CPSC 421/501 December 1, 2025

2 improvements 1993

- Today:

<u>Thm</u> (Subbotovskaya, 1961): Let f_n be a Boolean formula in $x_1, \ldots, x_n$ and $\vee, \wedge, \neg$ for $x_1 \oplus \cdots \oplus x_n$; let

S_n = min size possible of such an f_n.

Then $S_n \geq n^{1.5}/\sqrt{8}$. $\left(\begin{array}{c}\text{Immediate} \\ S_n \geq n\end{array}\right)$

See §2-5 of "Intro to Solving P vs. NP, and Subbotovskaya's Restriction Method.

Fundamental Lemma:

$$S_n \left(1 - \frac{1.5}{n}\right) \geq S_{n-1}$$

Note: $S_n\left(1-\frac{1}{n}\right) \geq S_{n-1}$

is easy and gives nothing...

Recall: deMorgan's laws:

$\neg(f \wedge g) = (\neg f) \vee (\neg g)$

$\neg(\ldots \vee \ldots) = \ldots \wedge \ldots$

<u>Lemma</u>: For any $g: \{T,F\}^n \to \{T,F\}$:

$x_1 \wedge g(x_1,\ldots,x_n) = x_1 \wedge g(T, x_2, \ldots, x_n)$

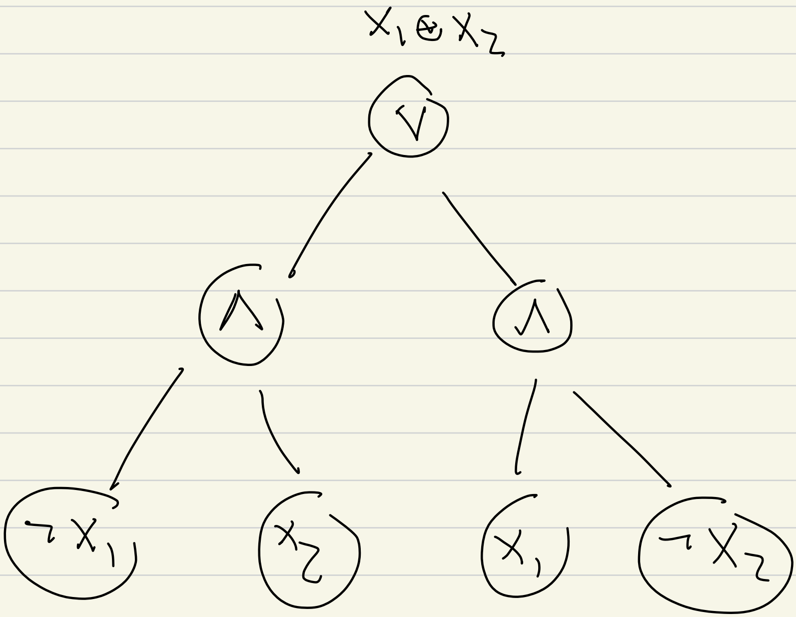
$\neg x_1 \wedge g \ldots = \neg x_1 \wedge g(F, x_2, \ldots, x_n)$

$x_1 \vee g \ldots = x_1 \vee g(F, \ldots)$

$\neg x_1 \vee g \ldots = \neg x_1 \vee g(T, \ldots)$

Then "random restriction"

$$x_1 \oplus x_2 = (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)$$

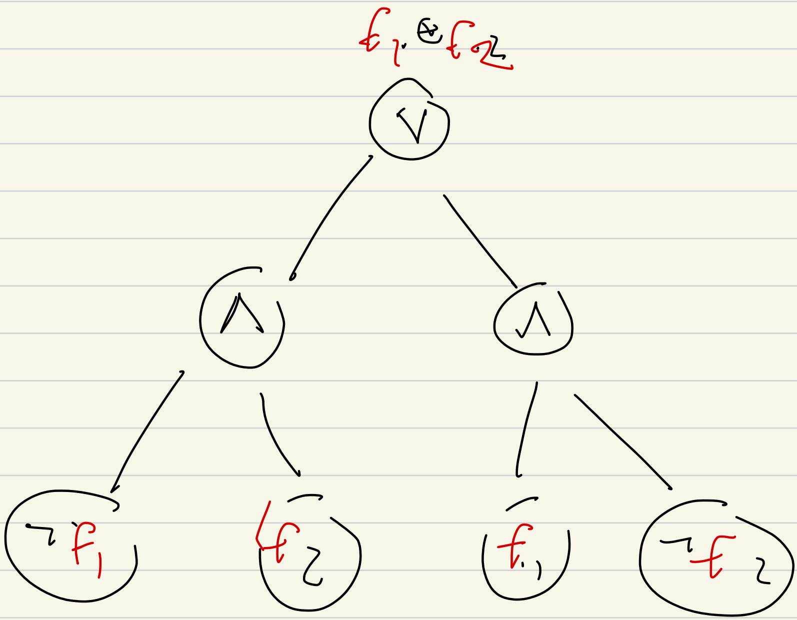


Claim: $x_1 \oplus x_2 \oplus \dots \oplus x_{2^k}$

you can write a formula of

size n^2, where $n = 2^k$.

$$f_1 \oplus f_2 = (\neg f_1 \wedge f_2) \vee (f_1 \wedge \neg f_2)$$



Use induction:

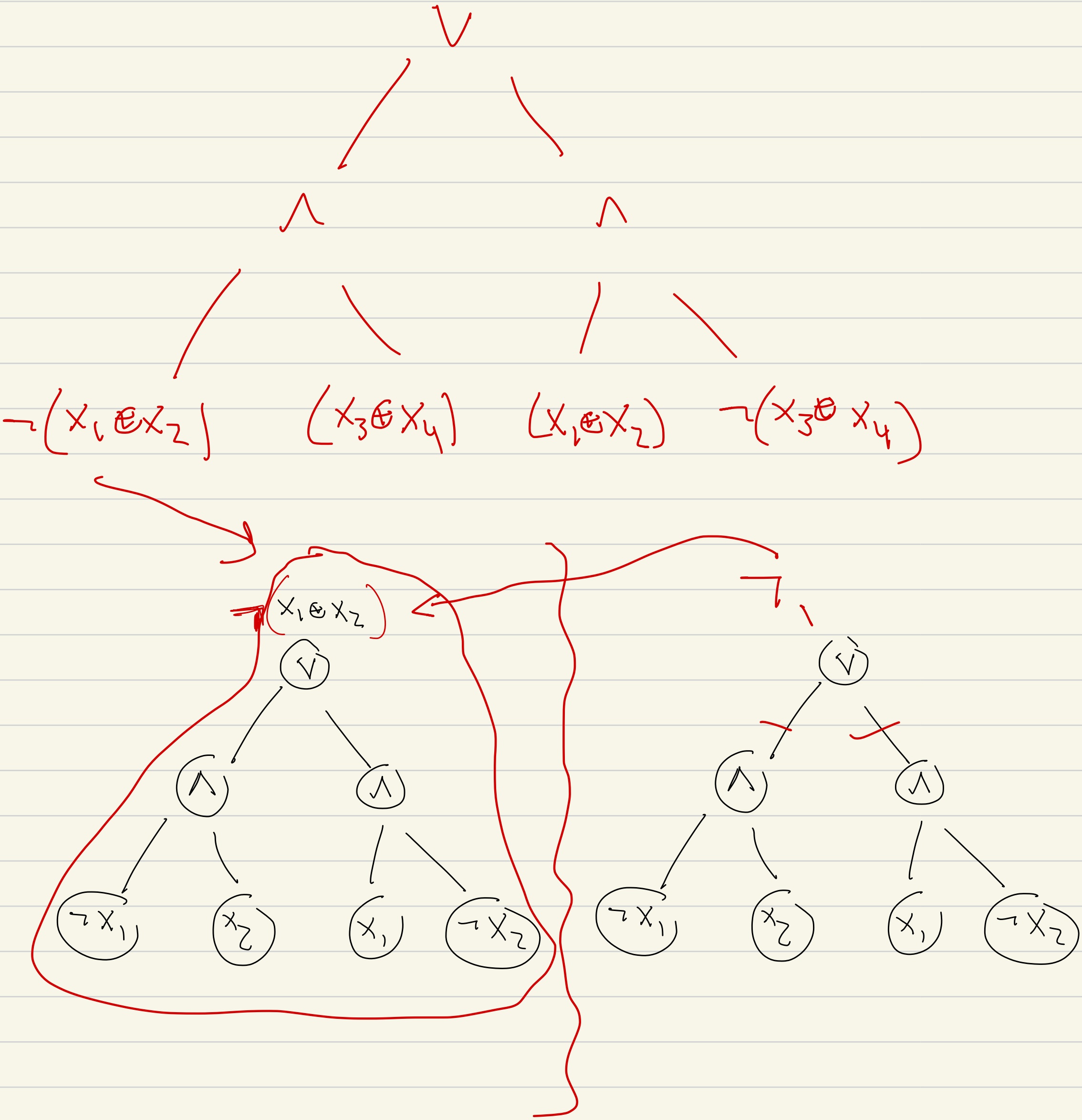
$$\boxed{f_1 = x_1 \oplus x_2 \qquad f_2 = x_3 \oplus x_4}$$

- Then $f_1 = x_1 \oplus \_\_ \oplus x_4, \quad f_2 = x_5 \oplus \_\_ \oplus x_8$

⋮

-4.5-

$x_1 \oplus x_2 \oplus x_3 \oplus x_4$



$$\begin{tikzcd}[column sep=small]
& \neg \arrow[d] & \\
& \lor \arrow[dl] \arrow[dr] & \\
\text{whatever}_1 & & \text{whatever}_2
\end{tikzcd}$$

$\Big\Downarrow$ de Morgan's rules

$$\begin{tikzcd}[column sep=small]
& \land \arrow[dl] \arrow[dr] & \\
\neg\,\text{whatever}_1 & & \neg\,\text{whatever}_2
\end{tikzcd}$$

Filter down the $\neg$ through all $\land$, $\lor$ operations

Hence

$$S_{2n} \le 4 S_n$$

$$\le 16 S_{n/2}$$

$$\le 4^3 S_{n/4} \cdots$$

S_n = min formula size for

$x_1 \oplus \cdots \oplus x_n$

Claim

$$S_{n-1} \le \left(1 - \frac{1}{n}\right) S_n$$

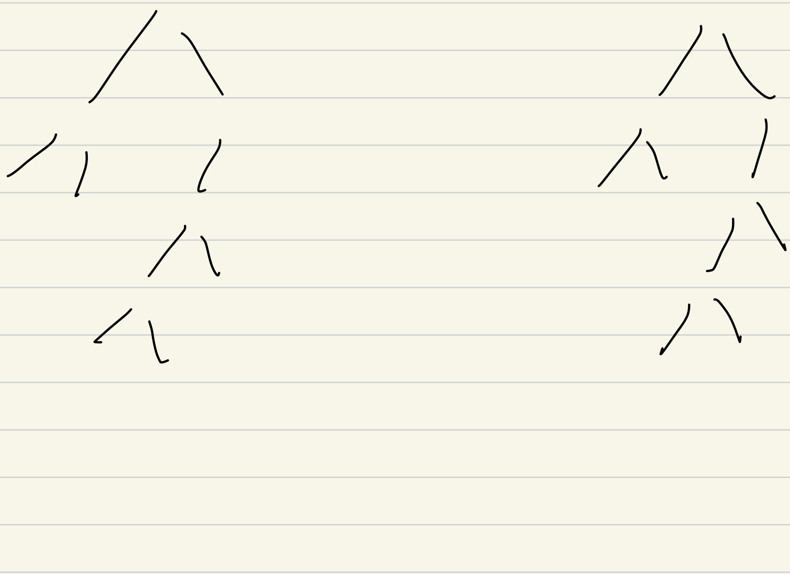
Think of a formula for $X_1 \oplus \dots \oplus X_n$

min size, S_n, then

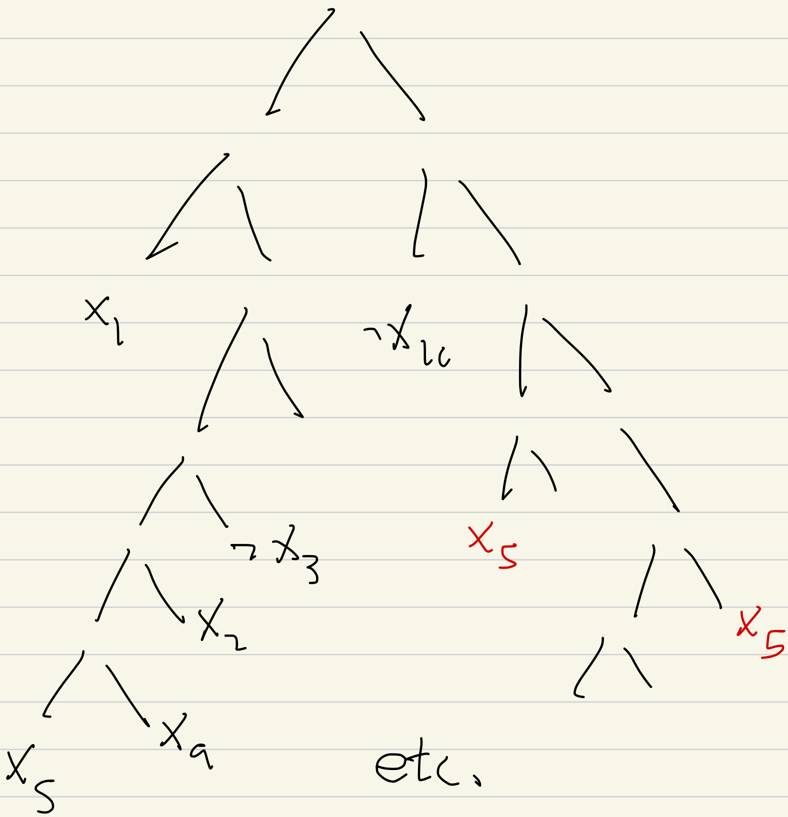
$\neg(X_1 \oplus \dots \oplus X_n)$ has min formula size

S_n

$(X_1 \oplus \dots \oplus X_n)$ $\qquad\qquad$ $\neg(X_1 \oplus \dots \oplus X_n)$



$x_1 \oplus x_2 \oplus \ldots \oplus x_n$



etc.

You have S_n leaves

$$(\# \; x_1, \neg x_1) + (\# \; x_2, \neg x_2) + \ldots + (\# \; x_n, \neg x_n) = S_n$$

Hence

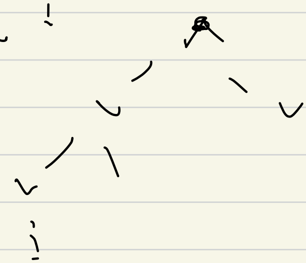
$$\underset{i=1,\dots,n}{\text{Average}} \; \#(x_i, \neg x_i \text{ leaves}) = \frac{S_n}{n}$$

Hence:

- take a random (average) x_i
  $i = 1, \dots, n$

- set $x_i = \begin{cases} T & \text{prob } 1/2 \\ F & \text{prob } 1/2 \end{cases}$

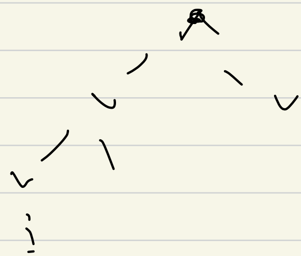
Say formula:



leaves

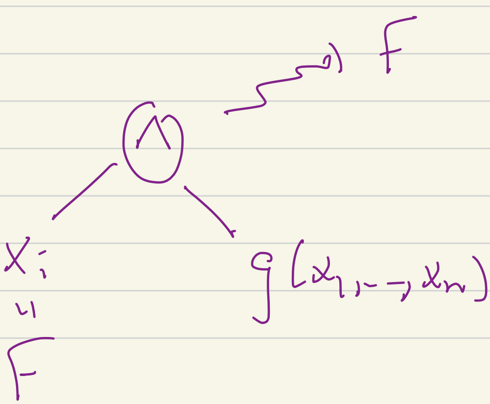
$x_i \qquad x_i \qquad \neg x_i \qquad x_i \qquad \neg x_i$

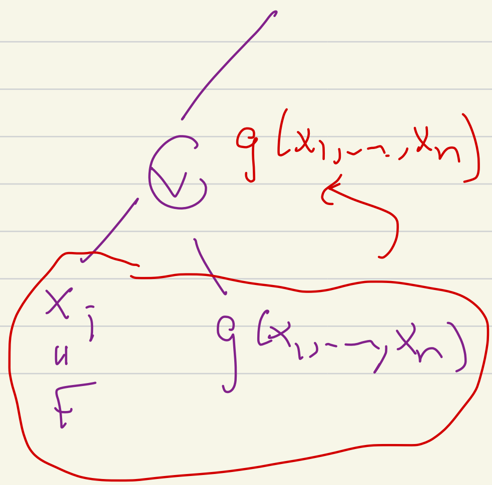
Setting, say $x_i \to F$



leaves

x_i	x_i	$\neg x_i$	x_i	$\neg x_i$
F	F	$\neg F$	F	$\neg F$
		$=$		$=$
		T		T





So

$$S_{n-1} \le \left(1 - \frac{1}{n}\right) S_n$$

$$\underbrace{X_1 \otimes \cdots \otimes X_n}$$

↑

eliminating
some X_i

↙ ↘
F T

So

$$S_1 \le \left(1 - \frac{1}{2}\right) S_2 \le \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) S_3$$

$$\le \cdots \le \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\cdots\left(1 - \frac{1}{n}\right) S_n$$

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) \cdots \left(1-\frac{1}{n}\right)$$

$$\underbrace{\frac{1}{2} \quad \frac{2}{3} \quad \frac{3}{4} \quad \frac{4}{5} \cdots \frac{n-1}{n}}_{\frac{1}{n}}$$

$$S_1 \le \frac{1}{n} S_n$$

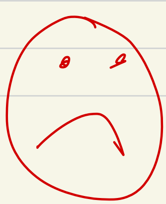
x_1

Size

$S_1 \ge 1$

y

$S_n \ge n$



Rem!

$$\left(1-\frac{1.5}{2}\right)\left(1-\frac{1.5}{3}\right)(\cdots)\left(1-\frac{1.5}{n}\right)$$

$$\approx 1/n^{1.5} \quad \sim\sim\sim$$

Class Ends

$x_i \qquad \tilde{T} \quad - \quad S_{n-1} \leq \lfloor \tfrac{k-1}{2} \rfloor S_n$

$F \quad - \quad S_{n-1} \leq (\tfrac{k-1}{2}) S_n - 1$

$f' = x_1 \oplus \cdots \oplus x_{i-1} \oplus x_{i+1} \oplus \cdots \oplus x_n$

$$f = \left(\begin{array}{l} (\neg x_i \wedge (\cancel{x_1 \oplus \cdots \oplus x_n})) \\ \qquad\qquad f' \\ \vee (x_i \wedge (\neg f')) \end{array} \right)$$

$= x_1 \oplus \cdots x_{i-1} \oplus x_{i+1}$

$x_1 \oplus \dots \oplus x_n$