

Today  
 - Alg  
 - kSAT  
 - Hitting Set  
 = OV

## Sat of Boolean Formulas

$\wedge \vee \neg \neg$   
 Def. (SAT)

Input: Bool. Formula  $\varphi$

Task: Decide if there is assignment to variables of  $\varphi$  st  $\varphi$  evaluates to true

$N$ : # variables

CNF-SAT:  $\varphi = C_1 \wedge C_2 \wedge \dots \wedge C_M$

$C_i = l_{i1} \vee l_{i2} \vee \dots \vee l_{ik_i}$

$l_{ij} = x$  or  $l_{ij} = \bar{x}$  for some var.  $x$

**K-SAT**.  $C_i = l_{i1} \vee \dots \vee l_{ik}$

$(a \vee b \vee \bar{c}) \wedge (\bar{a} \vee \bar{b} \vee d) \wedge (\bar{a} \vee c \vee d)$

Observation:  $SETH \Rightarrow ETH \Rightarrow P \neq NP$

Fastest known alg. (Baseline  $2^N \cdot \text{poly}(M, N)$ )

2-SAT:  $O(M+N)$

3-SAT:  $1.31^N \cdot \text{poly}(M, N)$

4-SAT:  $1.47^N \cdot \text{poly}(M, N)$

[Paturi et al '98]

k-SAT:  $2^{N(1-\epsilon/k)} \cdot \text{poly}(M, N)$  for some constant  $\epsilon$

CNF-SAT:  $2^{(1-\theta(N \log(M/N)))N} \cdot \text{poly}(M, N)$  [Galbraith et al '06]

Conjecture [Impagliazzo/Paturi]: [Exponential Time Hypothesis]

$\forall k \geq 3, \exists$  constant  $c_k$  st. no  $2^{c_k N} \cdot \text{poly}(M, N)$ -time algorithm for k-SAT

( $\Rightarrow$  No  $2^{o(N)}$ -alg. for 3-SAT) (No  $2^{o(N)}$ -time)

Conjecture [I/P] Strong Exp Time Hyp. (SETH)

For  $s > 0, \exists k$  st. no  $2^{(1-s)N} \cdot \text{poly}$ -time for k-SAT

( $\Rightarrow$  no  $2^{(1-s)N} \cdot \text{poly}(M, N)$ -time algorithm for CNF-SAT (for any  $s > 0$ ))

param.  $k$   
 $f(k) \cdot \text{poly}(n)$   
 $\uparrow$   
 $k^k$

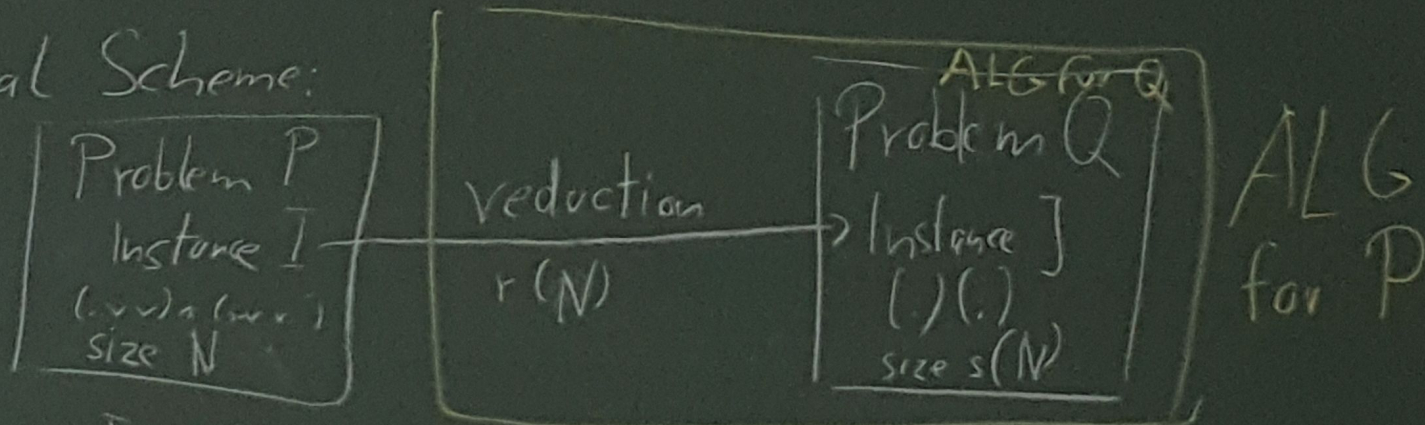
# From CNF-SAT to Orthogonal Vectors

OV: Given  $A, B \subseteq \{0, 1\}^d$ , Q:  $\exists a \in A, b \in B$  s.t.  $a \perp b$

Def: Orthogonal Vectors Hypothesis (OVH)  
There is alg with running time  $n^{2-\epsilon}$  poly(d) for OV for any  $\epsilon > 0$

Theorem:  $SETH \Rightarrow OVH$

General Scheme:



$I$  is 'yes'-instance  $\Leftrightarrow J$  is a 'yes'-instance

Then  $t(n)$ -time alg for Q implies  
 $r(N) + t(s(N))$ -time alg for P

Or in other words If P has no  $r(N) + t(s(N))$ -time alg, then Q has no  $t(n)$ -time alg.

Today

- Alg 9
- kSAT
- Hitting Set
- OV

$$\varphi \rightarrow A, B \quad \varphi = C_1 \wedge \dots \wedge C_M$$

Variables of  $\varphi$ :  $x_1, x_2, \dots, x_N$

$\mathcal{U} = \{0, 1\}^{N/2}$  all possible truth value assignments to variables  $x_1, \dots, x_{N/2}$

$\mathcal{V} = \{0, 1\}^{N/2}$   $x_{N/2+1}, \dots, x_N$

Partial assignment satisfies clause  $C$  if

•  $\exists i$  st.  $x_i$  evaluates to 1 under ass  $u$  and  $x_i$  appears in  $C$

write:  $\text{sat}(u, C) = \begin{cases} 1 & \text{if } u \text{ sat } C \\ 0 & \text{o.w.} \end{cases}$

$$\text{unsa}(u, C) = 1 - \text{sat}(u, C)$$

$$A := \{(\text{unsa}(u, C_1), \dots, \text{unsa}(u, C_M)) \mid u \in \mathcal{U}\}$$

$$B := \{(\text{unsa}(v, C_1), \dots, \text{unsa}(v, C_M)) \mid v \in \mathcal{V}\}$$

Claim:  $\varphi \text{ sat.} \Leftrightarrow A, B \text{ has orth pair}$

Proof  $\Rightarrow$  Consider satisfying assignment  $w^*$  of  $\varphi$

Let  $u^*$  and  $v^*$  be partial assignments on

first  $N/2$  var. second  $N/2$  var. st.  $w^* = (u^*, v^*)$

Then for every clause  $C$ :

$u^* \text{ sat. } C$  or  $v^* \text{ sat. } C$

$$\Leftrightarrow \text{sat}(u^*, C) = 1 \text{ or } \text{sat}(v^*, C) = 1$$

$$\Leftrightarrow \text{unsa}(u^*, C) = 0 \text{ or } \text{unsa}(v^*, C) = 0$$

$\Rightarrow \exists$  vectors in  $A, B$  (corr to  $u^*$  and  $v^*$ ) that are orthogonal

Time complexity: size OV instance

$$|A| = |\mathcal{U}| = 2^{N/2} = |B| \quad d = M$$

Running for creating OV instance  $2^{N/2} \cdot M$

Conjecture [I/P] Strong Exp Time Hyp (SETH)

For  $\delta > 0$ ,  $\exists k$  st. no  $2^{(1-\delta)N}$  poly-time for  $k$ -SAT

$\Rightarrow$  no  $2^{(1-\delta)N}$  poly( $n, N$ )-time algorithm for CNF-SAT (for any  $\delta > 0$ )

Theorem Assuming SETH, there is no  $n^{2-\epsilon} \text{poly}(d)$ -time  
alg. for OV [Or  $\text{SETH} \Rightarrow \text{OVH}$ ]

Proof  $n^{2-\epsilon} \text{poly}(d)$  time

Then for our instances  $n = 2^{N/2} \cdot M$   $d = M$

$$n^{2-\epsilon} \text{poly}(d) = \left(2^{N/2} M\right)^{2-\epsilon} \cdot \text{poly}(M)$$

$$= 2^{(2-\epsilon)N/2} \text{poly}(M)$$

$$= 2^{(1-2\epsilon)N} \text{poly}(M) \text{ violates SETH}$$

