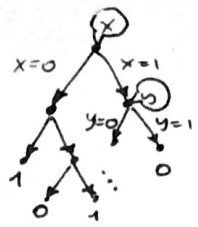
# Lecture 9 : "the Switching Lemma more in details and towards l.b. for PHP and random 3-XOR for Res(k)"

## Recap:

- binary decision trees :




$T$ - paths in $T$ are partial assignments
- leaves 0/1, $Br_0(T)$ $Br_1(T)$

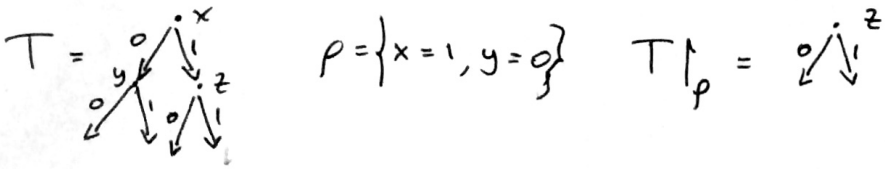
- $T$ strongly represents $\bigvee_{i=1}^{m} t_i$ with $t_i$ terms iff
  - $\forall \pi \in Br_0(T)\ \forall i \in [m]\ \ t_i\restriction_\pi = 0$
  - $\forall \pi \in Br_1(T)\ \exists i \in [m]\ \ t_i\restriction_\pi = 1$

  stronger requirement than saying just that $(\bigvee t_i)$ is semantically equivalent to 1

$h(\bigvee_{i=1}^{m} t_i)$ = min height of a tree $T$ strongly representing $\bigvee_{i=1}^{m} t_i$

- $\rho$ partial assignment $T\restriction_\rho$ obtained from $T$ deleting all edges inconsistent with $\rho$ and contracting the ones in $\rho$ and taking the connected component of the root of $T$.

eg.




- covering number of $\bigvee_i t_i$, $t_i$ terms

  $cov(\bigvee_i t_i)$ = smallest set of variables intersecting the variables of each $t_i$

obs: • $\varphi$ K-DNF then there are $\geq \frac{cov(\varphi)}{K}$ variable disjoint terms in $\varphi$.

- $cov(t) = 1$ if $t$ is a term
- $cov(C) = |C|$ if $C$ is a clause

- $\varphi$ K-DNF $\rho$ p.a with domain $cov(\varphi)$ then $\varphi\restriction_\rho$ is a $(K-1)$-DNF.

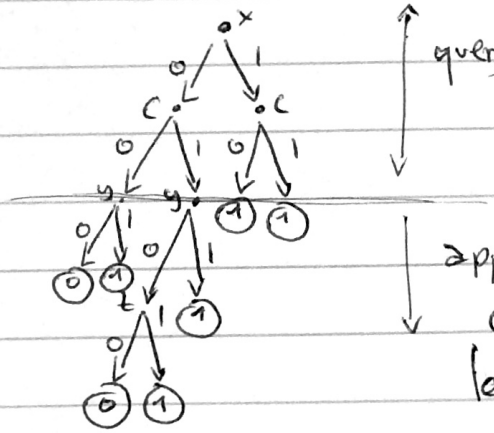
example

$\varphi = (x \wedge y \wedge \bar{z}) \vee (x \wedge a) \vee (y \wedge b) \vee (z \wedge c)$

$cov(\varphi) = 3$ $\quad S = \{x, b, c\}$ is a covering of $\varphi$

$\rho = \{a = 1, b = 1\}$

The tree we build strongly representing $\varphi|_\rho$ is

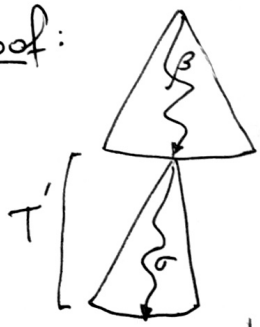


**Lemma**: Let $\varphi$ be a K-DNF and $\rho$ a partial assignments, then the decision tree $T$ build as follows strongly represents $\varphi|_\rho$:


first build the complete decision tree on the variables in a set $S$ that covers $\varphi$ that are not set by $\rho$ of minimal size. For each path $\beta$ append a tree strongly representing $\varphi|_{\rho\circ\beta}$ of minimal depth.

So in particular the height of $T$ is $= \text{cov}(\varphi) + \max_{\beta\in\{0,1\}^S} h(\varphi|_{\rho\circ\beta})$.

**proof**:




let $\beta$ a path in the first part of $T$ and $\sigma$ its continuation in a tree strongly representing $\varphi|_{\rho\circ\beta}$.

we have to consider the two cases where $\beta\circ\sigma$ leads to a 0 leaf or to a 1 leaf.

**1-leaf case**: since $T'$ strongly represents $\varphi|_{\rho\circ\beta}$ then there is some term $t' \in \varphi|_{\rho\circ\beta}$ such that $t'|_\sigma = 1$

this implies that $t' = t|_\beta$ with $t \in \varphi|_\rho$ so $t'|_\sigma = t|_{\beta\circ\sigma} = 1$

**0-leaf case**: for each non-zero term $t' \in \varphi|_{\rho\circ\beta}$ $t'|_\sigma = 0$ so as before $t' = t|_\beta$ with $t \in \varphi|_\rho$

the zeroed terms in $\varphi|_\rho$ by $\beta$ of course are still zeroed by $\beta\circ\sigma$.

□

**Theorem 1:** Let $k \geq 1$, $s_0, \ldots, s_{k-1}$, $p_1, \ldots, p_k$ positive numbers, $\mathcal{D}$ a distribution on partial assignments s.t.

$$\forall i \leq k \ \forall \varphi \text{ i-DNF } \left[ \text{if } cov(\varphi) > s_{i-1} \text{ then } \Pr_{\alpha \in \mathcal{D}}[\varphi|_\alpha \neq 1] \leq p_i \right] \quad (*)$$

then for every $k$-DNF $\psi$, $\Pr_{\alpha \in \mathcal{D}}\left[h(\psi|_\alpha) > \sum_{i=0}^{k-1} s_i\right] \leq \sum_{i=1}^{k} p_i \cdot 2^{\left(\sum_{j=i}^{k-1} s_j\right)}$

Before reviewing this proof let's prove the corollary we will actually use.

**Corollary:** Let $k, s, d$ positive integers, $\delta \in (0,1]$ and $\mathcal{D}$ a distribution on partial assignments s.t.

$$\forall \varphi \ k\text{-DNF} \quad \Pr_{\alpha \in \mathcal{D}}[\varphi|_\alpha \neq 1] \leq d\, 2^{-\delta\, cov(\varphi)}$$

then for every $k$-DNF $\psi$, $\Pr_{\alpha \in \mathcal{D}}[h(\psi|_\alpha) > 2s] \leq dk\, 2^{-\delta' s}$, where $\delta' = 2\left(\frac{\delta}{4}\right)^k$

proof of corollary from thm: Set $s_i = \left(\frac{\delta}{4}\right)^i \cdot s$ then set $p_i$ s.t. the hyp $(*)$ of thm is satisfied, so suppose you are given an $i$-DNF $\varphi$ s.t. $cov(\varphi) < s_{i-1}$, by hyp of corollary we know that

$$\Pr_\alpha[\varphi|_\alpha \neq 1] \leq d\, 2^{-\delta\, cov(\varphi)} \leq d\, 2^{-\delta s_{i-1}} \leq \underbrace{d\, 2^{-4 s_i}}_{\text{set this as } p_i}$$

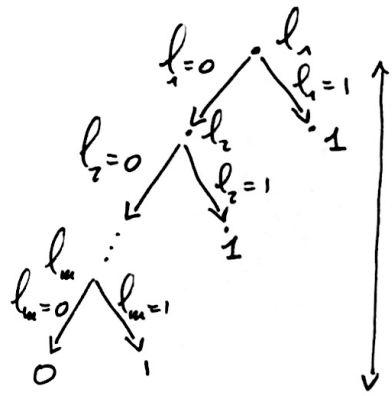
Then $\sum_{j=i}^{k-1} s_i = s_i \sum_{j=i}^{k-1} \left(\frac{\delta}{4}\right)^{j-i} \leq 2 s_i$ so

$$\Pr_\alpha[h(\varphi|_\alpha) > 2s] \leq \Pr_\alpha\left[h(\varphi|_\alpha) > \sum_{i=0}^{k-1} s_i\right] \overset{\text{thm}}{\leq} \sum_{i=0}^{k-1} p_i \cdot 2^{\left(\sum_{j=i}^{k-1} s_j\right)}$$

$$\leq \sum_{i=0}^{k-1} d\, 2^{2s_i - 4s_i} \leq dk\, 2^{-2s_k}$$

proof of theorem 1: by induction on K:

- "K=1" $\varphi$ 1-DNF, i.e. a clause $\ell_1 \vee \dots \vee \ell_m$ and $|cov(\varphi)| = m$




Let T be this tree. T strongly represents $\varphi$.

① if $cov(\varphi) \leq s_0$ then $m \leq s_0$ so $depth(T) \leq s_0$ and hence $\Pr_\alpha[h(\varphi|_\alpha) > s_0] = 0$

② if $cov(\varphi) > s_0$ by hyp $\Pr_\alpha[h(\varphi|_\alpha) > s_0] \leq$

$$\leq \Pr_\alpha[\varphi|_\alpha \neq 1] \leq p_1 \quad (*)$$

- "$K \to K+1$" let $\varphi$ be a $(K+1)$-DNF and

$s_0, \dots, s_K$ $p_1, \dots, p_{K+1}$ param. satisf. the hyp of the thm.

① if $cov(\varphi) > s_K$ then $\Pr_\alpha[\varphi|_\alpha \neq 1] \leq p_{K+1}$ so as in $(*)$ we have that

$$\Pr_\alpha\left[h(\varphi|_\alpha) > \sum_{i=0}^{K} s_i\right] \leq \Pr_\alpha[\varphi|_\alpha \neq 1] \leq p_{K+1} \leq \sum_{i=1}^{K+1} p_i \, 2^{\left(\sum_{j=i}^{K} s_j\right)}$$

② if $cov(\varphi) \leq s_K$ we have two subcases. Given $\alpha \in \mathcal{D}$ and $S$ a cover of $\varphi$ of size $cov(\varphi)$ we have:

ⓐ $\underbrace{\exists \beta \in \{0,1\}^S \; h(\varphi|_{\alpha\beta}) > \sum_{i=0}^{K-1} s_i}_{=B}$, in this case we have that

$$\Pr_\alpha\left[h(\varphi|_\alpha) > \sum_{i=0}^{K} s_i\right] \leq \Pr_\alpha[B] \leq 2^{|S|} \cdot \Pr_\alpha\left[h((\varphi|_\beta)|_\alpha) > \sum_{i=0}^{K-1} s_i\right]$$

$$\leq 2^{s_K} \cdot \sum_{i=1}^{K} p_i \, 2^{\sum_{j=i}^{K-1} s_j} \leq \sum_{i=1}^{K+1} p_i \, 2^{\sum_{j=i}^{K} s_j}$$

$\varphi|_\beta$ is a K-DNF and $|S| = |cov(\varphi)| \leq s_K$

ⓑ $\forall \beta \in \{0,1\}^S \; h(\varphi|_{\alpha\beta}) \leq \sum_{i=0}^{K-1} s_i$, in this case we construct the tree for $\varphi|_\alpha$ from the lemma, it will have depth $\leq \sum_{i=0}^{K} s_i$. □

In this lecture we want to use the machinery set up in the last two lectures to prove a lower bound for the formula $PHP_n^{cn}$ where $c$ is constant. That is we will prove the following result:

> **Theorem**: for each $c>1$ there exists $\varepsilon>0$ s.t. for all $n$ sufficiently large, if $k < \sqrt{\frac{\log n}{\log\log n}}$ then every $Res(k)$ refutation of $PHP_n^{cn}$ require size $\geq 2^{n^\varepsilon}$.

- Recall that $PHP_n^{cn}$ is the following CNF formula resulting from the conjunction of the following clauses
  - (pigeon clauses) for each $i \in [cn]$ we have in $PHP_n^{cn}$ the clause
    $$P_i = x_{i1} \vee x_{i2} \vee \cdots \vee x_{in}$$
  - (hole clauses) for each $i, i' \in [cn]$ $i \neq i$ and for each $j \in [n]$ we have the clause: $H_j^{i,i'} = \overline{x}_{ij} \vee \overline{x}_{i'j}$.

- The lines in $Res(k)$ are $k$-DNF formulas and as set of inference rules we use the following:

$$\frac{A}{A \vee \ell} \qquad \frac{A \vee \ell_1 \quad \cdots \quad A \vee \ell_k}{A \vee (\ell_1 \wedge \cdots \wedge \ell_k)} \qquad \frac{A \vee (\ell_1 \wedge \cdots \wedge \ell_j)}{A \vee \ell_i} \; \ell_i \in \{\ell_1, \ldots, \ell_j\}, j \leq k$$

$$\frac{A \vee (\ell_1 \wedge \cdots \wedge \ell_j) \quad B \vee \overline{\ell}_1 \vee \cdots \vee \overline{\ell}_j}{A \vee B}$$

In all such rules $A, B$ are $k$-DNFs and $\ell_1, \ldots, \ell_j$ are literals $(\overline{\ell}_i = \neg \ell_i)$.

Sanity check: control that $Res(k)$ with those rules is p-equivalent to any other definition you saw before.

Regarding the Thm we are going to prove:

- the proof we present follows closely the one from [Segerlind-Buss-Impagliazzo '04]
- the bound we show is not optimal in $\kappa$: [Razborov '15] pushed the technique to work till $\kappa < \frac{\log n}{\log\log n}$ getting a l.b. for the size of $PHP_n^{cn}$ of the form $2^{n/(\log n)^{O(\kappa)}}$.
- $PHP_n^{cn}$ for $c \geq 2$ has quasi-polynomial Res(polylog n) refutations, i.e. refutations of size $\leq 2^{(\log n)^{O(1)}}$.
- The result we show is actually stronger in the sense that it holds for a variation of the $PHP_n^{cn}$ formula called the "graph PHP", PHP(G).

---

**Def:** (PHP(G)) Let $G$ be a bipartite graph with bipartition $P = [cn]$ and $H = [n]$ and let $E$ be the set of edges of $G$. PHP(G) is the CNF formula obtained restricting the $PHP_n^{cn}$ formula with the partial restriction $\alpha$ setting $x_{ij} = 0$ iff $\{i,j\} \notin E$.

obs: Every size l.b. we are able to prove for PHP(G) will also hold for the corresponding $PHP_n^{cn}$. (why?) (The size l.b. are intended in "good" proof systems such as Res, Res(k) ...)

**Theorem 2:** If $G = (P \dot\cup H, E)$ is an $(r,\delta)$-boundary expander then every resolution refutation of PHP(G) will contain (at least) a clause of width $\frac{\delta r}{2}$. We denote this fact with the notation $\text{width}(PHP(G) \vdash) \geq \frac{\delta r}{2}$.

- A graph $G = (U \dot\cup V, E)$ is an $(r,\delta)$-boundary expander iff for each $A \subseteq U$ $|A| \leq r \longrightarrow |\partial A| \geq \delta |A|$, where $\partial A$ denotes here the "unique neighbors" of $A$: $\partial A = \{v \in V : \exists! u \in A \ \{u,v\} \in E\}$

proof of Thm 2: Let $\pi = (C_1, \ldots, C_\ell)$ be a resolution proof of PHP(G).

for any clause consider the measure $\mu$ defined as follows:

$$\mu(C) = \min\left\{ |I| : I \subseteq P \ \&\ \bigwedge_{i \in I} P_i \wedge \bigwedge_{\substack{i,i' \in P \\ i \neq i' \\ j \in H}} H_j^{i,i'} \models C \right\}$$

1. if $C$ is in PHP(G) then $\mu(C) \leq 1$
2. $\mu(\perp) \geq r$ because $G$ is an $(r, \delta)$-boundary expander and hence any subset of $P$ of size $\leq r$ admit a matching in $G$ (why?)
3. $\mu$ is sub additive, i.e. $\mu(C \vee D) \leq \mu(C \vee x) + \mu(D \vee \bar{x})$ for every $C, D$ clauses and $x$ variable

(1)+(2)+(3) $\Rightarrow \exists C \in \pi$ s.t. $\frac{r}{2} \leq \mu(C) \leq r$.

Fix such $C$ and let $I_C$ be the subset of $P$ realizing $\mu(C)$.

claim: for each $v \in \partial I_C$ there exist some $u \in P$ s.t. $x_{uv} \in C$.

(then claim $\Rightarrow |C| \geq |\partial I_C| \geq \delta |I_C| \geq \frac{\delta r}{2}$ — since $|I_C| \leq r$)

proof of claim: suppose none of the variables $x_{uv}$ appears in $C$. let $\tilde{u}$ be the unique neighbor of $v$ in $I_C$

by minimality of $I_C$,

$$\bigwedge_{i \in I_C \setminus \{\tilde{u}\}} P_i \wedge \bigwedge H_j^{i,i'} \not\models C$$

take an assignment $\alpha$ that satisfies $\bigwedge_{i \in I_C \setminus \{\tilde{u}\}} P_i \wedge \bigwedge H_j^{i,i'}$ but falsifies $C$

extend it to $\alpha'$ in the following way:

$$\alpha' = \alpha \cup \{x_{\tilde{u}v} = 1\} \cup \{x_{uv} = 0\}_{u \neq \tilde{u}}$$

- $\alpha'(C) = \alpha(C) = \text{false}$ but $\alpha'$ satisfies $\bigwedge_{i \in I_C} P_i \wedge \bigwedge H_j^{i,i'}$.

Contradicting the choice of $I_C$

▨