高级算法设计与分析

- 任课教师：孙晓明，蔡少伟，夏盟佶，田国敬

- 时间安排：
  - 第1-5周：孙晓明
  - 第6-10周：蔡少伟
  - 第11-15周：夏盟佶
  - 第16-19周：田国敬

Randomized Algorithm

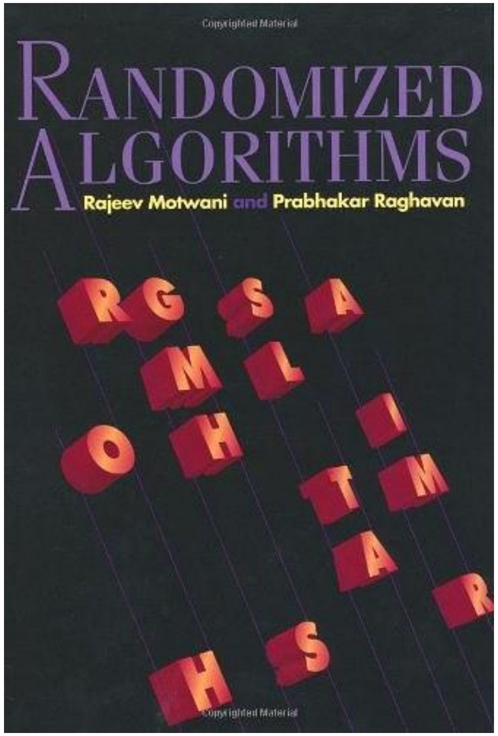
孙晓明

中国科学院计算技术研究所

sunxiaoming@ict.ac.cn

2022-2-21

- Rajeev Motwani, Probhakar Raghavan. 《Randomized Algorithms》
  - 第1, 3, 4, 7, 14章



1. Probability

Birthday Paradox

2022 寅

1月

26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

2月

30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5

3月

27	28	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

4月

27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

5月

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

6月

29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2

7月

26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

8月

31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3

9月

28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1

10月

25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

11月

30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

12月

27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

$N = 23$, Pr > 0.5

- N=23,
  Pr(有**两人**同一天生日)
  =1-(1-1/365)(1-2/365)…(1-22/365)=0.507297

10	20	23	30	50	57	80
11.7%	41.1%	50.7%	70.6%	97%	99%	>99.9 %

- N=88,
  Pr(有**三人**同一天生日) > 0.5

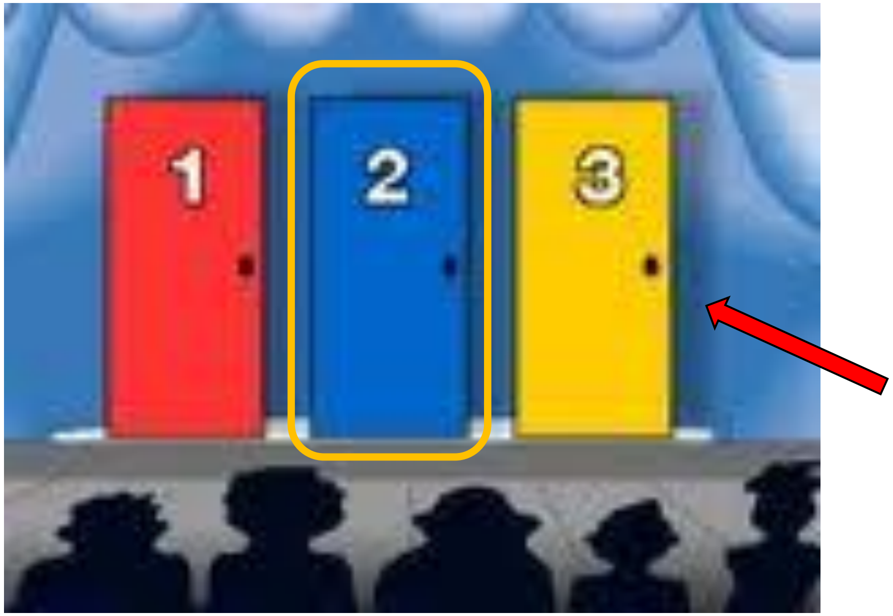
Two envelopes problem

要不要换？

½*250+½*1000=**625**

Monty Hall Problem

要不要换？

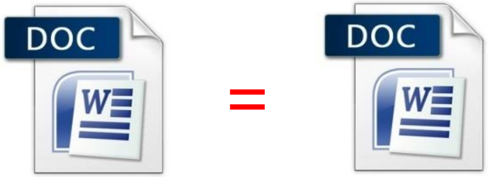


1/2? 2/3?

2. The Power of Randomized Algorithms

Equality Test

$x = y?$



Cloud storage: Dropbox, icloud…

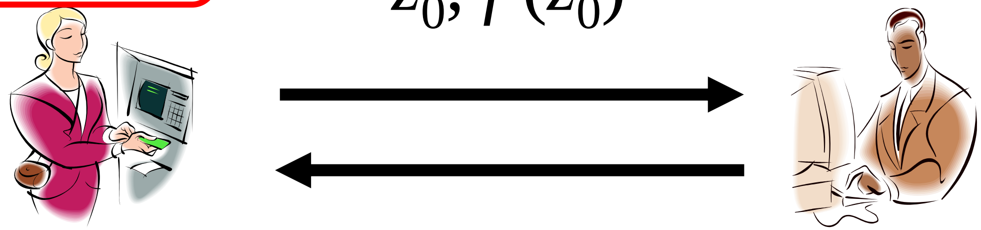
Deterministic alg: $\Theta(n)$

Randomized alg: $\Theta(\log n)$

Randomized protocols

- $f(z) = x_0 + x_1 z + \ldots + x_n z^n$
- $g(z) = y_0 + y_1 z + \ldots + y_n z^n$

$z \in \mathrm{F}_p \, (n^2 \leq p < 2n^2)$



$z_0, f(z_0)$

$\mathrm{I}_{[g(z_0)=f(z_0)]}$

$x \in \{0,1\}^n$ $y \in \{0,1\}^n$

Error

$= \Pr (f(z_0) = g(z_0) \mid x \neq y)$

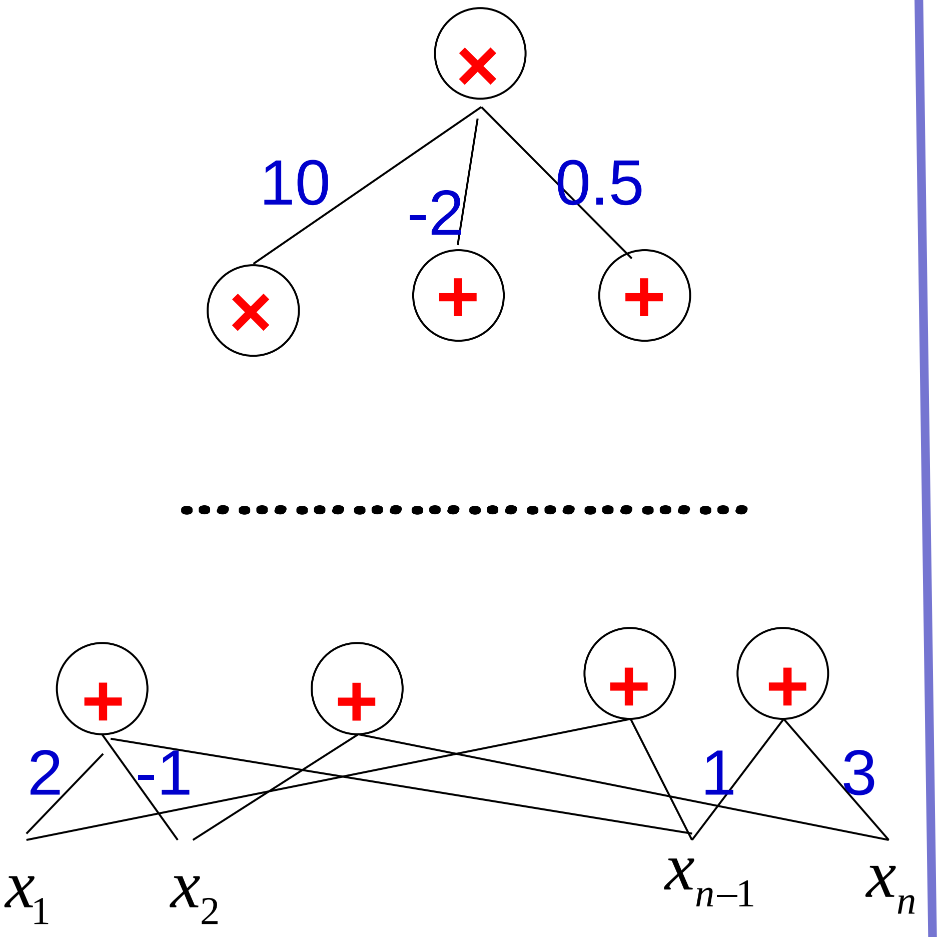
$= \Pr (z_0 \text{ is a root of } f(z)\text{-g}(z) = 0)$

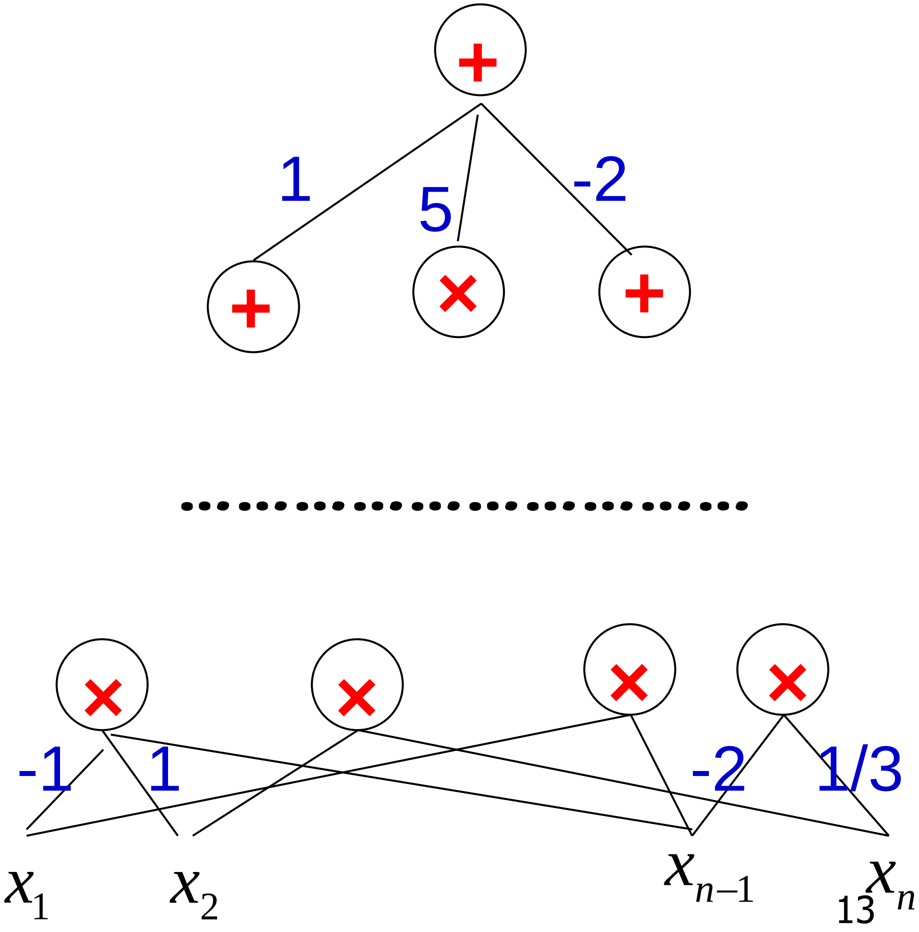
$= \Pr (z_0 \text{ is a root of } c_0 + c_1 z + \ldots + c_n z^n = 0 \bmod p)$

$(c_i = x_i - y_i)$

$$\leq \frac{n}{p} \leq \frac{1}{n}$$

Polynomial Identity Testing





Polynomial Identity Testing(2)

- $f(x) = (2x_1 - x_2)(x_3 - x_4 + 1) \dots (x_{n-1} - 2x_n) + \cdots$
- $g(x) = (x_1 + x_3)(x_2 - x_4 + x_7) \dots (x_{n-3} + 2x_{n-4} - x_n) + \cdots$

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2)$$
$$= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2$$
$$+(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2$$

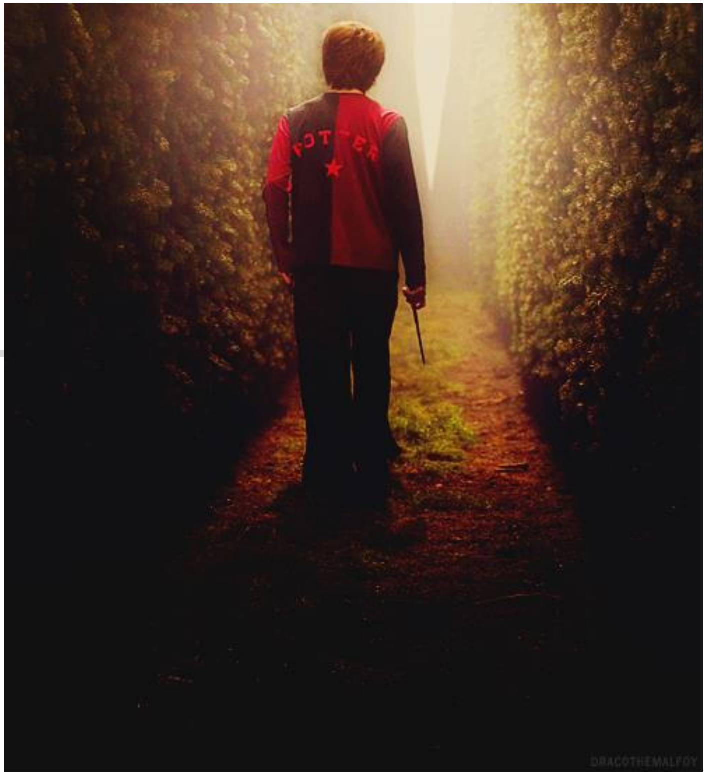
$$(x + y + z)^7 - (x^7 + y^7 + z^7)$$
$$= 7(x + y)(y + z)(z + x)[(x^2 + y^2 + z^2 + xy + yz + zx)^2$$
$$+ xyz(x + y + z)]$$

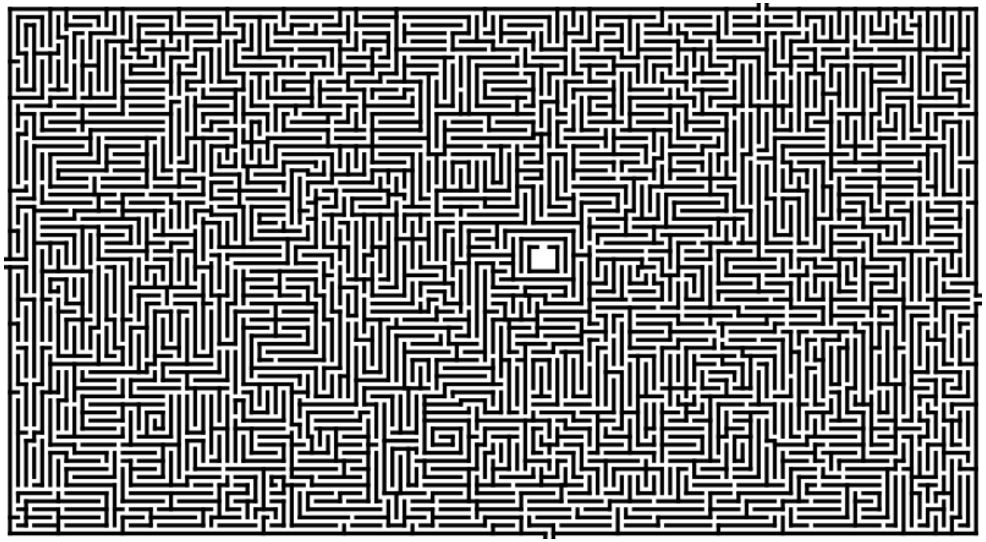
Schwartz–Zippel lemma

- Let $\mathrm{P}(x_1,x_2,\ldots,x_n)$ be a polynomial of degree d over a field F. Let S be a finite subset of F and let $r_1, r_2, \ldots, r_n$ be selected randomly from S, then

$$\mathbf{Pr}\ (\mathrm{P}(r_1,r_2,\ldots, r_n) = 0) \leq \boldsymbol{d} \,/\, |\mathbf{S}|$$

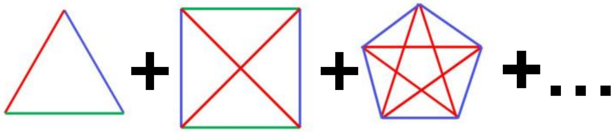
Maze





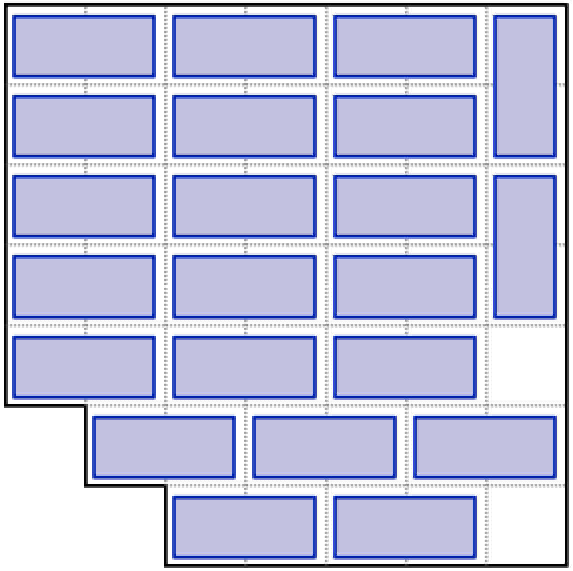
w.h.p. random walk with $O(n^2)$ steps will visit **every** corner

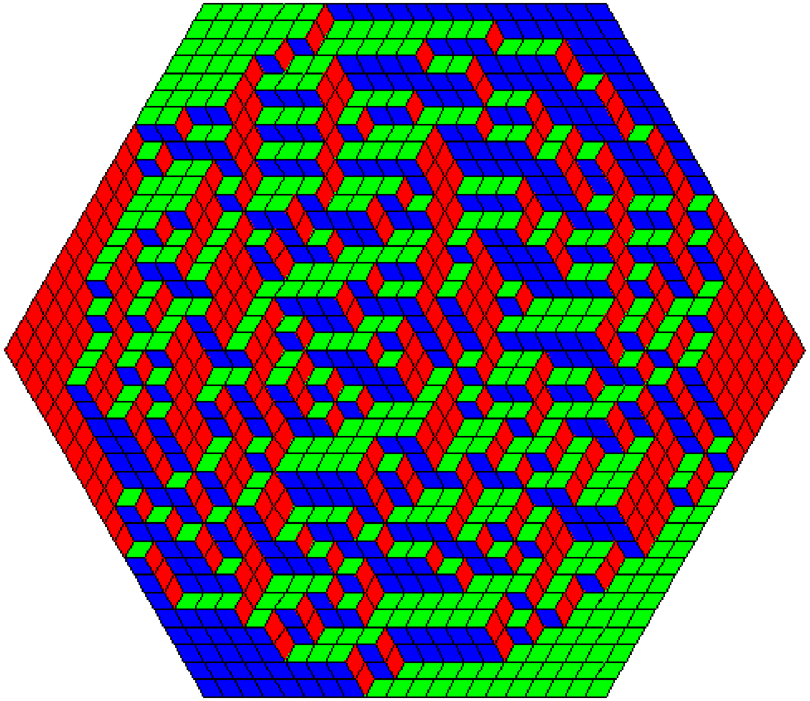
Counting



Counting(2)

- Domino tiling





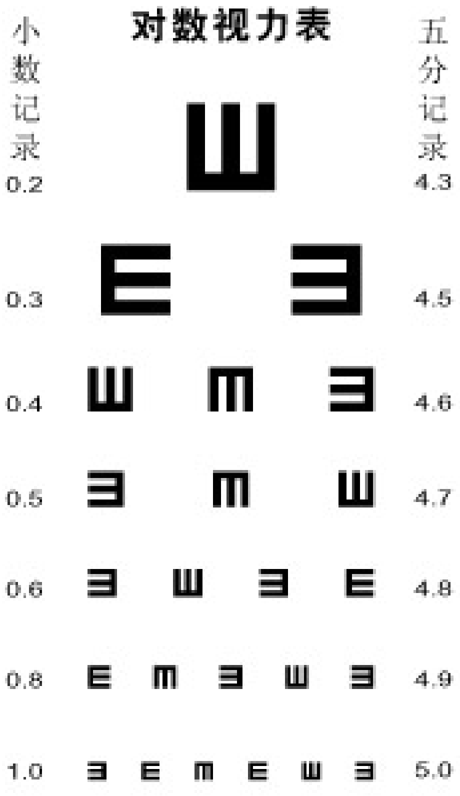
Markov-Chain Monte-Carlo Method

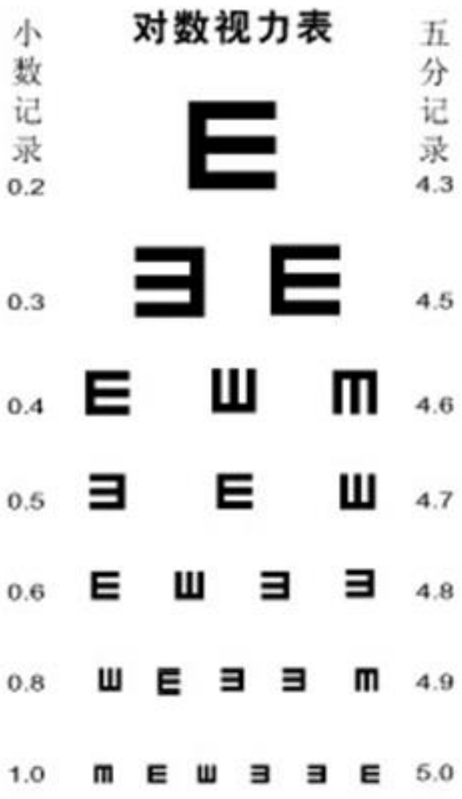
Zero Knowledge

- 2012 Turing Awards: Goldwasser, Micali

Goldwasser and Micali’s work helped make cryptography a precise science. The mathematical structures they created, including formal notions of privacy, adversaries, **pseudorandomness, interactive proofs, zero-knowledge proof,** and …, set cryptography on rigorous foundations of the highest standards …

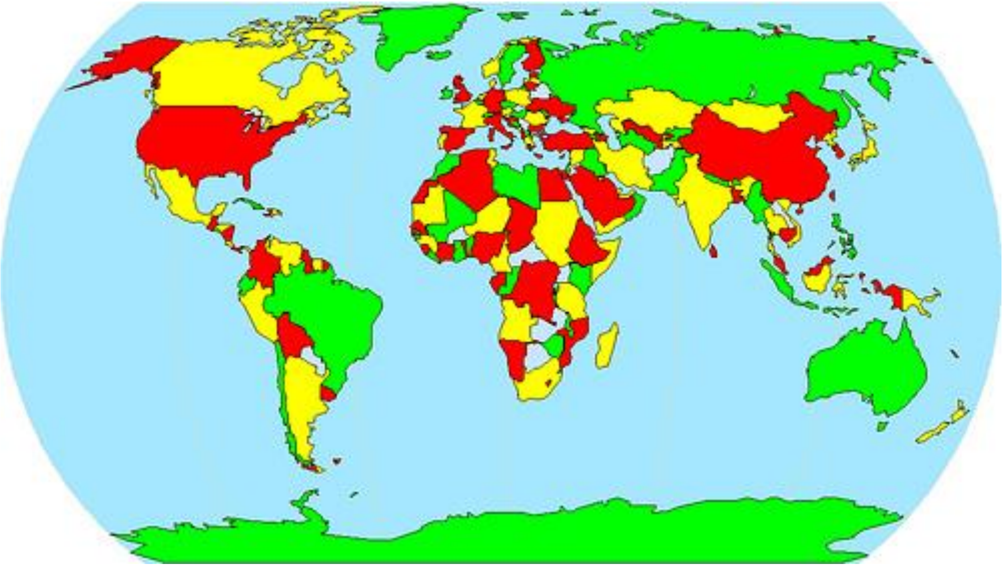
Zero Knowledge(2)



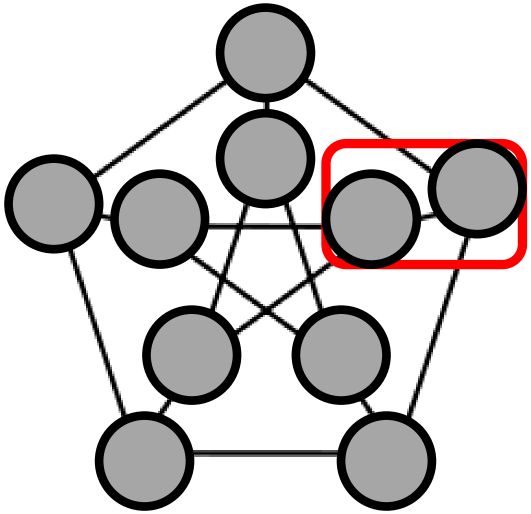


Zero Knowledge(3)

- 4-coloring



3-coloring?



3. Pseudorandomness (Limitation of Randomized Algorithms)

Panasonic

HDV
SONY
HDV

Canon

TH
TH

- Pi = 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
0

Every digit (e.g. 7) occurs **1/10** of the time

Every pair (e.g. 99) occurs **1/100** of the time

Every triple (eg 666) occurs **1/1000** of the time…

(Conjectured)

2

3344685035 2619311881 7101000313 7838752886 5875332083 8142061717
7669147303 5982534904 2875546873 1159562863 8823537875 9375195778
1857780532 1712268066 1300192787 6611195909 2164201989 ......

Prime number looks random

- Copeland–Erdős constant:

  0.2357111317192329313741434753596167… is normal

- Green-Tao Theorem:

  5, 11, 17, 23, 29

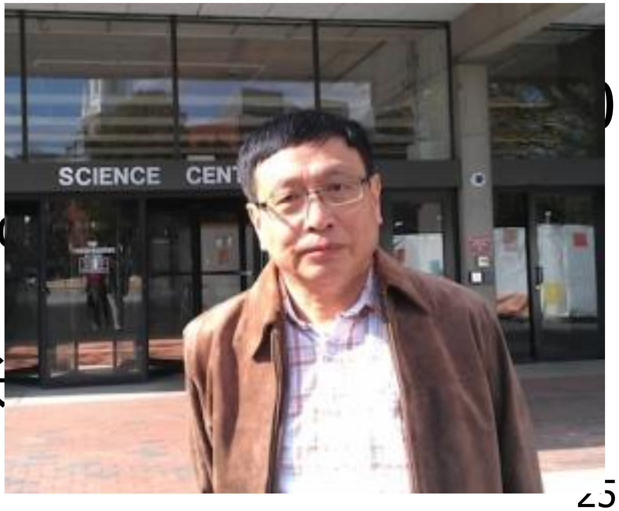
  the sequence of prime numbers contains arbitrarily long arithmetic progressions

- Twins Prime Conjecture:

  There are infinitely many primes p suc

  prime

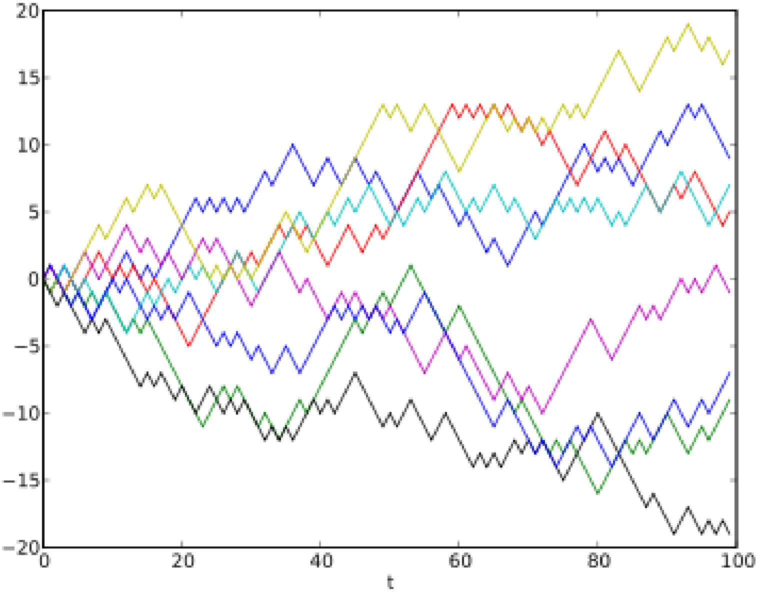
  - Weaker Twins Prime Theorem (张



Riemann Hypothesis

- Pr(↑) = Pr(↓) = 1/2

$$|\sum_{i=1}^{N} x_i| \approx \sqrt{N}$$

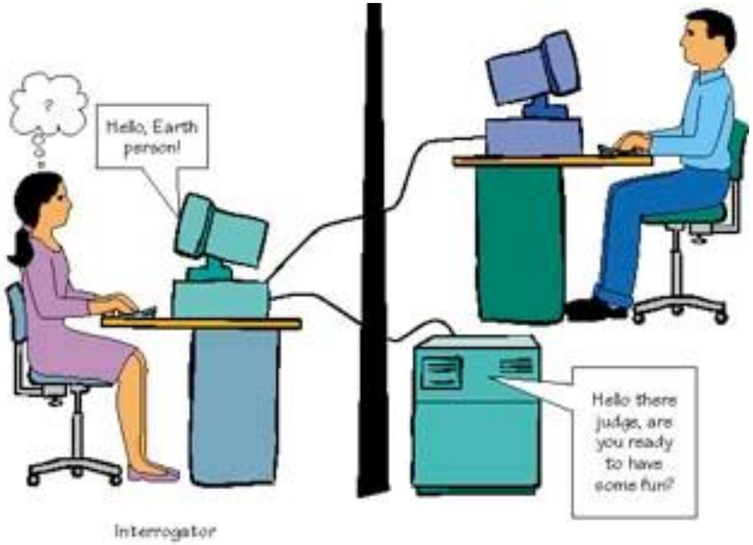


- Mertens Theorem:
  - Riemann Hypothesis
  - $|\sum_{x \le N} \mu(x)| \approx \sqrt{N}$

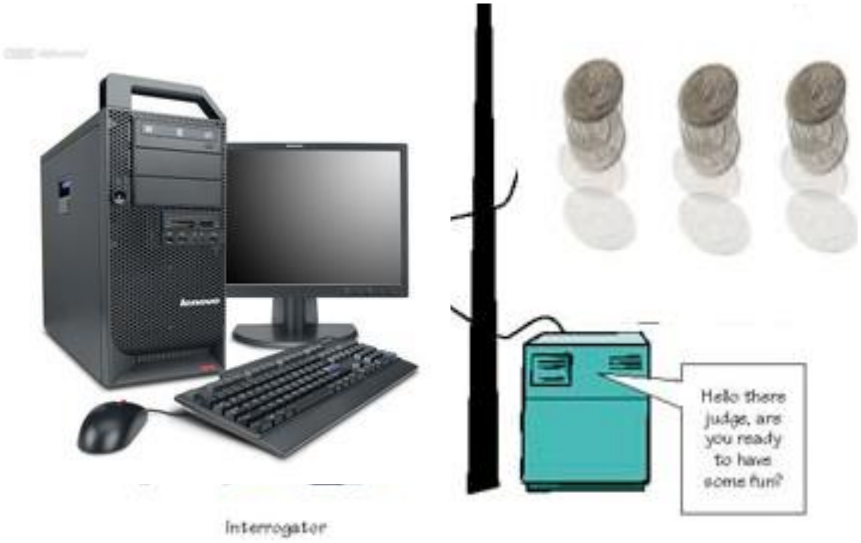
($\mu()$: Möbius function)

are **equivalent** !!

Turing Test


?
Hello, Earth person!
Hello there judge, are you ready to have some fun?
Interrogator

Pseudorandom Generators



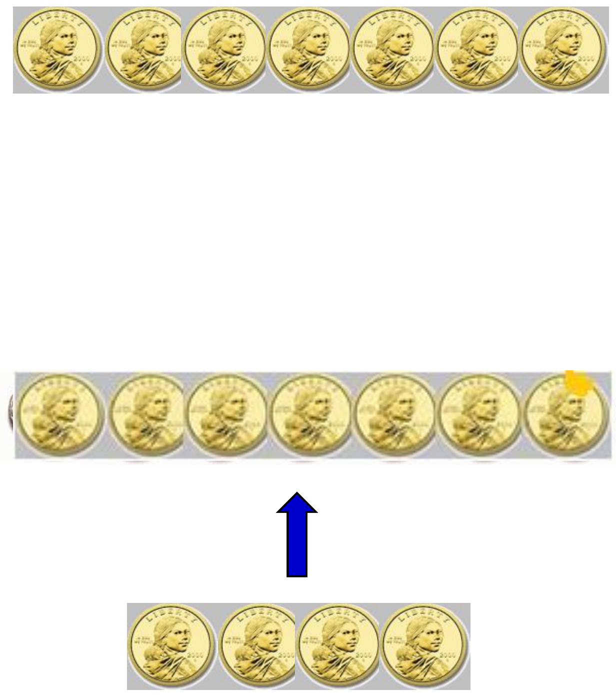
polynomial time alg. A

polynomial time alg. A

perfect coins

$(1/2+1/2^n)$-coins

polynomial time alg. A



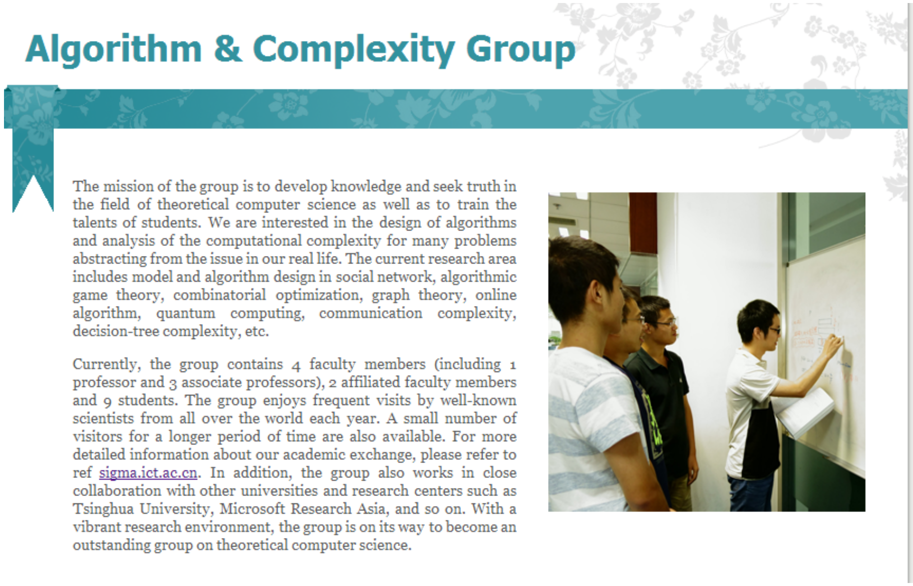
- If #random coins = $O(\log n)$

  ➡ Polynomial time

- [Impagliazzo, Wigderson] **P = BPP** if E requires **exponential** circuits
  - derandomization

计算所量子计算与算法理论实验室

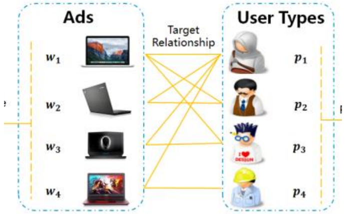
http://theory.ict.ac.cn



Algorithm & Complexity Group

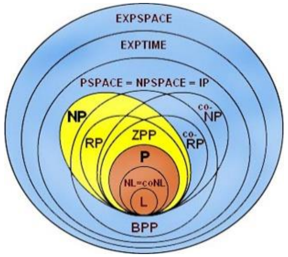
The mission of the group is to develop knowledge and seek truth in the field of theoretical computer science as well as to train the talents of students. We are interested in the design of algorithms and analysis of the computational complexity for many problems abstracting from the issue in our real life. The current research area includes model and algorithm design in social network, algorithmic game theory, combinatorial optimization, graph theory, online algorithm, quantum computing, communication complexity, decision-tree complexity, etc.

Currently, the group contains 4 faculty members (including 1 professor and 3 associate professors), 2 affiliated faculty members and 9 students. The group enjoys frequent visits by well-known scientists from all over the world each year. A small number of visitors for a longer period of time are also available. For more detailed information about our academic exchange, please refer to ref sigma.ict.ac.cn. In addition, the group also works in close collaboration with other universities and research centers such as Tsinghua University, Microsoft Research Asia, and so on. With a vibrant research environment, the group is on its way to become an outstanding group on theoretical computer science.

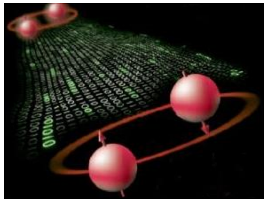


online algorithms

social networks



complexity



quantum computing

game theory

谢谢！