Title: Does ignorance of the whole imply ignorance of the parts?

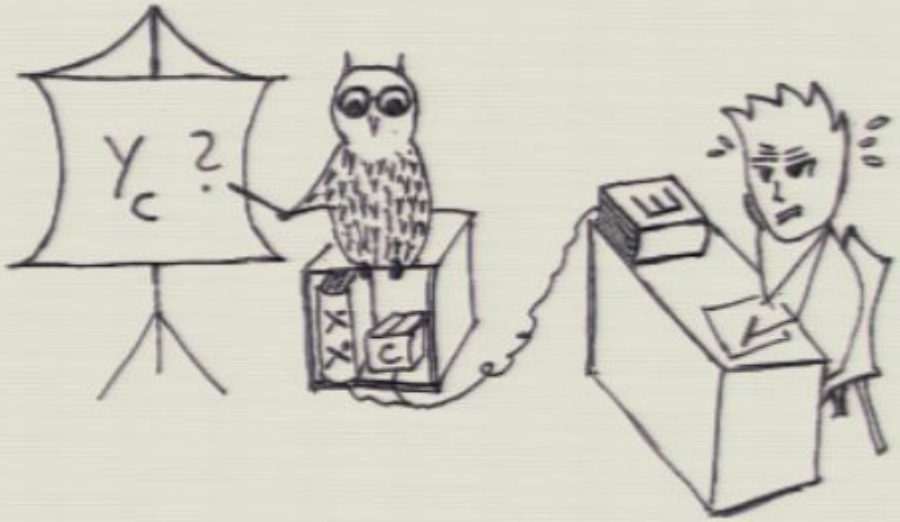
Date: May 12, 2011 05:00 PM

URL: http://pirsa.org/11050049

Abstract: A central question in our understanding of the physical world is how our knowledge of the whole relates to our knowledge of the individual parts. One aspect of this question is the following: to what extent does ignorance about a whole preclude knowledge of at least one of its parts? Relying purely on classical intuition, one would certainly be inclined to conjecture that a strong ignorance of the whole cannot come without significant ignorance of at least one of its parts. Indeed, we show that this reasoning holds in any non-contextual hidden variable model (NC-HV). Curiously, however, such a conjecture is false in quantum theory: we provide an explicit example where a large ignorance about the whole can coexist with an almost perfect knowledge of each of its parts. More specifically, we provide a simple information-theoretic inequality satisfied in any NC-HV, but which can be arbitrarily violated by quantum mechanics. Our inequality has interesting implications for quantum cryptography.

Does ignorance of the whole imply ignorance of the parts?

Stephanie Wehner



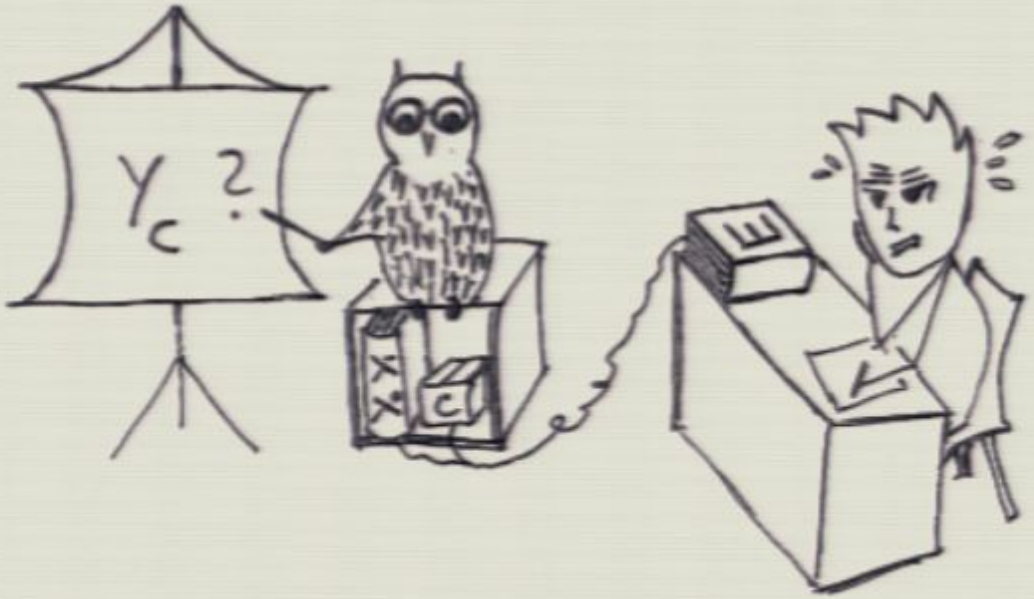
Joint work with Thomas Vidick

arXiv:1011.6448

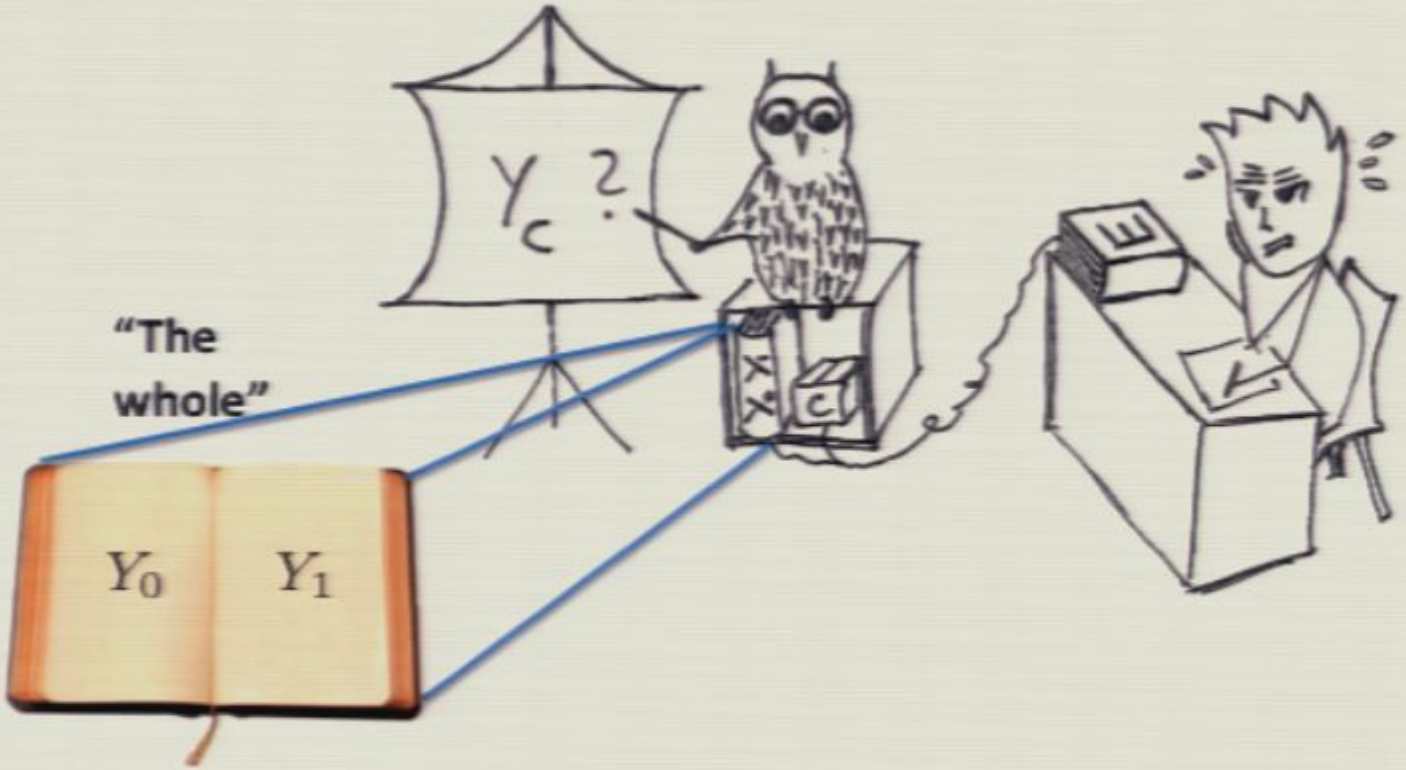
Centre for Quantum Technologies

NUS National University of Singapore

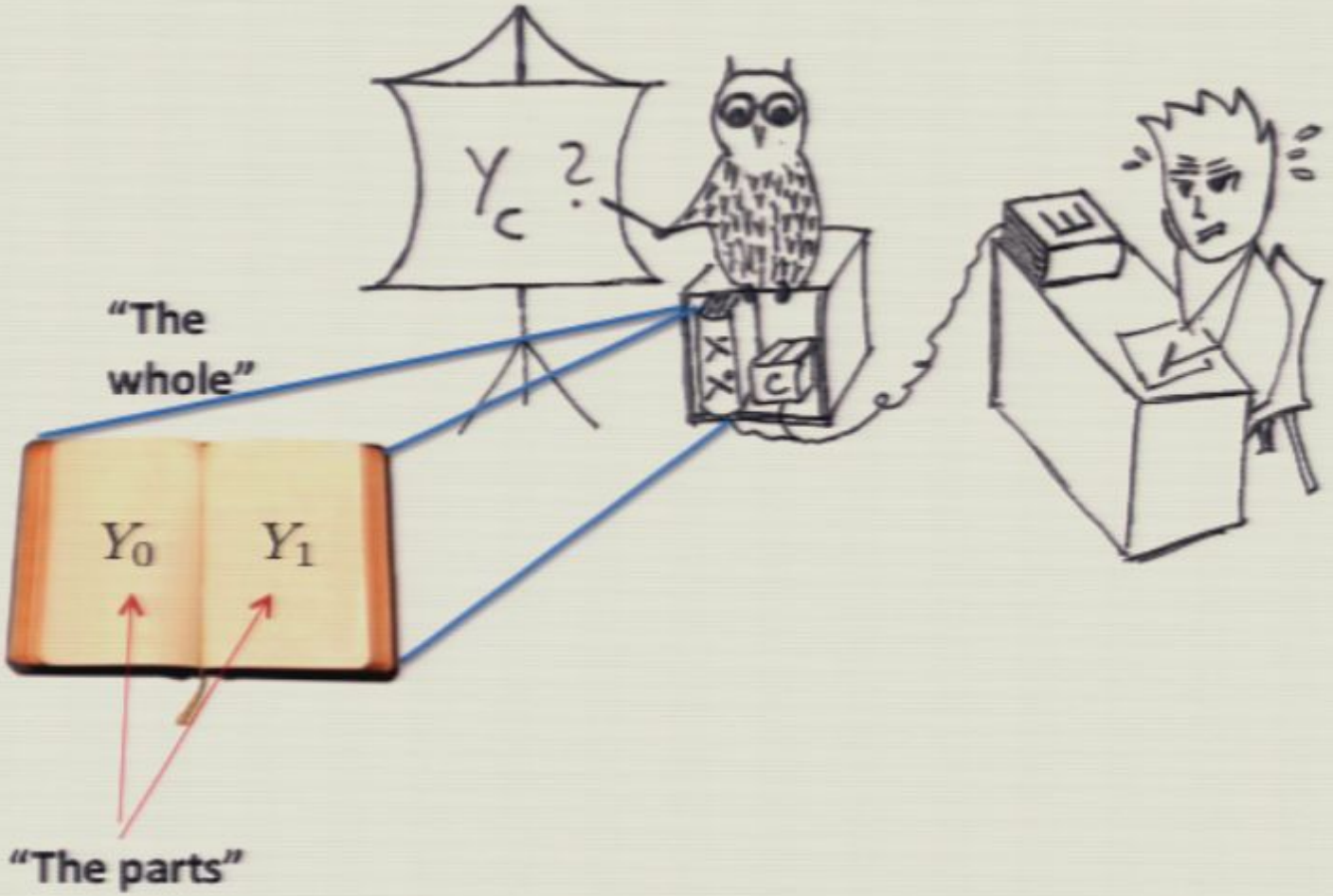
The problem



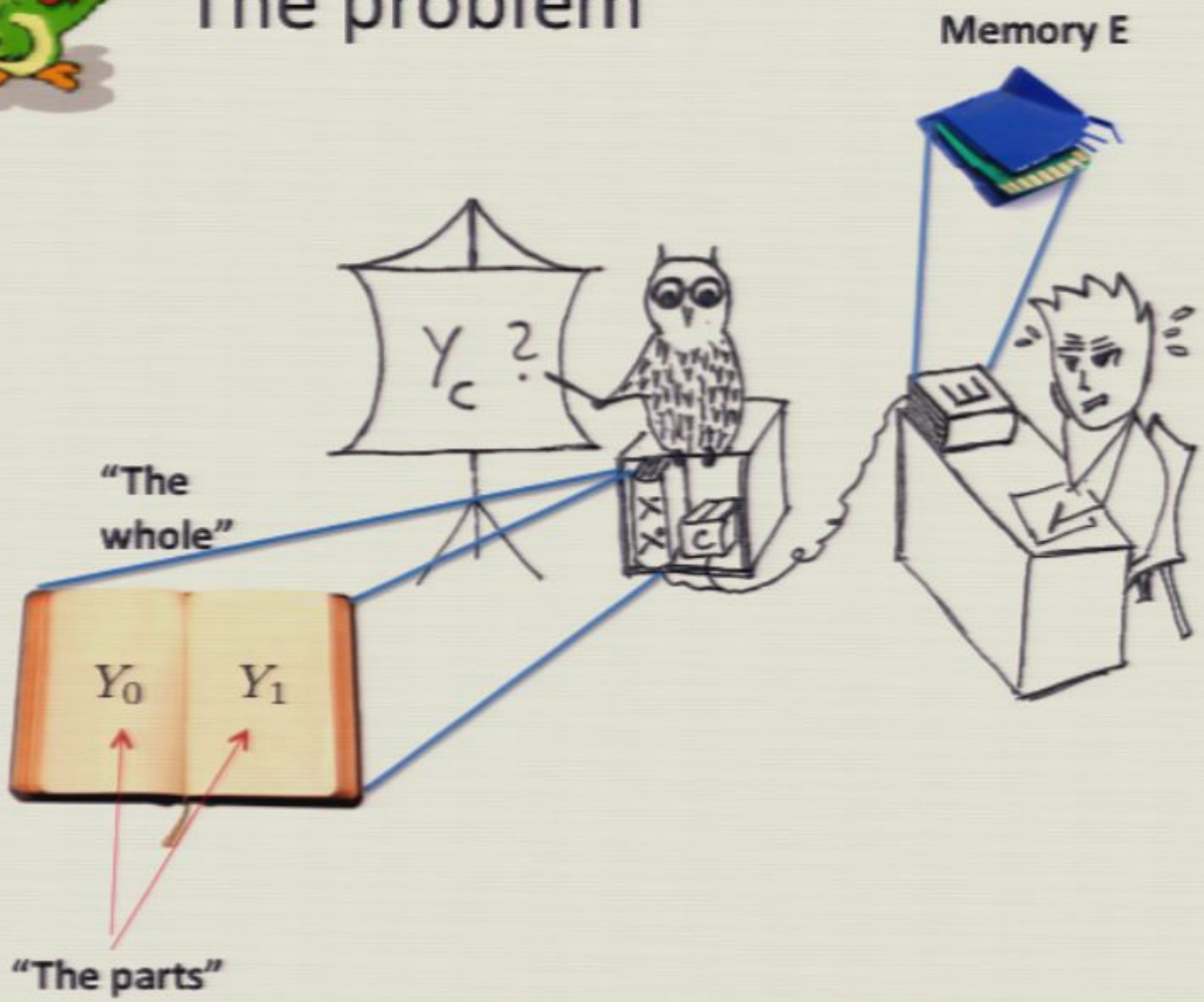
The problem



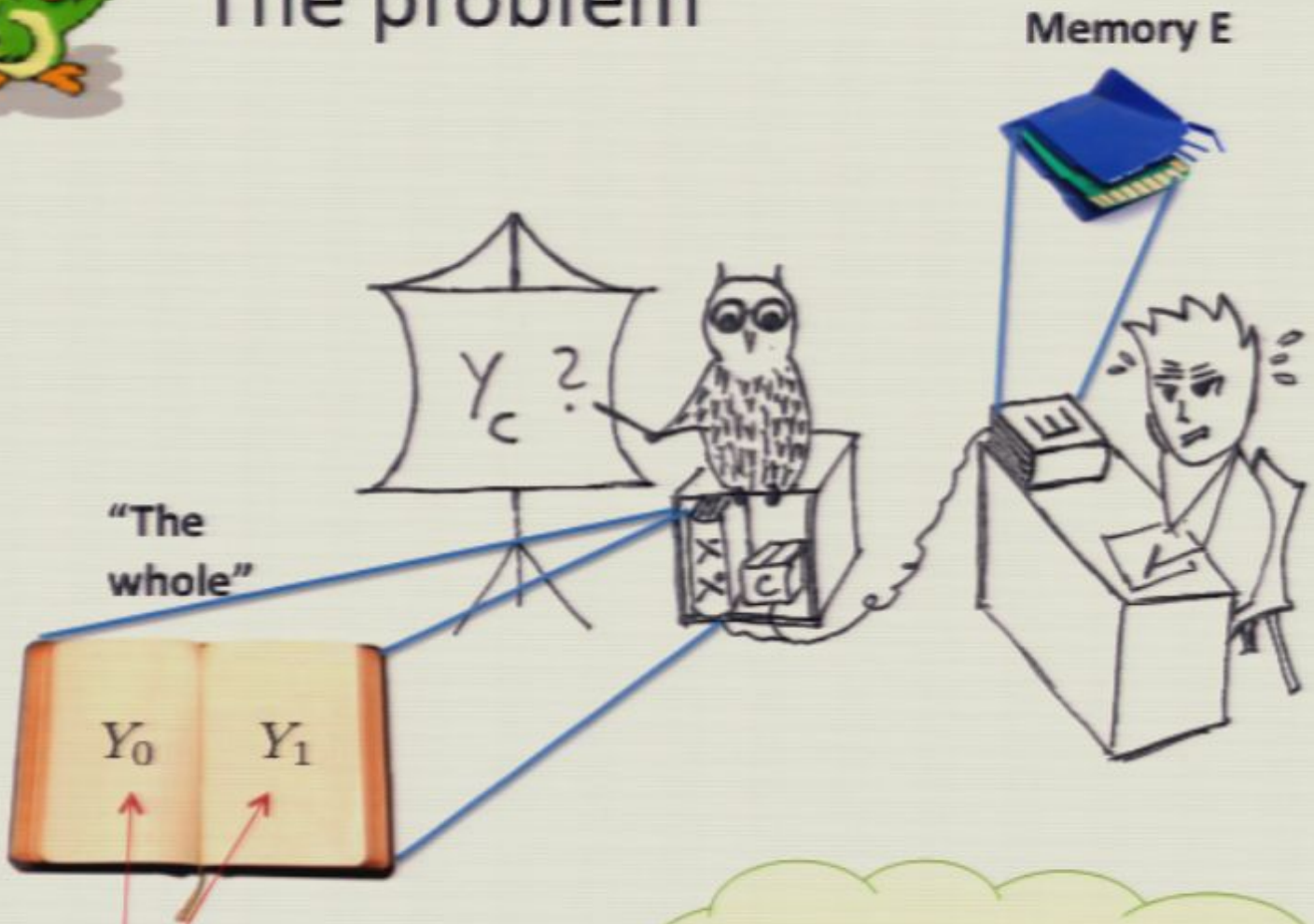
The problem



The problem



The problem

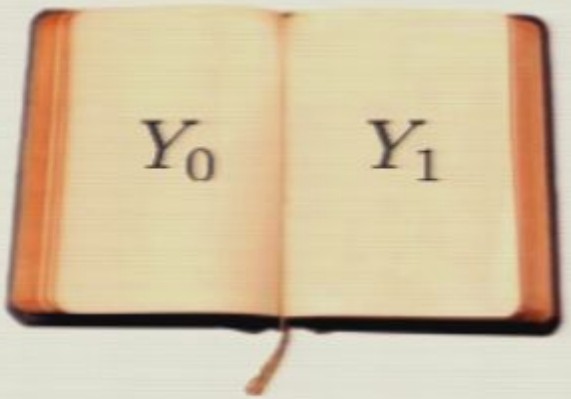


Does Bob's ignorance about the whole imply we can point to a part Bob is ignorant about?

Outline

1. How do we quantify ignorance?
2. The problem – this time more formal
3. Classical/non-contextual case
4. Violation in quantum mechanics
5. Open questions

Quantifying ignorance



Memory E

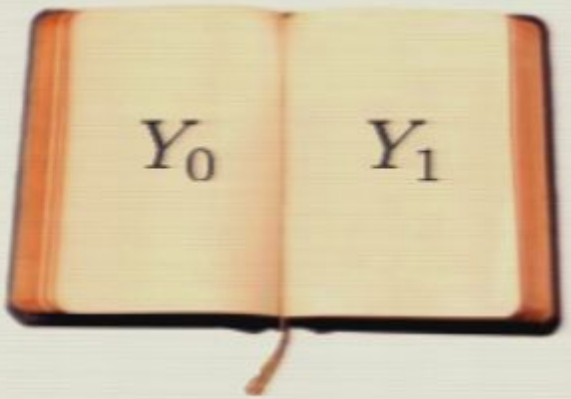
Encoding

Koenig, Renner, et al '08

Outline

1. How do we quantify ignorance?
2. The problem – this time more formal
3. Classical/non-contextual case
4. Violation in quantum mechanics
5. Open questions

Quantifying ignorance

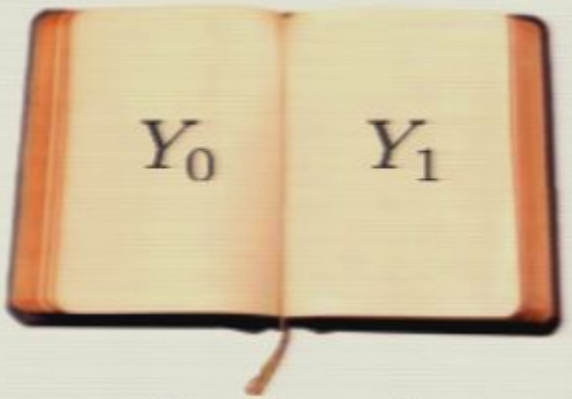


Memory E

Encoding

Koenig, Renner, et al '08

Quantifying ignorance



$P_{Y_0Y_1}(y_0, y_1)$

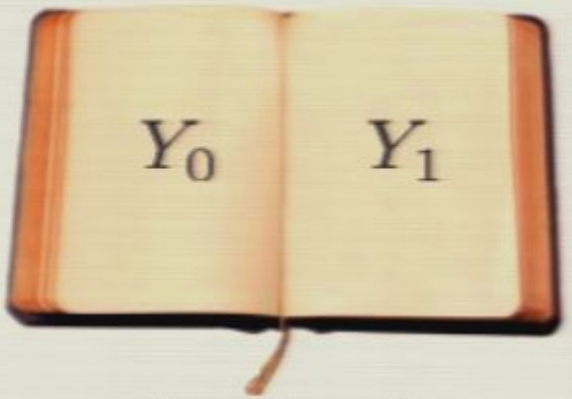
Memory E

Encoding

ρ_{y_0,y_1}

Koenig, Renner, et al '08

Quantifying ignorance



Memory E

Encoding

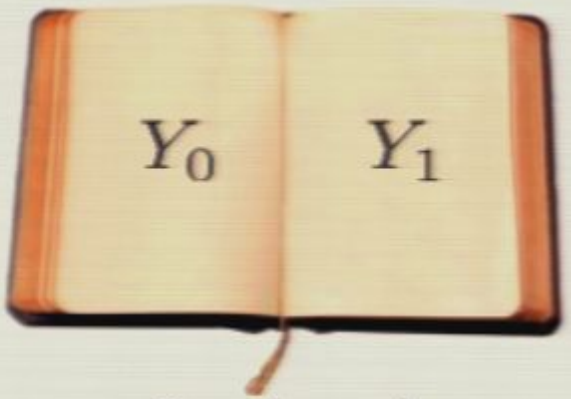
$P_{Y_0Y_1}(y_0, y_1)$

$$\rho_{Y_0Y_1E} = \sum_{y_0,y_1=1}^{d} P_{Y_0Y_1}(y_0,y_1) \underbrace{|y_0y_1\rangle\langle y_0y_1|}_{Y_0Y_1} \otimes \underbrace{\rho_{y_0y_1}}_{E}$$

ρ_{y_0,y_1}

Koenig, Renner, et al '08

Quantifying ignorance



Memory E

Encoding

$P_{Y_0Y_1}(y_0, y_1)$ ρ_{y_0,y_1}

$$\rho_{Y_0Y_1E} = \sum_{y_0,y_1=1}^{d} P_{Y_0Y_1}(y_0,y_1) \underbrace{|y_0y_1\rangle\langle y_0y_1|}_{Y_0Y_1} \otimes \underbrace{\rho_{y_0y_1}}_{E}$$

Min-entropy $H_\infty(Y_0Y_1|E) = -\log P_{guess}(Y_0Y_1|E)$

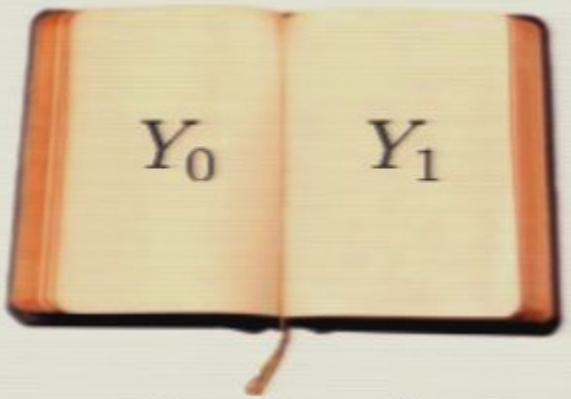
Koenig, Renner, et al '08

$$P_{guess}(Y_0Y_1|E) = \max_{\substack{\{M_{y_0y_1}\geq 0\}_{y_0y_1} \\ \sum_{y_0y_1} M_{y_0y_1}=\mathsf{id}}} \sum_{y_0y_1} P_{Y_0Y_1}(y_0y_1)\mathrm{tr}\left[M_{y_0y_1}\rho_{y_0y_1}\right]$$

Outline

1. How do we quantify ignorance?
2. The problem – this time more formal
3. Classical/non-contextual case
4. Violation in quantum mechanics
5. Open questions

A question – this time more formal



Memory E

Encoding

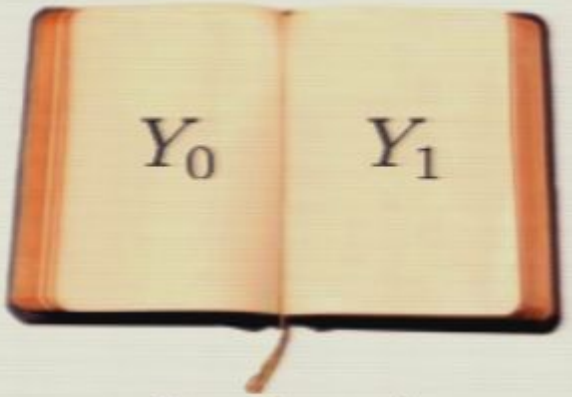
$P_{Y_0Y_1}(y_0, y_1)$

$$\rho_{Y_0Y_1E} = \sum_{y_0,y_1=1}^{d} P_{Y_0Y_1}(y_0, y_1) \underbrace{|y_0y_1\rangle\langle y_0y_1|}_{Y_0Y_1} \otimes \underbrace{\rho_{y_0y_1}}_{E}$$

ρ_{y_0,y_1}

A question – this time more formal

Memory E



Encoding

$P_{Y_0Y_1}(y_0, y_1)$

$$\rho_{Y_0Y_1E} = \sum_{y_0,y_1=1}^{d} P_{Y_0Y_1}(y_0,y_1) \underbrace{|y_0y_1\rangle\langle y_0y_1|}_{Y_0Y_1} \otimes \underbrace{\rho_{y_0y_1}}_{E}$$

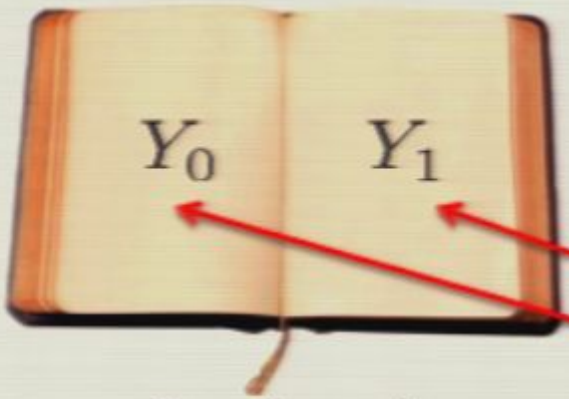
ρ_{y_0,y_1}

How does ignorance about the whole relate to ignorance of the parts?

How does $H_\infty(Y_0Y_1|E)$ relate to $H_\infty(Y_C|EC)$?

$C \in \{0,1\}$

The problem – this time more formal



Encoding

Memory E

$P_{Y_0Y_1}(y_0, y_1)$

$$\rho_{Y_0Y_1E} = \sum_{y_0,y_1=1}^{d} P_{Y_0Y_1}(y_0, y_1) \underbrace{|y_0y_1\rangle\langle y_0y_1|}_{Y_0Y_1} \otimes \underbrace{\rho_{y_0y_1}}_{E}$$

ρ_{y_0,y_1}

C

Outline

1. How do we quantify ignorance?
2. The problem – this time more formal
3. Classical/non-contextual case
4. Violation in quantum mechanics
5. Open questions

Classically/Non-contextual

Ignorance about the whole ***does*** imply that we can point to a part that we are ignorant about:

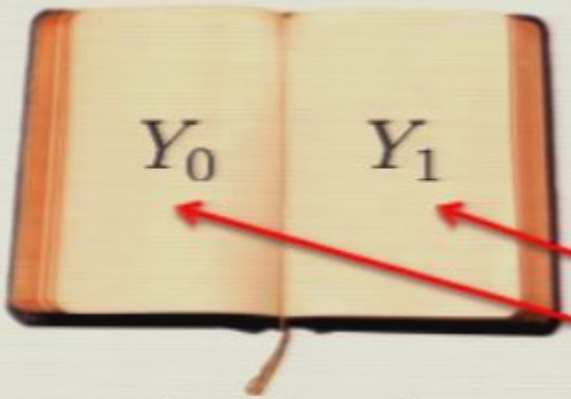
$$\exists \text{ consistent } \rho_{Y_0 Y_1 EC}$$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1$$

Wullschleger '07

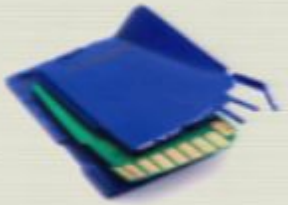
Extension to non-contextual LHVs (deterministic).

The problem – this time more formal



Memory E

Encoding



$P_{Y_0Y_1}(y_0, y_1)$

$$\rho_{Y_0Y_1E} = \sum_{y_0,y_1=1}^{d} P_{Y_0Y_1}(y_0, y_1) \underbrace{|y_0y_1\rangle\langle y_0y_1|}_{Y_0Y_1} \otimes \underbrace{\rho_{y_0y_1}}_{E}$$

ρ_{y_0,y_1}

C

Given large "ignorance" $H_\infty(Y_0Y_1|E)$

Can we determine a pointer $C \in \{0,1\}$ such that we have large $H_\infty(Y_C|EC)$?

C **consistent** pointer to the unknown

$$\mathrm{tr}_C(\rho_{Y_0Y_1EC}) = \rho_{Y_0Y_1E}$$

Outline

1. How do we quantify ignorance?
2. The problem – this time more formal
3. Classical/non-contextual case
4. Violation in quantum mechanics
5. Open questions

Classically/Non-contextual

Ignorance about the whole ***does*** imply that we can point to a part that we are ignorant about:

$$\exists \text{ consistent } \rho_{Y_0 Y_1 EC}$$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1$$

Wullschleger '07

Extension to non-contextual LHVs (deterministic).

Classically/Non-contextual

Ignorance about the whole ***does*** imply that we can point to a part that we are ignorant about:

$$\exists \text{ consistent } \rho_{Y_0 Y_1 EC}$$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1$$

Even when "leaking"/giving away m extra bits of information

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1 - m$$

Classically/Non-contextual

Ignorance about the whole ***does*** imply that we can point to a part that we are ignorant about:

$$\exists \text{ consistent } \rho_{Y_0 Y_1 EC}$$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1$$

Even when "leaking"/giving away m extra bits of information

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1 - m$$

Here: "Splitting inequality" can be violated arbitrarily in quantum mechanics.

"Knowledge" vs. "ignorance": The role of the pointer C

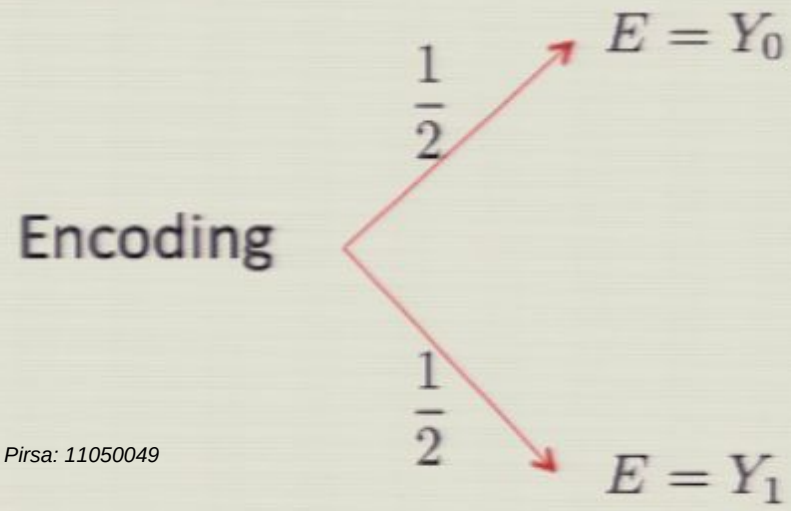
Even classically it can be that $H_\infty(Y_0Y_1|E)$ is very large, yet $H_\infty(Y_0|E), H_\infty(Y_1|E)$ are both very small.

$$y_0, y_1 \in \{0, \ldots, d-1\}, \qquad P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2}$$

"Knowledge" vs. "ignorance": The role of the pointer C

Even classically it can be that $H_\infty(Y_0Y_1|E)$ is very large, yet $H_\infty(Y_0|E), H_\infty(Y_1|E)$ are both very small.

$$y_0, y_1 \in \{0, \ldots, d-1\}, \qquad P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2}$$



"Knowledge" vs. "ignorance": The role of the pointer C

Even classically it can be that $H_\infty(Y_0Y_1|E)$ is very large, yet $H_\infty(Y_0|E), H_\infty(Y_1|E)$ are both very small.

$$y_0, y_1 \in \{0, \ldots, d-1\}, \qquad P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2}$$

Encoding

$\frac{1}{2}$ → $E = Y_0$ $\qquad H_\infty(Y_0Y_1|E) \approx \log d$

$\frac{1}{2}$ → $E = Y_1$

"Knowledge" vs. "ignorance": The role of the pointer C

Even classically it can be that $H_\infty(Y_0Y_1|E)$ is very large, yet $H_\infty(Y_0|E), H_\infty(Y_1|E)$ are both very small.

$$y_0, y_1 \in \{0, \ldots, d-1\}, \qquad P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2}$$

Encoding

$\frac{1}{2}$ → $E = Y_0$ $\qquad H_\infty(Y_0Y_1|E) \approx \log d$

$\frac{1}{2}$ → $E = Y_1$ $\qquad P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2d}$

$H_\infty(Y_0|E) = H_\infty(Y_1|E) \approx 1$

"Knowledge" vs. "ignorance": The role of the pointer C

Even classically it can be that $H_\infty(Y_0Y_1|E)$ is very large, yet $H_\infty(Y_0|E), H_\infty(Y_1|E)$ are both very small.

$$y_0, y_1 \in \{0, \ldots, d-1\}, \qquad P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2}$$

Encoding

$\frac{1}{2}$ → $E = Y_0$

$\frac{1}{2}$ → $E = Y_1$

H

In each case we can point to a part unknown to us.

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2d}$$

$$H_\infty(Y_0|E) = H_\infty(Y_1|E) \approx 1$$

Outline

1. How do we quantify ignorance?
2. The problem – this time more formal
3. Classical/non-contextual case
4. Violation in quantum mechanics
5. Open questions

Steps

Construct a specific encoding

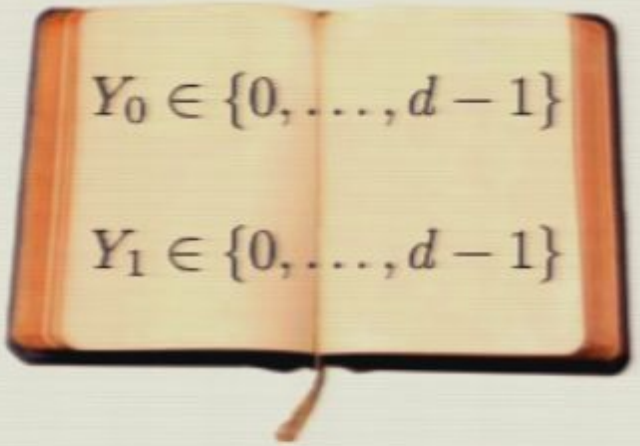
Show ignorance about the whole

Intermediate step: A random access encoding

Pointer C

Done!

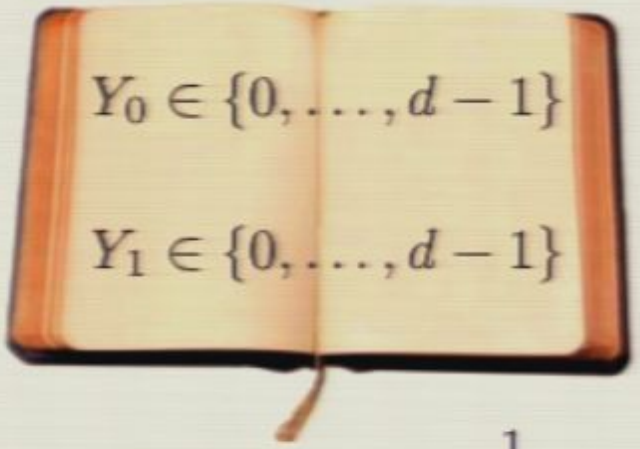
A specific encoding



Memory

Encoding

A specific encoding



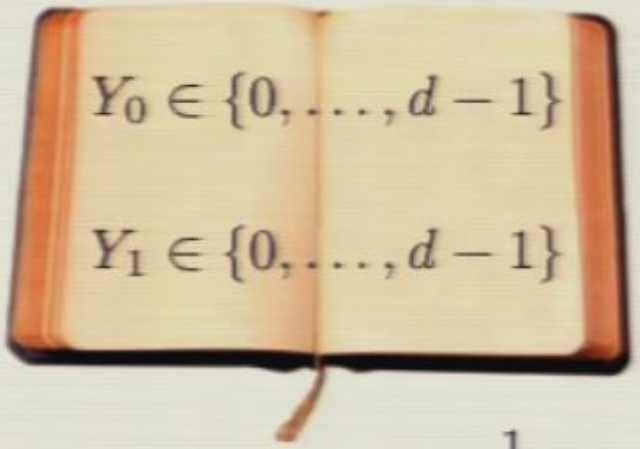
$$P_{Y_0 Y_1}(y_0 y_1) = \frac{1}{d^2}$$

Memory

Encoding

$$\rho_{y_0 y_1} = |\psi_{y_0 y_1}\rangle\langle\psi_{y_0 y_1}|$$

A specific encoding



Memory

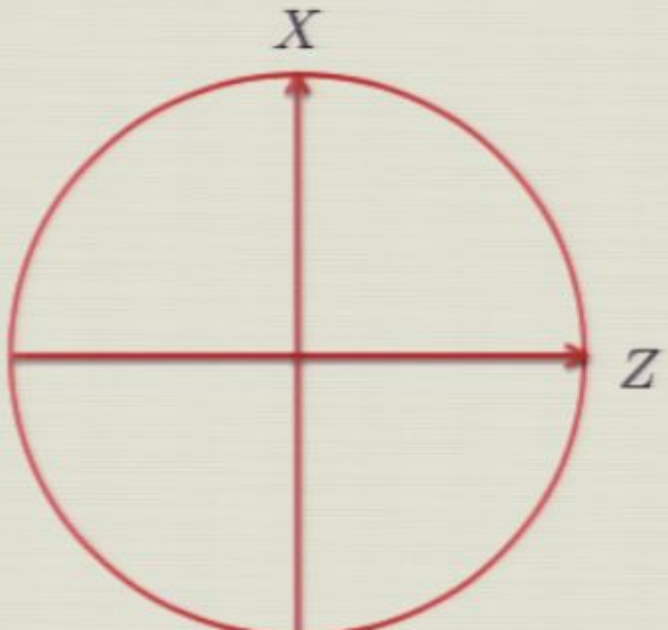
Encoding

$$\rho_{y_0 y_1} = |\psi_{y_0 y_1}\rangle\langle\psi_{y_0 y_1}|$$

$$|\psi_{y_0 y_1}\rangle = X^{y_0} Z^{y_1} |\phi\rangle$$

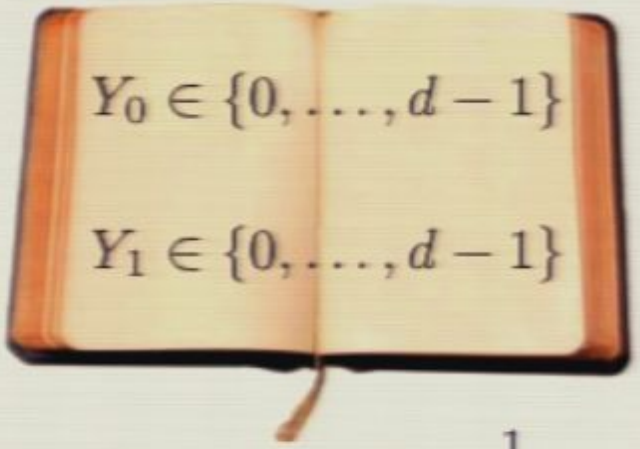
$$|\phi\rangle = \frac{1}{\sqrt{2\left(1 + \frac{1}{\sqrt{d}}\right)}} (|0\rangle + F|0\rangle)$$

$$P_{Y_0 Y_1}(y_0 y_1) = \frac{1}{d^2}$$



Example d=2

A specific encoding



$$P_{Y_0 Y_1}(y_0 y_1) = \frac{1}{d^2}$$

Memory

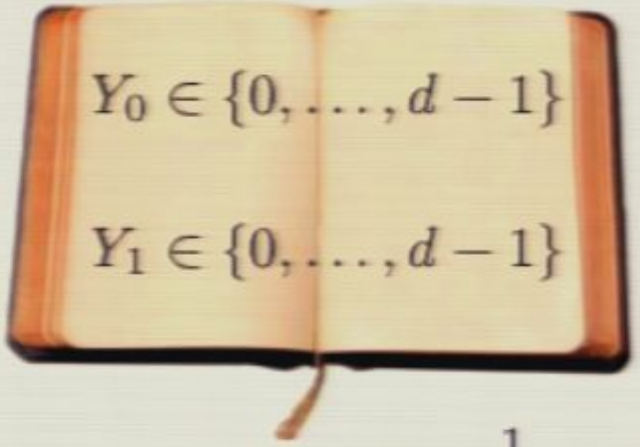
Encoding

$$\rho_{y_0 y_1} = |\psi_{y_0 y_1}\rangle\langle\psi_{y_0 y_1}|$$

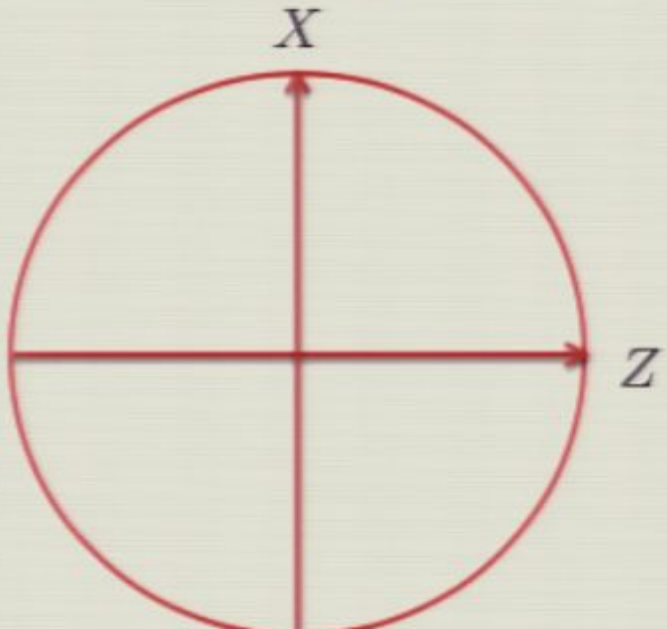
$$|\psi_{y_0 y_1}\rangle = X^{y_0} Z^{y_1} |\phi\rangle$$

$$|\phi\rangle = \frac{1}{\sqrt{2\left(1 + \frac{1}{\sqrt{d}}\right)}} (|0\rangle + F|0\rangle)$$

A specific encoding



$$P_{Y_0 Y_1}(y_0 y_1) = \frac{1}{d^2}$$



Memory

Encoding

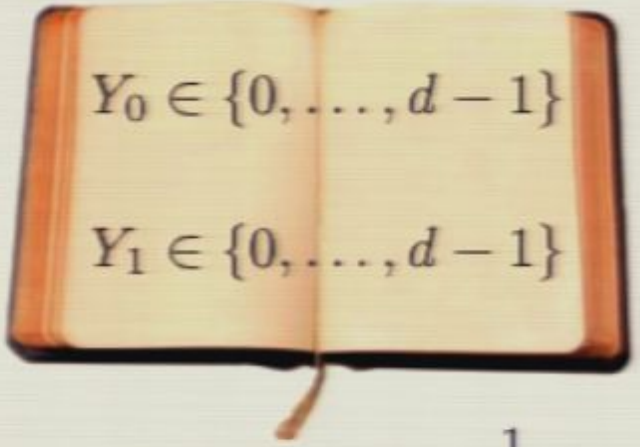
$$\rho_{y_0 y_1} = |\psi_{y_0 y_1}\rangle\langle\psi_{y_0 y_1}|$$

$$|\psi_{y_0 y_1}\rangle = X^{y_0} Z^{y_1} |\phi\rangle$$

$$|\phi\rangle = \frac{1}{\sqrt{2\left(1 + \frac{1}{\sqrt{d}}\right)}} (|0\rangle + F|0\rangle)$$

Example d=2

A specific encoding



Memory

Encoding

$$\rho_{y_0 y_1} = |\psi_{y_0 y_1}\rangle\langle\psi_{y_0 y_1}|$$

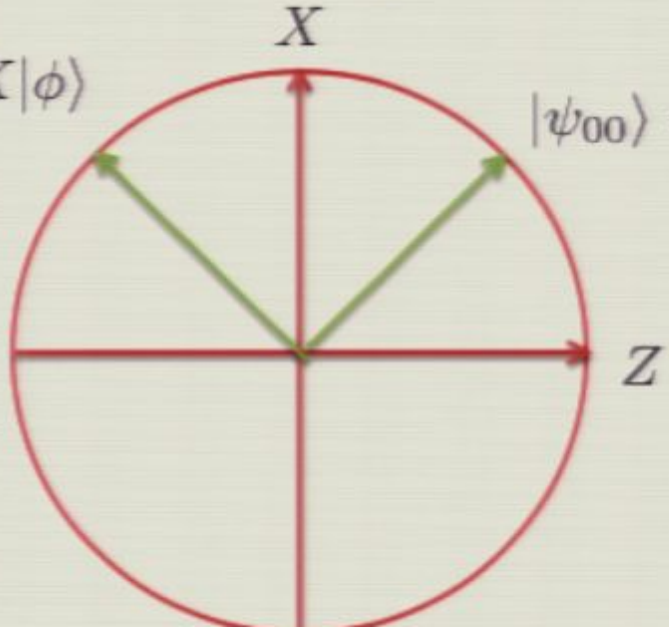
$$|\psi_{y_0 y_1}\rangle = X^{y_0} Z^{y_1} |\phi\rangle$$

$$|\phi\rangle = \frac{1}{\sqrt{2\left(1 + \frac{1}{\sqrt{d}}\right)}} (|0\rangle + F|0\rangle)$$

$$P_{Y_0 Y_1}(y_0 y_1) = \frac{1}{d^2}$$

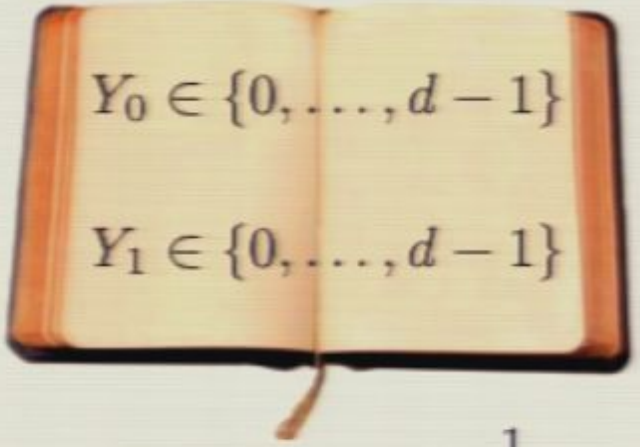
$|\psi_{10}\rangle = X|\phi\rangle$

$|\psi_{00}\rangle = |\phi\rangle$



Example d=2

A specific encoding



Memory

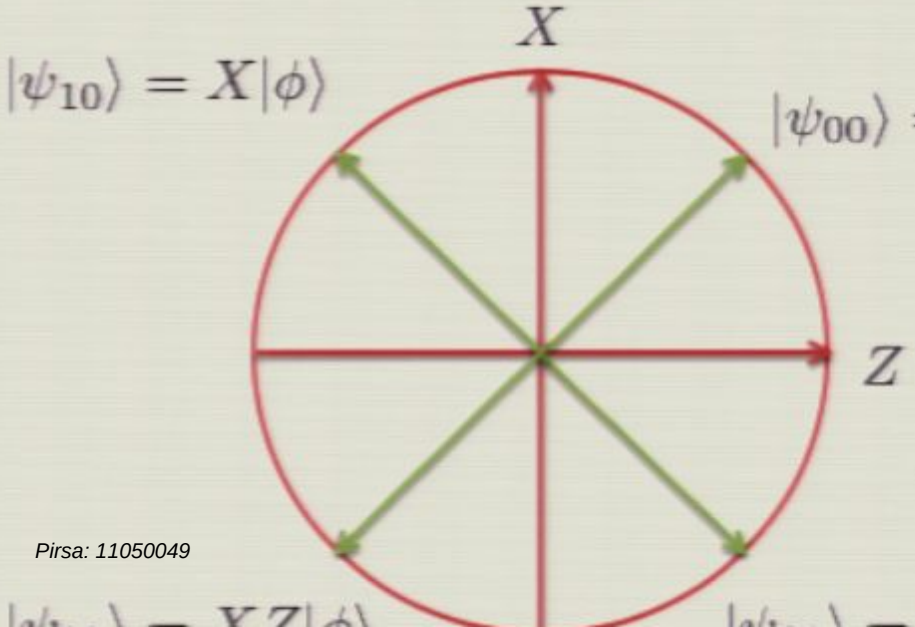
Encoding

$$\rho_{y_0 y_1} = |\psi_{y_0 y_1}\rangle\langle\psi_{y_0 y_1}|$$

$$|\psi_{y_0 y_1}\rangle = X^{y_0} Z^{y_1} |\phi\rangle$$

$$|\phi\rangle = \frac{1}{\sqrt{2\left(1 + \frac{1}{\sqrt{d}}\right)}} (|0\rangle + F|0\rangle)$$

$$P_{Y_0 Y_1}(y_0 y_1) = \frac{1}{d^2}$$



Example d=2

Steps

Construct a specific encoding

Show ignorance about the whole

Intermediate step: A random access encoding

Pointer C

Done!

Ignorance about the whole

$$P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2} \qquad |\psi_{y_0y_1}\rangle = X^{y_0}Z^{y_1}|\phi\rangle \qquad |\phi\rangle = \frac{1}{\sqrt{2\left(1+\frac{1}{\sqrt{d}}\right)}}(|0\rangle + F|0\rangle)$$

Ignorance about the whole

$$P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2} \qquad |\psi_{y_0y_1}\rangle = X^{y_0}Z^{y_1}|\phi\rangle \qquad |\phi\rangle = \frac{1}{\sqrt{2\left(1+\frac{1}{\sqrt{d}}\right)}}(|0\rangle + F|0\rangle)$$

Guessing probability as an SDP
(Yuen, Kennedy, Lax '75)

$$P_{\text{guess}}(Y_0Y_1|E) = \frac{1}{d}$$

$$H_\infty(Y_0Y_1|E) = \log d$$

Measurement

$$M_{y_0y_1} = \frac{1}{d}|\psi_{y_0y_1}\rangle\langle\psi_{y_0y_1}|$$

Steps

Construct a specific encoding

Show ignorance about the whole

Intermediate step: A random access encoding

Pointer C

Done!

Ignorance about the whole

$$P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2} \qquad |\psi_{y_0y_1}\rangle = X^{y_0}Z^{y_1}|\phi\rangle \qquad |\phi\rangle = \frac{1}{\sqrt{2\left(1+\frac{1}{\sqrt{d}}\right)}}(|0\rangle + F|0\rangle)$$

Guessing probability as an SDP
(Yuen, Kennedy, Lax '75)

$$P_{\text{guess}}(Y_0Y_1|E) = \frac{1}{d}$$

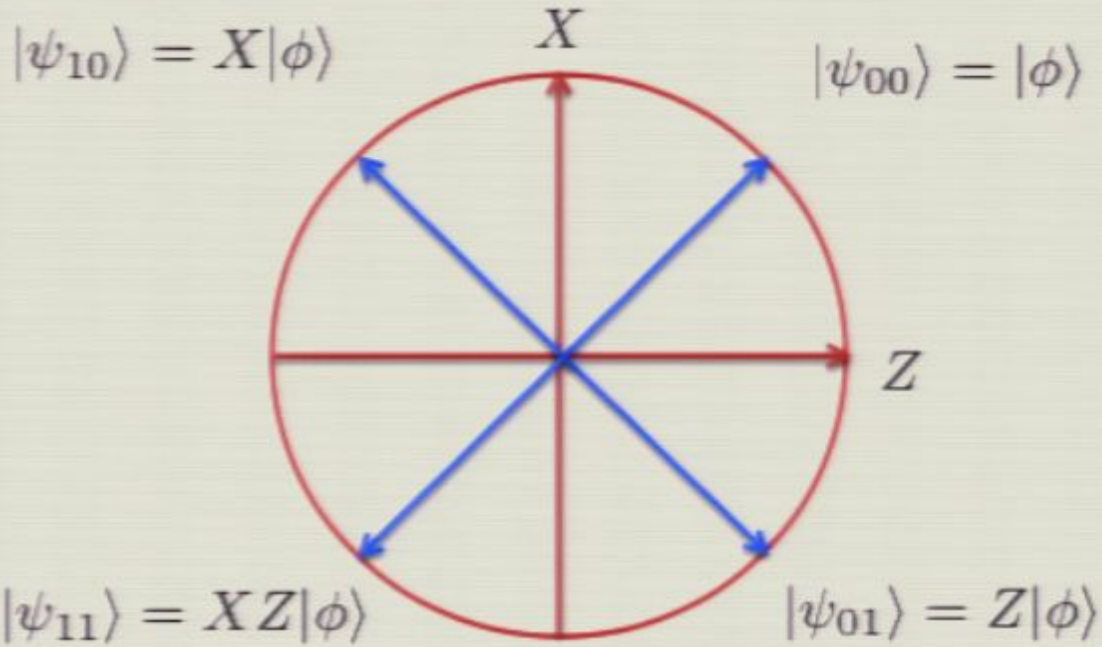
$$H_\infty(Y_0Y_1|E) = \log d$$

Measurement

$$M_{y_0y_1} = \frac{1}{d}|\psi_{y_0y_1}\rangle\langle\psi_{y_0y_1}|$$

Ignorance about the whole

$$P_{Y_0Y_1}(y_0y_1) = \frac{1}{d^2} \qquad |\psi_{y_0y_1}\rangle = X^{y_0}Z^{y_1}|\phi\rangle \qquad |\phi\rangle = \frac{1}{\sqrt{2\left(1+\frac{1}{\sqrt{d}}\right)}}(|0\rangle + F|0\rangle)$$



Guessing probability as an SDP
(Yuen, Kennedy, Lax '75)

$$P_{\text{guess}}(Y_0Y_1|E) = \frac{1}{d}$$

$$H_\infty(Y_0Y_1|E) = \log d$$

Measurement

$$M_{y_0y_1} = \frac{1}{d}|\psi_{y_0y_1}\rangle\langle\psi_{y_0y_1}|$$

Steps

Construct a specific encoding

Show ignorance about the whole

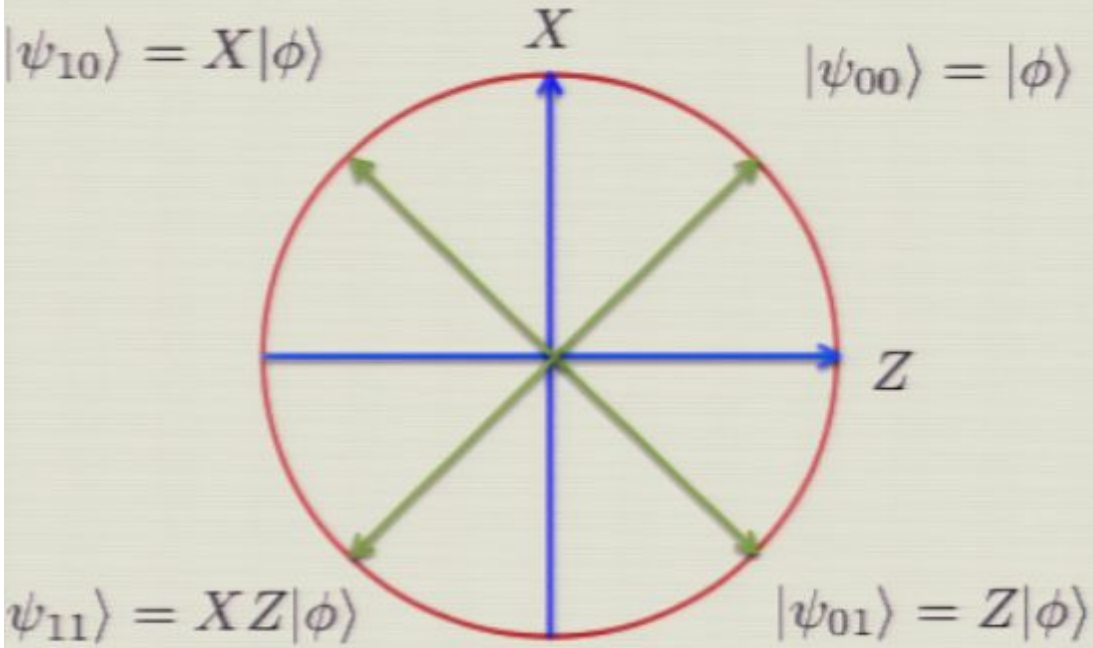
Intermediate step: A random access encoding

Pointer C

Done!

Decoding the parts

Intermediate step: Compute $H_\infty(Y_0|E)$ and $H_\infty(Y_1|E)$ and their optimal measurements



Guessing probability as an SDP

$$P_{\text{guess}}(Y_0|E) =$$

$$P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Optimal measurements

Eigenbasis of

$$Z \text{ (for } Y_0) \text{ and } X \text{ (for } Y_1)$$

(Random access code for a d-dimensional alphabet)

Decoding measurement

Let's suppose we want to extract just one entry using the same measuremet.

Measuring in the Z or X eigenbasis

$$|\langle y_0|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}} ,$$

$$|\langle y_1|F^\dagger|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Hence also for any other distribution over the strings

$$P'_{\text{guess}}(Y_0|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$P'_{\text{guess}}(Y_1|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Decoding measurement

Let's suppose we want to extract just one entry using the same measuremet.

Measuring in the Z or X eigenbasis

$$|\langle y_0|\psi_{y_0 y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}} ,$$

$$|\langle y_1|F^\dagger|\psi_{y_0 y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Decoding measurement

Let's suppose we want to extract just one entry using the same measuremet.

Measuring in the Z or X eigenbasis

$$|\langle y_0|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}} ,$$

$$|\langle y_1|F^\dagger|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Hence also for any other distribution over the strings

$$P'_{\text{guess}}(Y_0|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$P'_{\text{guess}}(Y_1|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Decoding measurement

Let's suppose we want to extract just one entry using the same measuremet.

Measuring in the Z or X eigenbasis

$$|\langle y_0|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}} ,$$

$$|\langle y_1|F^\dagger|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Hence also for any other distribution over the strings

$$P'_{\text{guess}}(Y_0|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$P'_{\text{guess}}(Y_1|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Steps

Construct a specific encoding

Show ignorance about the whole

Intermediate step: A random access encoding

Pointer C

Done!

The pointer C

Goal: For any consistent $\rho_{Y_0 Y_1 EC}$ we have that for any c that $H_\infty(Y_c|EC=c)$ is small

$$\rho_{Y_0 Y_1 E|C=c} = \sum_{y_0,y_1} \tilde{q}^c_{y_0 y_1} |y_0\rangle\langle y_0| \otimes |y_1\rangle\langle y_1| \otimes |\psi_{y_0 y_1}\rangle\langle \psi_{y_0 y_1}|$$

The pointer C

Goal: For any consistent $\rho_{Y_0 Y_1 EC}$ we have that for any c that $H_\infty(Y_c|EC=c)$ is small

$$\rho_{Y_0 Y_1 E|C=c} = \sum_{y_0,y_1} \tilde{q}^c_{y_0 y_1} |y_0\rangle\langle y_0| \otimes |y_1\rangle\langle y_1| \otimes |\psi_{y_0 y_1}\rangle\langle \psi_{y_0 y_1}|$$

For any distribution over the strings

$$P'_{\text{guess}}(Y_0|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$P'_{\text{guess}}(Y_1|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

The pointer C

Goal: For any consistent $\rho_{Y_0 Y_1 EC}$ we have that for any c that $H_\infty(Y_c|EC=c)$ is small

$$\rho_{Y_0 Y_1 E|C=c} = \sum_{y_0,y_1} \tilde{q}^c_{y_0 y_1} |y_0\rangle\langle y_0| \otimes |y_1\rangle\langle y_1| \otimes |\psi_{y_0 y_1}\rangle\langle \psi_{y_0 y_1}|$$

For any distribution over the strings

$$P'_{\text{guess}}(Y_0|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$P'_{\text{guess}}(Y_1|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$H_\infty(Y_c|EC=c) \approx 1$$

Outline

1. How do we quantify ignorance?
2. The problem – this time more formal
3. Classical/non-contextual case
4. Violation in quantum mechanics
5. Summary and open questions

To summarize

Classically

$\exists$ consistent $\rho_{Y_0 Y_1 EC}$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1$$

To summarize

Classically

$\exists$ consistent $\rho_{Y_0 Y_1 EC}$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1$$

Quantumly

There exists an example where

$$H_\infty(Y_0 Y_1|E) = \log d$$

$\forall$ consistent $\rho_{Y_0 Y_1 EC}$

$$\forall c, H_\infty(Y_c|EC = c) \approx 1$$

To summarize

Classically

$\exists$ consistent $\rho_{Y_0 Y_1 EC}$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0 Y_1|E)}{2} - 1$$

Ignorance about the whole, means significant ignorance about at least one of the parts.

Quantumly

There exists an example where

$$H_\infty(Y_0 Y_1|E) = \log d$$

$\forall$ consistent $\rho_{Y_0 Y_1 EC}$

$$\forall c, H_\infty(Y_c|EC = c) \approx 1$$

To summarize

Classically

$\exists$ consistent $\rho_{Y_0 Y_1 EC}$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0Y_1|E)}{2} - 1$$

Ignorance about the whole, means significant ignorance about at least one of the parts.

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0Y_1|E)}{2} - 1 - m$$

Quantumly

There exists an example where

$$H_\infty(Y_0Y_1|E) = \log d$$

$\forall$ consistent $\rho_{Y_0 Y_1 EC}$

$$\forall c, H_\infty(Y_c|EC = c) \approx 1$$

Ignorance about the whole does **not** Imply ignorance about any of the two parts.

Open questions

- Role of "complementarity":
  Typically stated that "we may learn invididual properties (Y0 or Y1), but not all (Y0Y1) at once": not so surprising for random access codes..

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

vs.

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2d}$$

Open questions

- Role of "complementarity":
  Typically stated that "we may learn invididual properties (Y0 or Y1), but not all (Y0Y1) at once": not so surprising for random access codes..

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

vs.

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2d}$$

Open questions

- Maximal violation in a fixed dimension?

$$\Delta = \min_C H_\infty(Y_0 Y_1|E) - H_\infty(Y_C|EC)$$

$\Delta \approx \log d$ Optimal?

Open questions

- Role of "complementarity":
  Typically stated that "we may learn invididual properties (Y0 or Y1), but not all (Y0Y1) at once": not so surprising for random access codes..

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

vs.

$$P_{\text{guess}}(Y_0|E) = P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2d}$$

Open questions

- More general theories?
- General non-contextual models?

Open questions

- Maximal violation in a fixed dimension?

$$\Delta = \min_C H_\infty(Y_0 Y_1|E) - H_\infty(Y_C|EC)$$

$\Delta \approx \log d$ Optimal?

Open questions

- Experimentally verifiable?

Tricky: would need to show that for any C guessing probability is low., but just exhibiting a d-dimensional random access encoding may be too weak.

Advantage: robust

Open questions

- Experimentally verifiable?

Tricky: would need to show that for any C guessing probability is low., but just exhibiting a d-dimensional random access encoding may be too weak.

Advantage: robust

Thank you!

To summarize

Classically

$\exists$ consistent $\rho_{Y_0 Y_1 EC}$

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0Y_1|E)}{2} - 1$$

Ignorance about the whole, means significant ignorance about at least one of the parts.

$$H_\infty(Y_C|EC) \geq \frac{H_\infty(Y_0Y_1|E)}{2} - 1 - m$$

Quantumly

There exists an example where

$$H_\infty(Y_0Y_1|E) = \log d$$

$\forall$ consistent $\rho_{Y_0 Y_1 EC}$

$$\forall c, H_\infty(Y_c|EC = c) \approx 1$$

Ignorance about the whole does **not** Imply ignorance about any of the two parts.

The pointer C

Goal: For any consistent $\rho_{Y_0 Y_1 EC}$ we have that for any c that $H_\infty(Y_c|EC=c)$ is small

$$\rho_{Y_0 Y_1 E|C=c} = \sum_{y_0,y_1} \tilde{q}^c_{y_0 y_1} |y_0\rangle\langle y_0| \otimes |y_1\rangle\langle y_1| \otimes |\psi_{y_0 y_1}\rangle\langle \psi_{y_0 y_1}|$$

For any distribution over the strings

$$P'_{\text{guess}}(Y_0|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$P'_{\text{guess}}(Y_1|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Steps

Construct a specific encoding

Show ignorance about the whole

Intermediate step: A random access encoding

Pointer C

Done!

Decoding measurement

Let's suppose we want to extract just one entry using the same measuremet.

Measuring in the Z or X eigenbasis

$$|\langle y_0|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}} ,$$

$$|\langle y_1|F^\dagger|\psi_{y_0y_1}\rangle|^2 = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

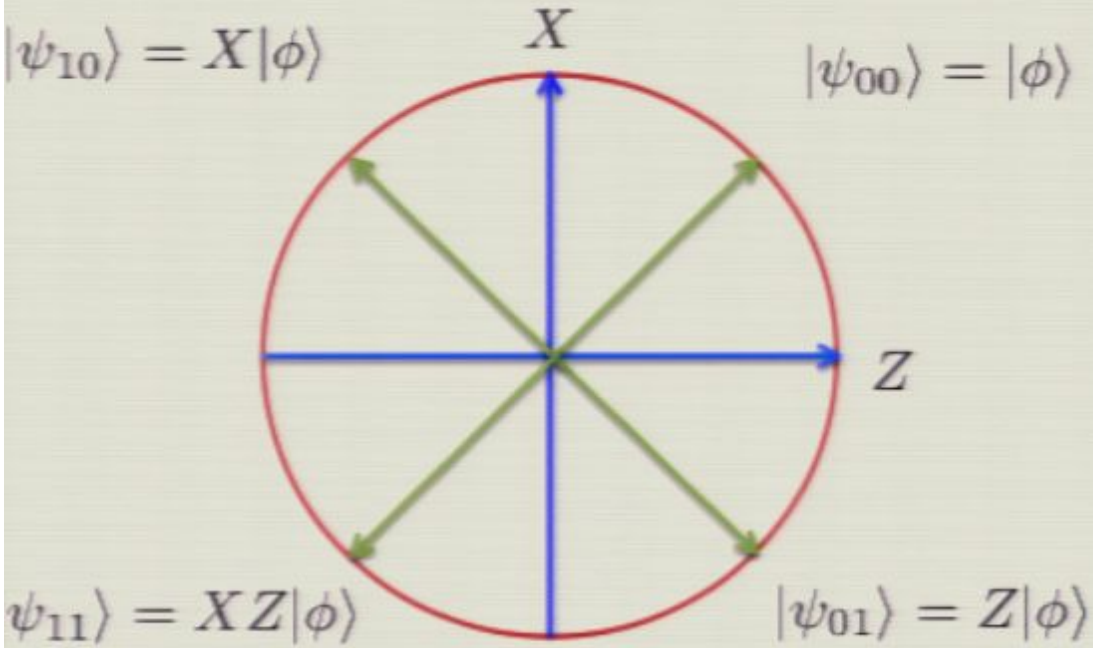
Hence also for any other distribution over the strings

$$P'_{\text{guess}}(Y_0|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

$$P'_{\text{guess}}(Y_1|E) \geq \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Decoding the parts

Intermediate step: Compute $H_\infty(Y_0|E)$ and $H_\infty(Y_1|E)$ and their optimal measurements



Guessing probability as an SDP

$$P_{\text{guess}}(Y_0|E) =$$

$$P_{\text{guess}}(Y_1|E) = \frac{1}{2} + \frac{1}{2\sqrt{d}}$$

Optimal measurements

Eigenbasis of

$$Z \text{ (for } Y_0) \text{ and } X \text{ (for } Y_1)$$

(Random access code for a d-dimensional alphabet)