Title: Optimal quantum self-tests based on binary nonlocal XOR games

Date: Nov 07, 2012 04:00 PM

URL: http://pirsa.org/12110067

Abstract: Self-testing a multipartite quantum state means verifying the existence of the state based on the outcomes of unknown or untrusted measurements.

This concept is important in device-independent quantum cryptography.

There are some previously known results on self-testing which involve nonlocal binary XOR games such as the CHSH test and the GHZ paradox. In our work we expand on these results. We provide a general criterion which, when satisfied, guarantees that a given nonlocal binary XOR game is a robust self-test. The error term in this result is quadratic, which is the best possible. In my talk I will explain the conceptual basis for the criterion and offer some examples. This is joint work with Yaoyun Shi (arXiv:1207.1819).

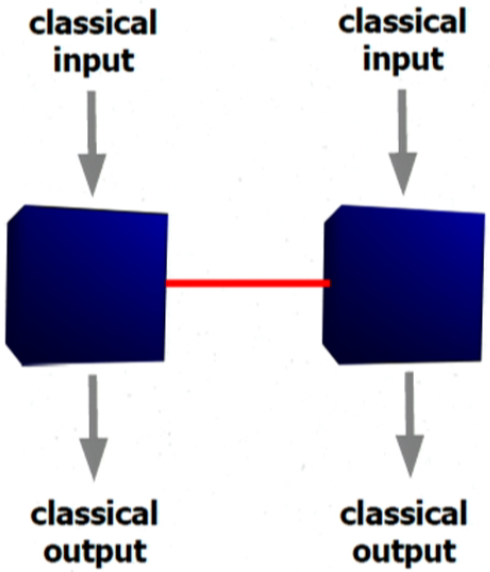
Self-Testing Properties for Binary Nonlocal XOR Games

Carl Miller
Electrical Engineering & Computer Science Department
University of Michigan, Ann Arbor

Intro: Self-Testing

Intro: Self-Testing

Intro: Self-Testing



Intro: Self-Testing

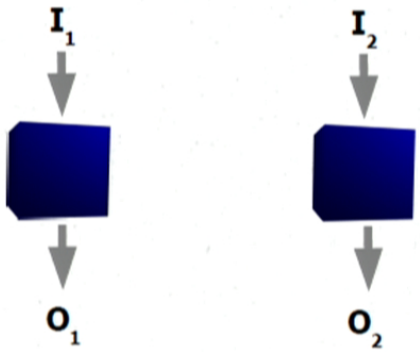
Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$

Intro: Self-Testing

Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$

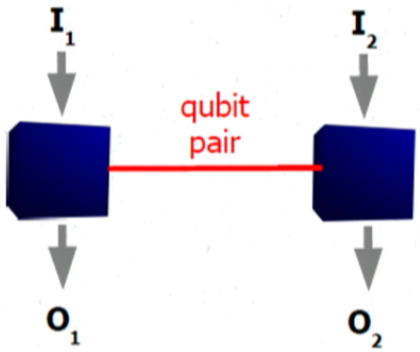
Intro: Self-Testing

Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$



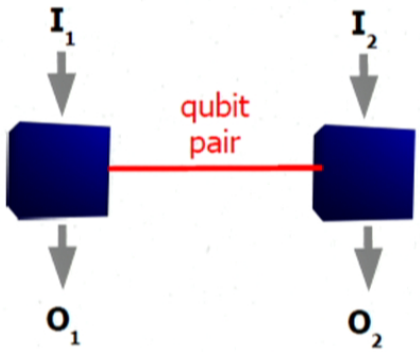
Intro: Self-Testing

Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$



Intro: Self-Testing

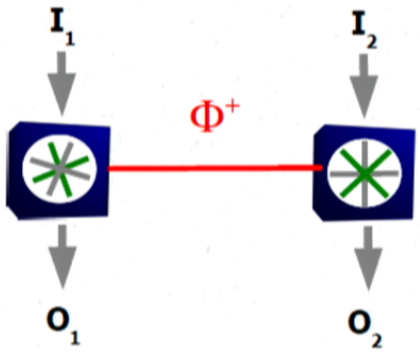
Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$



If **E** [F] (on random inputs) is $\sqrt{2}/2$, then the state and measurements are uniquely determined.

Intro: Self-Testing

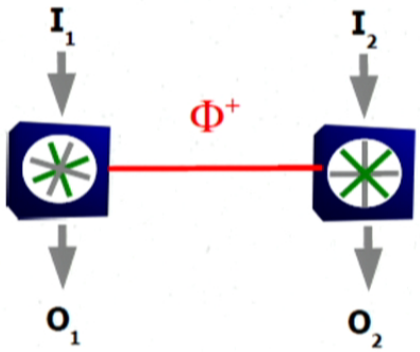
Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$

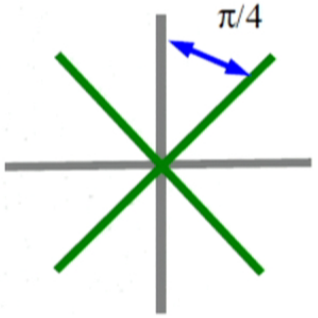


If **E** [F] (on random inputs) is $\sqrt{2}/2$, then the state and measurements are uniquely determined.

Intro: Self-Testing

Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$





If **E** [F] (on random inputs) is $\sqrt{2}/2$, then the state and measurements are uniquely determined.

Overview of Talk

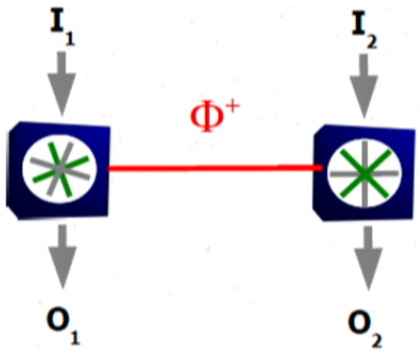
Goal: Begin a general theory for proving self-testing results.

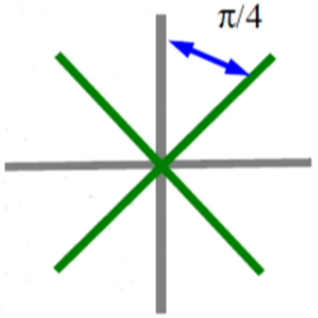
Overview of Talk

Goal: Begin a general theory for proving robust self-testing results.

Intro: Self-Testing

Let $F(I_1, I_2, O_1, O_2) = \begin{cases} +1 & \text{if } O_1 \oplus O_2 = I_1 \wedge I_2 \\ -1 & \text{otherwise} \end{cases}$





If **E** [F] (on random inputs) is $\sqrt{2}/2$, then the state and measurements are uniquely determined.

Overview of Talk

Goal: Begin a general theory for proving robust self-testing results.

Overview of Talk

Goal: Begin a general theory for proving robust self-testing results.

I. Background

Motivation: Randomness expansion and QKD.

Overview of Talk

Goal: Begin a general theory for proving robust self-testing results.

I. Background

Motivation: Randomness expansion and QKD.

Overview of Talk

Goal: Begin a general theory for proving **robust** self-testing results.

I. Background

Motivation: Randomness expansion and QKD.

II. Concepts.

Key idea: Nonlocal binary XOR games ⟶ sinusoidal functions.

Overview of Talk

Goal: Begin a general theory for proving **robust** self-testing results.

I. Background

Motivation: Randomness expansion and QKD.

II. Concepts.

Key idea: Nonlocal binary XOR games ⟶ sinusoidal functions.

III. Main result.

A criterion for robust self-tests.

Overview of Talk

Goal: Begin a general theory for proving **robust** self-testing results.

I. Background

Motivation: Randomness expansion and QKD.

II. Concepts.

Key idea: Nonlocal binary XOR games ⟶ sinusoidal functions.

III. Main result.

A criterion for robust self-tests.

IV. Examples.

Overview of Talk

Goal: Begin a general theory for proving robust self-testing results.

I. Background
Motivation: Randomness expansion and QKD.

II. Concepts.
Key idea: Nonlocal binary XOR games ⟶ sinusoidal functions.

III. Main result.
A criterion for robust self-tests.

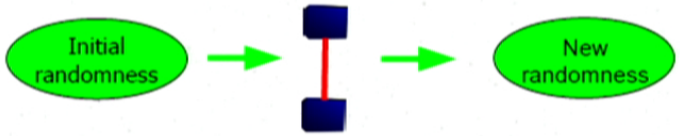
IV. Examples.

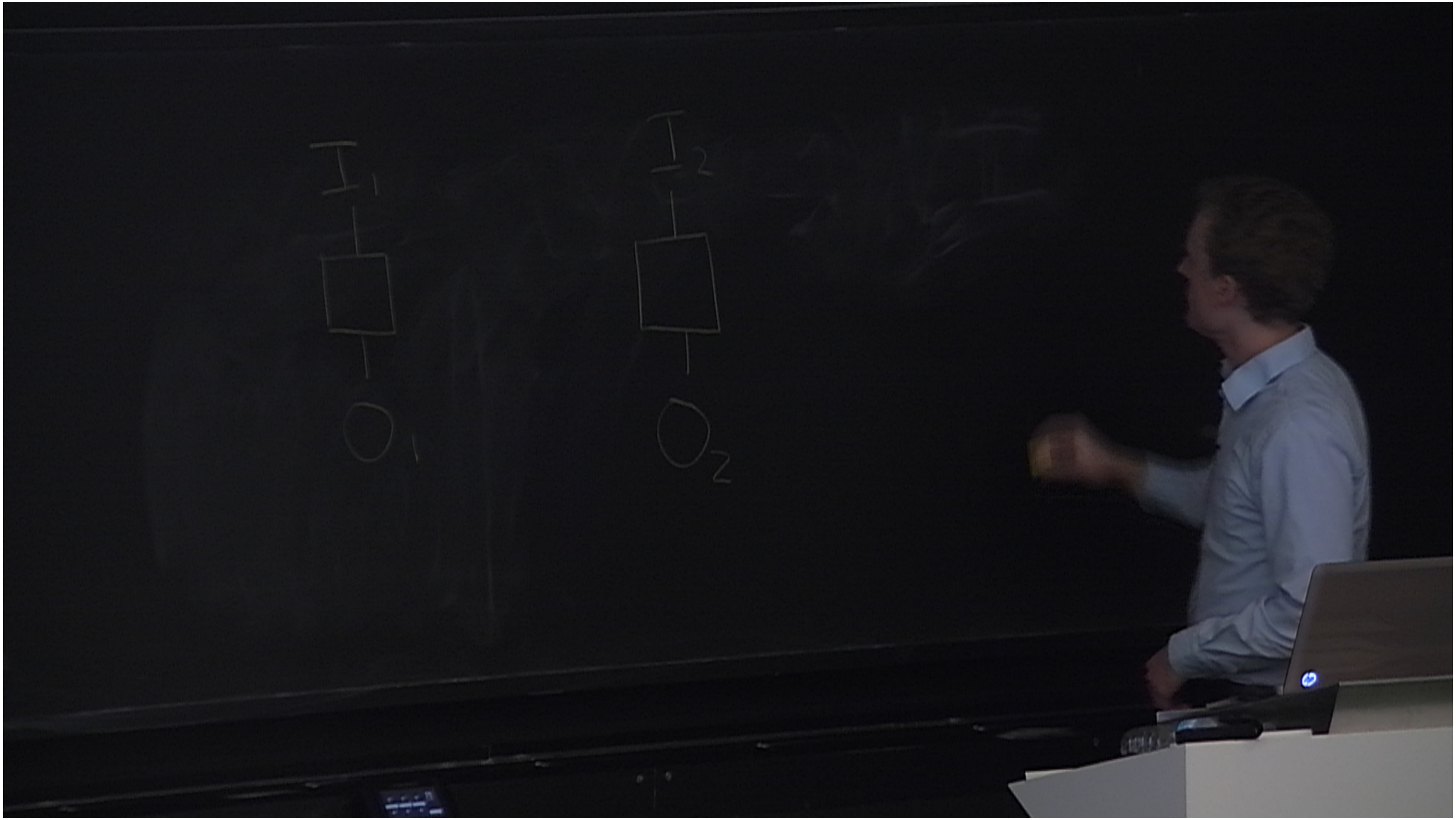
This is joint work with Yaoyun Shi. (arXiv:1207.1819)

Background

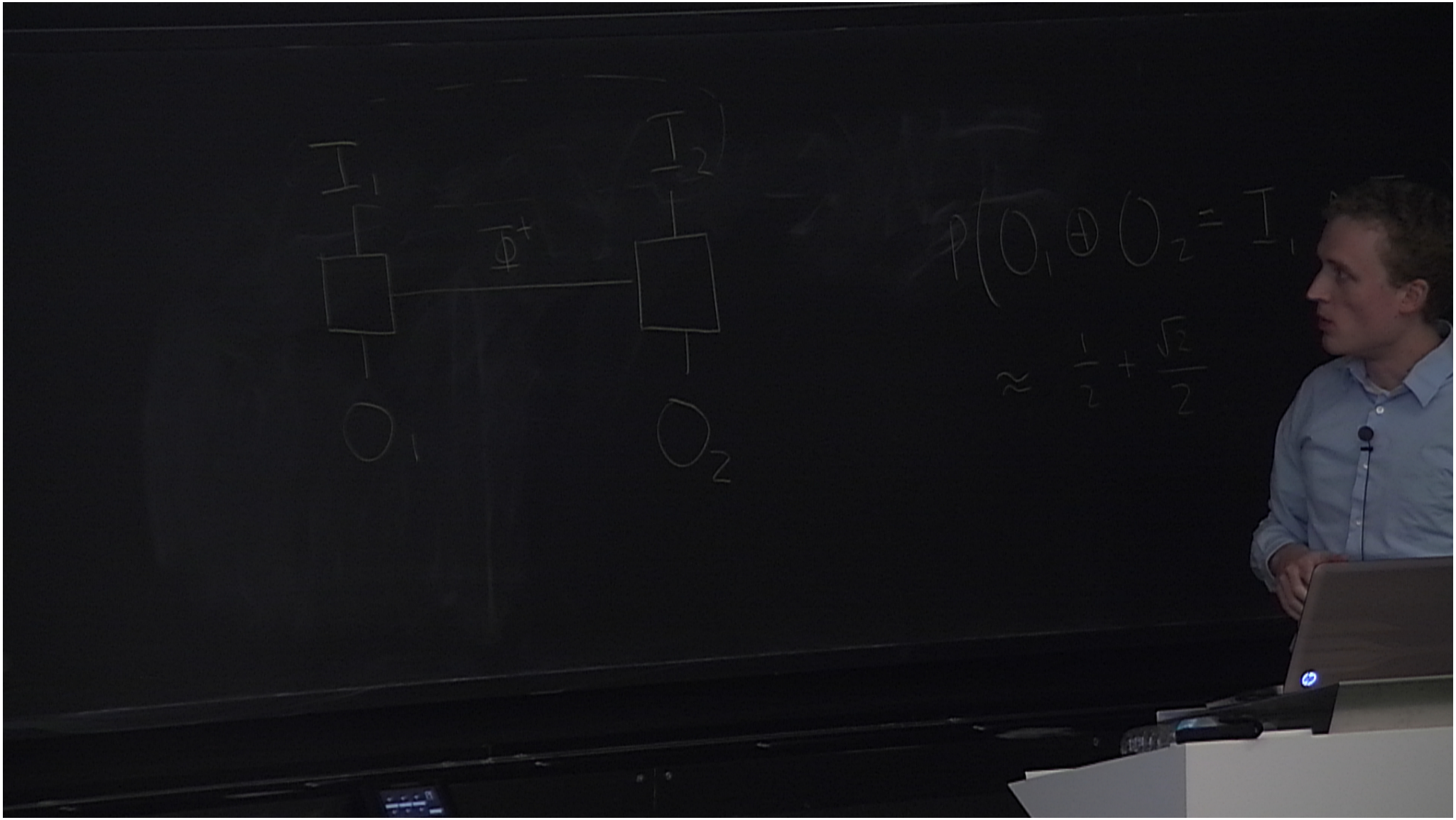
Some motivating problems:

Randomness expansion from an untrusted device.




I1
O1
I2
O2

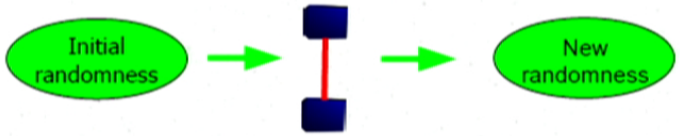

I1
I2
O1
P(O1 ⊕ O2 = I1 ∧ I2
≈ 1/2 + √2/2


I_1
I_2
Φ^+
O_1
O_2
$P(O_1 \otimes O_2 = I_1$
$\approx \frac{1}{2} + \frac{\sqrt{2}}{2}$

Background

Some motivating problems:

Randomness expansion from an untrusted device.

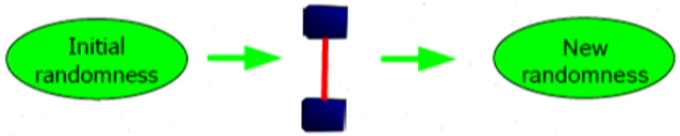


Randomness amplification with an untrusted device.

Background

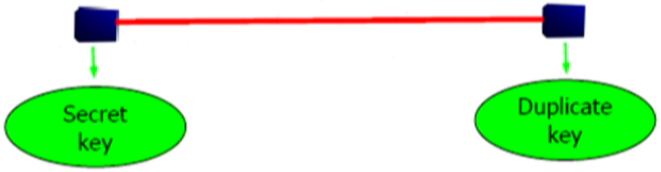
Some motivating problems:

Randomness expansion from an untrusted device.



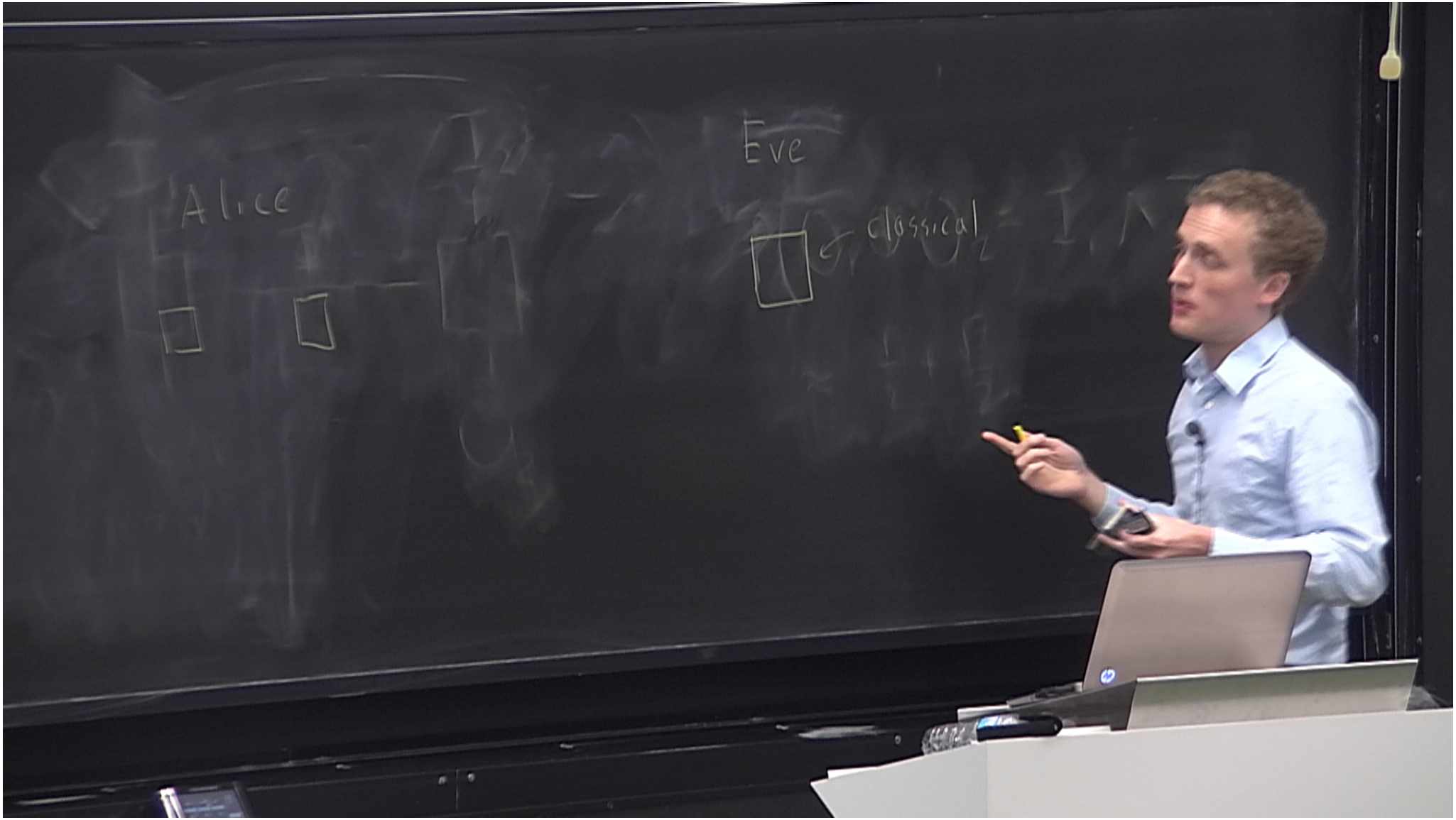
Randomness amplification with an untrusted device.

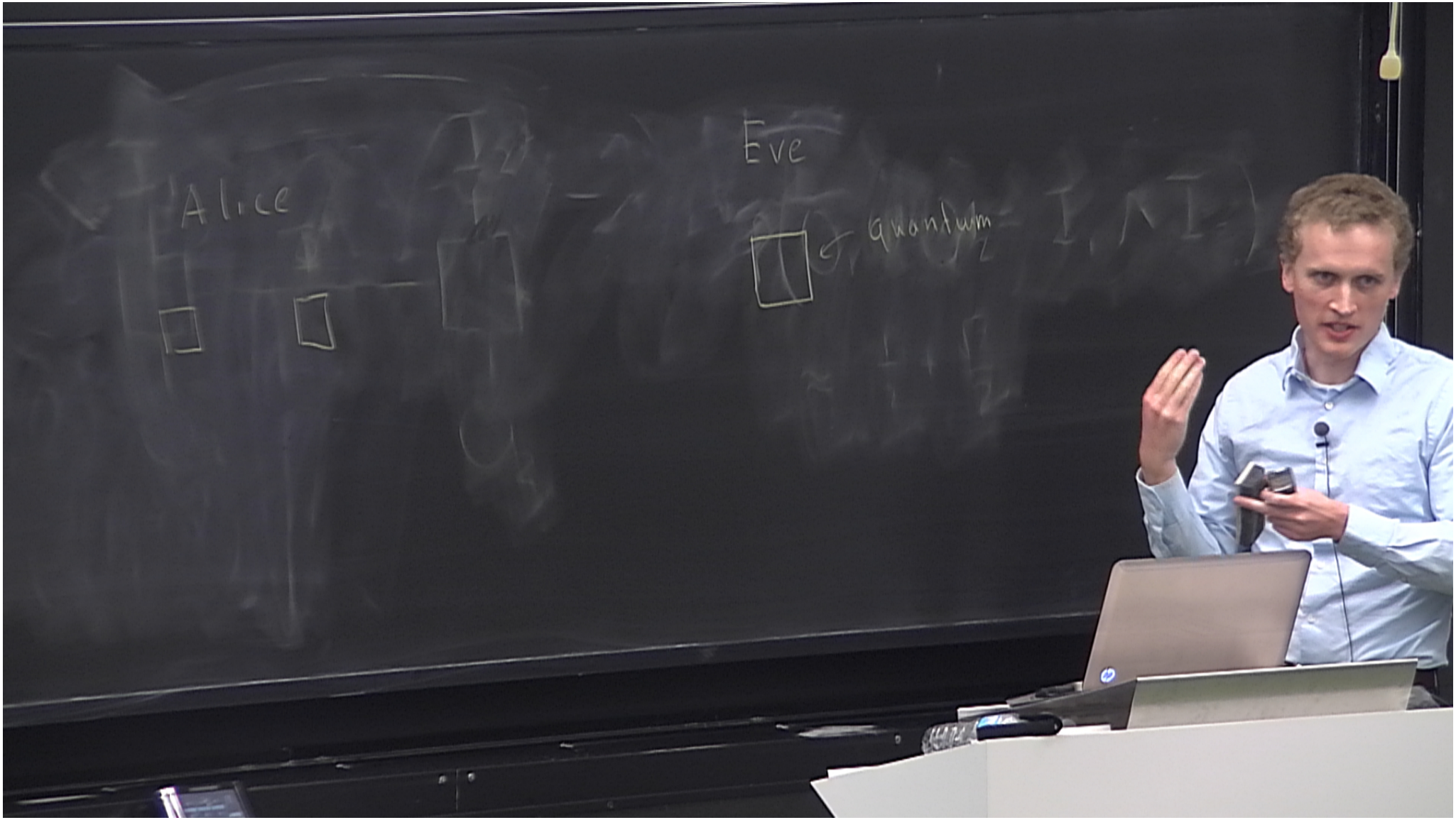
Device-independent QKD.



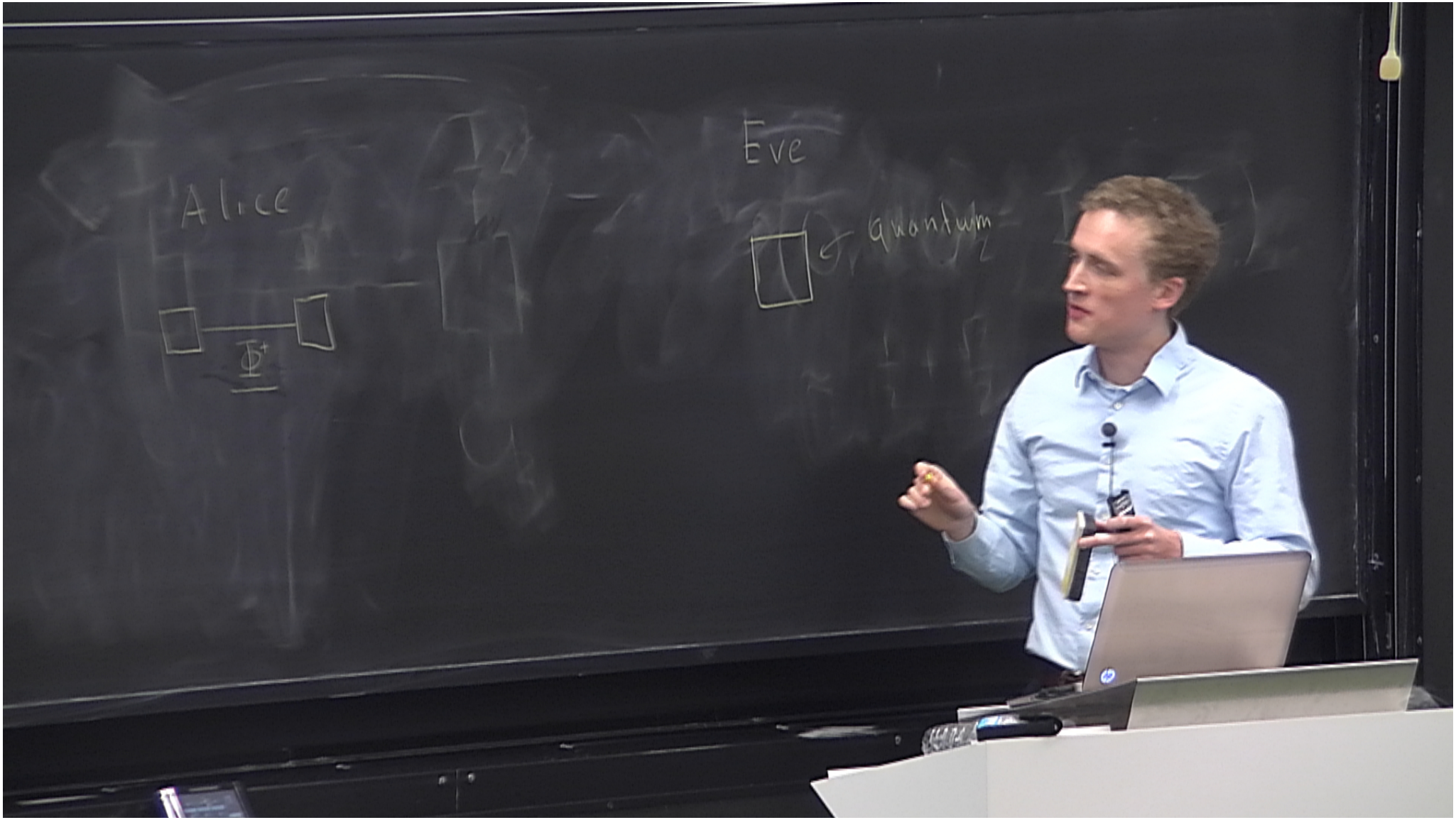
Background

Self-testing results may be critical for proving **quantum** security of device-independent protocols.


Alice
Eve
classical


Alice
Eve
quantum


Alice
Eve
quantum
Φ^+


Alice
Eve
quantum
Φ^+

Background

Some important papers:

[Popescu 1992]: Proves an early result on self-testing for CHSH.

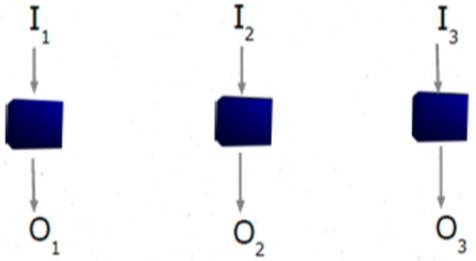
[Mayers, Yao 1998]: Introduces self-testing in the context of QKD.

[Colbeck 2006]: Proves a (non-robust) self-testing result for the GHZ paradox.

[McKague 2012]: Proves a robust self-testing result for CHSH.

Concepts

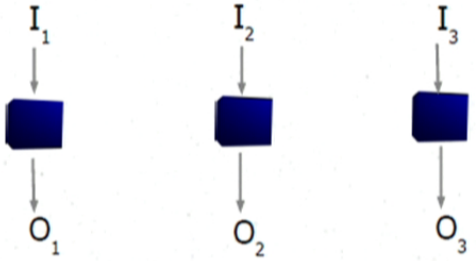
Binary nonlocal XOR games.



The score depends only on the XOR of the outputs.

Concepts

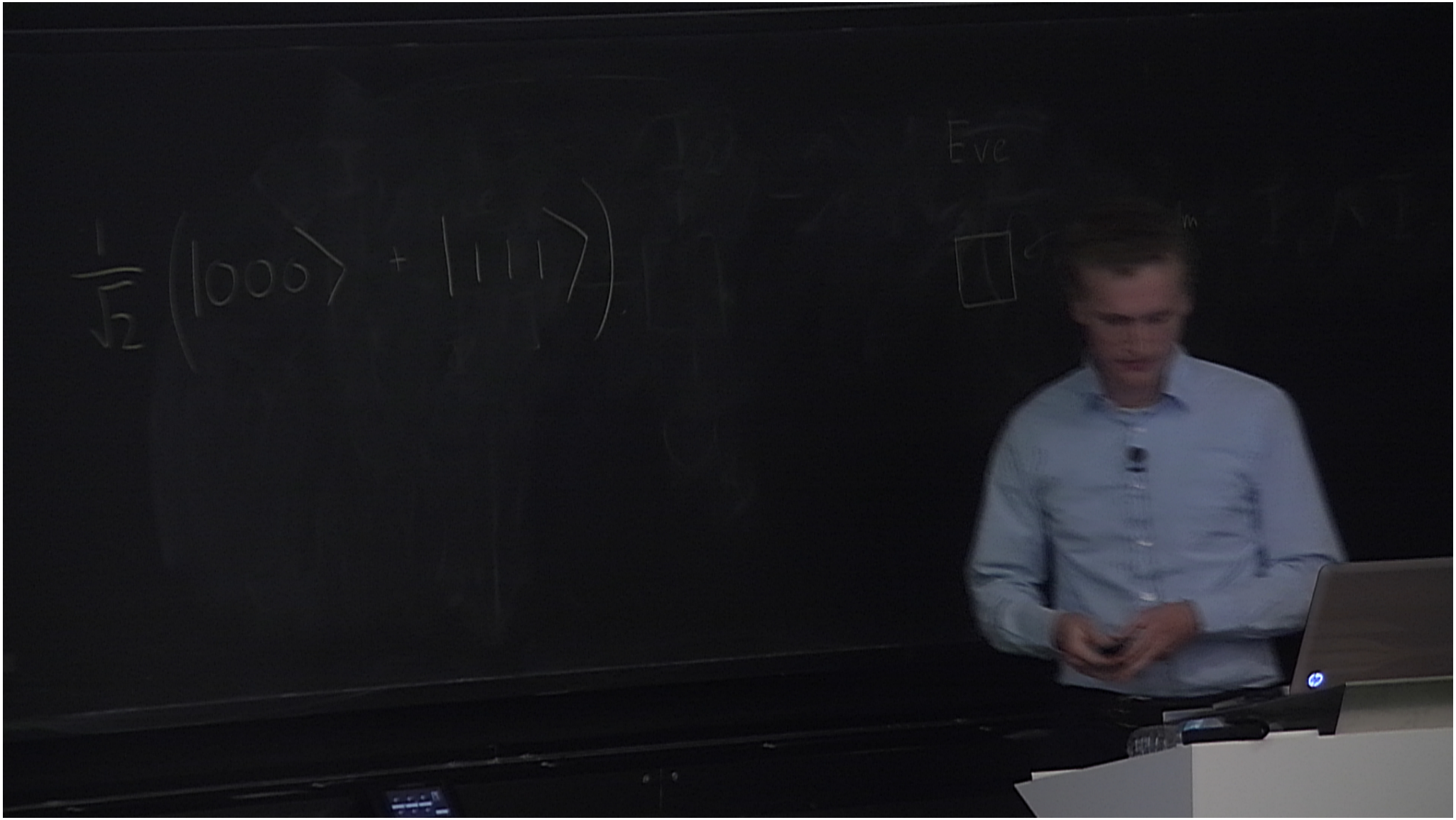
Binary nonlocal XOR games.



The score depends only on the XOR of the outputs.

Example: The GHZ game.

	Score if $O_1 \oplus O_2 \oplus O_3 = 0$	Score if $O_1 \oplus O_2 \oplus O_3 = 1$
000	-1	+1
110	+1	-1
101	+1	-1
011	+1	-1


$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$
Eve

Concepts

Multivariable sinusoidal functions.

To each binary XOR game we associate a function.

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = (+1)\cos(\lambda) + (+1)\cos(\lambda + \theta_2) + (+1)\cos(\lambda + \theta_1) + (-1)\cos(\lambda + \theta_1 + \theta_2).$$

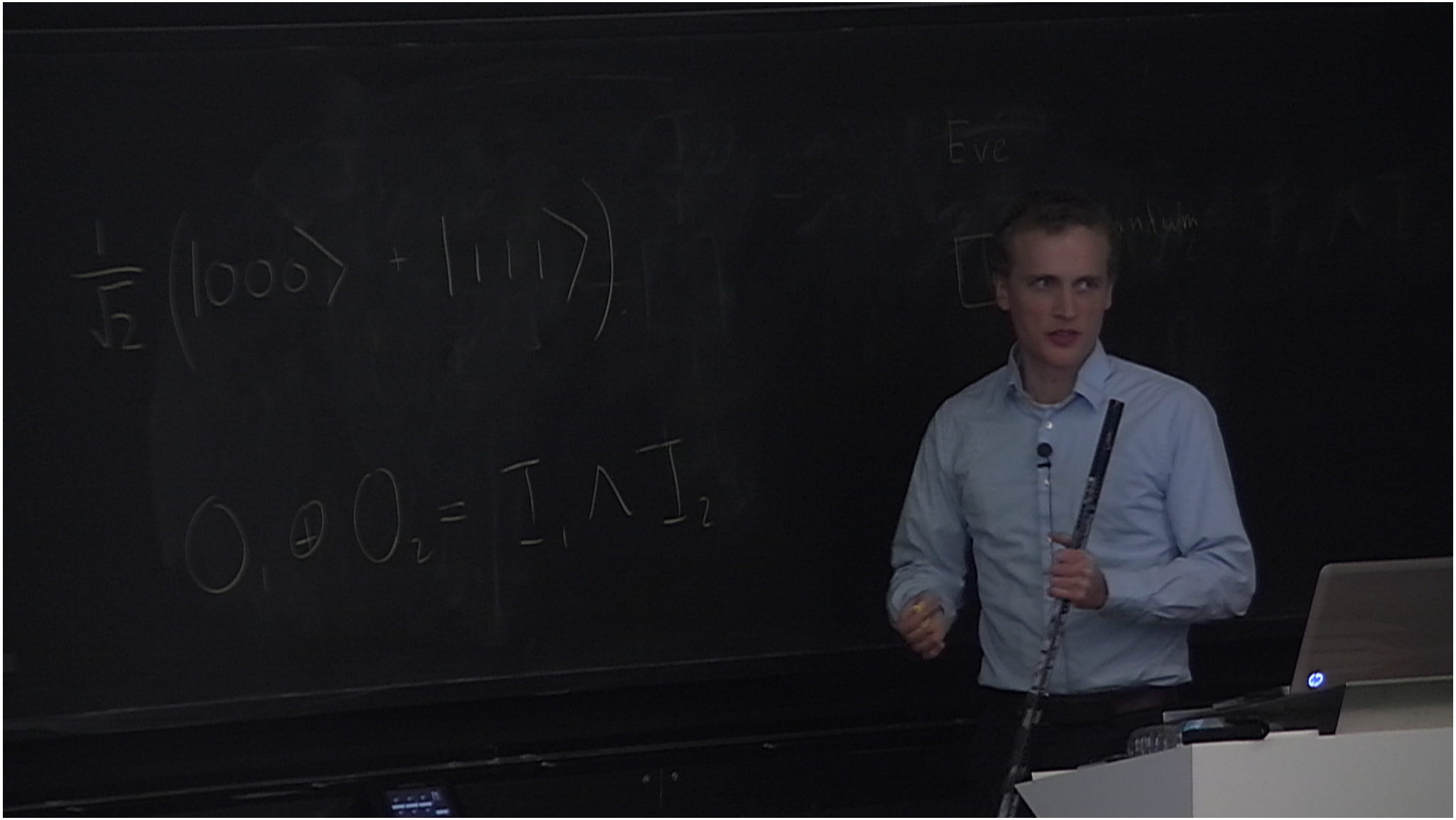
Concepts

Multivariable sinusoidal functions.

To each binary XOR game we associate a function.

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = (+1)\cos(\lambda) \quad \leftarrow \text{Input 00}$$
$$+ (+1)\cos(\lambda + \theta_2) \quad \leftarrow \text{Input 01}$$
$$+ (+1)\cos(\lambda + \theta_1) \quad \leftarrow \text{Input 10}$$
$$+ (-1)\cos(\lambda + \theta_1 + \theta_2). \quad \leftarrow \text{Input 11}$$

Score


Eve

Concepts

Multivariable sinusoidal functions.

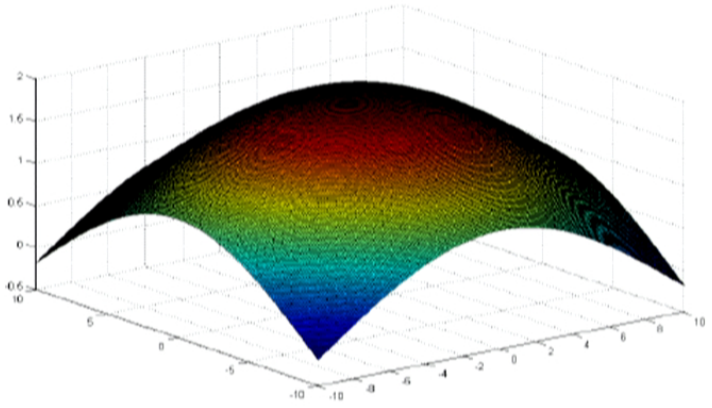
To each binary XOR game we associate a function.

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = (+1)\cos(\lambda) + (+1)\cos(\lambda + \theta_2) + (+1)\cos(\lambda + \theta_1) + (-1)\cos(\lambda + \theta_1 + \theta_2).$$

The values of this function correspond to scores achievable by quantum devices.

Concepts

The Hessian.

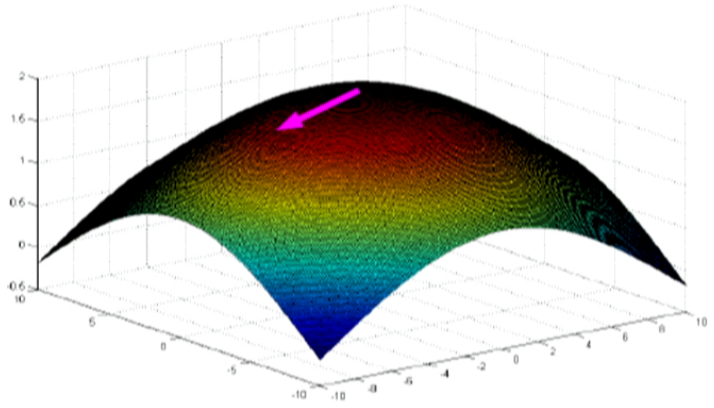


z = F(x,y)

$$H = \begin{bmatrix} \partial^2 F/\partial x^2 & \partial^2 F/\partial x\,\partial y \\ \partial^2 F/\partial x\,\partial y & \partial^2 F/\partial y^2 \end{bmatrix}$$

Concepts

The Hessian.



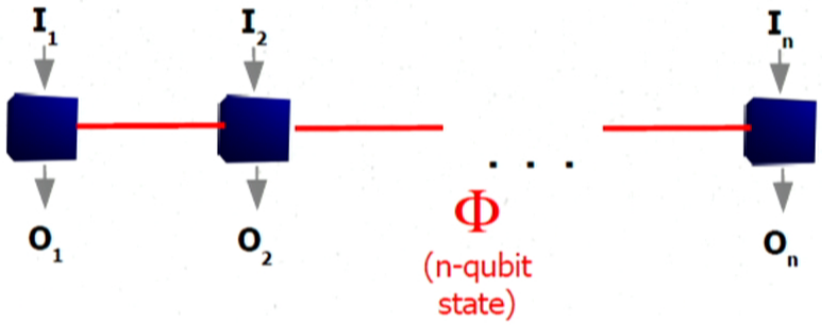
$z = F(x,y)$

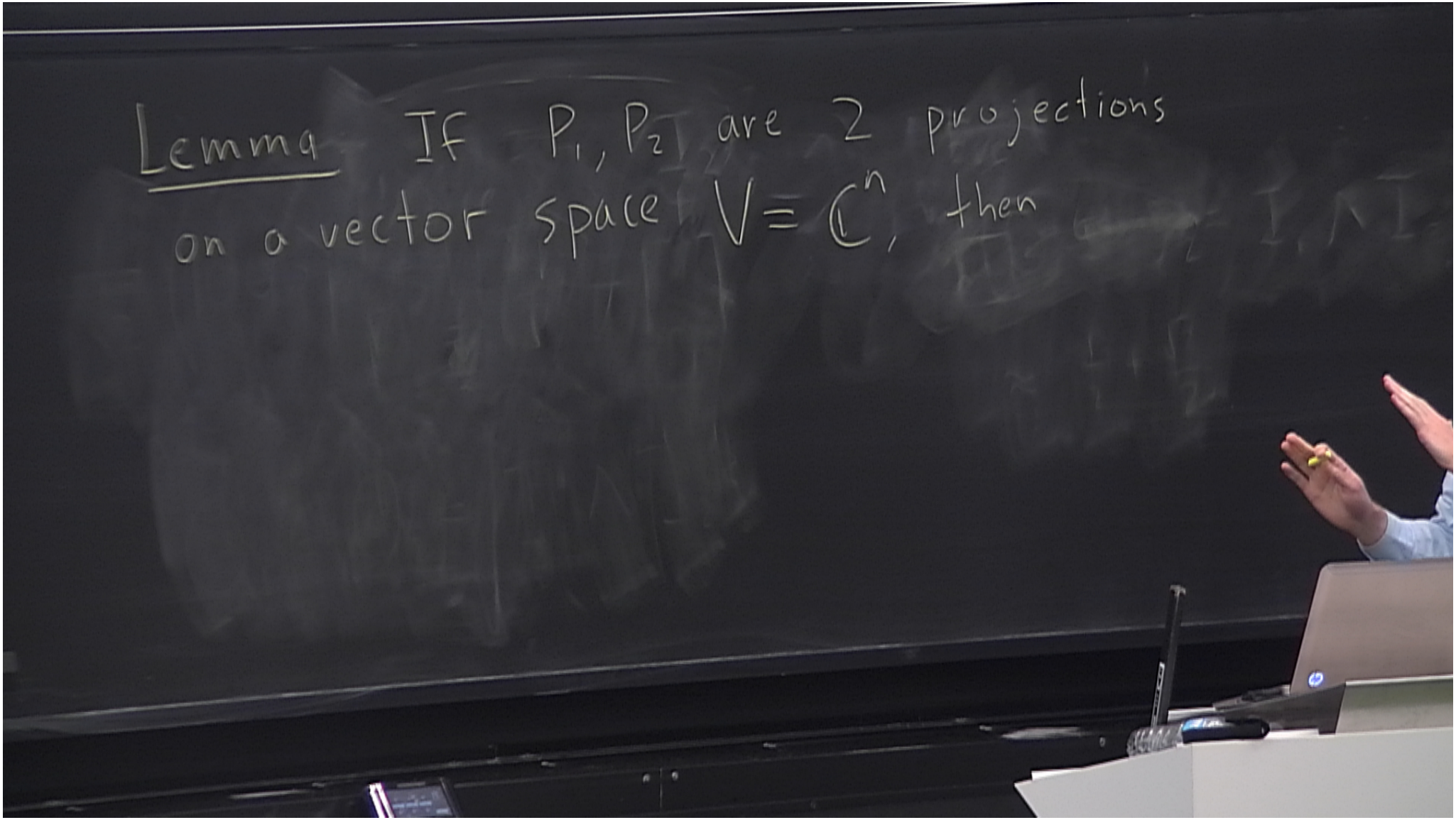
$$H = \begin{bmatrix} \partial^2 F/\partial x^2 & \partial^2 F/\partial x\,\partial y \\ \partial^2 F/\partial x\,\partial y & \partial^2 F/\partial y^2 \end{bmatrix}$$

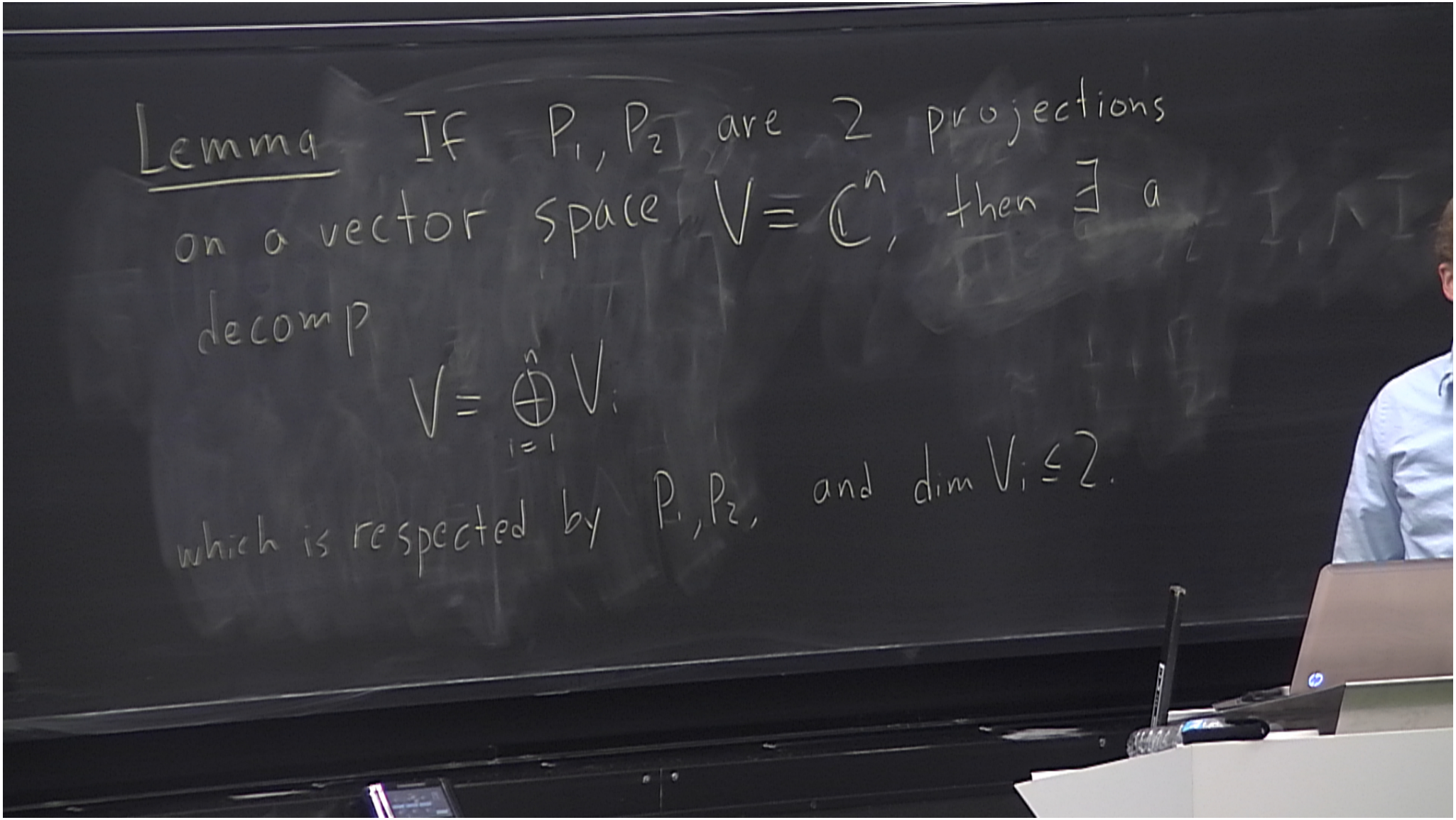
$(v^T H v)$ = second derivative of F in the direction of v

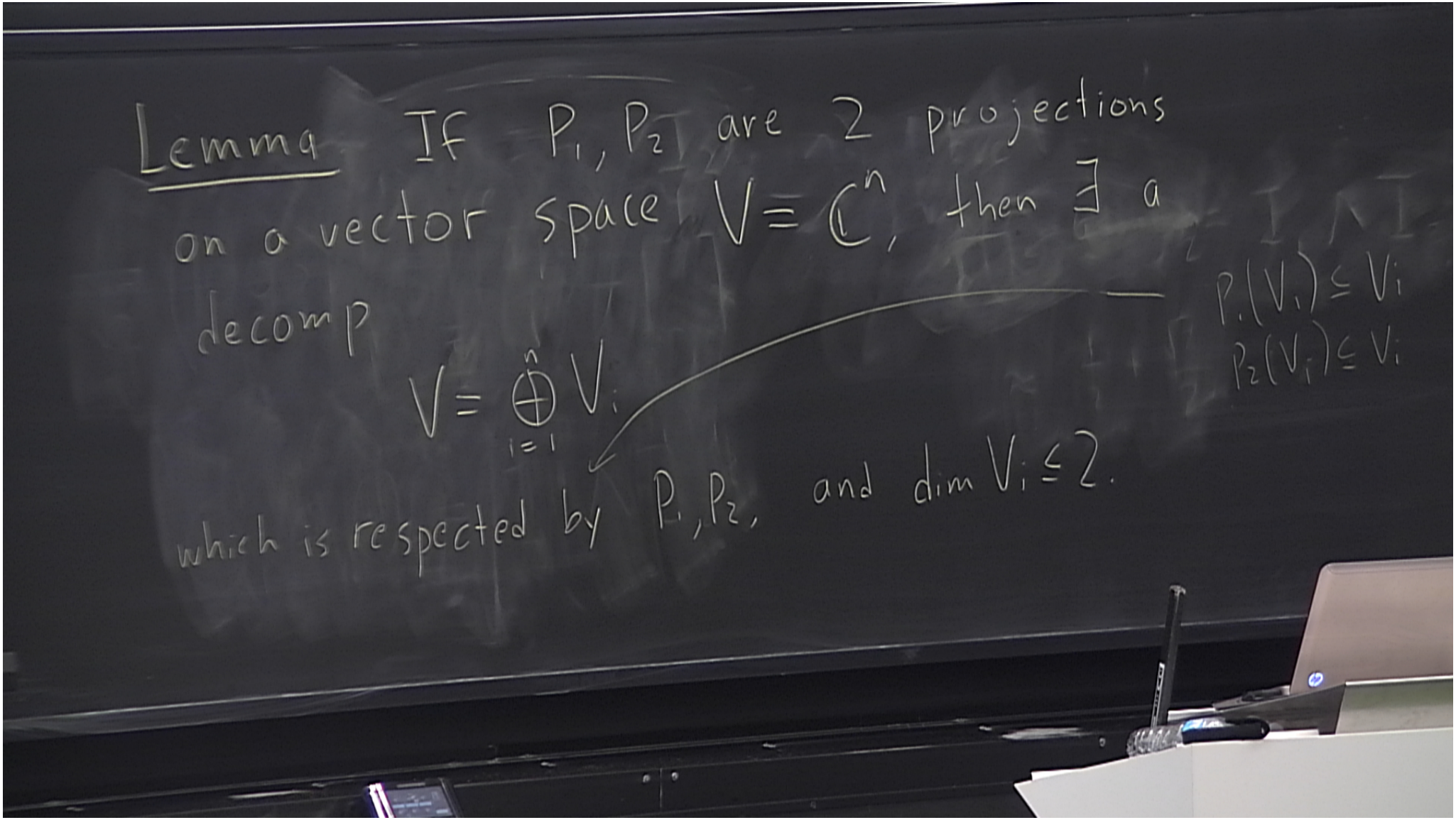
Main result

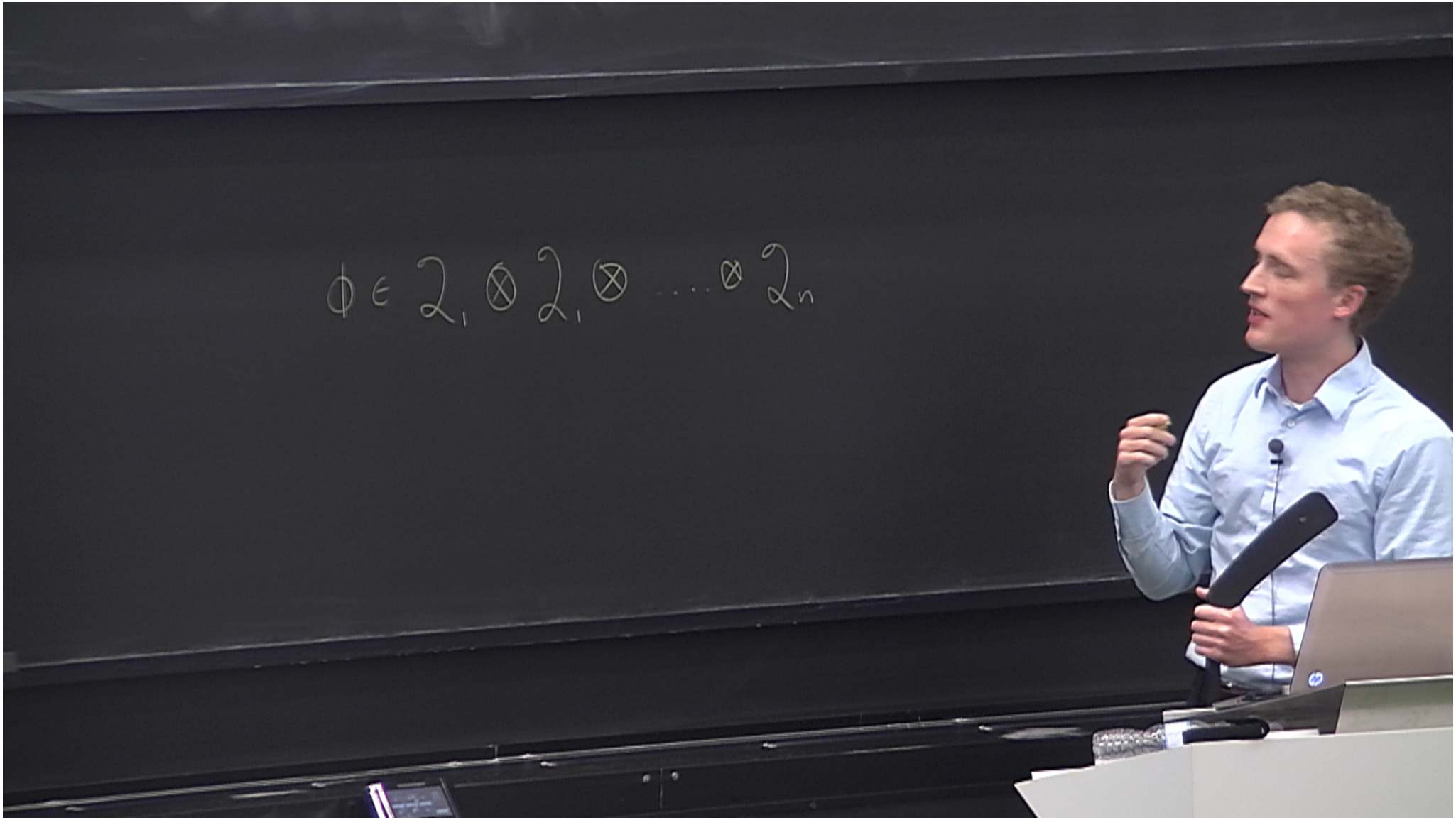
By Jordan's lemma, any self-testing problem involving binary games can be reduced to **qubit** devices.

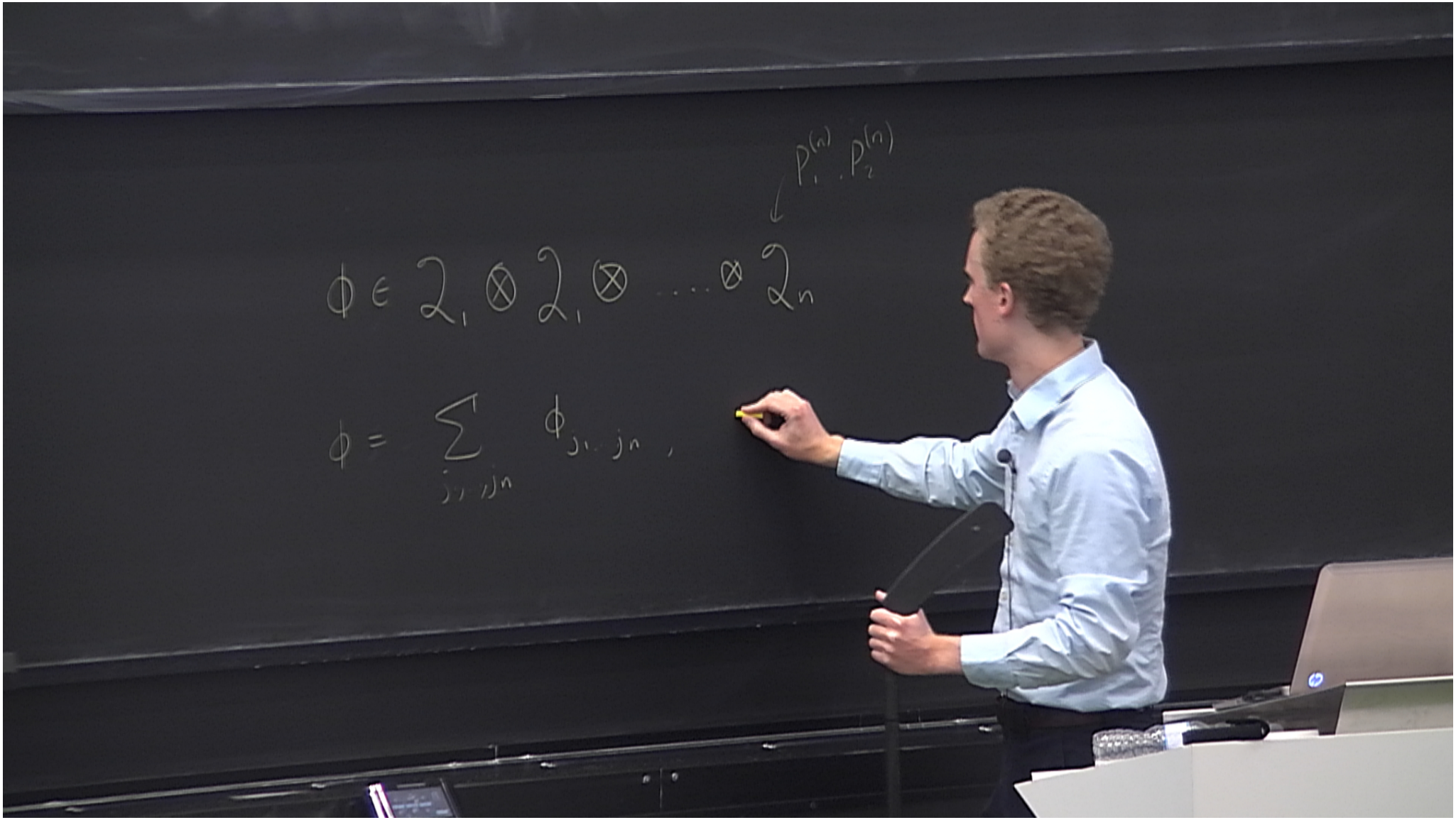


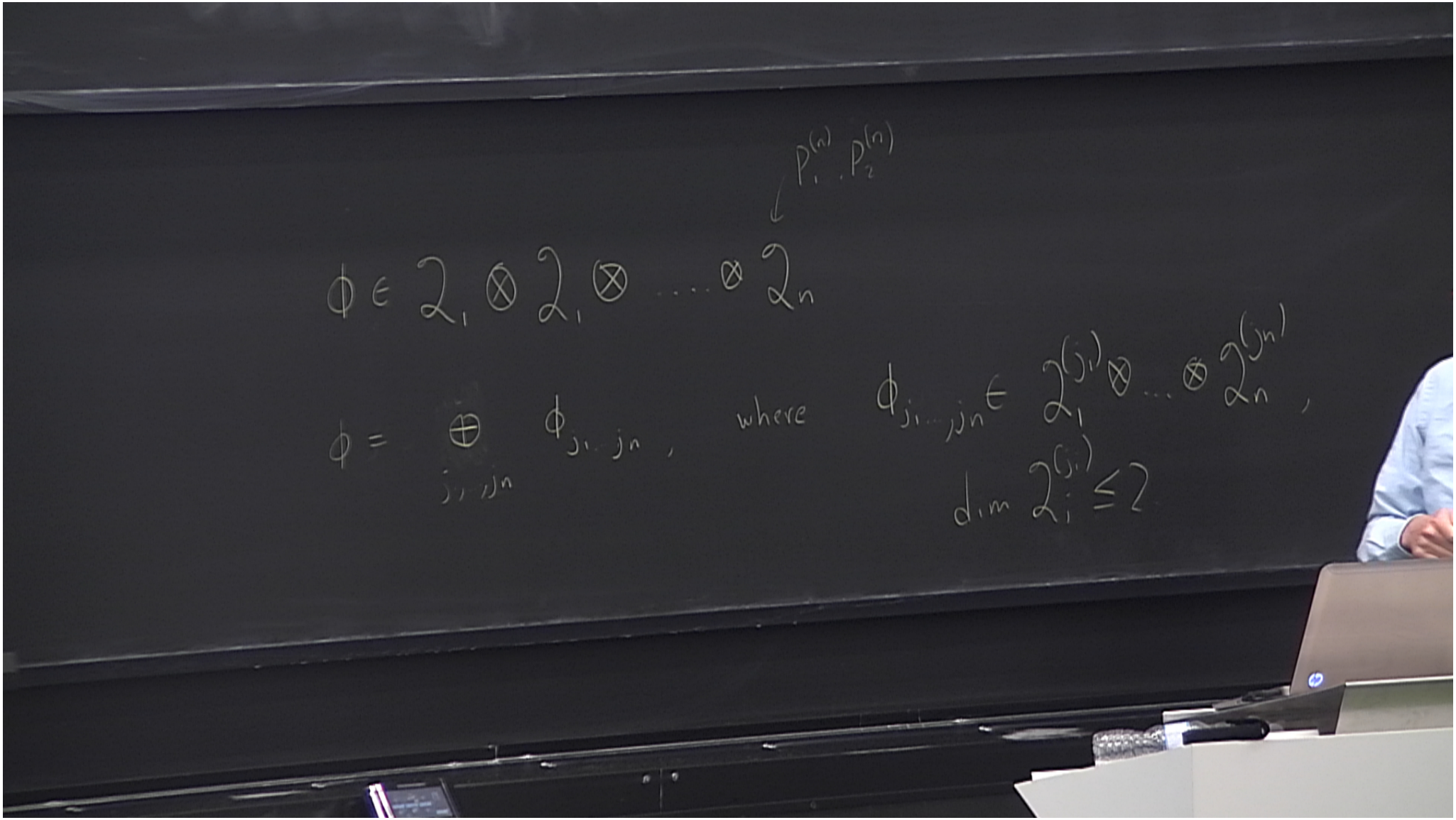

Lemma If P_1, P_2 are 2 projections
on a vector space $V = \mathbb{C}^n$, then


Lemma If P_1, P_2 are 2 projections on a vector space $V = \mathbb{C}^n$, then $\exists$ a decomp
$V = \hat{\bigoplus_{i=1}} V_i$
which is respected by P_1, P_2, and $\dim V_i \leq 2$.


Lemma If P_1, P_2 are 2 projections on a vector space $V = \mathbb{C}^n$, then $\exists$ a decomp
$V = \bigoplus_{i=1}^{n} V_i$
which is respected by P_1, P_2, and $\dim V_i \leq 2$.
$P_1(V_i) \leq V_i$
$P_2(V_i) \leq V_i$

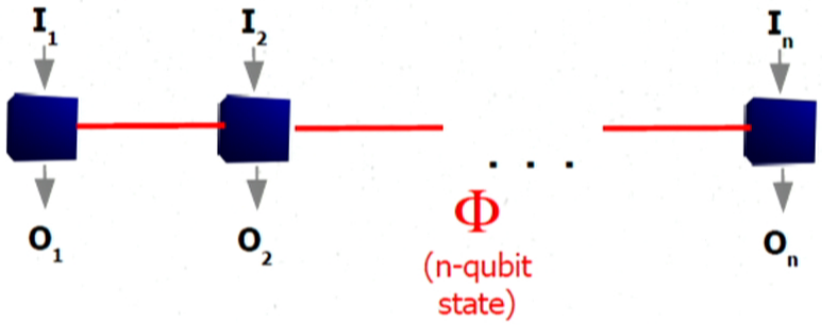

$\phi \in \mathcal{Z}_1 \otimes \mathcal{Z}_1 \otimes \cdots \otimes \mathcal{Z}_n$


$\phi \in \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$
$P_1^{(n)} \cdot P_2^{(n)}$
$\phi = \sum_{j_1 \ldots j_n} \phi_{j_1 \ldots j_n}$


$\phi \in \mathcal{Z}_1 \otimes \mathcal{Z}_1 \otimes \cdots \otimes \mathcal{Z}_n$
$P_1^{(n)} \cdots P_2^{(n)}$
$\phi = \bigoplus_{j_1 \ldots j_n} \phi_{j_1 \ldots j_n}$, where $\phi_{j_1 \ldots j_n} \in \mathcal{Z}_1^{(j_1)} \otimes \cdots \otimes \mathcal{Z}_n^{(j_n)}$,
$\dim \mathcal{Z}_i^{(j_i)} \leq 2$

Main result

By Jordan's lemma, any self-testing problem involving binary games can be reduced to **qubit** devices.



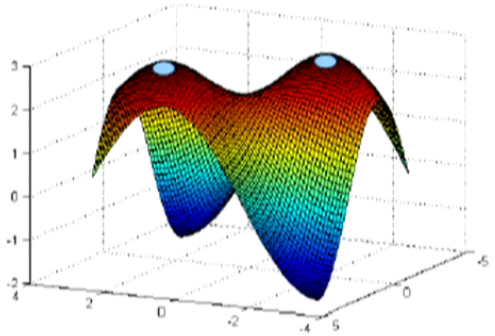
Question: Which binary games have the property that all optimal (qubit) devices behave the same?

Main result

Let S_n be the class of all n-player binary XOR games f such that:

(1) The function Z_f has two maxima in $[-\pi, \pi]^{n+1}$.

(2) The Hessian at each maximum is nonsingular.

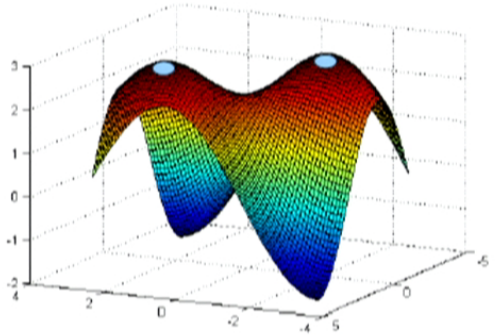


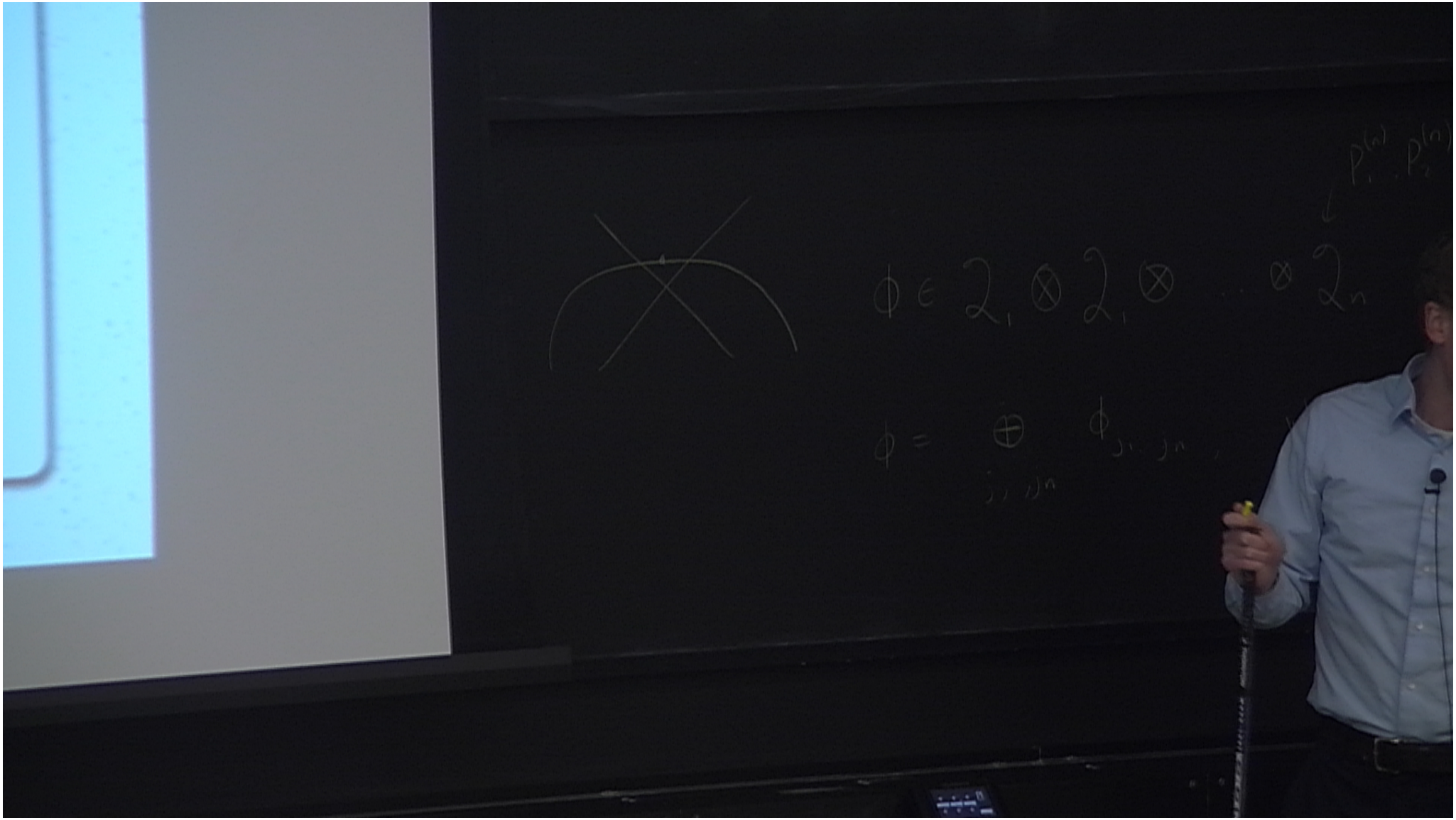
Main result

Let S_n be the class of all n-player binary XOR games f such that:

(1) The function Z_f has two maxima in $[-\pi, \pi]^{n+1}$.

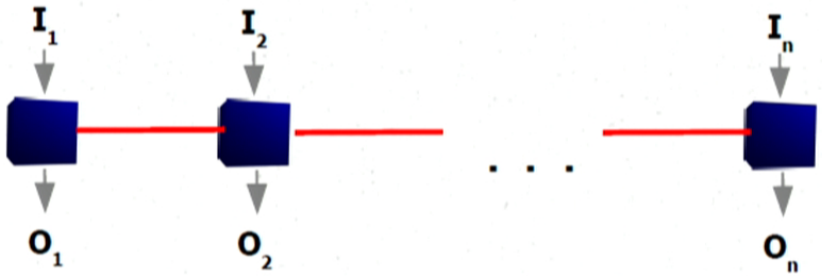
(2) The Hessian at each maximum is nonsingular.




$\phi \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$
$\phi = \bigoplus_{j_1, \ldots, j_n} \phi_{j_1, \ldots, j_n}$

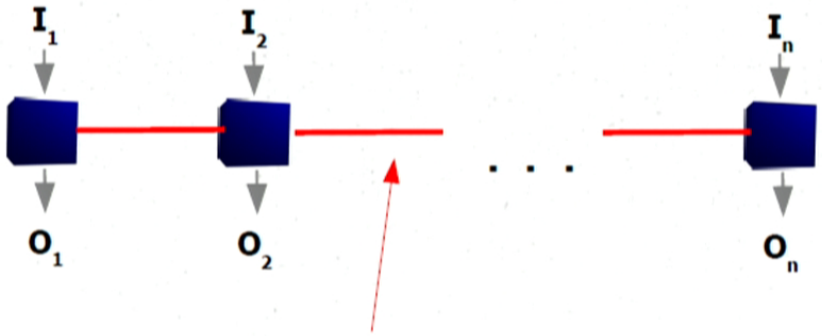
Main result

Proposition 1. Let $f \in S_n$. Then, there is a single optimal qubit device to which all optimal qubit devices are equivalent.



Main result

Proposition 1. Let $f \in S_n$. Then, there is a single optimal qubit device to which all optimal qubit devices are equivalent.



$\Lambda_n = (1/\sqrt{2})[|00\ldots0\rangle + |11\ldots1\rangle]$

(the extended GHZ state)

Main result

Proposition 2. Let $f \in S_n$. Then, for any qubit-device whose score is within ε of optimal, there exists an optimal qubit-device such that

Main result

Proposition 2. Let $f \in S_n$. Then, for any qubit-device whose score is within ε of optimal, there exists an optimal qubit-device such that

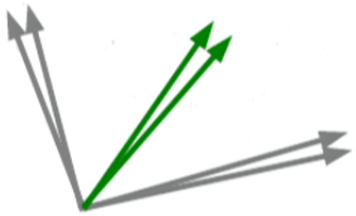
(1) The respective states Φ, Ψ satisfy $|\langle \Phi, \Psi \rangle| \geq 1 - C\varepsilon$.

Main result

Proposition 2. Let $f \in S_n$. Then, for any qubit-device whose score is within ε of optimal, there exists an optimal qubit-device such that

(1) The respective states Φ, Ψ satisfy $|\langle\Phi, \Psi\rangle| \geq 1 - C\varepsilon$.

(2) The respective measurement vectors $\{v_i^{jk}\}$, $\{w_i^{jk}\}$ satisfy $|\langle v_i^{jk}, w_i^{jk}\rangle| \geq 1 - K\varepsilon$. (For some constants C, K.)



Applications

The CHSH game.

Applications

The CHSH game. The function

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = \cos(\lambda) + \cos(\lambda + \theta_2) + \cos(\lambda + \theta_1) - \cos(\lambda + \theta_1 + \theta_2)$$

has two maxima: $(-\pi/4, \pi/2, \pi/2)$ and $(\pi/4, -\pi/2, -\pi/2)$.

Applications

The CHSH game. The function

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = \cos(\lambda) + \cos(\lambda + \theta_2) + \cos(\lambda + \theta_1) - \cos(\lambda + \theta_1 + \theta_2)$$

has two maxima: $(-\pi/4, \pi/2, \pi/2)$ and $(\pi/4, -\pi/2, -\pi/2)$.

The Hessian at these maxima is

$$(1/\sqrt{2}) \begin{bmatrix} -4 & -2 & -2 \\ -2 & -2 & -1 \\ -2 & -1 & -2 \end{bmatrix},$$

which is nonsingular.

Applications

The CHSH game. The function

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = \cos(\lambda) + \cos(\lambda + \theta_2) + \cos(\lambda + \theta_1) - \cos(\lambda + \theta_1 + \theta_2)$$

has two maxima: $(-\pi/4, \pi/2, \pi/2)$ and $(\pi/4, -\pi/2, -\pi/2)$.

The Hessian at these maxima is

$$(1/\sqrt{2}) \begin{bmatrix} -4 & -2 & -2 \\ -2 & -2 & -1 \\ -2 & -1 & -2 \end{bmatrix},$$

which is nonsingular. Thus, CHSH is a robust self-test for the state $\Lambda_2 = (1/\sqrt{2})[|00> + |11>]$.

Applications

The CHSH game. The function

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = \cos(\lambda) + \cos(\lambda + \theta_2) + \cos(\lambda + \theta_1) - \cos(\lambda + \theta_1 + \theta_2)$$

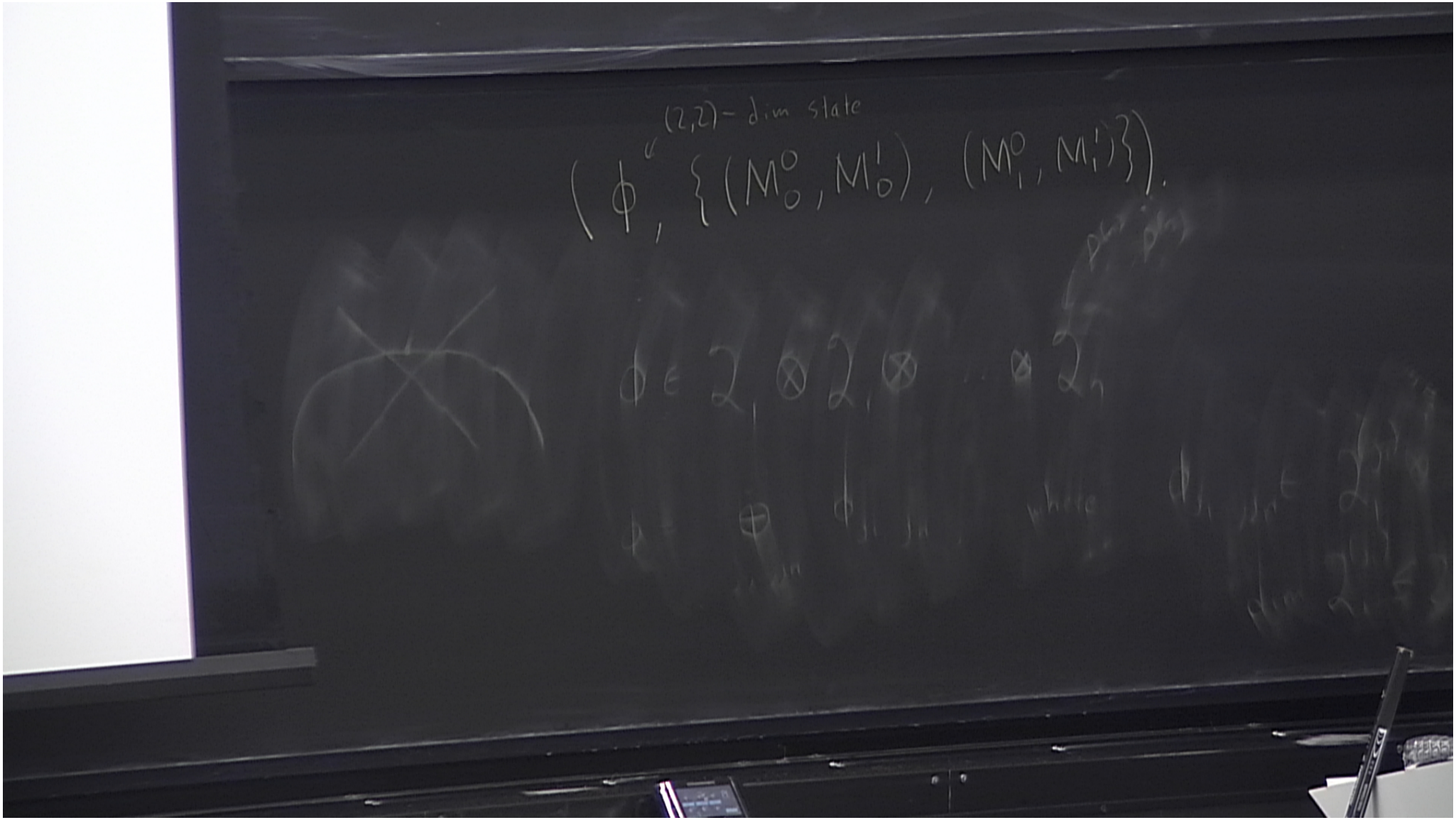
has two maxima: $(-\pi/4, \pi/2, \pi/2)$ and $(\pi/4, -\pi/2, -\pi/2)$.

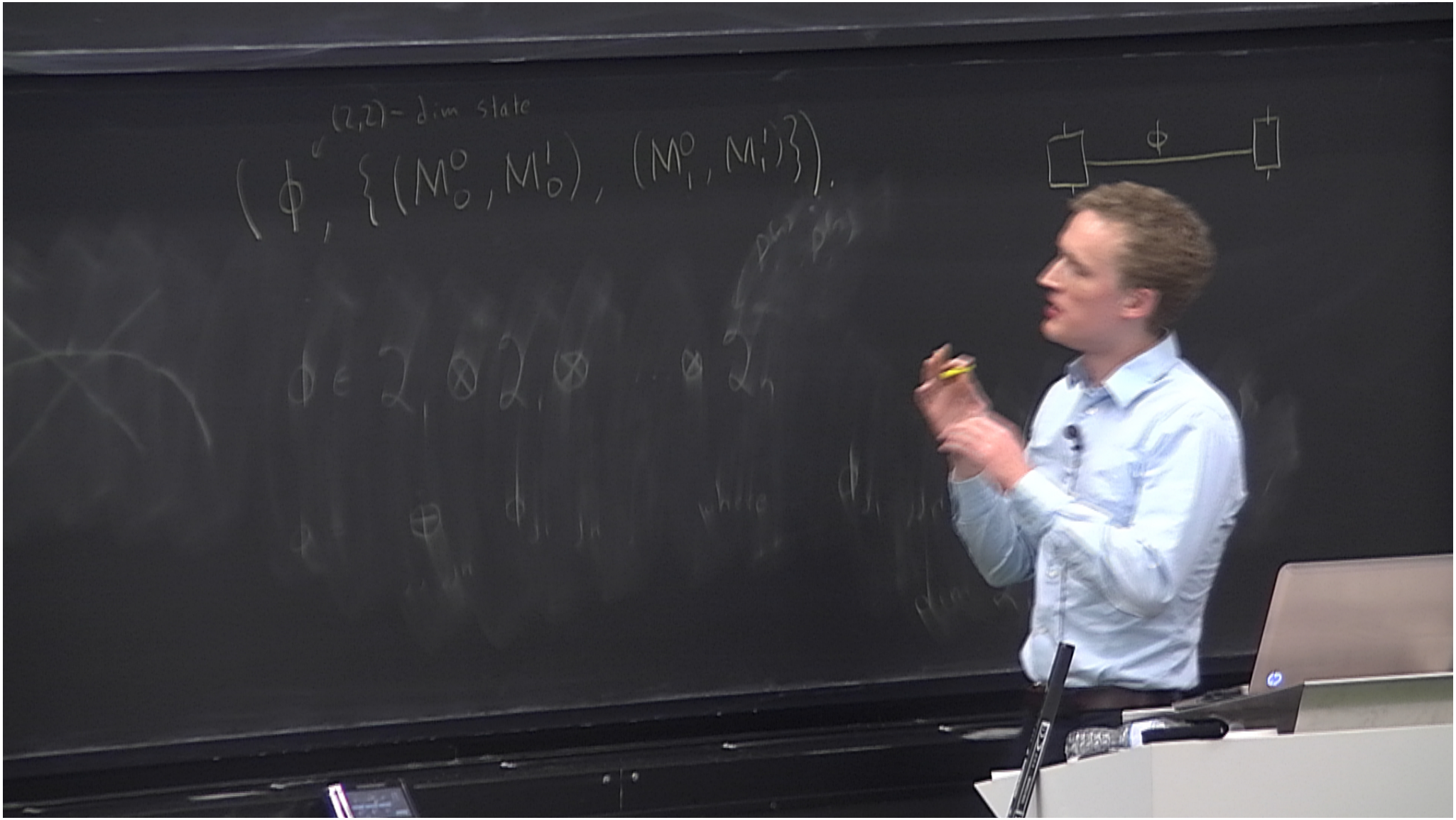
The Hessian at these maxima is

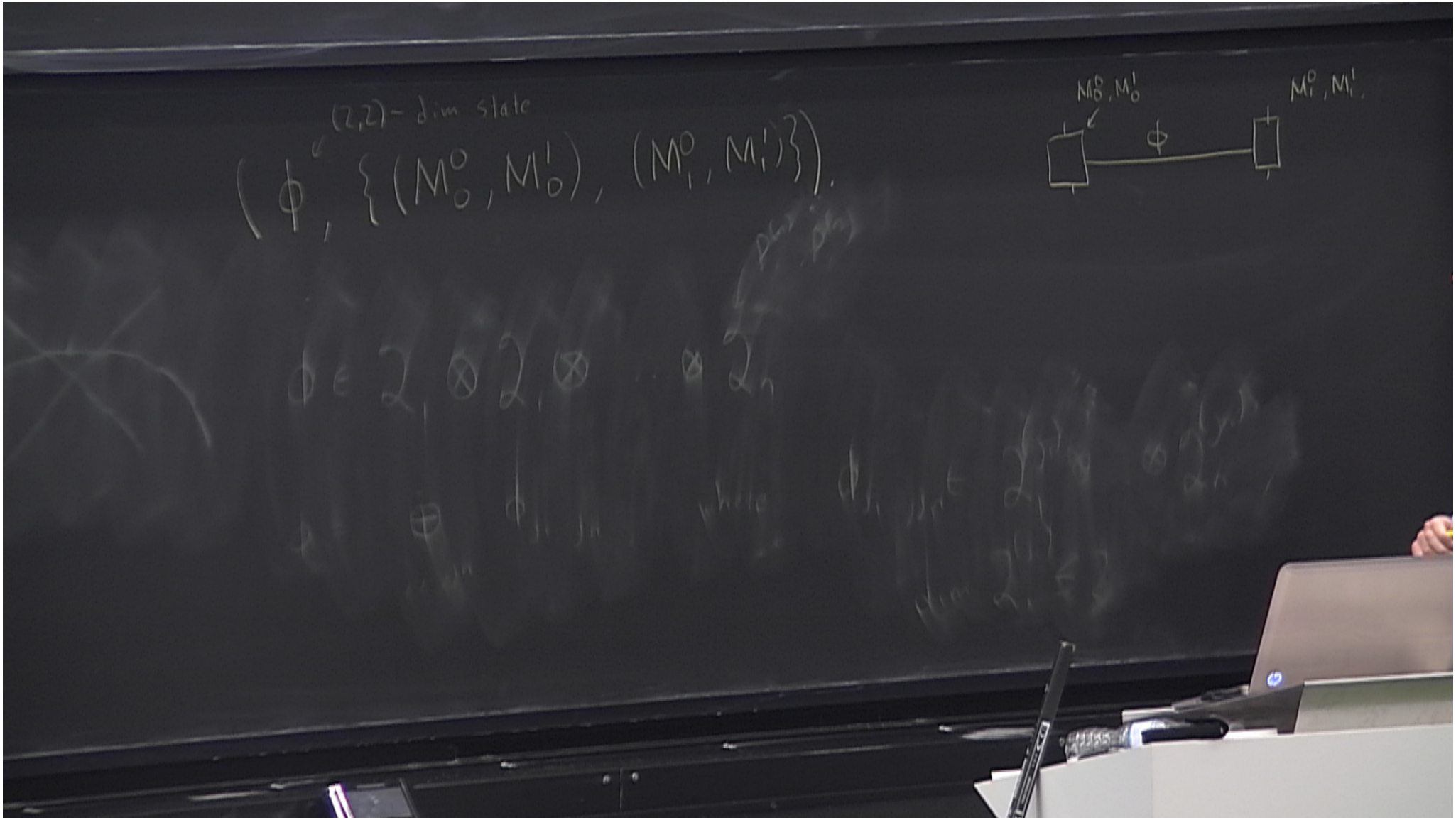
$$(1/\sqrt{2}) \begin{bmatrix} -4 & -2 & -2 \\ -2 & -2 & -1 \\ -2 & -1 & -2 \end{bmatrix},$$

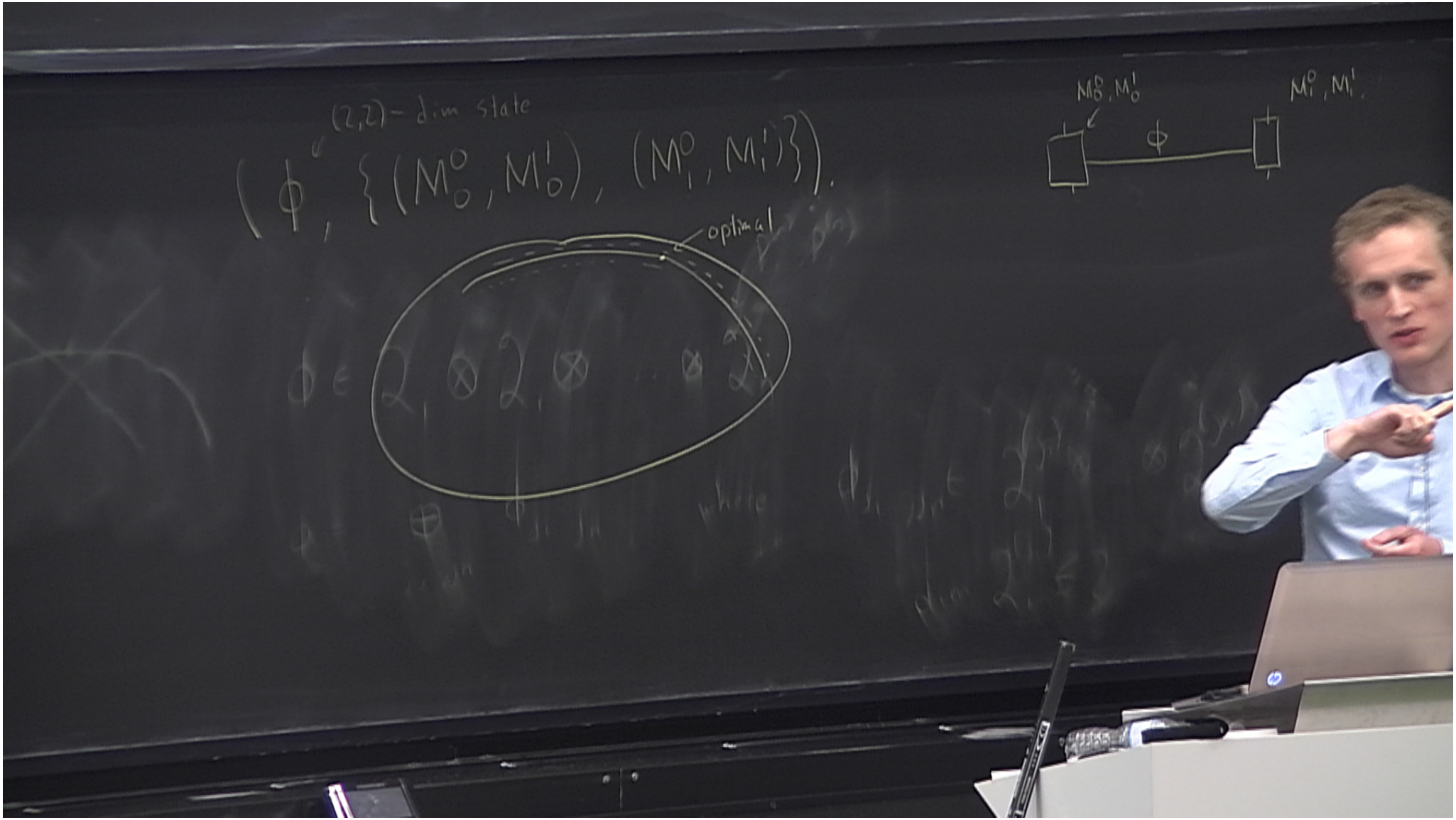
This improves on [McKague 2012] and matches [Reichardt 2012].

which is nonsingular. Thus, CHSH is a robust self-test for the state $\Lambda_2 = (1/\sqrt{2})[|00> + |11>]$.


(2,2)- dim state
$(\phi^{(2,2)}, \{(M^0_0, M^1_0), (M^0_1, M^1_1)\})$.


(2,2)-dim state
$(\phi, \{(M^0_0, M^1_0), (M^0_1, M^1_1)\})$.
$\phi \in 2_1 \otimes 2_2 \otimes \cdots \otimes 2_n$
ϕ


(2,2)-dim state
$(\phi, \{(M^0_0, M^1_0), (M^0_1, M^1_1)\})$
M^0_0, M^1_0
ϕ
M^0_1, M^1_1


(2,2)-dim state
optimal

Applications

The GHZ game.

$$Z_{GHZ}(\lambda, \theta_1, \theta_2) = -\cos(\lambda) + \cos(\lambda + \theta_1 + \theta_2) + \cos(\lambda + \theta_1 + \theta_3) + \cos(\lambda + \theta_2 + \theta_3).$$

The GHZ game is a robust self test. (This is can also be proved from [McKague 2010].)

Applications

Variants of the CHSH game.

Applications

Variants of the CHSH game. Take $\alpha > 1$. Consider the game whose function is

$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = (\alpha)\cos(\lambda) + (\alpha)\cos(\lambda + \theta_2) + \cos(\lambda + \theta_1) - \cos(\lambda + \theta_1 + \theta_2).$$

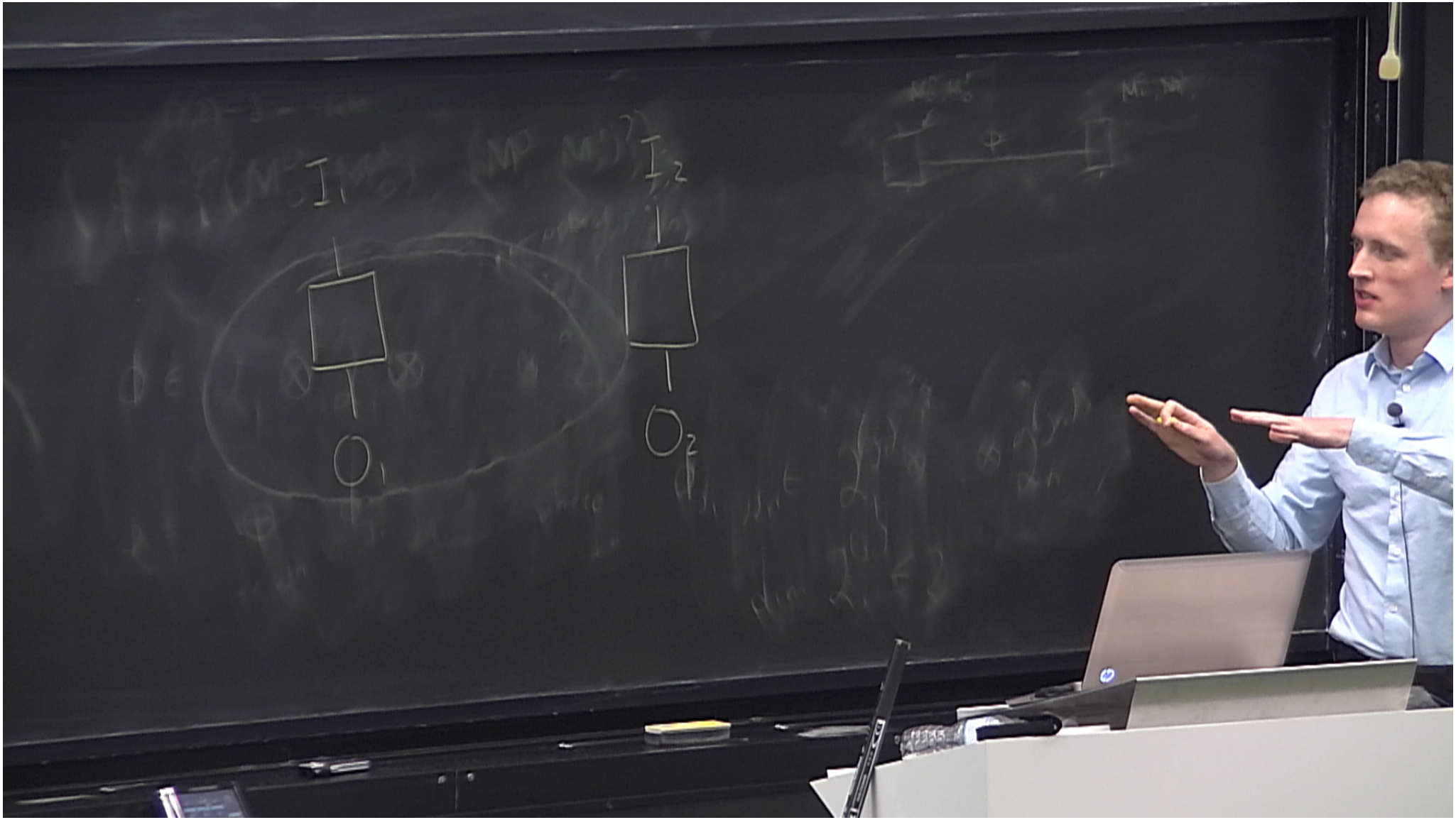
Applications

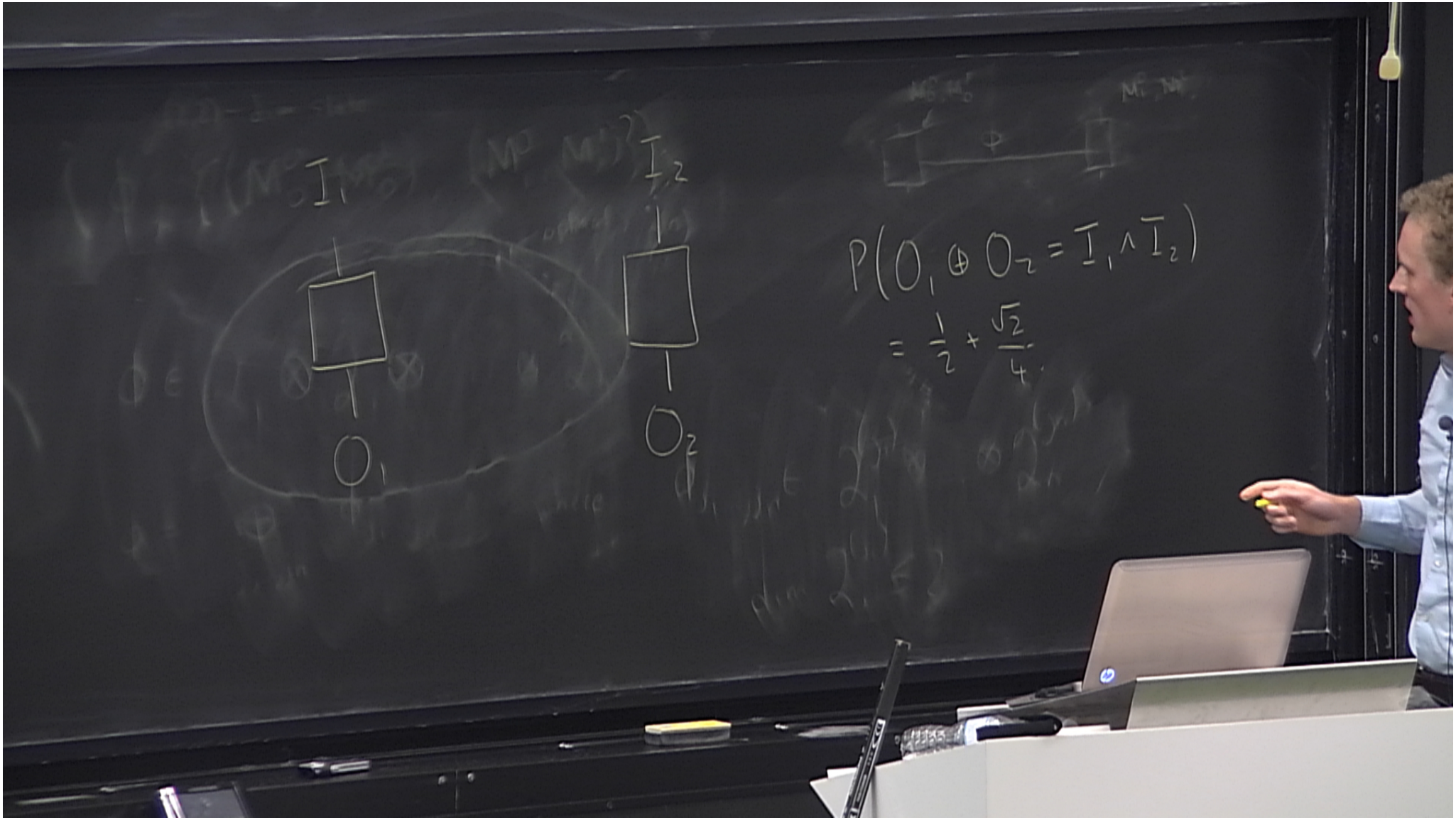
Variants of the CHSH game. Take $\alpha > 1$. Consider the game whose function is

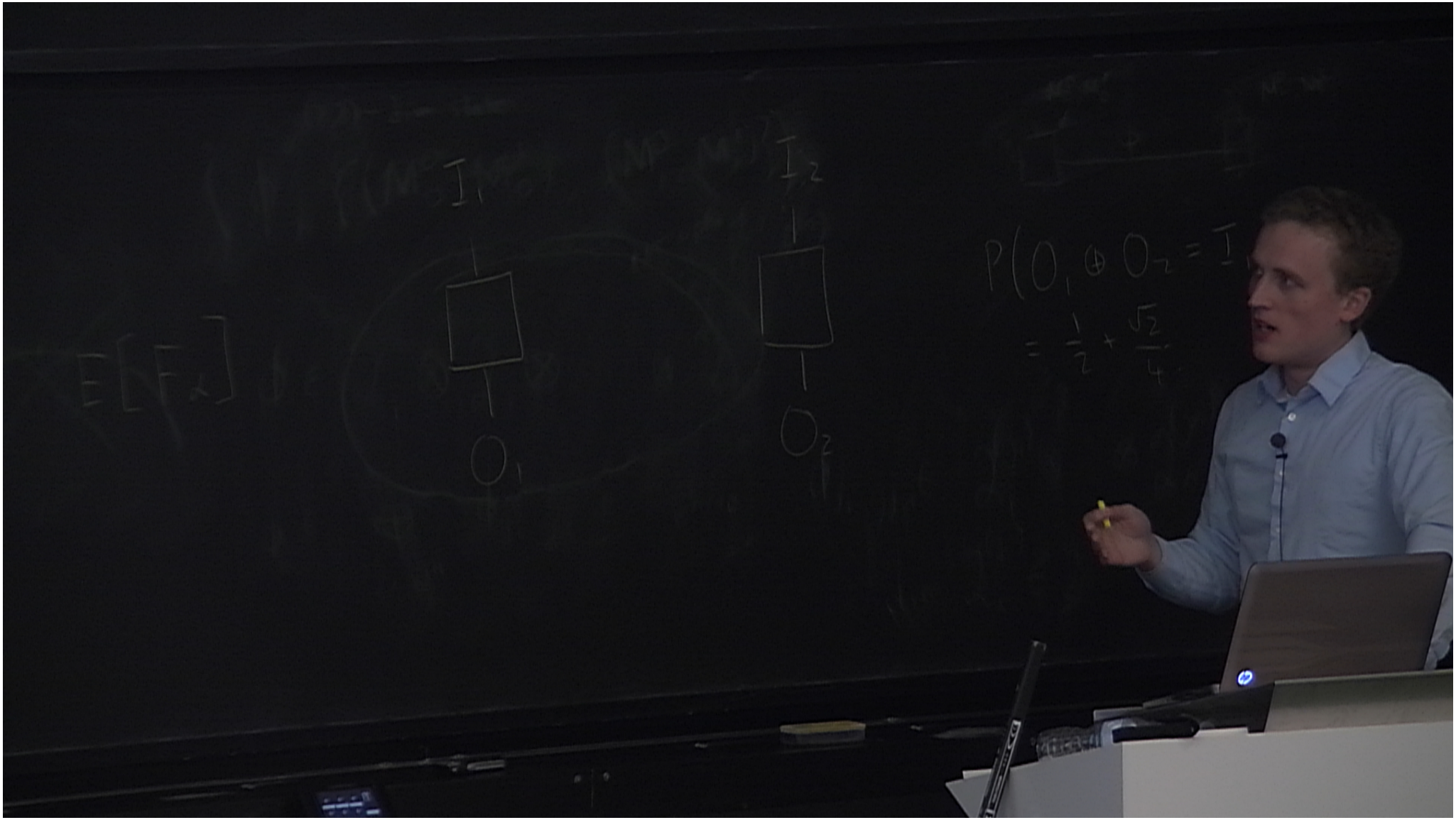
$$Z_{CHSH}(\lambda, \theta_1, \theta_2) = (\alpha)\cos(\lambda) + (\alpha)\cos(\lambda + \theta_2) + \cos(\lambda + \theta_1) - \cos(\lambda + \theta_1 + \theta_2).$$

(This game was proposed in [Acin 2012] in the context of randomness expansion.)

By our criterion, this game is a robust self-test.


I_1
I_2
O_1
O_2

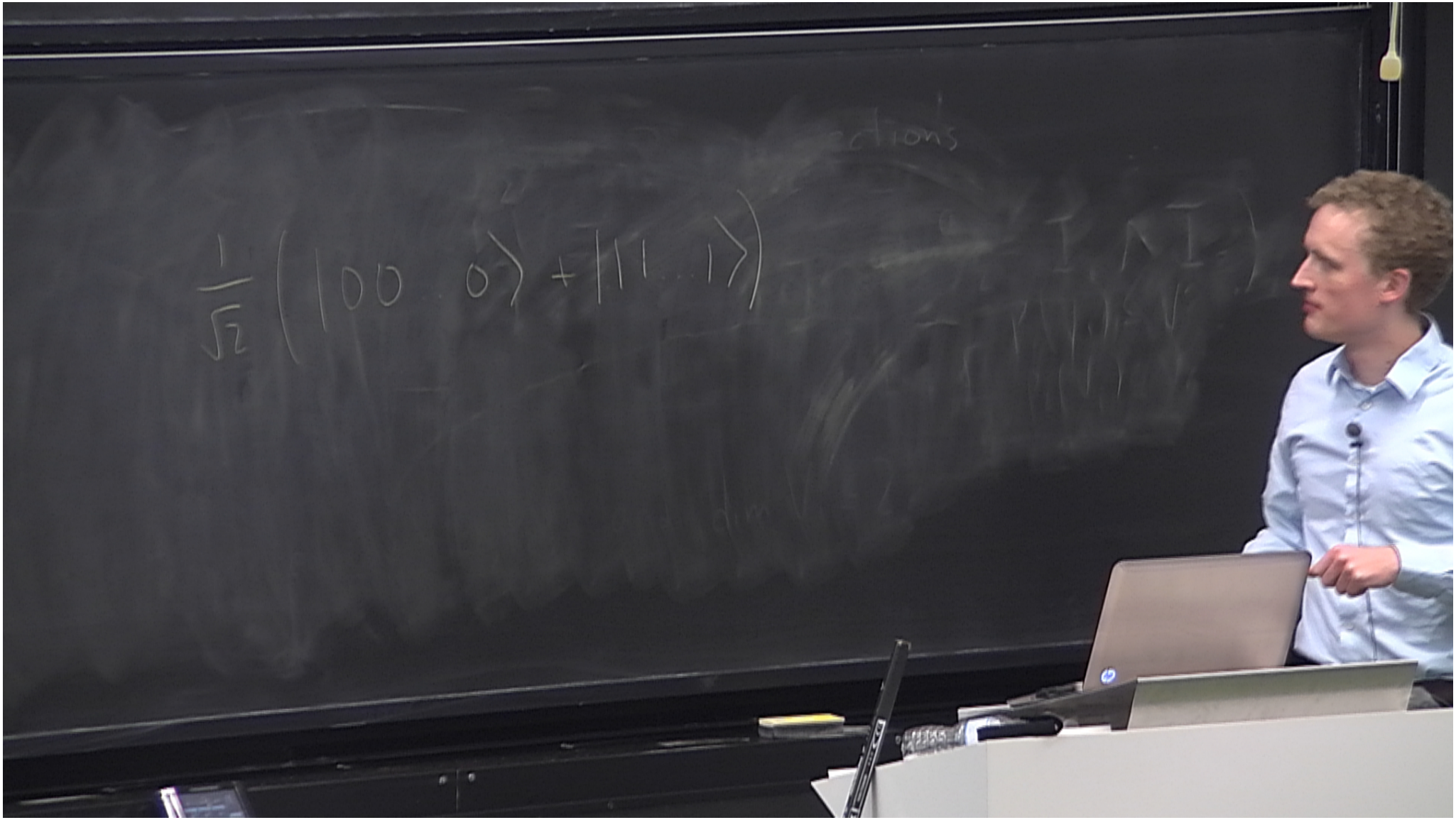

I_1
I_2
O_1
O_2
$P(O_1 \oplus O_2 = I_1 \wedge I_2)$
$= \frac{1}{2} + \frac{\sqrt{2}}{4}$


I_1
I_2
O_1
O_2
$P(O_1 \oplus O_2 = I$
$= \frac{1}{2} + \frac{\sqrt{2}}{4}$


I_1
I_2
$P(O_1 \oplus O_2 = I_1 \wedge I_2)$
$= \frac{1}{2} + \frac{\sqrt{2}}{4}$
$\frac{3}{4}$

Future Goals

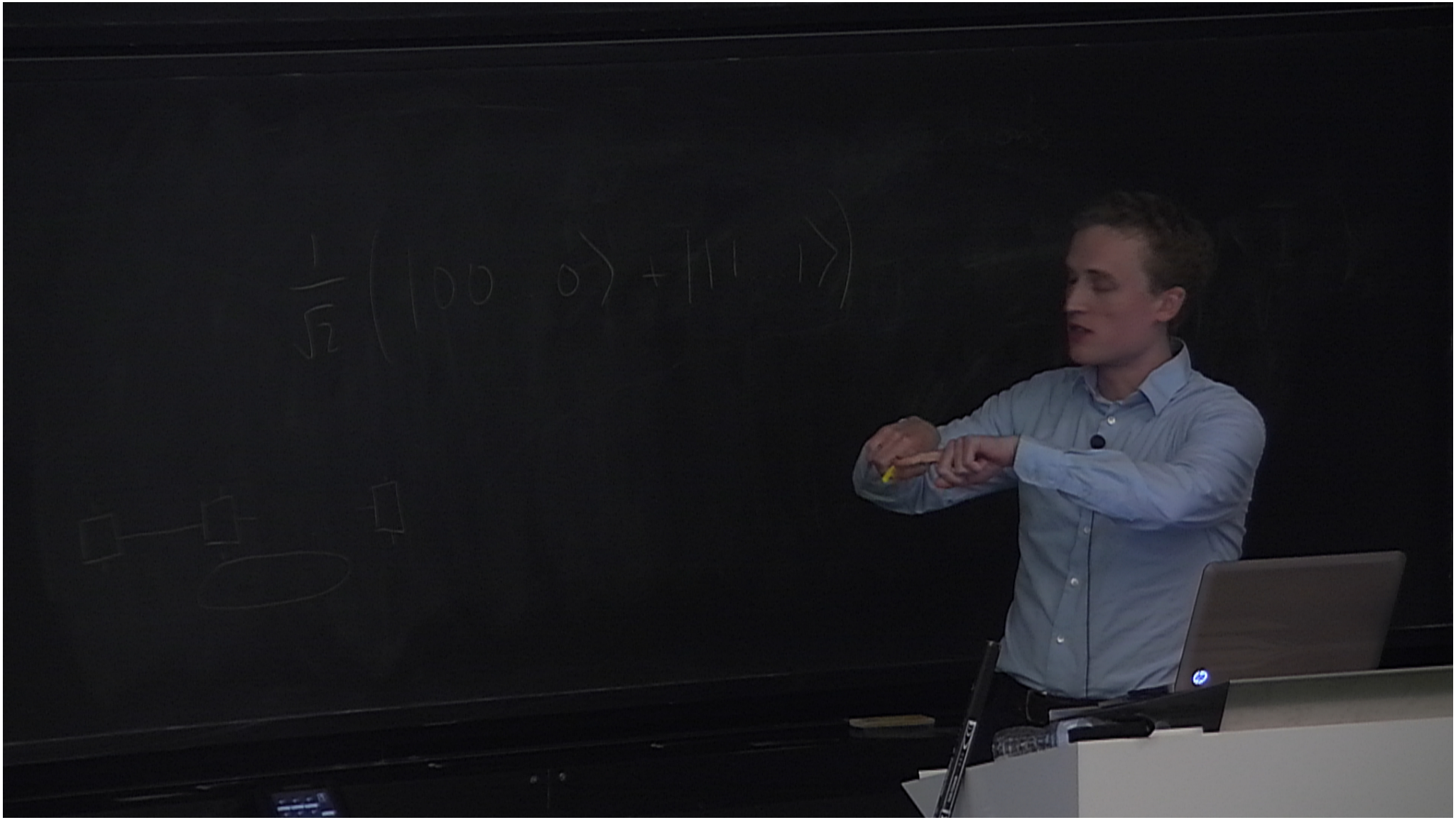
- Prove criteria for robust self-tests of states other than $\{\Lambda_n\}$.


$\frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle)$

Future Goals

- Prove criteria for robust self-tests of states other than $\{\Lambda_n\}$.

M. McKague. Self-testing graph states. arXiv:1010:1989


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

Future Goals

- Prove criteria for robust self-tests of states other than $\{\Lambda_n\}$.

  M. McKague. Self-testing graph states. arXiv:1010:1989

- Devise strong security proofs for randomness expansion, randomness amplification, and QKD.

References

[Miller, Shi 2012] C. Miller, Y. Shi. Robust self-testing quantum states and binary nonlocal XOR games. arXiv:1207.1819.

[Reichardt 2012] B. Reichardt, F. Unger, U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. arXiv:1209.0448

[Acin 2012] A. Acin, S. Massar, S. Pironio. Randomness versus Nonlocality and Entanglement. PRL 108, 100402 (2012).

[McKague 2012] M. McKague, T. Yang, V. Scarani. Robust Self Testing of the Singlet. arXiv:1203.2976.

[McKague 2010] M. McKague. Self-testing graph states. arXiv:1010.1989.

References

[Popescu 1992] S. Popescu, D. Rohrlich. Which states violate Bell's inequality maximally? Physics Letters A 169, no. 6, 411-414. (1992)

[Mayers, Yao 1998] D. Mayers, A. Yao. Quantum Cryptography with Imperfect Apparatus. FOCS 1998, 503-509.

[Colbeck 2006] R. Colbeck. Quantum and Relativistic Protocols for Secure Multi-Party Computation. Ph.D. Thesis, University of Cambridge. (2006)