Title: Relation of Mathematics to the Physical World

Date: Jun 25, 2008 11:30 AM

URL: http://pirsa.org/08060196

Abstract:

RELATION OF MATHEMATICS TO THE PHYSICAL WORLD

Horace P. Yuen
Northwestern University

- The "Unreasonable Effectiveness of Math in Phys".
- Relations of Math to ALL SORTS of Reality — Cognition, emotion, ...

— General connection between "internal representation" and "external reality"

1. Foundational
   language and interpretation
2. Meaning & Representation
   language and reality
3. Completeness of Math Repre
   robustness or sensitivity
4. Significance of Math Guarantee
   operational meaning

FOUNDATIONAL

reference to reality

1/ physical meaning of math axioms

2/ infinity and real #

e.g. time and bandwidth
frequency duration

3/ proper digitization

* Proving mathematical theorems via physics

- Meaning of Probability in
  - classical — epistemological
  - vs quantum physics — ontological
- Radical ontology in qt physics never before addressed in history of philosophy
  - Relation of "Uncountable" vs "Countable" infinite in physics
  - where exactly does the power of qt. Computation, dense coding, etc. lie — classical?

Meaning and Representation

capture natural language concepts mathematically

how to characteize all (versus recognize one presented)

1/ cloning procedures
2/ attacks in cryptographical problems
3/ (local) hidden variable theory
4/ mechanical procedures
5/ protocols in cryptography, e.g., QBC

and Impossibility claim

Completeness of Math Representation
for a given problem situation

— protocol security
— robustness to small disturbance

e.g. Schrodinger Cat
NOON state in qt metrolog

"loss" huge trouble in "quantum" syste
↳ nonclassical state

↳ classicalization theorem

Problems of experimental QIS&T

even in small scale

- Why can't one generate single-photon (on demand) (in a single space-time mode)
- Why can't one generate EPR pairs (...)
- Why can't one have "long" quantum memory
- Why can't one make a Bell measurement (complete, ...)
- Why can't one build a "good" CNOT gate

Completeness of Math Representation
for a given problem situation

- protocol security
- robustness to small disturbance

e.g. Schrodinger Cat
"NOON" state in qt metrology

"loss" huge trouble in "quantum" systems
↳ classicalization ↑ ↓ nonclassical

Significance of Mathematical Guarantee

operational meaning of a quantitative statement

1/ asymptotic vs finite
2/ meaning and validation of proofs
3/ operational meaning of entropy in crypto

MEASURE OF EVE'S "INFORMATION"

K^g key generated by A and B

Y_E Eve's observation

K' Eve's side information

$I(K^g; Y^E K')$ mutual information

→ usually the criterion used, with K' omitted

$$I(K^g; Y_E K') = H(K^g) - H(K^g \mid Y_E K')$$

$$\uparrow$$

$$|K^g|$$

X n-bit sequence with probabilities $p_1 \geq p_2 \geq \cdots \geq p_M$

$M = 2^n$

WHAT is the maximum p_1 under the constraint of fixed $H(X)$

$$H(X) = \mathrm{H}_2(p_1) + (1 - p_1)\log(M - 1)$$

p_i uniform on $\{2, \ldots, M\}$

$p_1 \sim 2^{-I}$ for $I \sim n \cdot 2^{-I}$

ex. $n \sim 100$, $p_1 \sim 0.01$ for $I \sim 1$

$\Rightarrow$ need to know $\{p_i\}$, or at least p_1

EVE'S ERROR PROFILE -- from $p(x_n \mid y_n^E, k')$

X n-bit sequence with probabilities $p_1 \geq p_2 \geq \cdots \geq p_M$

$M = 2^n$

WHAT is the maximum p_1 under the constraint of fixed $H(X)$

$\downarrow$

$H(X) = \mathrm{H}_2(p_1) + (1-p_1)\log(M-1)$ $\quad p_i$ uniform on $\{2,\ldots,\mathrm{M}\}$

$\mathrm{p}_1 \sim 2^{-I}$ for $I \sim n \cdot 2^{-I}$

ex. $n \sim 100$, $p_1 \sim 0.01$ for $I \sim 1$

$\Rightarrow$ need to know $\{p_i\}$, or at least p_1

$\uparrow$

EVE'S ERROR PROFILE -- from $\bar{p}(x_n \mid \mathrm{y}_\mathrm{n}^\mathrm{E}, \mathrm{k}')$

EVE'S TRIAL COMPLEXITY

$$\tau_t = \sum_{i=1}^{M} i \cdot p_i \qquad M = 2^n$$

- $p_1 \le 2^{-l}$ needs to be imposed

$\Downarrow$

- $\tau_t \ge \left(2^l + 1\right)/2, \qquad I_E \le n - l$

❖ p_1 , the success probability of Eve's optimal estimate, should be used as criterion instead of I_E

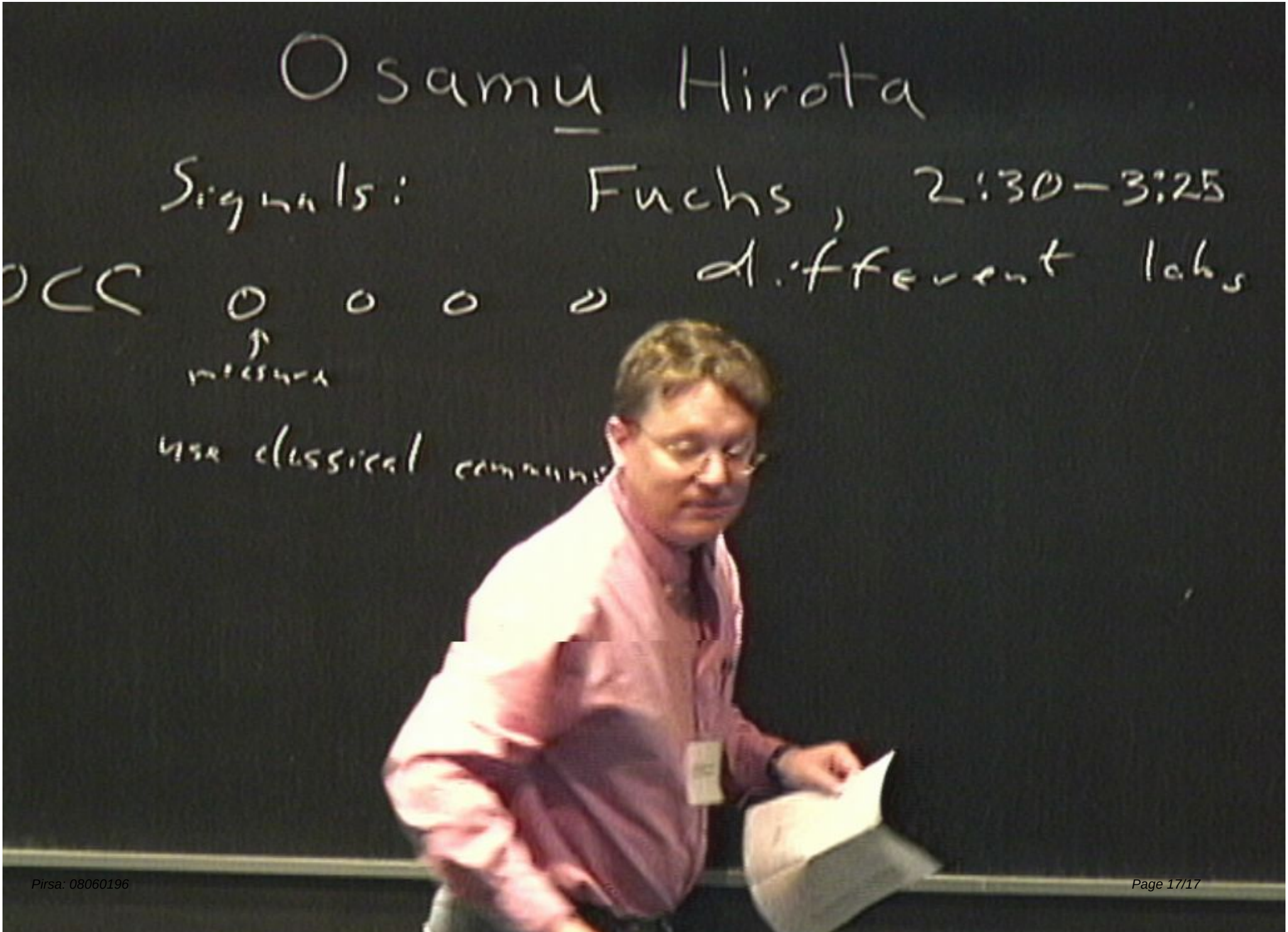
COMPARISON OF I_E BOUND versus p_1 BOUND

$n \sim 100, \quad I_E \leq 1 \Rightarrow p_1 \sim 10^{-2}$ possible!

$n \sim 100, \quad p_1 \leq 2^{-80} \Rightarrow I_E \sim 20$ possible

$\Downarrow$

$\tau_t \geq 2^{80} \Rightarrow$ no harm


Osamu Hirota
Signals: Fuchs, 2:30-3:25
different labs