Title: SDP / Quantum Lecture Series

Speakers: Jamie Sikora
Date: July 22, 2019 - 10:00 AM

URL: http://pirsa.org/19070072

Lecture 3-E

Diamond norm

Recall from last lecture, that

$$F(\mathcal{S},\sigma) = \max \frac{1}{2}\mathrm{Tr}(X) + \frac{1}{2}\mathrm{Tr}(X^*)$$

$$\begin{bmatrix} \mathcal{S} & X \\ X^* & \sigma \end{bmatrix} \geq 0$$

Lecture 3-E

Diamond norm

Recall from last lecture, that

$$F(\rho,\sigma) = \max \frac{1}{2}\mathrm{Tr}(X) + \frac{1}{2}\mathrm{Tr}(X^*)$$
$$\begin{bmatrix} \rho & X \\ X^* & \sigma \end{bmatrix} \geq 0$$

The diamond norm is a useful norm for quantum channels. This is also called the completely bounded 1-norm

$\Phi : L(X) \to L(Y)$

operators from $X \to X$

The induced norm

$$\|\Phi\|_1 = \max \left\{ \|\Phi(X)\|_1 : X \in L(X), \|X\|_1 \leq 1 \right\}$$

is the 1-norm

Lecture 3: E

Diamond norm

Recall from last lecture, that

$$F(\rho,\sigma) = \max \frac{1}{2}\mathrm{Tr}(X) + \frac{1}{2}\mathrm{Tr}(X^*)$$
$$\begin{bmatrix} \rho & X \\ X^* & \sigma \end{bmatrix} \geq 0$$

The diamond norm is a useful norm for quantum channels. This is also called the completely bounded 1-norm.

$$\overline{\Phi}: L(X) \to L(Y)$$

operators from $X \to X$

The induced norm

$$\|\overline{\Phi}\|_1 = \max\left\{ \|\overline{\Phi}(X)\|_1 : X \in L(X), \|X\|_1 \leq 1 \right\}$$

is the 1-norm

The completely bounded version is

$$\|\overline{\Phi}\| = \sup_{k \geq 1} \|\overline{\Phi} \otimes 1_{L(\mathbb{C}^k)}\|_1$$

Channel discrimination problem

$\underline{\underline{\Phi}}_0$, $\underline{\underline{\Phi}}_1$

If these are chosen w.p. $1/2$ then the optimal probability of learning which channel is

$$\frac{1}{2} + \frac{1}{4} \left\| \underline{\underline{\Phi}}_0 - \underline{\underline{\Phi}}_1 \right\|_1$$

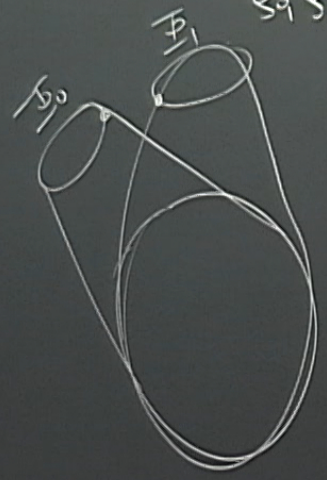
on problem

$\frac{1}{2}$

ity of

Defn: $F_{max}(\mathcal{F}_0, \mathcal{F}_1) = \max F(\mathcal{F}_0(\rho_0), \mathcal{F}_1(\rho_1))$

ρ_0, ρ_1 quantum states



$\Phi_1(\rho_1))$

quantum states

SDP: $F_{max}(\Phi, \Psi) = \max \frac{1}{2}\mathrm{Tr}(X) + \frac{1}{2}\mathrm{Tr}(X^*)$

$$\begin{bmatrix} \Phi_0(\rho_0) & X \\ X^* & \Phi_1(\rho_1) \end{bmatrix}$$

$\rho_0, \rho_1 \geq 0$

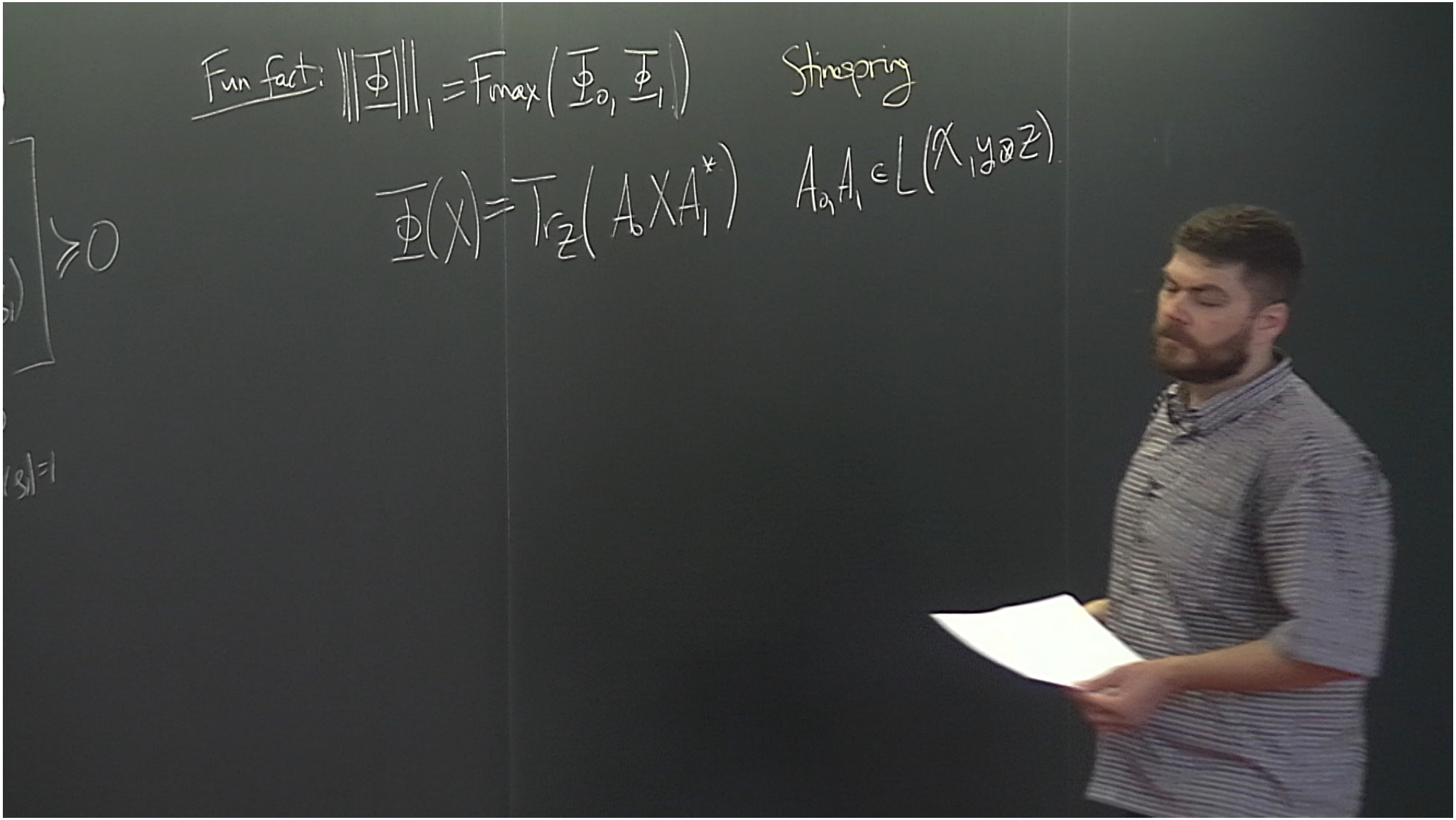
$\mathrm{Tr}(\rho_0) = \mathrm{Tr}(\rho_1) = 1$

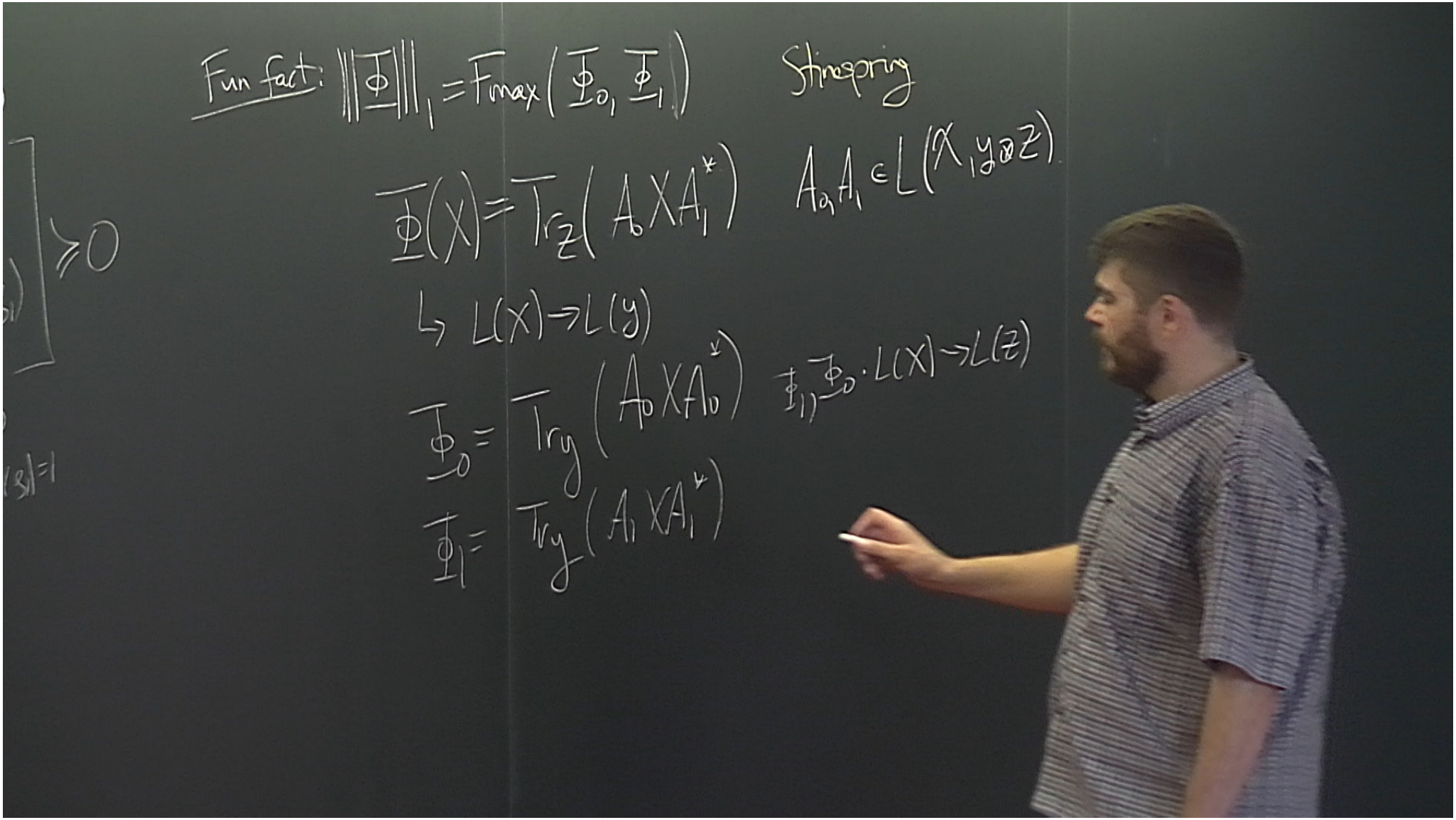
Fun fact: $\|\Phi\|_1 = F\max(\Phi_0, \Phi_1)$

$\Phi(X) = \mathrm{Tr}_Z(A_0 X A_1^*)$ $A_0, A_1 \in L(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$

≥ 0

$|\beta\rangle = 1$

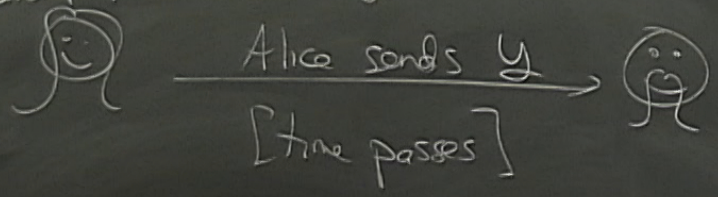

Fun fact: $\|\Phi\|_1 = F_{max}(\Phi_0, \Phi_1)$
Stinespring
$\Phi(X) = Tr_Z(A_0 X A_1^*)$
$A_0, A_1 \in L(X, Y \otimes Z)$
≥ 0


Fun fact: $\|\Phi\|_1 = F\max(\Phi_0, \Phi_1)$
Stinespring
$\Phi(X) = Tr_Z(AXA^*)$
$A_0, A_1 \in L(\mathcal{X}, \mathcal{Y}\otimes\mathcal{Z})$
$\hookrightarrow L(X) \to L(Y)$
$\Phi_0 = Tr_Y(A_0 X A_0^*)$
$\Phi_1 = Tr_Y(A_1 X A_1^*)$
$\Phi_0 \cdot L(X) \to L(Z)$

Lecture 3

Bit-Commitment

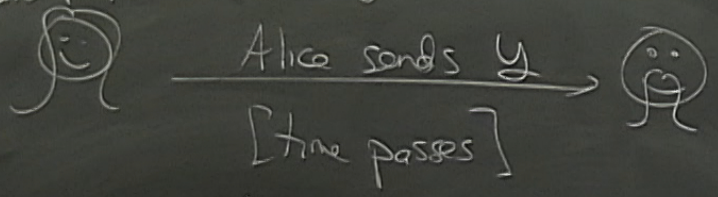
Alice chooses $a \in_R \{0,1\}$
and prepares $|\psi_a\rangle \in X \otimes Y$



Lecture 3

Bit-Commitment

Alice chooses $a \in_R \{0,1\}$
and prepares $|\psi_a\rangle \in X \otimes Y$



Alice sends $a \in X$

Bob checks if $X \otimes Y$ is in the state $|\psi_a\rangle$

$\{M_{accept}, M_{reject}\}$

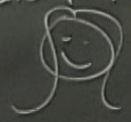
$M_{accept} = |\psi_a\rangle\langle\psi_a|$

$M_{reject} = \mathbb{1} - M_{accept}$

Lecture 3

Bit-Commitment

Alice chooses $a \in_R \{0,1\}$
and prepares $|\psi_a\rangle \in X \otimes Y$



Alice sends Y

[time passes]

Alice sends $a \& X$

Bob checks if $X \otimes Y$ is in the state $|\psi_a\rangle$
$\{M_{accept}, M_{reject}\}$

$M_{accept} = |\psi_a\rangle\langle\psi_a|$
$M_{reject} = \mathbb{1} - M_{accept}$

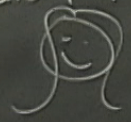
Objectives

- Bob should not be able to learn a from "Y message"
- Alice should not be able to "change a" before revealing

Lecture 3

Bit-Commitment

Alice chooses $a \in_R \{0,1\}$
and prepares $|\psi_a\rangle \in X \otimes Y$



Alice sends Y

[time passes]

Alice sends a & X

Bob checks if $X \otimes Y$ is in the state $|\psi_a\rangle$
$\{M_{accept}, M_{reject}\}$

$M_{accept} = |\psi_a\rangle\langle\psi_a|$
$M_{reject} = \mathbb{I} - M_{accept}$

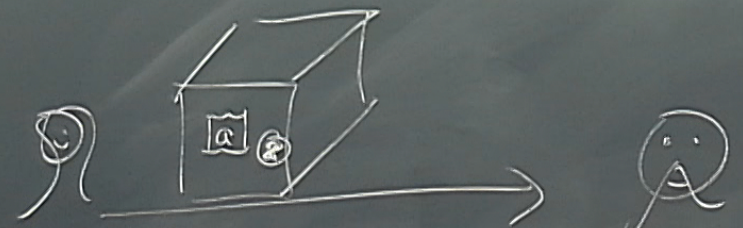
Objectives

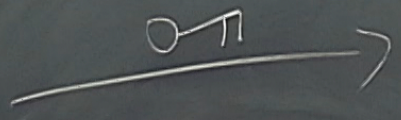
- Bob should not be able to learn a from "Y message" — hiding
- Alice should not be able to "change a" before revealing — binding

be able to learn a "message"

be able to change a "binding"

hiding

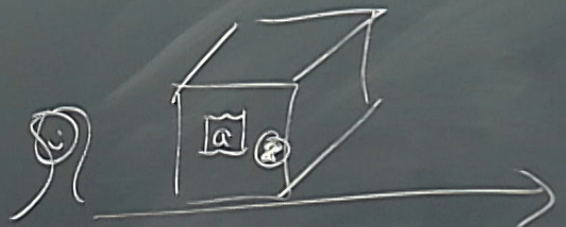


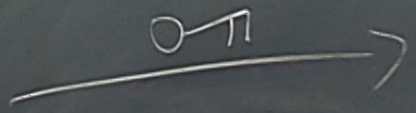


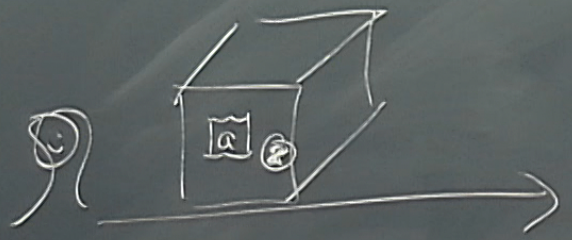
Objectives

- Bob should not be able to learn a from "y message" hiding
- Alice should not be able to "change a" before revealing binding

We will show with SDPs that both of these cannot hold



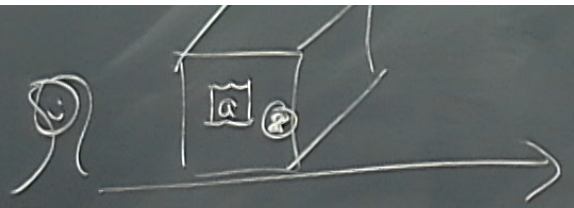




$$P_B^{\vee} = \sup \frac{1}{2}\langle M, \mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|)\rangle + \frac{1}{2}\langle M', \mathrm{Tr}_X(|\psi_1\rangle\langle\psi_1|)\rangle$$

$$M + M' = \mathbb{I}$$

$$M, M' \geq 0$$



$$0 \to \pi$$

$$P_B^{\vee} = \max \frac{1}{2}\langle M, \mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|)\rangle + \frac{1}{2}\langle M', \mathrm{Tr}_X(|\psi_1\rangle\langle\psi_1|)\rangle$$

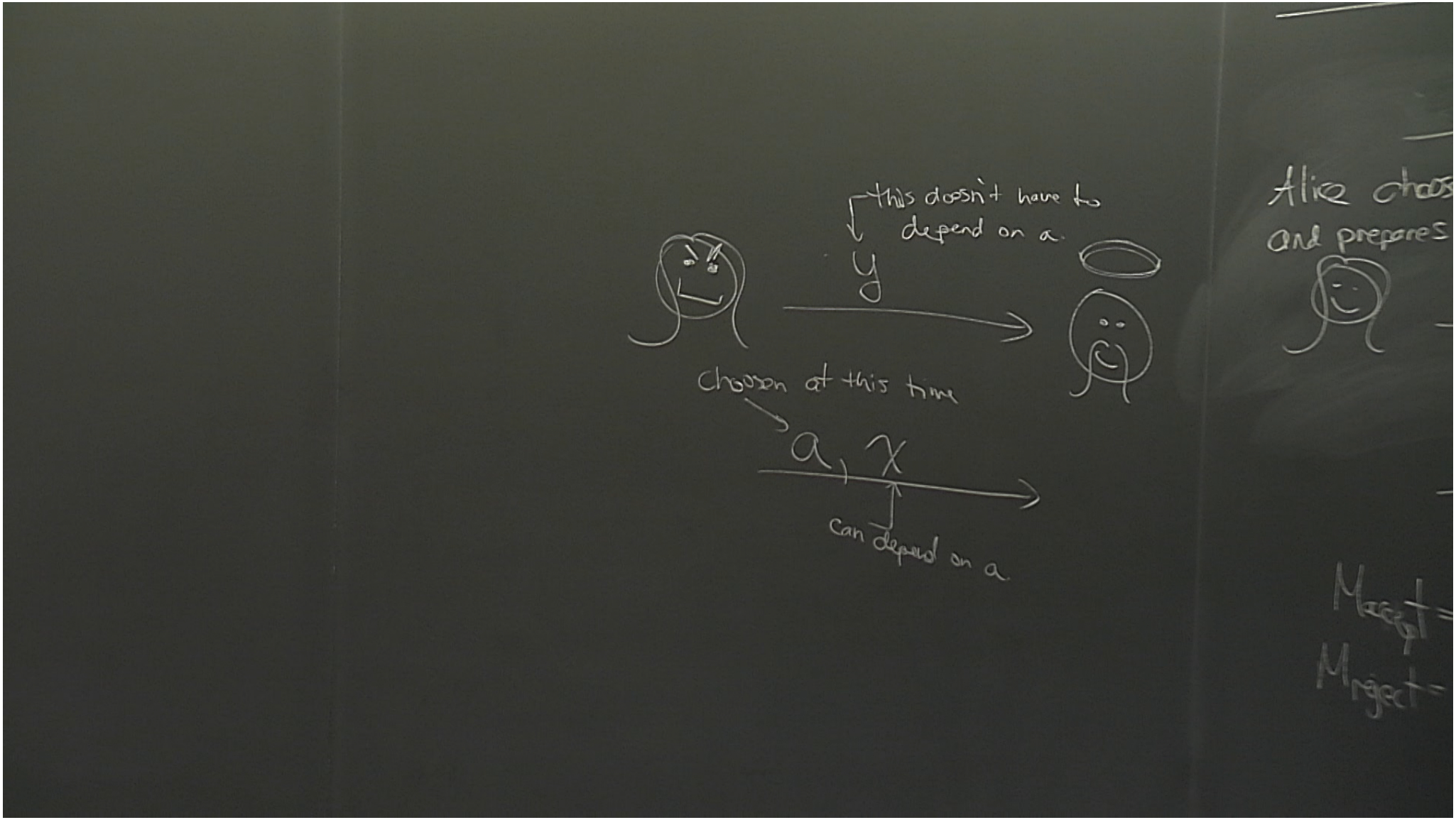
$$M + M' = \mathbb{I}$$

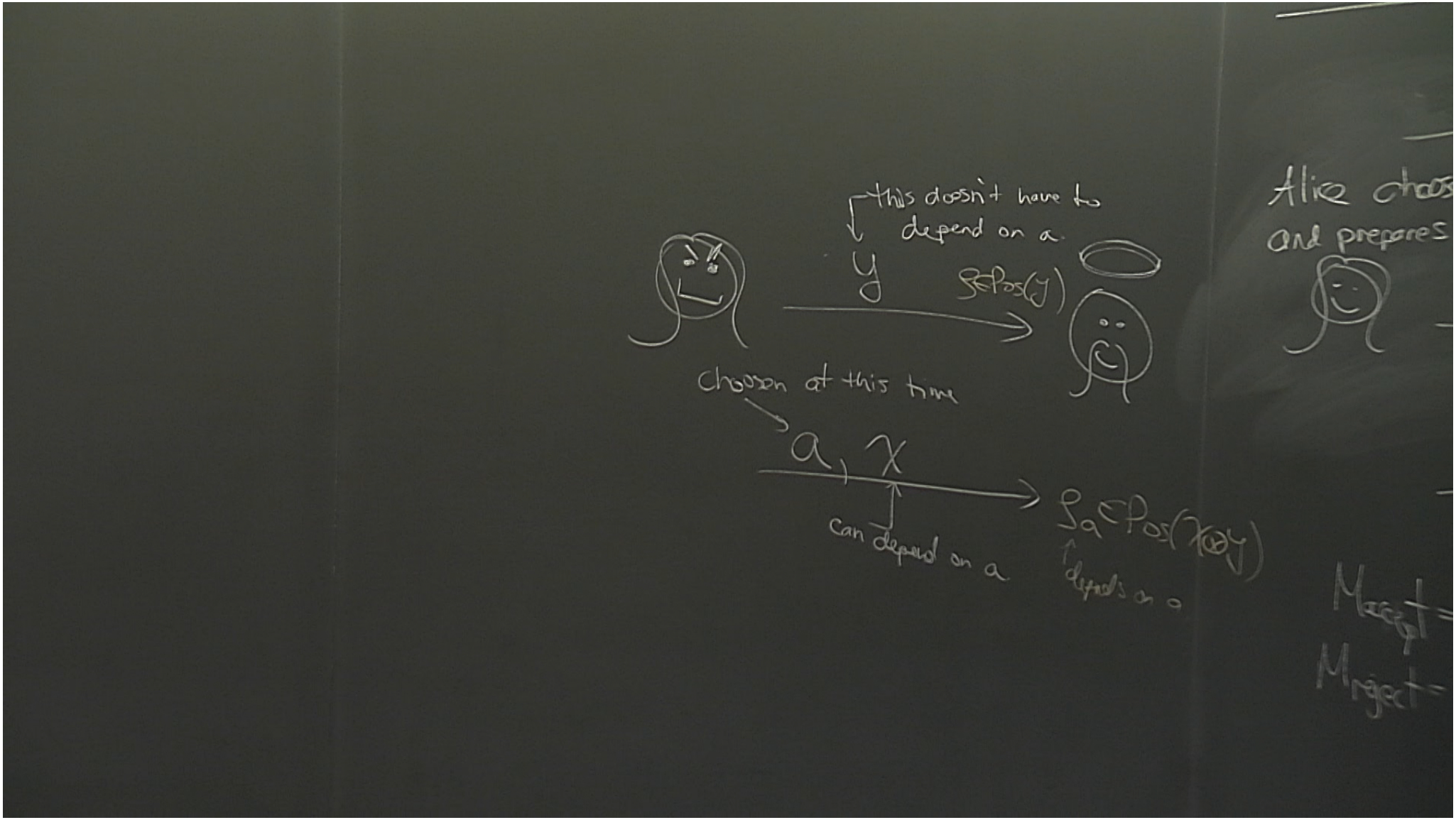
$$M, M' \geq 0$$

$$= \min \mathrm{Tr}(Y)$$

$$Y \geq \frac{1}{2}\mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|)$$

$$Y \geq \frac{1}{2}\mathrm{Tr}_X(|\psi_1\rangle\langle\psi_1|)$$


this doesn't have to depend on a
y
Alice choos
and prepares
Chosen at this time
a, x
can depend on a
Maccept =
Mreject =


this doesn't have to depend on a
y
$\rho \in Pos(Y)$
Alice choos
and prepares
Choosen at this time
a, x
$\rho_a \in Pos(X \otimes Y)$
can depend on a
depends on a
M accept
M reject

We have $\mathrm{Tr}_X(\rho_0) = \rho = \mathrm{Tr}_X(\rho_1)$

We have $\mathrm{Tr}_X(\sigma_0) = \sigma = \mathrm{Tr}_X(\sigma_1)$

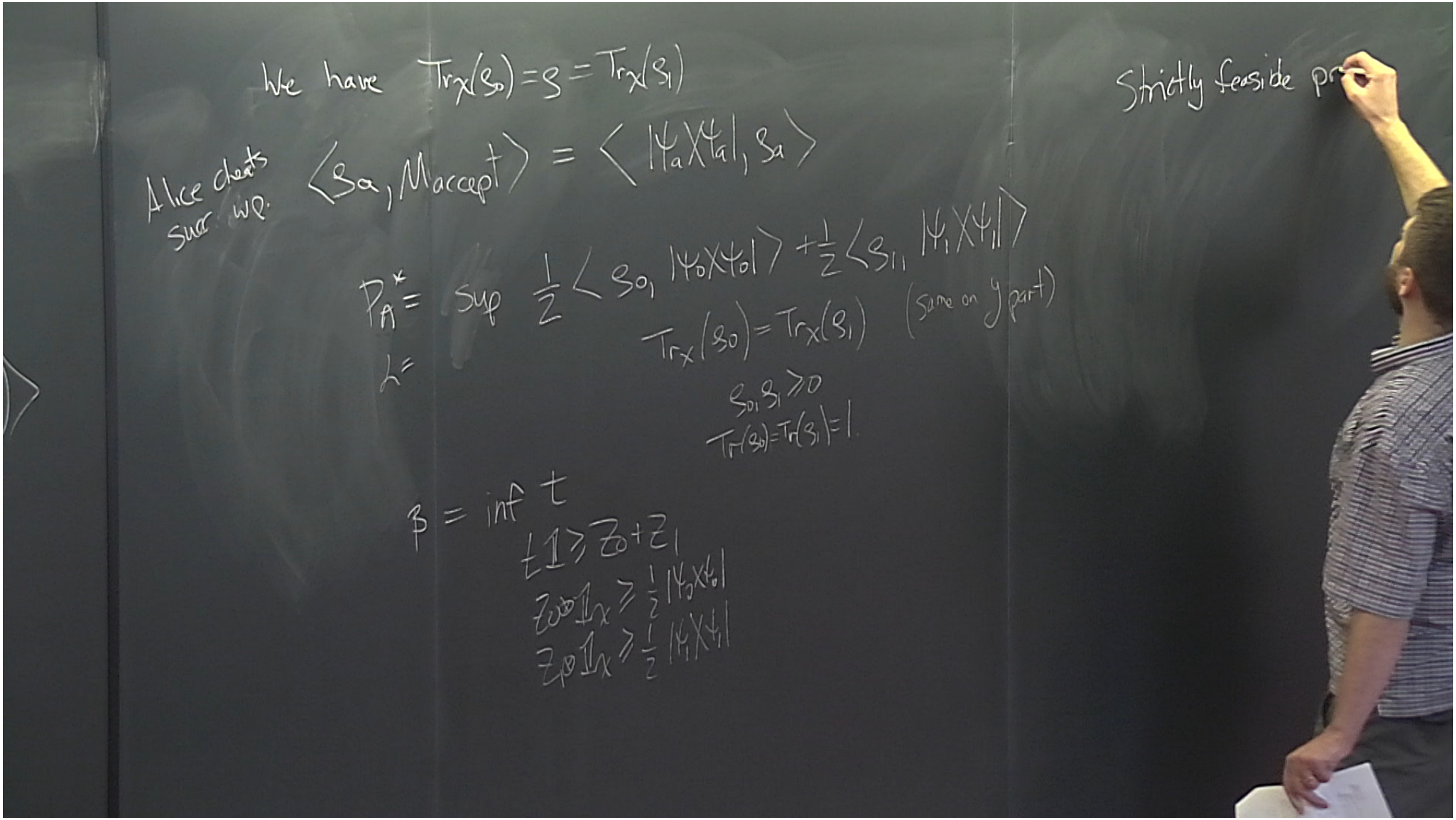
Alice cheats succ. wp. $\langle \sigma_a, M_{accept} \rangle = \langle |\psi_a X \psi_a|, \sigma_a \rangle$

$$P_A^* = \sup \frac{1}{2}\langle \sigma_0, |\psi_0 X \psi_0| \rangle + \frac{1}{2}\langle \sigma_1, |\psi_1 X \psi_1| \rangle$$

$\mathrm{Tr}_X(\sigma_0) = \mathrm{Tr}_X(\sigma_1)$ (same on y part)

$\sigma_0, \sigma_1 \geq 0$

$\mathrm{Tr}(\sigma_0) = \mathrm{Tr}(\sigma_1) = 1.$


We have $\mathrm{Tr}_X(\sigma_0) = \sigma = \mathrm{Tr}_X(\sigma_1)$
Strictly feasible pr
Alice cheats succ. wp.
$\langle \sigma_a, M_{accept} \rangle = \langle |\psi_a\rangle\langle\psi_a|, \sigma_a \rangle$
$p_A^* =$ sup $\frac{1}{2}\langle \sigma_0, |\psi_0\rangle\langle\psi_0| \rangle + \frac{1}{2}\langle \sigma_1, |\psi_1\rangle\langle\psi_1| \rangle$
$\lambda =$
$\mathrm{Tr}_X(\sigma_0) = \mathrm{Tr}_X(\sigma_1)$ (same on y part)
$\sigma_0, \sigma_1 \geq 0$
$\mathrm{Tr}(\sigma_0) = \mathrm{Tr}(\sigma_1) = 1$
$\beta =$ inf t
$t\mathbb{1} \geq Z_0 + Z_1$
$Z_0 \otimes \mathbb{1}_X \geq \frac{1}{2}|\psi_0\rangle\langle\psi_0|$
$Z_1 \otimes \mathbb{1}_X \geq \frac{1}{2}|\psi_1\rangle\langle\psi_1|$

$\mathrm{Tr}_X(S_1)$

$\langle |\psi_a X \psi_a|, S_a \rangle$

$S_0, |\psi_0 X \psi_0| \rangle + \frac{1}{2} \langle S_1, |\psi_1 X \psi_1| \rangle$ (same on y part)

$\mathrm{Tr}_X(S_0) = \mathrm{Tr}_X(S_1)$

$S_0, S_1 \geq 0$

$\mathrm{Tr}(S_0) = \mathrm{Tr}(S_1) = 1.$

$Z_0 + Z_1$

$\geq \frac{1}{2} |\psi_0 X \psi_0|$

$\geq \frac{1}{2} |\psi_1 X \psi_1|$

Strictly feasible primal solution is $S_0 = \frac{1}{4}$ (scaled)
$S_1 = \frac{1}{4}$ (scaled)

Strictly feasible dual solution is $Z_0 = \mathbb{1}$
$Z_1 = \mathbb{1}$
$t = 3$

So $\beta = p_A^*$ and the dual is attained.

$$\xrightarrow{\rho \to \Pi}$$

$$P_B^{\vee} = \max \frac{1}{2}\langle M, \mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|)\rangle + \frac{1}{2}\langle M', \mathrm{Tr}_X(|\psi_1\rangle\langle\psi_1|)\rangle$$

$$M + M' = \mathbb{I}$$

$$M, M' \geq 0$$

$$= \min \mathrm{Tr}(Y)$$

$$Y \geq \frac{1}{2}\mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|) \qquad Y \geq 0$$

$$Y \geq \frac{1}{2}\mathrm{Tr}_X(|\psi_1\rangle\langle\psi_1|)$$

Lecture 3

Ideally: $P_B^* = 1/2$ & $P_A^* = 1/2$ (or close to).

Let t, Z_0, Z_1 be dual opt for P_A^*
Let Y be dual opt for P_B^*

$$P_A^* P_B^* = t \cdot \mathrm{Tr}(Y)$$

$$= \langle tI, Y \rangle$$

$$\geq \langle Z_0 + Z_1, Y \rangle \qquad Y \geq 0$$

$$= \langle Z_0, Y \rangle + \langle Z_1, Y \rangle$$

$Z_0, Z_1 \geq 0$

$$\geq \left\langle Z_0, \tfrac{1}{2}\mathrm{Tr}_X\left(|\psi_0\rangle\langle\psi_0|\right) \right\rangle + \left\langle Z_1, \tfrac{1}{2}\mathrm{Tr}_X\left(|\psi_1\rangle\langle\psi_1|\right) \right\rangle$$

Lecture 3

Ideally: $P_B^* = 1/2$ & $P_A^* = 1/2$ (or close to).

Let t, Z_0, Z_1 be dual opt for A^*
Let Y be dual opt for P_B^*

$$P_A^* P_B^* = t \cdot \mathrm{Tr}(Y)$$

$$= \langle tI, Y \rangle$$

$$\geq \langle Z_0 + Z_1, Y \rangle \qquad Y \geq 0$$

$$= \langle Z_0, Y \rangle + \langle Z_1, Y \rangle \qquad Z_0, Z_1 \geq 0$$

$$\geq \left\langle Z_0, \tfrac{1}{2}\mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|) \right\rangle + \left\langle Z_1, \tfrac{1}{2}\mathrm{Tr}_X(|\psi_1\rangle\langle\psi_1|) \right\rangle$$

$$= \tfrac{1}{2}\langle Z_0 \otimes I_X, |\psi_0\rangle\langle\psi_0| \rangle + \tfrac{1}{2}\langle Z_0 \otimes I_X, |\psi_1\rangle\langle\psi_1| \rangle$$

Lecture 3

Ideally: $P_B^* = 1/2$ & $P_A^* = 1/2$ (or close to).

Let (t, Z_0, Z_1) be dual opt for P_A^*
Let Y be dual opt for P_B^*

$$P_A^* P_B^* = t \cdot \mathrm{Tr}(Y)$$

$$= \langle tI, Y \rangle$$

$$\geq \langle Z_0 + Z_1, Y \rangle \qquad Y \geq 0$$

$$= \langle Z_0, Y \rangle + \langle Z_1, Y \rangle$$

$Z_0, Z_1 \geq 0$

$$\geq \left\langle Z_0, \tfrac{1}{2}\mathrm{Tr}_X\left(|\psi_0\rangle\langle\psi_0|\right) \right\rangle + \left\langle Z_1, \tfrac{1}{2}\mathrm{Tr}_X\left(|\psi_1\rangle\langle\psi_1|\right) \right\rangle$$

$$= \tfrac{1}{2}\langle Z_0 \otimes I_X, |\psi_0\rangle\langle\psi_0| \rangle + \tfrac{1}{2}\langle Z_0 \otimes I_X, |\psi_1\rangle\langle\psi_1| \rangle$$

$$\geq \tfrac{1}{2}\left\langle \tfrac{1}{2} N_{\psi_0}\langle\psi_0|, |\psi_0\rangle\langle\psi_0| \right\rangle + \tfrac{1}{2}\left\langle \tfrac{1}{2}|\psi_1\rangle\langle\psi_1|, |\psi_1\rangle\langle\psi_1| \right\rangle$$

Lecture 3

Ideally: $P_B^* = 1/2$ & $P_A^* = 1/2$ (or close to)

$P_A^* P_B^* \geq \frac{1}{2} \Rightarrow \max\{P_A^*, P_B^*\} \geq \frac{1}{\sqrt{2}} \approx 71\%$

Let (t, Z_0, Z_1) be dual opt for A^*
Let Y be dual opt for P_B^*

$P_A^* P_B^* = t \cdot \mathrm{Tr}(Y)$

$= \langle t\mathbb{I}, Y \rangle$

$\geq \langle Z_0 + Z_1, Y \rangle \quad Y \geq 0$

$= \langle Z_0, Y \rangle + \langle Z_1, Y \rangle$

$Z_0, Z_1 \geq 0$

$\geq \langle Z_0, \frac{1}{2}\mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|) \rangle + \langle Z_1, \frac{1}{2}\mathrm{Tr}_X(|\psi_1\rangle\langle\psi_1|) \rangle$

$= \frac{1}{2}\langle Z_0 \otimes \mathbb{I}_X, |\psi_0\rangle\langle\psi_0| \rangle + \frac{1}{2}\langle Z_0 \otimes \mathbb{I}_X, |\psi_1\rangle\langle\psi_1| \rangle$

$\geq \frac{1}{2}\langle \frac{1}{2}|\psi_0\rangle\langle\psi_0|, |\psi_0\rangle\langle\psi_0| \rangle + \frac{1}{2}\langle \frac{1}{2}|\psi_1\rangle\langle\psi_1|, |\psi_1\rangle\langle\psi_1| \rangle$

$= \frac{1}{2}$

P_B^*

Lecture 3

Ideally: $P_B^* = 1/2$ & $P_A^* = 1/2$ (or close to)

Let t, z_0, z_1 be dual opt for A^*

Let y be dual opt for P_B^*

$$P_A^* P_B^* = t \cdot \mathrm{Tr}(y)$$

$$= \langle tI, y \rangle$$

$$\geq \langle z_0 + z_1, y \rangle \qquad y \geq 0$$

$$= \langle z_0, y \rangle + \langle z_1, y \rangle$$

$z_0, z_1 \geq 0$

$$\geq \left\langle z_0, \tfrac{1}{2}\mathrm{Tr}_X\left(|\psi_0\rangle\langle\psi_0|\right) \right\rangle + \left\langle z_1, \tfrac{1}{2}\mathrm{Tr}_X\left(|\psi_1\rangle\langle\psi_1|\right) \right\rangle$$

$$= \tfrac{1}{2}\langle z_0 \otimes I_X, |\psi_0\rangle\langle\psi_0| \rangle + \tfrac{1}{2}\langle z_0 \otimes I_X, |\psi_1\rangle\langle\psi_1| \rangle$$

$$\geq \tfrac{1}{2}\left\langle \tfrac{1}{2}|\psi_0\rangle\langle\psi_0|, |\psi_0\rangle\langle\psi_0| \right\rangle + \tfrac{1}{2}\left\langle \tfrac{1}{2}|\psi_1\rangle\langle\psi_1|, |\psi_1\rangle\langle\psi_1| \right\rangle$$

$$= \frac{1}{2}$$

$P_A^* P_B^* \geq \frac{1}{2} \Rightarrow \max\left\{P_A^* \| P_B^*\right\} \geq \frac{1}{\sqrt{2}} \approx 71\%$

So, quantum BC is impossible. □

Lecture 5

This form

$$P_A^* + P_B^* \geq \frac{3}{2}$$

FvdS ↑

Kitaev CF prof.

Ideally: $P_B^* = 1/2$ & $P_A^* = 1/2$ (or

let t, z_0, z_1 be dua

let y be dual

$$P_A^* P_B^* = t \cdot \mathrm{Tr}(y)$$

$$= \langle t\mathbb{I}, y \rangle$$

$$\geq \langle z_0 + z_1, y \rangle \qquad y \geq 0$$

$$= \langle z_0, y \rangle + \langle z_1, y \rangle$$

$z_0, z_1 \geq 0$

$$\geq \left\langle z_0, \tfrac{1}{2}\mathrm{Tr}_X(|\psi_0\rangle\langle\psi_0|) \right\rangle + \left\langle z_1, \tfrac{1}{2}\mathrm{Tr}_X \right.$$

$$= \tfrac{1}{2}\langle z_0 \otimes \mathbb{I}_X, |\psi_0\rangle\langle\psi_0| \rangle + \tfrac{1}{2}\langle z_0 \otimes \mathbb{I}_X, |\psi$$

$$\geq \tfrac{1}{2}\left\langle \tfrac{1}{2}|\psi_0\rangle\langle\psi_0|, |\psi_0\rangle\langle\psi_0| \right\rangle + \tfrac{1}{2}\left\langle \tfrac{1}{2}|\psi_1\rangle\langle\psi_1| \right.$$

$$= \frac{1}{2}$$

This form

$$P_A^* + P_B^* \geq \frac{3}{2}$$

FvdS ↑

Kitaev CF prof.

Lecture 3

Ideally: $P_B^* = 1/2$ & $P_A^* = 1/2$ (or

let t, z_0, z_1 be du

let y be dual

$$P_A^* P_B^* = t \cdot \mathrm{Tr}(y)$$

$$= \langle tI, y \rangle$$

$$\geq \langle z_0 + z_1, y \rangle \qquad y \geq 0$$

$$= \langle z_0, y \rangle + \langle z_1, y \rangle$$

$z_0, z_1 \geq 0$

$$\geq \left\langle z_0, \tfrac{1}{2}\mathrm{Tr}_X\left(|\psi_0\rangle\langle\psi_0|\right) \right\rangle + \left\langle z_1, \tfrac{1}{2}\mathrm{Tr}_X \right.$$

$$= \frac{1}{2}\langle z_0 \otimes I_X, |\psi_0\rangle\langle\psi_0| \rangle + \frac{1}{2}\langle z_0 \otimes I_{X_1}, |\psi$$

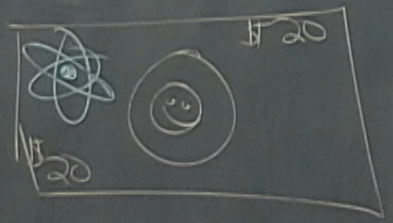
$$\geq \frac{1}{2}\left\langle \tfrac{1}{2}|\psi_0\rangle\langle\psi_0|, |\psi_0\rangle\langle\psi_0| \right\rangle + \frac{1}{2}\left\langle \tfrac{1}{2}|\psi_1\rangle\langle\psi_1| \right.$$

$$= \frac{1}{2}$$

≈71%

Quantum Money

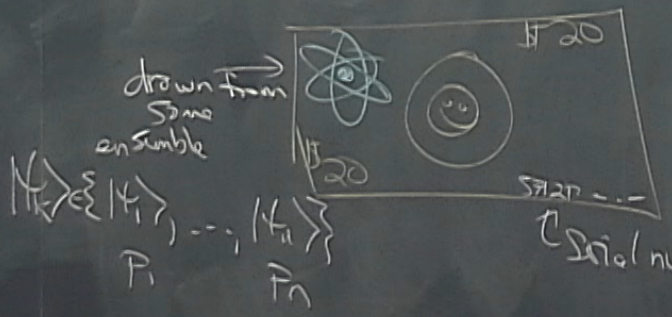
mint some money
verifies it later



≈ 71%

Quantum Money

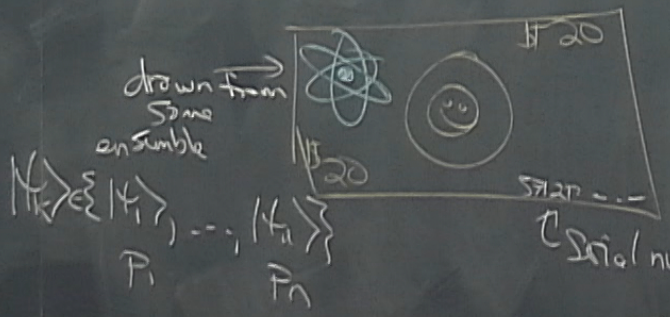
mint some money
verifies it later



≈ 71%

Quantum Money

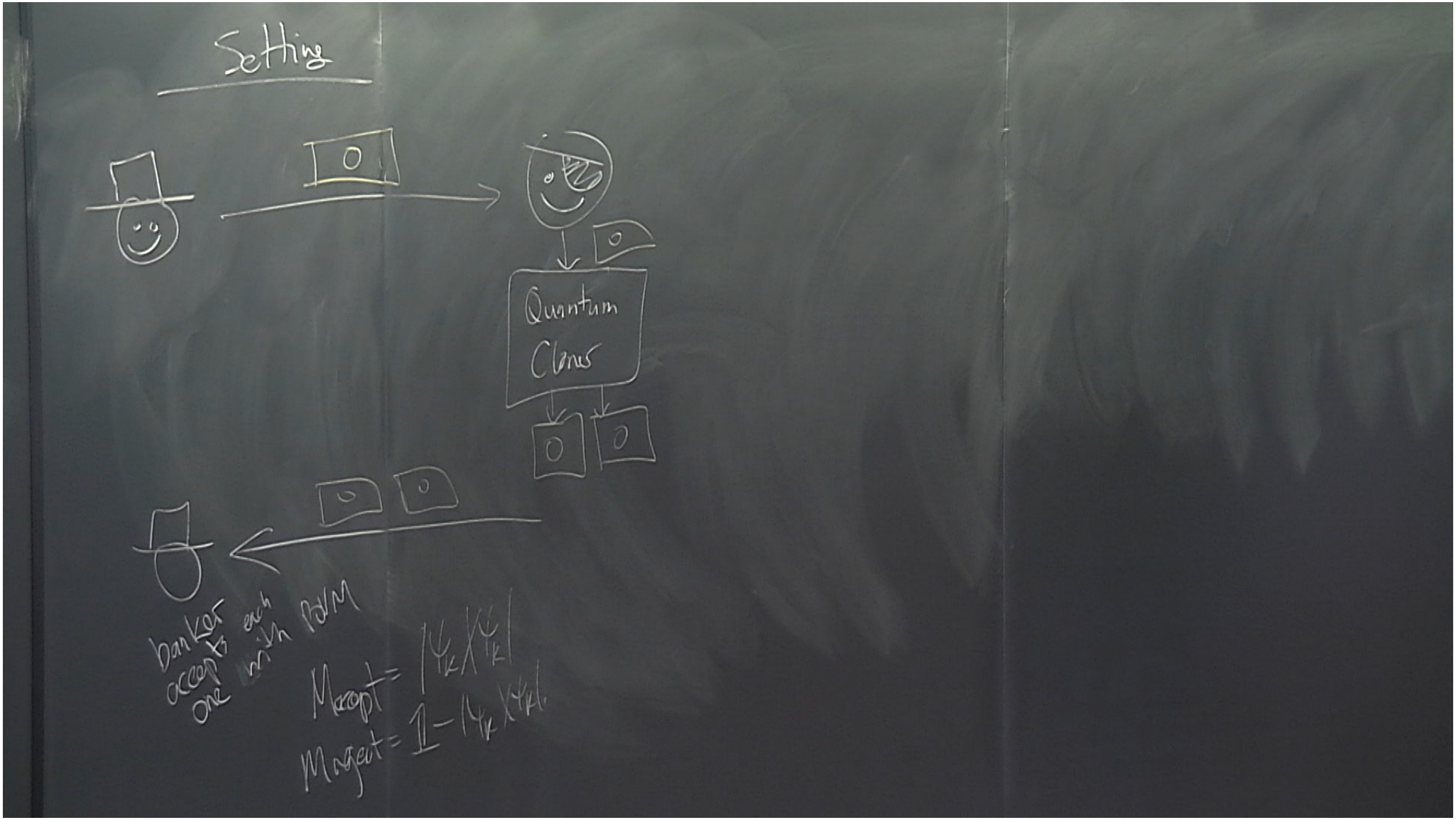
Mint some money
verifies it later

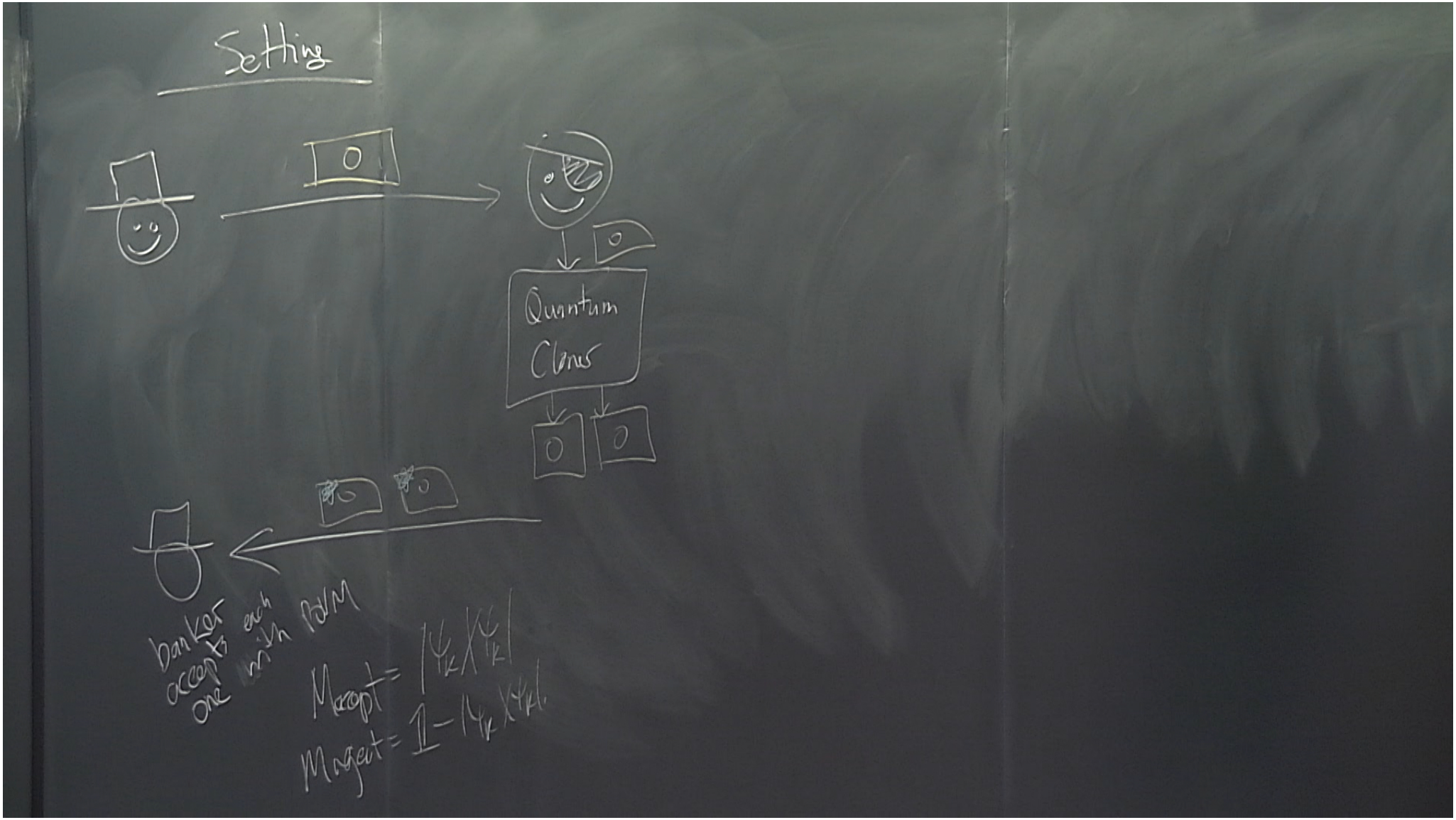


$\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$
P_1 P_n

(Serial number, ensemble and state chosen.)

A forger wants to copy the money.


Setting
Quantum Cloner
banker accepts each one with p≥M
$M_{accept} = |\psi_k\rangle\langle\psi_k|$
$M_{reject} = \mathbb{1} - |\psi_k\rangle\langle\psi_k|$


Setting
Quantum Cloner
banker accepts each with p(k)M
$M_{accept} = |\psi_k\rangle\langle\psi_k|$
$M_{reject} = \mathbb{1} - |\psi_k\rangle\langle\psi_k|$

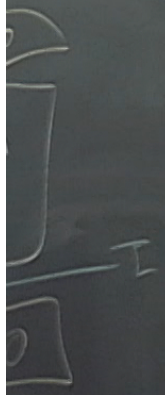
If an honest person returns a banknote, it will be accepted with certainty

Will the banks accept a forgery?

Let $\Sigma \in Pos(\mathcal{X} \otimes \mathcal{X})$ $\quad |\psi_k\rangle \in \mathcal{X}$.

The forger succeeds w.p. $\langle \Sigma, M_{accept} \rangle$

$= \langle \psi_k | \langle \psi_k | \Sigma | \psi_k \rangle | \psi_k \rangle$



If an honest person returns a banknote, it will be accepted with certainty

Will the banks accept a forgery?

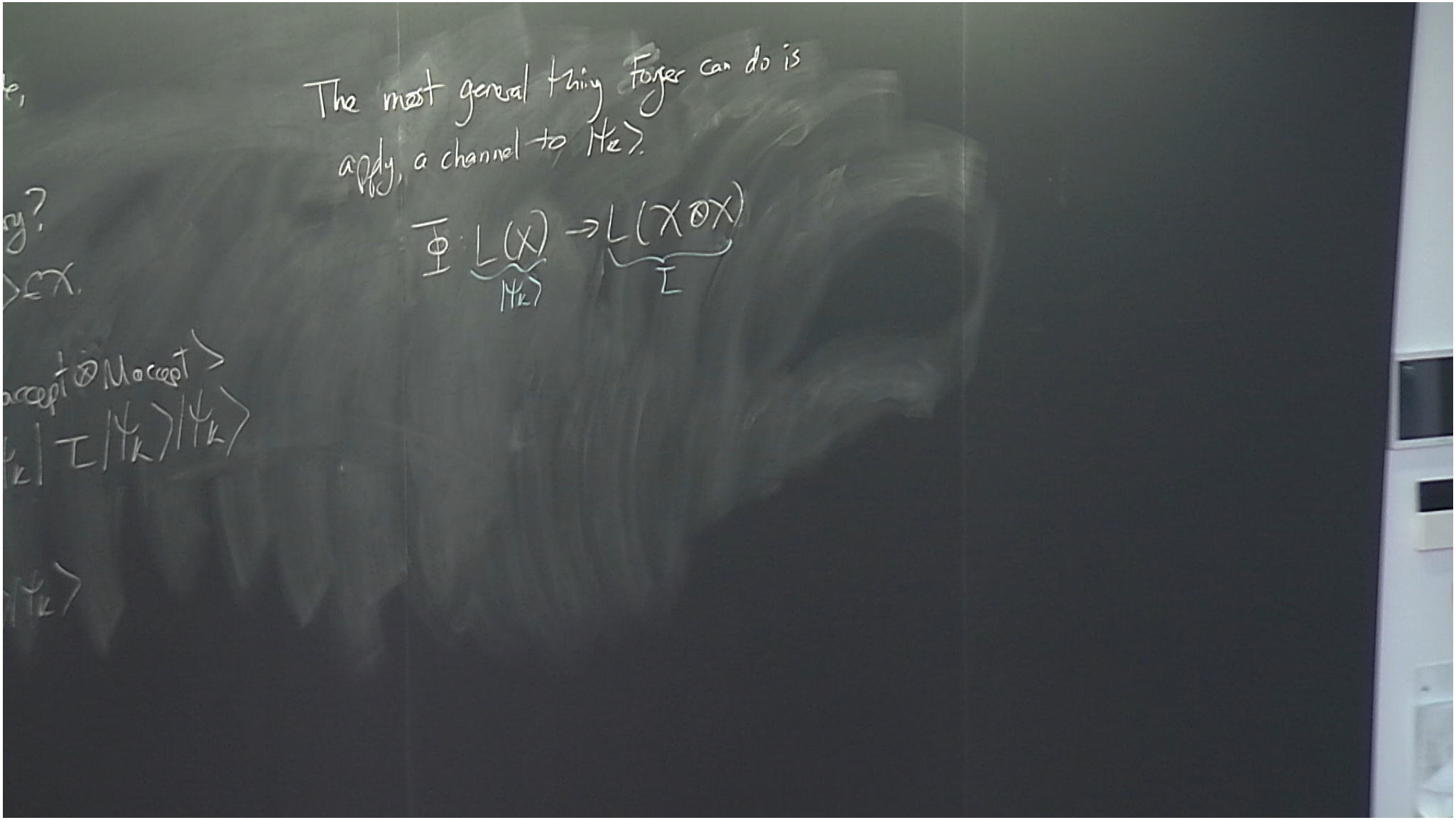
Let $\Sigma \in pos(\mathcal{X} \otimes \mathcal{X})$ $\quad |\psi_k\rangle \in \mathcal{X}$.

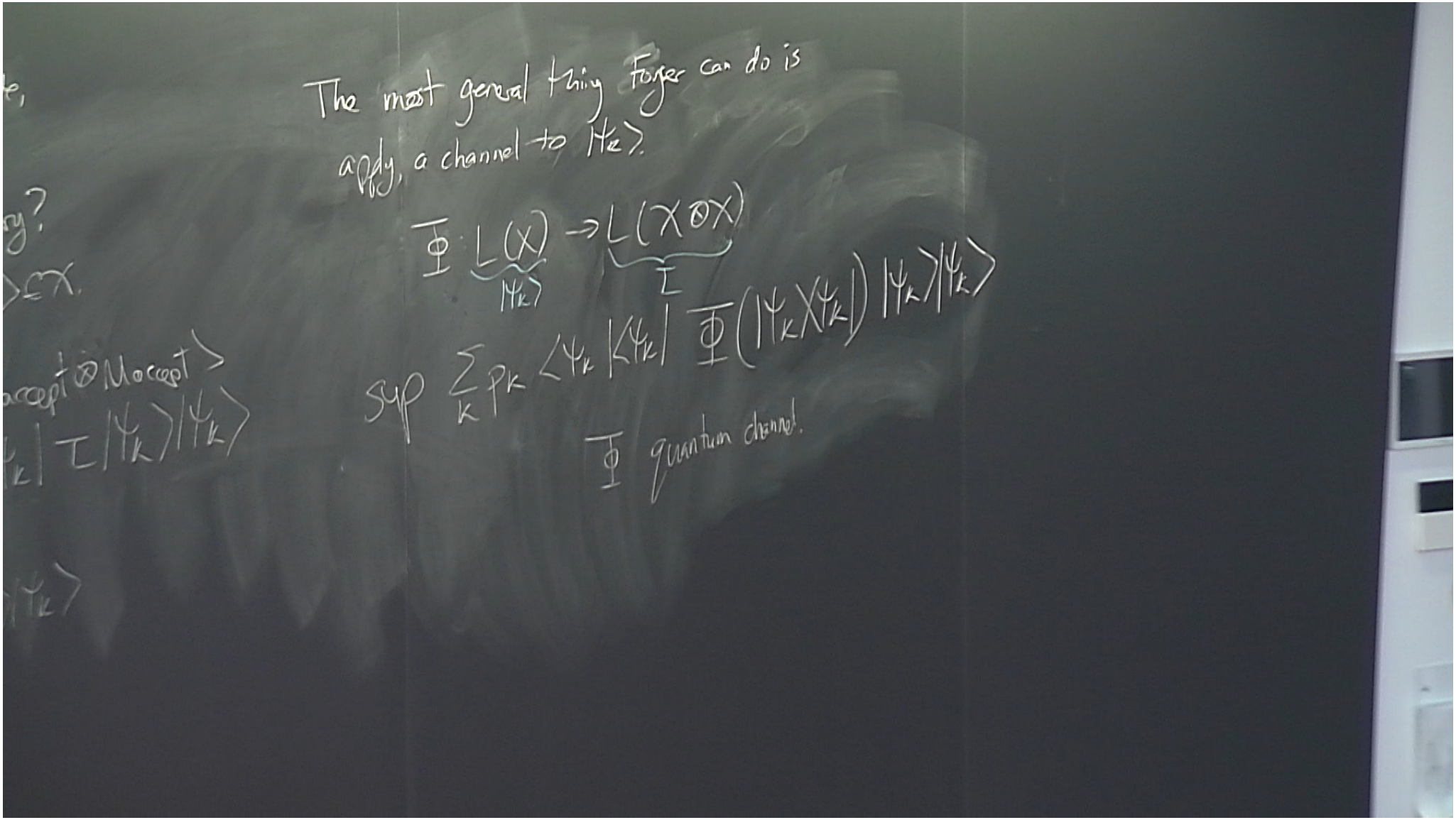
The forger succeeds w.p. $\langle \Sigma, M_{accept} \otimes M_{accept} \rangle$

$= \langle \psi_k | \langle \psi_k | \Sigma | \psi_k \rangle | \psi_k \rangle$

Average over k.

$\sum_k p_k \langle \psi_k | \langle \psi_k | \Sigma | \psi_k \rangle | \psi_k \rangle$


The most general thing Forger can do is
apply a channel to |ψ_k⟩.
Φ : L(X) → L(X⊗X)
|ψ_k⟩
I


The most general thing Forger can do is
apply a channel to $|\psi_k\rangle$.
$\Phi : L(X) \to L(X \otimes X)$
$|\psi_k\rangle$
$\sup \sum_k p_k \langle \psi_k | \Phi(|\psi_k\rangle\langle\psi_k|) |\psi_k\rangle |\psi_k\rangle$
Φ quantum channel.

Lecture 3

Choi-Jamiołkowski representation of quantum channels

$\Phi \in L(X) \to L(Y)$ $\longleftrightarrow$ $J(\Phi)$

$$J(\Phi) = \sum_{k,l} \Phi(|k\rangle\langle l|) \otimes |k\rangle\langle l| \in L(Y \otimes X)$$

Φ is trace-preserving $\iff$ $\mathrm{Tr}_Y(J(\Phi)) = \mathbb{1}_X$

Φ is completely-positive $\iff$ $J(\Phi) \geq 0$

Lecture 3

Choi–Jamiołkowski representation of quantum channels

$\Phi \longleftrightarrow J(\Phi)$

$\Phi : L(X) \to L(Y)$

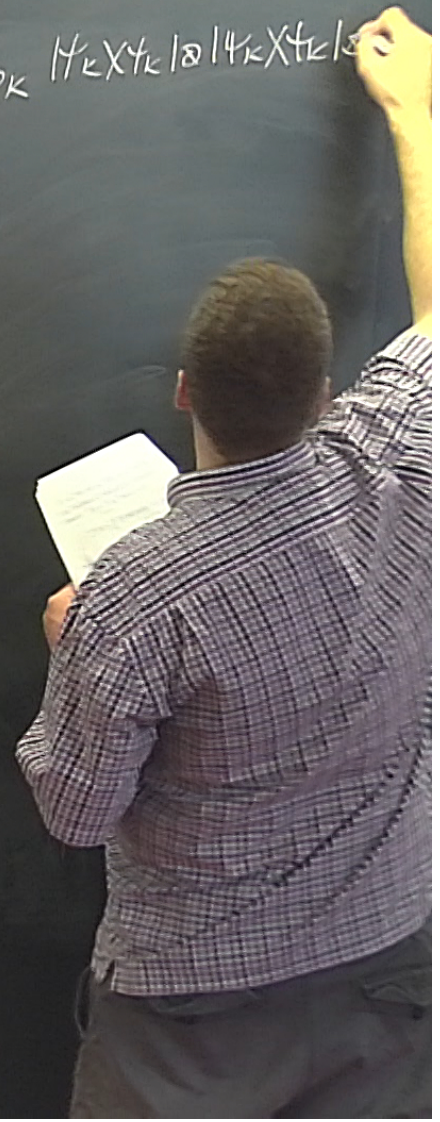
$$J(\Phi) = \sum_{k,\ell} \Phi(|k\rangle\langle\ell|) \otimes |k\rangle\langle\ell| \in L(Y \otimes X)$$

Φ is trace-preserving $\iff \mathrm{Tr}_Y(J(\Phi)) = \mathbb{1}_X$

Φ is completely-positive $\iff J(\Phi) \geq 0$

$$\langle \Phi(\rho), \sigma \rangle = \langle J(\Phi), \sigma \otimes \bar{\rho} \rangle$$

$$\sup \langle J, \sum_k p_k |\psi_k\rangle\langle\psi_k| \otimes |\phi_k\rangle\langle\phi_k| \rangle$$



$C \geq 0$

$|\psi_k\rangle\langle\psi_k| \otimes |\psi_k\rangle\langle\psi_k| \otimes |\overline{\psi_k}\rangle\langle\overline{\psi_k}|$

wski representation of

$\Phi \longleftrightarrow J(\Phi)$

$L(X) \to L(Y)$

$\Phi(|k\rangle\langle\ell|) \otimes |k\rangle\langle\ell| \in L(Y \otimes X)$

$\alpha = \sup \langle J, \sum_k p_k \; \cdot \; \rangle$

s.t. $\mathrm{Tr}_Y(J) = \mathbb{1}_X$

$J \geq 0$

$y = Y \otimes X$

$= \sup \langle J, C \rangle$

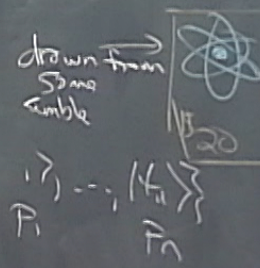
$\mathrm{Tr}_Y(J) = \mathbb{1}_X$

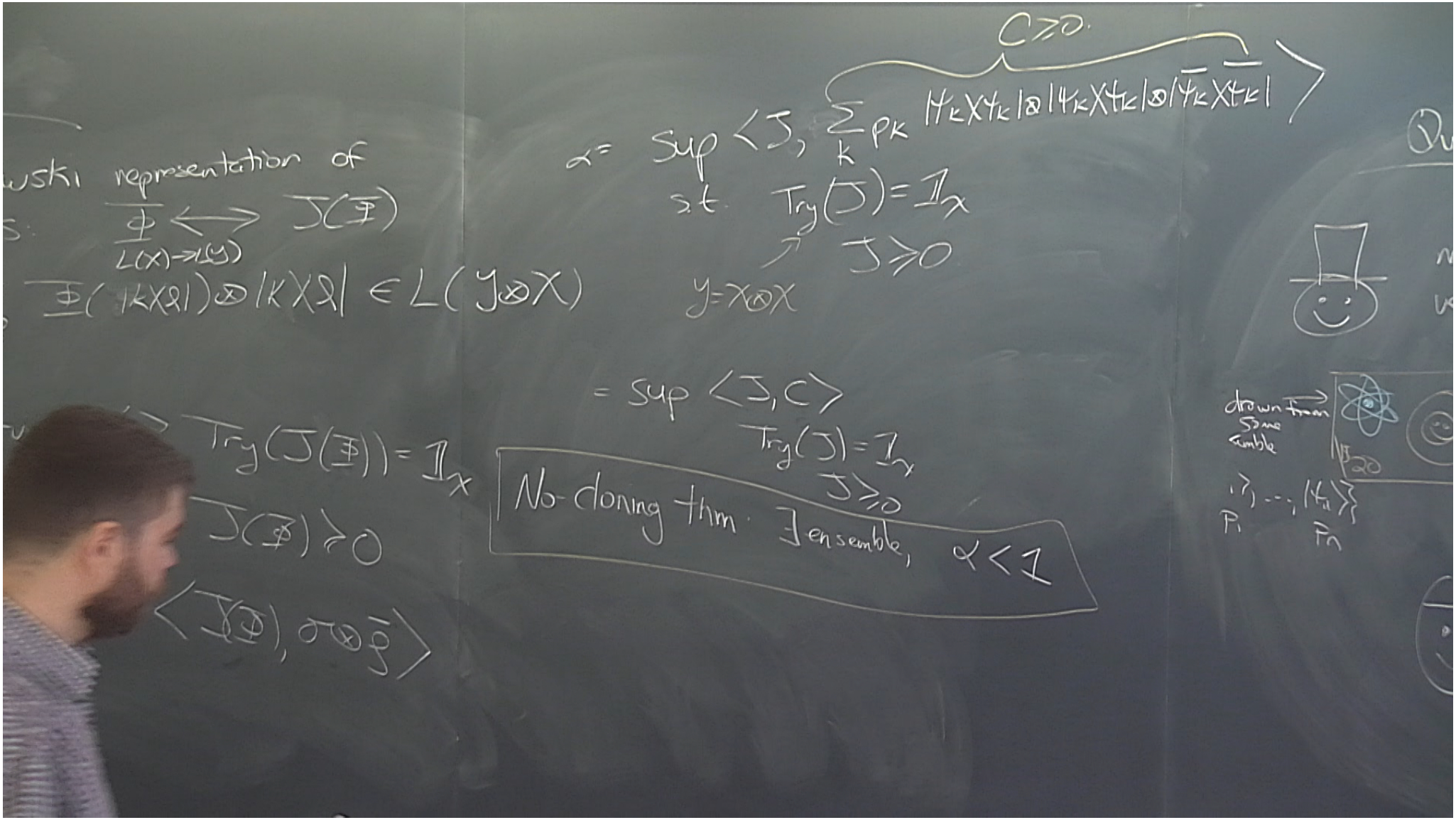
$J \geq 0$

uing $\Leftrightarrow \mathrm{Tr}_Y(J(\Phi)) = \mathbb{1}_X$

tive $\Leftrightarrow J(\Phi) \geq 0$

$\alpha\rangle = \langle J(\Phi), \sigma \otimes \overline{\sigma}\rangle$




C≥0
wski representation of
Φ ⟷ J(Φ)
L(X)→L(Y)
Φ(|k⟩⟨ℓ|)⊗|k⟩⟨ℓ| ∈ L(Y⊗X)
α = sup ⟨J, Σ_k p_k |ψ_k⟩⟨ψ_k|⊗|ψ_k⟩⟨ψ_k|⊗|ψ̄_k⟩⟨ψ̄_k|⟩
s.t. Tr_Y(J) = 𝟙_X
J≥0
Y=X⊗X
= sup ⟨J, C⟩
Tr_Y(J) = 𝟙_X
J≥0
Tr_Y(J(Φ)) = 𝟙_X
J(Φ)≥0
⟨J(Φ), σ⊗ρ⟩
No-cloning thm. ∃ ensemble, α<1
drawn from same ensemble
P_1
P_n

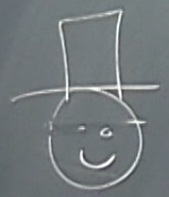
C ≥ 0

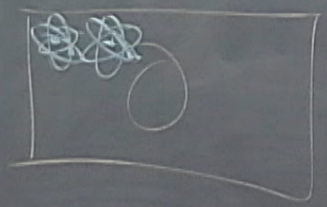
What if the banker is unhappy with d?

Can we boost security?

ensemble 1: $p_k \to |\psi_k\rangle$

ensemble 2: $q_k \to |\phi_k\rangle$





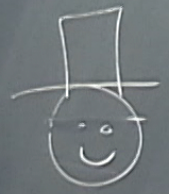
$\chi < 1$

C≥0.

$|\psi_k\rangle\otimes|\psi_k\rangle\langle\psi_k|\otimes|\bar{\psi}_k\rangle\langle\bar{\psi}_k|$

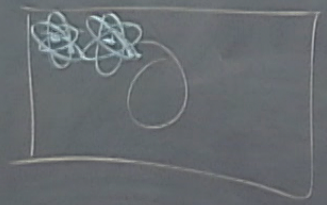
What if the banker is unhappy with d?

Can we boost security?



ensemble 1: $p_k \to |\psi_k\rangle$

ensemble 2: $q_k \to |\phi_k\rangle$



$\chi < 1$

$M_{acopt} = |\psi_k\rangle\langle\psi_k|\otimes|\phi_k\rangle\langle\phi_k|$

$= M_{acopt}^{(1)} \otimes M_{acopt}^{(2)}$

$\alpha_{1,2} = \sup \langle J, C_1 \otimes C_2 \rangle$

2 consistent assignments

$\mathrm{Tr}_{yy'}(J) = \mathbb{1}_{xx'}$

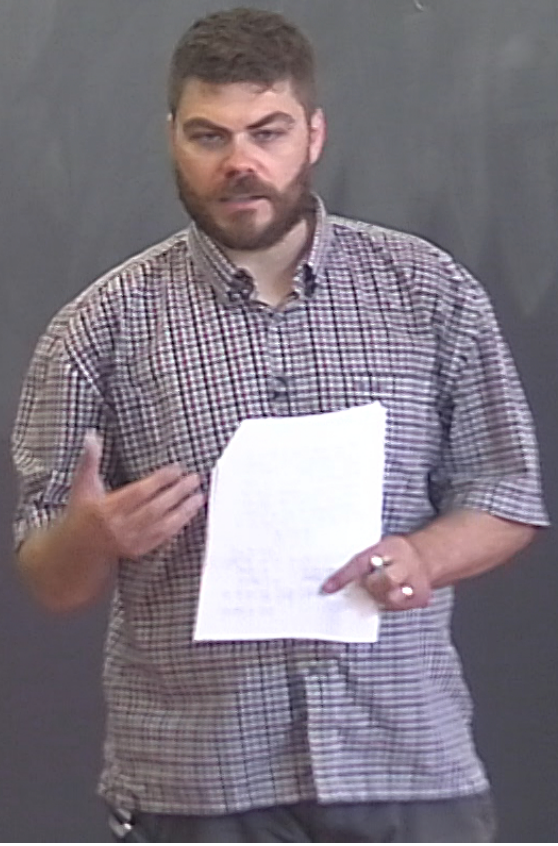
$J \geq 0$

Lemma: $\alpha_{1,2} = \alpha_1 \cdot \alpha_2$

$\alpha_i = \sup \langle J, C_i \rangle$

$\mathrm{Tr}_y(J) = \mathbb{1}_x$

$J \geq 0$



$\alpha_{1,2} = \sup \langle J, C_1 \otimes C_2 \rangle$
2 consulte ao

$\mathrm{Tr}_{y_1 y_2}(J) = \mathbb{1}_{x_0 x}$

$J \geq 0$

Lemma: $\alpha_{1,2} = \alpha_1 \cdot \alpha_2$

$\alpha_j = \sup \langle J, C_j \rangle$

$\mathrm{Tr}_{y_j}(J) = \mathbb{1}_x$

$J \geq 0$

$\beta_{12} = \inf \mathrm{Tr}(Z)$

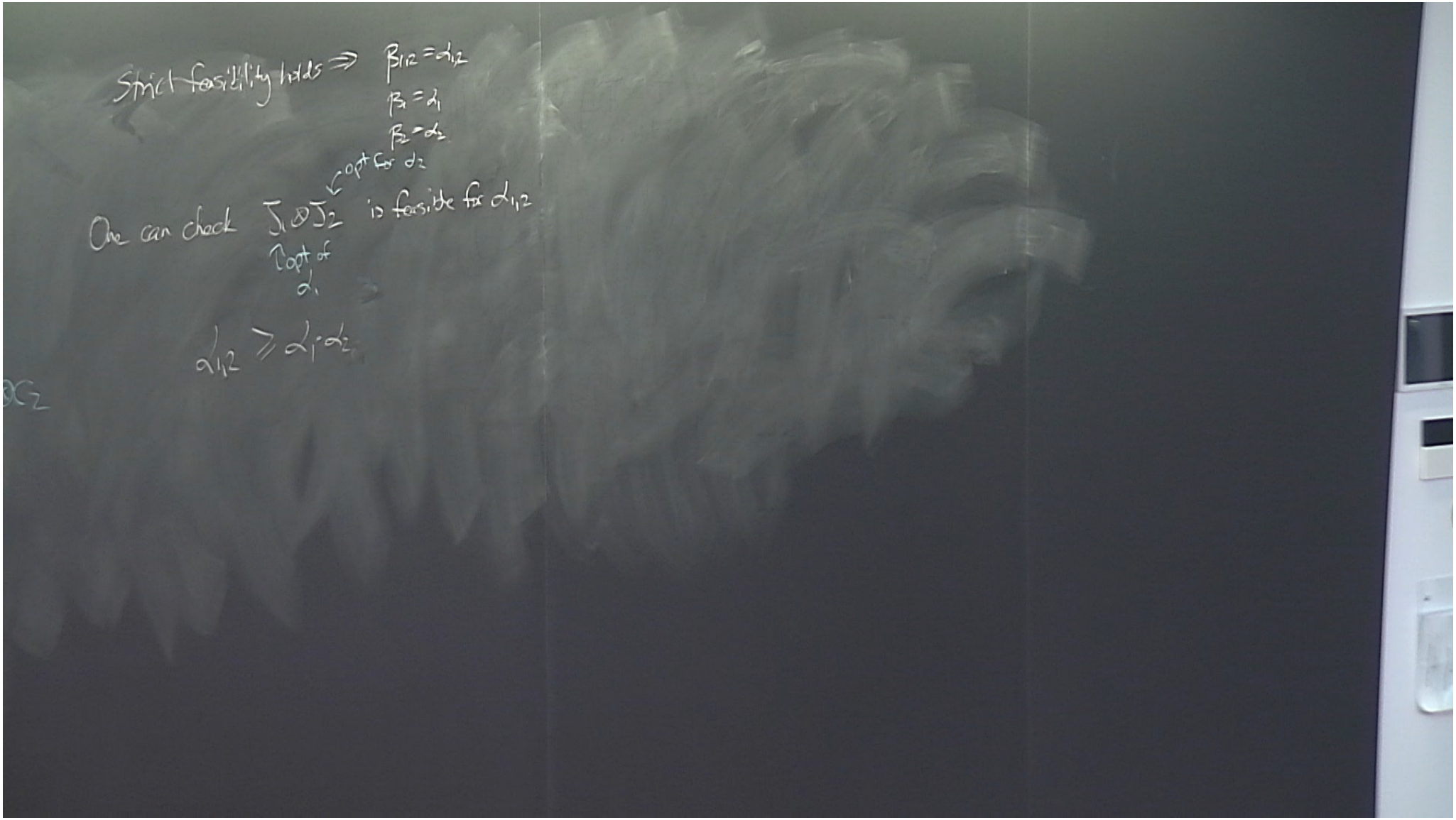
$Z \otimes \mathbb{1}_{y_1 y_2} \geq C_1 \otimes C_2$

$\beta_1 = \inf \mathrm{Tr}(Z)$

$Z \otimes \mathbb{1}_y \geq C_1$

$\beta_2 = \inf \mathrm{Tr}(Z)$

$Z \otimes \mathbb{1}_y \geq C_2$


Strict feasibility holds ⇒ $\beta_{1,2} = \alpha_{1,2}$
$\beta_1 = \alpha_1$
$\beta_2 = \alpha_2$
← opt for α_2
One can check $J_1 \otimes J_2$ is feasible for $\alpha_{1,2}$
↑ opt of α_1
$\alpha_{1,2} \geq \alpha_1 \cdot \alpha_2$

Lecture 3

We now $\beta_{1,2} \leq \beta_1 \cdot \beta_2$

$\alpha_{1,2} \quad \alpha_1 \quad \alpha_2$

Let Z_1 & Z_2 be dual opt.

$\mathrm{Tr}(Z_1) = \beta_1 \qquad \mathrm{Tr}(Z_2) = \beta_2$

$Z_1 \otimes I_y \geq C_1 \qquad Z_2 \otimes I_y \geq C_2$

Lecture 3

We now $\beta_{1,2} \leq \beta_1 + \beta_2$

$\alpha_{1,2} \quad \alpha_1 \quad \alpha_2$

Let Z_1 & Z_2 be dual opt.

$\mathrm{Tr}(Z_1) = \beta_1 \qquad \mathrm{Tr}(Z_2) = \beta_2$

$Z_1 \otimes I_y \geq C_1 \qquad Z_2 \otimes I_y \geq C_2$

$Z_1 \otimes I - C_1 \geq 0 \qquad Z_2 \otimes I - C_2 \geq 0$

Since $C_1 \geq 0$ $Z_1 \otimes I + C_1 \geq 0 \qquad Z_2 \otimes I + C_2 \geq 0$

$(Z_1 \otimes I - C_1) \otimes (Z_2 \otimes I + C_2) \geq 0$

Lecture 3

We now $\beta_{1,2} \leq \beta_1 \cdot \beta_2$

$\alpha_{1,2} \quad \alpha_1 \quad \alpha_2$

Let Z_1 & Z_2 be dual opt.

$\mathrm{Tr}(Z_1) = \beta_1$ $\quad$ $\mathrm{Tr}(Z_2) = \beta_2$

$Z_1 \otimes \mathbb{1}_y \geq C_1$ $\quad$ $Z_2 \otimes \mathbb{1}_y \geq C_2$

$Z_1 \otimes \mathbb{1} - C_1 \geq 0$ $\quad$ $Z_1 \otimes \mathbb{1} - C_2 \geq 0$

Since $C_1 \geq 0$ $\quad$ $Z_1 \otimes \mathbb{1} + C_1 \geq 0$ $\quad$ $Z_2 \otimes \mathbb{1} + C_2 \geq 0$

$(Z_1 \otimes \mathbb{1} - C_1) \otimes (Z_2 \otimes \mathbb{1} + C_2) \geq 0$

$(Z_1 \otimes \mathbb{1} + C_1) \otimes (Z_2 \otimes \mathbb{1} - C_2) \geq 0$

Add to get

$$2\left[Z_1 \otimes Z_2 \otimes \mathbb{1}_{yy} - C_1 \otimes C_2 \right] \geq 0$$

Lecture 3

We now $\beta_{1,2} \leq \beta_1 \cdot \beta_2$

$\alpha_{1,2} \quad \alpha_1 \quad \alpha_2$

Let Z_1 & Z_2 be dual opt.

$\mathrm{Tr}(Z_1) = \beta_1$ $\qquad$ $\mathrm{Tr}(Z_2) = \beta_2$

$Z_1 \otimes I_y \geq C_1$ $\qquad$ $Z_2 \otimes I_y \geq C_2$

$Z_1 \otimes I - C_1 \geq 0$ $\qquad$ $Z_1 \otimes I - C_2 \geq 0$

Since $C_1 \geq 0$ $\quad Z_1 \otimes I + C_1 \geq 0$ $\qquad$ $Z_2 \otimes I + C_2 \geq 0$

$(Z_1 \otimes I - C_1) \otimes (Z_2 \otimes I + C_2) \geq 0$

$(Z_1 \otimes I + C_1) \otimes (Z_2 \otimes I - C_2) \geq 0$

Add to get

$$2\left[Z_1 \otimes Z_2 \otimes 1_{yoy} - C_1 \otimes C_2 \right] \geq 0$$

So, $Z_1 \otimes Z_2$ is feasible for $\beta_{1,2}$

$\beta_{1,2} \leq \mathrm{Tr}(Z_1 \otimes Z_2) = \mathrm{Tr}(Z_1) \cdot \mathrm{Tr}(Z_2) = \beta_1 \cdot \beta_2$

□

$\beta_{1,2} \leq \beta_1 \cdot \beta_2$

$\alpha_{1,2} \quad \alpha_1 \quad \alpha_2$

be dual opt.

$\mathrm{Tr}(Z_2) = \beta_2$

$Z_2 \otimes \mathbb{I}_y \geq C_2$

$Z_1 \otimes \mathbb{I} - C_2 \geq 0$

$Z_2 \otimes \mathbb{I} + C_2 \geq 0$

$(Z_1 \otimes \mathbb{I} - C_1) \otimes (Z_2 \otimes \mathbb{I} + C_2) \geq 0$

$(Z_1 \otimes \mathbb{I} + C_1) \otimes (Z_2 \otimes \mathbb{I} - C_2) \geq 0$

Add to get

$$2\left[Z_1 \otimes Z_2 \otimes 1_{yy} - C_1 \otimes C_2 \right] \geq 0$$

So, $Z_1 \otimes Z_2$ is feasible for $\beta_{1,2}$

$\beta_{1,2} \leq \mathrm{Tr}(Z_1 \otimes Z_2) = \mathrm{Tr}(Z_1) \cdot \mathrm{Tr}(Z_2) = \beta_1 \cdot \beta_2$

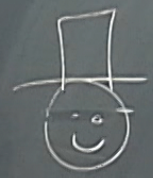
If ensemble with $q < 1$ □

Repeat n times to get q^n as new cheating of forging.

Quantum money is possible.

What if the bo

Can we boost s



ensemble 1: p

ensemble 2: q

$M_{accept} = |\psi_k\rangle\langle\psi_k| \otimes |\phi_k$

$= M_{accept}^{(1)} \otimes M_{accept}^{(2)}$