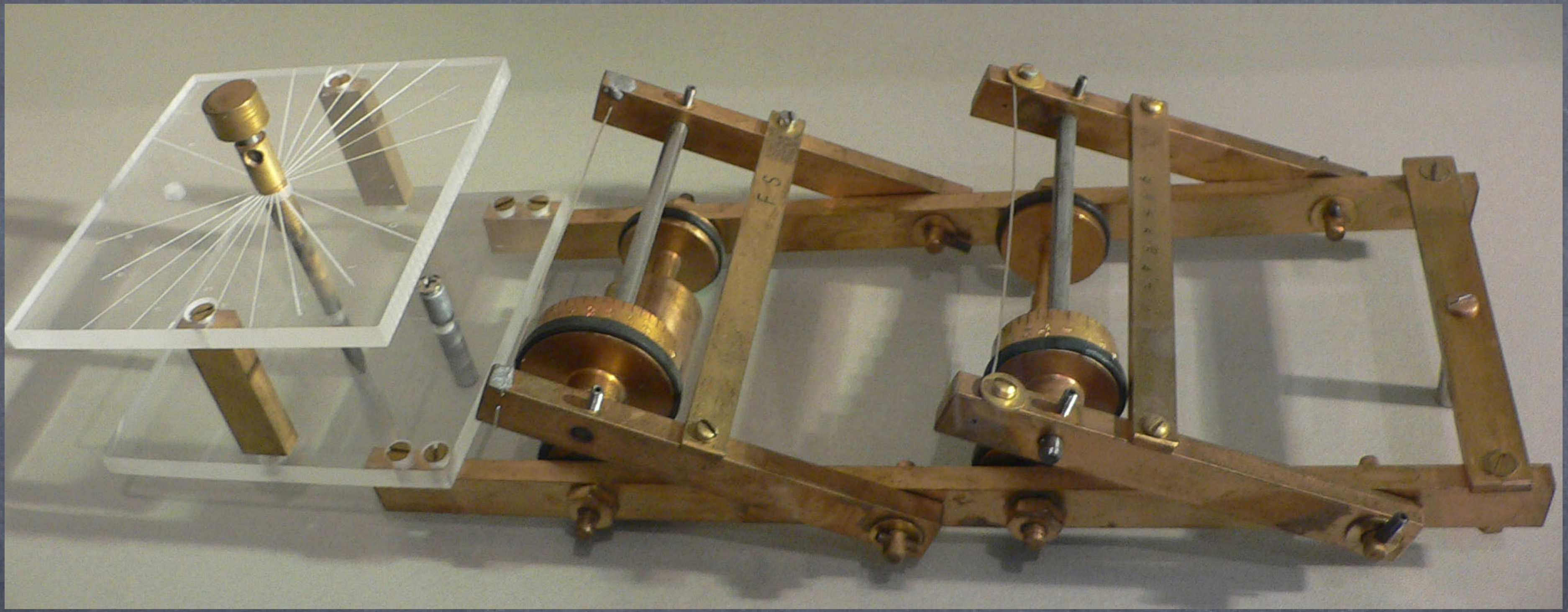
The power of quantum sampling



Aram Harrow
Bristol/UW
Feb 3, 2011

computer science $\longleftrightarrow$ physics computer science

physics

building computers:

-mechanical

-electronic

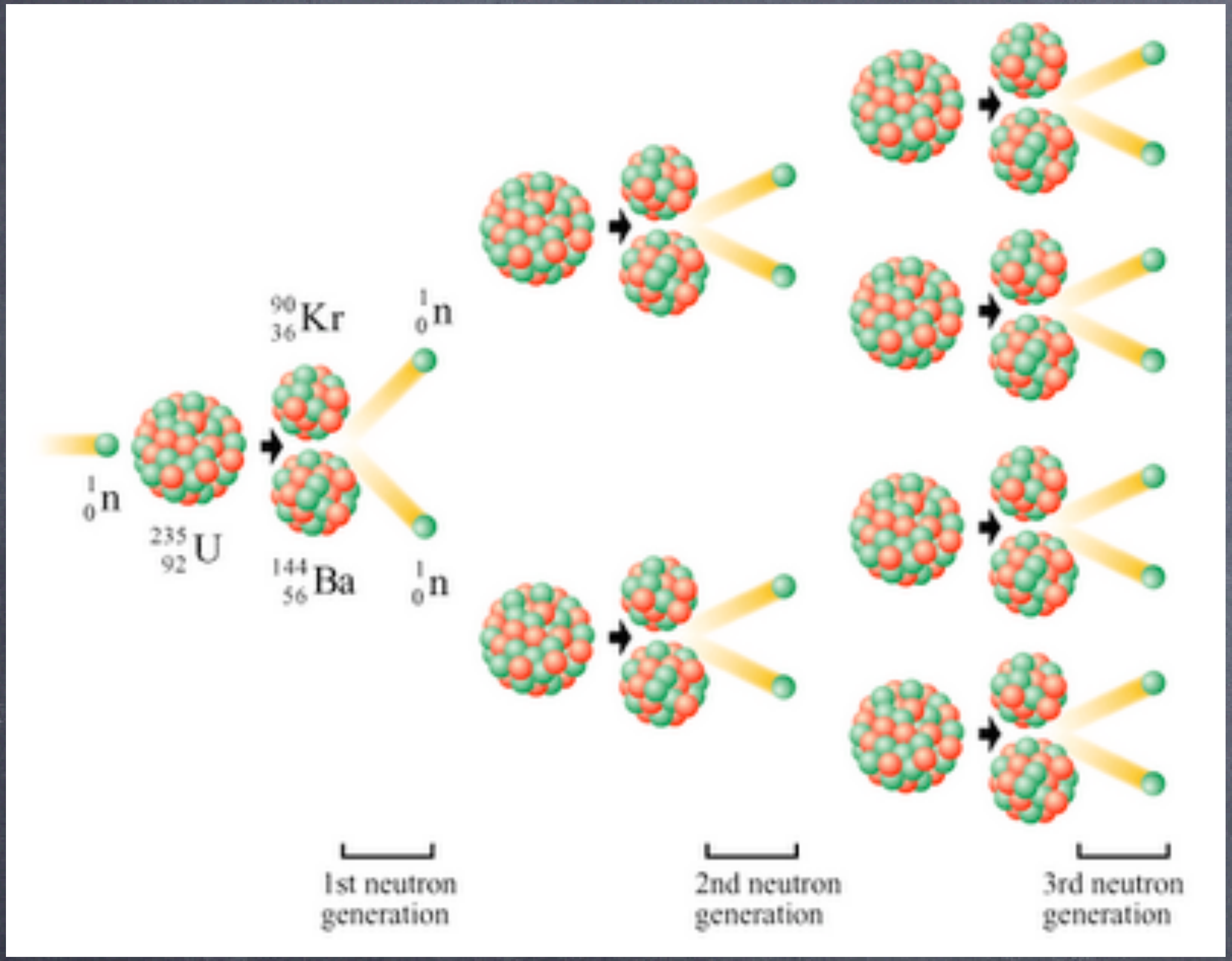
-quantum

computer science ⟷ physics

⟵ building computers:
- -mechanical
- -electronic
- -quantum

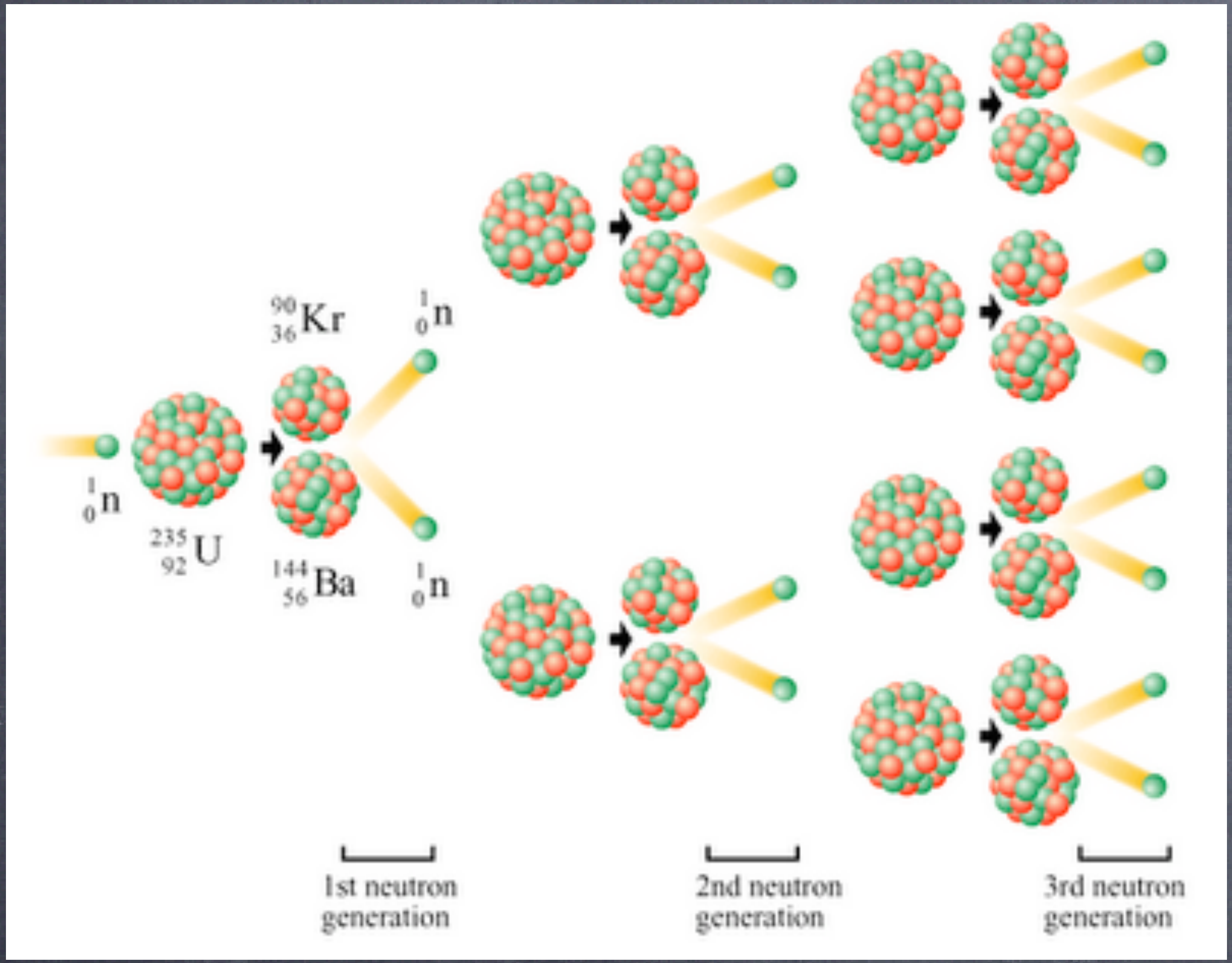
⟶ simulating physics

Theory?

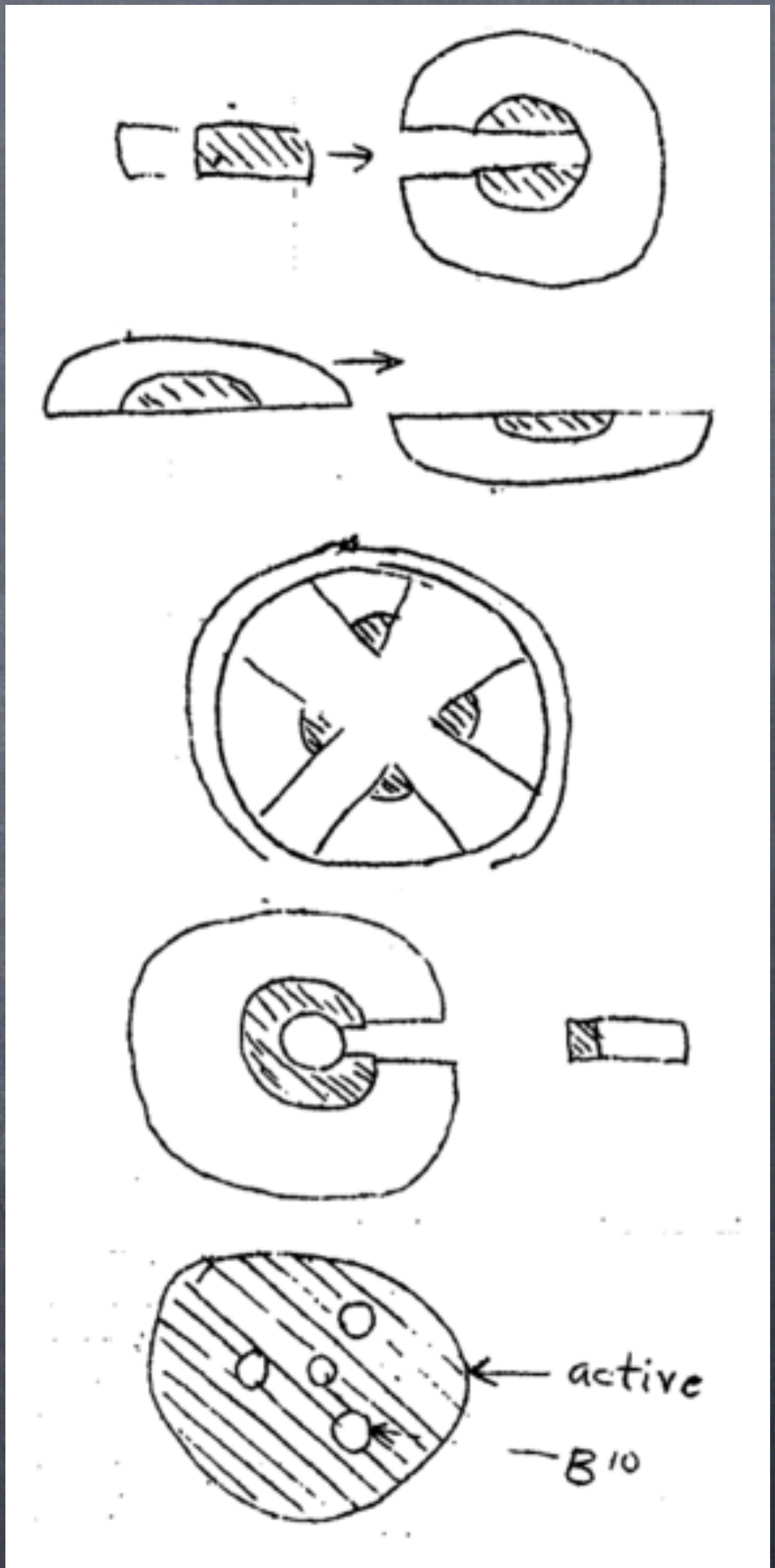


$^{1}_{0}n$
$^{235}_{92}U$
$^{90}_{36}Kr$
$^{144}_{56}Ba$
$^{1}_{0}n$
$^{1}_{0}n$
1st neutron generation
2nd neutron generation
3rd neutron generation

Theory?

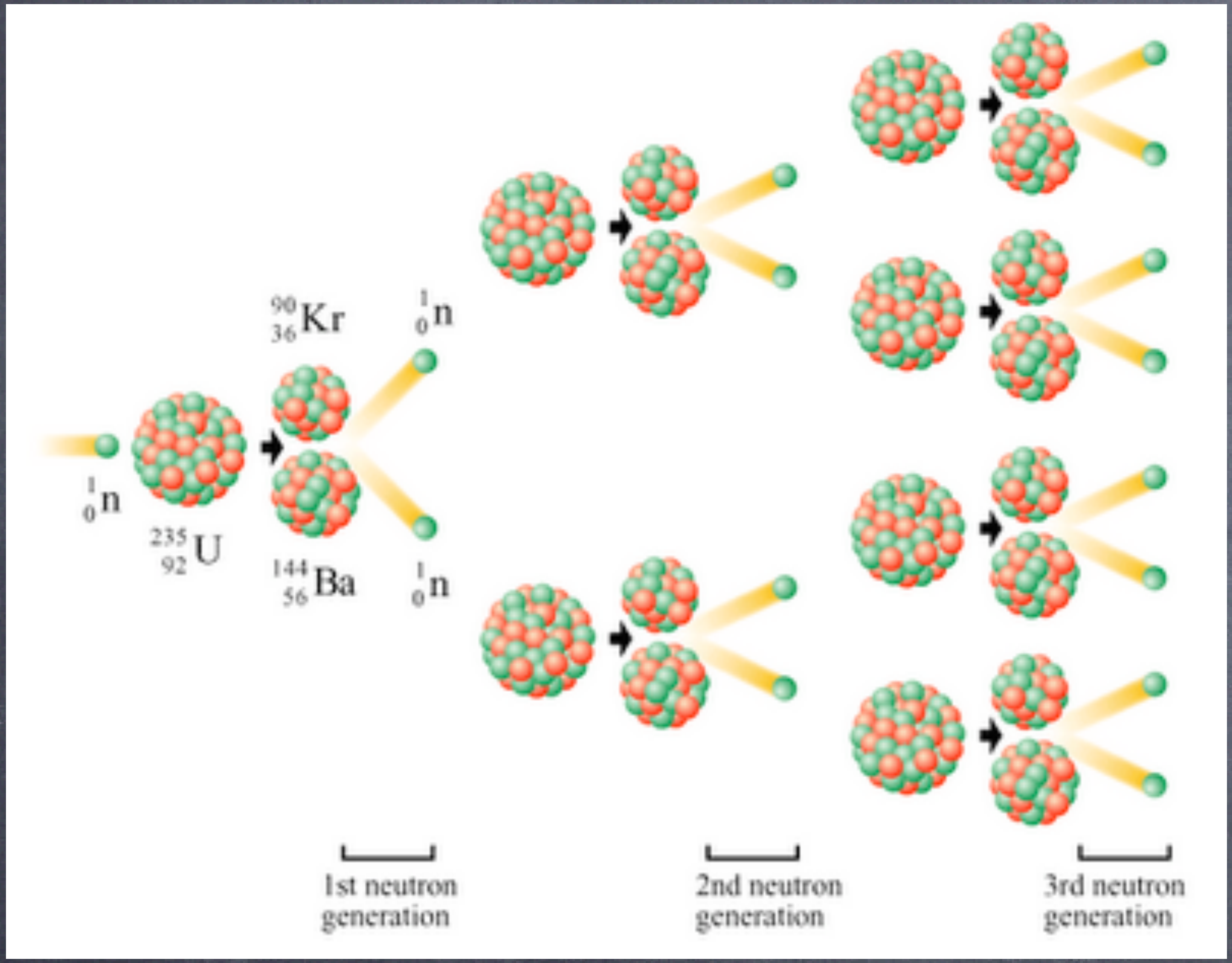


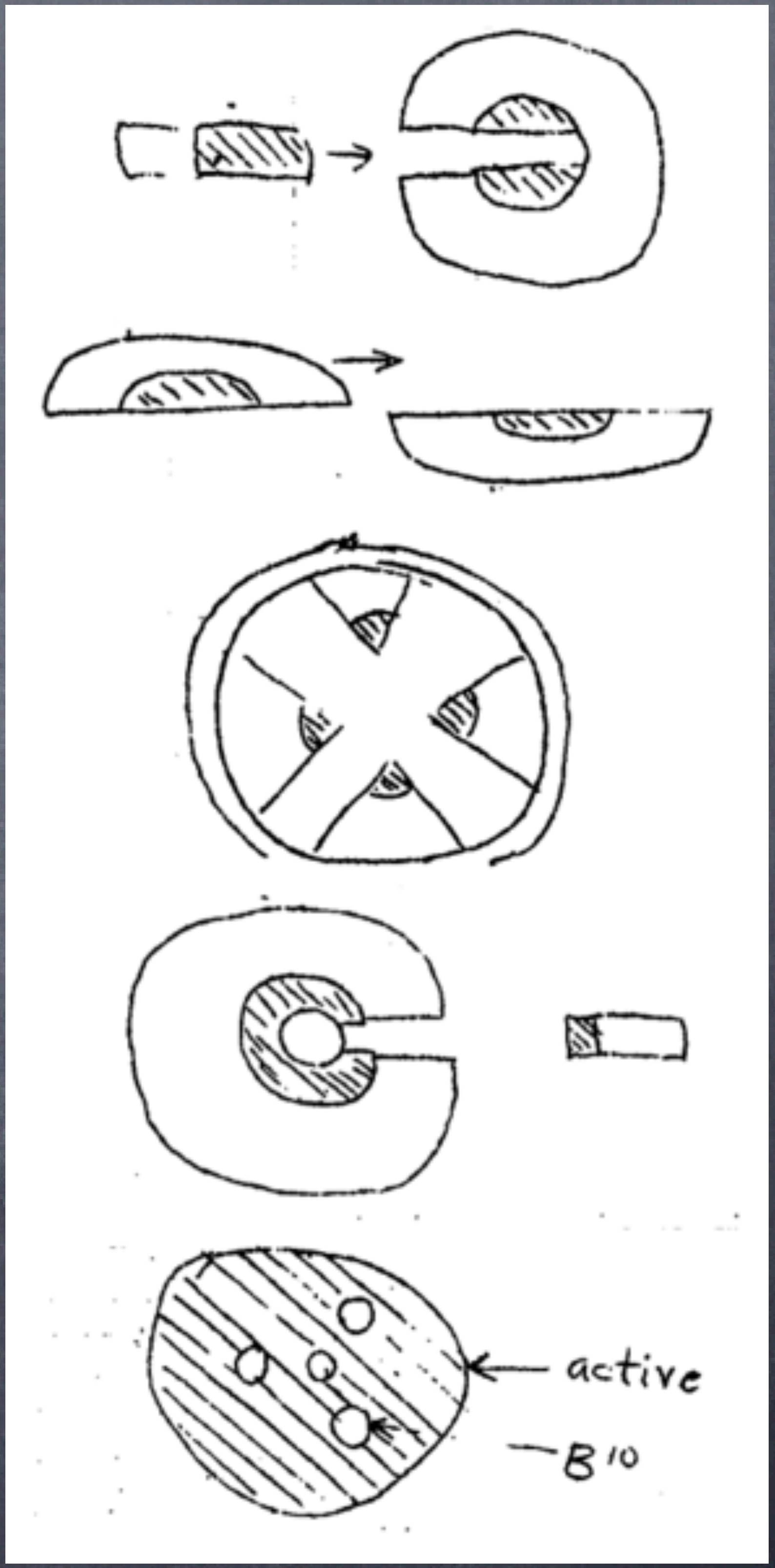
$^{1}_{0}n$
$^{235}_{92}U$
$^{90}_{36}Kr$
$^{144}_{56}Ba$
$^{1}_{0}n$
$^{1}_{0}n$
1st neutron generation
2nd neutron generation
3rd neutron generation



active
B^{10}

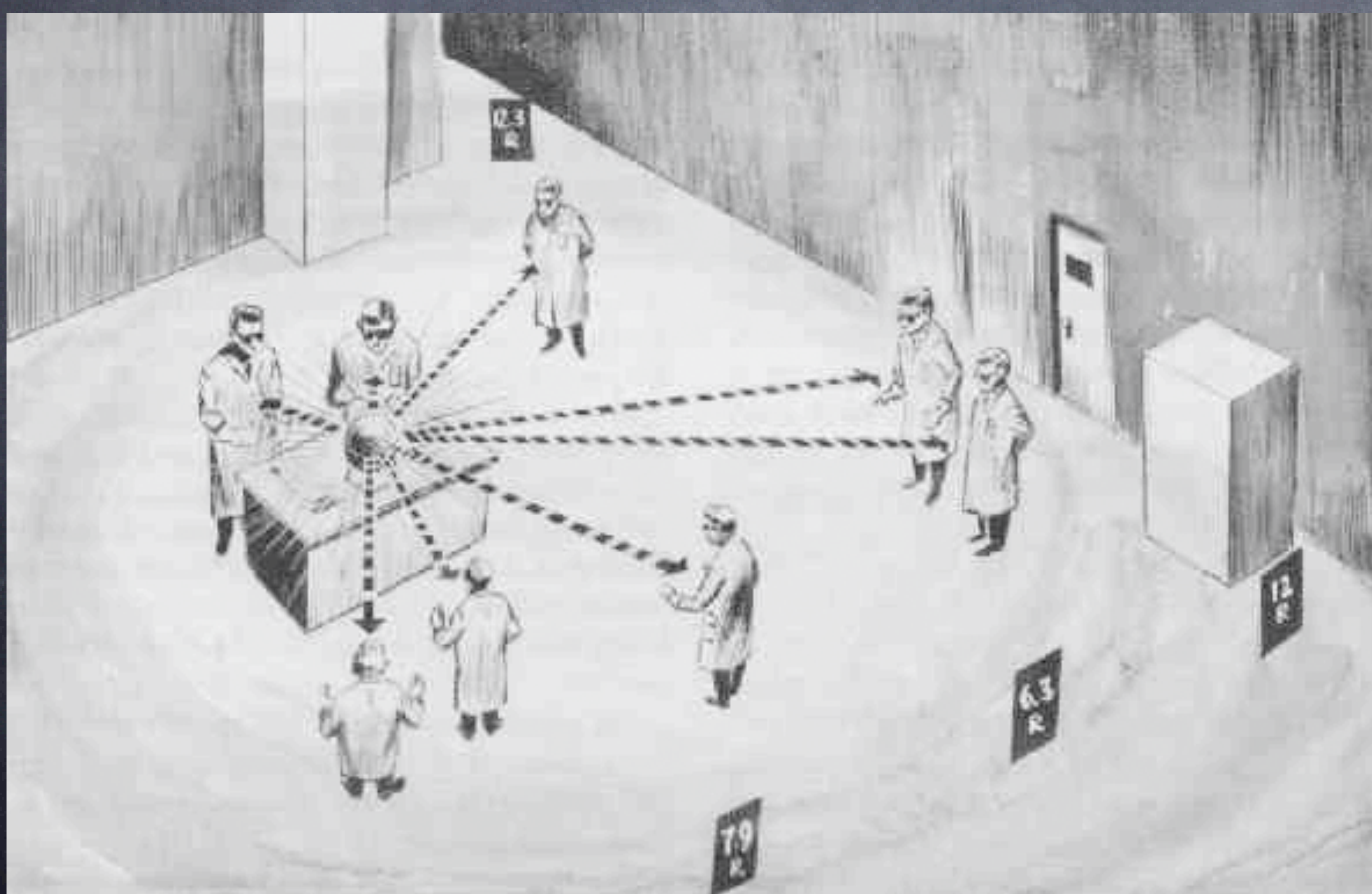
Theory?



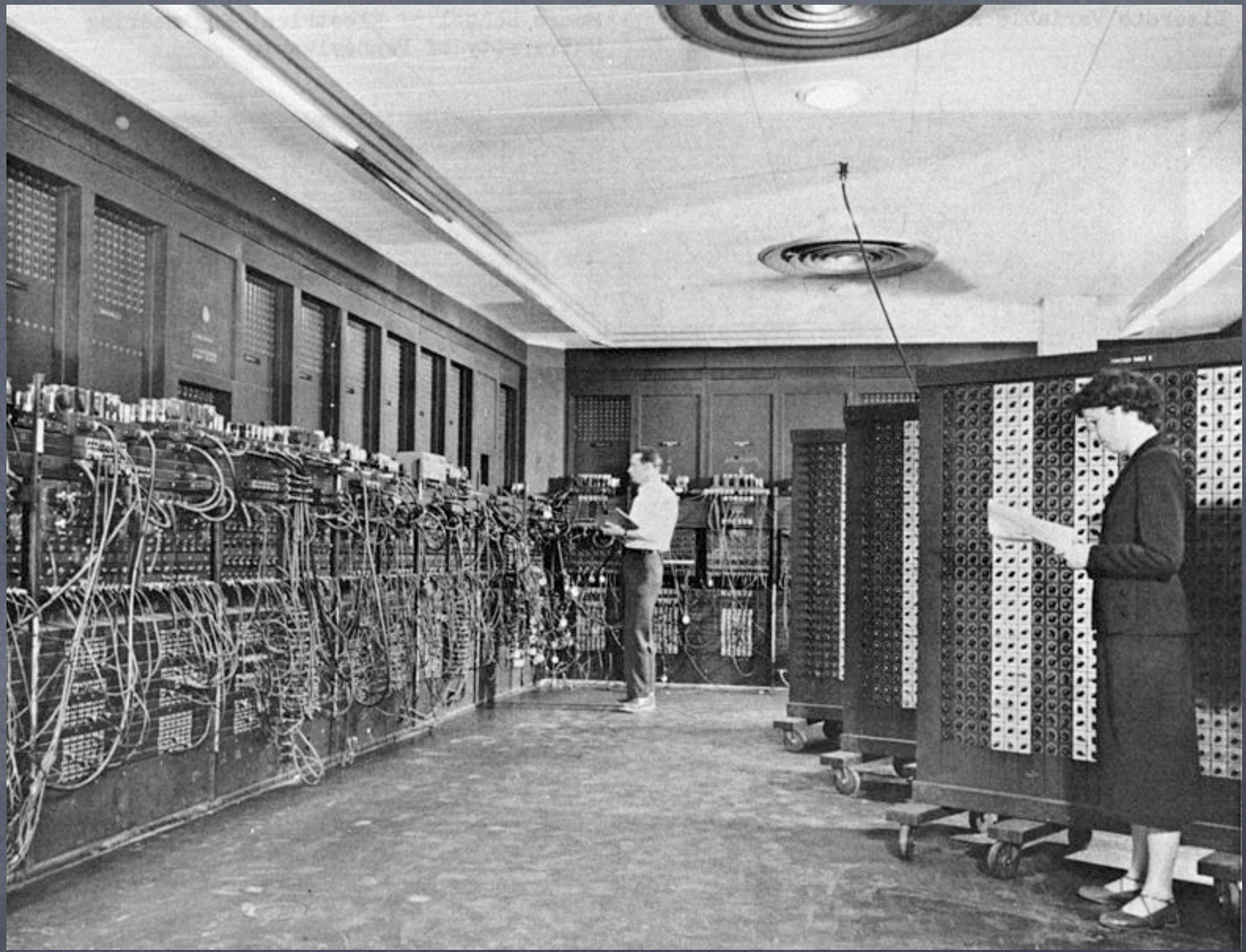


"Marge, I agree with you - in theory. In theory, communism works. In theory."
-- Homer Simpson

Experiment?

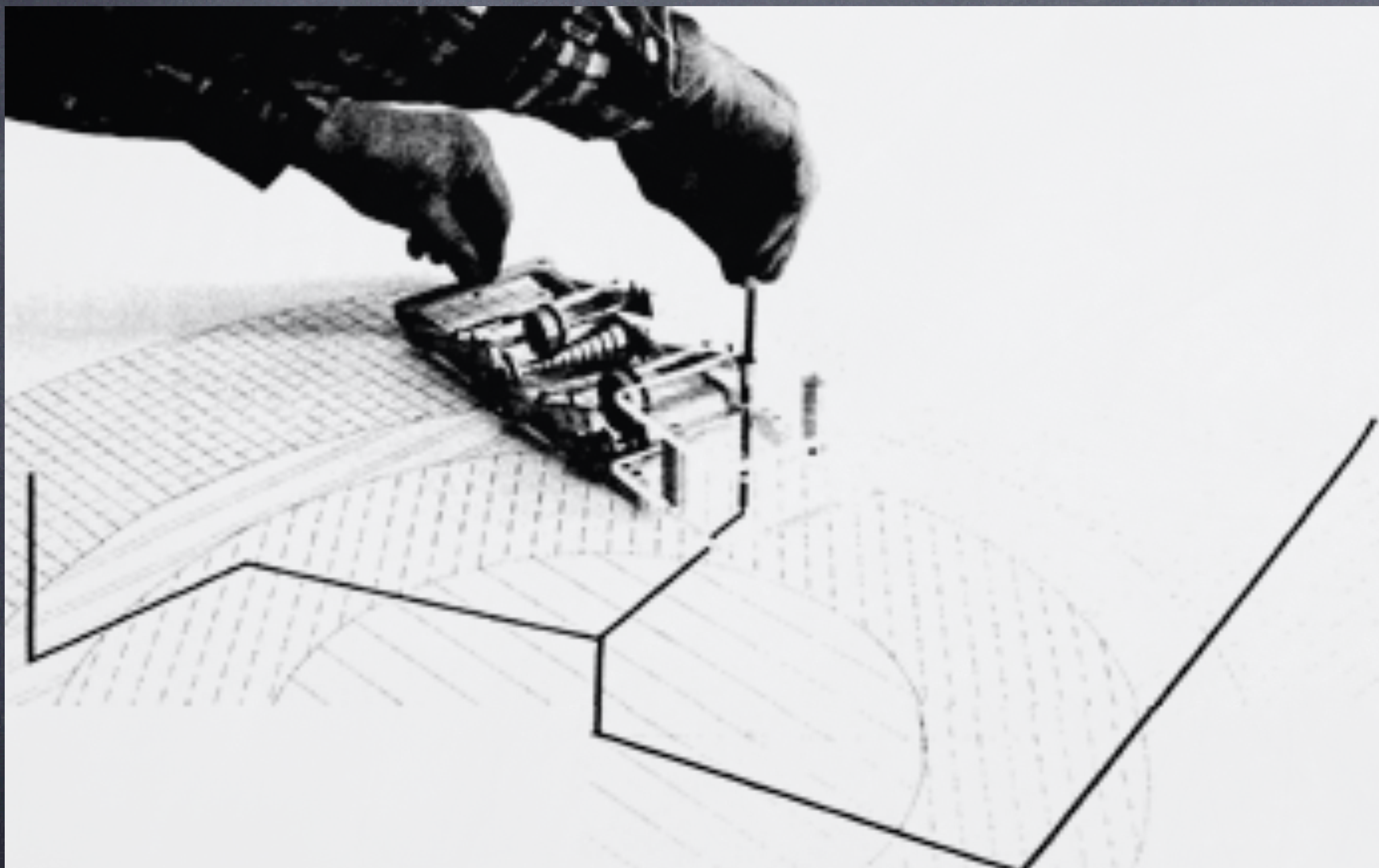


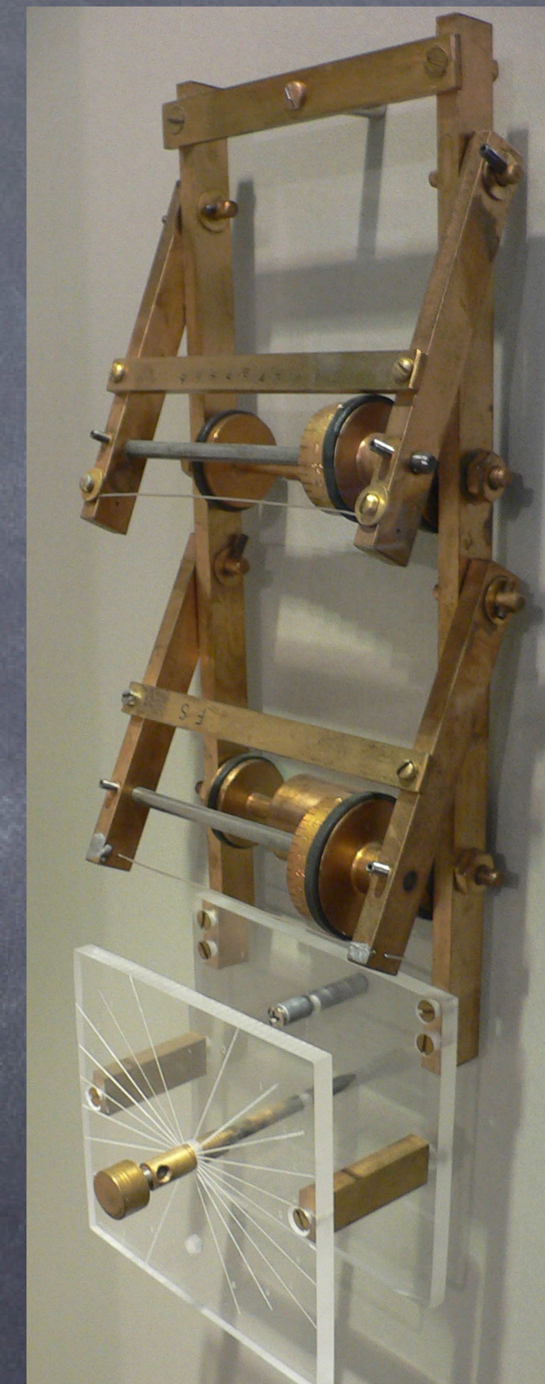
Simulation!



ENIAC (1946)

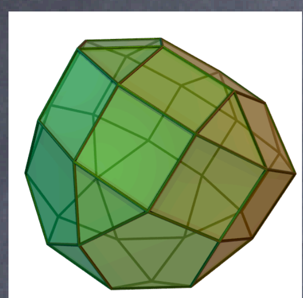
FERMIAC





modern uses of randomness

query complexity



If the election were held today...

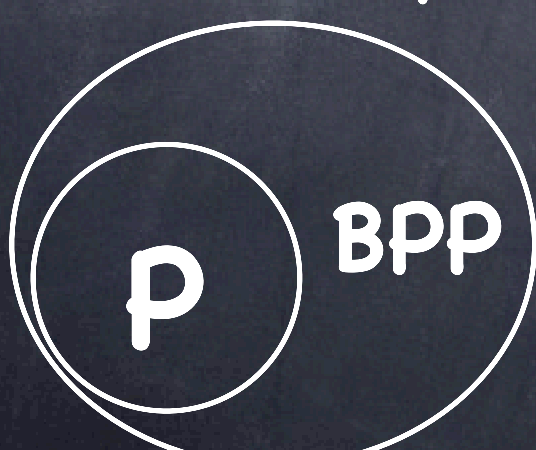
volume estimation

averages

communication complexity

e.g. equality testing

computational complexity



$$(x+y)(x-y) = x^2 - y^2$$

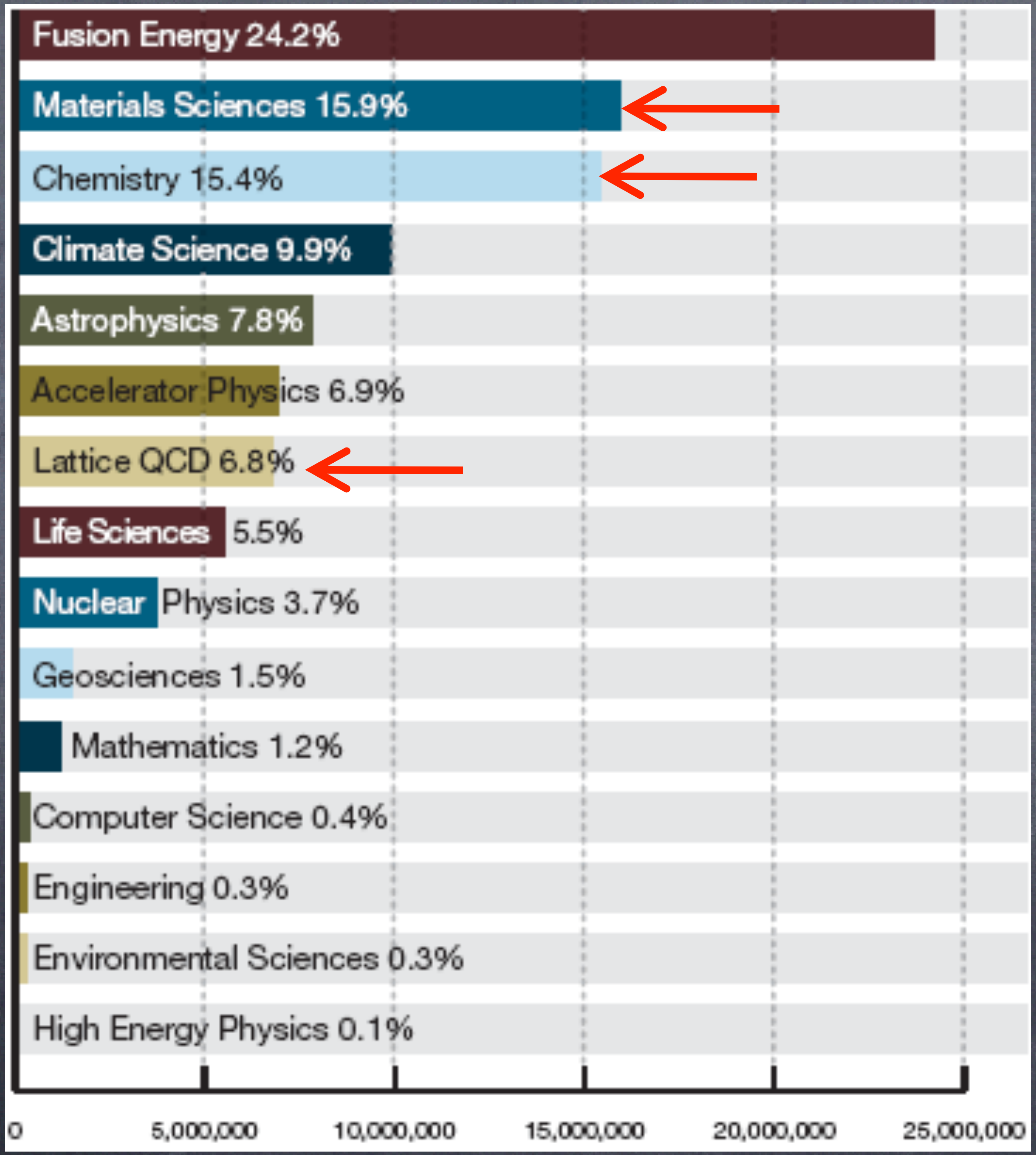
cryptography

quantum computing: also started with simulation

Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

Richard Feynman, 1982

use of DOE supercomputers by area



From a talk by S. Aaronson from a talk by A. Aspuru-Guzik.

beyond simulation

$$\boxed{\begin{array}{c}213981239012389123712938721 90\\387123987123891723981273910 2\\837129083712988964375843658\\716502364789231648712346291 8\\746231897462134876123874612 38\\794623914723164293147632494 1\end{array}} = \boxed{?} \times \boxed{?}$$

n digits

beyond simulation

21398123901238912371293872190
38712398712389172398127391O2
83712908371298896437584365 8
71650236478923164871234629 18
746231897462134876123874612 38
79462391472316429314763249 41

n digits

= ? × ?

Best classical algorithm:

time $O(\exp(n^{1/3}))$

beyond simulation

$$\boxed{\begin{matrix}213981239012389123712938 72190\\387123987123891723981273 9102\\837129083712988964375843658\\716502364789231648712346 2918\\746231897462134876123874 61238\\794623914723164293147632 4941\end{matrix}} = \boxed{?} \times \boxed{?}$$

n digits

Best classical algorithm:
time $O(\exp(n^{1/3}))$

Shor's algorithm (1994):
poly(n) time
on a quantum computer

Fourier sampling

A function f(x) has Fourier transform $\hat{f}(k)$.

Parseval's theorem:

If $\sum_x |f(x)|^2 = 1$ then $\sum_k |\hat{f}(k)|^2 = 1$

Fourier sampling

A function f(x) has Fourier transform $\hat{f}(k)$.

Parseval's theorem:

If $\sum_x |f(x)|^2 = 1$ then $\sum_k |\hat{f}(k)|^2 = 1$

Key tool in Shor's algorithm:

Quantum computers can sample from

$$\Pr[k] = |\hat{f}(k)|^2$$

probabilistic bits

probabilistic bits

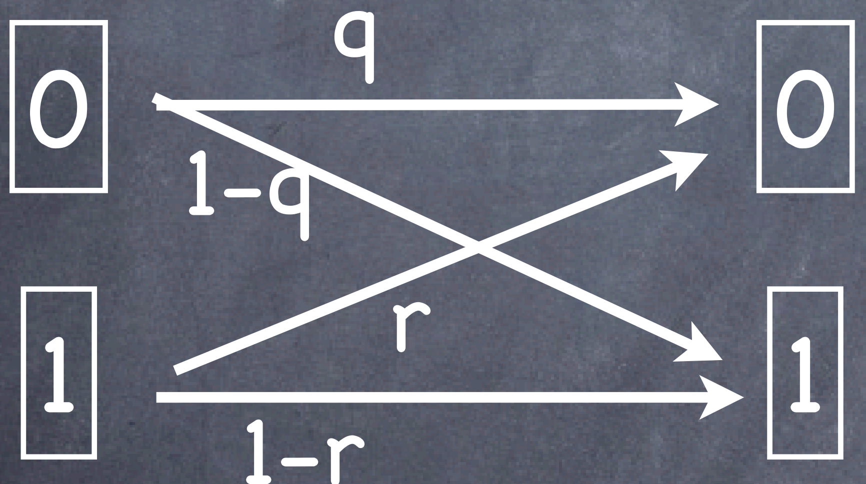
description: $\vec{p} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}$ $\qquad$ $p_0, p_1 \geq 0$, $p_0 + p_1 = 1$

probabilistic bits

description: $\vec{p} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}$ $\qquad p_0, p_1 \geq 0$

$p_0 + p_1 = 1$

evolution:



$$\begin{bmatrix} q & r \\ 1-q & 1-r \end{bmatrix}$$

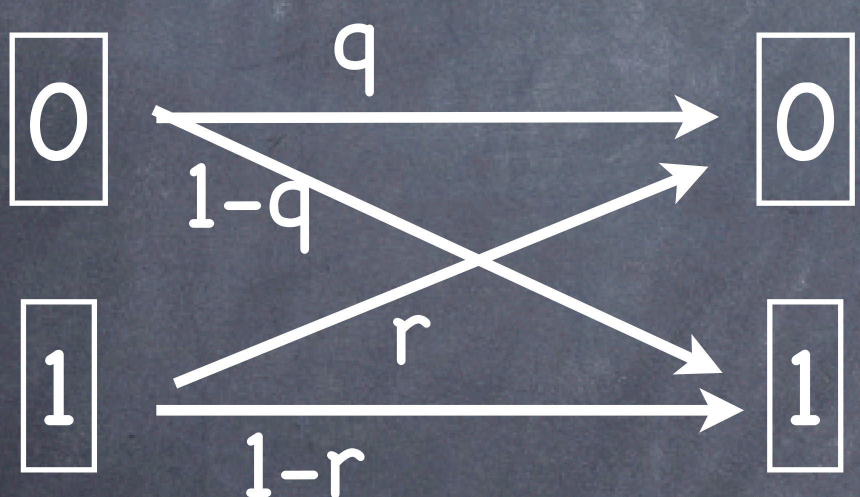
stochastic matrix

probabilistic bits

description: $\vec{p} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}$

$$p_0, p_1 \geq 0$$
$$p_0 + p_1 = 1$$

evolution:



$$\begin{bmatrix} q & r \\ 1-q & 1-r \end{bmatrix}$$

stochastic matrix

measurement:

$\vec{p} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}$

$\boxed{0}$ with probability p_0

$\boxed{1}$ with probability p_1

quantum bits (qubits)

quantum bits (qubits)

description: $|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$

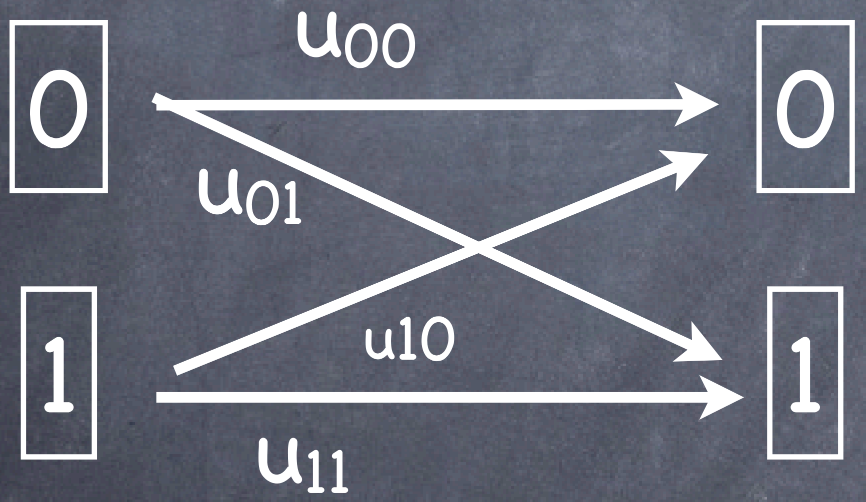
$$|a_0|^2 + |a_1|^2 = 1$$

quantum bits (qubits)

description: $$|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

$$|a_0|^2 + |a_1|^2 = 1$$

evolution:



$$\begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

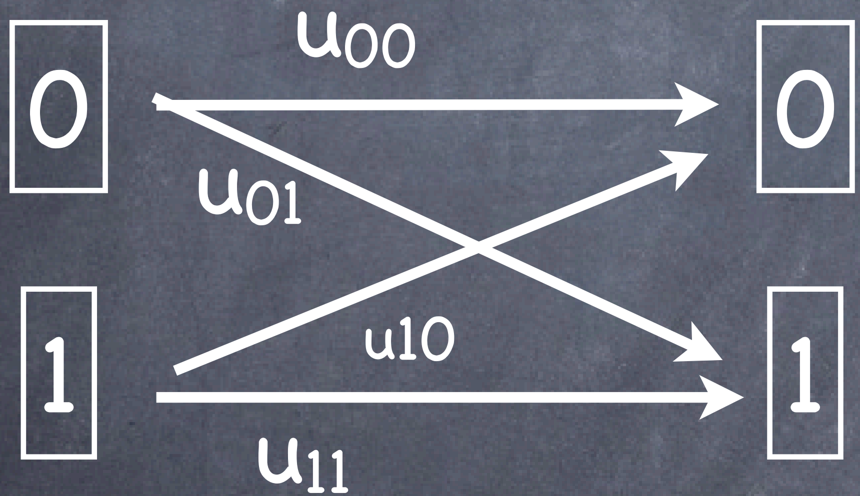
unitary matrix

quantum bits (qubits)

description: $$|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

$$|a_0|^2 + |a_1|^2 = 1$$

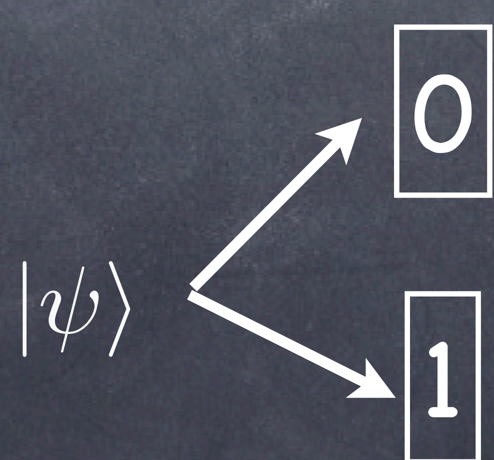
evolution:



$$\begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

unitary matrix

measurement:



with probability $|a_0|^2$

with probability $|a_1|^2$

basis dependence

n qubits = 2^n dimensions

Measurements can be in any basis.

The computational basis is one choice:

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

But not the only one...

quantum analogues of sampling

1. Sampling from a distribution, but encoded in an unknown basis.

2. Sampling in a known basis

3. The ability to prepare $$\sum_{i=1}^{N} \sqrt{p_i}|i\rangle$$

1. the birthday problem

Distinguish BIG from small

samples needed?

Classical	Draw random items from a set of size N or N/2.	
Quantum	Draw random vectors from a subspace of dimension N or N/2.	

1. the birthday problem

Distinguish BIG from small

samples needed?

Classical	Draw random items from a set of size N or N/2.	$\sqrt{N}$
Quantum	Draw random vectors from a subspace of dimension N or N/2.	

1. the birthday problem

Distinguish BIG from small

samples needed?

Classical	Draw random items from a set of size N or N/2.	$\sqrt{N}$
Quantum	Draw random vectors from a subspace of dimension N or N/2.	N

1. the birthday problem

Distinguish BIG from small

samples needed?

Classical	Draw random items from a set of size N or N/2.	$\sqrt{N}$
Quantum	Draw random vectors from a subspace of dimension N or N/2.	N

Proof/algorithm uses Schur-Weyl duality between representation theory of symmetric and unitary groups

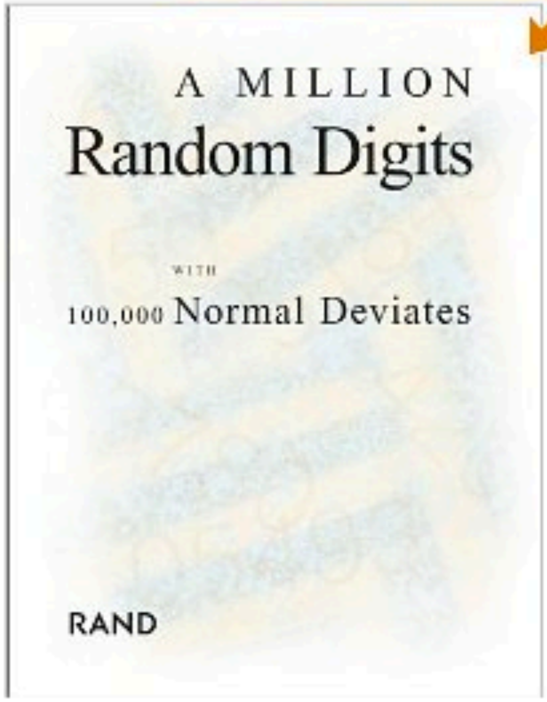
[Childs, H, Wocjan. STACS '07]

2. testing probability distributions

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Random numbers are valuable, but how do you know you're getting what you pay for?

Click to LOOK INSIDE!



Share your own customer images

Search inside this book

A Million Random Digits with 100,000 Normal Deviates [Paperback]

RAND Corporation (Author)

(213 customer reviews)

List Price: ~~$90.00~~

Price: $81.01 & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $8.99 (10%)

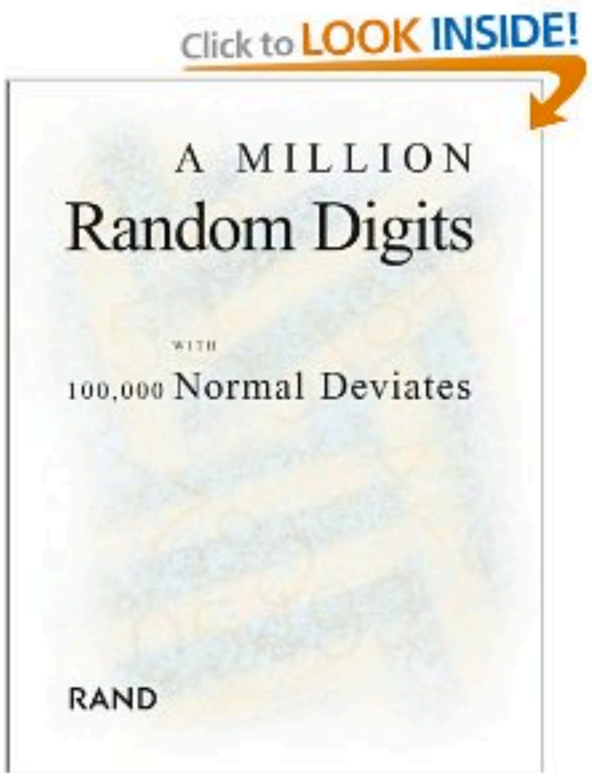
Usually ships within 1 to 2 months.

Ships from and sold by **Amazon.com**. Gift-wrap available.

8 new from $78.61 **7 used** from $75.36

Formats	Amazon Price	New from	Used from
Hardcover	--	--	$94.58
Paperback	$81.01	$78.61	$75.36

Show 1 more format



Share your own customer images

Search inside this book

A Million Random Digits with 100,000 Normal Deviates [Paperback]

RAND Corporation (Author)

(213 customer reviews)

List Price: ~~$90.00~~

Price: $81.01 & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $8.99 (10%)

Usually ships within 1 to 2 months.

Ships from and sold by **Amazon.com**. Gift-wrap available.

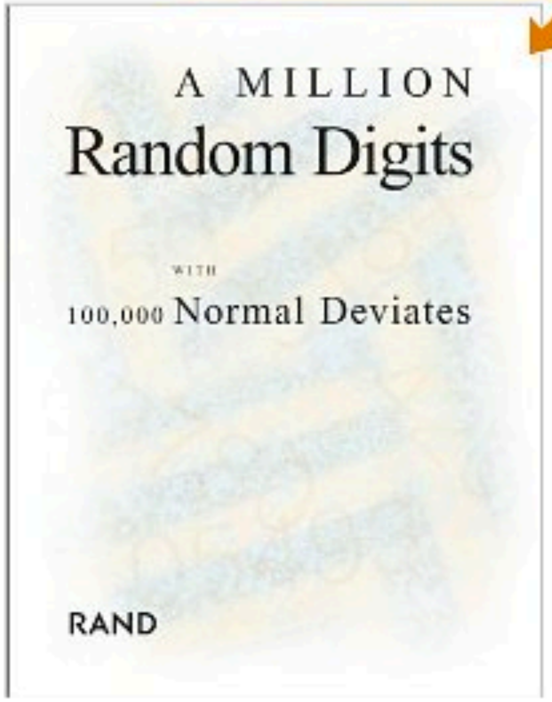
8 new from $78.61 7 used from $75.36

Formats	Amazon Price	New from	Used from
Hardcover	--	--	$94.58
Paperback	$81.01	$78.61	$75.36

Show 1 more format

00250	59467	58309	87834	57213	37510	33689	01259	62486	56320	46265
00251	73452	17619	56421	40725	23439	41701	93223	41682	45026	47505
00252	27635	56293	91700	04391	67317	89604	73020	69853	61517	51207
00253	86040	02596	01655	09918	45161	00222	54577	74821	47335	08582
00254	52403	94255	26351	46527	68224	90183	85057	72310	34963	83462
00255	49465	46581	61499	04844	94626	02963	41482	83879	44942	63915
00256	94365	92560	12363	30246	02086	75036	88620	91088	67691	67762
00257	34261	08769	91830	23313	18256	28850	37639	92748	57791	71328
00258	37110	66538	39318	15626	44324	82827	08782	65960	58167	01305
00259	83950	45424	72453	19444	68219	64733	94088	62006	89985	36936
00260	61630	97966	76537	46467	30942	07479	67971	14558	22458	35148
00261	01929	17165	12037	74558	16250	71750	55546	29693	94984	37782
00262	41659	39098	23982	29899	71594	77979	54477	13764	17315	72893
00263	32031	39608	75992	73445	01317	50525	87313	45191	30214	19769
00264	90043	93478	58044	06949	31176	88370	50274	83987	45316	38551

Click to LOOK INSIDE!



Share your own customer images

Search inside this book

A Million Random Digits with 100,000 Normal Deviates [Paperback]

RAND Corporation (Author)

(213 customer reviews)

List Price: ~~$90.00~~

Price: **$81.01** & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $8.99 (10%)

Usually ships within 1 to 2 months.

Ships from and sold by **Amazon.com**. Gift-wrap available.

8 new from $78.61 7 used from $75.36

Formats	Amazon Price	New from	Used from
Hardcover	--	--	$94.58
Paperback	$81.01	$78.61	$75.36

Show 1 more format

6 TABLE OF RANDOM DIGITS

Sloppy., July 27, 2005

By **B. MCGROARTY** (United States) - See all my reviews

REAL NAME

This review is from: A Million Random Digits with 100,000 Normal Deviates (Paperback)

The book is a promising reference concept, but the execution is somewhat sloppy. Whatever algorithm they used was not fully tested. The bulk of each page seems random enough. However at the lower left and lower right of alternate pages, the number is found to increment directly.

Help other customers find the most helpful reviews

Was this review helpful to you? Yes No

Report abuse | Permalink

Comments (13)

classical sampling algorithm $\longrightarrow$ i with probability p_i

classical sampling algorithm $\longrightarrow$ i with probability p_i

Take the internal coin-flips outside

Random seed $r \in \{0,1\}^m$ $\longrightarrow$ classical sampling algorithm $\longrightarrow$ $i=f(r)$

where $p_i = \frac{|f^{-1}(i)|}{2^m}$

classical sampling algorithm $\longrightarrow$ i with probability p_i

Take the internal coin-flips outside

Random seed $r \in \{0,1\}^m$ $\longrightarrow$ classical sampling algorithm $\longrightarrow$ $i = f(r)$

where $p_i = \dfrac{|f^{-1}(i)|}{2^m}$

Note: too unstructured for exponential speedup!

Samples/queries needed

Problem	Classical	Quantum
Uniformity testing	$N^{1/2}$	$N^{1/3}$
Statistical distance	$N^{1-o(1)}$	$N^{1/2}$
Orthogonality	$N^{1/2}$	$N^{1/3}$

[Bravyi, H, Hassidim. IEEE Trans. Inf. Th. 2011]

Samples/queries needed

SZK

Problem	Classical	Quantum
Uniformity testing	$N^{1/2}$	$N^{1/3}$
Statistical distance	$N^{1-o(1)}$	$N^{1/2}$
Orthogonality	$N^{1/2}$	$N^{1/3}$

[Bravyi, H, Hassidim. IEEE Trans. Inf. Th. 2011]

Where this is going

- Classical distribution testing has a "canonical tester" [Valiant, STOC '08].
- All of our quantum algorithms look different.
- What can quantum computers do with unstructured problems? Is there a quantum canonical tester?

3. q-sampling

$$\sum_{i=1}^{N} \sqrt{p_i}|i\rangle$$

3. q-sampling

$$\sum_{i=1}^{N} \sqrt{p_i} |i\rangle$$

SWAP test: Given q-samples of p and q, the swap test accepts with probability

$$\frac{1 + \left(\sum_{i=1}^{N} \sqrt{p_i q_i}\right)^2}{2}$$

Uniformity testing, etc. with O(1) samples.

product test

Problem: p is a distribution on $\overbrace{[d] \times \cdots \times [d]}^{n}$
Is p close or far from a product distribution?

Classically: Need $O(d^{n/2})$ samples.

With q-samples: 2 samples suffice
[H, Montanaro. FOCS 2010]

Applications: complexity of tensor problems

q-samples and Markov chains

$\Pr[j] = \mathbf{M}_{ji}$

$i \longrightarrow$ Markov chain $\mathbf{M}$ $\longrightarrow j$

q-samples and Markov chains

$\Pr[j] = \mathbf{M}_{ji}$

$i \longrightarrow$ **Markov chain M** $\longrightarrow j$

Def: π is stationary distribution $\Leftrightarrow$ $M\pi=\pi$

q-samples and Markov chains

$\Pr[j] = \mathbf{M}_{ji}$

$i \longrightarrow$ **Markov chain M** $\longrightarrow j$

Def: π is stationary distribution $\Leftrightarrow M\pi=\pi$

Thm: q-samples of π can be distinguished from orthogonal states for reasonable M

q-samples and Markov chains

$\Pr[j] = \mathbf{M}_{ji}$

$i \longrightarrow$ Markov chain **M** $\longrightarrow j$

Def: π is stationary distribution $\Leftrightarrow$ $M\pi=\pi$

Thm: q-samples of π can be distinguished from orthogonal states for reasonable M

Used for testing quantum money.

Pseudo-entanglement

- Entanglement is a q-sample of correlated randomness.
- Are there quantum versions of pseudo-randomness? Goal: fool low-communication protocols
- Can test entanglement using quantum expanders and very little communication.
- Therefore, pseudo-entanglement is impossible.

Reversing dynamics

Reversing dynamics

- Probabilistic dynamics are irreversible, but quantum mechanics is reversible.

Reversing dynamics

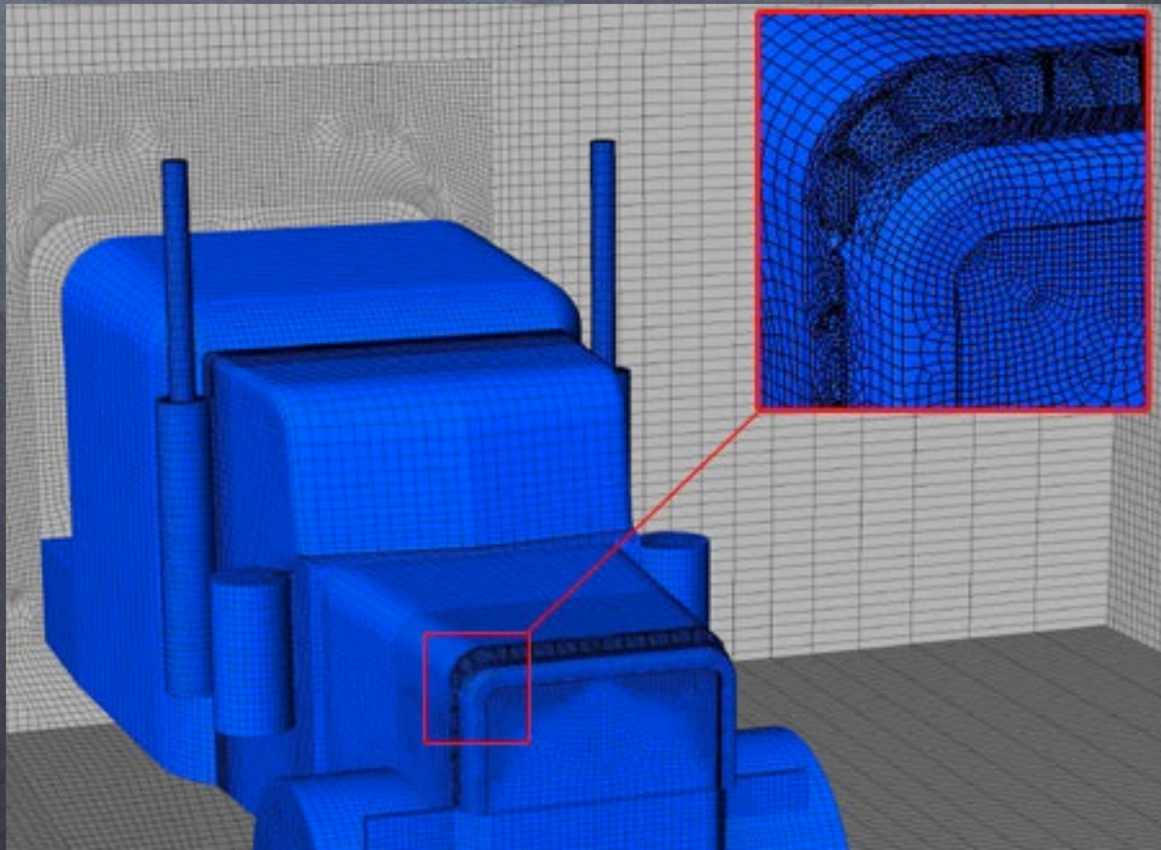
- Probabilistic dynamics are irreversible, but quantum mechanics is reversible.
- With q-samples we can apply M or M^{-1}.

Reversing dynamics

- Probabilistic dynamics are irreversible, but quantum mechanics is reversible.
- With q-samples we can apply M or M^{-1}.
- Linear systems of equations:
  Given A,b solve $Ax=b$.

Reversing dynamics

- Probabilistic dynamics are irreversible, but quantum mechanics is reversible.
- With q-samples we can apply M or M^{-1}.
- Linear systems of equations:
  Given A,b solve Ax=b.
- Exponential speedup (sometimes).
  [H, Hassidim, Lloyd. Phys. Rev. Lett. '09]



Recap

Quantum versions of sampling can:

1. Estimate quantum states
2. Estimate probability distributions
3. Create powerful new quantum algorithms

Recap

Quantum versions of sampling can:

1. Estimate quantum states
2. Estimate probability distributions
3. Create powerful new quantum algorithms

...and can help answer the big questions:

What advantages do quantum computers offer?

How should we think about quantum information?

For more information

visit me: CSE 596

or my website:

http://www.cs.washington.edu/homes/aram

or my (quantum) class 599D

MW10:30-11:50