CPSC 536F   Jan 25

If you can functions $f_n : \{0,1\}^n \to \{0,1\}$

Boolean functions in NP s.t.

$\boxed{\text{Min Circuit Size}}(f_n) \geq$ any poly in n,

then $P \neq NP$.

Open problem: find Boolean functions

$f_n : \{0,1\}^n \to \{0,1\}$, for some

$n \to \infty$ s.t.

(1) $\boxed{\text{Min formula size } (f_n) \geq n^{3.001}}$

(2) f_n is in NP (or P)

(or ...)

Today: "Shrinkage exponent"

Theorem (as of mid 1990's):

1. To compute XOR, parity

$$f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$$

in a DeMorgan formula requires

$\geq c n^2$ size

$\Omega(n^2)$ = bounded below by const. n^2

2. There is a function, Andreev function, that requires $\Omega(n^3/\log^2 n)$ size formulas.

Comments:

- Most Boolean functions require at least $2^n/\log n$ formula size.
- Any function that depends on all of its ~~n~~ variables, $f = f(x_1, \ldots, x_n)$ requires at least size n.

$2^n/\log n$ most

superpolynomial ← hope to prove $P \neq NP$

← e.g. $n^{\log n}$

current bound → n^3

n trivial

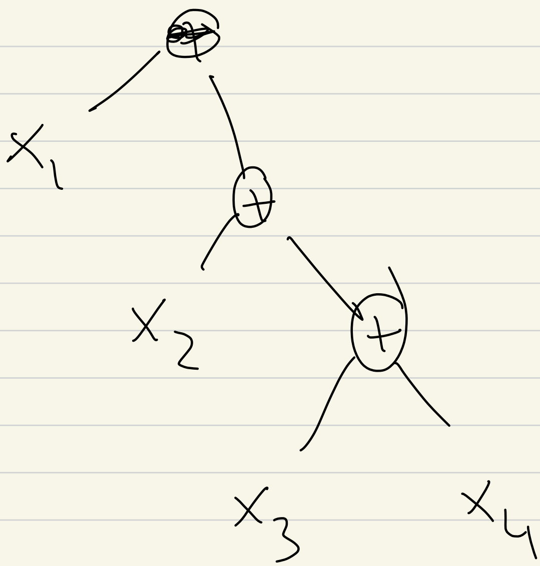
However, there are recent works on "communication complexity" that people have looked at recently that might improve on $\Omega(n^3)$ ...

Parity or XOR

$$f(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if the number of } x_i = 1 \text{ is odd} \\ 0 & \text{if the number of } x_i = 1 \text{ is even} \end{cases}$$

One formula!

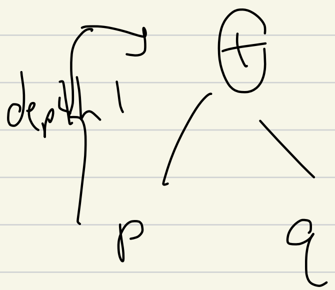
$$f(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$$



If you allow $\oplus$ gates, there is a formula size n that computes parity.

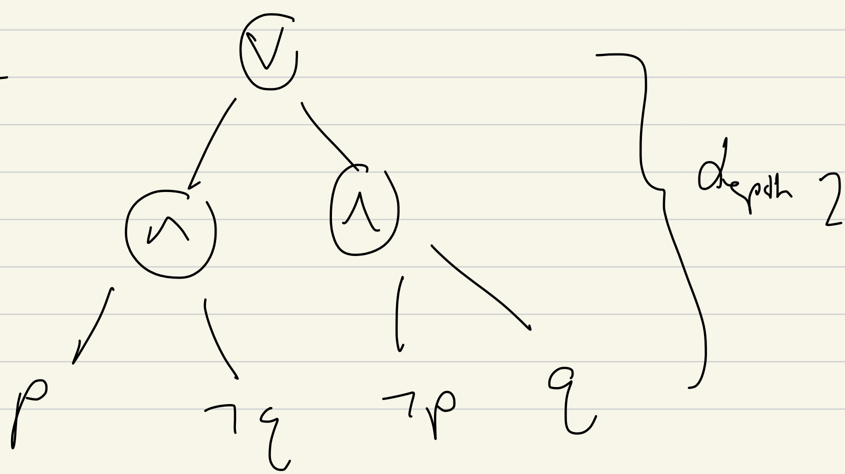
But, in a DeMorgan:

1. There are formula's size n^2 for parity!

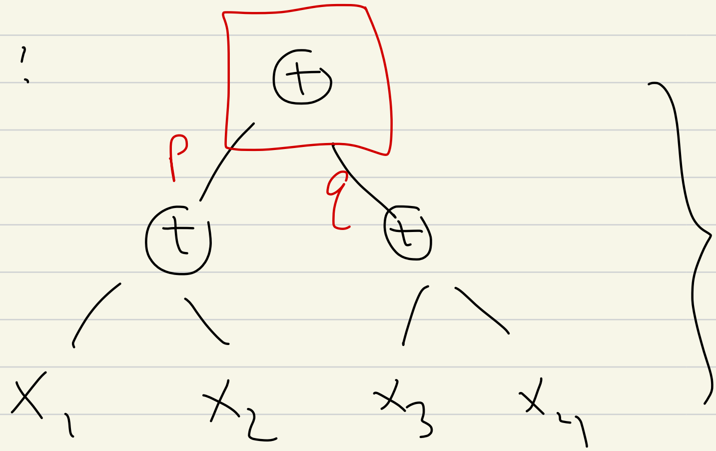


= either $p \wedge \neg q$ OR $\neg q \wedge p$

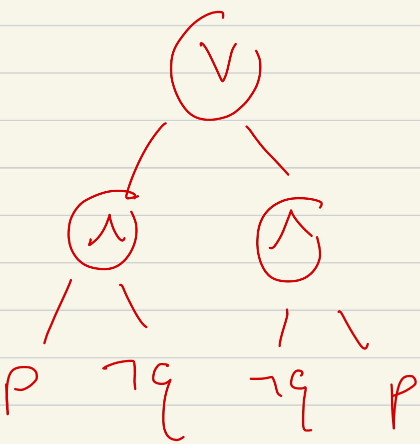
=

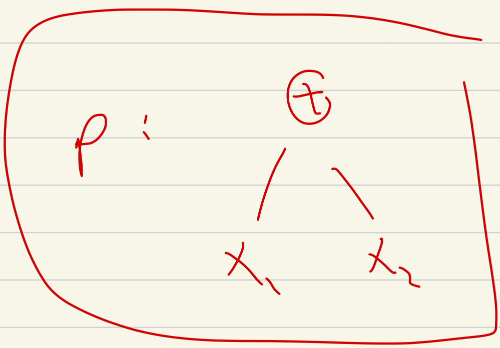


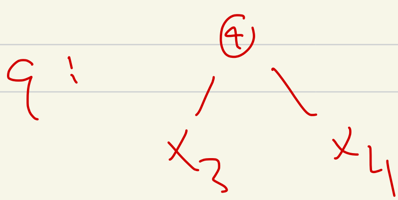
Now!

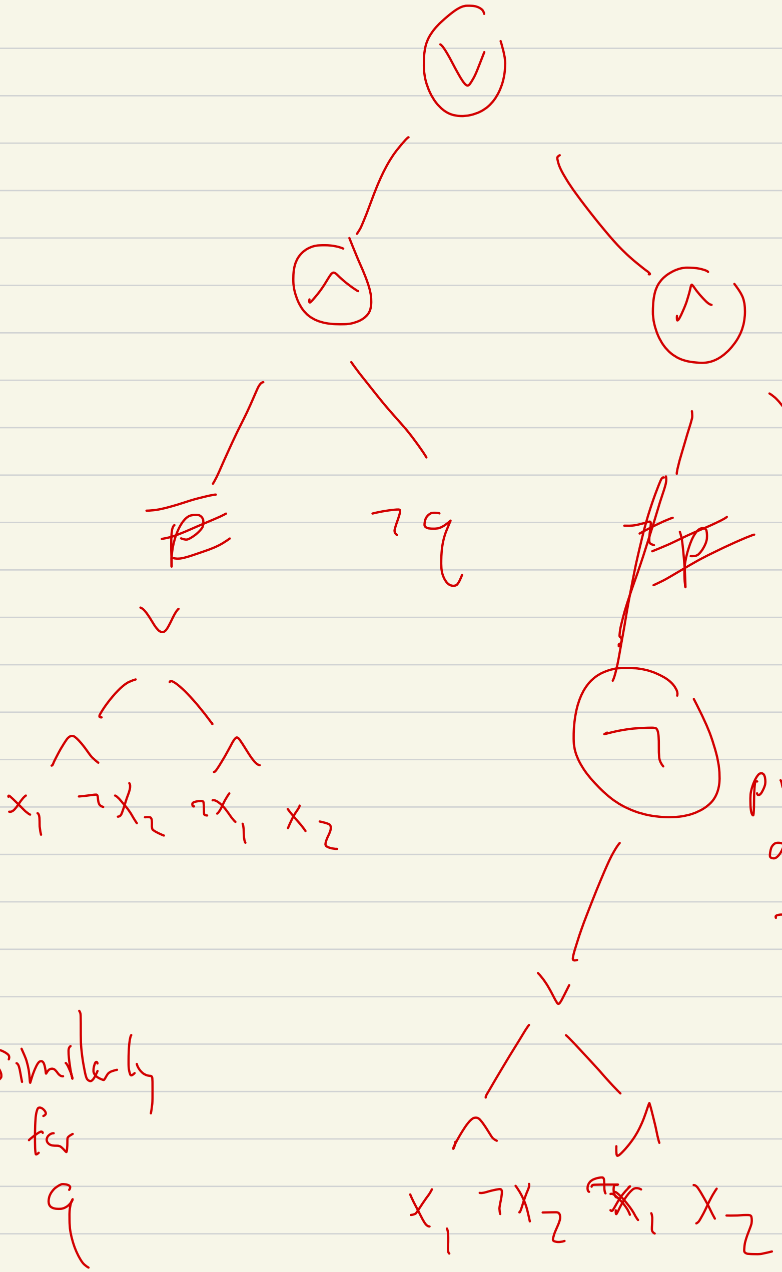


Can get a formula twice as deep for parity in De Morgan form









push ¬ down to the leaves

similarly for q

So formula depth k in $\oplus$ of 2^k vars $x_1, \ldots, x_{2^k}$ can be converted to De Morgan formula size $2^{2k} = (2^k)^2$

So size n^2 if n is a power of 2.

If n is not a power of 2, round n up to the nearest power of 2. Gives $O(n^2)$ size formula.

First result, 1961, by Subbotovskaya is that parity requires $\geq n^{3/2}$ size formula.

More importantly, this paper is probably the first use of "random restrictions"

Idea!

Take $f(x_1, \ldots, x_n)$

and with some probability ρ,

each $x_1, \ldots, x_n$ remains

untouched with probability ρ,

and otherwise!

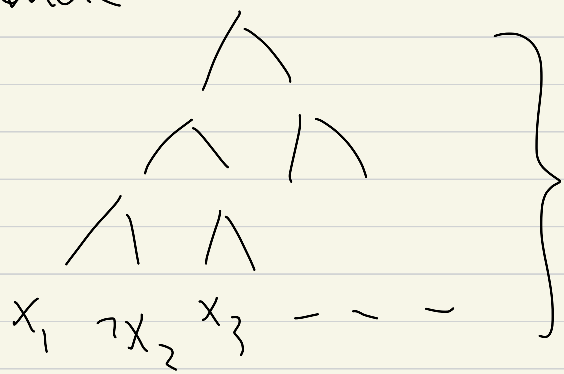
set to 1 prob $\frac{1-\rho}{2}$

set to 0 " $\frac{1-\rho}{2}$

The net result:

$$f(x_1, \ldots, x_n)$$

formula



formula size L

Roughly np of the variables $x_1, \ldots, x_n$ survive, and the formula simplifies.

Subbotovskaya (1961!)

(not improved until 1991 or so...)

Pick one of

$x_1, \ldots, x_n$ "at random"

uniformly, each with probability

$\frac{1}{n}$. Set x_i you pick!

$$x_i = \begin{cases} 0 & \text{prob } \frac{1}{2} \\ 1 & \text{prob } 1/2 \end{cases}$$

So, you consider one of $2n$ simplifications to f:

Claim: Expected / average size of formula L it is

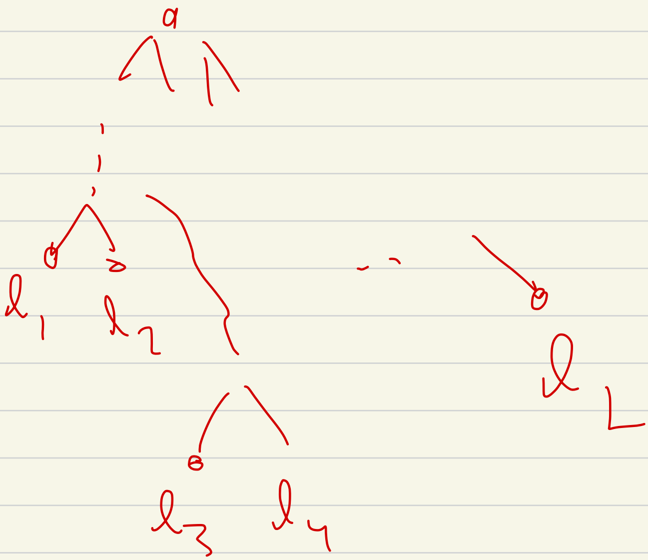
$$\leq L\left(1 - \frac{3/2}{n}\right)$$

Immediate observation

Expected size $\leq L\left(1 - \frac{1}{n}\right)$

formula, L leaves, each leaf.

disappears with prob $\frac{1}{n}$,



L leaves

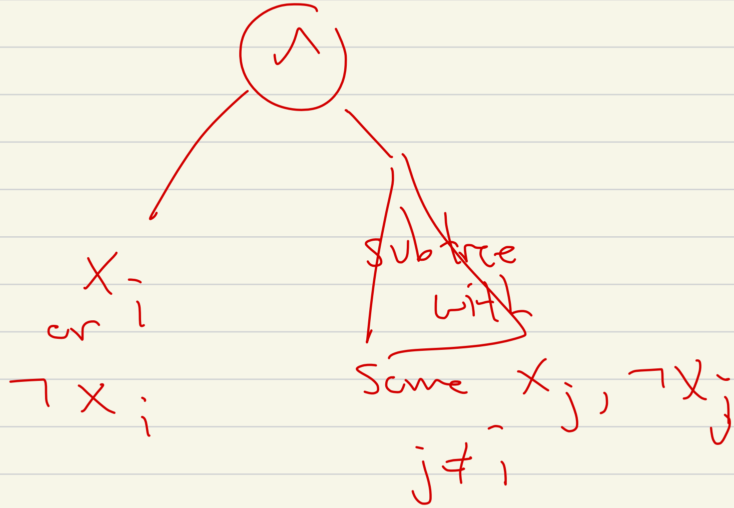
But consider: De Morgan

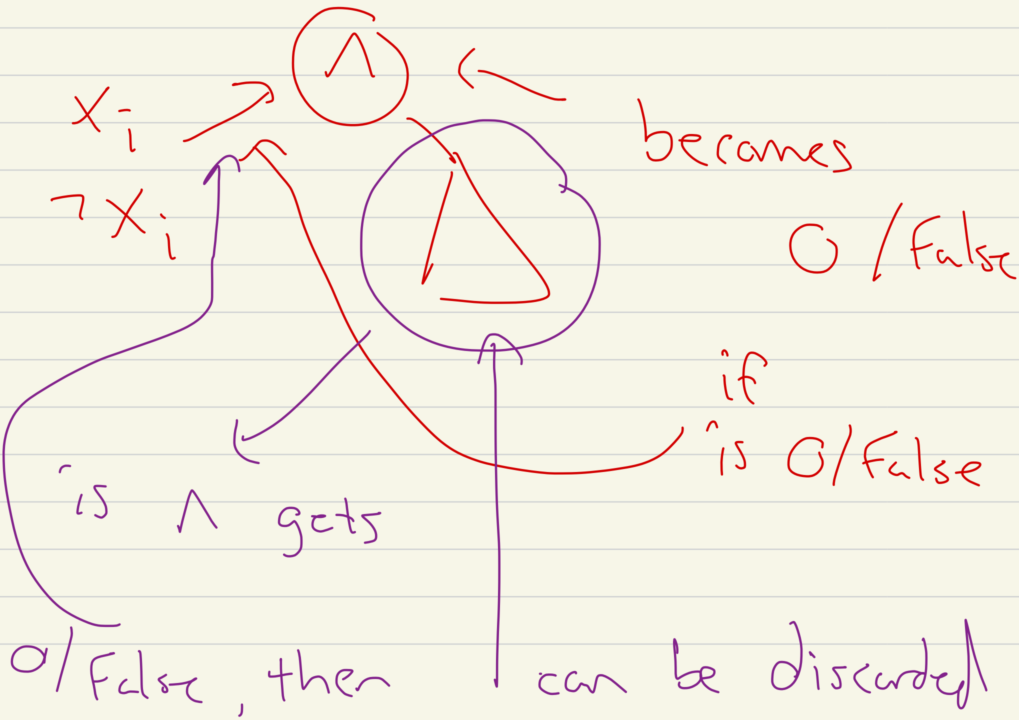
$\wedge$ or $\vee$

each leaf x_i $\neg x_i$

at least one variable below that is not x_i or $\neg x_i$

So say


∧
x_i
or
$\neg x_i$
subtree with
some $x_j, \neg x_j$
$j \neq i$


∧
x_i
$\neg x_i$
becomes
0/False
if
is 0/False
is ∧ gets
0/False, then
can be discarded

Now : one x_i restricted $\begin{cases} 0 & \text{prob } 1/2 \\ 1 & \text{" "} \end{cases}$

then

$$f(x_1, \ldots, x_n) \longrightarrow \text{some } g(\text{n-1 variables})$$

and

$$\text{Avg}\left(\begin{array}{c}\text{remaining} \\ \text{formula} \\ \text{size}\end{array}\right) \le \overset{\text{original}}{L}\left(1 - \frac{3/2}{n}\right)$$

This is $n \to n-1$ variables

Now $n-1 \to n-2$ "

$\vdots$

$\vdots$ m variables

After we're left with m variables

(m will be a constant),

$$\begin{pmatrix}\text{Avg Size} \\ \text{formula} \\ \text{on } m \\ \text{vars}\end{pmatrix} \leq L\left(1-\frac{3/2}{n}\right)\left(1-\frac{3/2}{n-1}\right)\cdots\left(1-\frac{3/2}{m}\right)$$

But, for any m, n

$$P = \left(1 - \frac{3/2}{n}\right)\left(1 - \frac{3/2}{n-1}\right) \cdots \left(1 - \frac{3/2}{m}\right)$$

then

$$\log_e P \simeq -\frac{3}{2}\left(\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{m}\right)$$

let's make this precise after break

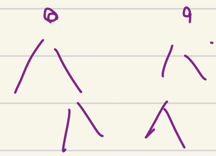
$$\simeq -\frac{3}{2}\int_m^n \frac{1}{x}\,dx$$

$$= -\frac{3}{2}\left(\log_e n - \log_e m\right)$$

So

$$P \simeq e^{\left(\quad\right)} = \frac{m^{3/2}}{n^{3/2}}$$

Now take $m = 3$



then

$$L \cdot p \approx L \cdot \frac{c}{n^{3/2}}$$

so

formula size L

shrinks to formula size

$$L \cdot \frac{c}{n^{3/2}} .$$

But if $f(x_1, \dots, x_n) =$ parity

then after setting $n-m$ variables

to 0, 1 but leaving m variables

the remaining function is

$$x_1 \oplus x_2 \oplus \cdots \oplus x_n$$

some are 0, 1

rest remain

$$= x_{i_1} \oplus \cdots \oplus x_{i_m}$$

or

$$\neg(\qquad \qquad).$$

Hence $L \geq \dfrac{n^{3/2}}{c}$, or

else $\dfrac{\text{Avg formula size}}{} < 1$

which is impossible, since

All formulas size $\geq m$ or, better yet, size of formula for parity of m variables

since they depend on all m variables

You can take $m = 1$

(set all $n-1$ others variables to be 0, 1)

$$x_1 \oplus \underline{\quad} \underline{\quad} \oplus x_n$$

one

$$\underline{\text{constants}} \oplus x_j \oplus \underline{\text{constants}}$$

left

=

After break: parity n-vars $\geq n^{1.5}$

Andre'ev $\geq n^{2.5}$

Break : 10:28 – 10:33

(1) Estimate carefully to really get $L \rightsquigarrow$ Avg size $\leq L\left(\frac{m}{n}\right)^{3/2}$

(2) Andreev introduced 1987 his "Andreev function", which given (1), must have formula size $\geq n^{2.5}$

(3) Subbotovskaya's result can be improved to $L\left(\frac{m}{n}\right)^{2-\varepsilon}$

for any $\varepsilon > 0$,

Since parity has De Morgan formula size $O(n^2)$,

it's impossible that

$$\begin{pmatrix}\text{Avg} \\ \text{formula} \\ \text{size}\end{pmatrix} \leq L \cdot C \cdot \left(\frac{m}{n}\right)^{2.00001}$$

Since this would imply

$$\Rightarrow \quad \text{parity of } n \text{ vars} \geq c \cdot n^{2.00001}$$

Andre'ev function requires $\geq n^3 / \log n$

Say that DeMorgan formulas

have shrinkage γ if

choosing m of n variables

to remain in any DeMorgan

formula size L on n ~~v~~ variables

implies that

$$\begin{pmatrix}\text{avg size} \\ \text{remaining} \\ \text{formula}\end{pmatrix} \leq L \cdot c \left(\frac{m}{n}\right)^{\gamma}$$

c is $c > 0$, independent of m, n.

Subbotovskaya 1961: $\gamma \geq 1.5$

Parity has n^2 size formula: $\gamma \leq 2$

Today: Shrinkage exponent in DeMorgan formulas, and its story:

History: See:

Hastad: The Shrinkage Exponent of De Morgan Formulas is 2, SIAM J. Computing, 1998 (recieved 1994, final version 1995)

=

Subbotovskaya 1961 (!):

Introduces γ = Shrinkage Exponent,

shows (1) $\gamma \geq 1.5$ (also $\gamma \leq 2$)

(2) Parity requires n^{γ} size De Morgan formulas

Krapchenko 1971: Parity requires at least $\Omega(n^2)$ size (in a DeMorgan formula)

Andre'ev: 1987 Andre'ev's function (which is in P) requires $\Omega(n^{1+\gamma}/\log^2 n)$ size

Nisan & Impagliazzo 1991, pub 1993

$$\gamma \geq \frac{21-\sqrt{73}}{8} \approx 1.55$$

Patterson & Zwick (same years, a bit later)

$$\gamma \geq \frac{5-\sqrt{3}}{2} \approx 1.63$$

Hastad pub 1998

$$\gamma = 2-\varepsilon$$

Let's estimate!

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

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

$\approx$

$$\log_e(1+x) = \cancel{x} - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

from Taylor series

$|x|<1$

also

$$\log_e(1+x) = x + O_\varepsilon(x^2)$$

for $|x| \le 1/2$ (really any $|x| \le 1-\varepsilon$)

via Taylor's Thm,

$$\underbrace{\log_e\left(1-\frac{3/2}{n}\right)}_{x=\frac{-3/2}{n}}$$

$$= \frac{-3/2}{n} + 3/2\, O\left(\frac{1}{n^2}\right)$$

the constant is universal (for $n \geq 2$.

$$\log_e\left(1-\frac{3/2}{n}\right) + \ldots + \log_e\left(1-\frac{3/2}{m}\right)$$

$$= \frac{-3/2}{n} + \ldots + \frac{-3/2}{m}$$

$$+ O\left(\frac{1}{n^2} + \frac{1}{(n-1)^2} + \ldots + \frac{1}{m^2}\right)$$

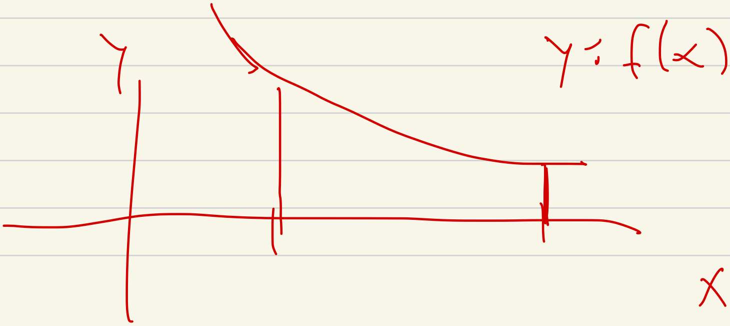
$$\frac{1}{n^2} + \frac{1}{(n-1)^2} + \cdots + \frac{1}{m^2}$$

$$< \frac{1}{n^2} + \frac{1}{(n-1)^2} + \cdots + ($$

bounded (as $n \to \infty$ equals $\frac{\pi^2}{6}$)

bound

$$\frac{1}{n} + \cdots + \frac{1}{m} \; ;$$



$y = f(x) = \frac{1}{x}$ monotone decreasing

$$\leq \int_{1/(n-1)}^{1/n} \frac{1}{x}\,dx \quad \text{etc.}$$

=

Class ends

=