

19 IP = PSPACE, Average-P

IP = PSPACE

given:

QBF build IP-system

Idea: Arithmetization φ

of $\exists_{\vec{a}_1} x_1 \forall_{\vec{a}_2} x_2 \exists x_2 \forall x_3 (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3)$

$\Rightarrow F; f() \Rightarrow f(x_1) \Rightarrow f(x_1, x_2) \dots$

$f(x_1, \dots, x_n) = \varphi(x_1, \dots, x_n)$

19 IP = PSPACE, Average-P

P

 coefficients of

 P_1, P_2

 $P_1(v) = P_2(v)$

 error probability

 $\leq \frac{\text{degree of } p!}{P}$

V

 random

 $v \in \mathbb{Z}_P$

 check whether

 $P_1(v) = P_2(v)$

$q = \underbrace{(x_1 \vee \bar{x}_2)}_{C_1} \wedge \underbrace{(x_2 \vee \bar{x}_3)}_{C_2}$

$F(x_1, x_2, \dots, x_n) = \prod_{C_1, \dots, C_m} \left(1 - \prod_{x_i \in C_j} (1 - \{x_i, 1-x_i\}) \right)$

$F(b_1, b_2, \dots, b_n) = q(b_1, b_2, \dots, b_n) \mid b_i \in \{0, 1\}$

19 IP = PSPACE, Average-P

$$f_0() = Q_1 x_1 \dots Q_n x_n \psi(x_1 \dots x_n)$$

$$f_i(x_1 \dots x_i) = Q_{i+1} x_{i+1} \dots Q_n x_n \psi(x_1 \dots x_n)$$

$$Q_{i+1} = \text{"}\forall\text{"} \quad f_i(x_1 \dots x_i) = \prod_{b \in \{0,1\}} f_{i+1}(x_1 \dots x_i, b)$$

$$Q_{i+1} = \text{"}\exists\text{"} : f_i(x_1 \dots x_i) = 1 - \prod_{b \in \{0,1\}} (1 - f_{i+1}(x_1 \dots x_i, b))$$

19 IP = PSPACE, Average-P

What is the degree of f_n ?

$$\left(\left((x^m)^2 \right)^2 \right)^2$$

degree of F is at least m .

degree of f_{n-1} is at least $2m$

degree of $f_{n-2} \leq 2^2 m$

$f_{n-3} \leq 2^3 m$

$f_1 \leq 2^n m$

$$p \geq 2^n m \cdot n$$

p is prime

How to find such a prime?

New Gadget : Degree Reducer

$$R_x \quad f'(x_1, x_2, \dots, x_n, x) = (1-x) \cdot f(x_1, \dots, x_n, 0)$$

$$+ x \cdot f(x_1, \dots, x_n, 1)$$

$$x=0 : f'(x_1, \dots, x_n, x) = f(x_1, \dots, x_n, 0) \quad \checkmark$$

$$x=1 : f'(x_1, \dots, x_n, x) = f(x_1, \dots, x_n, 1) \quad \checkmark$$

\Rightarrow correct arithmetization! \checkmark

Properties of $R_{x,f}(x_1, \dots, x_n, x)$

- Same for $x_1, \dots, x_n \in \mathbb{Z}_p, x \in \{0, 1\}$
- degree in x is ≤ 1
- degree in x_i for constant $\{x_1, \dots, x_n, x\} \setminus \{x_i\}$ is the same
- There exists a IP to show correctness.

19 IP = PSPACE, Average-P

$$\exists x_1 \forall x_2 \exists x_3 \underbrace{(x_1 \vee \bar{x}_2) \wedge (x_1 \vee x_3)}_{F(x)}$$

$$Q_{x_1} R_{x_2} Q_{x_3} \dots Q_{x_{n-1}} R_{x_n} \dots R_{x_{n-1}} Q_{x_n} R_{x_1} R_{x_2} \dots R_{x_n} F(x_1, \dots, x_n)$$

$\{ \exists, \forall \}$

$$S_{x_1} S_{x_2} S_{x_3} \dots S_{x_n} F(x_1, \dots, x_n)$$

$$S \in \{ \forall, \exists, R \} \rightarrow \text{depth is at most } \underline{m}$$



Average-P and Dis-NP

Graph-Coloring is NP-complete
- for 3 colors

given undir. graph $G = (V, E)$, $c \in \mathbb{N}$

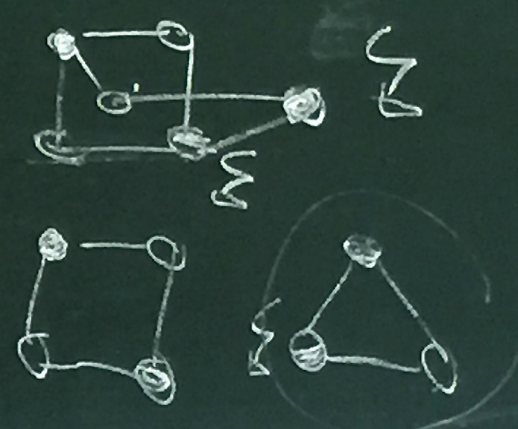
$\exists f: V \rightarrow \{1, 2, \dots, c\}$

$\{u, v\} \in E \Rightarrow f(u) \neq f(v)$

19 IP = PSPACE, Average-P

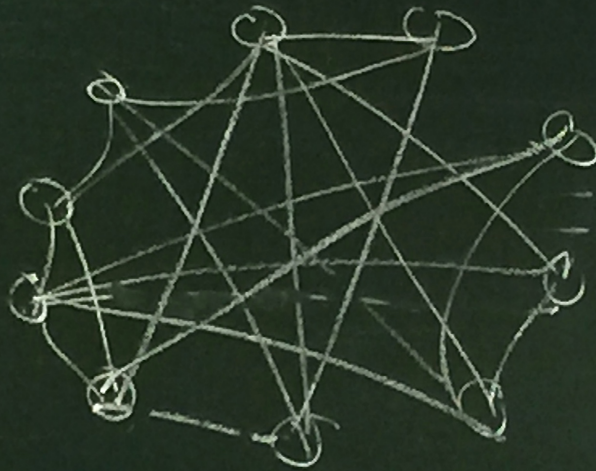
$c=1$ color $\begin{matrix} 1 & 1 & \checkmark \\ \cdot & \cdot & \\ \swarrow & \searrow & \\ 1 & 1 & \\ \swarrow & \searrow & \\ \cdot & \cdot & \end{matrix}$

$c=2$ Black: \bullet
 White: \circ



19 IP = PSPACE, Average-P

$C = 3$ NP-complete

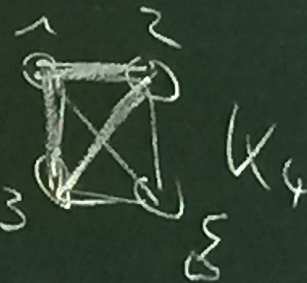


practical.

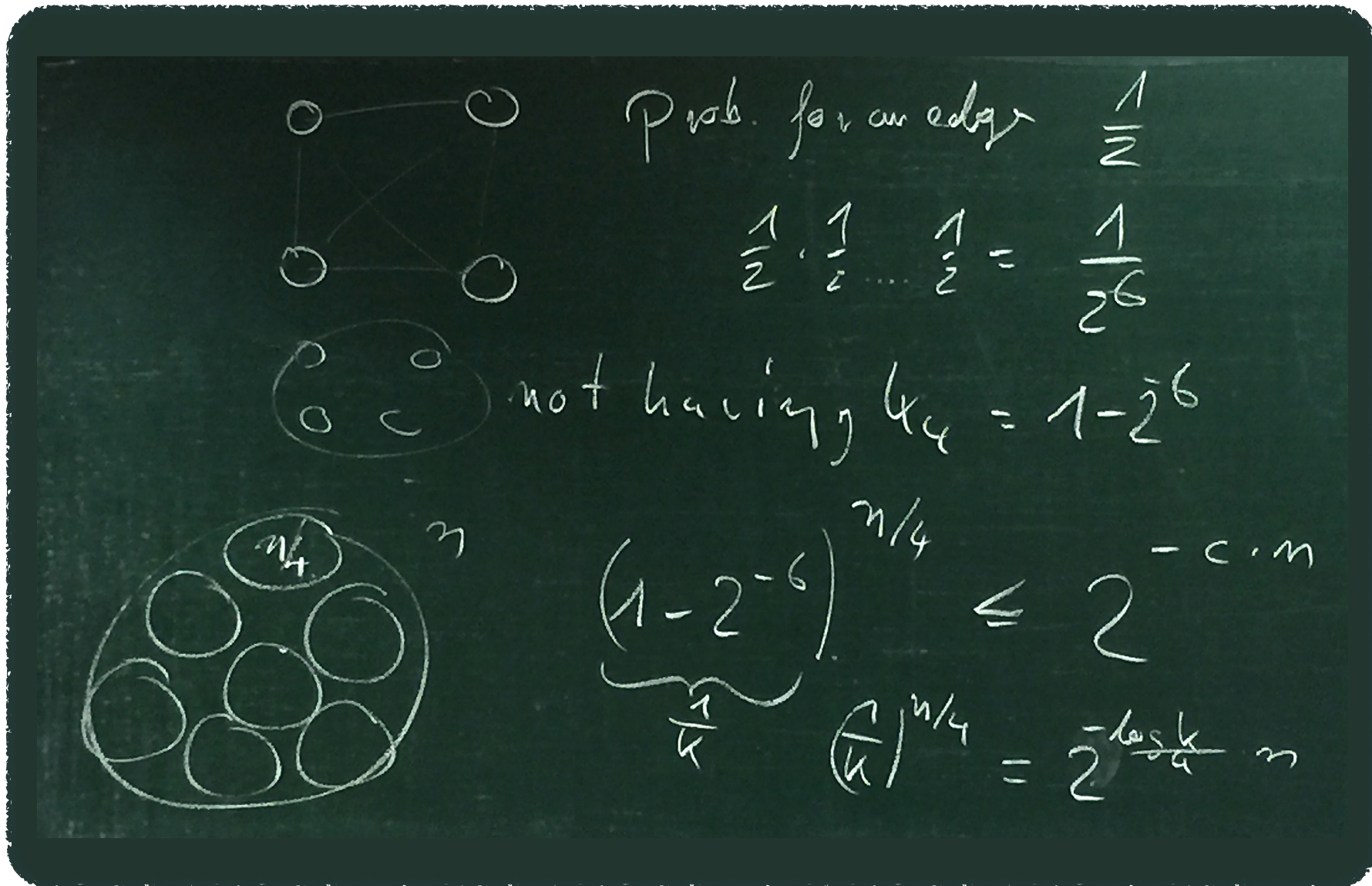
each edge has prob. $1/2$

1. Find K_4 in G

$$n^2 \cdot n \cdot n = O(n^4)$$



19 IP = PSPACE, Average-P



Prob. for an edge $\frac{1}{2}$

$\frac{1}{2} \cdot \frac{1}{2} \dots \frac{1}{2} = \frac{1}{2^6}$

not having $k_4 = 1 - 2^{-6}$

$\binom{n}{k}^{n/4} \leq 2^{c \cdot n}$

$\binom{n}{k}^{n/4} = 2^{-\frac{\log k}{24} n}$

Diagrams:

- A graph with 4 nodes and 6 edges.
- A set of 4 nodes with one node circled.
- A large circle containing 6 smaller circles, with one small circle circled.

19 IP = PSPACE, Average-P

$$2^{-cm} \cdot 2^{c'n} + \underbrace{(1 - 2^{-cm})}_{\leq 1} \cdot n^4 = E(\text{time}(G))$$

$c' < c$
 $\underbrace{c' - c}_{< 0}$
 $2^{(c' - c)n} + n^4$
 run-time for some alg
 solver 3-COLOR

$2^{(c' - c)n} + n^4$
 Hamiltonian Cycles

Theorem [Goldberg 79]
 A random SAT-formula with
 n -variables, m clauses
 can be solved in time $O(m n^2)$
 expected

19 IP = PSPACE, Average-P

Davis-Putnam-Alg ($\phi \in \text{CNF}$)

if Φ is empty then return 1

else if \exists empty clause then return 0

else if \exists clause with only one literal x_i (\bar{x}_i)
 then $x_i = 1$ (0)

DP(ϕ with $x_i = 1$)⁽⁰⁾

else if x_i never occurs ^(advant) _{negated}

then $x_i = 1$ (0)

DP(ϕ with $x_i = 1$)⁽⁰⁾

else choose x_i from ϕ

if $\text{DP}(\phi, x_i = 1) = 1$ then return 1

if $\text{DP}(\phi, x_i = 0) = 1$ then return 1

else return 0

$f_i \neq i$

Is SAT easy?

$\exists x_1 \exists x_2 \exists x_3 (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3)$

literal
 ↓
 clause

n : # of variables

m : # of clauses

k : # of literals in a clause

19 IP = PSPACE, Average-P

