Randomness
(and Pseudorandomness)

Avi Wigderson
IAS, Princeton

Plan of the talk

Perfect Randomness

Uniform distribution
Full entropy

Prob[T]=Prob[H]=½, Independent

HHTHTTTHHHTHTTHTTTHHHHTHTTTTTHHTHH

HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH

The amazing utility of randomness - lots of examples. Are they real?

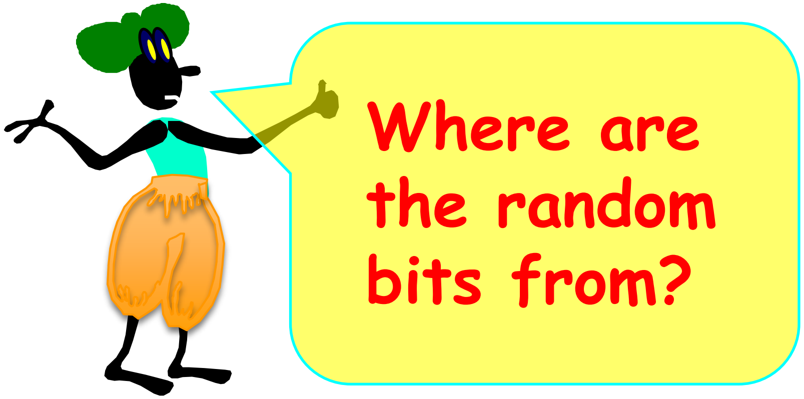
Pseudorandomness

Deterministic structures which share *some* properties of random ones

Lots of examples & applications

Surviving weak or no randomness

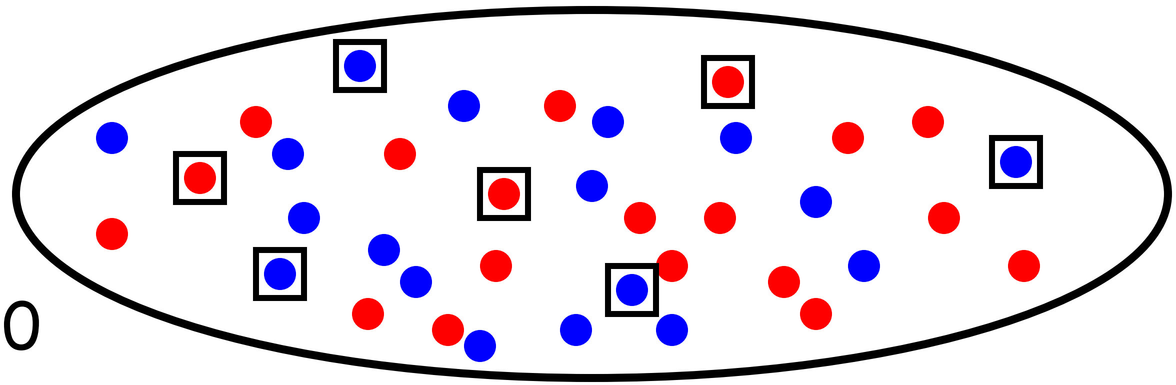
The remarkable utility of randomness



Fast Information Acquisition

Population: 280 million, voting blue or red

Random Sample: 2,000

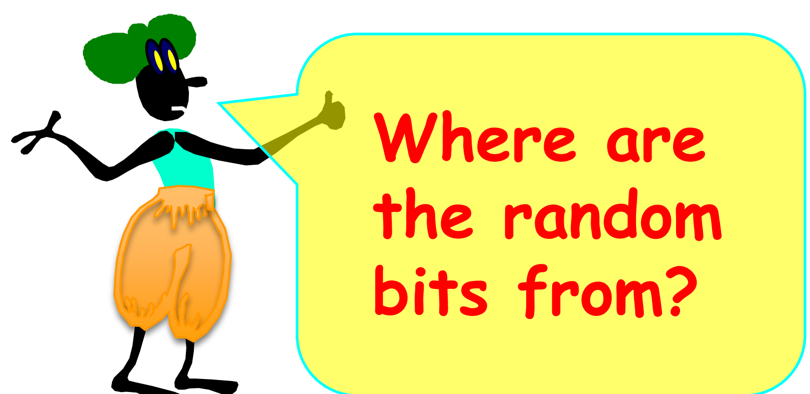


Theorem: With probability > .99

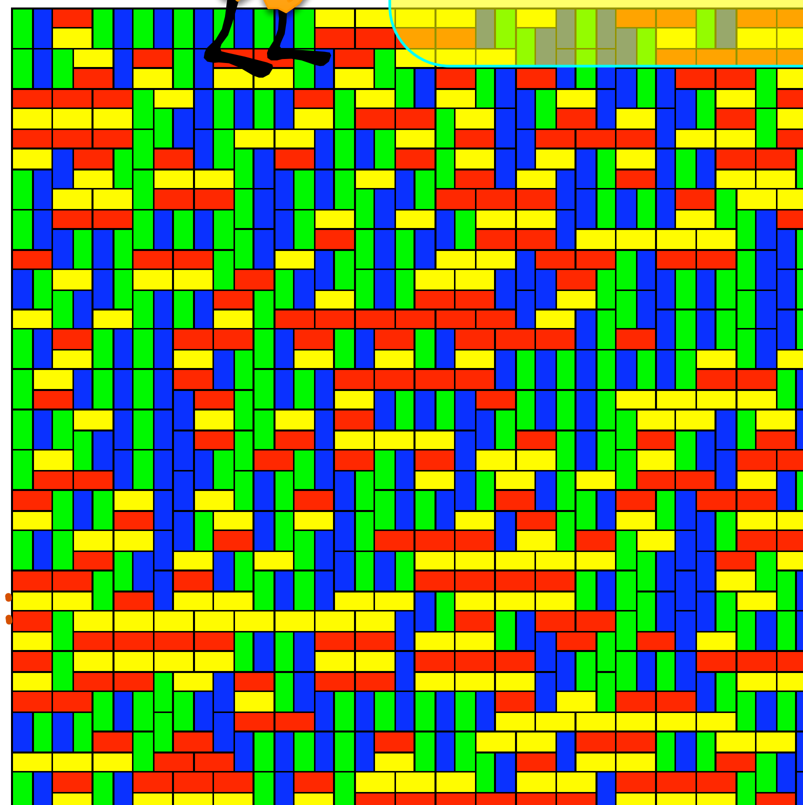
% in sample = % in population $\pm$ 2%

independent of population size

Deterministically, need to ask the whole population!



Efficient (!!) Probabilistic Algorithms



Given a region in space, how many domino tilings does it have?

Monomer-Dimer problem.

Captures thermodynamic properties of matter (free energy, phase transitions,...)

Theorem [Jerrum-Sinclair-Vigoda]: Efficient probabilistic approximate counting algorithm ("Monte-Carlo" method [von Neumann-Ulam])

Best deterministic algorithm known requires exponential time!

One of numerous examples

Probabilistic algorithms in math

Number theory
- Finding large primes

Algebra
- Factoring multivariate polynomials over finite fields

Geometry
- Approximating the volume of convex sets in high dimension

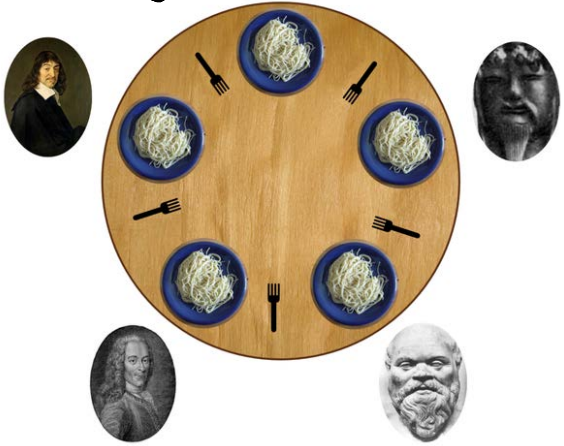
Analysis
- Computing large Fourier coeffs of multivariate functions

Fast probabilistic algorithms

Best known deterministic algorithms require exponential time

Distributed computation

Randomness makes impossible problems possible



The dining philosophers problem

Captures resource allocation and sharing in asynchronous systems

Theorem [Dijkstra]:
No deterministic solution

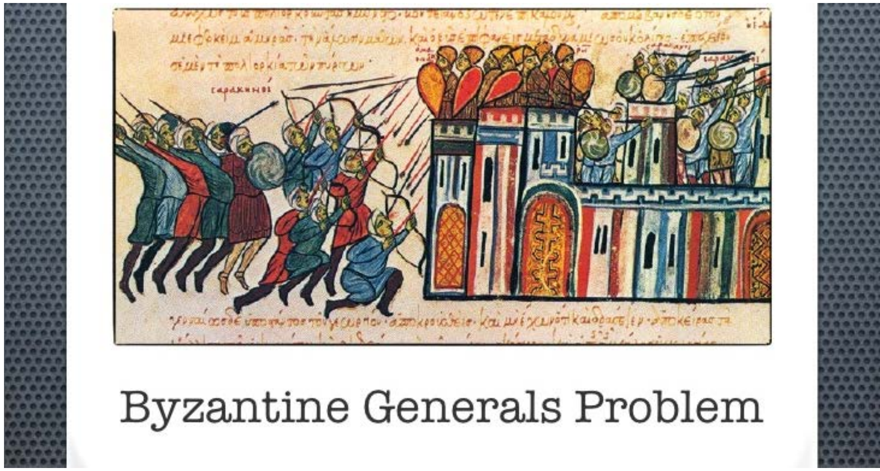
Theorem [Lehman-Rabin]:
A probabilistic program works

The Byzantine generals problem

Captures coordination with faults

Theorem [Fisher-Lynch-Paterson]:
No deterministic solution

Theorem [Ben-or, Rabin]:
A probabilistic program works



Game Theory – Rational behavior

Chicken game [Aumann]

A: Aggressive
C: Cautious

	C	A
C	1 1	0 2
A	2 0	-3 -3

Nash Equilibrium: No player has an incentive to change its strategy given the opponent's strategy.

Theorem [Nash]: Every game has an equilibrium in mixed (random) strategies
(Pr[C] $= \frac{3}{4}$, Pr[A]$= \frac{1}{4}$)

False for pure (deterministic) strategies

Cryptography & E-commerce

Secrets

Theorem [Shannon] A secret is as good as the entropy in it. (if you pick a 9 digit password randomly, my chances of guessing it is $1/10^9$)

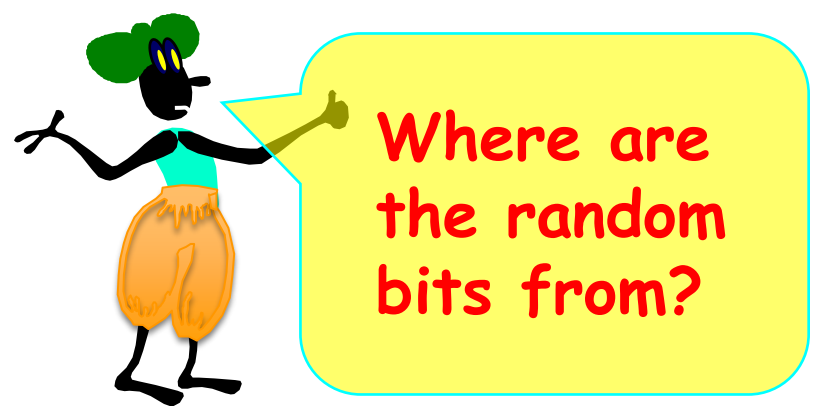
Public-key encryption (on-line shopping)

Digital signature (identification)

Zero-Knowledge Proofs (enforcing correctness)

………

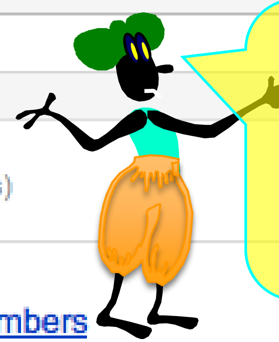
All require randomness



Gambling

Google

true random bits



Where are the random bits from?

Search

About 3,730,000 results (0.20 seconds)

Everything
Images
Maps
Videos
News
Shopping
More

Princeton, NJ
Change location

Any time
Past hour
Past 24 hours
Past week
Past month
Past year
Custom range...

All results
Sites with images
Related searches
Timeline

[HotBits: Genuine Random Numbers](www.fourmilab.ch/hotbits/)
www.fourmilab.ch/hotbits/
HotBits is a service which generates **random** data from the decay of radioactive material and sends it over the internet.

[Hardware random number generator - Wikipedia, the free ...](en.wikipedia.org/wiki/Hardware_random_number_generator)
en.wikipedia.org/wiki/Hardware_random_number_generator
Other designs use what are believed to be **true random bits** as the key for a high quality block cipher algorithm, taking the encrypted output as the random bit ...

[RANDOM.ORG - True Random Number Service](www.random.org/)
www.random.org/
ORG offers **true** random numbers to anyone on the Internet. The randomness comes ... ORG has generated 1032 billion **random bits** for the Internet community. ...

[Quantis RNG - True Random Number Generator - Overview](www.idquantique.com/true-random-number.../products-overview.ht...)
www.idquantique.com/true-random-number.../products-overview.ht...
Contrary to existing products, Quantis produces random numbers at a very high bite r up to 16Mbps. This is the highest **truly-random bit** rate available to date. ...

[True random number generators](www.robertnz.net/true_rng.html)
www.robertnz.net/true_rng.html
true random number generator. ... If you sample the output (not too quickly) you (hop to) get a series of **bits** which are statistically independent. These can be ...

[Quantum Random Bit Generator Service](random.irb.hr/)
random.irb.hr/
true randomness of data served (high per-**bit**-entropy of served data); high speed of data generation and serving; high availability of the service (including easy ...

Radiactive decay

Atmospheric noise

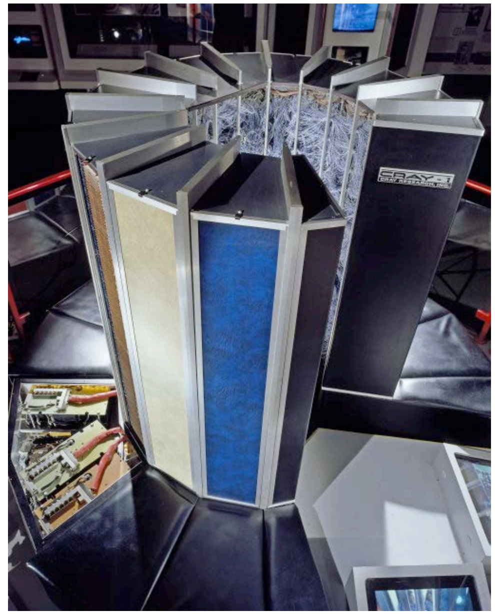
Is it working? [C,VV,MS,…]

Photons measurement

Defining randomness

[Blum-Micali ’81]

What is random?



I toss the coin, you guess how it will land

Probability of guessing correctly? 1/2

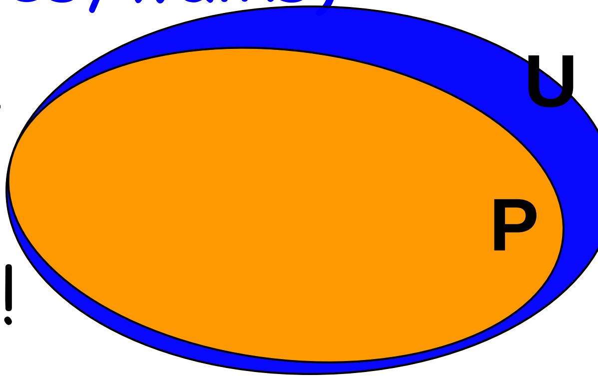
Randomness is in the ~~eye~~ of the beholder
computational power

Operative, subjective definition!

Pseudorandomness

The study of deterministic structures (numbers, graphs, sequences, tables, walks)

with **some** "random-like" properties.



Almost all $x \in U$ is also in P

P - what the limited observer tests!

Mathematics: Study of random-like properties of *natural* structures: "is $x_0 \in P$?

Computer Science: Efficiently *find* structures with random-like properties:

"find any $x \in P$"

"find hay in a haystack"

Normal Numbers

3.1415926535 8979323846 2643383279 5028841971 6939937510 5820974944 5923078164
0628620899 8628034825 3421170679 8214808651 3282306647 0938446095 5058223172
5359408128 4811174502 8410270193 8521105559 6446229489 5493038196 4428810975 6659334461
2847564823 3786783165 2712019091 4564856692 3460348610 4543266482 1339360726
0249141273 7245870066 0631558817 4881520920 9628292540 9171536436 7892590360
0113305305 4882046652 1384146951 9415116094 3305727036 5759591953 0921861173 8193261179
3105118548 0744623799 6274956735 1885752724 8912279381
8301194912 9833673362 4406566430 8602139494 6395224737 1907021798 6094370277
0539217176 2931767523 8467481846 7669405132 0005681271 4526356082 7785771342
7577896091 7363717872 1468440901 2249534301 4654958537 1050792279 6892589235
4201995611 2129021960 8640344181 5981362977 4771309960 5187072113 4999999837 2978049951
0597317328 1609631859 ………

- Every digit (e.g. 7) occurs 1/10 th of the time,
- Every pair (e.g. 54) occurs 1/100 th of the time,
- Every triple (eg 666) occurs 1/1000 th of the time,…

in every base!

Pseudorandom Property

Theorem[Borel]: A *random* real number is normal

Open: Is **π** normal? Are √2, **e** normal?

(we know efficient algs for generating normal numbers)

Major problems of Math & CS are about Pseudorandomness

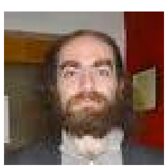
Clay Millennium Problems - $1M each

- Birch and Swinnerton-Dyer Conjecture
- Hodge Conjecture
- Navier-Stokes Equations

Pseudorandom Property

- P vs. NP

Random functions are hard to compute. Prove the same for the TSP (Traveling Salesman Problem)!



- ~~Poincaré Conjecture~~

Pseudorandom Property

- Riemann Hypothesis

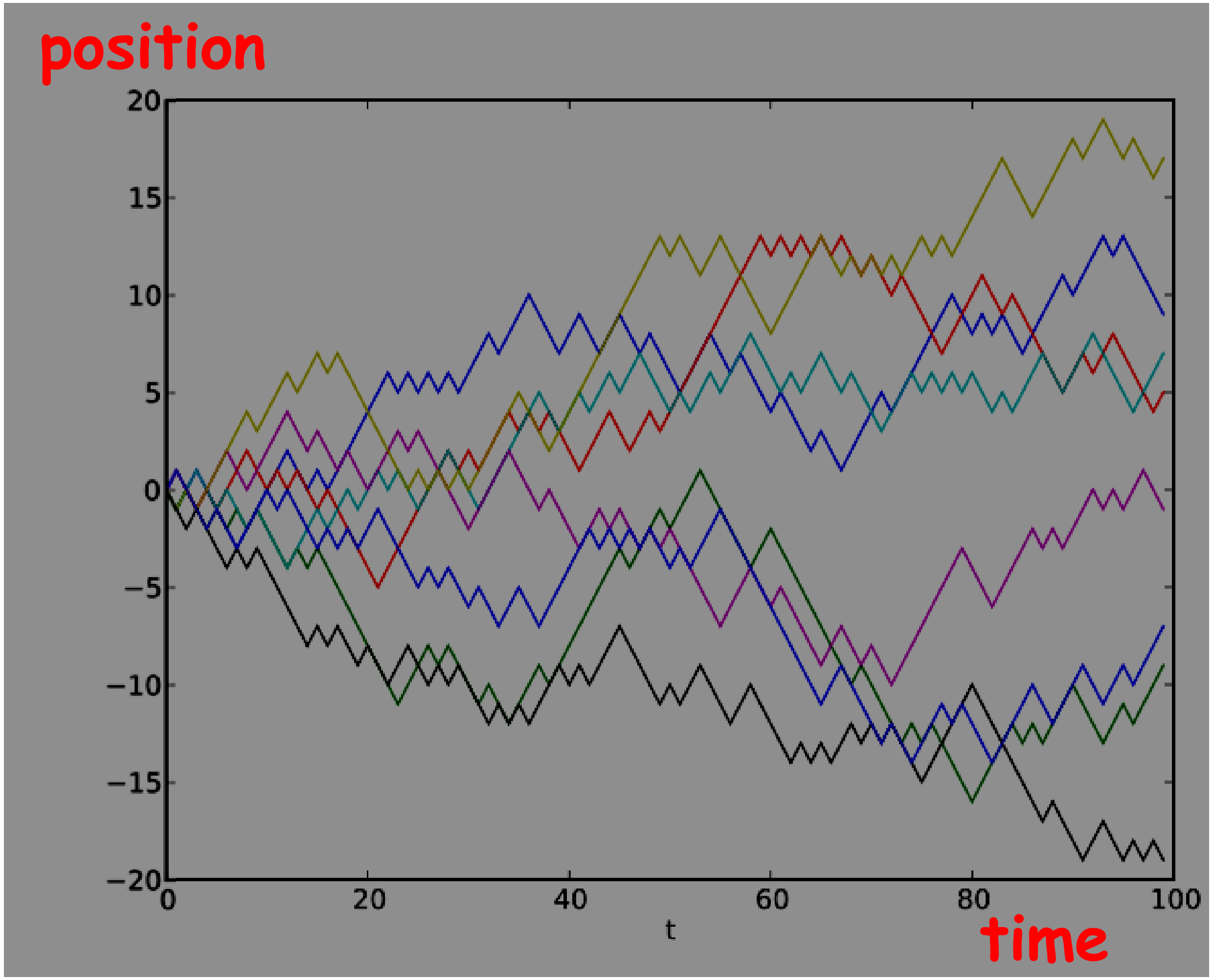
Random walks stay close to the origin. Prove the same for the Möbius walk!

- Yang-Mills Theory

Riemann Hypothesis
& the drunkard's walk

Start: 0
Each step -
Up: +1
Down: -1
Randomly.

Almost surely, after N steps distance from 0 is ~√N



Möbius' walk

x integer, p(x) number of distinct prime divisors

$$\mu(x) = \begin{cases} 0 & \text{if } x \text{ has a square divisor} \\ 1 & p(x) \text{ is even} \\ -1 & p(x) \text{ is odd} \end{cases}$$

x =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
μ(x)=	1	−1	−1	0	−1	1	−1	0	0	1	−1	0	−1	1	1	0

Theorem [Mertens 1897]: These are equivalent:

- For all N $|\Sigma_{x<N}\, \mu(x)| \sim \sqrt{N}$
- The Riemann Hypothesis

Coping in a world without perfect randomness

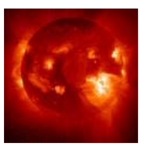
Major developments of the last 3 decades

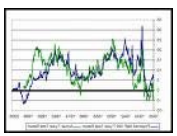
Possible worlds

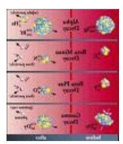
- Perfect randomness

- Weak random sources

Biased, dependent bits







- No randomness

assuming "P≠NP"

All require different
Pseudorandom notions

Applications

all applications

all algorithms

Extractor theory

[B,SV,NZ,T,…,GUV,DW,…]

purifying randomness

all *efficient* algorithms

Hardness vs. Randomness

[BM,Y,…NW,IW,…]

Every efficient prob alg has
a deterministic counterpart

Weak random sources and randomness purification

Applications:
Analyzed on perfect randomness

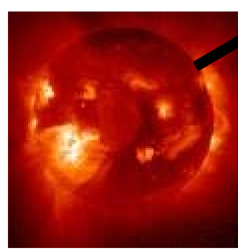
Statistics, Cryptography, Algorithms, Game theory, Gambling,……

Unbiased, independent

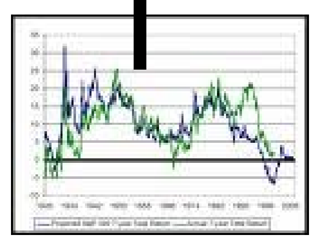
Extractor Theory

biased, dependent

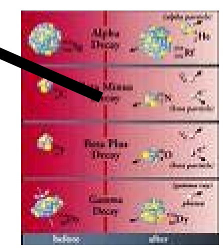
Reality:
Sources of imperfect randomness



Sun spots



Stock market fluctuations



Radioactive decay

Pseudorandom Tables

Random nxn table Entries in [n]

X	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	12	3	10	3	3	7	15	4	9	12	4	1	7	12	11
2	2	3	8	4	3	9	9	11	1	13	1	14	6	6	7
3	1	5	1	8	10	10	3	8	14	2	2	9	8	13	9
4	5	7	12	3	11	4	8	10	4	3	8	8	7	1	11
5	4	15	3	6	7	2	2	1	2	15	8	3	10	2	1
6	2	5	1	8	4	10	3	8	4	2	1	9	8	13	3
7	5	4	14	11	8	7	9	4	9	1	4	3	7	12	8
8	6	2	8	6	13	5	9	11	1	13	14	8	4	6	12
9	8	5	13	2	7	2	2	1	2	15	8	3	10	2	1
10	11	4	14	5	13	5	4	3	6	7	9	2	1	8	8
11	15	4	9	12	4	1	7	12	11	3	6	7	2	12	15
12	1	8	10	10	3	8	14	6	2	8	6	13	5	9	11
13	7	12	3	8	6	5	13	5	9	11	1	2	15	8	3
14	10	3	3	9	8	14	6	2	11	1	2	13	14	8	4
15	12	10	9	1	3	10	3	8	7	15	4	9	2	5	15

Thm: In a random matrix, *every* small window is "rich": have many different entries.

Pseudorandom Property

rich: Eg $k \times k$ windows to have $k^{1.1}$ distinct entries,

for $k \sim n^{0.1}$

Addition table

+	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

von Neumann: "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin."

1983 Erdos-Szemeredi, 2004 Bourgain-Katz-Tao:

Every … rich … one …

Independent-source extractors

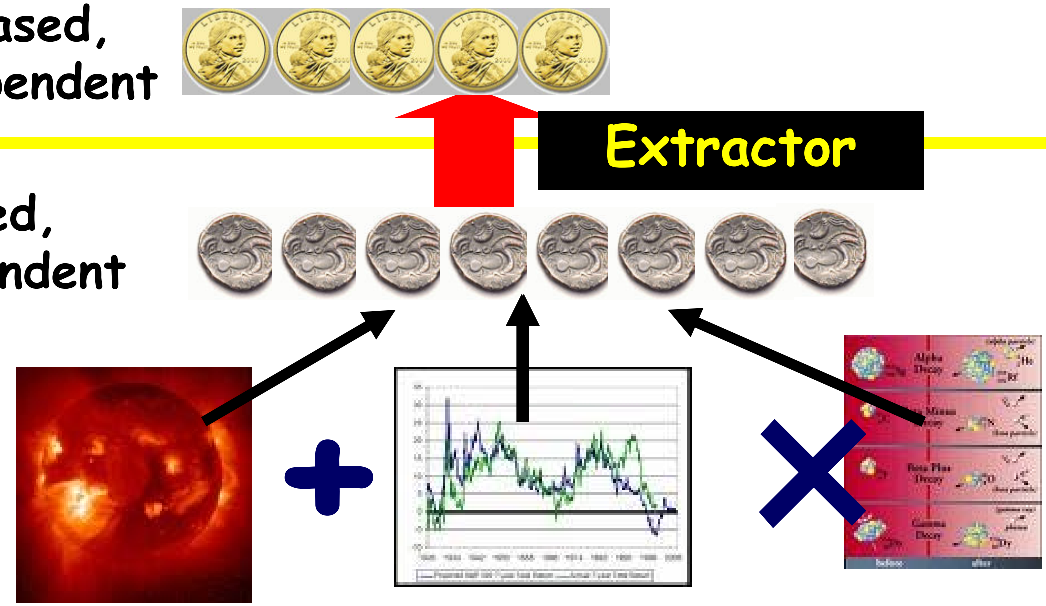
Applications:

Analyzed on perfect randomness

Statistics, Cryptography, Algorithms, Game theory, Gambling,……

Unbiased, independent

biased, dependent



Sun spots

Stock market fluctuations

Radioactive decay

Reality:

Independent weak sources of randomness

Theorem [Barak-Impagliazzo-W '05]:

Extractor for independent sources

Summary

- **Randomness** is in the eye of the beholder:
  A pragmatic, subjective definition

- **Pseudorandomness** "tests" ←→ "applications"
  Capture many basic problems and areas in Math & CS

- **Applications** of randomness survive in a world without
  perfect (or any) randomness

- **Pseudorandom** objects often find uses beyond their
  intended application (expanders, extractors,…)

Thank you!


The best throw of
a die is to throw
the die away
Lucky Numbers: 5, 22, 23, 4, 33, 17

Single-source extractors

input → algorithm A → output correct with high probability

n unbiased, independent

input → algorithm A → ~~output correct with high probability??~~

n biased, dependent

Naïve implementation fails!

Reality: one weak random source (all randomness correlated)

Single-source extractors

Probabilistic algorithms with 1 weak random source

input → **algorithm A**

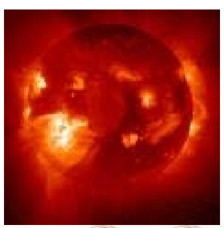
n unbiased, independent

Many other applications:
- Hardness of approx
- Derandomization,
- Data structures
- Error correction
- Certifying randomness

input → **Algorithm A'**

Run A on each, and take a majority vote

→ correct whp!!



n^3 biased, dependent entropy n^2

↓

Extractor →

Bl, SV, NZ,
………….
Ta, Tr, ISW,
………….
LRVW, GUV
Dv, DW,…

Deterministic de-randomization

Hardness vs. Randomness

input → *Efficient* algorithm A → output correct with high probability

n unbiased, independent

All efficient probabilistic algorithms have efficient deterministic counterparts

input → *Ef*

Run A on ea
take a majority vote

ways!

Reality: Universe is deterministic

"P ≠ NP": TSP is hard

0010001 1111101
11 0111110
11 10
00 01
0101101 1000001

A perfect sample

BM, Y, …
…………
NW, IW,…
…………
IKW, KI,...