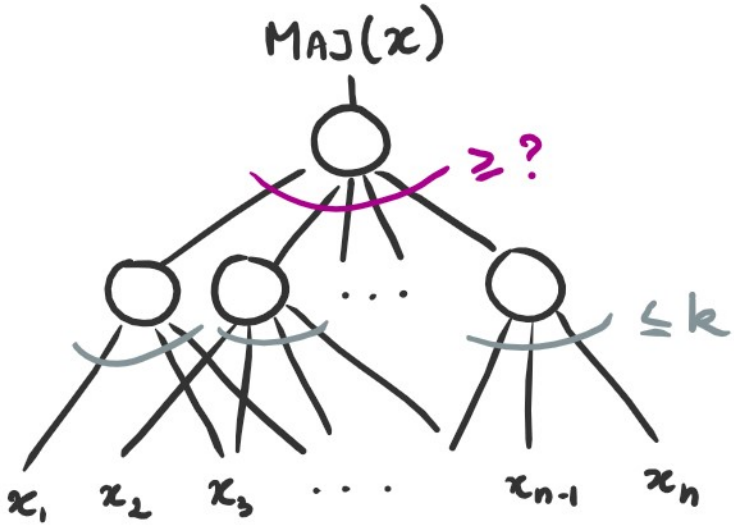
Composition complexity

Friday, July 8, 2022 14:50

The Composition Complexity of Majority



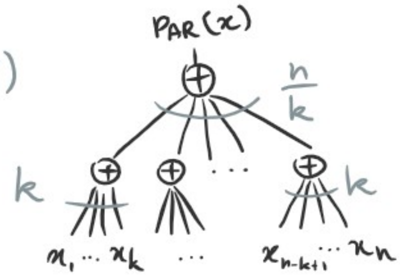
joint with

Prasanna Ramakrishnan

Li-Yang Tan

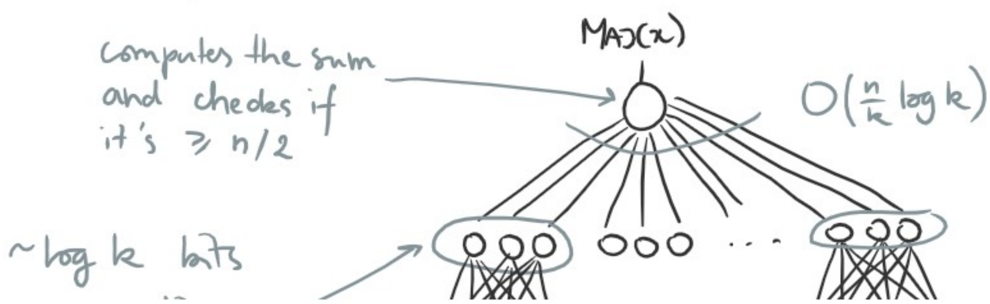
Parity decomposes nicely

Can:
- split vars into groups of k (e.g. $k=\sqrt{n}$)
- compute parity of each group
- combine those

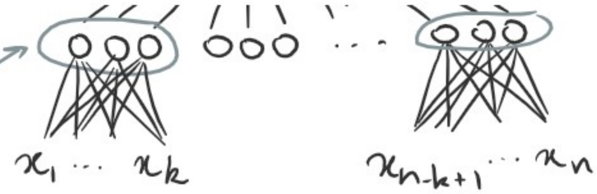


How about majority?

Seems like you need to know the Hamming weight of each group!

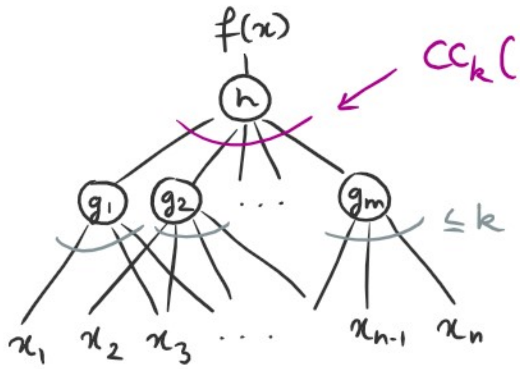


~log k bits representing $x_1 + \dots + x_k$ in binary



Can you do better?

If you want to compute $\mathrm{MAJ}(x)$ from functions of k variables, how many do you need?



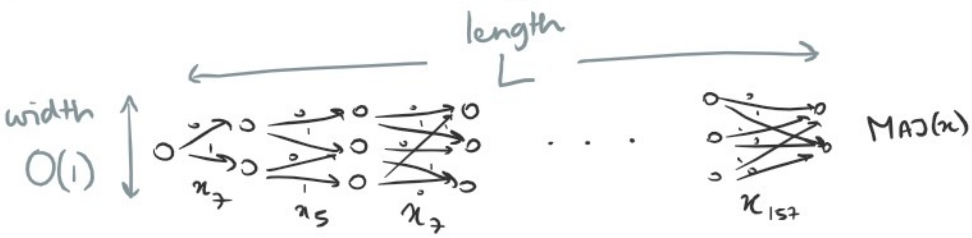
$CC_k(f) :=$ how large m needs to be

e.g. $CC_k(\mathrm{PAR}) = \frac{n}{k}$

Previous slide shows $CC_k(\mathrm{MAJ}) \le O\left(\frac{n}{k} \log k\right)$.

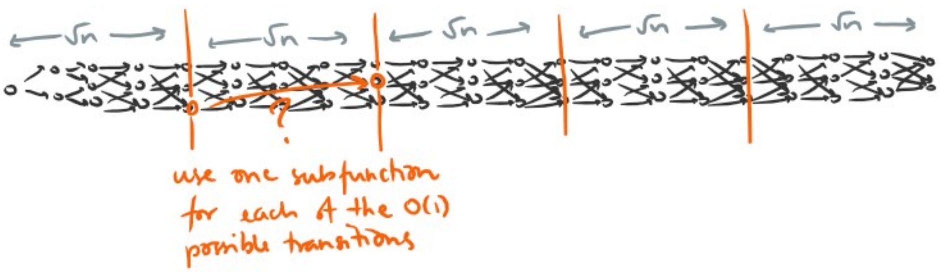
We show $CC_k(\mathrm{MAJ}) \ge \Omega\left(\frac{n}{k} \log k\right)$.

Connection 1 : branching programs



Claim $L \geq \Omega(n \log n)$. (recovers [AM'86], [BPRS'90])

Proof Constant-width BP of length $L \Rightarrow CC_{\sqrt{n}}(\mathrm{MAJ}) \leq O\left(\frac{L}{\sqrt{n}}\right)$.



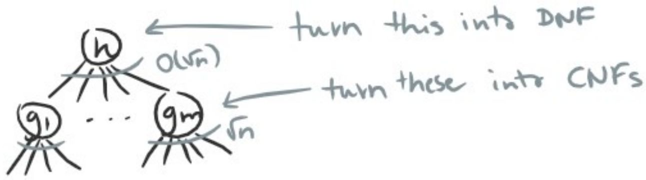
But $CC_{\sqrt{n}}(\mathrm{MAJ}) \geq \Omega(\sqrt{n} \log n) \Rightarrow L \geq \Omega(n \log n)$. $\square$

Connection 2 : small-depth circuits

Claim $CC_{\sqrt{n}}(f) \leq O(\sqrt{n}) \Rightarrow f$ has $2^{O(\sqrt{n})}$-size depth-3 ckts

turn this into DNF

Proof

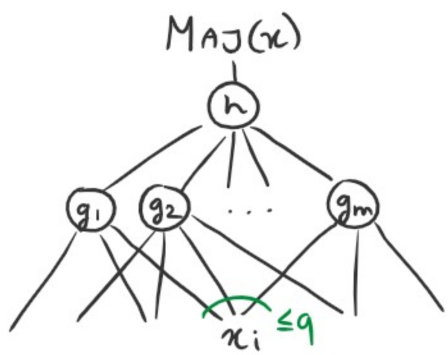


$\square$

So showing $CC_{\sqrt{n}}(f) \geq \omega(\sqrt{n})$ is a prerequisite for breaking the $2^{O(\sqrt{n})}$ barrier on lower bounds.

We do this for MAJ !

A counter-intuitive lemma



If x_i queried $\leq q$ times,

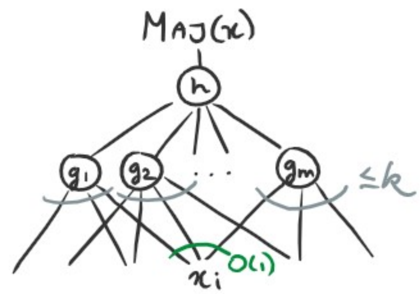
$$I[X_i : g_1(X), \dots, g_m(X)] \geq 2^{-O(q)}.$$

(i.e. can learn a lot about X_i by looking at $g_1(x), \dots, g_m(x)$)

The less you query it, the more you must reveal it.

Why this implies the lower bound

<u>Intuition</u> Much fewer subfunctions than variables, so there's no way they can learn that much!



<u>Proof</u> Suppose $m \leq O(n/k)$

$\Rightarrow$ total # queries $\leq O(n)$

$\Rightarrow \geq \frac{n}{2}$ vars queried $\leq O(1)$ times

$\Rightarrow I[x_i : g_1(x), \dots, g_m(x)] \geq 2^{-O(q)} \geq \Omega(1)$.

So by independence,

$$I[X : g_1(X), \dots, g_m(X)] \geq \sum_i I[X_i : g_1(X), \dots, g_m(X)]$$

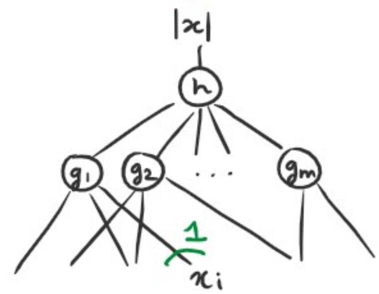
$$\geq \frac{n}{2} \cdot \Omega(1)$$

$$\gg m.$$

But $g_1(X), \dots, g_m(x)$ is only m bits, contradiction! $\square$

Baby version : $q=1$ for Hamming weight

switch to Hamming weight instead of majority



<u>Lemma</u> If x_i queried $\leq q$ times, then

$$I[X_i : g_1(X), \dots, g_m(X)] \leq 2^{-O(q)}.$$

$$\Big\downarrow q=1$$

If x_i queried only once, then

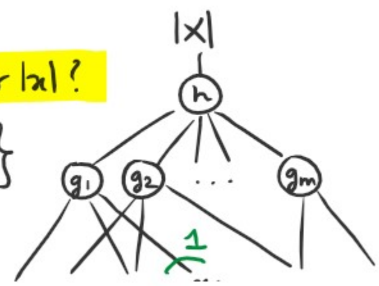
$$I[X_i : g_1(X), \dots, g_m(X)] = 1$$

i.e. can compute X_i from $g_1(X), \dots, g_m(X)$.

Proof of baby version

Fix any x.

Given $\underbrace{g_2(x), \dots, g_m(x)}_{\text{subfunctions not querying } x_i}$, how many possible values for $|x|$?



$$W = \{h(0, g_2(x), \dots, g_m(x)),\ h(1, g_2(x), \dots, g_m(x))\}$$

Now consider $x^{\oplus i}$ (x with x_i flipped), then

Now consider $x^{\oplus i}$ (x with x_i flipped), then
$g_j(x^{\oplus i}) = g_j(x)$ for $j = 2, \dots, m$, so $|x^{\oplus i}| \in W$, and

(assume WLOG x_i queried by g_1)

$$W = \{ |x|, |x^{\oplus i}| \}$$

And $\begin{cases} x_i = 0 \Rightarrow |x^{\oplus i}| = |x| + 1 \\ x_i = 1 \Rightarrow |x^{\oplus i}| = |x| - 1 \end{cases}$

So just check whether $|x|$ is the big or small element of W!

both can be computed from $g_1(x), \dots, g_m(x)$

Hints for the rest

— $q = 1 \rightarrow$ general q

Still look at

$W = \{$ possible values for $|x|$ given subfunctions <u>not</u> querying $x_i \}$

but only try to make a <u>guess</u> at x_i better than 50/50.

— Hamming weight $\rightarrow$ majority

mostly a reduction

Takeaways

- information theory is cool (and sometimes counter-intuitive)
- try proving your lower bound for a related <u>multi-output</u> function first

Open questions

We saw that

fan-in-$O(\sqrt{n})$ function of fan-in-$O(\sqrt{n})$ functions $\xrightarrow{\text{(reduction)}}$ size-$2^{o(\sqrt{n})}$ depth-3 ckts

OUR PAPER

?

BIG OPEN QUESTION

There are other interesting intermediate steps!

There are other interesting intermediate steps.

fan-in-$O(\sqrt{n})$ function of fan-in-$O(\sqrt{n})$ functions	$\xrightarrow{\text{(trivial)}}$	depth-$O(\sqrt{n})$ DT of fan-in-$O(\sqrt{n})$ functions	$\xrightarrow{\text{(reduction)}}$	size-$2^{o(\sqrt{n})}$ depth-3 ckts
✗ OUR PAPER		? YOUR PAPER?		? BIG OPEN QUESTION

(see paper for many others)

QUESTIONS?

Please leave them in the comments or send us an email.