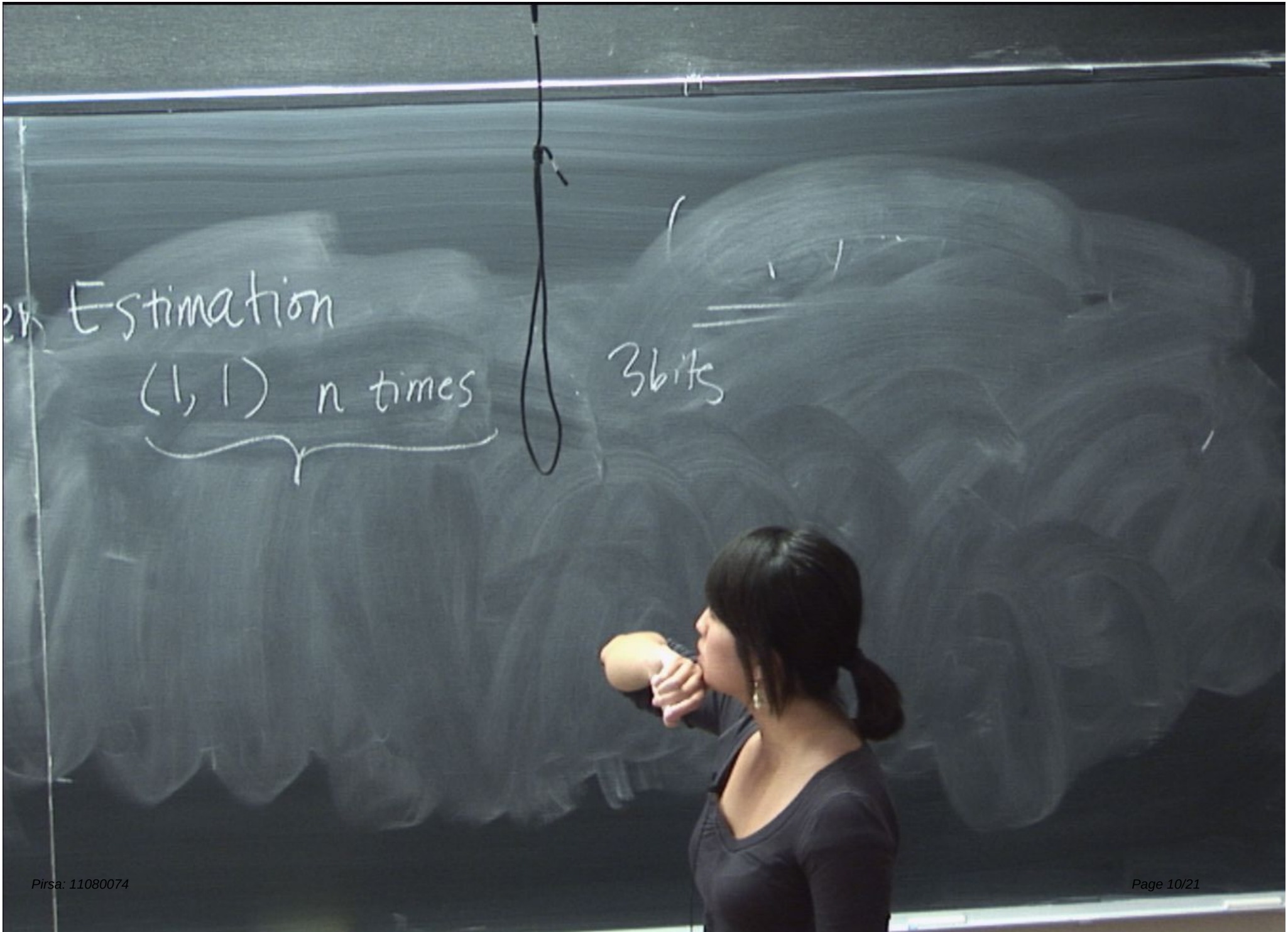

1. Parameter Estimation
$0 \le k, p, \eta \le 1$
1. $(P_{XY|AB})^{\otimes n}$
2. $1-k$: (a^*, b^*)
k: random from $|A||B|$
$\propto$
3. Alice counts # of

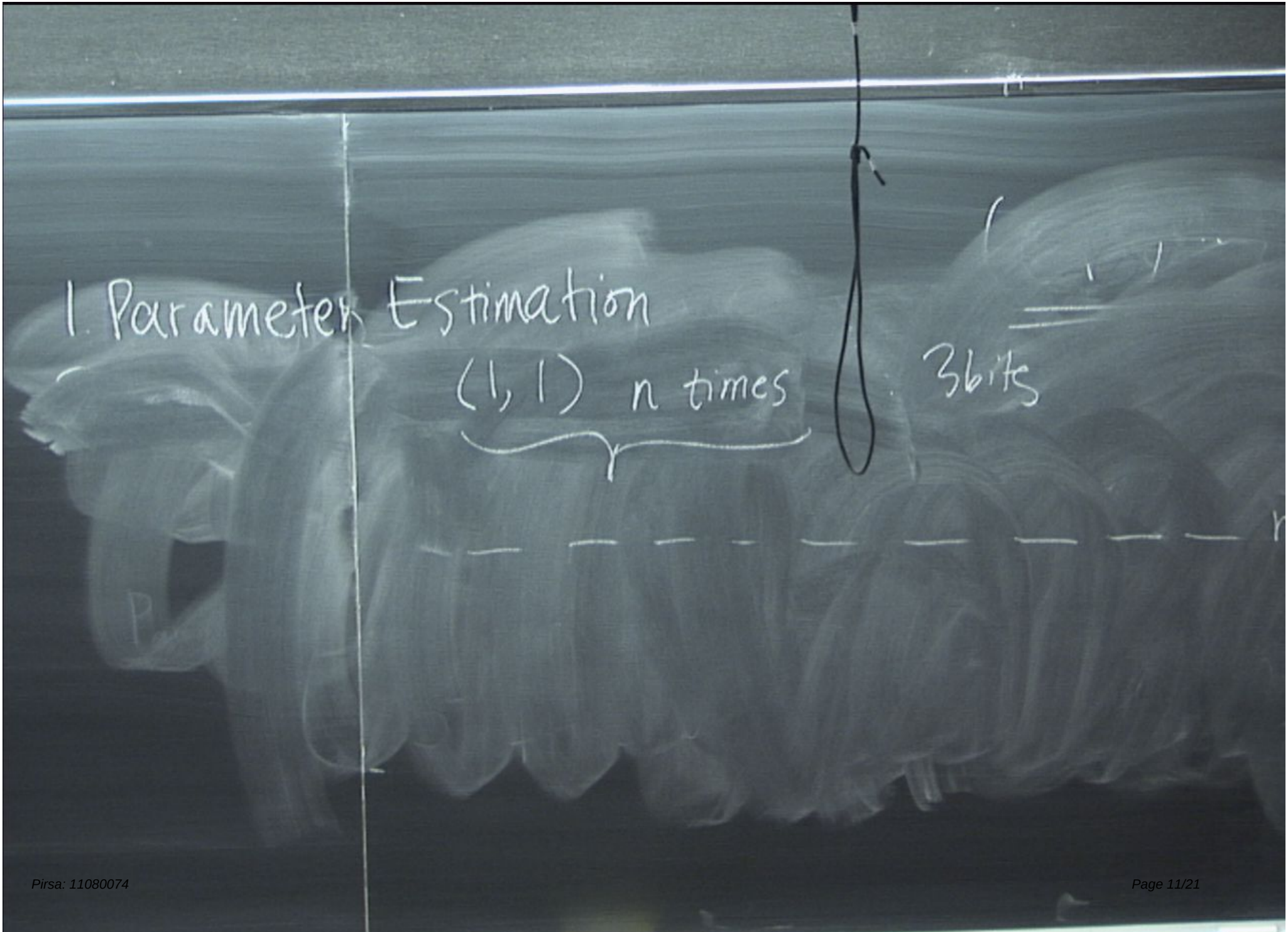

ter Estimation
0 ≤ k, p, η ≤ 1
1. $(P_{XY|AB})^{\otimes n}$
2. 1-k: (a^*, b^*)
k: random from $|A||B|$
3. Alice counts # of forbidden outcomes n
$((\epsilon p^*)+\eta)^{\otimes n}$
$\varepsilon(n) = C \cdot e^{\frac{-t n^2 p}{8 C}}$
$\frac{knp}{|A||B|}$

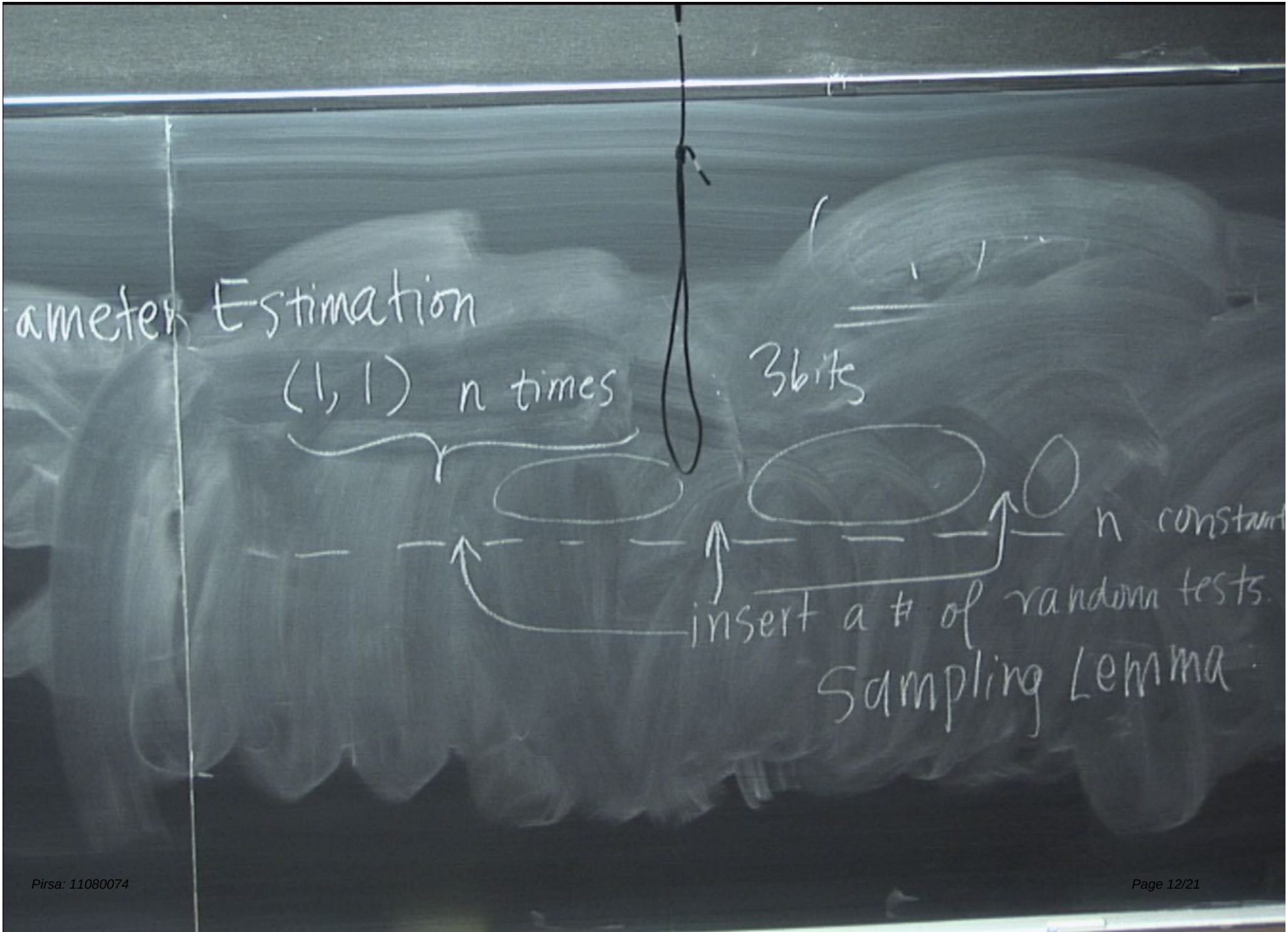

eter Estimation
$0 \le k, p, n \le 1$
1. $(P_{XY|AB})^{\otimes n}$
2. $1-k$: (a^*, b^*)
k: random from $|A||B|$
3. Alice counts # of forbidden outcome
$((\epsilon P^*)+n)^{\otimes n}$
$\varepsilon(n) = C \cdot e^{\frac{-t n^2 p}{8\epsilon}}$
$t \equiv kn$
$\frac{knp}{|A||B|}$
$\frac{}{|A||B|}$
$\hat{P} \ge (P^*)$

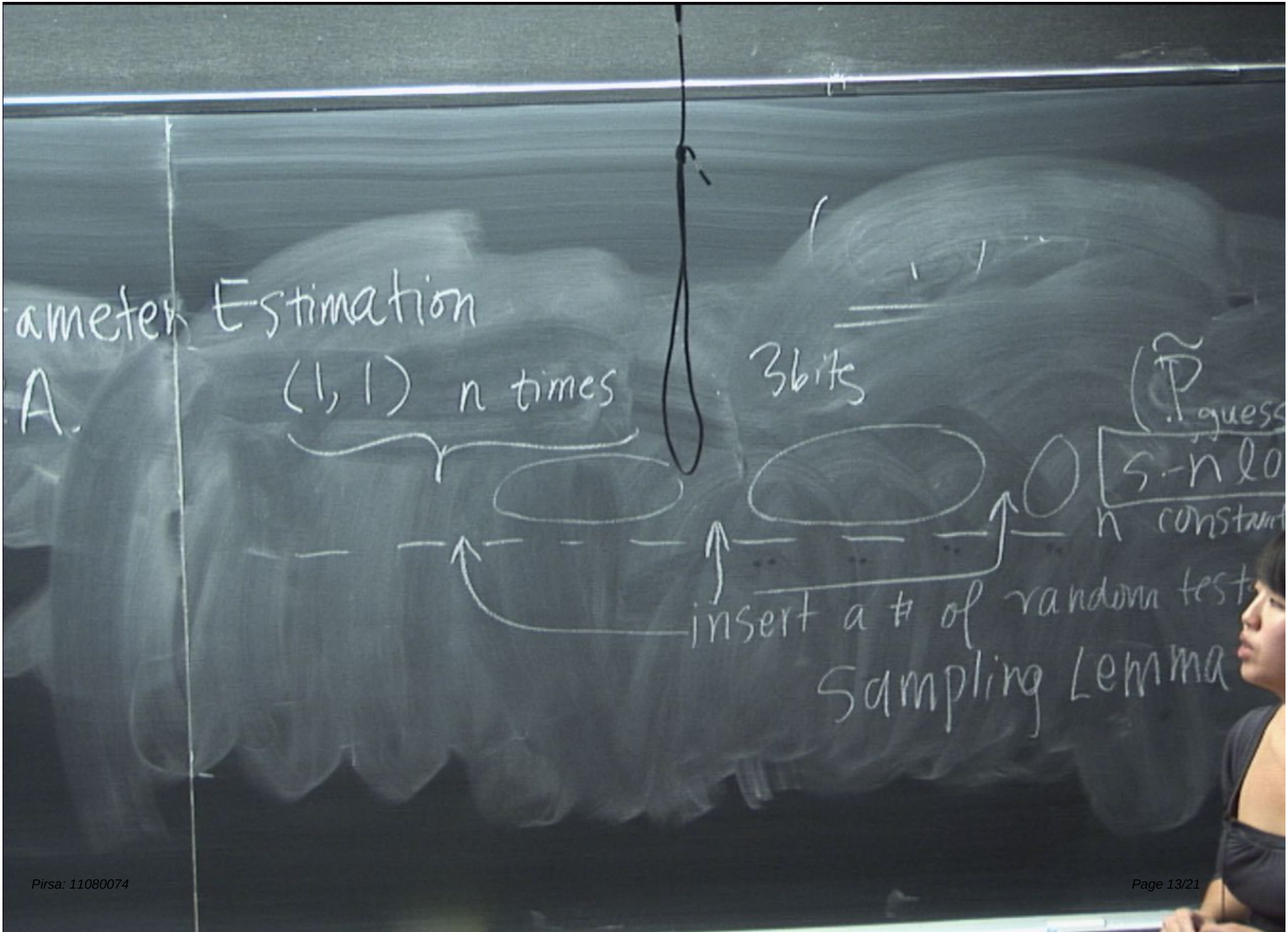

Estimation
$n \leq 1$
$\varepsilon(n) = C \cdot e^{\frac{-t n^2 p}{8C}}$
$t \equiv kn$
$\frac{knp}{|A||B|}$
$\frac{knp}{|A||B|}$
$\hat{p} \geq (p^*) +$
constant
of forbidden outcome

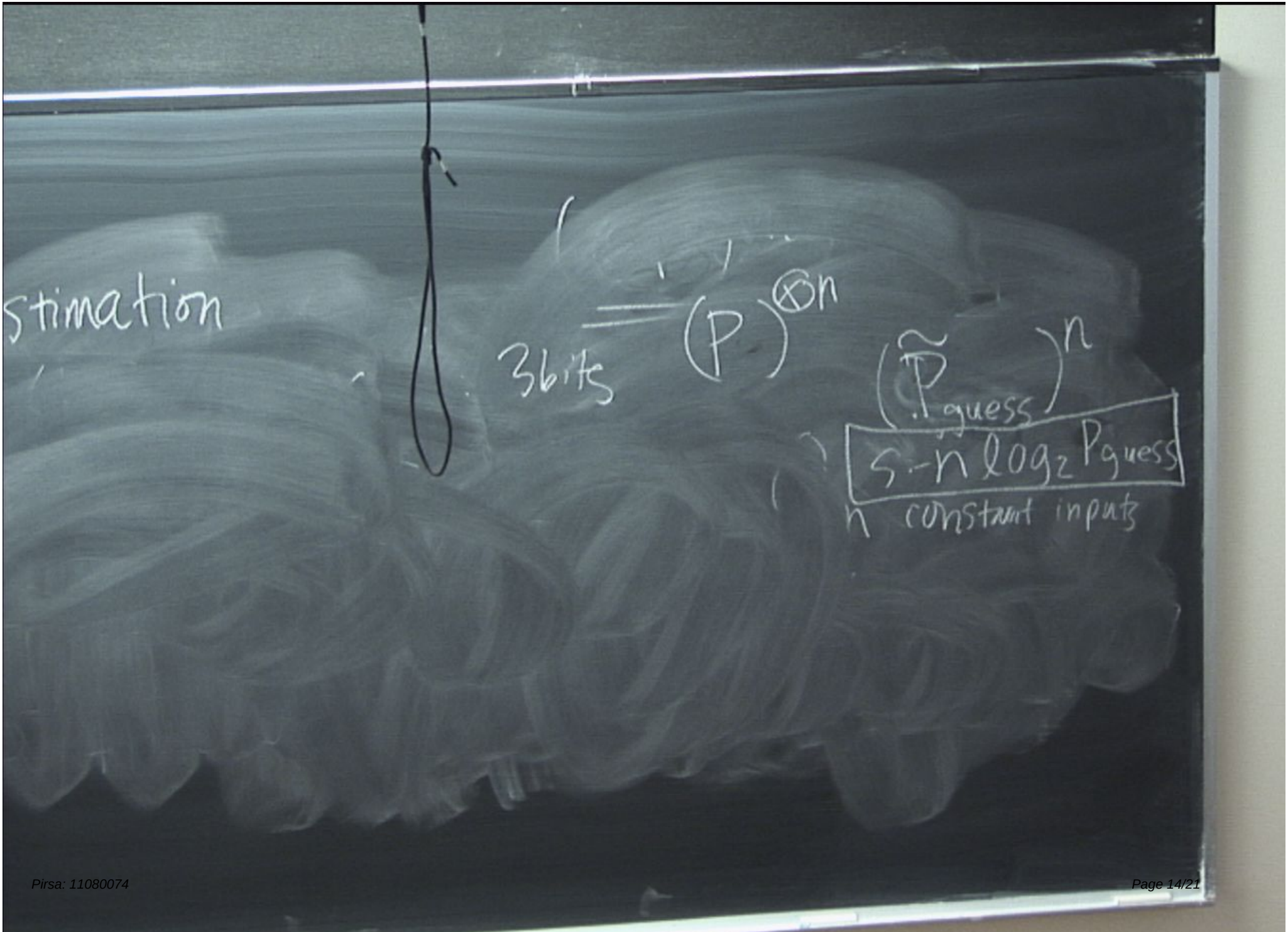

1. Parameter Estimation
2 Privacy Amplification
2^s (s: min-entropy)
$-\log_2(P_{guess})$ $\frac{1}{4}$
$-\log_2[(\frac{1}{4})^n] = 2n$

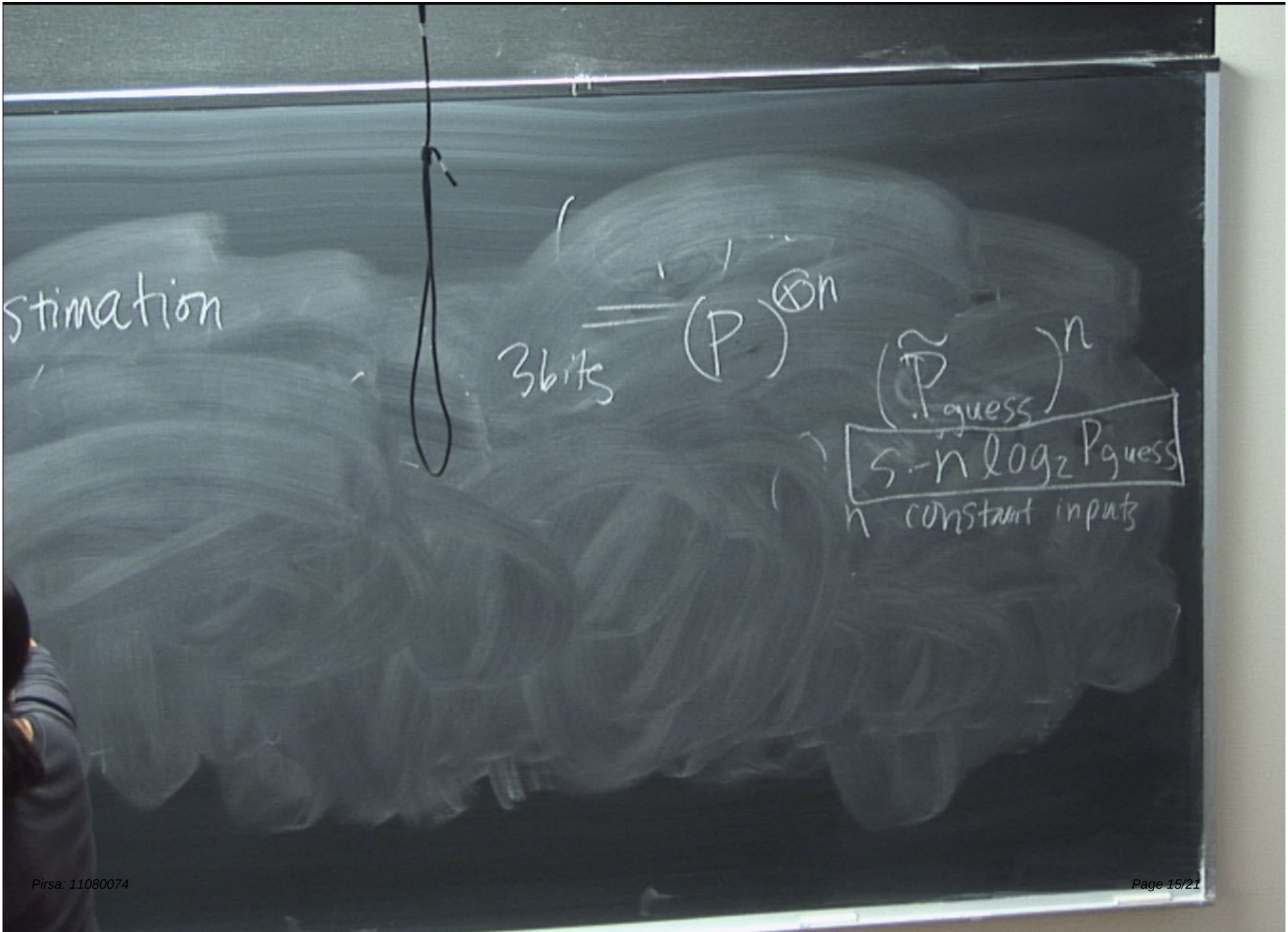

Estimation
(1, 1) n times
36 bits

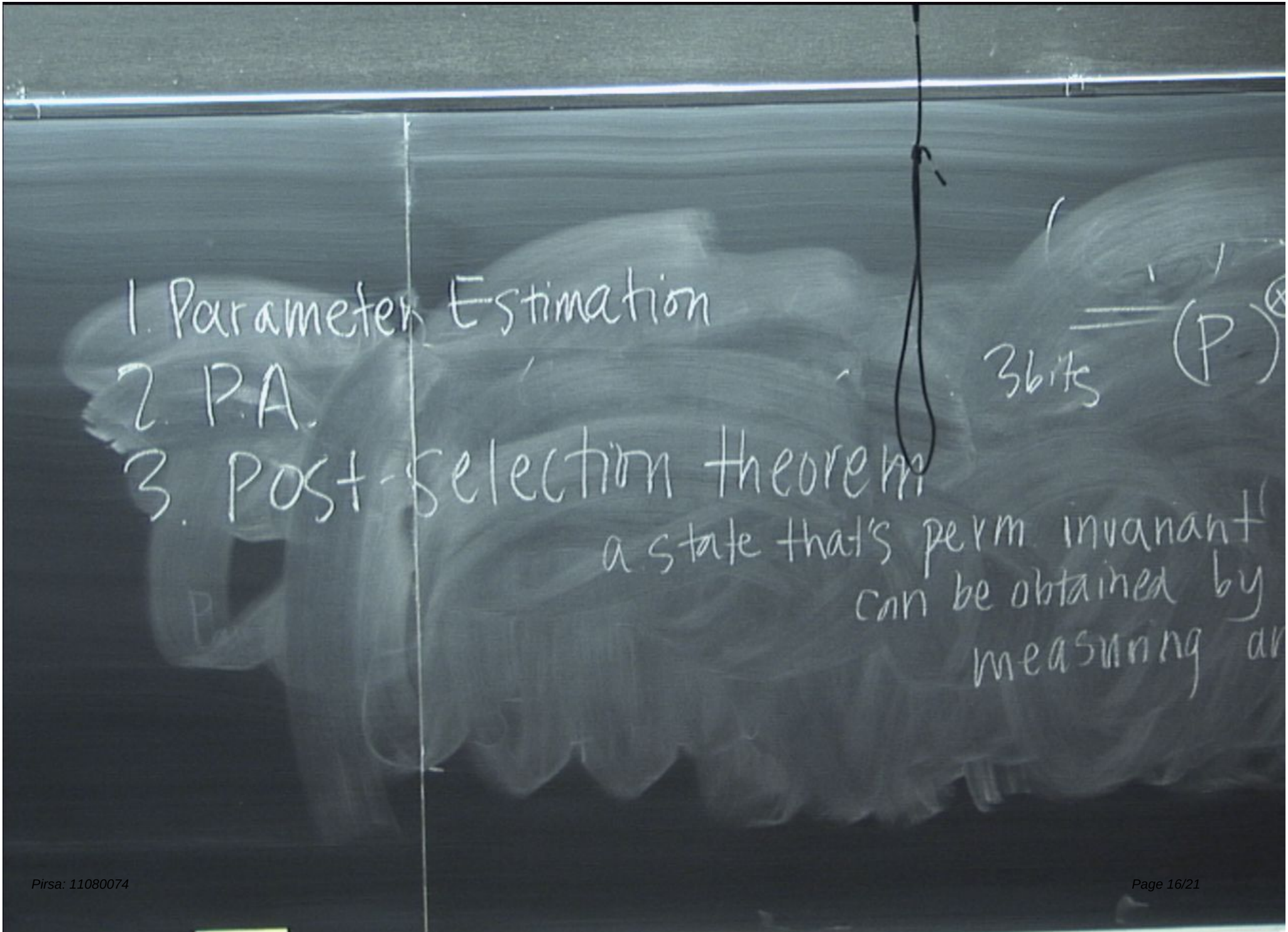

1. Parameter Estimation
(1, 1) n times
36 bits

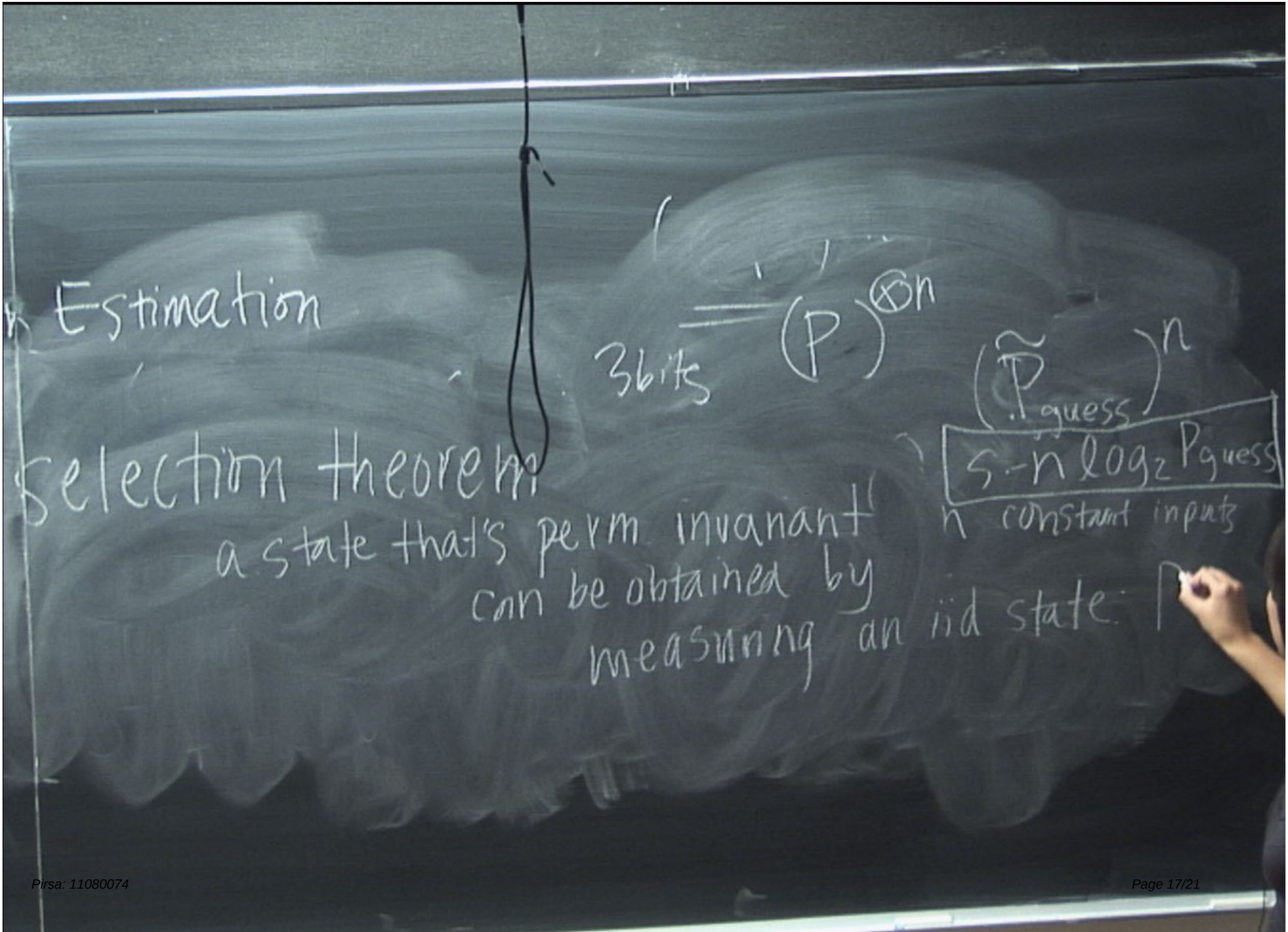

ameter Estimation
(1, 1) n times
3bits
n constant
insert a # of random tests.
Sampling Lemma

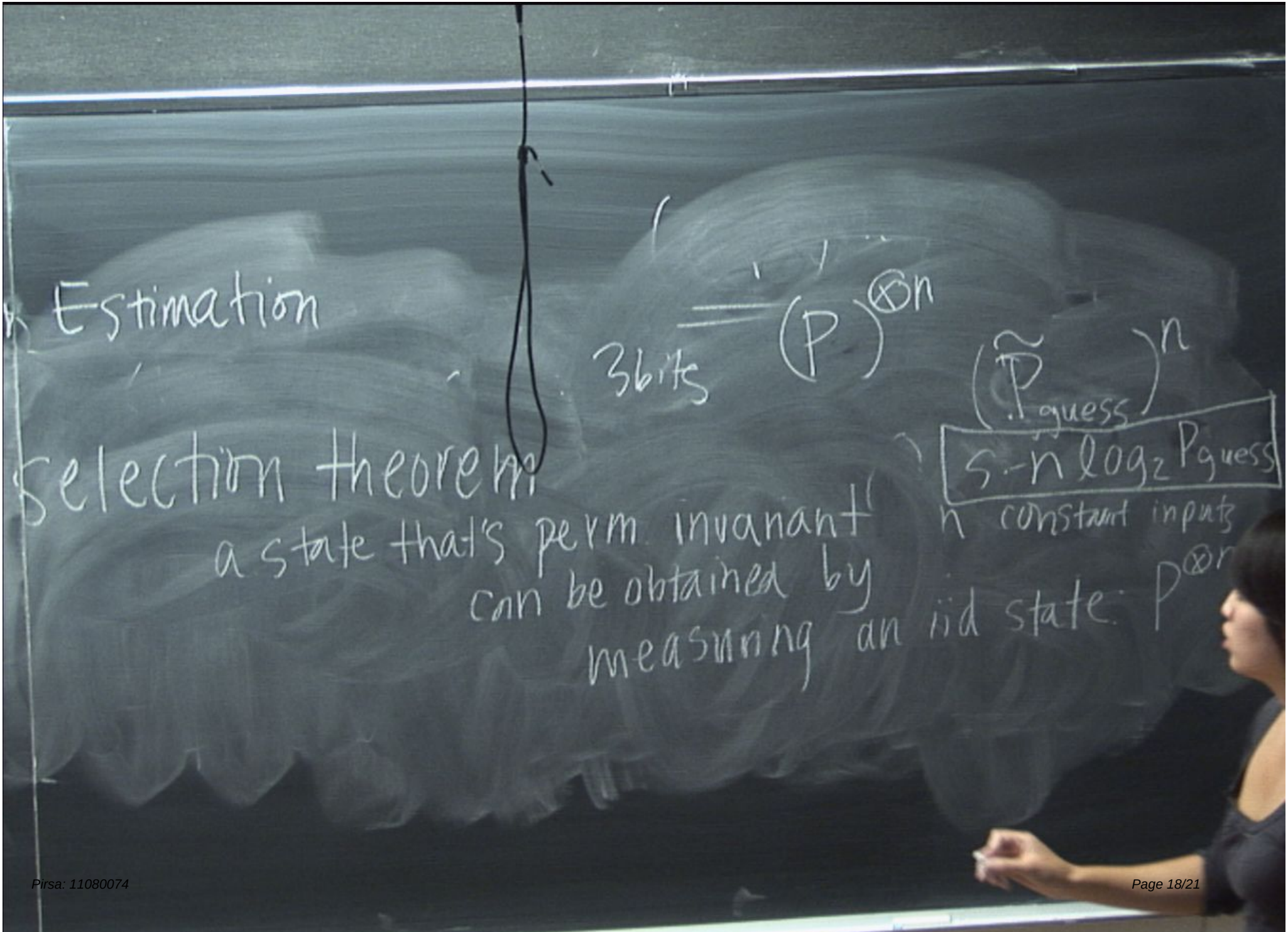

ameter Estimation
A.
(1, 1) n times
3bits
(P̃
guess
s.-n lo
n constant
insert a # of random test
Sampling Lemma

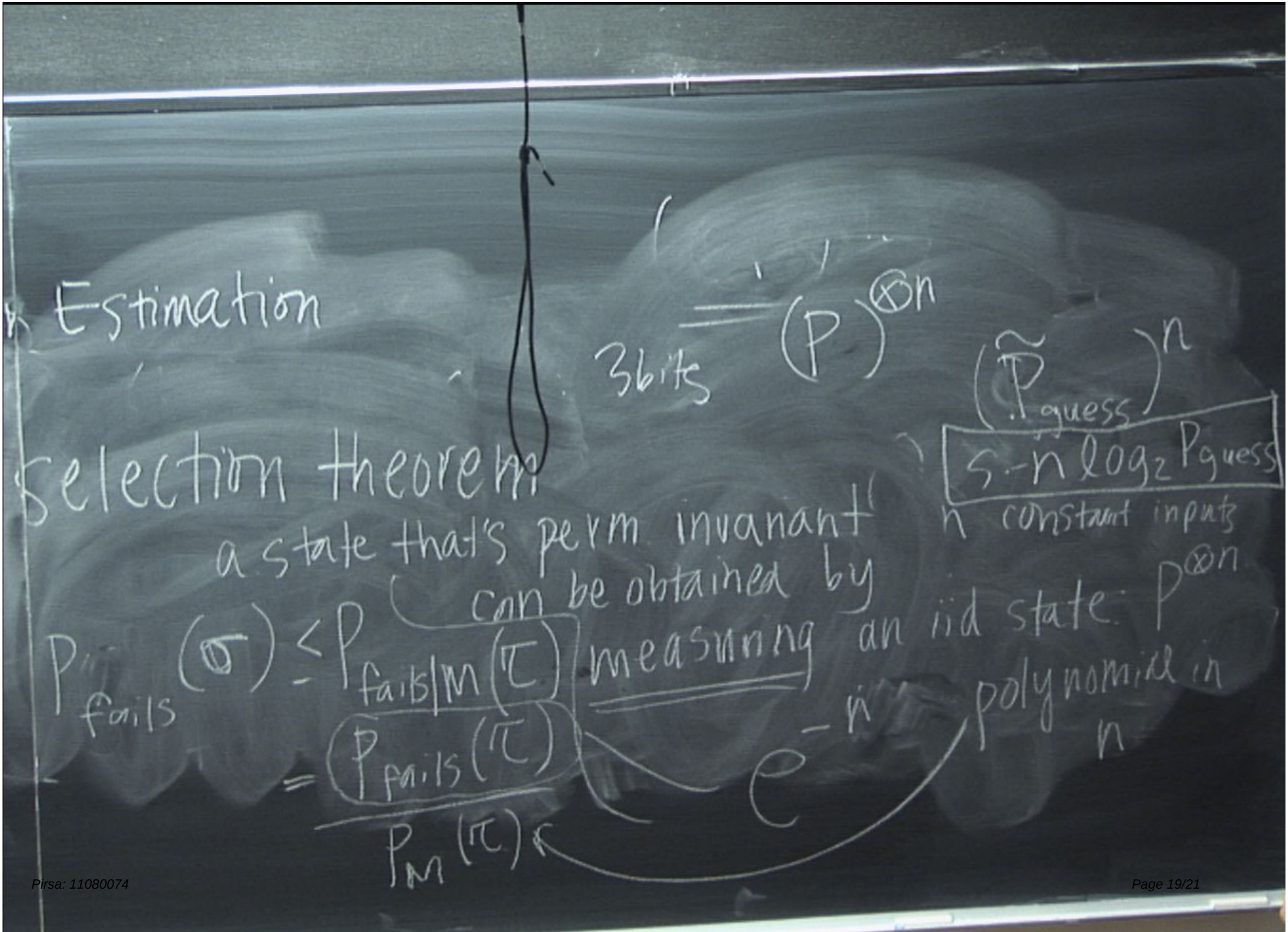

stimation
36 bits
$(P)^{\otimes n}$
$(\tilde{P}_{guess})^n$
$s \sim n \log_2 P_{guess}$
n constant inputs

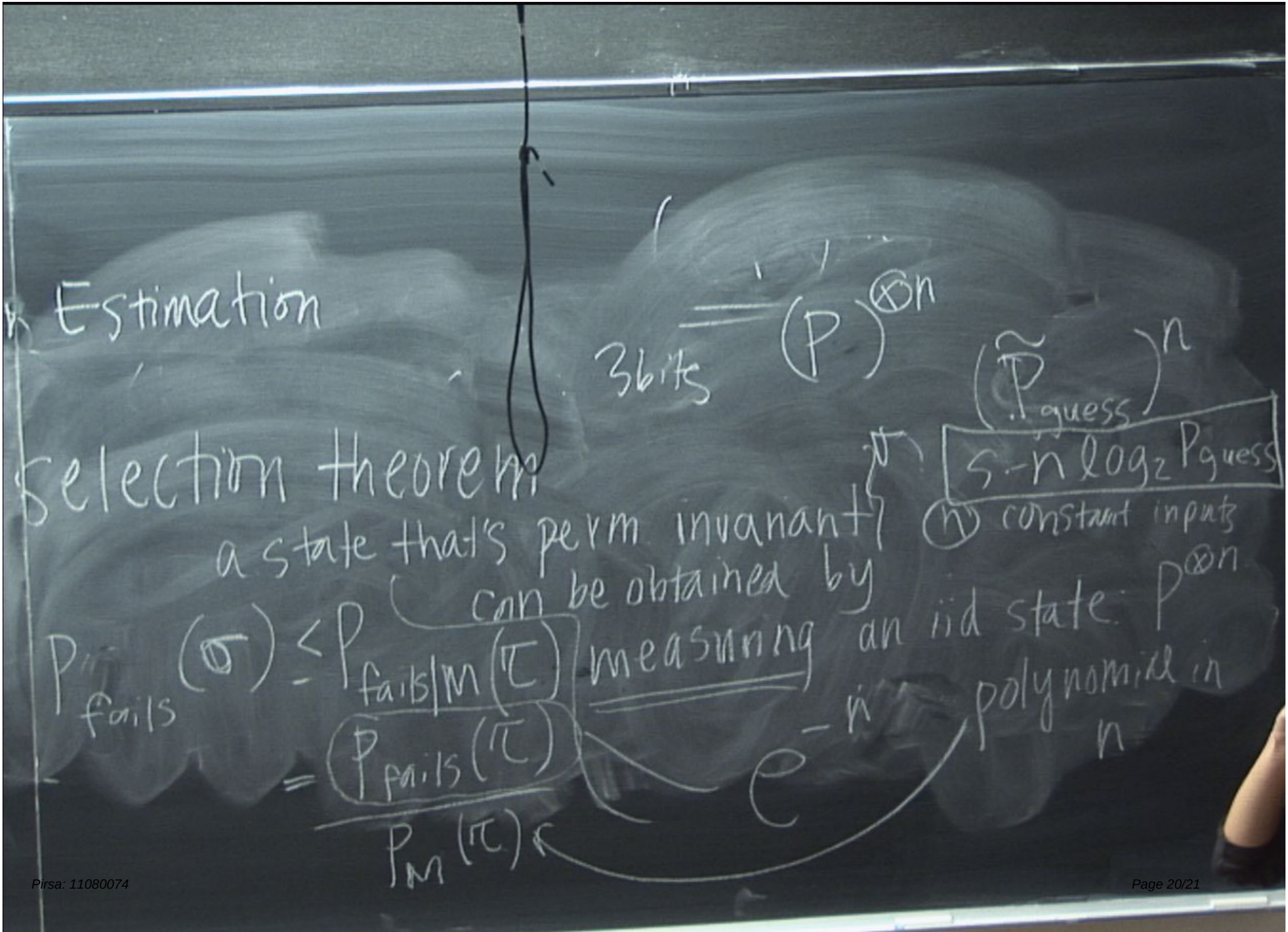

stimation
36 bits
$(P)^{\otimes n}$
$(\tilde{P}_{guess})^n$
$s \cdot -n \log_2 P_{guess}$
n constant inputs

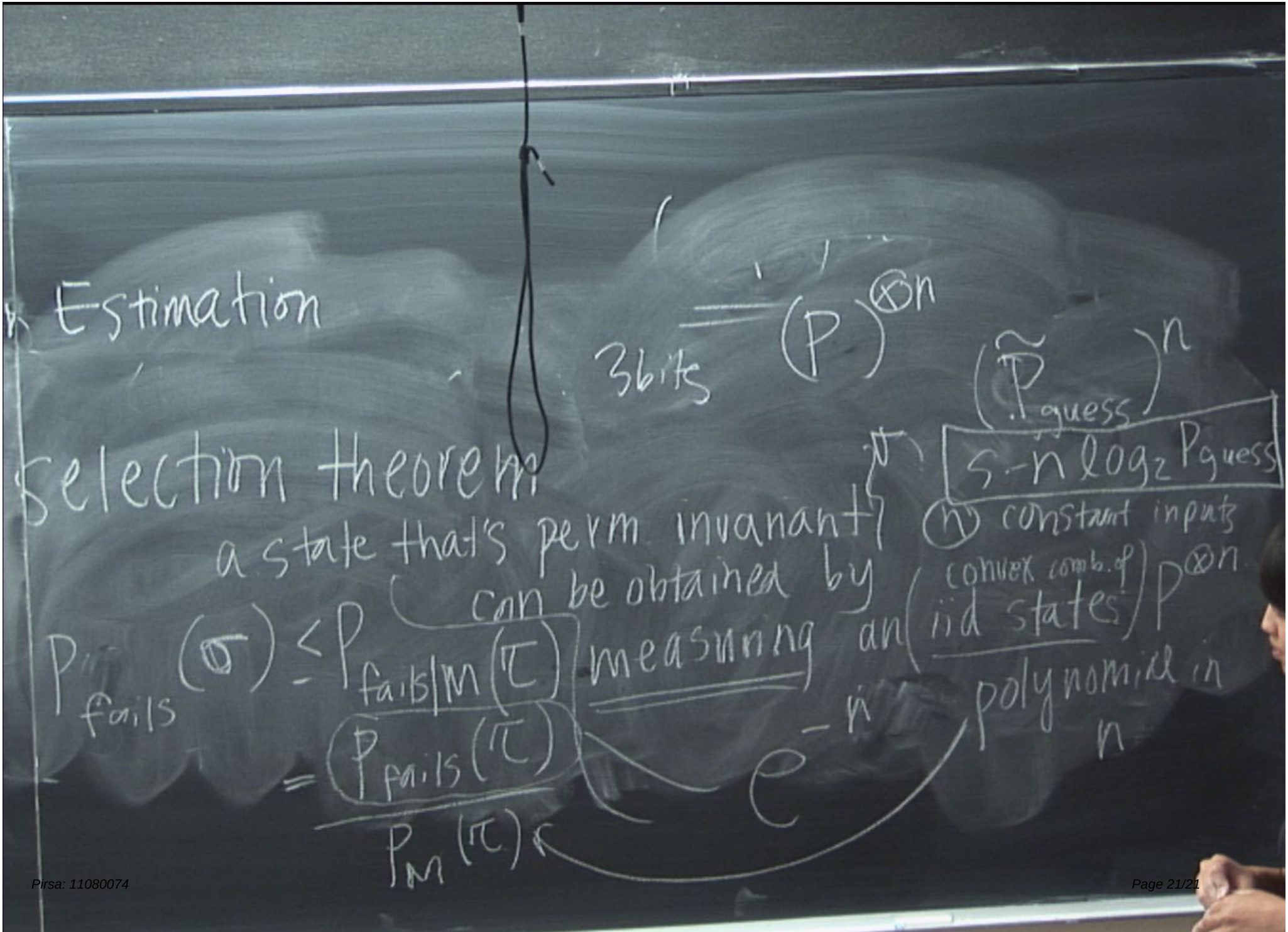

1. Parameter Estimation
2. P.A.
3. Post-selection theorem
36 bits
(P)
a state that's perm invanant
can be obtained by
measuring


Estimation
36 bits
$(P)^{\otimes n}$
$(\tilde{P}_{guess})^n$
$S \sim n \log_2 P_{guess}$
n constant inputs
selection theorem
a state that's perm invariant
can be obtained by
measuring an iid state:


Estimation
36 bits
$(P)^{\otimes n}$
$(\tilde{P}_{guess})^n$
$S \sim n \log_2 P_{guess}$
n constant inputs
selection theorem
a state that's perm invariant
can be obtained by
measuring an iid state: $P^{\otimes n}$


Estimation
36 bits
$(P)^{\otimes n}$
$(\tilde{P}_{guess})^n$
$s \sim n \log_2 P_{guess}$
n constant inputs
selection theorem
a state that's perm invariant
can be obtained by
measuring an iid state: $P^{\otimes n}$
$P_{fails}(\sigma) \leq P_{fails|M}(\pi)$
$= \frac{P_{fails}(\pi)}{P_M(\pi)} \leq$
e^{-n}
polynomial in n


Estimation
36 bits
$(P)^{\otimes n}$
$(\tilde{P}_{guess})^n$
selection theorem
$S = n \log_2 P_{guess}$
a state that's perm invariant
n constant inputs
can be obtained by
measuring an iid state $P^{\otimes n}$
$P_{fails}(\sigma) \leq P_{fails|M}(\pi)$
$= \frac{P_{fails}(\pi)}{P_M(\pi)} \leq e^{-n}$ polynomial in n


Estimation
selection theorem
a state that's perm invariant
can be obtained by
measuring an
(convex comb. of iid states)
polynomial in n
constant inputs
$P_{fails}(\sigma) \leq P_{fails|M}(\pi)$
$= \frac{P_{fails}(\pi)}{P_M(\pi)} \leq$
e^{-n}
$(P)^{\otimes n}$
$(\tilde{P}_{guess})^n$
$\leq -n \log_2 P_{guess}$