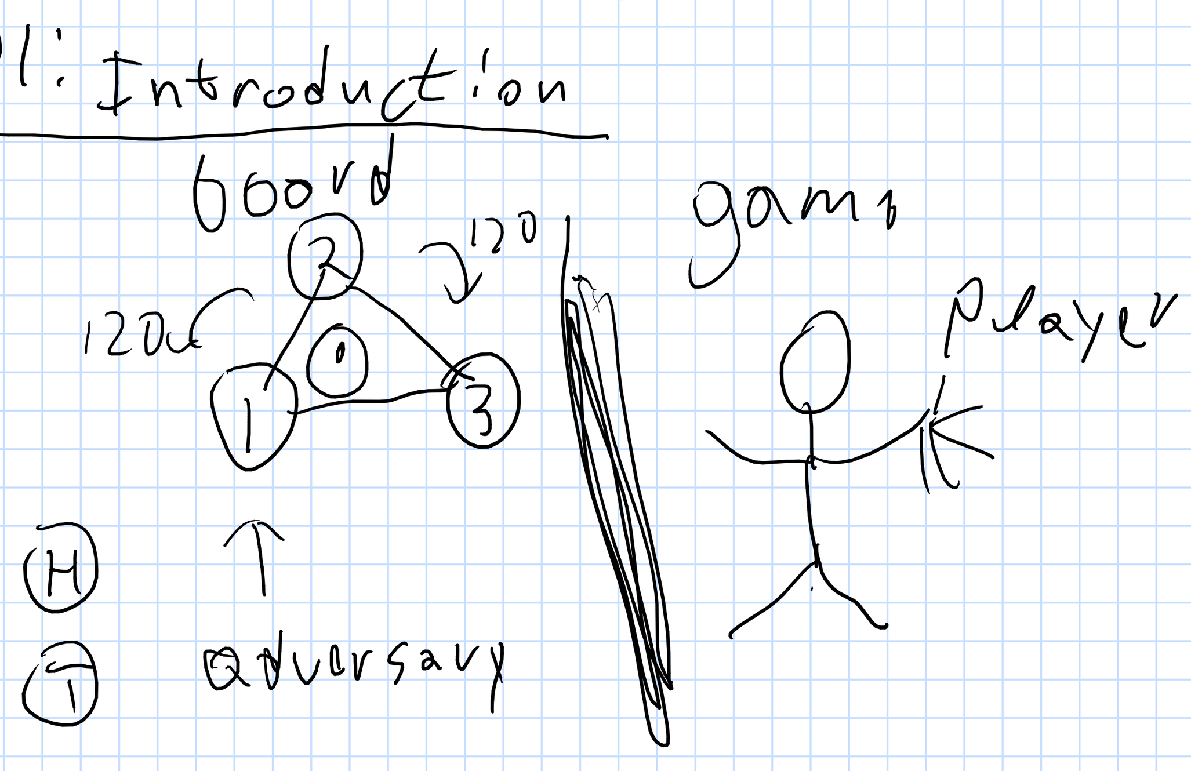
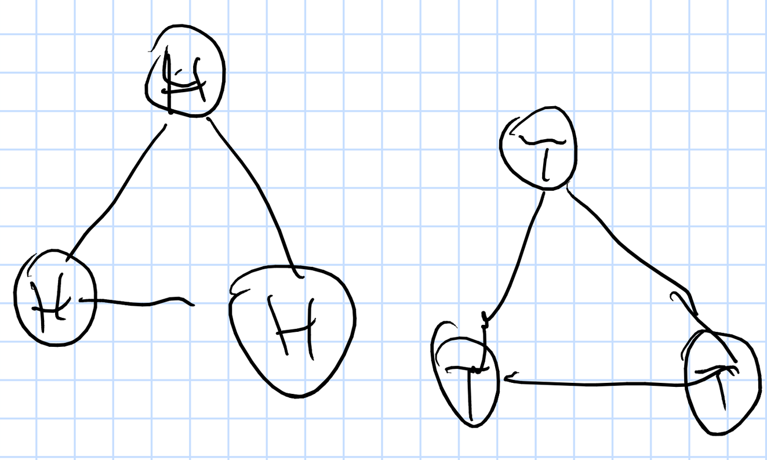
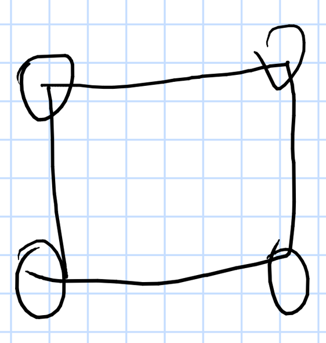
Randomized Algorithms — 11/18/22

L01: Introduction







Deterministic strategy

0	1	1		0	0	1
1	0	1		0	1	0
1	1	0		1	0	0

$\frac{1}{3}$ $\frac{2}{3}$

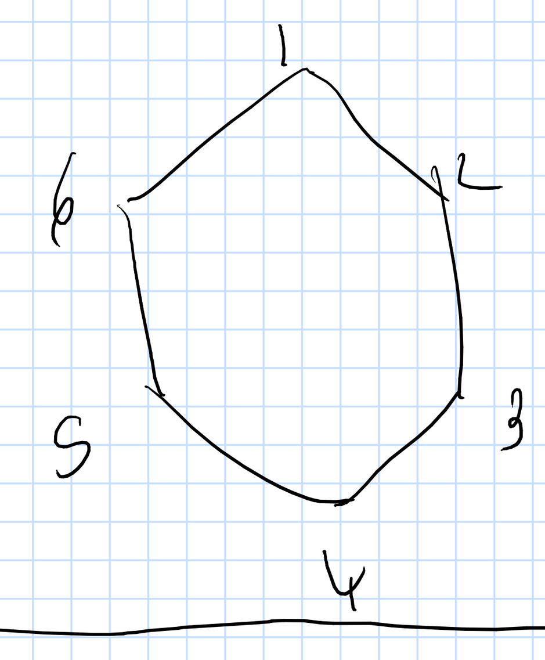
Geometric variable $\frac{1}{3}$ $\boxed{3}$

$$\left(1-\frac{1}{3}\right)^i \le \exp\left(-\frac{1}{3}\right)^i = \exp\left(-\frac{i}{3}\right) = \frac{1}{e^{i/3}}$$

$$1 - x \le \exp(-x) \qquad x \ge 0$$

Worst case analysis

2SAT



2SAT $x_1, x_2, \ldots x_n$

F:

$(x_1 \vee x_2) \wedge (x_7 \vee \bar{x}_{16}) \ldots$ — n # variables, m clauses

Q: Compute a satisfying assignment.

$O(n+m)$: SCC

$x_1 = 0, x_2 = 0, \ldots x_n = 0$

$F(x_1, \ldots x_n) = \ldots \wedge (\bar{x}_i \wedge x_j)$

Flip the value of x_i.

Thm In expectation the randomized alg executes $O(n^2)$ iterations.

3SAT NP Complete.

$(x_i \vee x_j \vee x_k)$

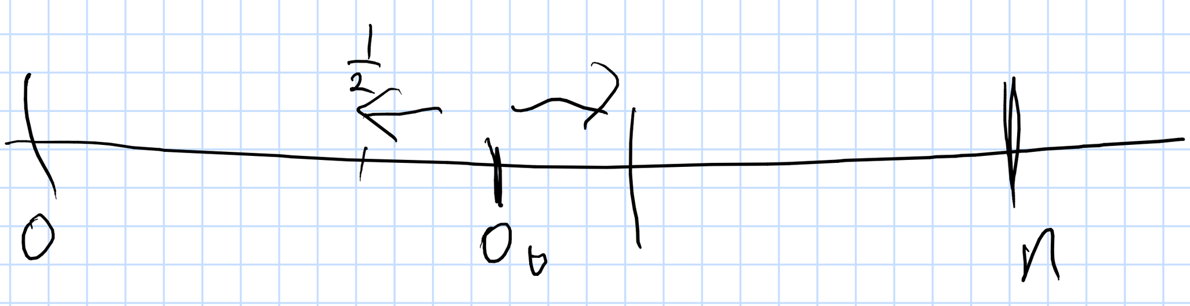
$(x \vee y)$

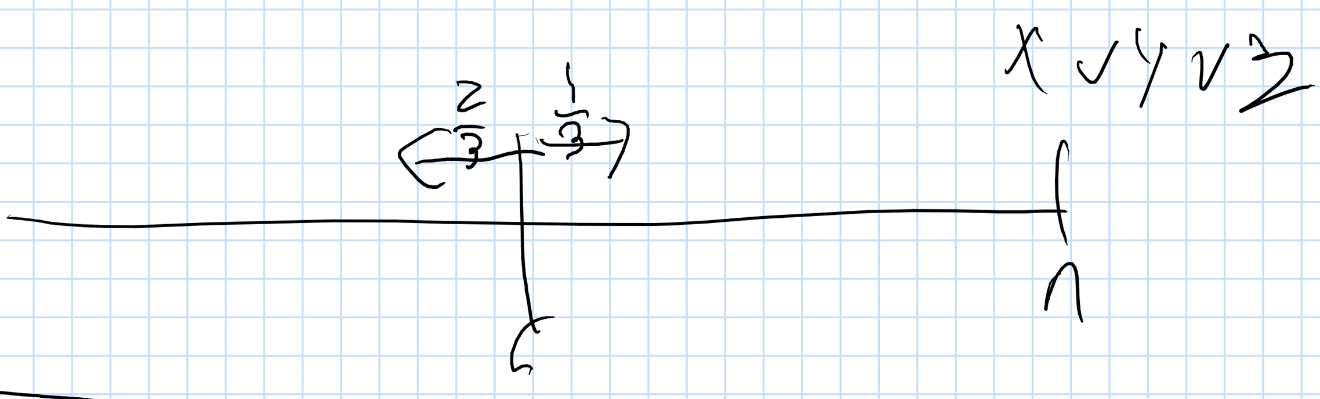
$O_i \equiv$ # of variables in the assignment at time i which agrees with the satisfying assignment.

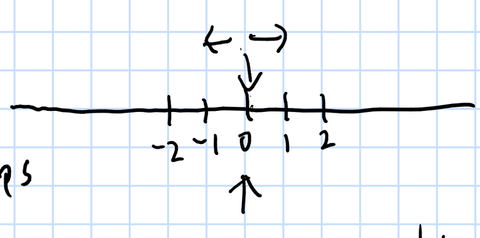
$O_i = n$

$|O_i - O_{i+1}| = 1$

Random walk







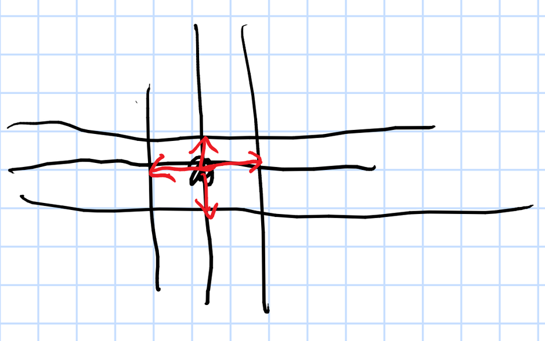
2n steps

many times did you visit the origin?

$$\frac{\binom{2n}{n}}{2^n} \approx \frac{1}{\sqrt{n}}$$

$$\binom{2n}{n} \approx \Theta\left(\frac{2^n}{\sqrt{n}}\right) \qquad \frac{\binom{2n}{n}}{2^n} \approx \sum_{n=1}^{\infty} \frac{1}{\sqrt{n}} = \infty$$

$$\sum_{n=1}^{\infty} \frac{1}{n} = \infty$$



RSA and primality testing

p, q: Compute two large random prime number

n = pq: public key

Factoring: How to do efficiently?

Fact 1

There are $\Theta\left(\frac{n}{\log n}\right)$ prime number between 1 and n.

Testing primality

197? Rabin

x ⟹ (Randomized algorithm)
- prime — wrong with probability half.
- not prime — always correct.

t digits in base 2

primality testing 10t times

$$\frac{1}{2^{10t}}$$

$O(\log^3 n)$

Motwani and Raghavan ⟵
