Testing physics with quantum computers

Ben Reichardt
USC

Based on joint work with Rui Chao, Chris Sutherland, Falk Unger, Umesh Vazirani, Thomas Vidick

Challenges in Quantum Computation
Berkeley 6/12/2018

How can we test small quantum computers?

Is nature exponential?

(Do n qubits give 2^n dimensions?)

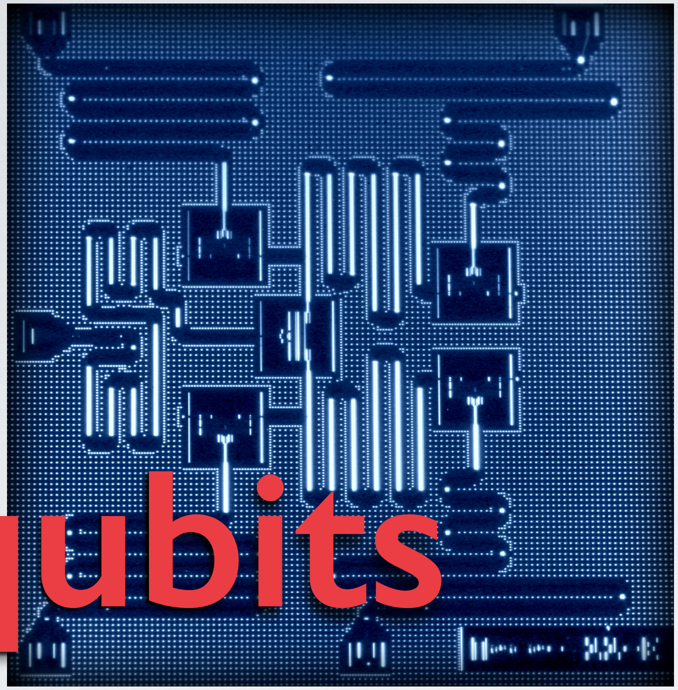
Does God play dice?

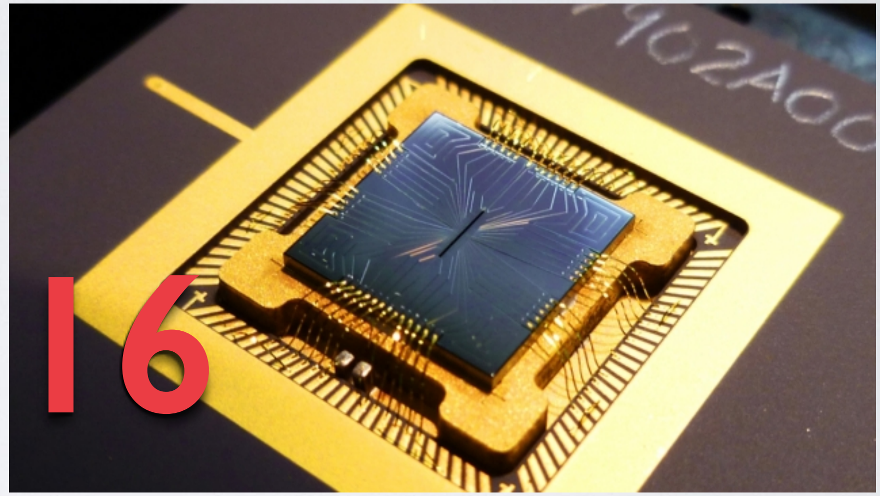
(Is there an underlying classical model?)

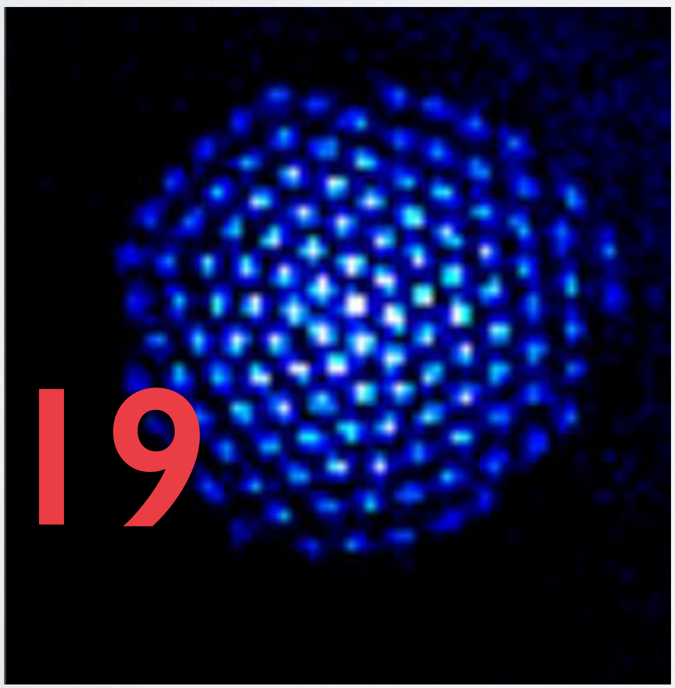
Does entanglement break down?

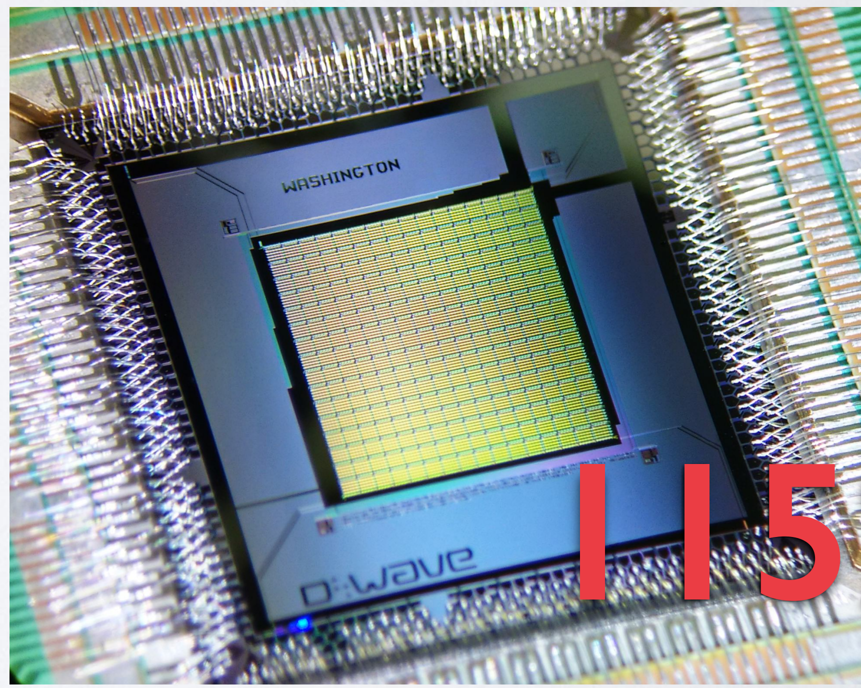
Locality: Are errors independent?

Dimension test


5 qubits
IBM


16
NIST/UMD


219
NIST


WASHINGTON
1152
D-Wave

Is nature exponential?

Huge $\mathcal{H}$

2^n

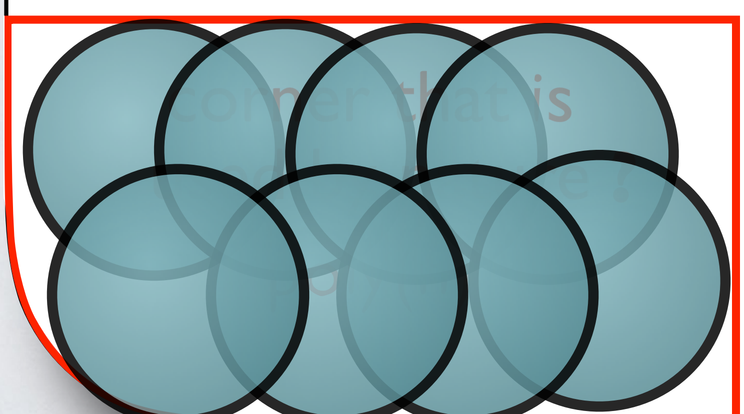
corner that is
used by nature ?

poly(n)

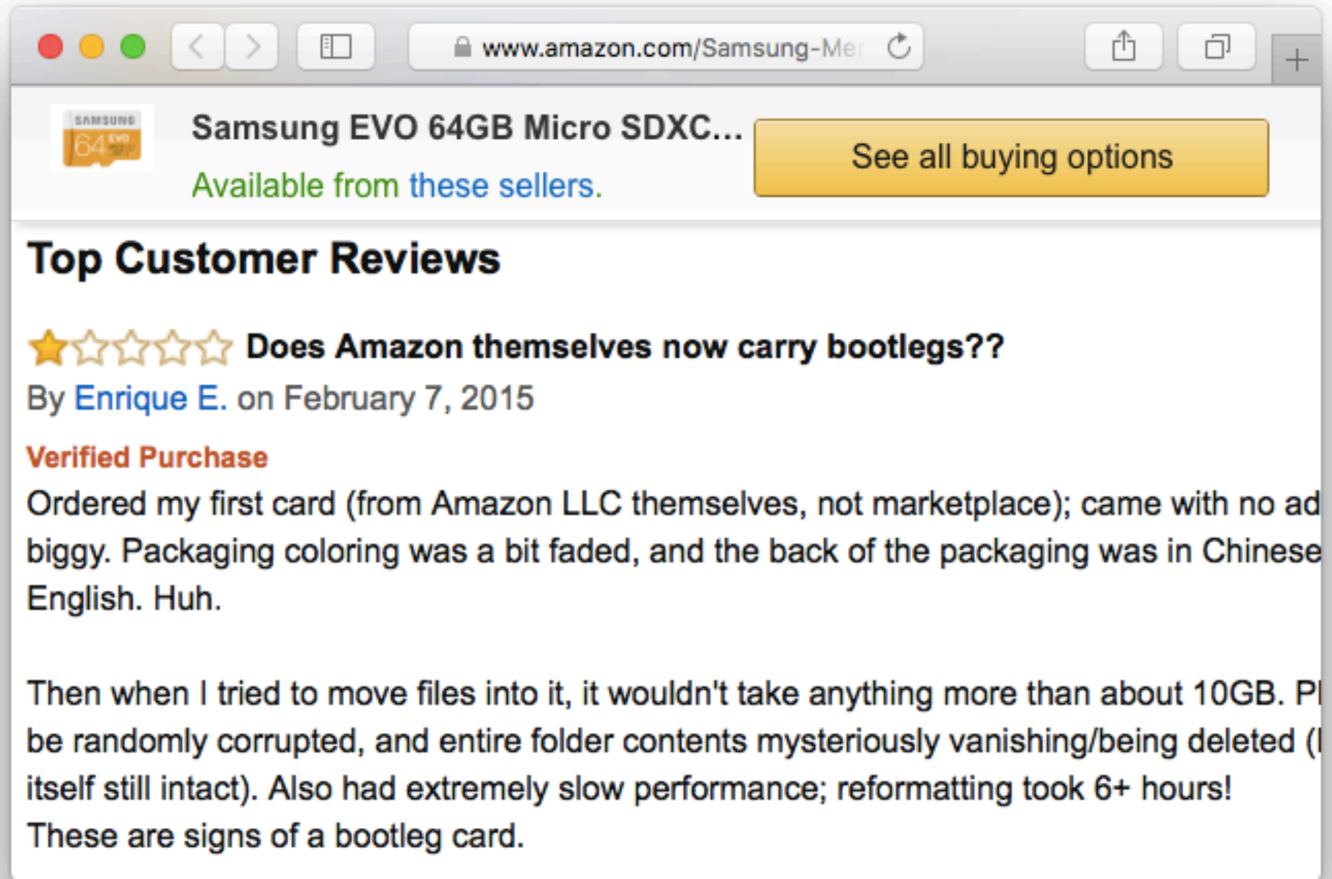
Is nature exponential?

Huge $\mathcal{H}$

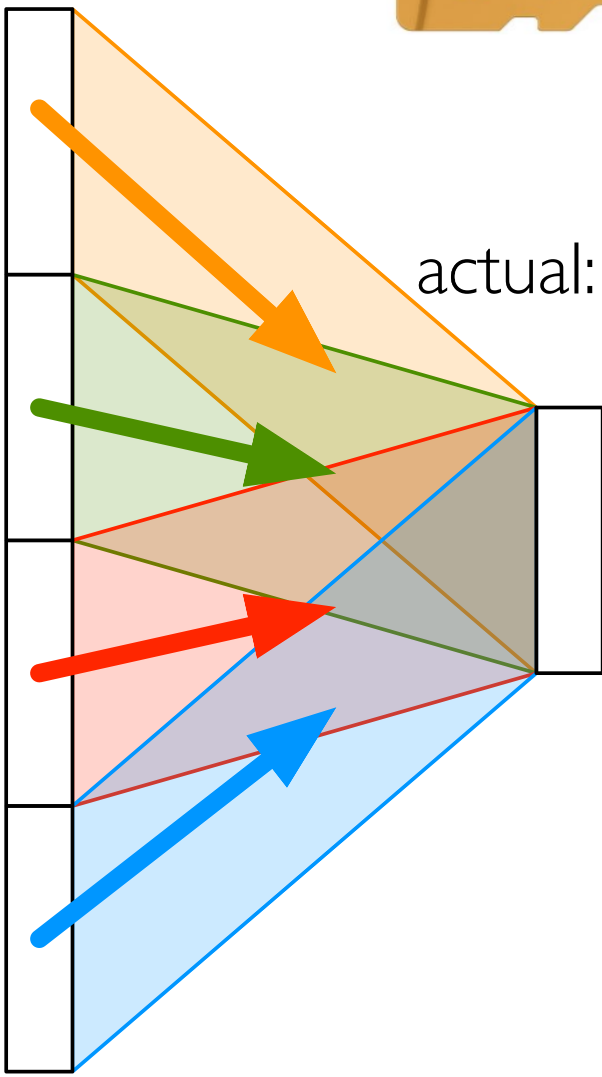
2^n



www.amazon.com/Samsung-Me
SAMSUNG
64 EVO
micro SD XC
Roll over image to zoom in
Samsung EVO 64GB Micro SDXC Memory Card with Adapter up to 48/MB/s (MB-MP64DA/AM)
11,932 customer reviews
| 946 answered questions
Available from these sellers.
Compatible with devices with SDXC slots-usage in non SDXC slot lead to reduced performance
Great for Cell phones, Smartphones, Android Tablets, Tablet PCs.
Great speed and performance for full HD video recording, high resolution pictures, mobile gaming, music and more.
Water proof, Temperature Proof, X-Ray proof, Magnetic proof
New (28) from $23.57 & FREE shipping.

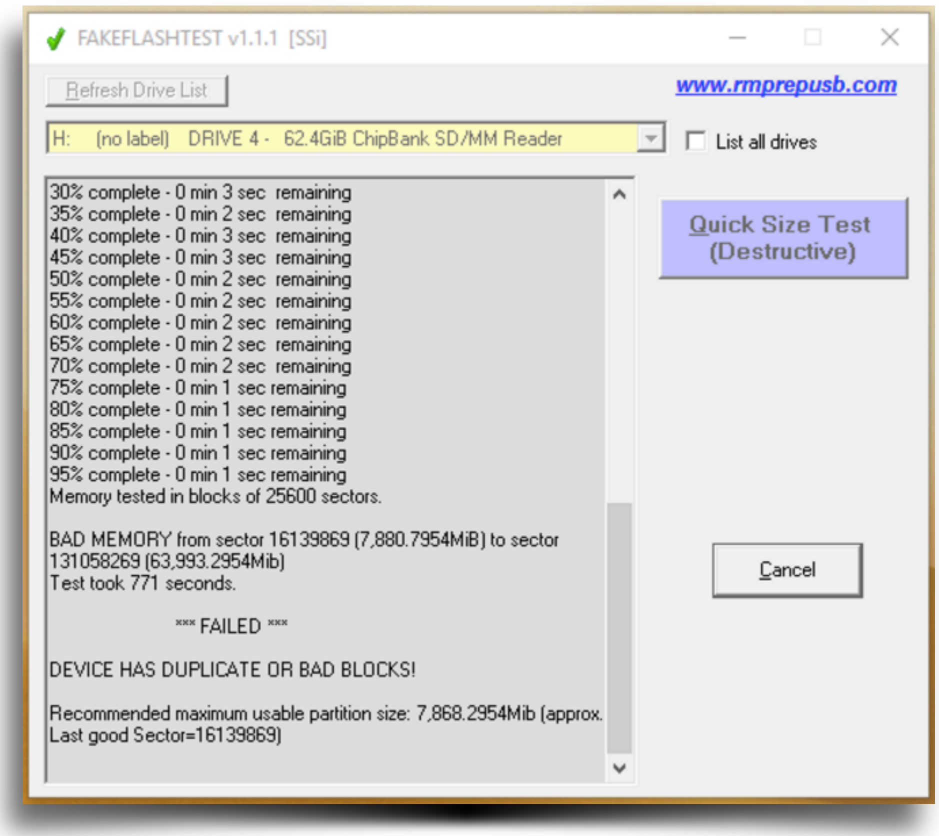

www.amazon.com/Samsung-Me
Samsung EVO 64GB Micro SDXC...
Available from these sellers.
See all buying options
Top Customer Reviews
Does Amazon themselves now carry bootlegs??
By Enrique E. on February 7, 2015
Verified Purchase
Ordered my first card (from Amazon LLC themselves, not marketplace); came with no ad
biggy. Packaging coloring was a bit faded, and the back of the packaging was in Chinese
English. Huh.
Then when I tried to move files into it, it wouldn't take anything more than about 10GB. Pl
be randomly corrupted, and entire folder contents mysteriously vanishing/being deleted (l
itself still intact). Also had extremely slow performance; reformatting took 6+ hours!
These are signs of a bootleg card.

reported capacity:
64GB

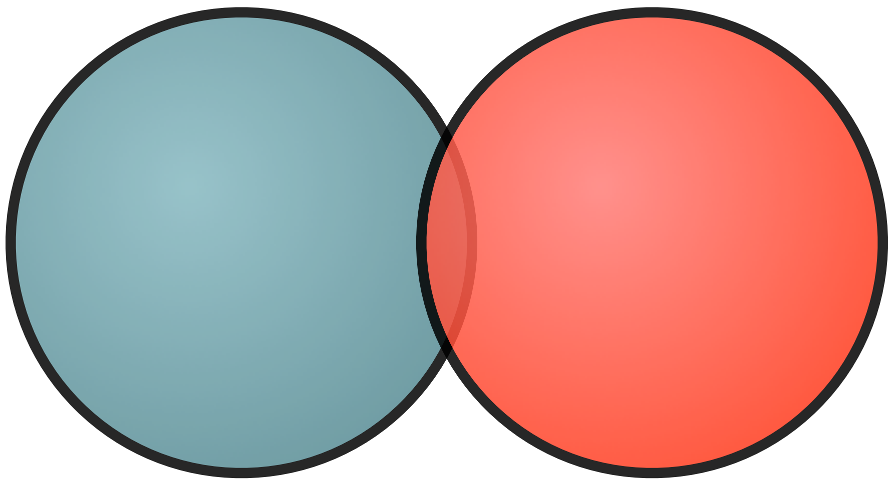


Memory test:

1. Store n random bits
2. Retrieve a random index & check it's correct



Quantum systems are continuous,
so can cheat in more interesting ways…



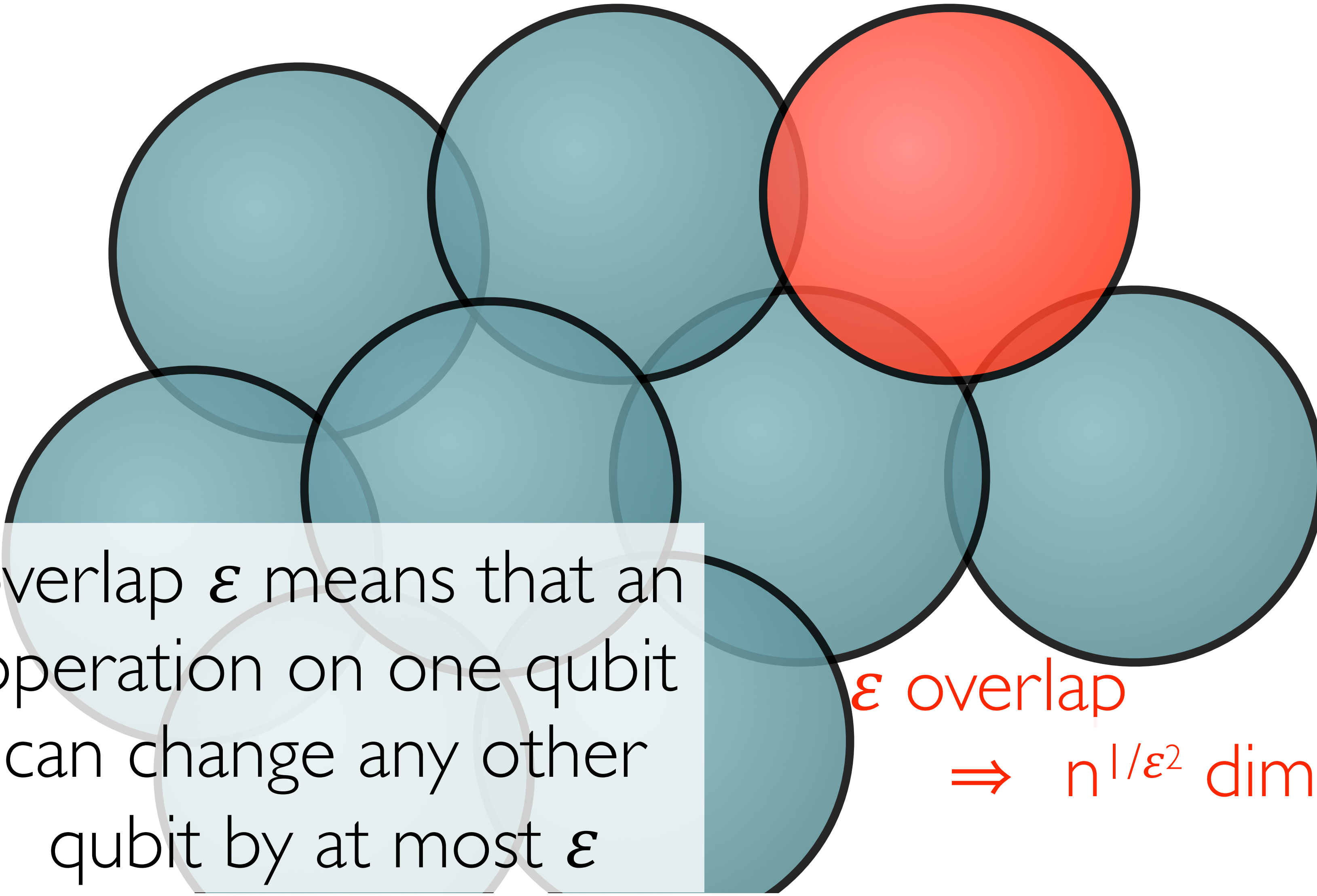
These qubits *slightly* overlap.

Behind the scenes:

"Access qubit 1"	"Access qubit 2"
$\Downarrow$	$\Downarrow$
qubit 1	Apply U, qubit 2, U^{-1}
	$\|U - I\| \leq \epsilon$

Theorem 1:

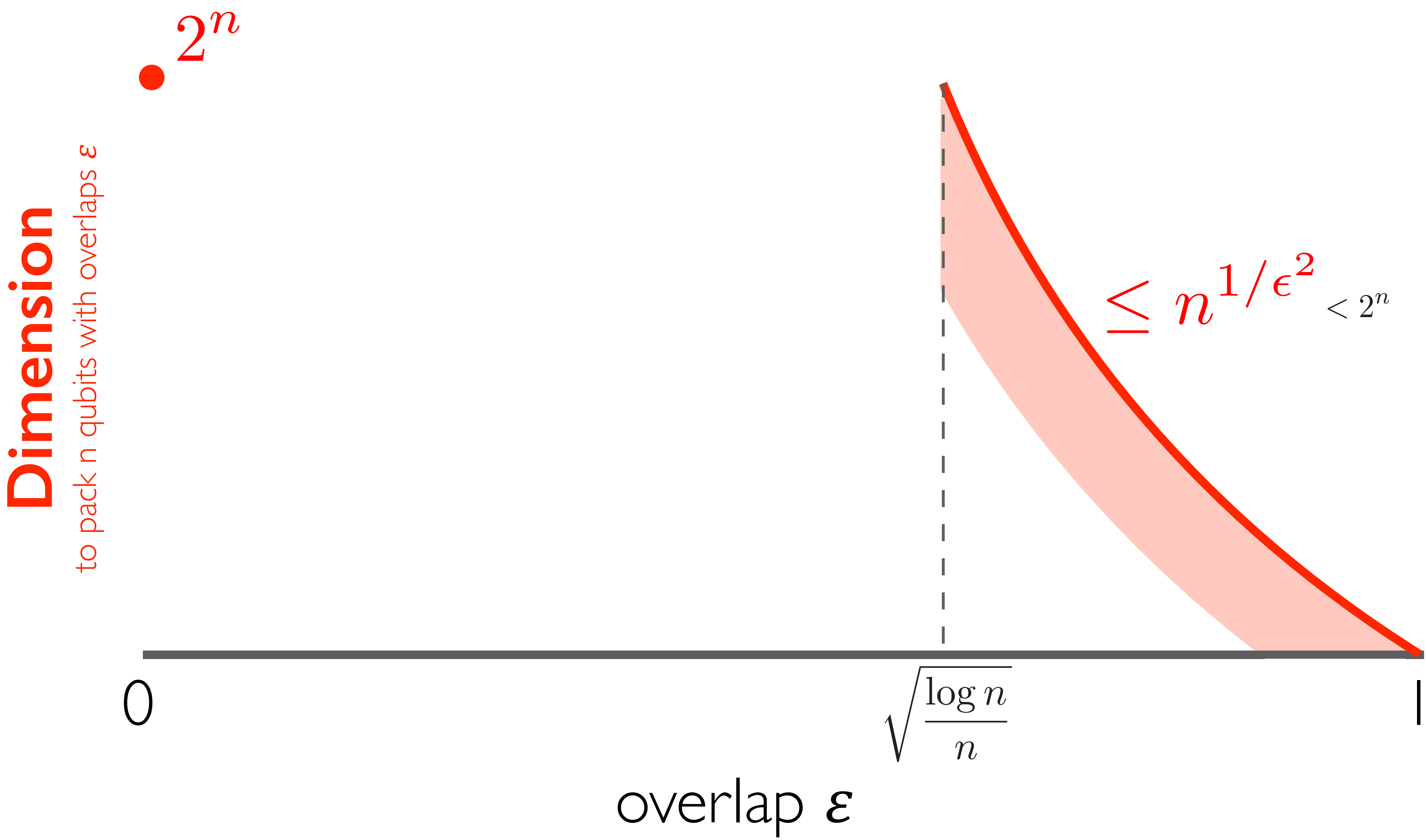
n overlapping qubits can fit in poly(n) dimensions



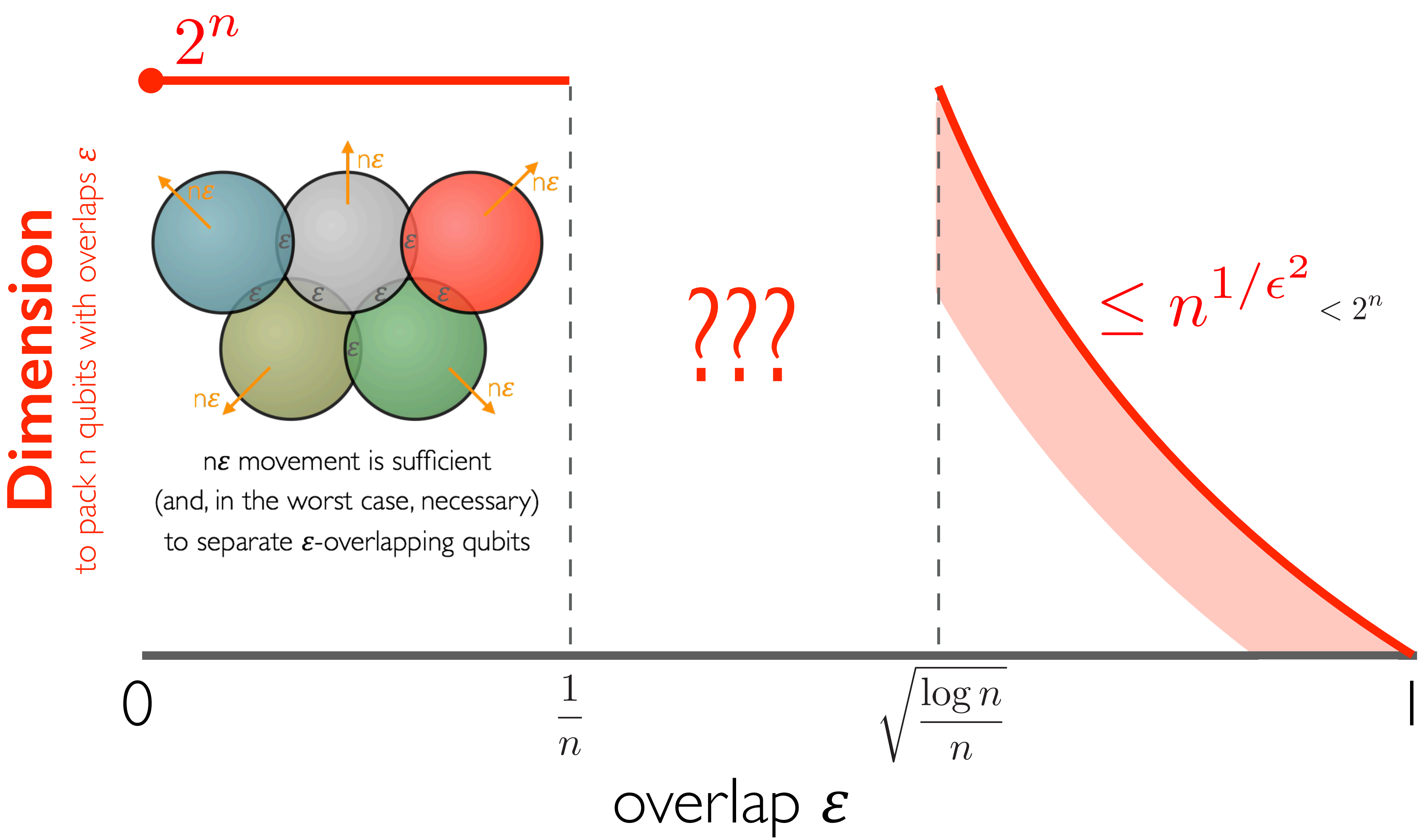
overlap ε means that an operation on one qubit can change any other qubit by at most ε

ε overlap

$\Rightarrow\ n^{1/\varepsilon^2}$ dimensions

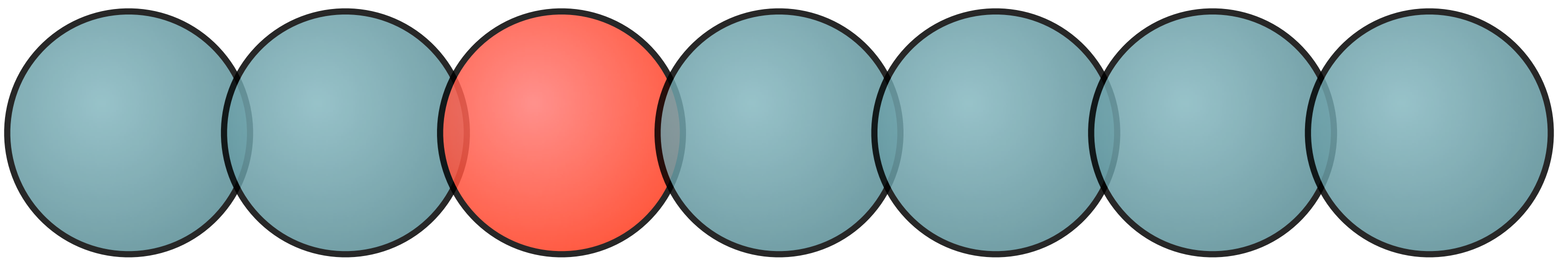


2^n
Dimension
to pack n qubits with overlaps ε
$\leq n^{1/\epsilon^2} < 2^n$
0
$\sqrt{\frac{\log n}{n}}$
1
overlap ε


Dimension
to pack n qubits with overlaps ε
2^n
nε
ε
nε movement is sufficient
(and, in the worst case, necessary)
to separate ε-overlapping qubits
???
$\leq n^{1/\epsilon^2} < 2^n$
0
$\frac{1}{n}$
$\sqrt{\frac{\log n}{n}}$
1
overlap ε

Dimension test

1. Store n random **qubits** (sequentially, each either $|0\rangle, |1\rangle, |+\rangle, |-\rangle$)
2. Retrieve a random index & check it's correct



Theorem 2:

$$\Pr[\text{pass test}] \geq 1 - \delta \;\Rightarrow\; \text{dimension} \geq (1 - n^2\delta)\, 2^n$$

The conclusion is actually stronger: Sequences of qubit operators are close to tensor-product operators, in their effects on a random state.

c.f. Nayak (FOCS '99)

Dimension test

Entanglement test

How to verify entanglement?

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

Answer: Measure $Z \otimes Z$

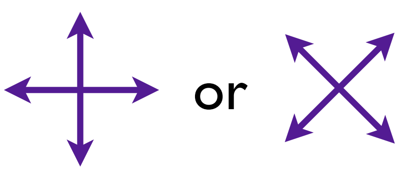
Measure $X \otimes X$

Quantum key distribution

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

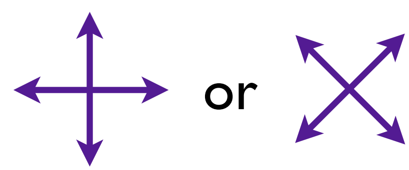
Alice

measure in basis



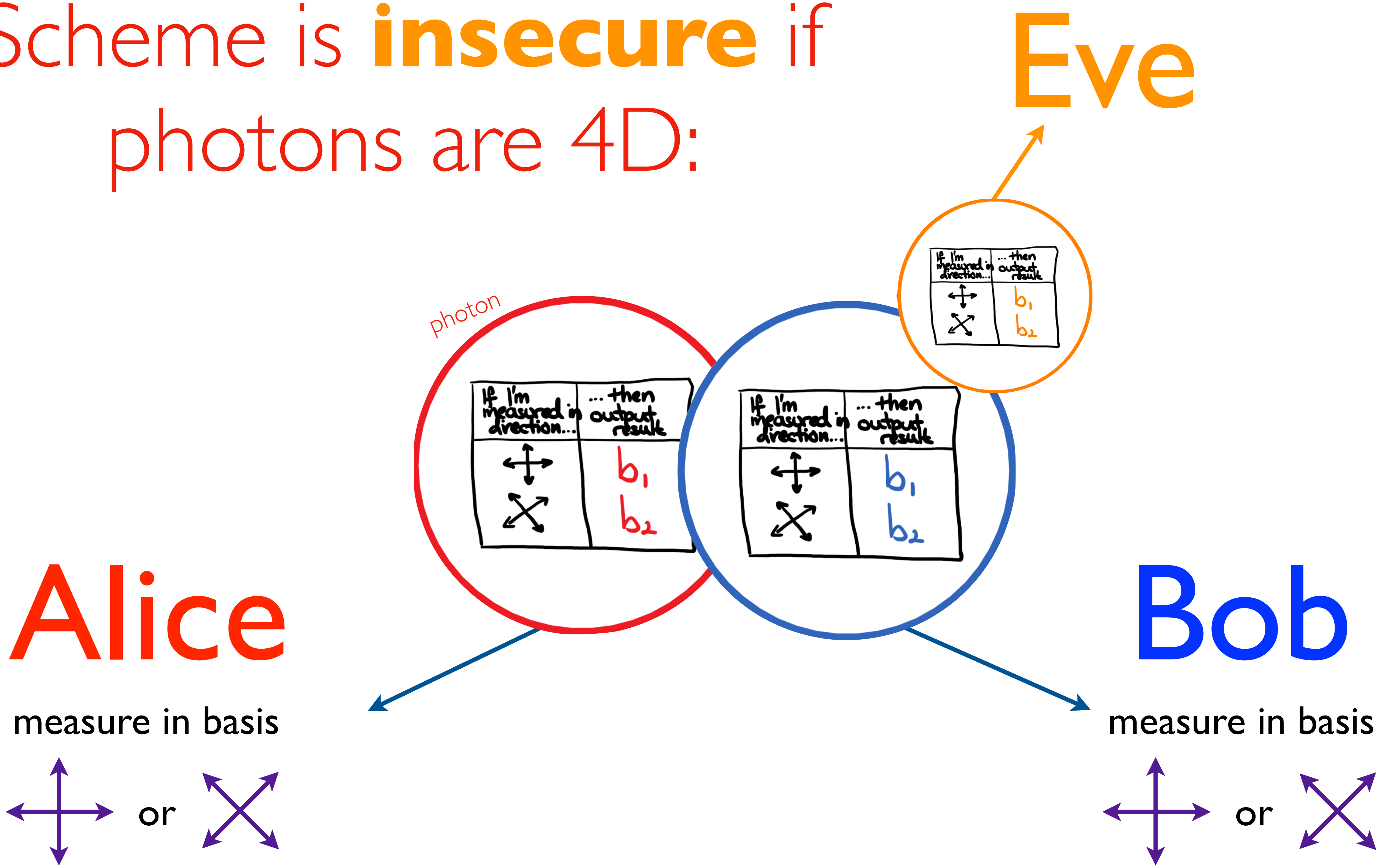
Bob

measure in basis



same basis ⇒ one key bit

Scheme is **insecure** if photons are 4D:



nature International weekly journal of science

current issue ▸ letters ▸ article

NATURE | LETTER

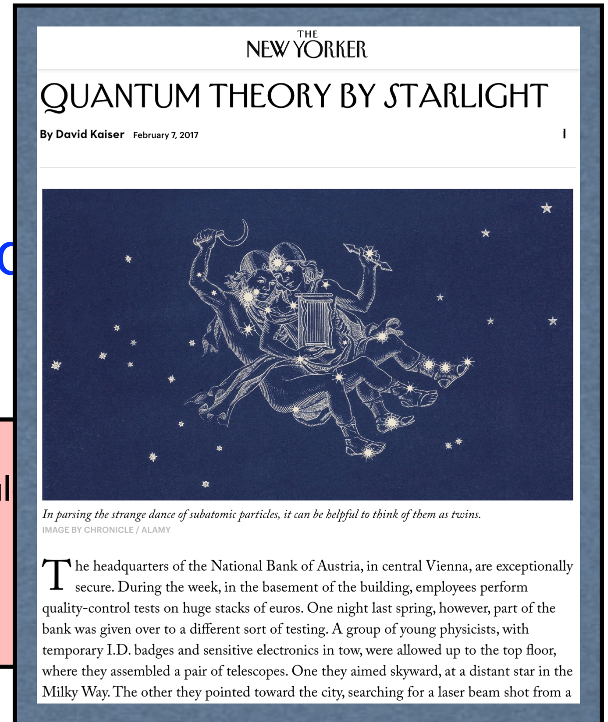
Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau & R. Hanson

Nature **526**, 682–686 (29 October 2015)

Editor's summary

The celebrated Bell inequality, a theorem published by John Bell in 1964, has long served as a basis for experimentally testing whether nature satisfies local realism. All experiments conducted to date have implied rejection of local-realist hypotheses. But because of experimental limitations all those tests suffered from loopholes — either the locality or the detection loophole. Here, Ronald Hanson and colleagues perform a Bell test that closes these loopholes. Their results are consistent with a violation of the inequality, although the authors reject local-realist hypotheses by two standard deviations only. The experimental setup allows for improvements in the statistics that may consolidate the result. In addition to its fundamental importance, a loophole-free Bell test is an important building block in quantum information processing.



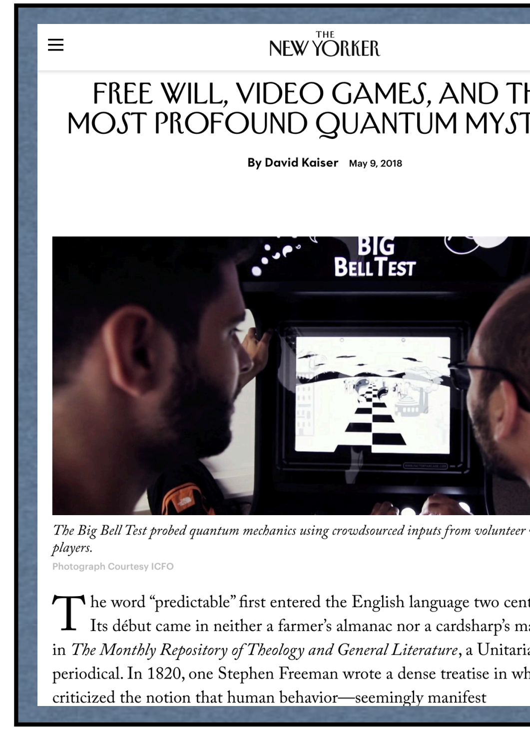
THE NEW YORKER

QUANTUM THEORY BY STARLIGHT

By David Kaiser February 7, 2017

In parsing the strange dance of subatomic particles, it can be helpful to think of them as twins.
IMAGE BY CHRONICLE / ALAMY

The headquarters of the National Bank of Austria, in central Vienna, are exceptionally secure. During the week, in the basement of the building, employees perform quality-control tests on huge stacks of euros. One night last spring, however, part of the bank was given over to a different sort of testing. A group of young physicists, with temporary I.D. badges and sensitive electronics in tow, were allowed up to the top floor, where they assembled a pair of telescopes. One they aimed skyward, at a distant star in the Milky Way. The other they pointed toward the city, searching for a laser beam shot from a



THE NEW YORKER

FREE WILL, VIDEO GAMES, AND TH MOST PROFOUND QUANTUM MYST

By David Kaiser May 9, 2018

The Big Bell Test probed quantum mechanics using crowdsourced inputs from volunteer players.
Photograph Courtesy ICFO

The word "predictable" first entered the English language two cent Its début came in neither a farmer's almanac nor a cardsharp's m in *The Monthly Repository of Theology and General Literature*, a Unitari periodical. In 1820, one Stephen Freeman wrote a dense treatise in wh criticized the notion that human behavior—seemingly manifest

Alice

X

different!

same

(just like in the QKD protocol,
same question ⇒ same answer)

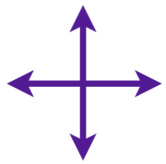
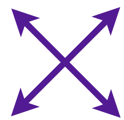
Classical devices win with probability ≤ 75%

Entangled quantum devices can win with probability 85%

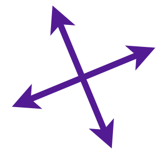
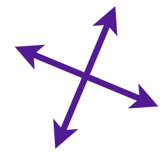
Optimal quantum strategy

$$\frac{1}{\sqrt{2}}\left(|{\color{red}0}{\color{blue}0}\rangle + |{\color{red}1}{\color{blue}1}\rangle\right)$$

Alice measures

 or 

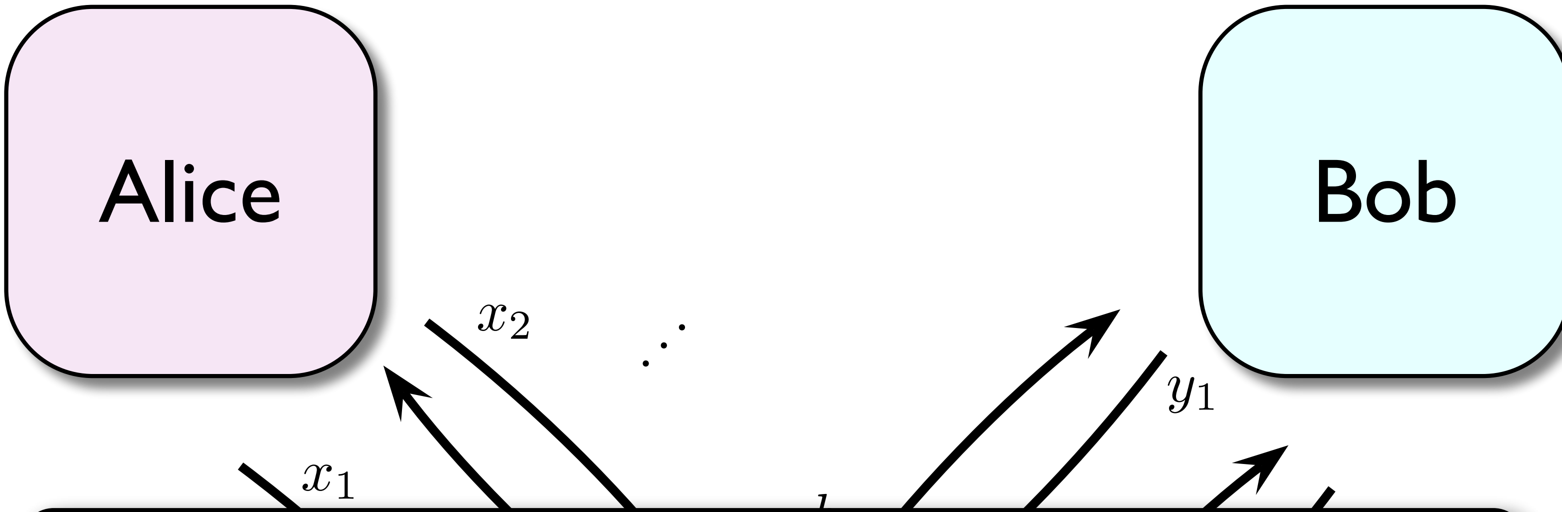
Bob measures

 or 

Theorem: This is the *only* way of winning with 85% probability.

Pr[win] ≥ 85%-ε ⇒ State and measurements are √ε-close to above strategy (up to local isometries)

To establish <u>many</u> qubits of entanglement, consider <u>many</u> CHSH games



Main Theorem:

If $\Pr[\text{win} \approx 85\% \text{ of games}] \approx 1$

$\Rightarrow$ W.h.p. for a random set of $n^{1/c}$ sequential games,

Devices' strategy $\approx$ Ideal strategy

Secure channel

Device-Independent QKD

- Assumptions:
  1. Authenticated classical communication
  2. Random bits can be generated locally
  3. Isolated laboratories
  4. Quantum theory is correct

~~Computational assumptions~~

~~Trusted devices~~

quantum computer

How do you know it works?

- For some problems, you can check the answer

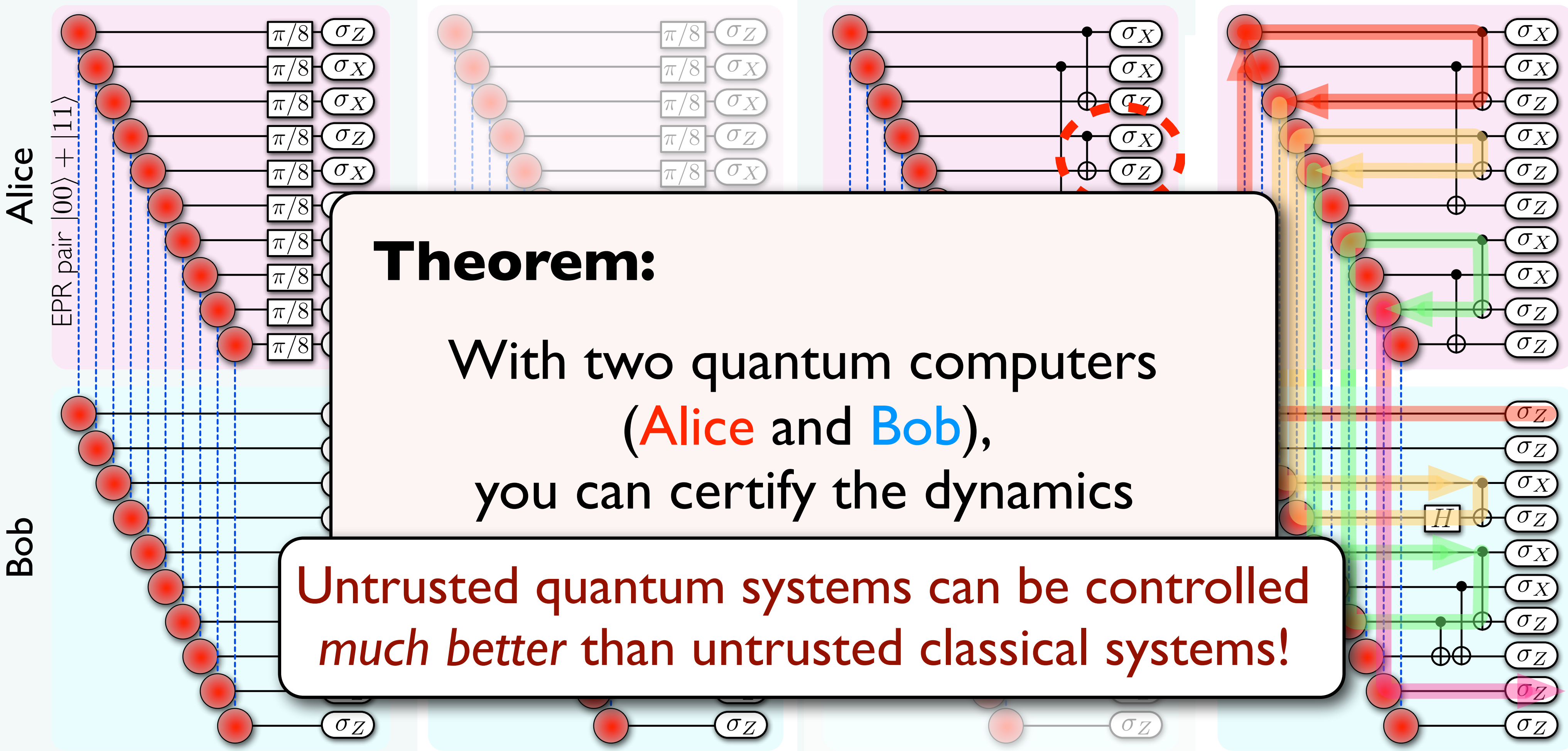
$3 \times 5 = 15$

- But not always! (e.g., quantum simulation)

Secure delegated quantum computation

Run one of four protocols, at random:

(a) CHSH games **(b) State tomography** **(c) Process tomography** **(d) Computation**



Theorem:

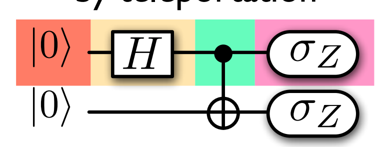
With two quantum computers (Alice and Bob), you can certify the dynamics

Untrusted quantum systems can be controlled *much better* than untrusted classical systems!

ask Bob to prepare resource states on Alice's side by collapsing EPR pairs (Alice can't tell the difference)

ask Alice to apply Bell measurements (Bob can't tell the difference)

by teleportation



Theorem: If tests a-c pass w.h.p., then protocol d's output is correct.

Dimension test

Entanglement test

Nonlocality test

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

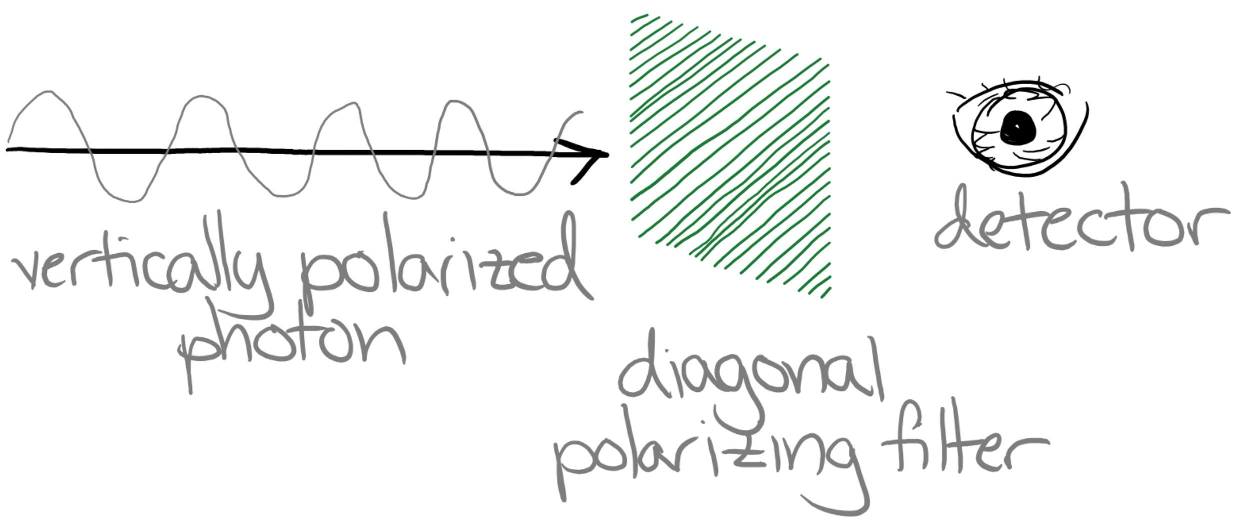
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

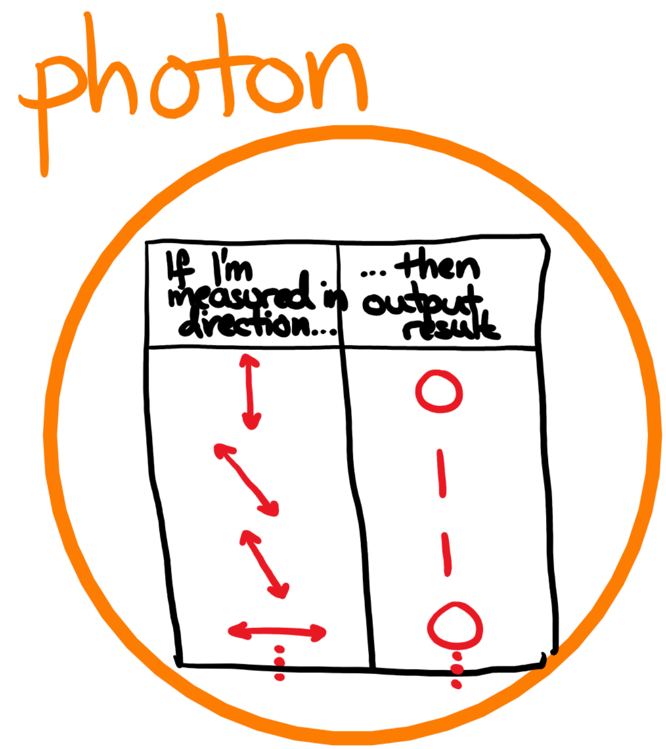
A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

Does God play dice?

(Is the universe random or deterministic?)





Local hidden variable model

Models for the universe

Local realist

Einstein-Podolsky-Rosen

① "Local" : Alice's result depends only on measurement setting
(no faster-than-light communication from Bob)

② "Realist" = deterministic

Quantum

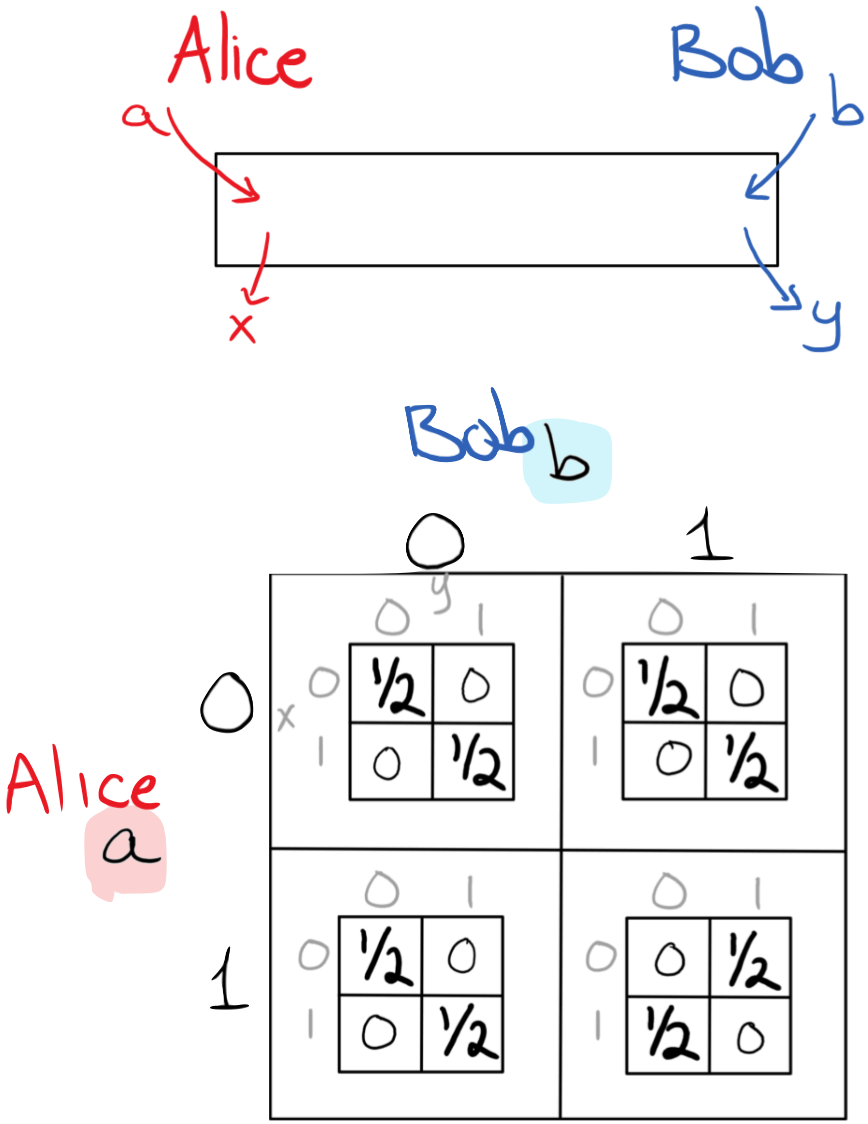
✕ game with

Local realist = 75%

Quantum ≈ 85%

What about a local *randomized* classical model?

Popescu-Rohrlich nonlocal box



- Each player's marginal output distⁿ depends only on her input (no FTL comm.)
- But $x + y = a \cdot b \pmod 2$ always!

Models for the universe

Local realist

Einstein-Podolsky-Rosen

① "Local" : Alice's result depends only on measurement setting (no faster-than-light communication from Bob)

② "Realist" = deterministic

Quantum

"Nonsignaling" (local randomized)

× game with

Local realist = 75%

Quantum ≈ 85%

NS = 100%

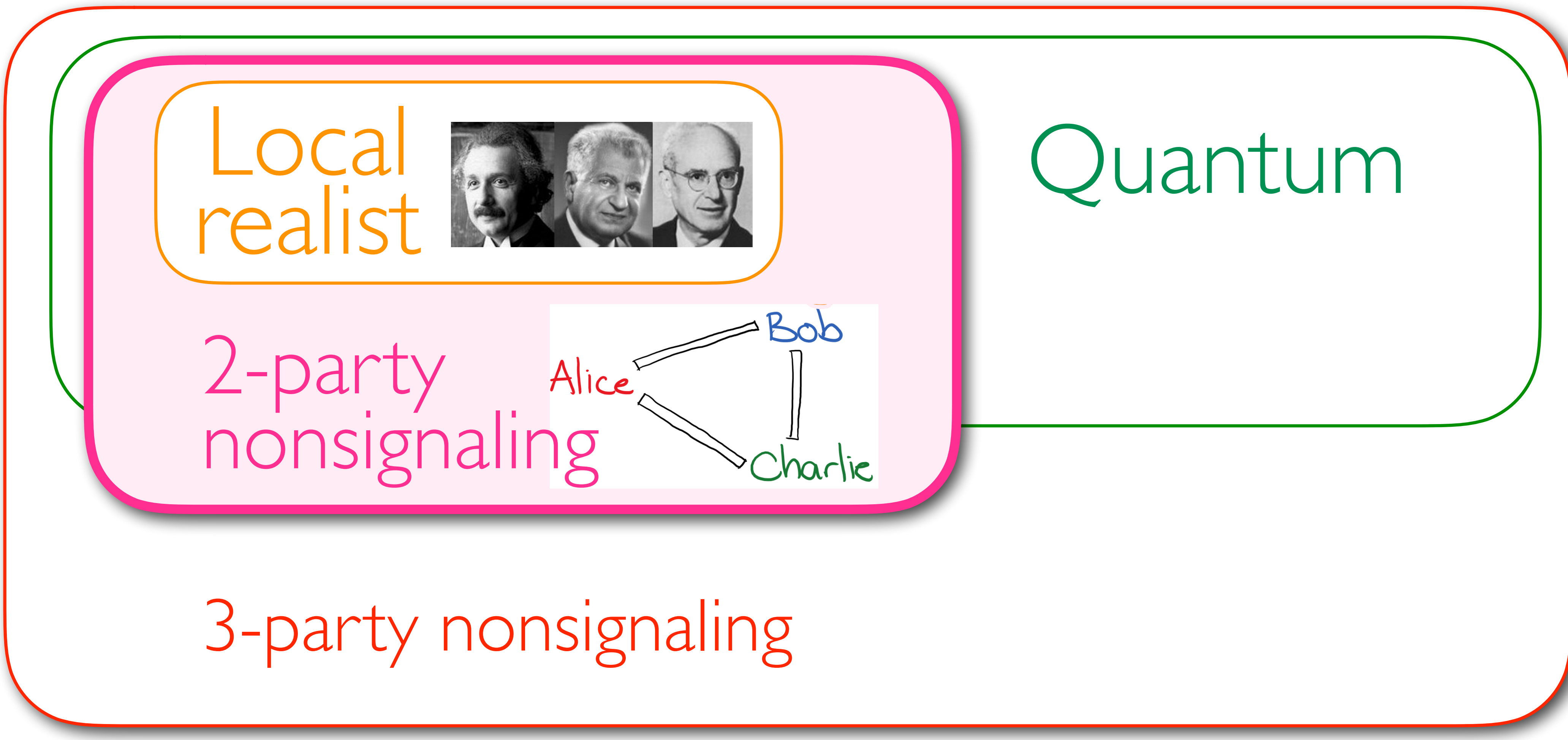
Models with 3 parties

Theorem:

There exists a 3-party game with

Quantum ≥ 92.6%

2-party NS ≤ 87.5%

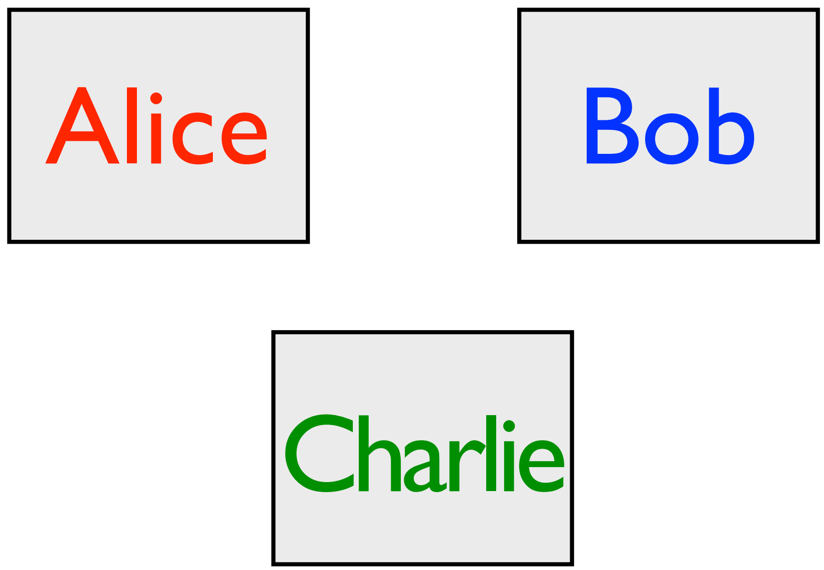


Theorem:

There exists a 3-party game with

Quantum $\geq$ 92.6%

2-party NS $\leq$ 87.5%



Alice-Charlie

Ⓐ Consistency subgame

$a = c = 0$

want outputs $x = z$

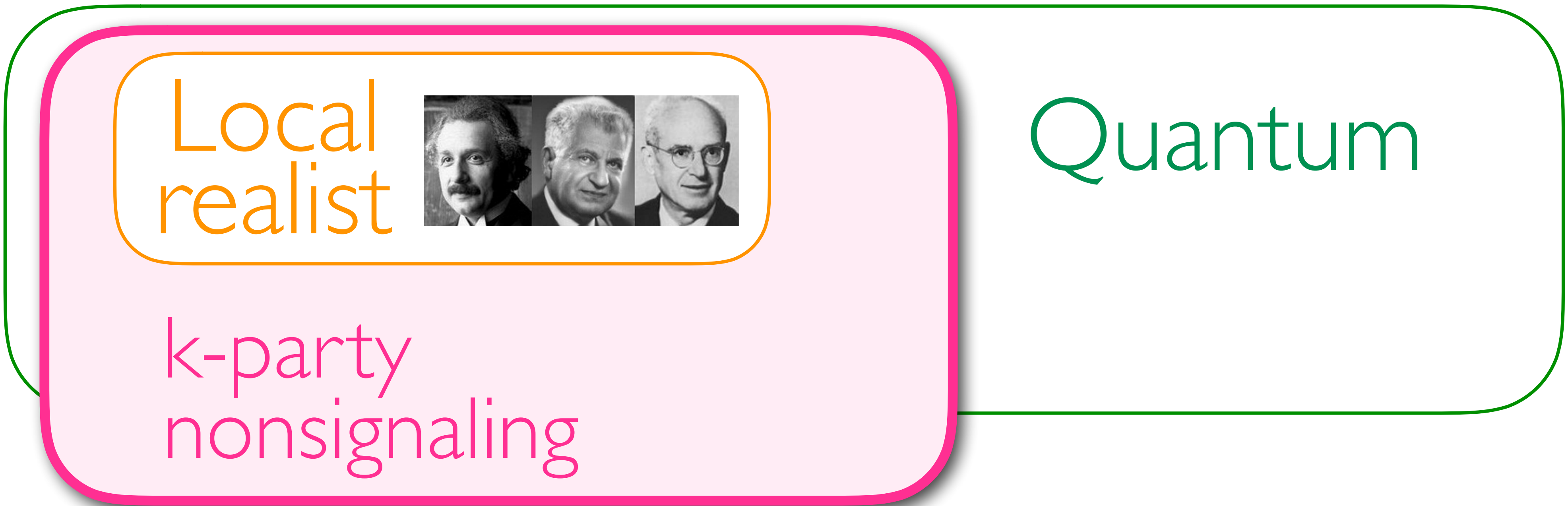
Alice-Bob

Ⓑ CHSH subgame

$c = 1$

want $x + y = ab + z \pmod 2$

Models with k+1 parties



Theorem:

There exists a (k+1)-party game with

(Quantum - k-party NS) > ε

k+1	CHSH gap	Best CHSH$_n$ gap
3	$5.178 \cdot 10^{-2}$	$4.272 \cdot 10^{-2}$ (with $n = 3$)
4	$2.071 \cdot 10^{-2}$	$2.318 \cdot 10^{-2}$ ($n = 4$)
5	$7.397 \cdot 10^{-3}$	$1.079 \cdot 10^{-2}$ ($n = 5$)
6	$2.526 \cdot 10^{-3}$	$4.454 \cdot 10^{-3}$ ($n = 8$)
7	$8.488 \cdot 10^{-4}$	$1.695 \cdot 10^{-3}$ ($n = 13$)
8	$2.837 \cdot 10^{-4}$	$6.122 \cdot 10^{-4}$ ($n = 22$)

Local realist

k-party nonsignaling

Quantum

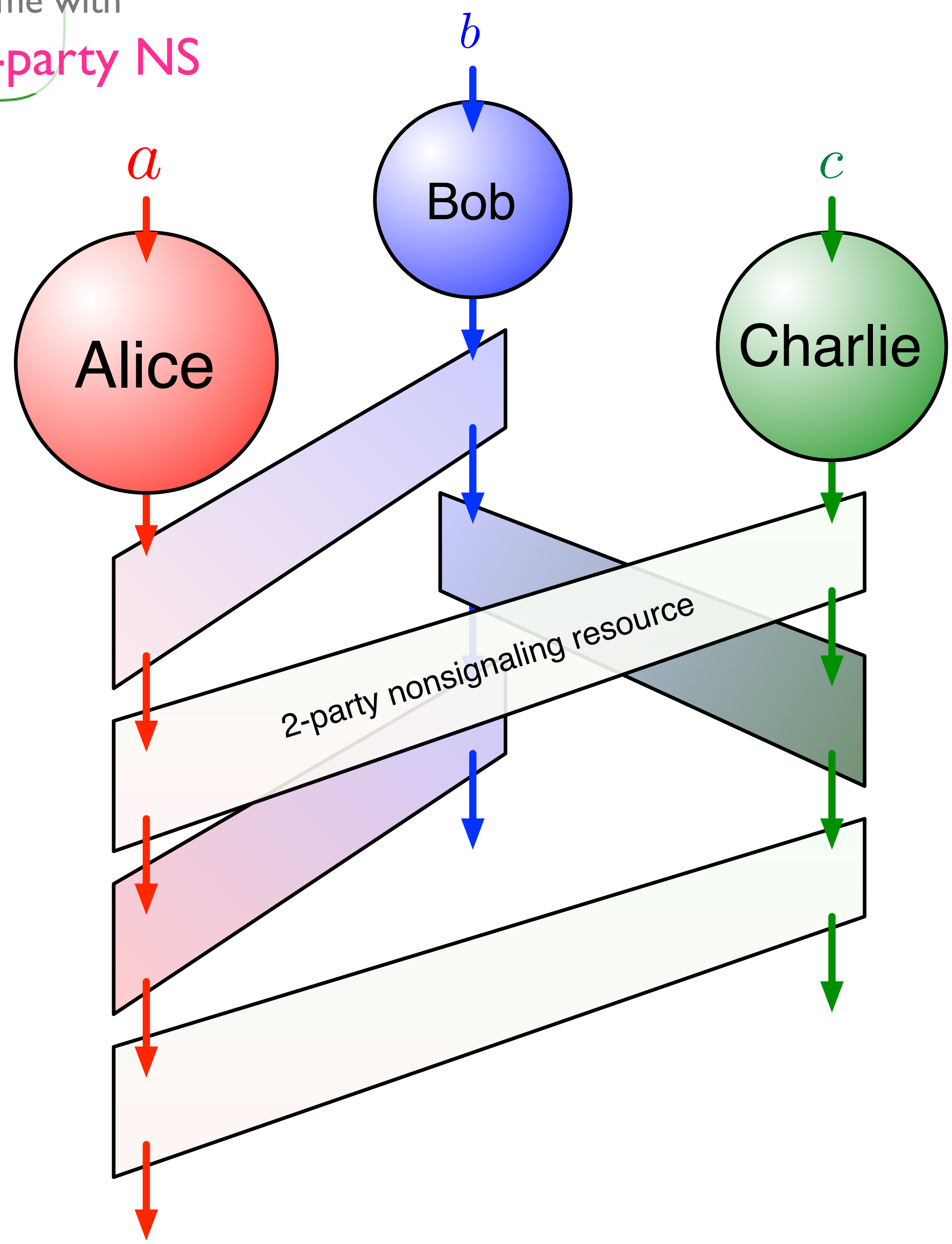
✕ (k+1)-party game with

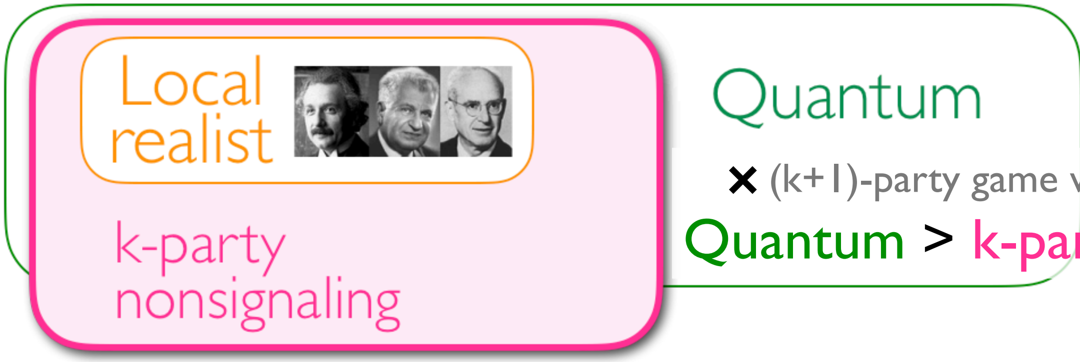
Quantum > k-party NS

Main proof difficulty:

Upper-bounding success probability for k-party nonsignaling

Adaptive strategies



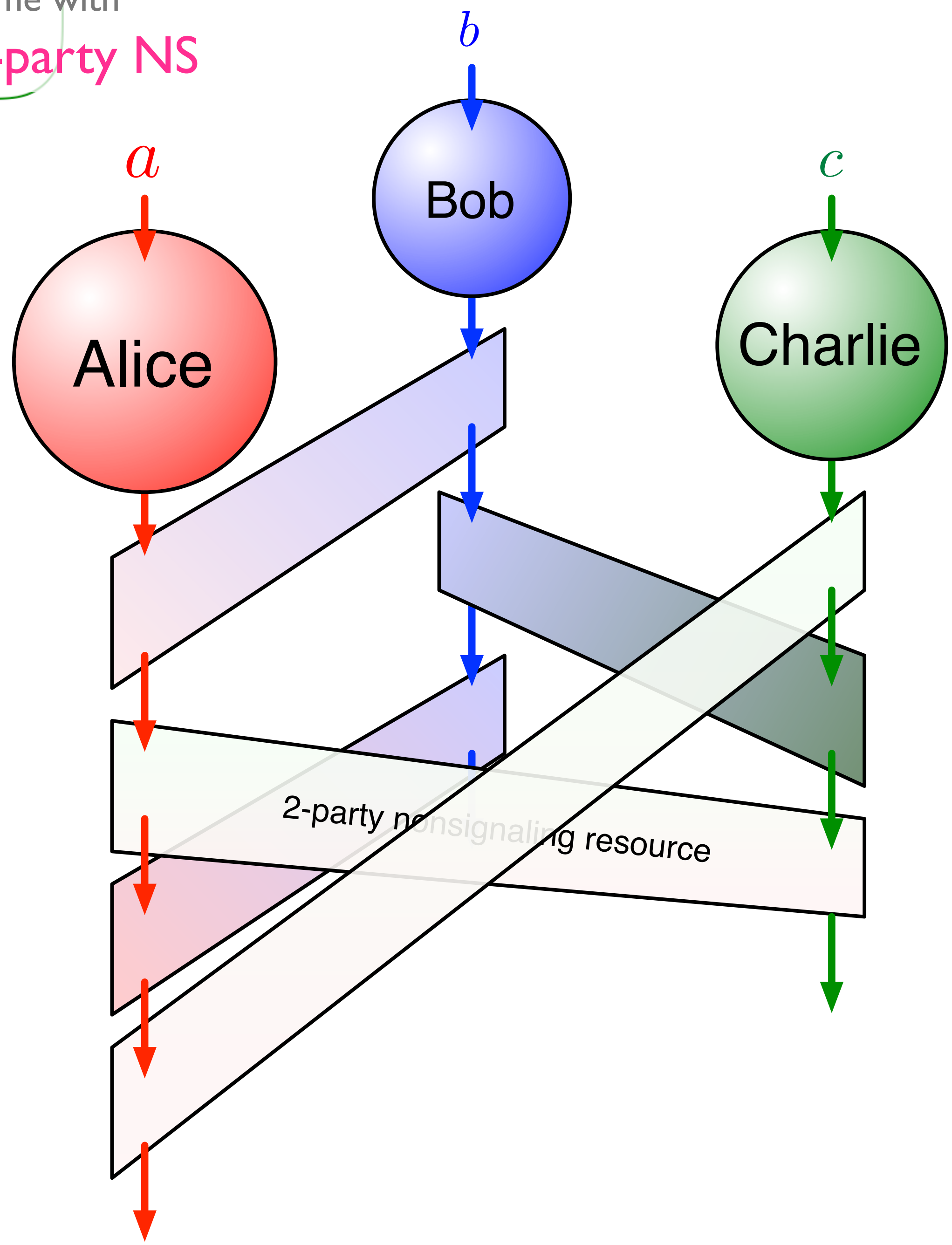


✕ (k+1)-party game with
Quantum > k-party NS

Main proof difficulty:

Upper-bounding success probability for k-party nonsignaling

Adaptive strategies



Dimension test

Entanglement test

Nonlocality test

Fault-tolerance test

Shor's algorithm
factors a 1024-bit numbers
using 10^{11} gates on 5000 qubits
⇒ need error $< 10^{-11}$ per gate

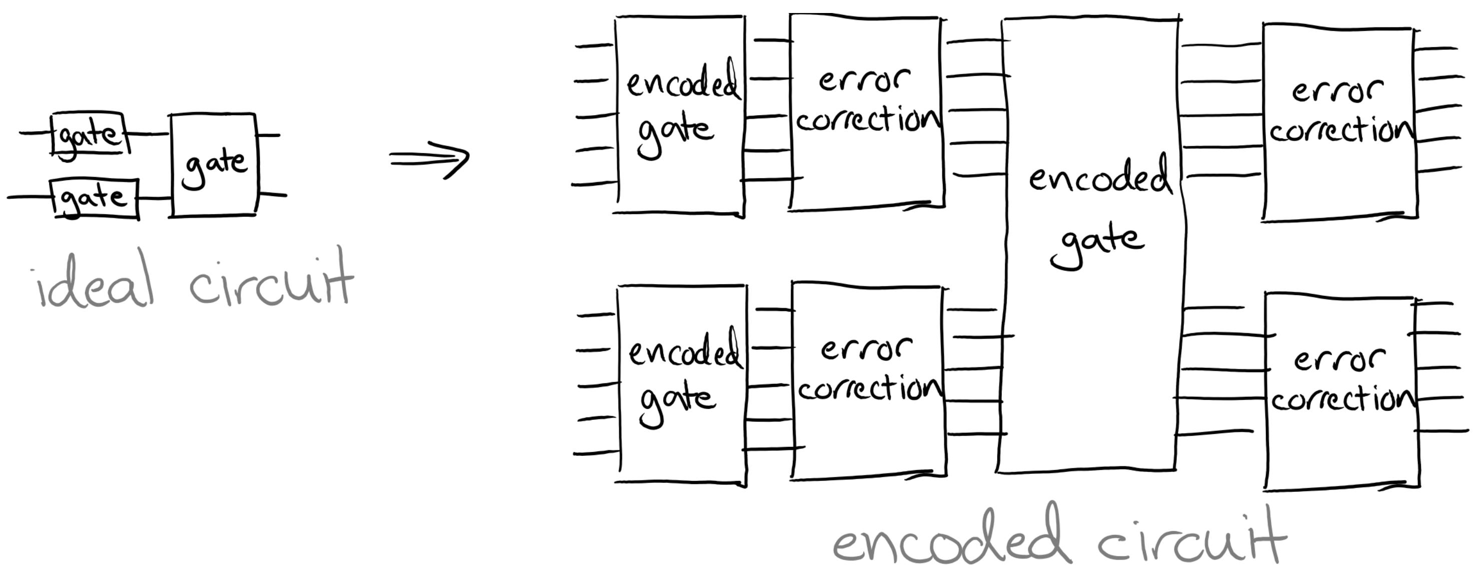
But typical noise rates are 10^{-2} to 10^{-4} per gate

Operation	Current duration	Current infidelity	Anticipated duration	Anticipated Infidelity
Single-qubit gates	$5\,\mu s$	$5 \cdot 10^{-5}$	$1\,\mu s$	$1 \cdot 10^{-5}$
Entangling (2 qubits)	$40\,\mu s$	$1 \cdot 10^{-2}$	$15\,\mu s$	$2 \cdot 10^{-4}$

Assessing the progress of trapped-ion processors towards fault-tolerant quantum computation

A. Bermudez, X. Xu, R. Nigmatullin, J. O'Gorman, V. Negnevitsky, P. Schindler, T. Monz, U. G. Poschinger, C. Hempel, J. Home, F. Schmidt-Kaler, M. Biercuk, R. Blatt, S. Benjamin, M. Müller

Fault tolerance is amazing!



Will fault tolerance work?

Threshold theorems are for ideal models, <u>might not apply to real noise</u>

1. Noise might be *correlated*

2. *Coherent* noise might have quadratically lower tolerable noise rates

Stochastic noise: $p + p + \cdots + p = np$

Coherent noise: $e^{i\theta} \times e^{i\theta} \times \cdots \times e^{i\theta} = e^{ni\theta}$

$\downarrow$

$n^2\theta^2$ error probability

Will fault tolerance work?

Threshold theorems are for ideal models, <u>might not apply to real noise</u>

1. Noise might be *correlated*
2. *Coherent* noise might have quadratically lower tolerable noise rates

How will fault tolerance work?

Concatenated codes

Good for low noise rates

Surface codes

Good with limited (2D) qubit connections

Will fault tolerance work?

Threshold theorems are for ideal models, <u>might not apply to real noise</u>

1. Noise might be *correlated*
2. *Coherent* noise might have quadratically lower tolerable noise rates

How will fault tolerance work?

Options:

Many codes,
many ways of using each code,
and they can all be combined

Regimes:

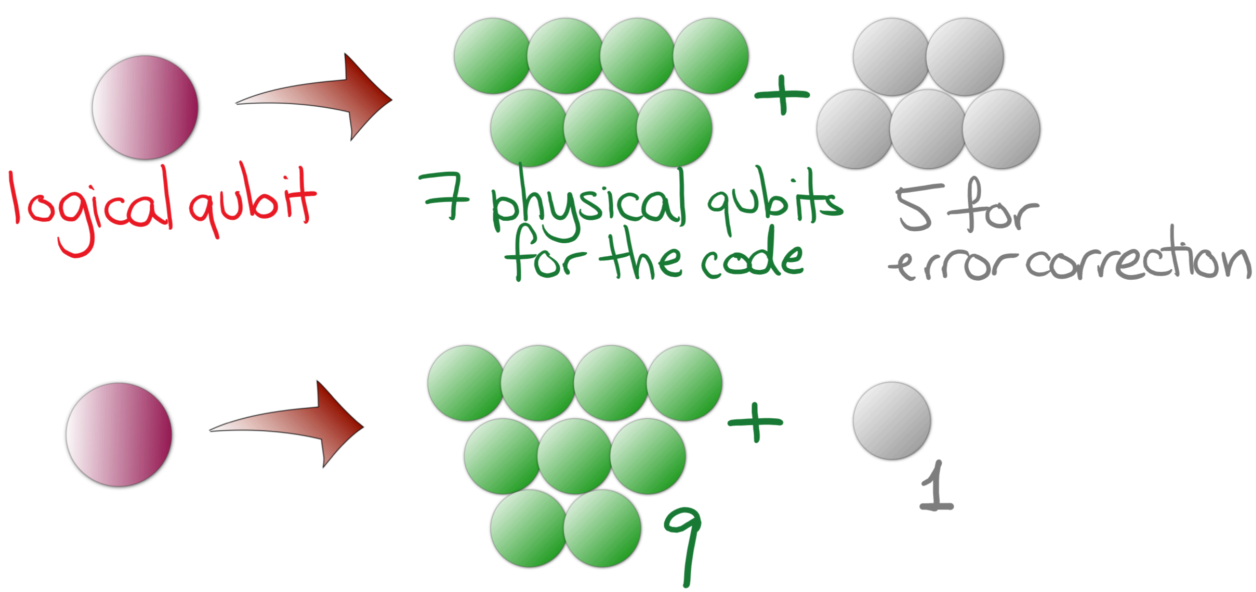
Local vs. ranged gates
Fast vs. slow measurements
Good vs. bad memory
High vs. low errors

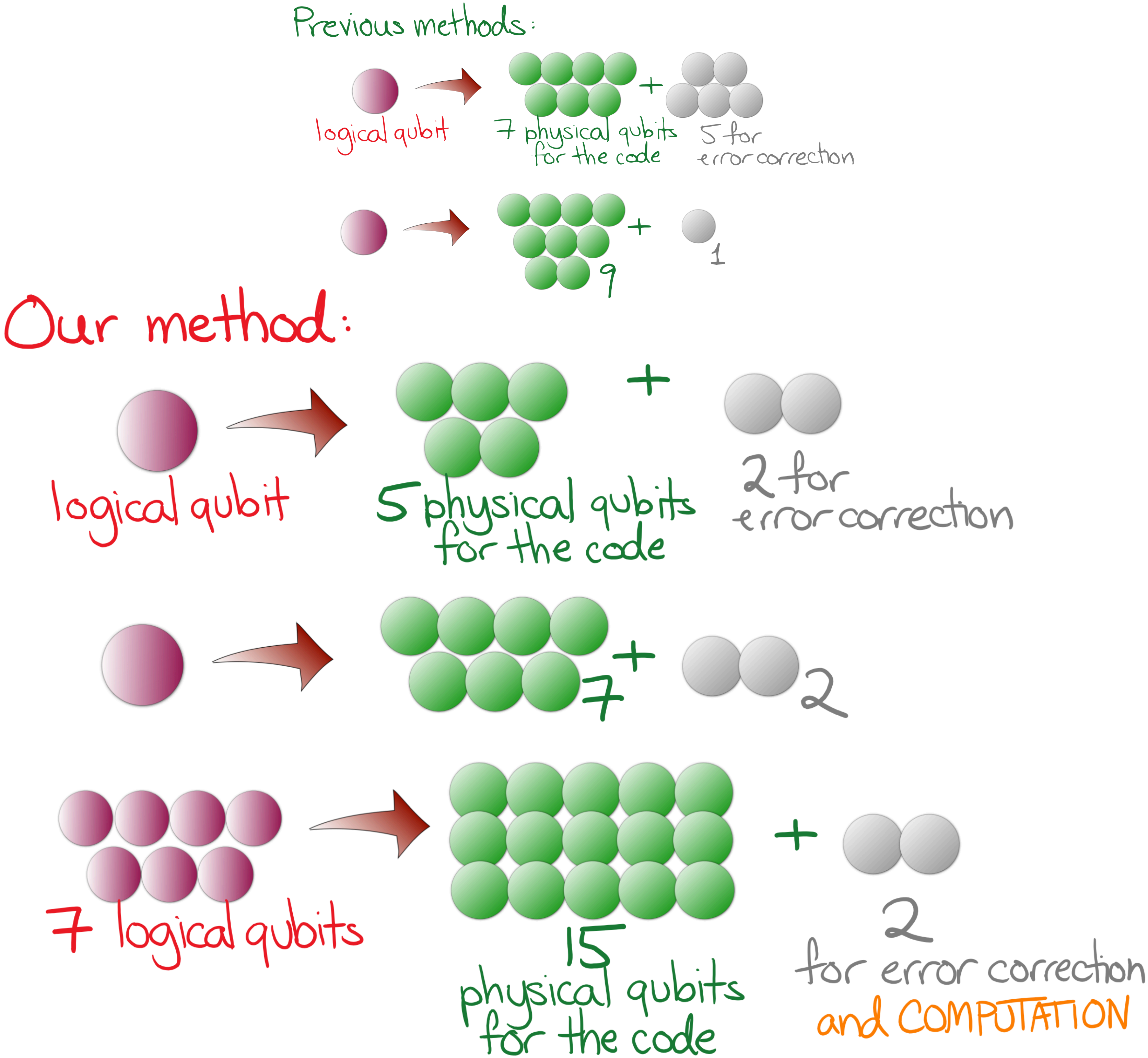
But simulations are difficult & bounds are too conservative

Goal: Implement fault-tolerant error correction and computation on small quantum devices

- to test/demonstrate the theory
- to assess FT schemes' performance in real error models
- to adapt FT schemes to real noise

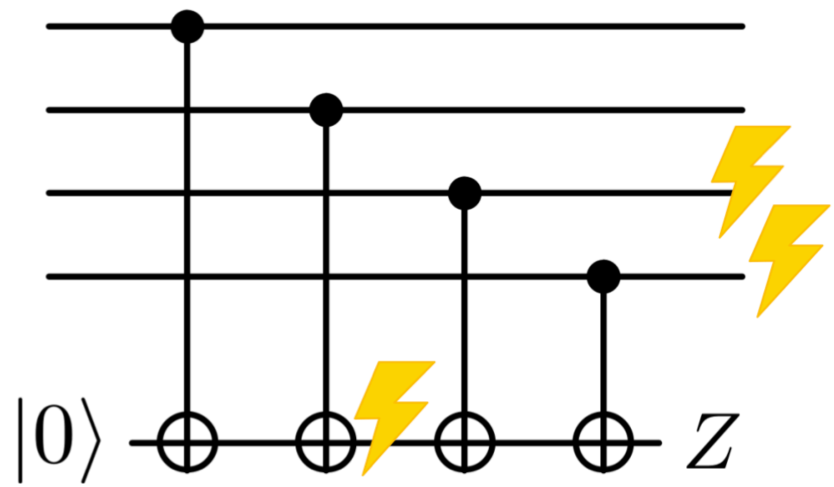
Previous methods:





Previous methods:
logical qubit
7 physical qubits for the code
5 for error correction
9
1
Our method:
logical qubit
5 physical qubits for the code
2 for error correction
7
2
7 logical qubits
15 physical qubits for the code
2 for error correction
and COMPUTATION

<u>Main problem</u>: Errors can spread



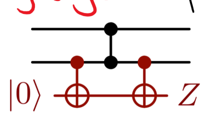
Previous approaches:

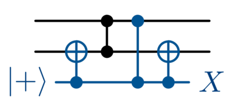
Try to avoid this

<u>Our idea</u>:

Catch the errors that spread

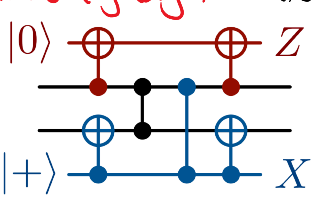
X gadget: applies CZ, catches XX, XY, YX, YY

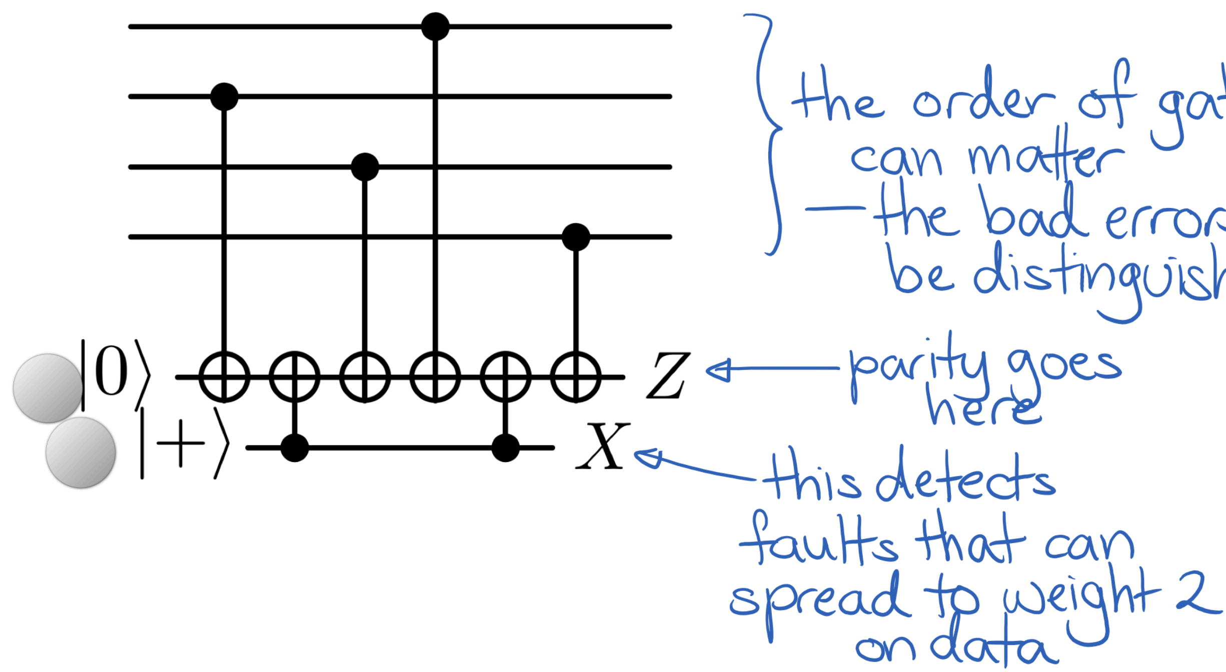




Z gadget: catches ZZ, YX

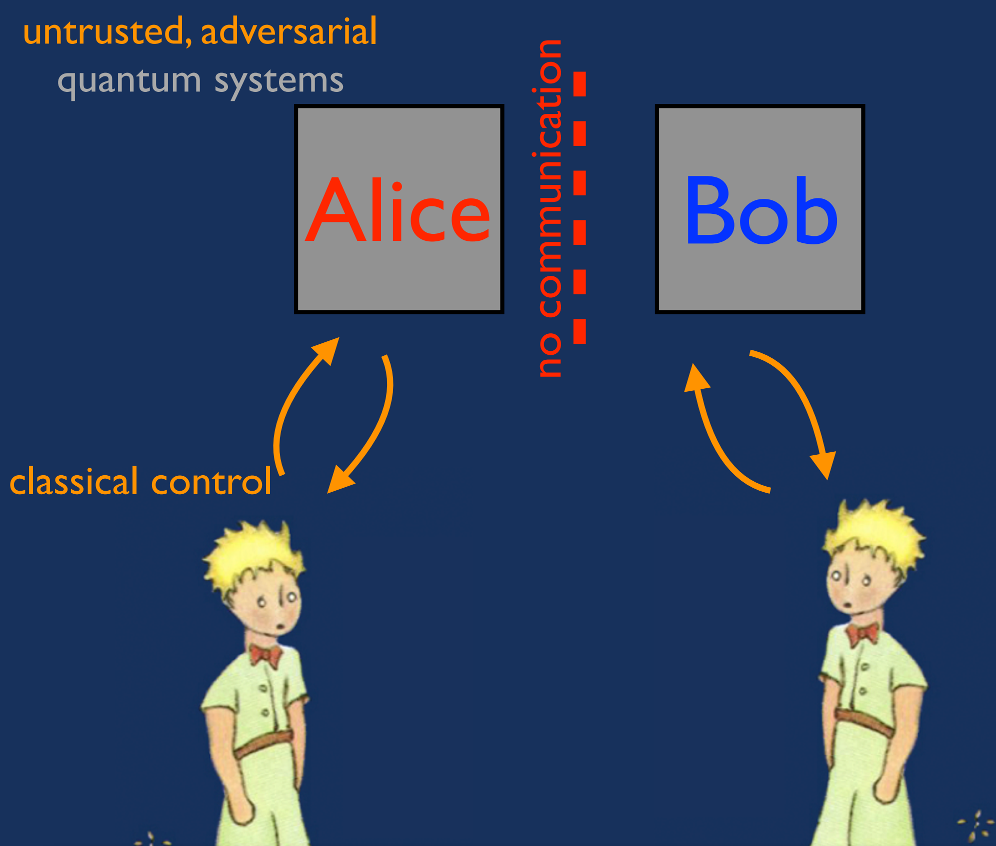
Combined gadget: catches all true 2-qubit failures



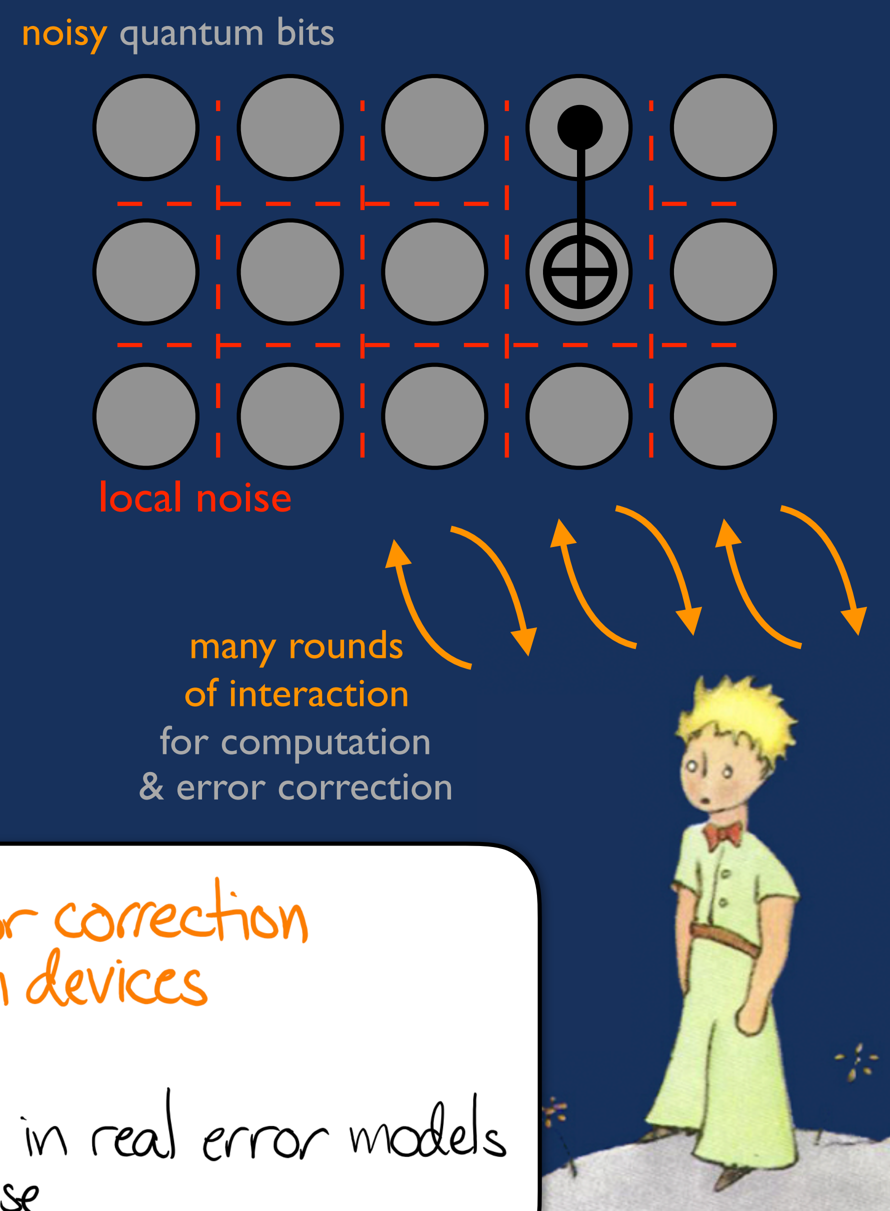


Thank you!

Locality & entanglement tests



Fault-tolerant computation



Goal: Implement fault-tolerant error correction and computation on small quantum devices

- to test/demonstrate the theory
- to assess FT schemes' performance in real error models
- to adapt FT schemes to real noise

nature International weekly journal of science

current issue ▸ letters ▸ article

NATURE | LETTER

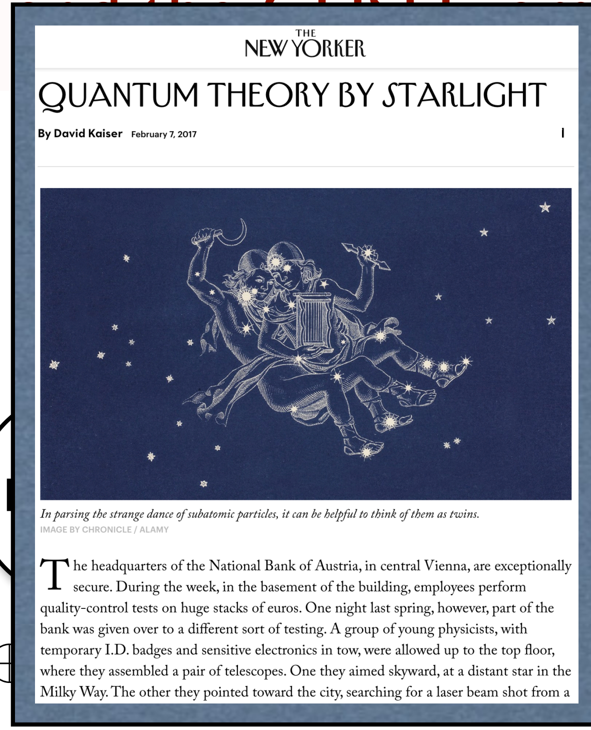
Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau & R. Hanson

Nature **526**, 682–686 (29 October 2015)

Editor's summary

The celebrated Bell inequality, a theorem published by John Bell in 1964, has long served as a basis for experimentally testing whether nature satisfies local realism. All experiments conducted to date have implied rejection of local-realist hypotheses. But because of experimental limitations all those tests suffered from loopholes — either the locality or the detection loophole. Here, Ronald Hanson and colleagues perform a Bell test that closes these loopholes. Their results are consistent with a violation of the inequality, although the authors reject local-realist hypotheses by two standard deviations only. The experimental setup allows for improvements in the statistics that may consolidate the result. In addition to its fundamental importance, a loophole-free Bell test is an important building block in quantum information processing.



THE NEW YORKER

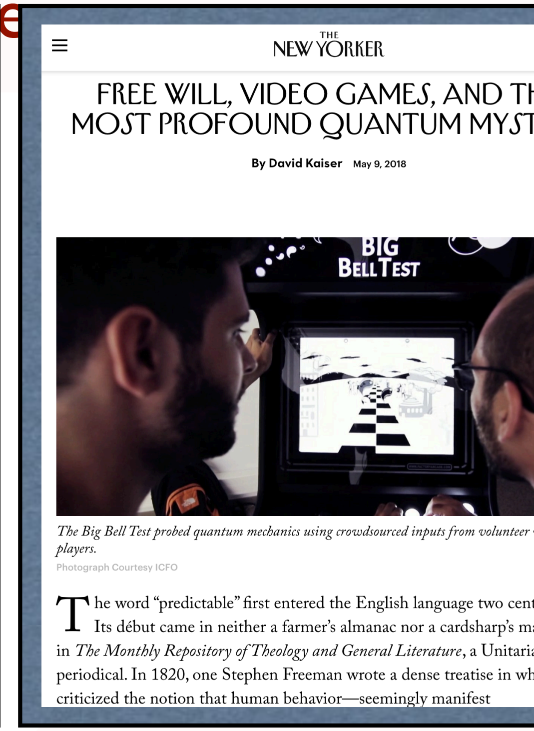
QUANTUM THEORY BY STARLIGHT

By David Kaiser February 7, 2017

In parsing the strange dance of subatomic particles, it can be helpful to think of them as twins.

IMAGE BY CHRONICLE / ALAMY

The headquarters of the National Bank of Austria, in central Vienna, are exceptionally secure. During the week, in the basement of the building, employees perform quality-control tests on huge stacks of euros. One night last spring, however, part of the bank was given over to a different sort of testing. A group of young physicists, with temporary I.D. badges and sensitive electronics in tow, were allowed up to the top floor, where they assembled a pair of telescopes. One they aimed skyward, at a distant star in the Milky Way. The other they pointed toward the city, searching for a laser beam shot from a



THE NEW YORKER

FREE WILL, VIDEO GAMES, AND TH
MOST PROFOUND QUANTUM MYST

By David Kaiser May 9, 2018

The Big Bell Test probed quantum mechanics using crowdsourced inputs from volunteer players.

Photograph Courtesy ICFO

The word "predictable" first entered the English language two cent
Its début came in neither a farmer's almanac nor a cardsharp's m
in *The Monthly Repository of Theology and General Literature*, a Unitari
periodical. In 1820, one Stephen Freeman wrote a dense treatise in wh
criticized the notion that human behavior—seemingly manifest

Classical devices ⇒ Pr[win]≤75%

Quantum devices can win with prob. up to ≈85%

Test for "quantum-ness"

Play game 10^6 times. If the devices win ≥800,000, say they're quantum.