P vs NP

$P \neq NP \Rightarrow$ certain problems (3SAT) can't be solved in polynomial time

$\boxed{O(n^{\log\log\log n})}$

Best algo for 3SAT runs in $O(1.308^n)$

brute force: $O(2^n n^3) = O(2.000001^n)$

Best algo for CircuitSAT runs in $O(2^n \cdot m)$

This is brute force

perebor algorithms

"Conjecture": Some natural problems require perebor

Impagliazzo Pitasi Zane '99:

EXPONENTIAL TIME HYPOTHESIS (ETH)

3SAT requires $\Omega(2^{\varepsilon n})$ for some $\varepsilon > 0$.

$\Omega(c^n)$ $\quad c > 1$

STRONG ETH: (SETH)

For any $\varepsilon > 0$, there is an integer k s.t. KSAT requires $\Omega(2^{(1-\varepsilon)n})$ time.

For any $c < 2$ $\exists k$ KSAT needs $\Omega(c^n)$ time.

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

$\Downarrow$

[I?15] Edit distance requires $\Omega(n^{2-\varepsilon})$ time for all $\varepsilon > 0$

Best algo: $O(n^2/\log n)$

~~Longest~~ Heaviest Common Subseq - - - $\Omega(n^{2-\varepsilon})$

$O(n^2/2^{\sqrt{\log n}})$ time

Orthogonal Vectors [W'05]

Given n vectors $V_1 \dots V_n \in \{0,1\}^d$

Are there indices i, j s.t. $\langle v_i, v_j \rangle = 0$

$$\sum_{k=1}^{d} V_{ik} \cdot V_{jk} = 0$$

Algo: for $i \leftarrow 1$ to n
for $j \leftarrow 1$ to n
if $\langle v_i, v_j \rangle = 0$
return T
return F

$\Big\} \; O(dn^2)$

SETH $\Rightarrow$ CNFSAT requires $\Omega(2^{(1-\varepsilon)n})$ time for all $\varepsilon > 0$.

IPZ: even if every variable appears in only $O(1)$ clauses

$\Rightarrow O(n)$ clauses overall

Theorem [Williams'05]

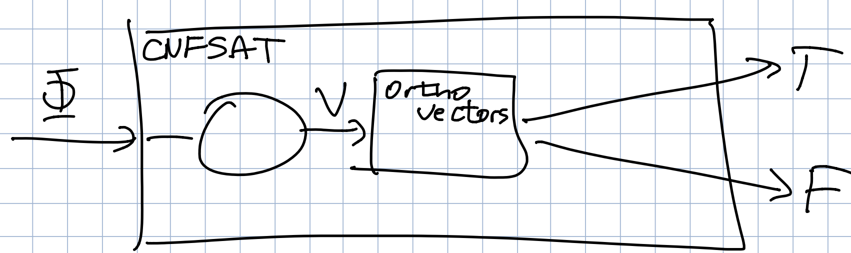
SETH $\Rightarrow$ OrthoVectors for n vectors $d = O(\log n)$ requires $\Omega(n^{2-\varepsilon})$ time for all $\varepsilon > 0$.

Obvious algo: $O(n^2 \log n) = O(N^2/\log N)$

$N = O(n \log n)$

Proof:

Suppose OV can be solved in $O(n^c)$ for some $c < 2$.



Fix a CNF formula Φ with n vars, $m = O(n)$ clauses

Partition n vars into two subsets of size $n/2$

$\Rightarrow 2 \cdot 2^{n/2}$ partial assignments

For each partial assignment α, define $v(\alpha)$

j^{th} bit in $v(\alpha) = 1$

$\Leftrightarrow$ α does not satisfy the j^{th} clause in Φ

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

a	b		
T	T	0001	01
T	F	0011	01
F	T		01
F	F		01

c	d		
T	T		10
T	F		10
F	T		10
F	F	1000	10

Orthogonal $v(\alpha), v(\beta) \Longleftrightarrow \alpha \cup \beta$ satisfies Φ

$\text{OrthoVector}(\underbrace{v(\alpha), v(\beta), \ldots}_{2\cdot 2^{n/2}})$ runs in $O((2\cdot 2^{n/2})^c)$

$c<2$

$O(2^{(1-\varepsilon)n})$ for some $\varepsilon>0$

$\Downarrow$

SETH is False

$\square$

Theorem: SETH $\Rightarrow$ $\cancel{L}$ HCS requires $\Omega(n^{2-\varepsilon})$ time for all ε.

Input: $x, y \in \Sigma^*$ $\quad w: \Sigma \to \mathbb{N}$ $\quad w(z) = \sum_i w(z_i)$

Find $\max\{w(z) \mid z$ is a subseq of x and a subseq of $y\}$

Reduce HCS to LCS:

Replace a with $a^{w(a)}$

Reduction From Ortho Vectors

Given sets A and B of n vectors in $\{0,1\}^d$

$d = O(\log n)$

Construct strings $x, y \in \{x, o, <, >, [,], \$, \bullet\}$

s.t. $HCS(x,y) > W \Leftrightarrow A, B$ contain ortho vects.

Coordinates:

$\alpha(0) = \langle x\, o \rangle \qquad \beta(0) = \langle o\, x \rangle \qquad w(0) = w(x) = 2$

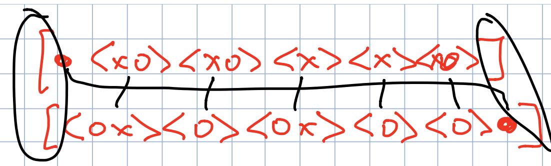
$\alpha(1) = \langle x \rangle \qquad \beta(1) = \langle o \rangle \qquad w(<) = w(>) = 1000d. = D$

$$LCS(\alpha(a), \beta(b)) = \begin{cases} 3 & \text{if } a\cdot b = 0 \\ 2 & \text{if } a \cdot b = 1 \end{cases}$$

$$WCS(\alpha(a), \beta(b)) = \begin{cases} 2D + 2 & \text{if } a\cdot b = 0 \\ 2D & \text{if } a\cdot b = 1 \end{cases}$$

Vectors: $\alpha(a_1 a_2 \ldots a_d) = [\bullet\, \alpha(a_1)\, \alpha(a_2) \cdots \alpha(a_d)] \qquad w([) = w(]) = D^2$

$\beta(b_1 \cdots b_d) = [\beta(b_1) \cdots \beta(b_d)\, \bullet] \qquad w(\bullet)$



Sets

$X = \$\, \alpha(a_1)\, \$\, \alpha(a_2)\, --- \,\$\, \alpha(a_n)\, \$$

$Y = \$\$\$\$\$\; \beta(b_1)\; \beta(b_2)\; --- \;\beta(b_n)\; \$\$\$\$\$$

$HCS(x,y) > W \iff A, B$ contain ortho vectors