CPSC 421/501 Nov 29

1. The formula size challenge
2. The circuit size challenge, and

   P vs. NP (§9.3 of [Sip])

This is how many people would approach P vs. NP

3. Subbotovskaya's method of (random) restrictions

(For formula size.)

[Notes on the above will appear.]

① Formula size:

Rem: $\{T, F\}$ or $\{0, 1\}$

$1 \leftrightarrow T, \quad 0 \leftrightarrow F$

Consider $(x_1, \ldots, x_n \in \{0,1\})$

$$Th_2(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } x_1 + \ldots + x_n \geq 2, \\ 0 & \text{otherwise} \end{cases}$$

$$= \underset{i<j}{\mathrm{OR}} \, (x_i \text{ AND } x_j)$$

$Th_2(x_1, \ldots, x_4)$

$$= (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_1 \wedge x_4)$$
$$\vee (x_2 \wedge x_3) \vee (x_2 \wedge x_4) \vee (x_3 \wedge x_4)$$

(i.e. some pair of variables $= 1$

or $= T$)

formula size 12

Alternate form

$Th_2 = T \iff$ any 3 variables, at least one $= T$

$$= (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_4)$$
$$\wedge (x_1 \vee x_3 \vee x_4) \wedge (x_2 \vee x_3 \vee x_4)$$

Rem: $Th_2(x_1,\dots,x_n) = \bigvee_{i<j} \underbrace{(x_i \wedge x_j)}_{2 \text{ vars}}$

$\stackrel{\#}{=} \binom{n}{2}$ clauses

$\text{size} = \binom{n}{2} \cdot 2 = \frac{n(n-1)}{2} \cdot 2$

$= n^2 - n =$ quadratic in n

Improvement:

$(x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_1 \wedge x_4)$

$= x_1 \wedge (x_2 \vee x_3 \vee x_4)$ ← size 4

$(x_2 \wedge x_3) \vee (x_2 \wedge x_4)$

$= x_2 \wedge (x_3 \vee x_4)$ ← size 3

$x_3 \wedge x_4$ $\leftarrow$ size $\cancel{2}$

---

size 9

Best possible = ?

size 3 for $Th_2(x_1, \ldots, x_4)$??

No — $Th_2(x_1, \ldots, x_4)$ depends on all its variables...

1 = 01 binary

2 = 10

3 = 11

4 = 100

$$Th_2(x_1, \dots, x_4) =$$

$$\left[(X_2 \text{ OR } X_4) \text{ AND } (X_1 \text{ OR } X_3)\right] \text{ OR }$$

$$\left[(X_1 \vee X_4) \wedge (X_2 \vee X_3)\right]$$

$$= (X_2 \text{ AND } X_1) \vee (X_4 \text{ AND } X_1) \text{ OR}$$

$$\dots$$

$$Th_2(x_1, \dots, x_8) =$$

Magic trick:

2 4
6 8

1st bit = 0

1 3
5 7

1st bit = 1

1 4
5 8

2nd bit = 0

2 3
6 7

2nd bit = 1

etc.

1 = 001
2 = 010
3 = 011
4 = 100
5 = 101
6 = 110
7 = 111
8 = 1000

This implies

$$\text{Formula size}\left(Th_2(x_1, \ldots, x_n)\right)$$

$$\leq n \cdot \left(\lceil \log_2 n \rceil\right)$$

Given $f : \{0,1\}^n \to \{0,1\}$

Best result: (essentially)

we can produce $f : \{0,1\}^n \to \{0,1\}$

that require size $\geq n^{3-\varepsilon}$

(ε any > 0).

It's not hard to see: most functions

$\{0,1\}^n \to \{0,1\}$

(or $\{T,F\}^n \longrightarrow \{T,F\}$)

require $\geq 2^n / (4 + \log_2 n)$

size formulas

Not hard to see any $\{0,1\}^n \to \{0,1\}$

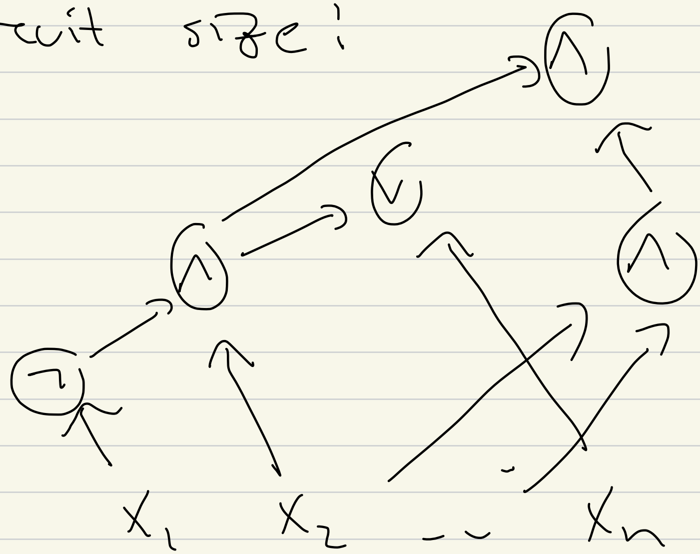
can expressed as formula

of size $n \cdot 2^{n-1}$

Next formulas vs circuits,

P vs NP $\longleftrightarrow$ min circuit size
of certain functions

Circuit size:



Boolean

Take an $L \subseteq \{T, F\}^*$

(or $\{0,1\}^*$) that is NP-complete.

Produce such an L!

$$3COLOR = \left\{ \langle G \rangle \;\middle|\; \begin{array}{c} G \text{ is a} \\ \text{3-colourable} \\ \text{graph} \end{array} \right\}$$

$3COLOR \subseteq \{0, 1, \ldots, 9, \#\}^*$

here we have 11 symbols

$$f \begin{cases} 0 \mapsto 0000 \\ 1 \mapsto 0001 \\ 2 \mapsto 0010 \\ \vdots \\ 9 \mapsto 1001 \\ \# \mapsto 1010 \end{cases}$$

$$\langle G \rangle \text{ is } \left. \begin{matrix} 33\#1\#2 \\ \#3\#7 \\ \# \ldots \end{matrix} \right\}$$

This converts

$\langle G \rangle$ to $\{0, \ldots, 9, \#\}^n$

$f(\langle G \rangle)$ to $\{0, 1\}^{4n}$

Claim:

$\{ f(\langle G \rangle) \mid$ G is a 3-colorable graph $\}$

then $\Updownarrow$ $f(\text{3COLOR})$

is also NP-complete.

Given $L \subset \{T, F\}^*$ or $\{0,1\}^*$

we get functions

$$\text{Function}_{L,n} : \{T, F\}^n \longrightarrow \{T, F\}$$

~~toty~~ by defining

$$\text{Function}_{L,n}(\sigma_1, \ldots, \sigma_n)$$

$$= \begin{cases} T & \text{if } \sigma_1 \ldots \sigma_n \in L \\ F & \text{otherwise} \end{cases} .$$

Thm If $L \in P$, then for all $n \in \mathbb{N}$, $\text{Function}_{L,n}$ can be expressed as a circuit of size $\leq \text{poly}(n)$.

Proof: Cook-Levin Theorem:

input $\sigma_1 \ldots \sigma_n$, and

$M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$

that decides L in time $\leq C n^k$

then we set

$\{X_{ij\gamma}, Y_{ij}, Z_{iq}\}$ as before.

Is $\sigma_1 \ldots \sigma_n \in L$??

q_0	σ_1	σ_2	$\ldots$	σ_n	$\sqcup$	$\sqcup$

Cn^k steps

X_{1jr}, Y_{1j}, Z_{1q} step 1

X_{2jr}, Y_{2j}, Z_{2q} step 2

is deterministic