Composition complexity (bonus)

Thursday, July 14, 2022 18:11

From $q=1$ to general q

<u>Goal</u> Enough to show $H[x_i \mid g_1(x), \dots, g_m(x)] \le 1 - 2^{-O(q)}$.

i.e. have a better than 50/50 guess at x_i

given $g_1(x), \dots, g_m(x)$, some of the time.

Let $J_i \subseteq [m]$ be the set of subfunctions querying x_i.

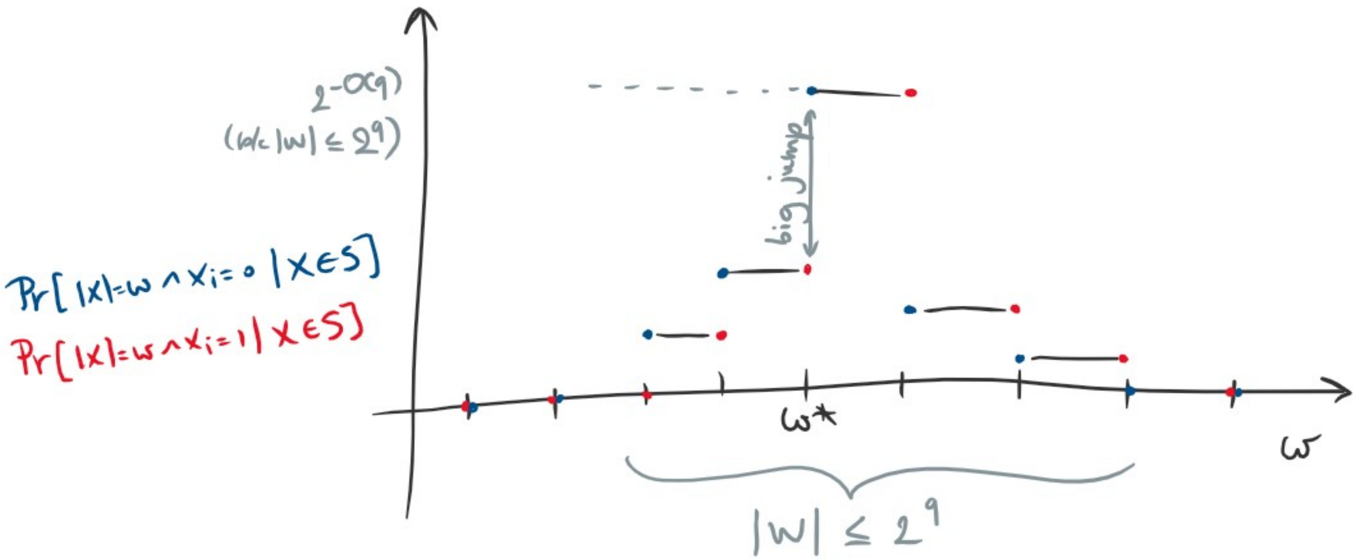
<u>Idea</u> Split based on subfunctions not querying x_i.

S = some set on which $g_j(x)$ fixed $\forall j \notin J_i$

Let $W = \{|x| : x \in S\}$.

(all possible Hamming weights)

$\Rightarrow |W| \le 2^q$.



Can find some $w^* \in W$ such that

$$Pr[\,|x|=w^* \wedge x_i=0 \mid x\in S] - Pr[\,|x|=w^* \wedge x_i=1 \mid x\in S]$$
$$\geq 2^{-O(q)}.$$

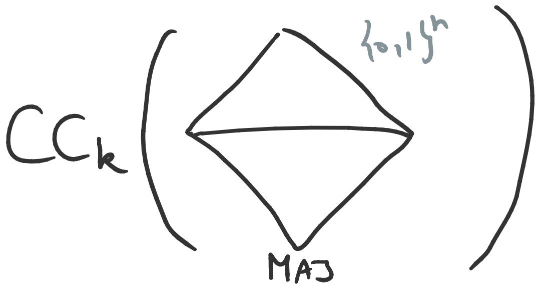
This implies $H[\,x_i \mid |x|, g_{\bar{J}_i}(x)] \le 1 - 2^{-O(q)}$

$$\vee\!/$$

$$H[x_i \mid g_1(x), \ldots, g_m(x)]$$

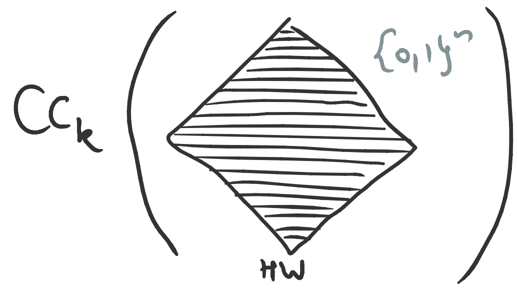
From Hamming weight to majority

Ideal reduction



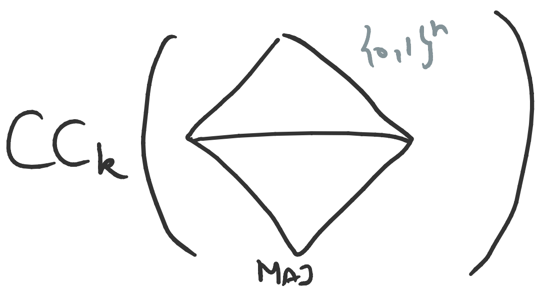
$\le O(n/k)$

$\Longrightarrow$



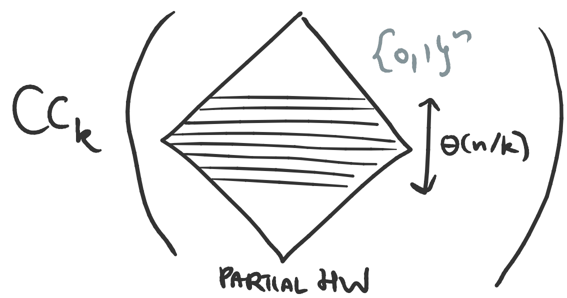
$\le O(n/k)$

Actual reduction



$\le O(n/k)$

$\Longrightarrow$



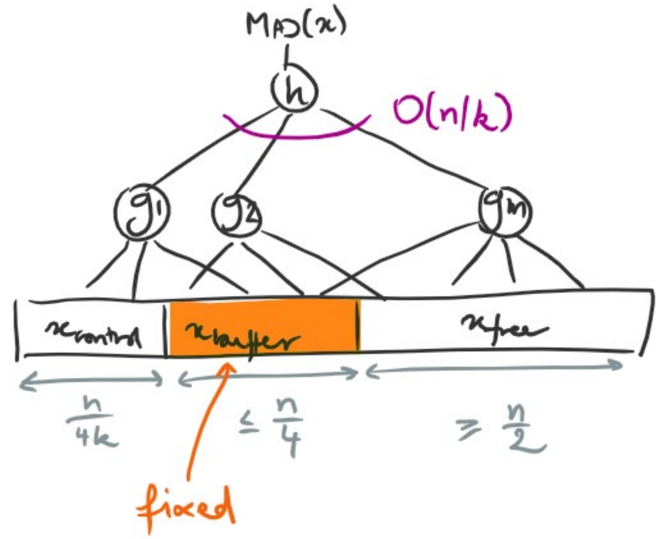
$\le O(n/k)$

Good news : we can also prove a LB for PARTIALHW.

Reduction setup

Split vars into 3 groups

- $x_{control}$: any $\frac{n}{4k}$ vars
- x_{buffer} : all vars sharing a subfunction with $x_{control}$
- x_{free} : the rest



<u>Idea</u> Can compute MAJ(x_{free}) if know:

- $x_{control}$
- x_{buffer} (fixed)

$\Big\}$ together determine rest of subfunctions

- subfunctions querying x_{free}

$\Rightarrow$ Can play with $x_{control}$ to figure out $|x_{free}|$ if it's close to half.