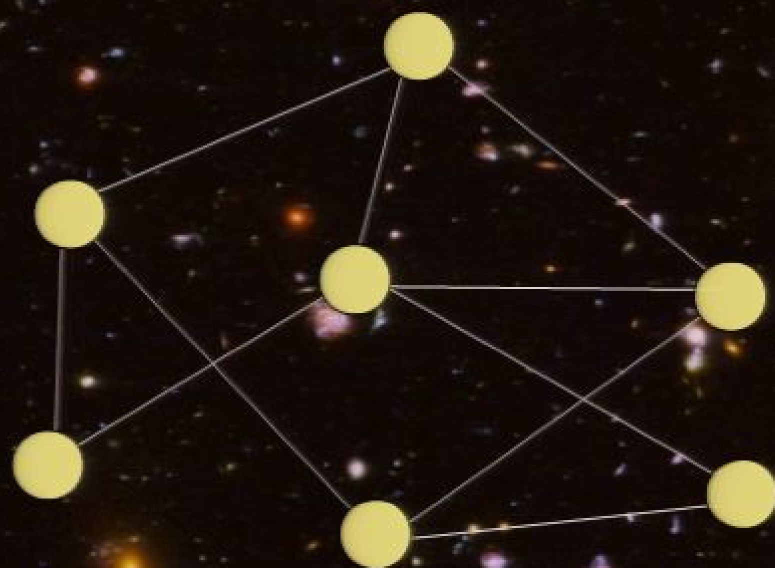
Title: Limits on efficient computation in the physics world

Date: Mar 15, 2006 04:00 PM

URL: http://pirsa.org/06030013

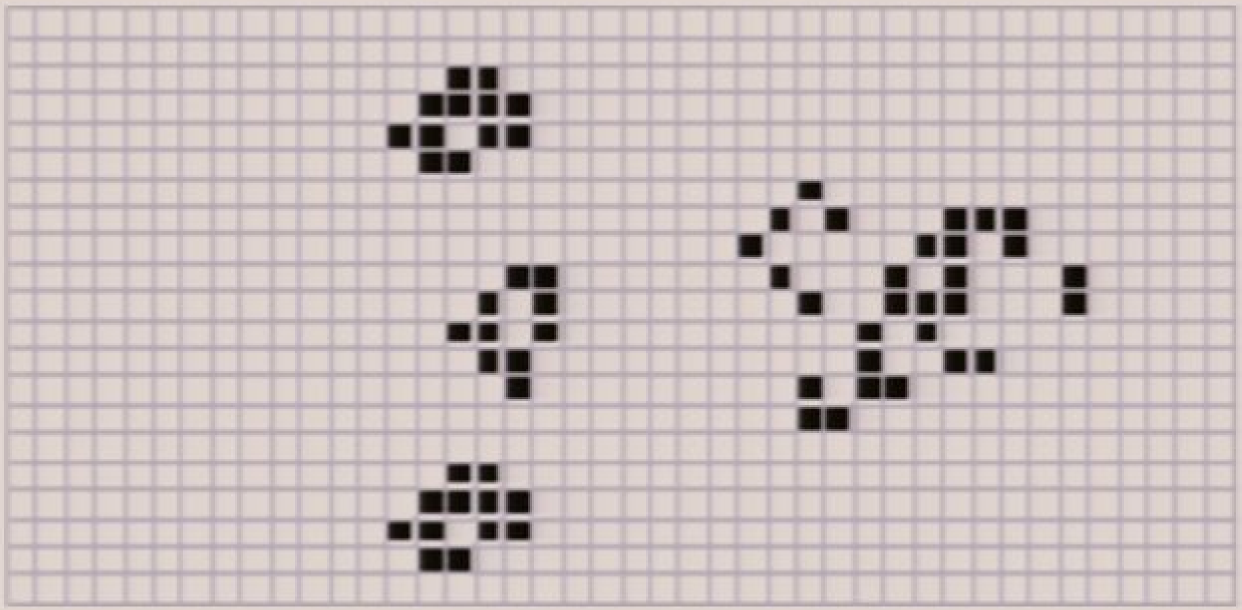
Abstract:

Limits on Efficient Computation in the Physical World



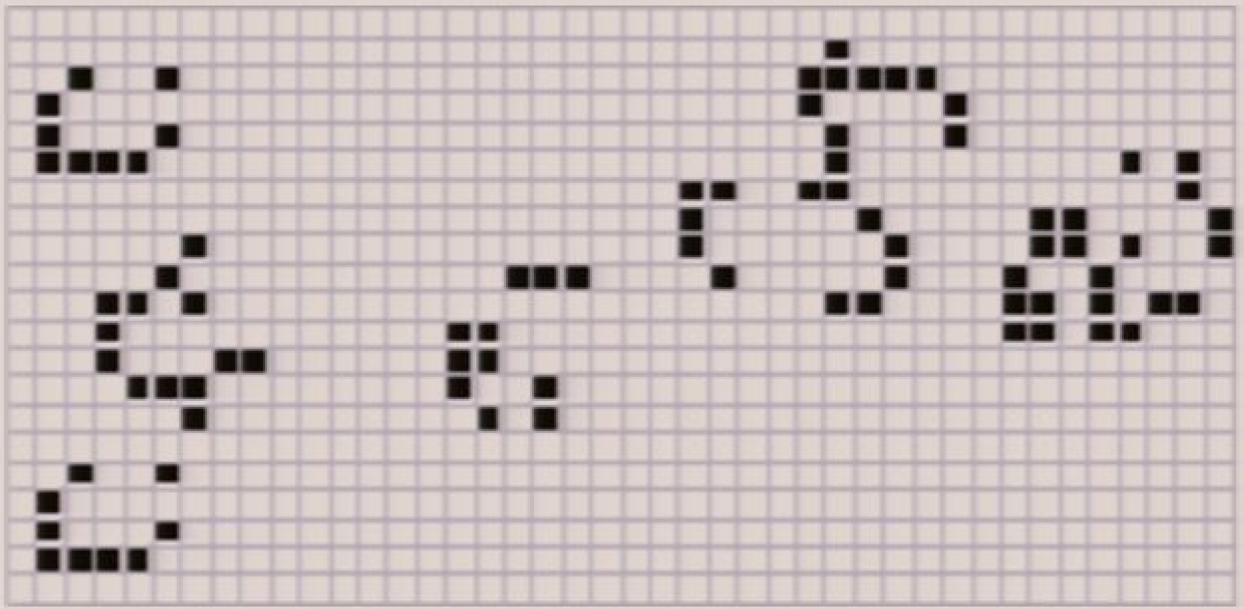
Scott Aaronson
University of Waterloo

The Computer Science Picture of Reality



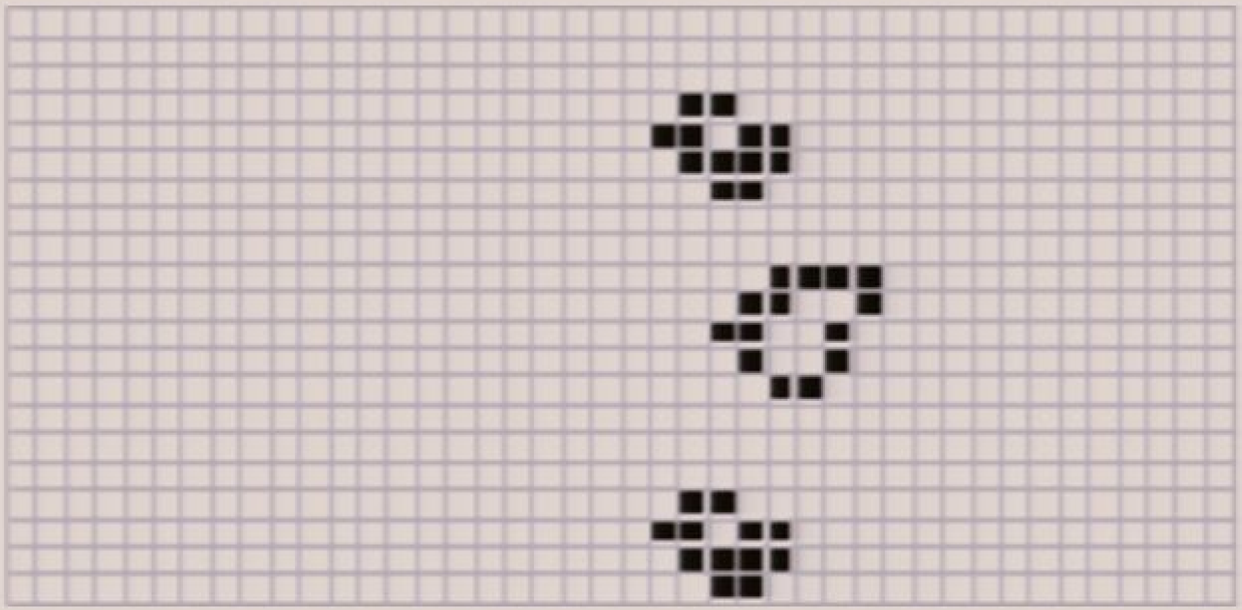
+ details

The Computer Science Picture of Reality



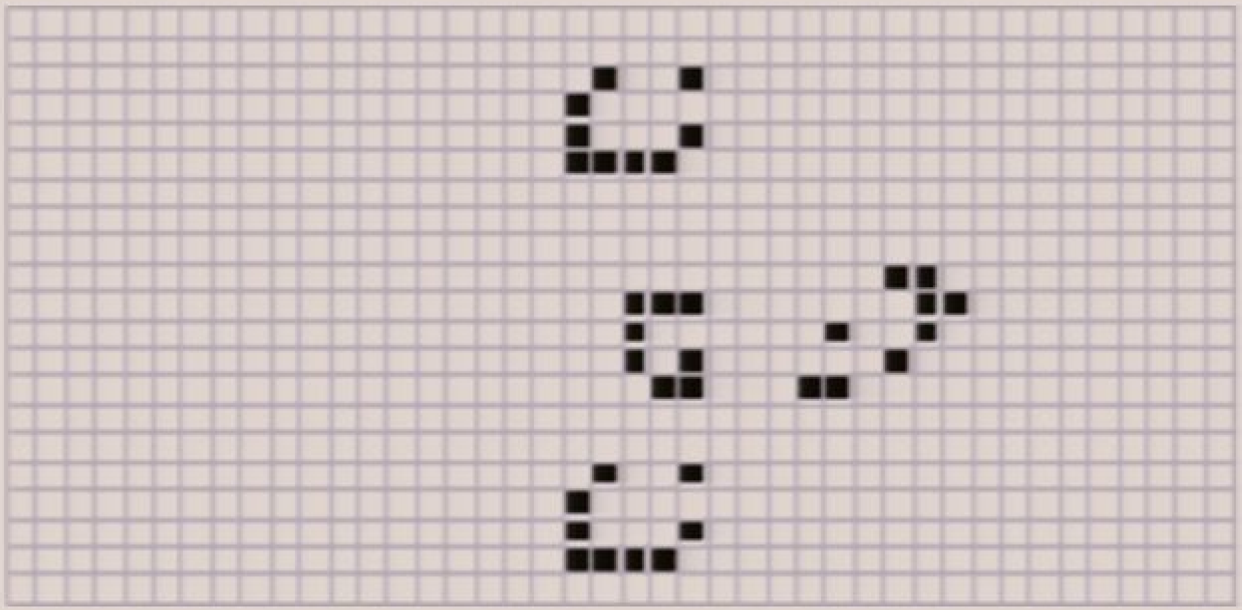
+ details

The Computer Science Picture of Reality



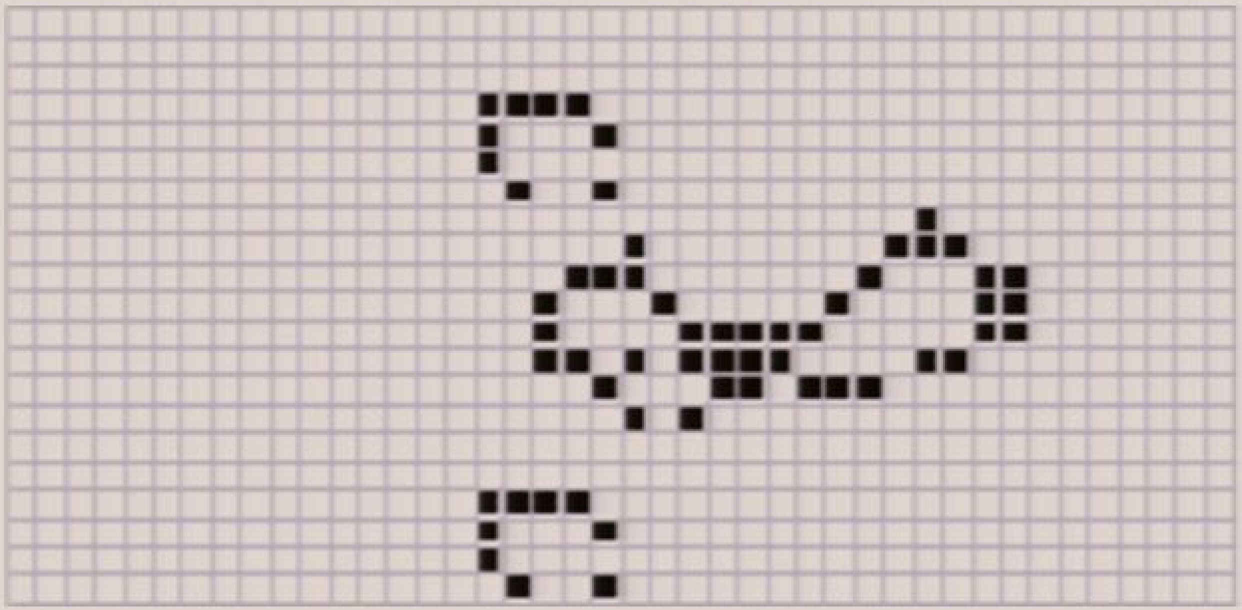
+ details

The Computer Science Picture of Reality



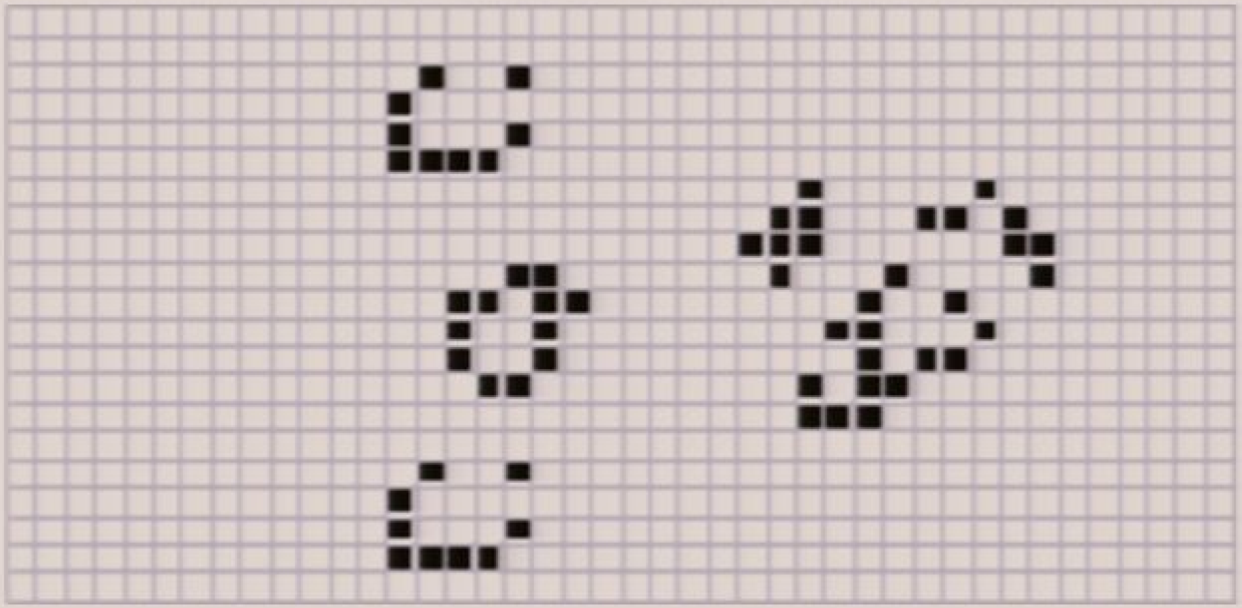
+ details

The Computer Science Picture of Reality



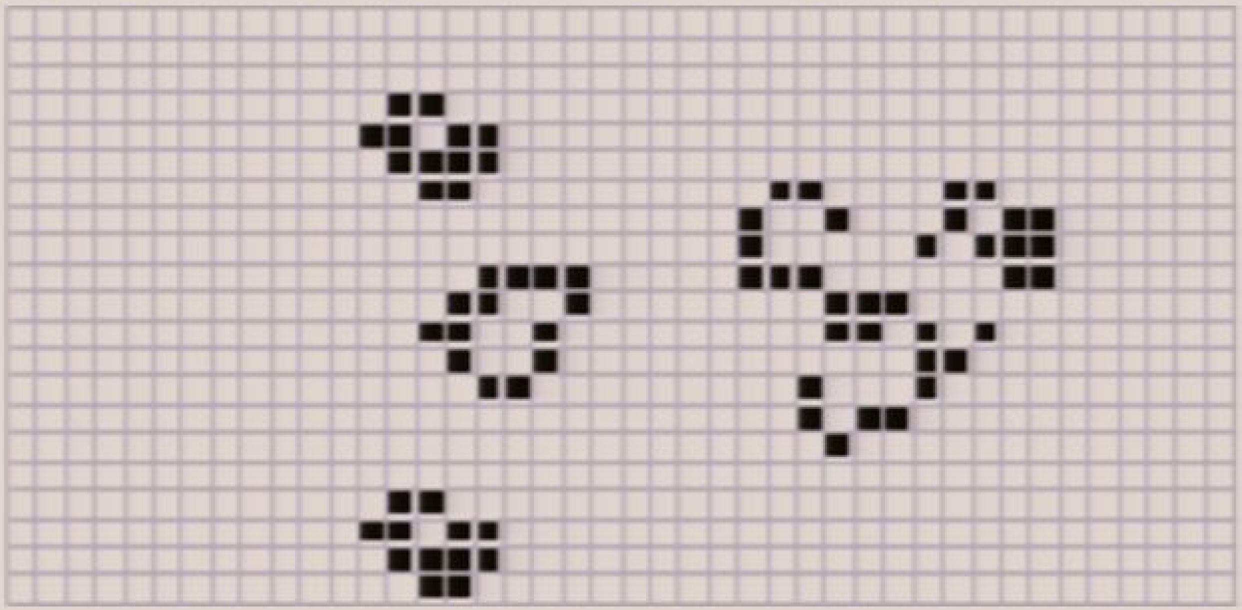
+ details

The Computer Science Picture of Reality



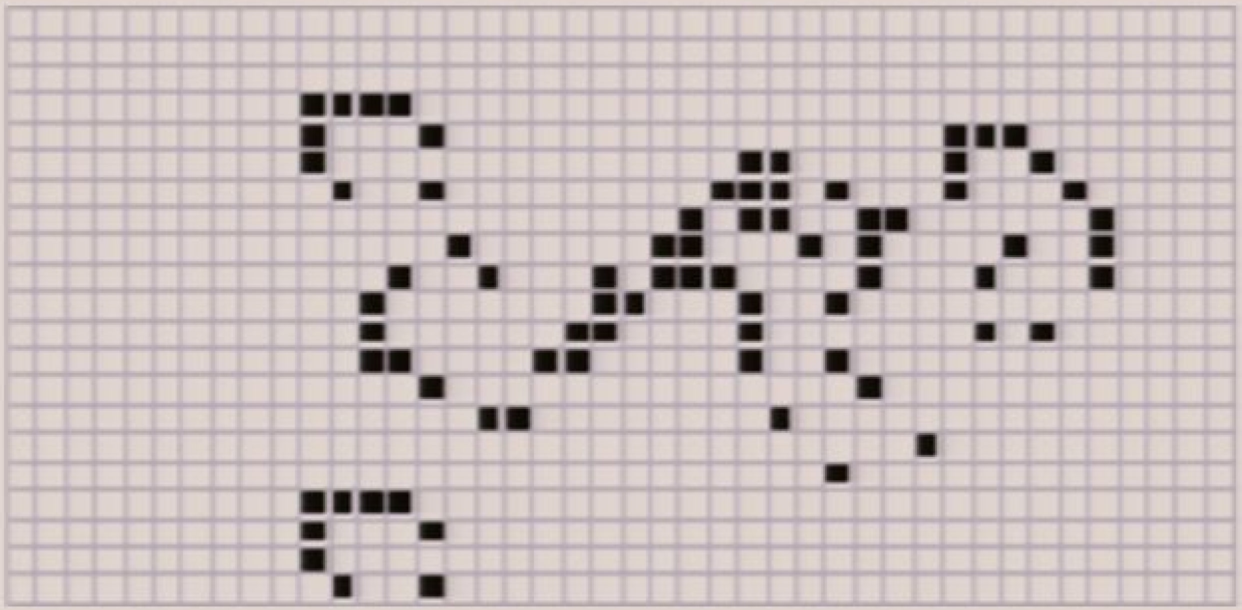
+ details

The Computer Science Picture of Reality



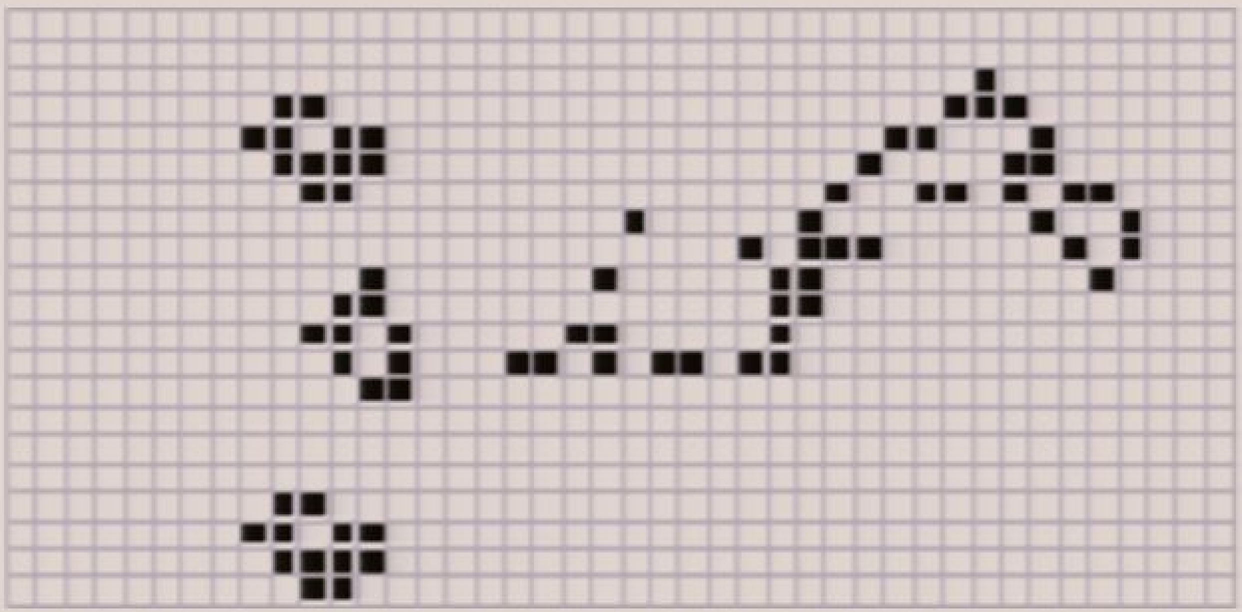
+ details

The Computer Science Picture of Reality



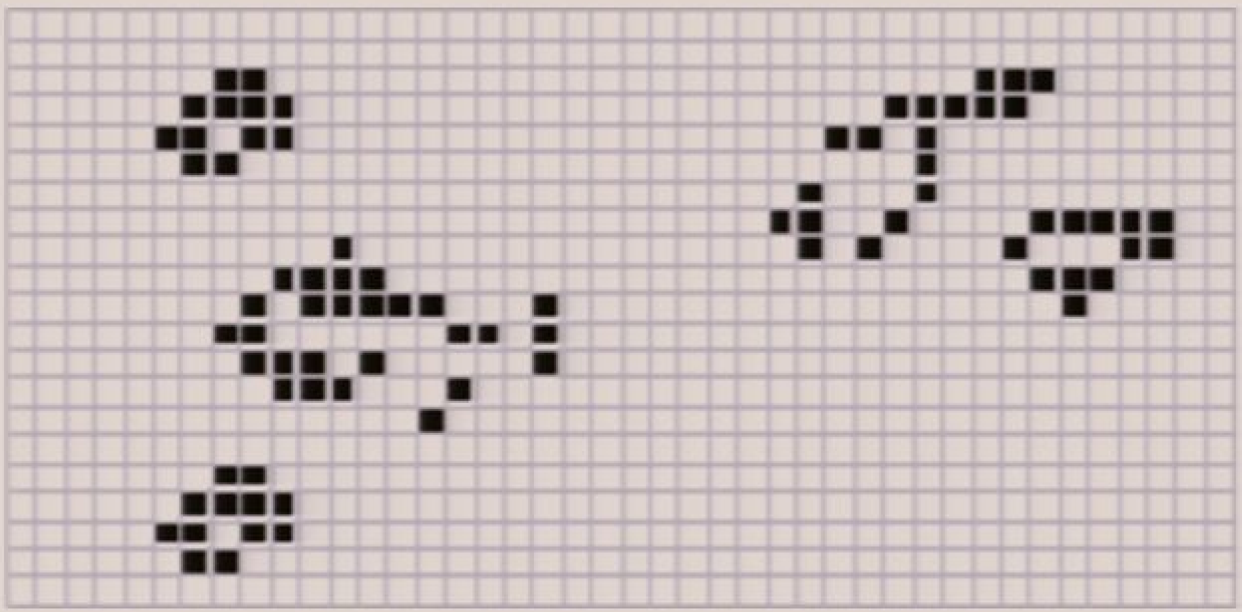
+ details

The Computer Science Picture of Reality



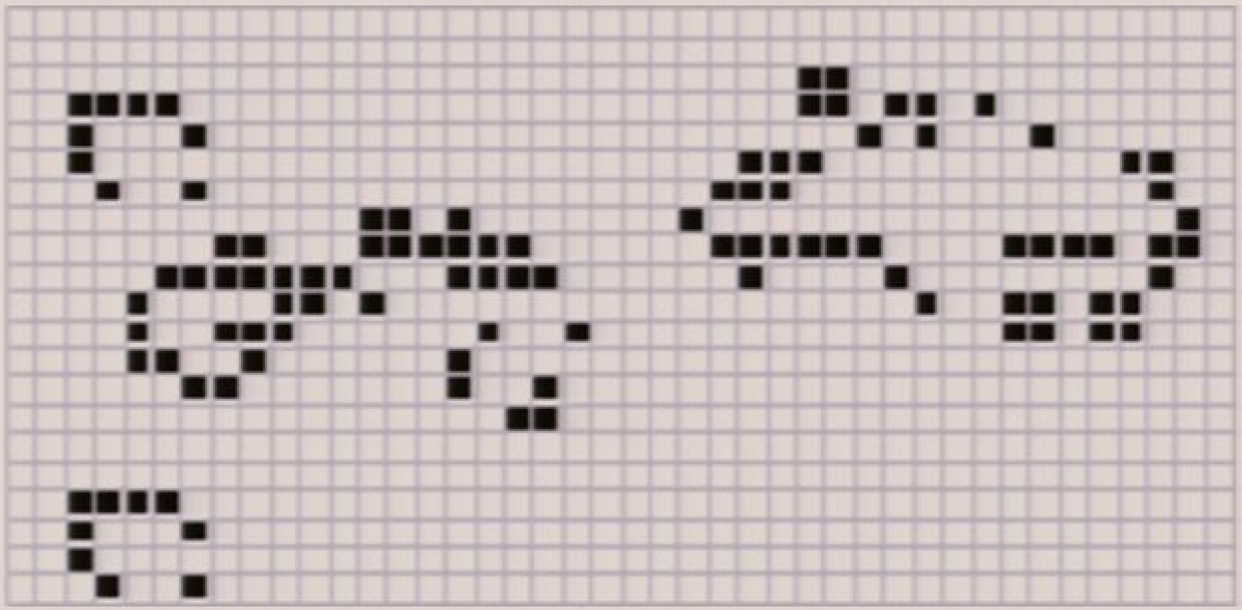
+ details

The Computer Science Picture of Reality



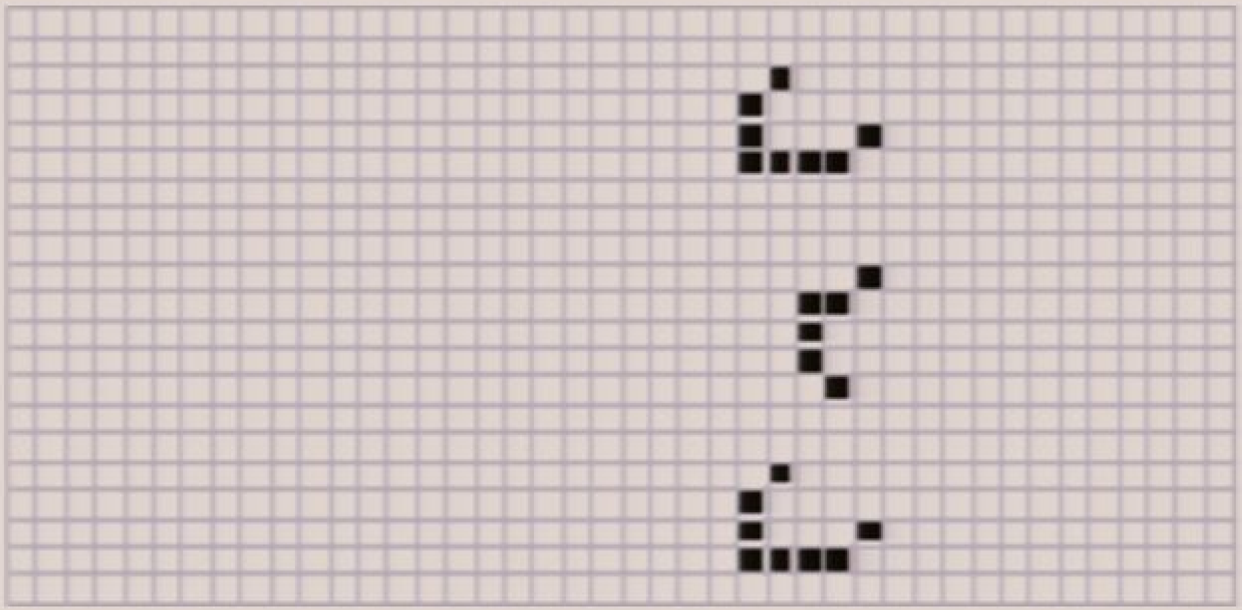
+ details

The Computer Science Picture of Reality



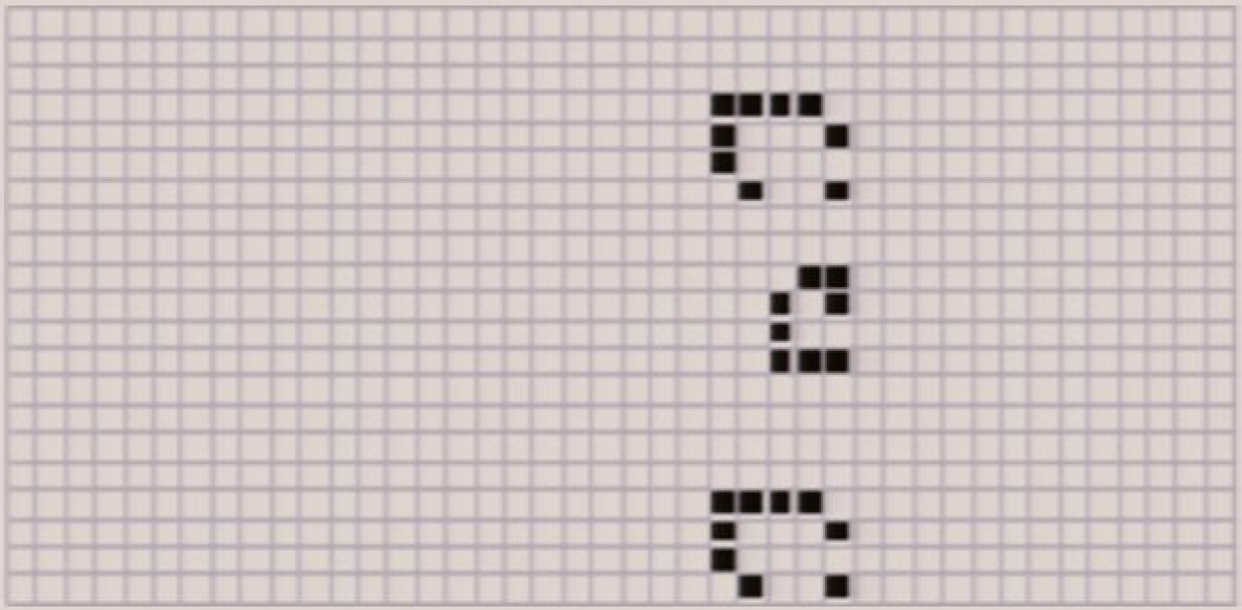
+ details

The Computer Science Picture of Reality



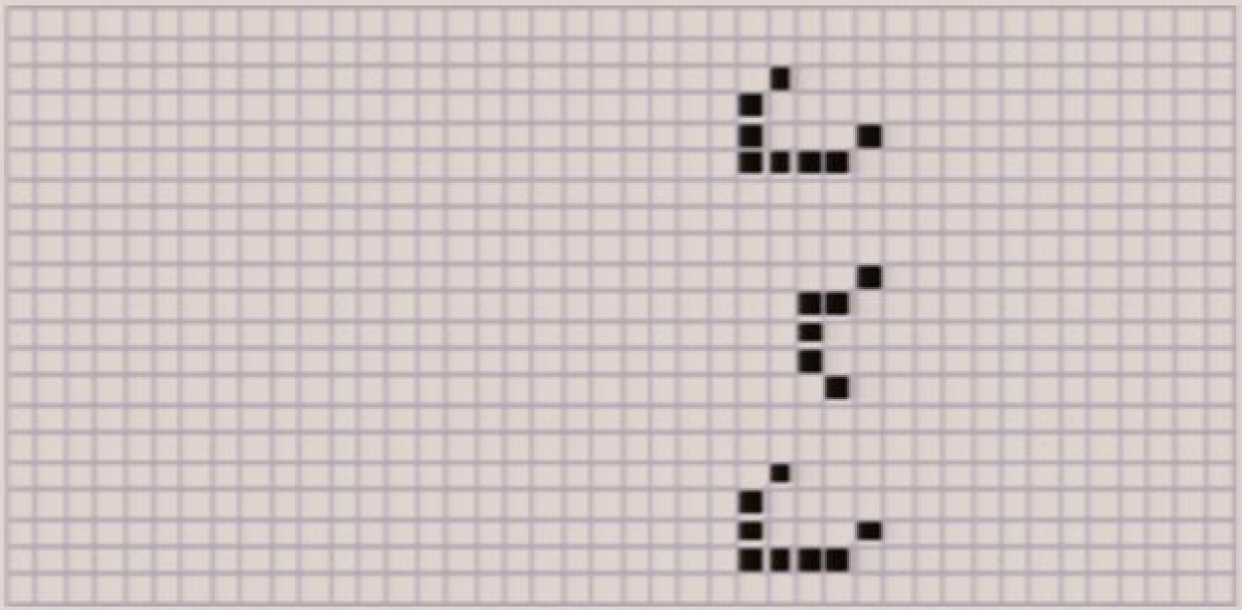
+ details

The Computer Science Picture of Reality



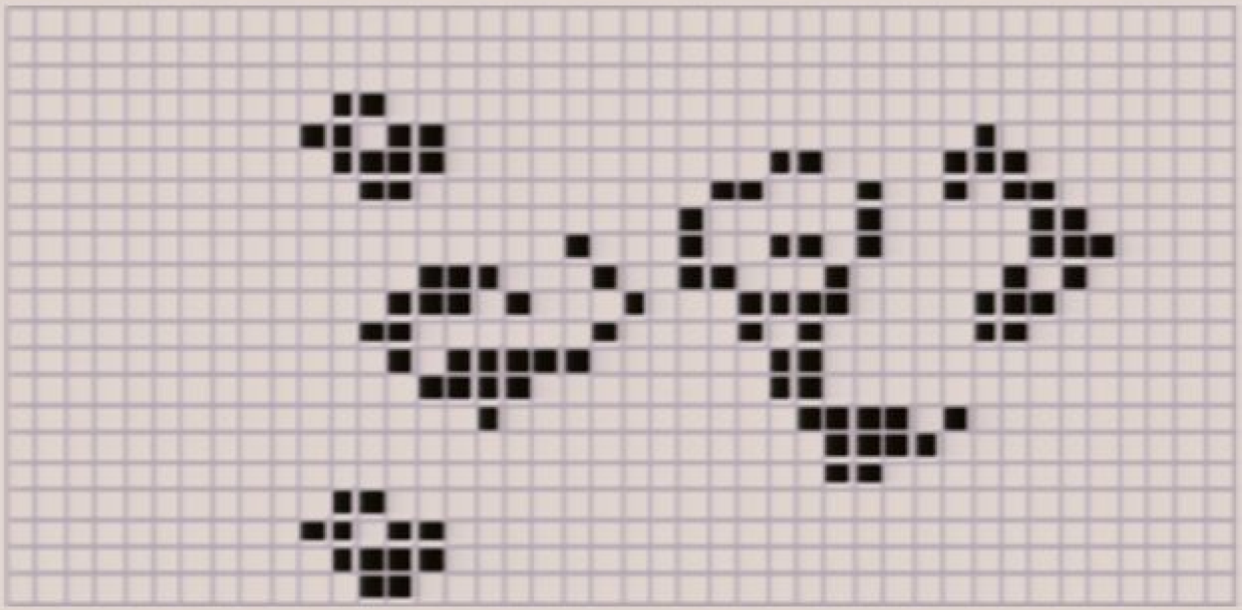
+ details

The Computer Science Picture of Reality



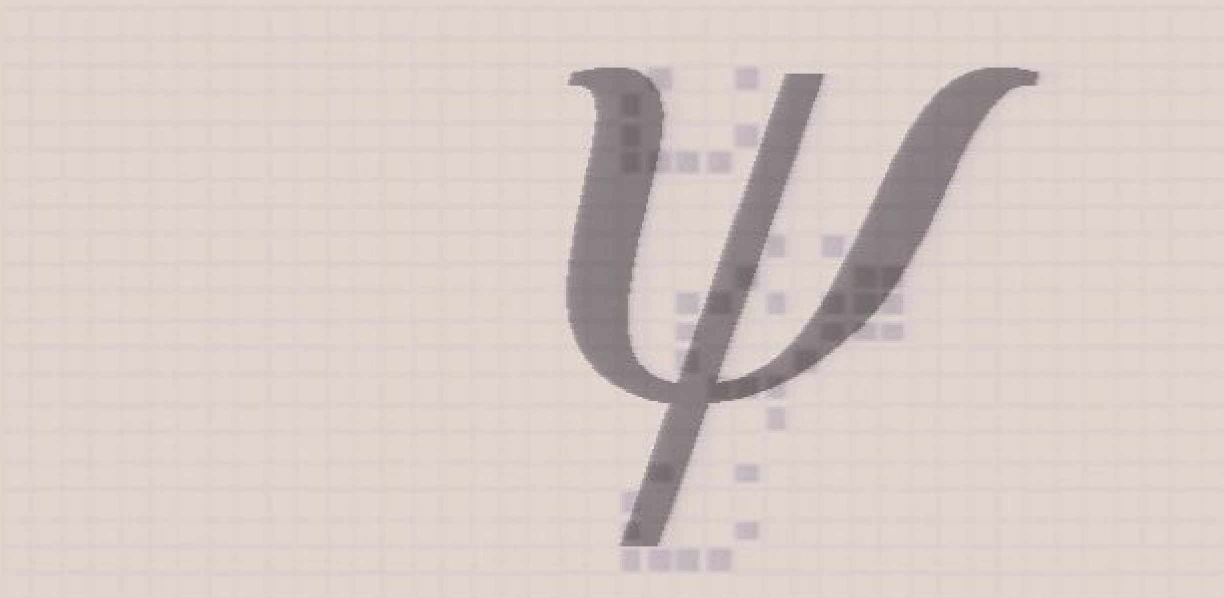
+ details

The Computer Science Picture of Reality



+ details

The Computer Science Picture of Reality



+ details

The Computer Science Picture of Reality

$$\psi$$

Quantum computing challenges this picture

That's why everyone should care about it, whether or not quantum factoring machines are ever built

The Computer Science Picture of Reality

$$\psi$$

Quantum computing challenges this picture

That’s why everyone should care about it, whether or not quantum factoring machines are ever built

PLAN OF TALK

Background

The gospel according to Shor

Part I: Limitations of Quantum Computers

A lower bound extravaganza

Part II: Models and Reality

Is the quantum computing model too powerful? Or not powerful enough?

Background

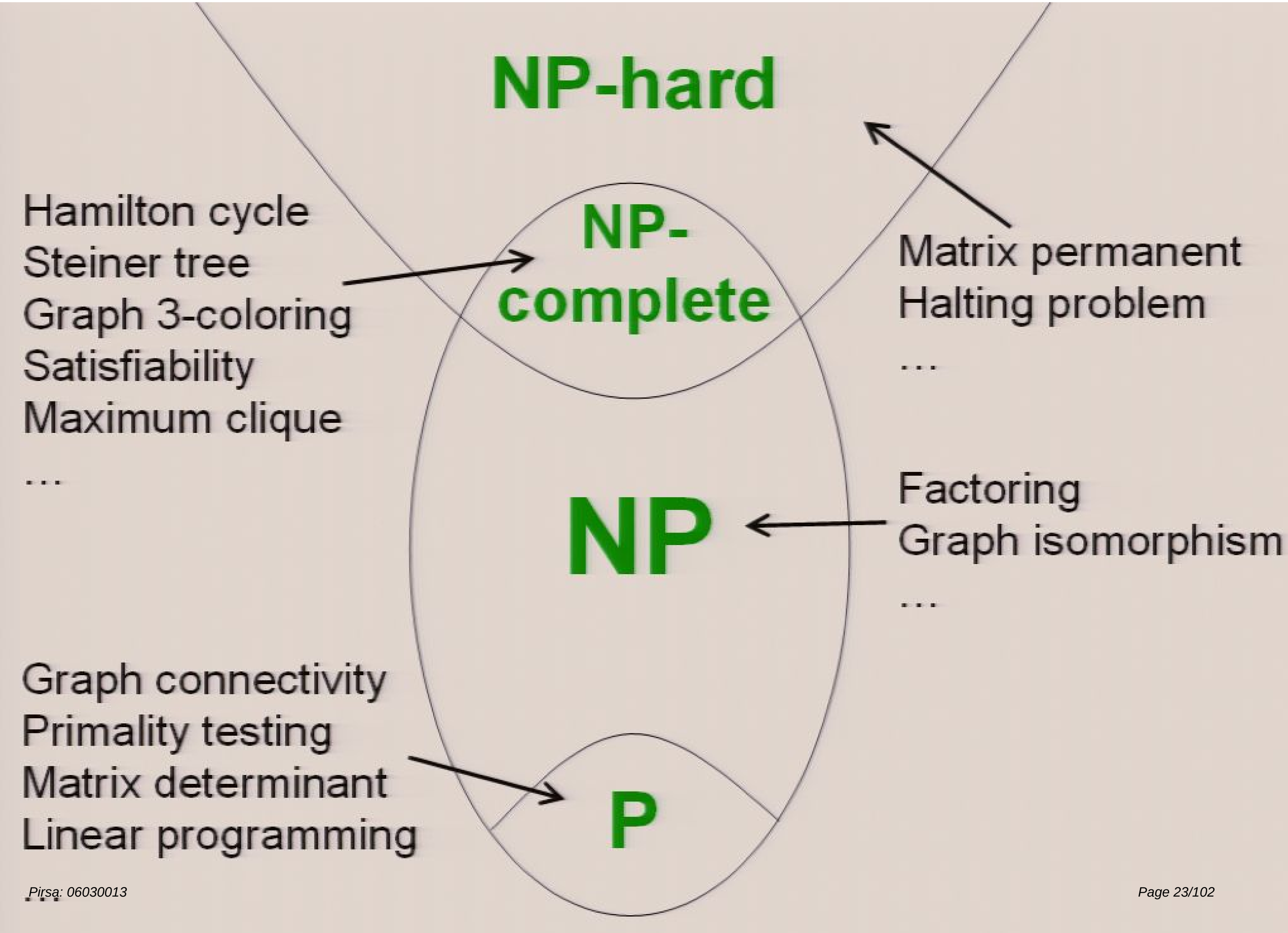
The gospel according to Shor

Part I: Limitations of Quantum Computers

A lower bound extravaganza

Part II: Models and Reality

Is the quantum computing model too powerful? Or not powerful enough?


NP-hard
Hamilton cycle
Steiner tree
Graph 3-coloring
Satisfiability
Maximum clique
…
NP-
complete
Matrix permanent
Halting problem
…
NP
Factoring
Graph isomorphism
…
Graph connectivity
Primality testing
Matrix determinant
Linear programming
P
…

Quantum Computing

A quantum state of n "qubits" takes 2^n complex numbers to describe:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

The goal of quantum computing is to exploit this exponentiality in Nature.

BQP: Bounded-Error Quantum Polynomial-Time

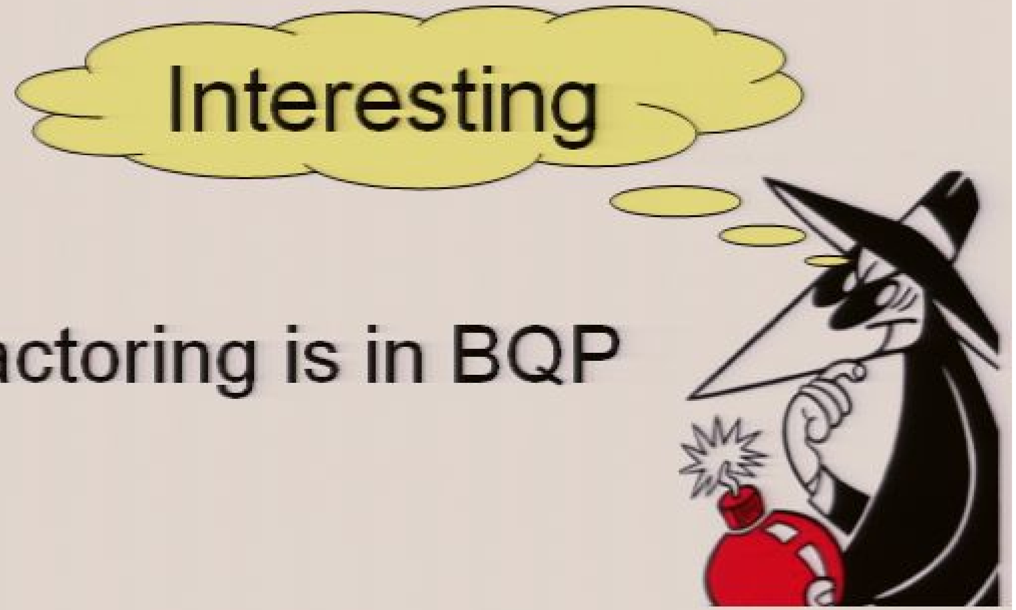
Class of problems solvable efficiently using a quantum computer

Bernstein-Vazirani 1993:

$$P \subseteq BQP \subseteq PSPACE$$

Bernstein-Vazirani 1993:

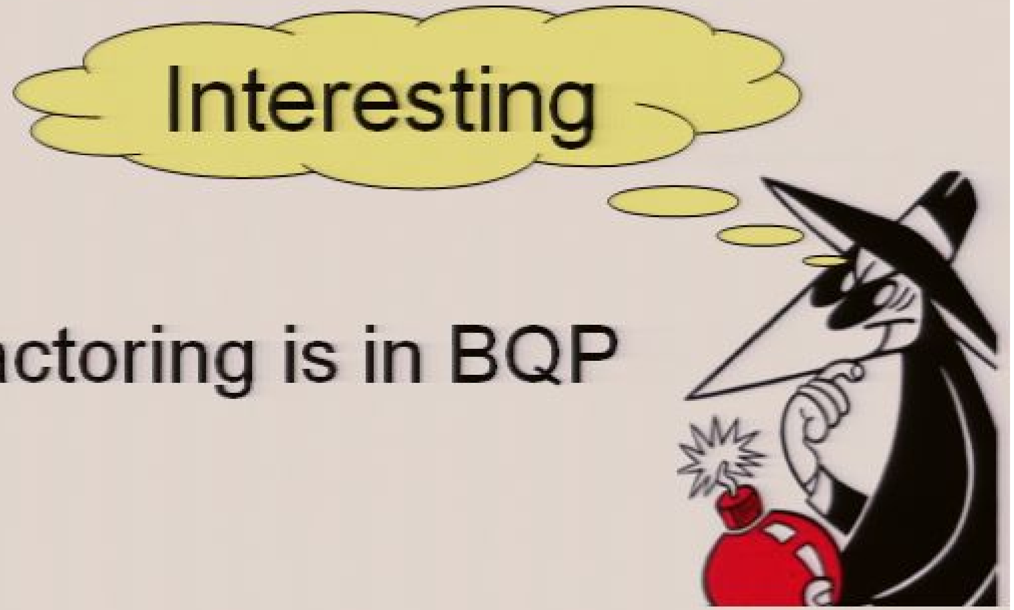
$$P \subseteq BQP \subseteq PSPACE$$



Shor 1994: Factoring is in BQP

Bernstein-Vazirani 1993:

$$P \subseteq BQP \subseteq PSPACE$$



Shor 1994: Factoring is in BQP

Grover 1996: Quantum algorithm to search an N-element array in $\sqrt{N}$ steps

Background

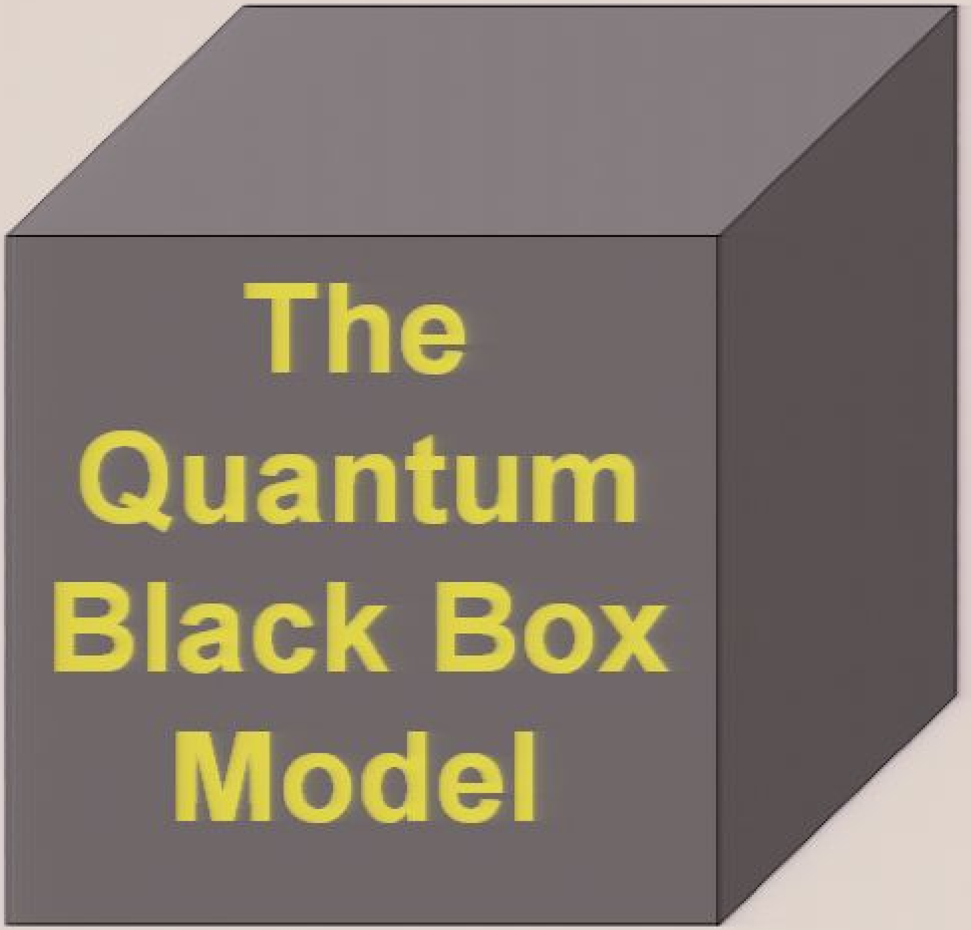
The gospel according to Shor

Part I: Limitations of Quantum Computers

A lower bound extravaganza

Part II: Models and Reality

Is the quantum computing model too powerful? Or not powerful enough?



I do believe it
Against an oracle.
—Shakespeare, *The Tempest*

We count only the number of **queries** to an **oracle**, not the number of computational steps

Example: Given a function $f:\{0,1\}^n \rightarrow \{0,1\}$, decide if there's an x such that $f(x)=1$

We count only the number of **queries** to an **oracle**, not the number of computational steps

Example: Given a function $f:\{0,1\}^n \rightarrow \{0,1\}$, decide if there's an x such that $f(x)=1$

- Like solving an NP-complete problem by brute force
- Classically, $\sim 2^n$ queries to f needed
- Grover's algorithm uses only $\sim 2^{n/2}$
- **BBBV 1997:** Grover is optimal
- Provides evidence that $NP \not\subset BQP$

Algorithm's state:

$$\sum_{x,w} \alpha_{x,w} |x,w\rangle$$

x: location to query
w: "workspace" qubits

After a query transformation:

$$\sum_{x,w} \alpha_{x,w} |x,w \oplus f(x)\rangle$$

Between two queries, we can apply an arbitrary unitary matrix that doesn't depend on f

Complexity = minimum number of queries needed to achieve

$$\sum_{\substack{|x,w\rangle \\ \text{corresponding to} \\ \text{right answer}}} |\alpha_{x,w}|^2 \geq \frac{2}{3}$$

for all oracles f

Problem: Find 2 numbers that are the same (each number appears twice)

28	12	18	76	96	82	94	99	21	78	88	93	39	44	64
32	99	70	18	94	82	92	64	95	46	53	16	35	42	72
31	40	75	71	93	32	47	11	70	37	78	79	36	63	40
69	92	10	28	85	41	80	10	52	63	88	65	43	84	67
57	31	98	39	65	74	24	90	26	83	60	91	27	96	35
20	26	52	95	57	66	97	54	30	62	79	33	84	50	38
49	17	47	24	54	48	98	23	41	16	66	75	38	13	58
56	86	34	73	61	73	21	44	62	34	14	51	74	76	83
37	90	58	13	71	25	29	25	56	68	12	11	51	23	77
68	72	43	69	46	87	97	45	59	14	30	19	81	81	49
60	85	80	50	61	59	89	67	89	29	86	48	22	15	17
55	36	27	42	55	77	19	45	15	53	22	91	87	20	33

Algorithm's state:

$$\sum_{x,w} \alpha_{x,w} \left| x, w \right\rangle$$

x: location to query
w: "workspace" qubits

After a query transformation:

$$\sum_{x,w} \alpha_{x,w} \left| x, w \oplus f(x) \right\rangle$$

Between two queries, we can apply an arbitrary unitary matrix that doesn't depend on f

Complexity = minimum number of queries needed to achieve

$$\sum_{\substack{|x,w\rangle \\ \text{corresponding to} \\ \text{right answer}}} \left| \alpha_{x,w} \right|^2 \geq \frac{2}{3}$$

for all oracles f

Problem: Find 2 numbers that are the same (each number appears twice)

28	12	18	76	96	82	94	99	21	78	88	93	39	44	64
32	99	70	18	94	82	92	64	95	46	53	16	35	42	72
31	40	75	71	93	32	47	11	70	37	78	79	36	63	40
69	92	10	28	85	41	80	10	52	63	88	65	43	84	67
57	31	98	39	65	74	24	90	26	83	60	91	27	96	35
20	26	52	95	57	66	97	54	30	62	79	33	84	50	38
49	17	47	24	54	48	98	23	41	16	66	75	38	13	58
56	86	34	73	61	73	21	44	62	34	14	51	74	76	83
37	90	58	13	71	25	29	25	56	68	12	11	51	23	77
68	72	43	69	46	87	97	45	59	14	30	19	81	81	49
60	85	80	50	61	59	89	67	89	29	86	48	22	15	17
55	36	27	42	55	77	19	45	15	53	22	91	87	20	33

Problem: Find 2 numbers that are the same (each number appears twice)

By **"birthday paradox"**, a randomized algorithm must examine $\sqrt{N}$ of the N numbers

28	12	18	76	96	82	94	99	21	78	88	93	39	44	64
32	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	53	16	35	42	72
31	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	78	79	36	63	40
69	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	88	65	43	84	67
57	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	60	91	27	96	35
20	26	52	95	57	66	97	54	30	62	79	33	84	50	38
49	17	47	24	54	48	98	23	41	16	66	75	38	13	58
56	86	34	73	61	73	21	44	62	34	14	51	74	76	83
37	90	58	13	71	25	29	25	56	68	12	11	51	23	77
68	72	43	69	46	87	97	45	59	14	30	19	81	81	49
60	85	80	50	61	59	89	67	89	29	86	48	22	15	17
55	36	27	42	55	77	19	45	15	53	22	91	87	20	33

Problem: Find 2 numbers that are the same (each number appears twice)

28 12 18 76 96 82 94 99 21 78 88 93 39 44 64
32 … 53 16 35 42 72
31 … 78 79 36 63 40
6 … 88 65 43 84 67
57 … 60 91 27 96 35
20 26 52 95 57 66 97 54 30 62 79 33 84 50 38
4 … 41 16 66 75 38 13 58
5 … 62 34 14 51 74 76 83
3 … 56 68 12 11 51 23 77
6 … 59 14 30 19 81 81 49
6 … 89 29 86 48 22 15 17
55 36 27 42 55 77 19 45 15 53 22 91 87 20 33

By **"birthday paradox"**, a randomized algorithm must examine $\sqrt{N}$ of the N numbers

Brassard, Høyer, Tapp: quantum algorithm (based on Grover) that makes $N^{1/3}$ queries

Problem: Find 2 numbers that are the same (each number appears twice)

28 12 18 76 96 82 94 99 21 78 88 93 39 44 64

By **"birthday paradox"**, a randomized algorithm must examine √N of the N numbers

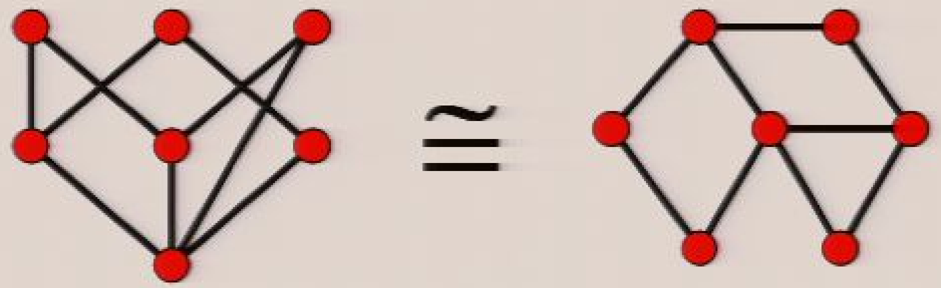
Brassard, Høyer, Tapp: quantum algorithm (based on Grover) that makes $N^{1/3}$ queries

Is that optimal? Proving a lower bound better than constant was open for 5 years

55 36 27 42 55 77 19 45 15 53 22 91 87 20 33

Motivation for the Collision Problem

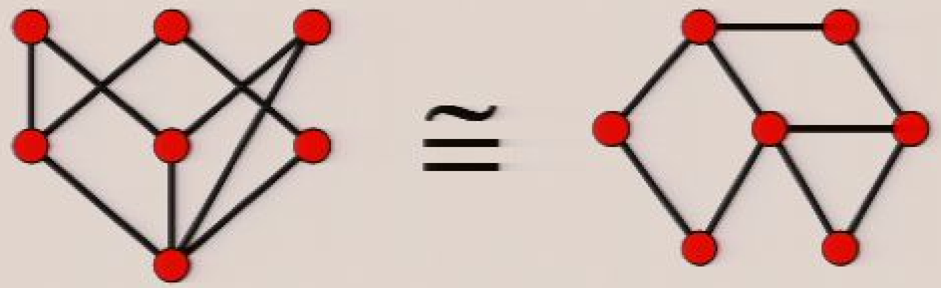
Cryptographic Hash Functions



Graph Isomorphism:
find a collision in
$\sigma_1(G),\ldots,\sigma_{n!}(G),\sigma_1(H),\ldots,\sigma_{n!}(H)$

Motivation for the Collision Problem

Cryptographic Hash Functions



Graph Isomorphism:

find a collision in

$\sigma_1(G),\ldots,\sigma_{n!}(G),\sigma_1(H),\ldots,\sigma_{n!}(H)$

What makes proving a lower bound hard is that a quantum computer can **almost** find a collision in 1 query:

$$\frac{1}{\sqrt{N}}\sum_{x=1}^{N}|x\rangle|f(x)\rangle \xrightarrow{\text{Measure 2}^{\text{nd}}\text{ register}} \frac{|x\rangle+|y\rangle}{\sqrt{2}}|f(x)\rangle$$

A. 2002: $N^{1/5}$ lower bound on quantum query complexity of the collision problem

Improved to $N^{1/3}$ and generalized by Shi, Kutin, Ambainis, and Midrijanis

Proof Sketch (only one in the talk)

T-query quantum algorithm that finds collisions in 2-to-1 functions

→

T-query algorithm that distinguishes 1-to-1 from 2-to-1 functions

Proof Sketch (only one in the talk)

T-query quantum algorithm that finds collisions in 2-to-1 functions

→ T-query algorithm that distinguishes 1-to-1 from 2-to-1 functions

→ **Beals et al. 1998:** Multilinear polynomial p of degree ≤ 2T, such that p(X) = probability algorithm says X is 2-to-1

$p(X) \in [0, 1/3]$ if X is 1-to-1

$p(X) \in [2/3, 1]$ if X is 2-to-1

Key insight: $p(X) \in [0, 1]$ even if X is 3-to-1, 4-to-1, etc.

Proof Sketch (only one in the talk)

T-query quantum algorithm that finds collisions in 2-to-1 functions

→ T-query algorithm that distinguishes 1-to-1 from 2-to-1 functions

↓

Beals et al. 1998: Multilinear polynomial p of degree ≤ 2T, such that p(X) = probability algorithm says X is 2-to-1

$p(X) \in [0, 1/3]$ if X is 1-to-1

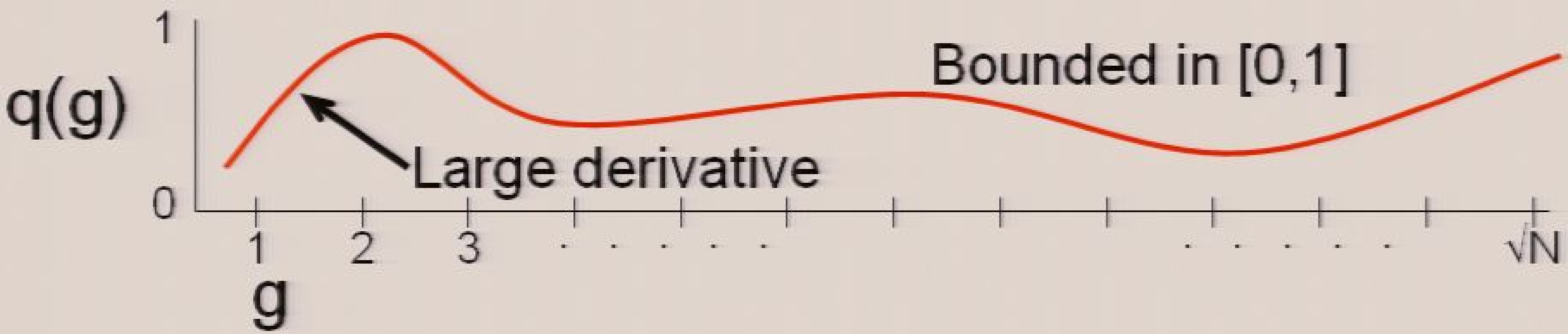
$p(X) \in [2/3, 1]$ if X is 2-to-1

Key insight: $p(X) \in [0,1]$ even if X is 3-to-1, 4-to-1, etc.

↓

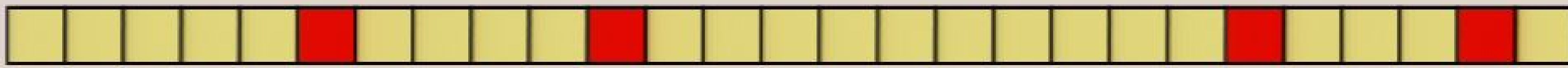
Univariate polynomial q such that deg(q)≤deg(p), and q(g) = average of p(X) over all g-to-1 functions X

Proof Sketch (only one in the talk)



Markov's Inequality implies such a polynomial must have large degree

Direct Product Theorem for Quantum Search



N items, K of them marked

A. 2004: With few ($\ll\sqrt{N}$) queries, the probability of finding all K marked items is $2^{-\Omega(K)}$

Proof uses polynomial method

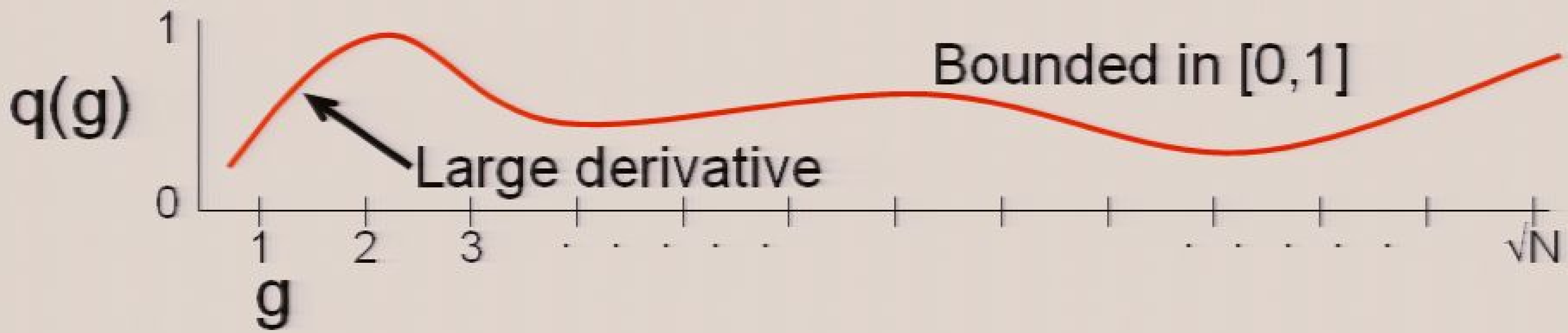
Corollary 1: Exists oracle relative to which

$$NP \not\subset BQP/qpoly$$

(BQP/qpoly = BQP with polynomial-size "quantum advice")

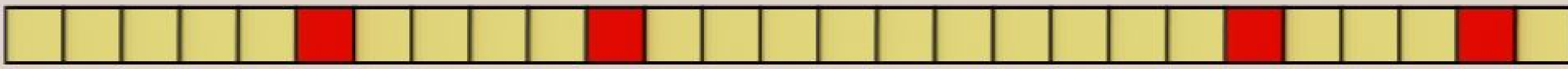
Corollary 2: Fixes flawed result of Klauck on quantum time-space tradeoffs for sorting

Proof Sketch (only one in the talk)



Markov's Inequality implies such a polynomial must have large degree

Direct Product Theorem for Quantum Search



N items, K of them marked

A. 2004: With few ($\ll\sqrt{N}$) queries, the probability of finding all K marked items is $2^{-\Omega(K)}$

Proof uses polynomial method

Corollary 1: Exists oracle relative to which

$$NP \not\subset BQP/qpoly$$

(BQP/qpoly = BQP with polynomial-size “quantum advice”)

Corollary 2: Fixes flawed result of Klauck on quantum time-space tradeoffs for sorting

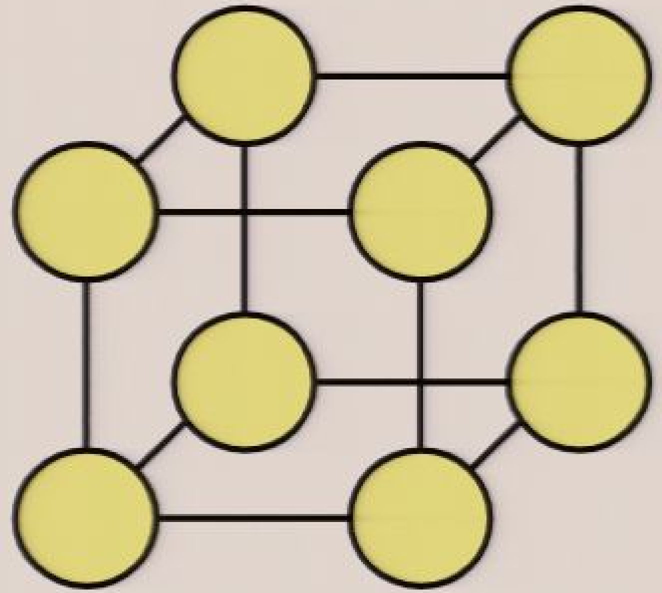
Can quantum ideas help us prove *classical* lower bounds?

Can quantum ideas help us prove *classical* lower bounds?

Quantum Generosity … Giving back because we care™

Examples: Kerenidis & de Wolf 2003, Aharonov & Regev 2004

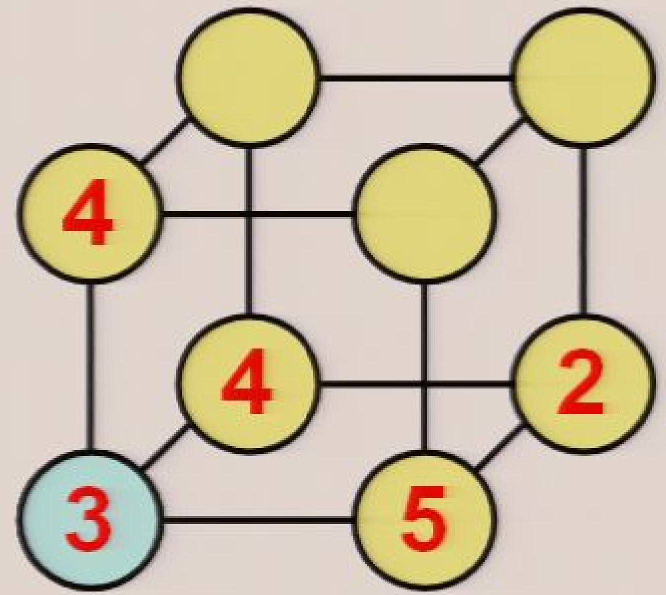
Can quantum ideas help us prove *classical* lower bounds?



Local Search: Given oracle access to $f:\{0,1\}^n \rightarrow \mathbb{Z}$, find a local minimum of f using as few queries as possible

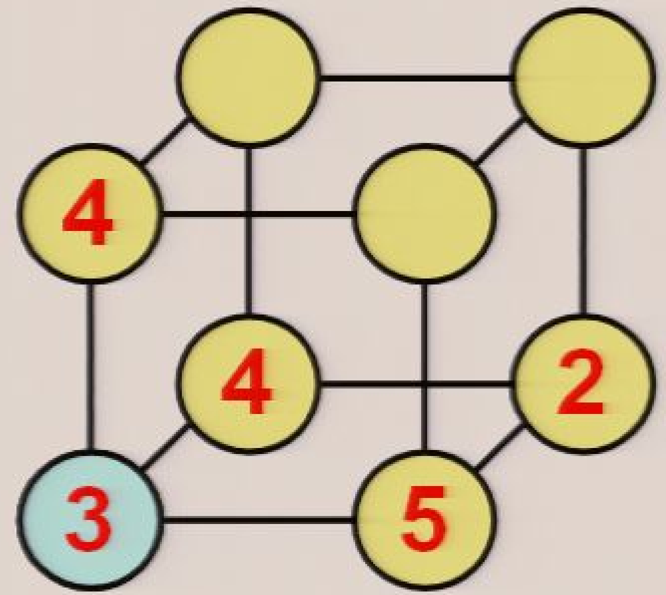
Can quantum ideas help us prove *classical* lower bounds?

Local Search: Given oracle access to $f:\{0,1\}^n \rightarrow \mathbb{Z}$, find a local minimum of f using as few queries as possible



Can quantum ideas help us prove *classical* lower bounds?

Local Search: Given oracle access to $f:\{0,1\}^n \rightarrow \mathbb{Z}$, find a local minimum of f using as few queries as possible



Aldous 1983: Randomized algorithm needs $2^{n/2-o(n)}$ queries

A. 2004: Quantum algorithm needs $2^{n/4}/n$ queries

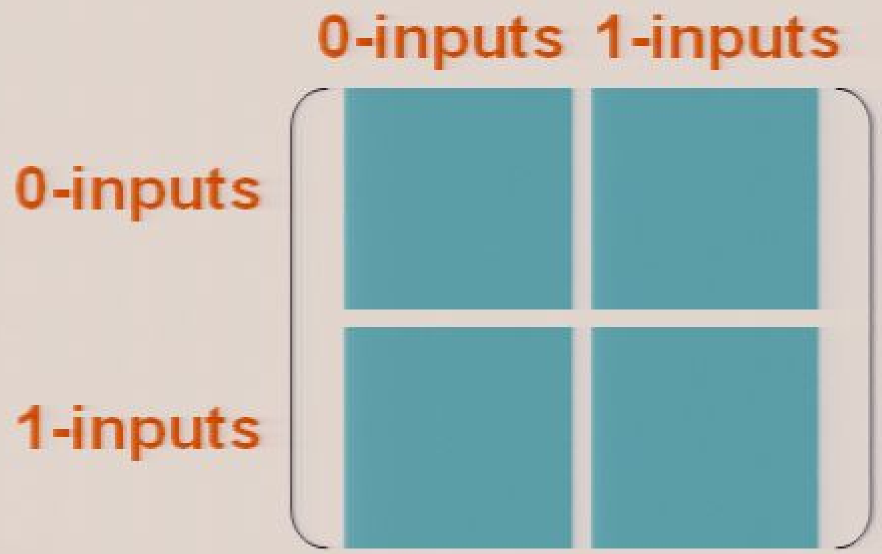
$\Rightarrow$ PLS (Polynomial Local Search) is hard for BQP relative to oracle

Upper bounds:
$2^{n/2}\sqrt{n}$ randomized,
$2^{n/3}n^{1/6}$ quantum

Can quantum ideas help us prove *classical* lower bounds?

Proof technique based on **Ambainis' quantum adversary method**

Each query only separates 0-inputs from 1-inputs by so much



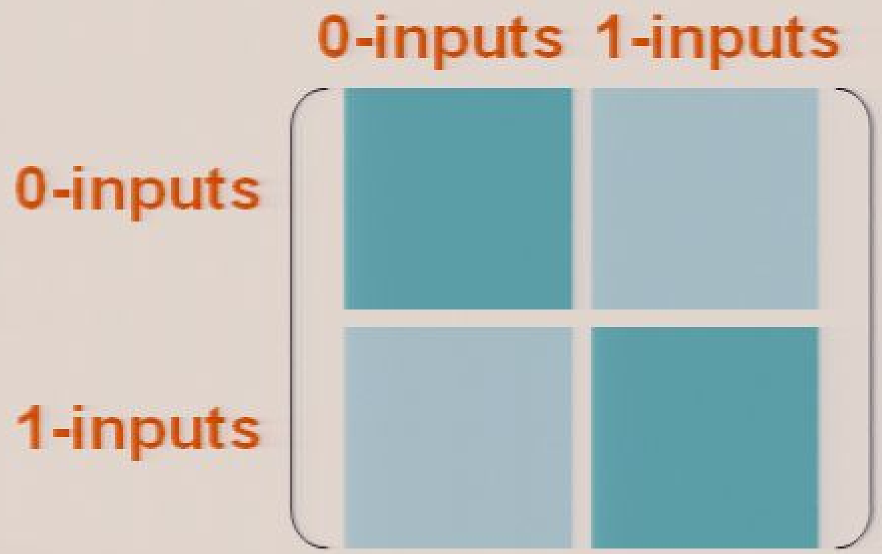
Technique also yields

- $2^{n/2}/n^2$ randomized lower bound
- First lower bounds (randomized or quantum) for constant-dimensional grid graphs

Can quantum ideas help us prove *classical* lower bounds?

Proof technique based on **Ambainis' quantum adversary method**

Each query only separates 0-inputs from 1-inputs by so much



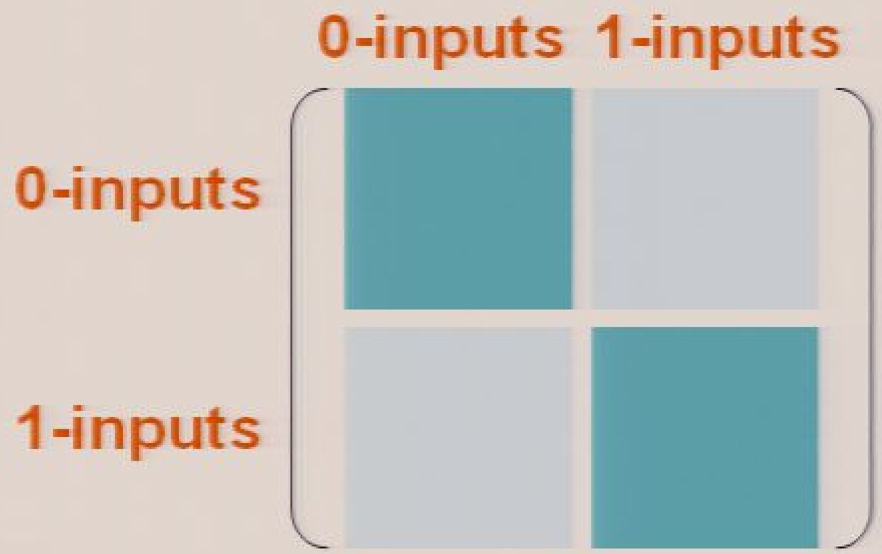
Technique also yields

- $2^{n/2}/n^2$ randomized lower bound
- First lower bounds (randomized or quantum) for constant-dimensional grid graphs

Can quantum ideas help us prove *classical* lower bounds?

Proof technique based on **Ambainis' quantum adversary method**

Each query only separates 0-inputs from 1-inputs by so much



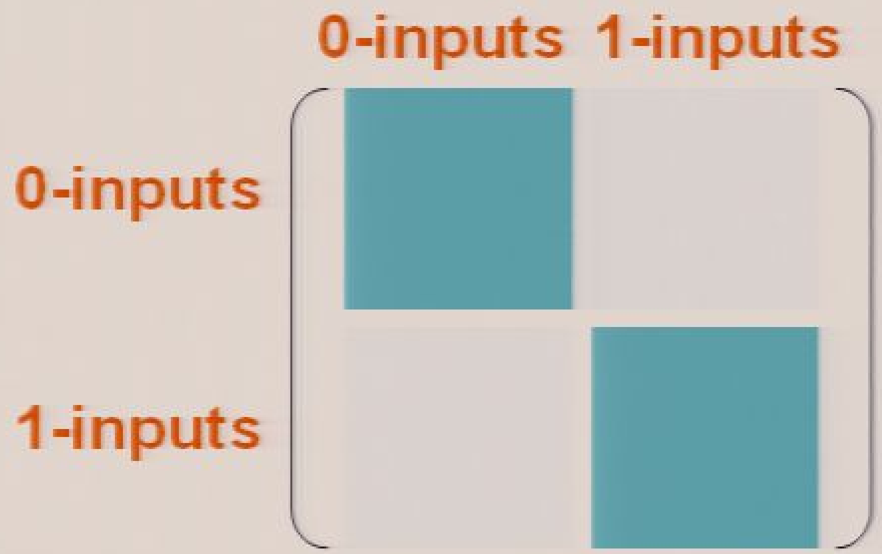
Technique also yields

- $2^{n/2}/n^2$ randomized lower bound
- First lower bounds (randomized or quantum) for constant-dimensional grid graphs

Can quantum ideas help us prove *classical* lower bounds?

Proof technique based on **Ambainis' quantum adversary method**

Each query only separates 0-inputs from 1-inputs by so much

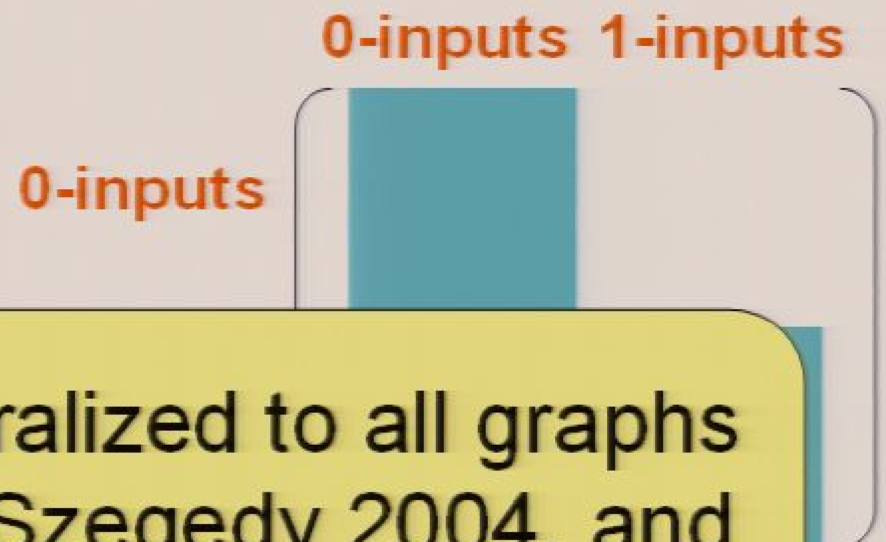


Technique also yields

- $2^{n/2}/n^2$ randomized lower bound
- First lower bounds (randomized or quantum) for constant-dimensional grid graphs

Can quantum ideas help us prove *classical* lower bounds?

Proof technique based on **Ambainis' quantum adversary method**



Each query only separates 0-inputs from 1 inputs by so

Results generalized to all graphs by Santha & Szegedy 2004, and tightened by Zhang 2006

Techn

• $2^{n/2}/$r

• First lower bounds (randomized or quantum) for constant-dimensional grid graphs

Summary

- The Art of the Quantum Lower Bound
  - –Polynomials and adversaries—the dynamic duo
  - –Techniques even applied classically

Summary

- The Art of the Quantum Lower Bound
  - –Polynomials and adversaries—the dynamic duo
  - –Techniques even applied classically
- Quantum computing is not a panacea
  - –Many problems still intractable: NP, collision-finding, local search…
  - –Even with quantum advice

Summary

- The Art of the Quantum Lower Bound
  - –Polynomials and adversaries—the dynamic duo
  - –Techniques even applied classically
- Quantum computing is not a panacea
  - –Many problems still intractable: NP, collision-finding, local search…
  - –Even with quantum advice
- Quantum computing $\neq$ exponential parallelism
  - –Popular articles get this wrong
  - –Because of linearity, one "parallel universe" can't shout above the others

Background

The gospel according to Shor

Part I: Limitations of Quantum Computers

A lower bound extravaganza

Part II: Models and Reality

Is the quantum computing model too powerful? Or not powerful enough?

Is quantum computing just *obvious* baloney?

Leonid Levin:
"We have never seen a physical law valid to over a dozen decimals"

Oded Goldreich:
Exponentially long vectors $\Rightarrow$ exponential time to manipulate

Sure/Shor separators

My response: What criterion separates the quantum states that suffice for factoring from the states we've already seen?

DIVIDING LINE

Sure/Shor separators

My response: What criterion separates the quantum states that suffice for factoring from the states we've already seen?

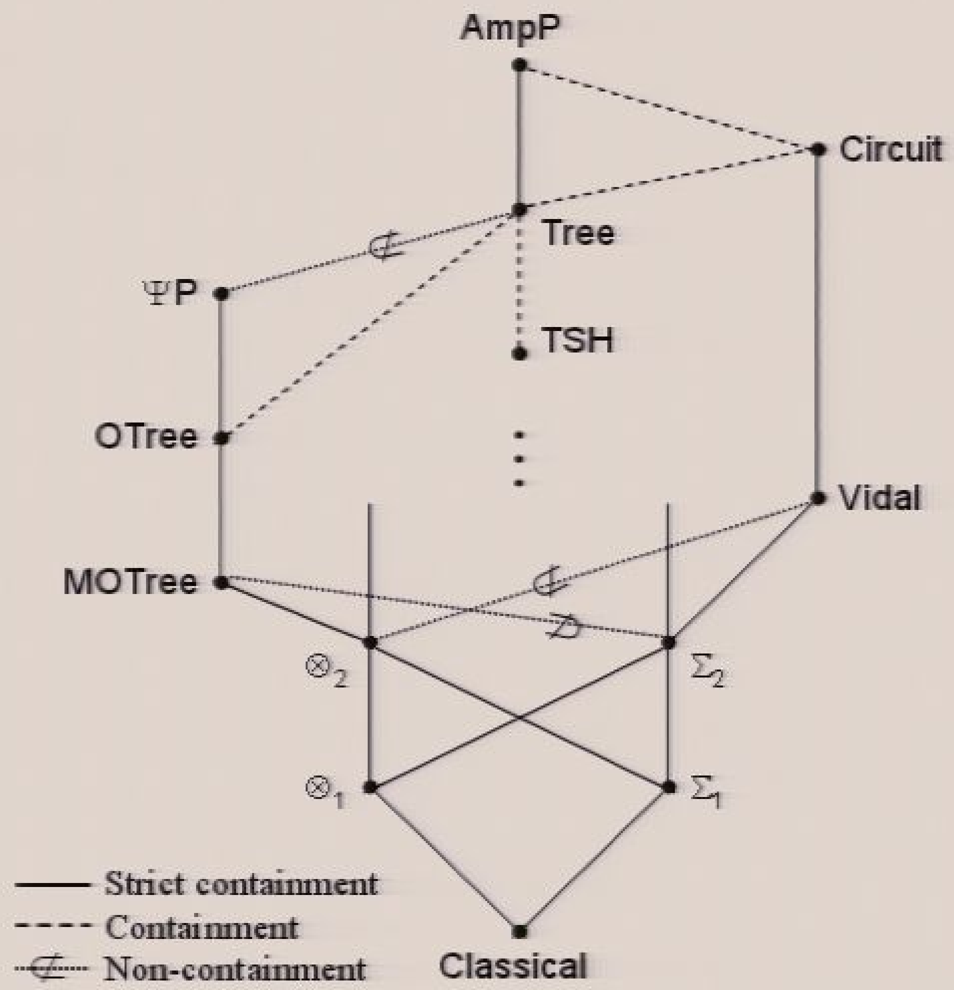
Not exponentially small amplitudes or thousands of coherent qubits

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes 10000} \qquad \frac{|0\rangle^{\otimes 10000}+|1\rangle^{\otimes 10000}}{\sqrt{2}}$$

A. 2004 proposes a complexity classification of quantum states to help answer this question

Main result: States arising in quantum error-correction take $n^{\Omega(\log n)}$ additions and tensor products to express

Proof applies Ran Raz's breakthrough lower bound on multilinear formula size



Are quantum states *really* "exponential-sized objects"?

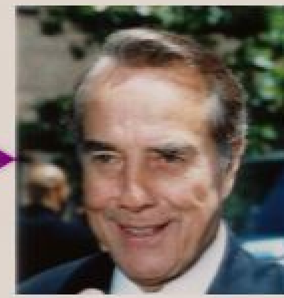
Are quantum states *really* "exponential-sized objects"?

x

Alice

$|\psi_x\rangle$

1-way communication



y

Bob

f(x,y)

Are quantum states *really* "exponential-sized objects"?

A., CCC'04: Given $f:\{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}$ (partial or total),

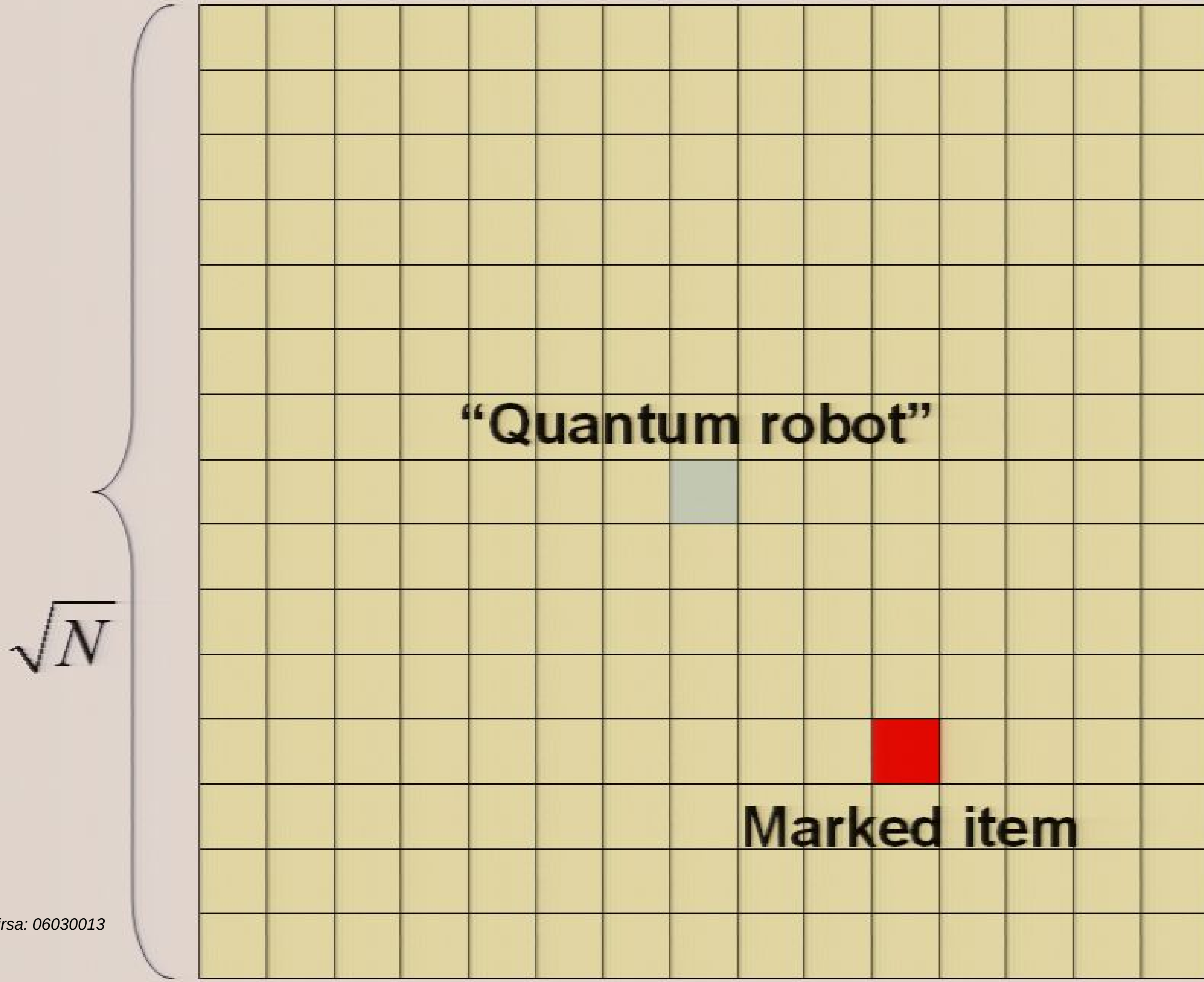
$$D^1(f) = O(m\, Q^1(f) \log Q^1(f))$$

$D^1(f)$ = deterministic 1-way communication complexity

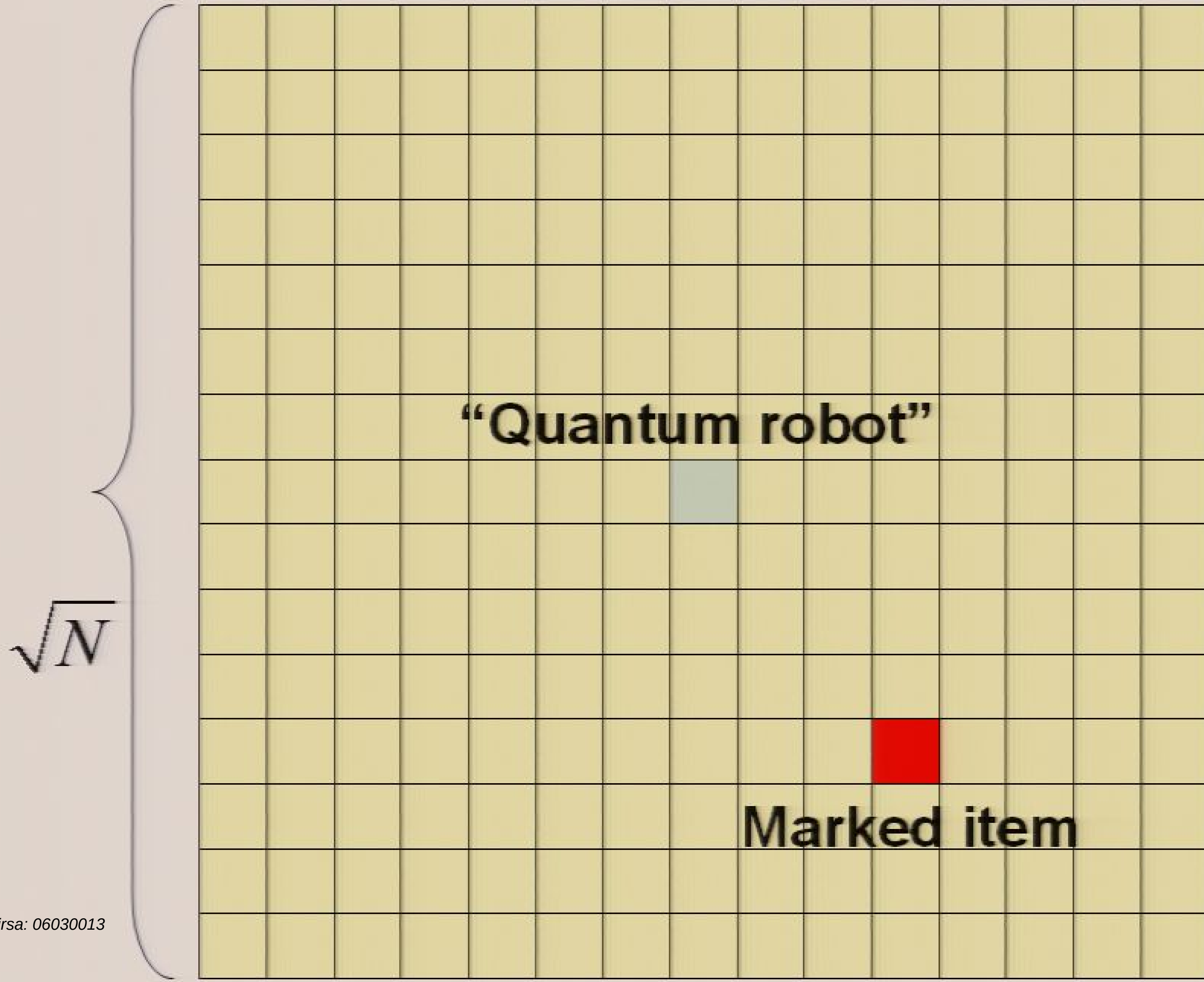
$Q^1(f)$ = bounded-error quantum 1-way complexity

Corollary: **BQP/qpoly $\subseteq$ PostBQP/poly**

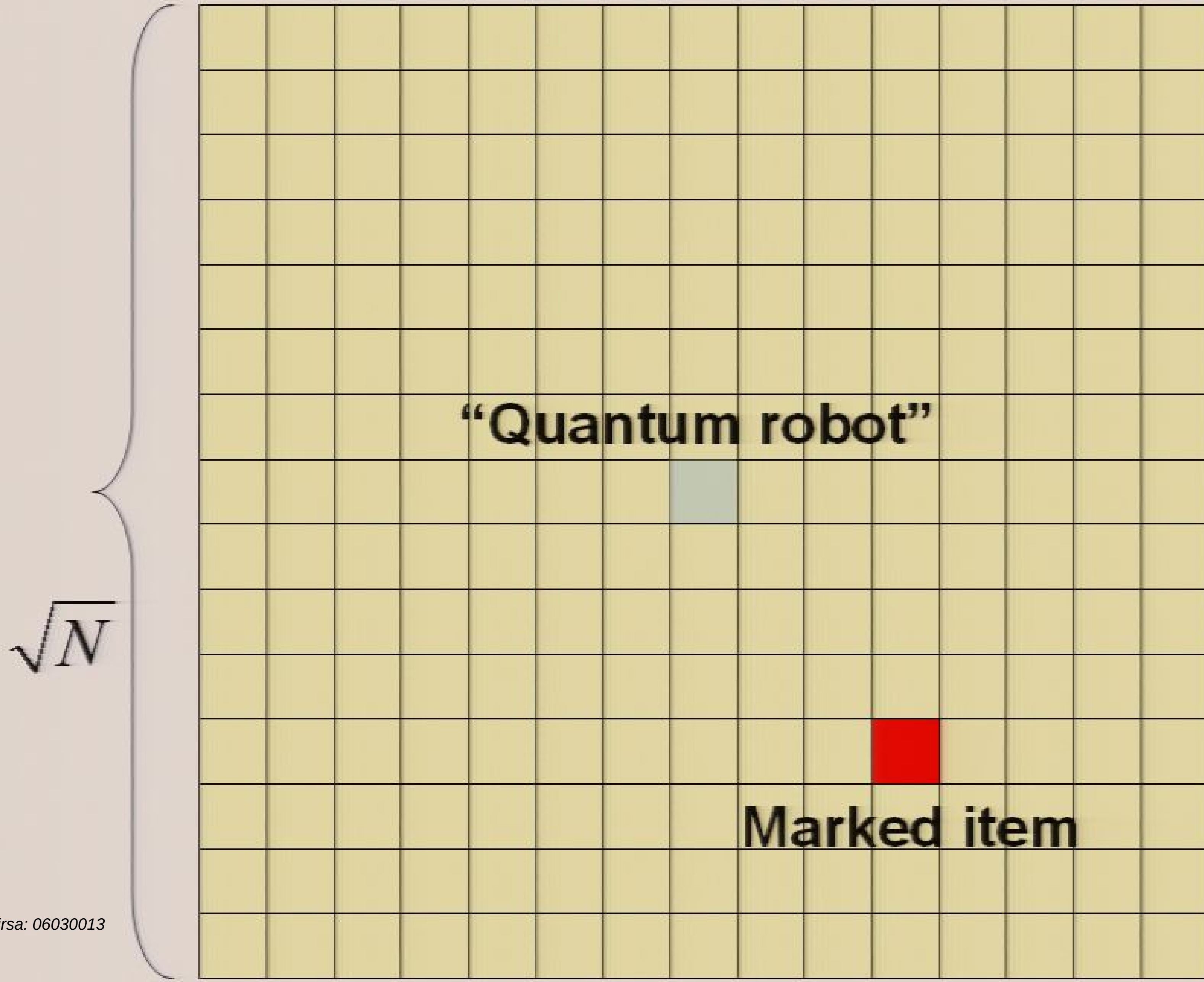
Grover Search of a Physical Region



Grover Search of a Physical Region



Grover Search of a Physical Region



Grover Search of a Physical Region

Benioff 2001: Each of the $\sqrt{N}$ Grover iterations takes $\sqrt{N}$ time, just to move the robot across the grid. So no improvement over classical

Grover Search of a Physical Region

Benioff 2001: Each of the $\sqrt{N}$ Grover iterations takes $\sqrt{N}$ time, just to move the robot across the grid. So no improvement over classical

A. and Ambainis 2003: Sadly, no lower bound… Using divide-and-conquer, can search d-dimensional cube in $\sqrt{N} \log^{3/2} N$ time for d=2, or $\sqrt{N}$ for $d \geq 3$

Corollary: $O(\sqrt{N})$-qubit disjointness protocol

Grover Search of a Physical Region

Benioff 2001: Each of the $\sqrt{N}$ Grover iterations takes $\sqrt{N}$ time, just to move the robot across the grid. So no improvement over classical

A. and Ambainis 2003: Sadly, no lower bound… Using divide-and-conquer, can search d-dimensional cube in $\sqrt{N} \log^{3/2} N$ time for d=2, or $\sqrt{N}$ for $d \geq 3$

Corollary: $O(\sqrt{N})$-qubit disjointness protocol

My motivation: What computational limitations are imposed by the speed of light being finite?

Foolproof Way to Solve NP Complete Problems Efficiently

Foolproof Way to Solve NP Complete Problems Efficiently

Guess a random solution by measuring electron spins. If solution is wrong, kill yourself

Foolproof Way to Solve NP Complete Problems Efficiently

Guess a random solution by measuring electron spins. If solution is wrong, kill yourself

$|0000\rangle$ $|0001\rangle$ $|0010\rangle$ $|0011\rangle$ $|0100\rangle$ $|0101\rangle$ $|0110\rangle$ $|0111\rangle$
$|1000\rangle$ $|1001\rangle$ $\mathbf{|1010\rangle}$ $|1011\rangle$ $|1100\rangle$ $|1101\rangle$ $|1110\rangle$ $|1111\rangle$

Foolproof Way to Solve NP Complete Problems Efficiently

Guess a random solution by measuring electron spins. If solution is wrong, kill yourself

$|0000\rangle$ $|0001\rangle$ $|0010\rangle$ $|0011\rangle$ $|0100\rangle$ $|0101\rangle$ $|0110\rangle$ $|0111\rangle$

$|1000\rangle$ $|1001\rangle$ $|1010\rangle$ $|1011\rangle$ $|1100\rangle$ $|1101\rangle$ $|1110\rangle$ $|1111\rangle$

Foolproof Way to Solve NP Complete Problems Efficiently

Guess a random solution by measuring electron spins. If solution is wrong, kill yourself

Let PostBQP (Postselected Bounded-Error Quantum Polynomial-Time) be class of problems solvable this way

A. 2004: PostBQP = PP

Corollary: Numerous "small" changes to quantum mechanics would let us solve PP-complete problems—nonunitary matrices, $|\alpha|^p$ for $p\neq 2$, …

Foolproof Way to Solve NP Complete Problems Efficiently

Guess a random solution by measuring electron spins. If solution is wrong, kill yourself

Let PostBQP (Postselected Bounded-Error Quantum Polynomial-Time) be class of problems solvable this way

A. 2004: PostBQP = PP

Corollary: Numerous "small" changes to quantum mechanics would let us solve PP-complete problems—nonunitary matrices, $|\alpha|^p$ for $p \neq 2$, …

Foolproof Way to Solve NP Complete Problems Efficiently

Guess a random so tion by m asuring el ctron spins. If solution is g, ki rse

Let PostBQP -Time) be cla

A. 2004:

Coro ntum mechanics te problems— p for 2, …

Immediately implies **Beigel-Reingold-Spielman Theorem** from classical CS:

PP is closed under intersection


Quantum mechanics
What we experience

Stochastic Hidden-Variable Theories

Time ↓

$$\alpha_1^{(1)}|1\rangle + \alpha_2^{(1)}|2\rangle + \alpha_3^{(1)}|3\rangle + \alpha_4^{(1)}|4\rangle + \alpha_5^{(1)}|5\rangle$$

$$\alpha_1^{(2)}|1\rangle + \alpha_2^{(2)}|2\rangle + \alpha_3^{(2)}|3\rangle + \alpha_4^{(2)}|4\rangle + \alpha_5^{(2)}|5\rangle$$

$$\alpha_1^{(3)}|1\rangle + \alpha_2^{(3)}|2\rangle + \alpha_3^{(3)}|3\rangle + \alpha_4^{(3)}|4\rangle + \alpha_5^{(3)}|5\rangle$$

$$\alpha_1^{(4)}|1\rangle + \alpha_2^{(4)}|2\rangle + \alpha_3^{(4)}|3\rangle + \alpha_4^{(4)}|4\rangle + \alpha_5^{(4)}|5\rangle$$

$$\alpha_1^{(5)}|1\rangle + \alpha_2^{(5)}|2\rangle + \alpha_3^{(5)}|3\rangle + \alpha_4^{(5)}|4\rangle + \alpha_5^{(5)}|5\rangle$$

Quantum state of the universe

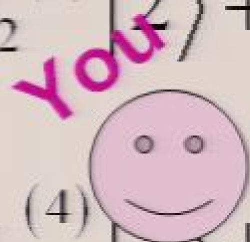
Stochastic Hidden-Variable Theories

Time

$$\alpha_1^{(1)}|1\rangle+\alpha_2^{(1)}|2\rangle+\alpha_3^{(1)}|3\rangle+\alpha_4^{(1)}|4\rangle+\alpha_5^{(1)}|5\rangle$$

$$\alpha_1^{(2)}|1\rangle+\alpha_2^{(2)}|2\rangle+\alpha_3^{(2)}|3\rangle+\alpha_4^{(2)}|4\rangle+\alpha_5^{(2)}|5\rangle$$

$$\alpha_1^{(3)}|1\rangle+\alpha_2^{(3)}|2\rangle+\alpha_3^{(3)}|3\rangle+\alpha_4^{(3)}|4\rangle+\alpha_5^{(3)}|5\rangle$$



$$\alpha_1^{(4)}|1\rangle+\alpha_2^{(4)}|2\rangle+\alpha_3^{(4)}|3\rangle+\alpha_4^{(4)}|4\rangle+\alpha_5^{(4)}|5\rangle$$

$$\alpha_1^{(5)}|1\rangle+\alpha_2^{(5)}|2\rangle+\alpha_3^{(5)}|3\rangle+\alpha_4^{(5)}|4\rangle+\alpha_5^{(5)}|5\rangle$$

Quantum state of the universe

Suppose your whole life history flashed before you in an instant

Let DQP (Dynamical Quantum Polynomial-Time) be the class of problems you could then solve efficiently (assuming transition probabilities satisfy two reasonable axioms—symmetry and locality)

A. 2002: DQP contains Graph Isomorphism (indeed all of Statistical Zero Knowledge)

$$\frac{1}{\sqrt{2}}\left(|\sigma\rangle+|\tau\rangle\right)|\sigma(G)\rangle$$

$$\frac{1}{\sqrt{2}}\left(|\sigma\rangle+|\tau\rangle\right)|\sigma(G)\rangle$$

Together with collision lower bound, strong evidence that BQP $\subset$ DQP

Quantum vs. Classical Proofs

QMA: Quantum version of NP

QCMA: Same as QMA, but with quantum verification of *classical* proofs

Quantum vs. Classical Proofs

QMA: Quantum version of NP

QCMA: Same as QMA, but with quantum verification of *classical* proofs

Does QMA = QCMA?

A. and Kuperberg 2006: "Quantum oracle separation" between QMA and QCMA

A. 2006: QMA/qpoly $\subseteq$ PSPACE/poly

Contrasts with result of Raz that QIP/qpoly=ALL

Quantum vs. Classical Proofs

QMA: Quantum version of NP

QCMA: Same as QMA, but with quantum verification of *classical* proofs

Quantum vs. Classical Proofs

QMA: Quantum version of NP

QCMA: Same as QMA, but with quantum verification of *classical* proofs

Does QMA = QCMA?

Quantum vs. Classical Proofs

QMA: Quantum version of NP

QCMA: Same as QMA, but with quantum verification of *classical* proofs

Does QMA = QCMA?

A. and Kuperberg 2006: "Quantum oracle separation" between QMA and QCMA

Quantum vs. Classical Proofs

QMA: Quantum version of NP

QCMA: Same as QMA, but with quantum verification of *classical* proofs

Does QMA = QCMA?

A. and Kuperberg 2006: "Quantum oracle separation" between QMA and QCMA

A. 2006: QMA/qpoly $\subseteq$ PSPACE/poly

Contrasts with result of Raz that QIP/qpoly=ALL

Current Work

- Quantum copy-protection and quantum software obfuscation
- Learning of quantum states / quantum Occam's Razor theorem
  AvgBQP/qpoly $\subseteq$ AvgQMA/poly
- BQP with closed timelike curves = PSPACE (with John Watrous)

Concluding Remarks

Concluding Remarks

- The Ogre of Intractability:
  - Not even quantum computers escape

Concluding Remarks

- The Ogre of Intractability:
  - Not even quantum computers escape
- Lower bound techniques “unreasonably effective”

Concluding Remarks

- The Ogre of Intractability:
  - Not even quantum computers escape
- Lower bound techniques “unreasonably effective”
- Challenge for quantum computing skeptics
  - Give us a better picture of the world

Concluding Remarks

- The Ogre of Intractability:
  - Not even quantum computers escape
- Lower bound techniques "unreasonably effective"

Concluding Remarks

- The Ogre of Intractability:
  - Not even quantum computers escape
- Lower bound techniques “unreasonably effective”
- Challenge for quantum computing skeptics
  - Give us a better picture of the world

Concluding Remarks

- The Ogre of Intractability:
  - Not even quantum computers escape
- Lower bound techniques “unreasonably effective”
- Challenge for quantum computing skeptics
  - Give us a better picture of the world
- Computer science and fundamental physics: a match made in Hilbert space
  - New perspective forces us to take QM seriously
  - Insights into hidden variables, postselection, holographic entropy bound, …
  - Computational input to quantum gravity?
  - Intractability as a physical axiom?

www.scottaaronson.com