LECTURE 11

$$x^b = \begin{cases} x & \text{if } b = 0 \\ \bar{x} & \text{if } b = 1 \end{cases}$$

So x^b is true (i.e., $x^b = 0$ in PCR) iff $x = b$

$\boxed{BPHP^m_n}$ For all pigeons $p_1, p_2 \in [0, m)$, $p_1 \neq p_2$, for all $h \in [0, n)$:

$$\bigvee_{i=0}^{\ell-1} x[p_1, i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[p_2, i]^{1-h_i}$$

HOLE AXIOM $H(p_1, p_2, h)$

$[n = 2^\ell, \quad h = h_{\ell-1} h_{\ell-2} \cdots h_1 h_0]$

Disjunctive commitment C $\quad x[p_1, i_1]^{b_1} \vee x[p_2, i_2]^{b_2}$

$p_1 \neq p_2 \quad \mathrm{dom}(C) = \{p_1, p_2\}$

Commitment set $\mathcal{A} = \{C_1, \ldots, C_s\}$

$\mathrm{dom}(C_i) \cap \mathrm{dom}(C_j) = \emptyset$ if $i \neq j$.

A (total) truth value assignment $\alpha : \mathrm{Vars}(BPHP^m_n) \to \{0,1\}$ is <u>well-behaved on and satisfies $\mathcal{A}$</u> if

(1) α is well-behaved on $\mathrm{dom}(\mathcal{A})$, i.e., defines matching for these pigeons.

(2) α satisfies $\mathcal{A}$.

$\mathcal{A}$ <u>entails</u> $\mathbb{P}$ over well-behaved assignments if every α that is well-behaved on and satisfies $\mathcal{A}$ must also satisfy $\mathbb{P}$ (i.e., $\forall p \in \mathbb{P} \quad p(\alpha) = 0$).

COROLLARY 7 ~~Suppose~~ $S, T \subseteq [0, m)$, $S \cap T = \emptyset$, $|S \cup T| \leq n/2$. X contains exactly one $x[p, i_p]^{b_p}$ for every $p \in T$. Then ~~any~~ α well-behaved on S ~~satisfying~~ can be modified to β wellbehaved on $S \cup T$ and satisfying X by only changing pigeons in T.

LOCALITY LEMMA [FLNTZ '11] (LEMMA 9)

Suppose $\mathcal{A}$ commitment set, $|\mathcal{A}| \leq n/4$

$\mathbb{P}$ PCR-config

$\mathcal{A}$ entails $\mathbb{P}$ over well-behaved commitments

Then there is a commitment set $\mathcal{B}$ of size $|\mathcal{B}| \leq 2 \cdot Sp(\mathbb{P})$ s.t. $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments

THM [FLNTZ '11]

$Sp_{PCR}(BPHP_n^m \vdash \bot) > n/8.$

Proof. Let $\pi = \{\mathbb{P}_0 = \emptyset, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ be any PCR-derivation in space $\leq n/8$ from $BPHP_n^m$.
We prove that for each $\mathbb{P}_t$ there is an $\mathcal{A}_t$ s.t. $|\mathcal{A}_t| \leq 2 \cdot Sp(\mathbb{P}_t)$ & $\mathcal{A}_t$ entails $\mathbb{P}_t$. By Cor 7 (with $S = \emptyset$) this means that $\mathcal{A}_t$ is satisfiable (we can even satisfy all literals in $\mathcal{A}_t$!) so $\mathbb{P}_t$ must be satisfiable.
Hence any refutation of $BPHP_n^m$ has space $> n/8$.

Construct $\mathcal{A}_t$ by induction.

Base case $\mathcal{A}_0 = \emptyset$ for $\mathbb{P}_0 = \emptyset$

Inductive step 3 cases: (i) download, (ii) inference, (iii) erasure.

for obtaining $\mathcal{A}_{t+1}$ from $\mathcal{A}_t$
when derivation does $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$

Axiom download

Two cases:

(a) Complementarity axioms $x + \bar{x} - 1$

Boolean axioms $x^2 + x$

Do nothing i.e. $\mathcal{A}_{t+1} = \mathcal{A}_t$

All truth value assignments will satisfy these axioms.

(b) Hole axiom $H(p_1, p_2, h)$

If $\{p_1, p_2\} \subseteq dom(\mathcal{A}_t)$, put $\mathcal{A}_{t+1} = \mathcal{A}_t$

Any well-behaved assignment sends p_1 & p_2 to different holes and so satisfies $H(p_1, p_2, h)$.

If $\{p_1, p_2\} \cap dom(\mathcal{A}_t) = \emptyset$, then add commitment $C = x[p_1, 0]^{1-h_0} \vee x[p_2, 0]^{1-h_0}$, say (any literal for p_1 + any literal for p_2 is fine).

If $p_1 \in dom(\mathcal{A}_t)$, $p_2 \notin dom(\mathcal{A}_t)$ fix $p^* \notin dom(\mathcal{A}_t) \cup \{p_2\}$ and let

$$C = x[p_2, 0]^{1-h_0} \vee x[p^*, 0]^0 \quad , \text{say}$$

This is just to get $p_2 \in dom(\mathcal{A}_{t+1})$ for $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$.

Again any well-behaved assignment sends p_1 & p_2 to distinct holes and so satisfies $H(p_1, p_2, h)$.

At axiom download, space increases by (at least) 1 and we never add more than $1 < 2$ commitments, so we're in good shape.

<u>Inference step</u>

$\mathbb{P}_{t+1} = \mathbb{P}_t \cup \{q\}$ where q semantically follows from $\mathbb{P}_t$ i.e., if $\forall p \in \mathbb{P}_t \; p(\alpha) = 0$ then $q(\alpha) = 0$. Let $\mathcal{A}_{t+1} = \mathcal{A}_t$.

Any well-behaved α satisfying $\mathcal{A}_{t+1} = \mathcal{A}_t$ must satisfy $\mathbb{P}_t$ by induction hypothesis and hence also q as argued above, i.e, all of $\mathbb{P}_{t+1}$.

<u>Erasure step</u>

$\mathbb{P}_{t+1} = \mathbb{P}_t \setminus \{q\}$ for some $q \in \mathbb{P}_t$.

q could have very many monomials, and if so $Sp(\mathbb{P}_{t+1}) \ll Sp(\mathbb{P}_t)$. $\mathcal{A}_t$ entails $\mathbb{P}_{t+1}$, but is potentially (far) too large. What to do?

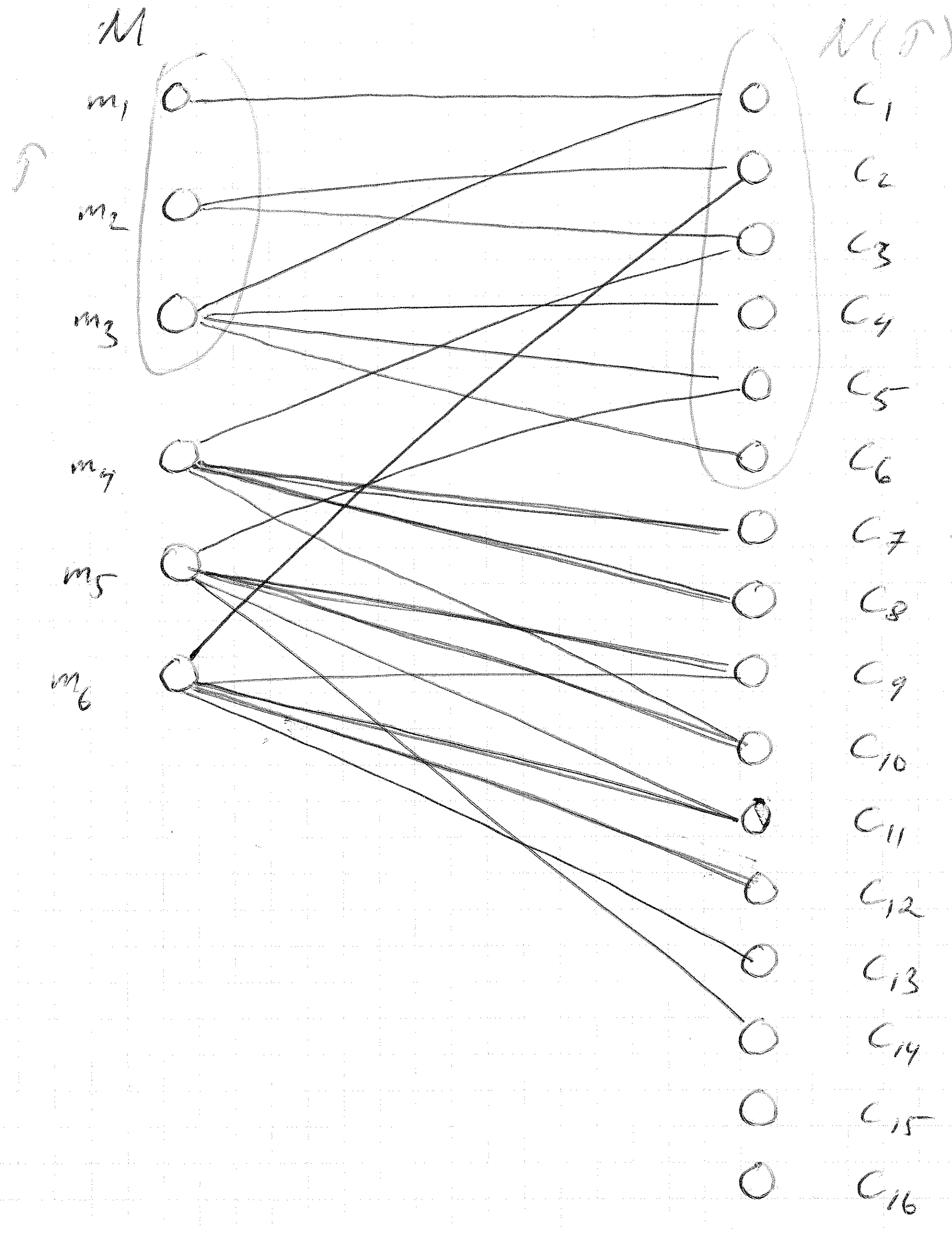
For instance, suppose $\mathbb{P}_{t+1}$ contains (after cancellations) a ~~some~~ single polynomial on the form

$$1 + \prod_{i=1}^{s} y_i$$

Then $Sp(\mathbb{P}_{t+1}) = 2$, but we need to set s variables to fix $\mathbb{P}_{t+1}$ to true !?

But no, Locality lemma says this cannot happen. We just apply the lemma with $\mathcal{A} = \mathcal{A}_t$ and $\mathbb{P} = \mathbb{P}_{t+1}$, and let $\mathcal{A}_{t+1}$ be the $\mathcal{B}$ produced by the lemma.

This takes care of all cases in the inductive step, and the theorem follows



$\cancel{x[p_1,i_1]^{b_1} \vee x[p_2,i_2]^{b_2}}$

$x[p',i']^{b'} \vee x[q',j']^{c'}$

$x[p'',i'']^{b''} \vee x[q'',j'']^{c''}$

Proof of Locality lemma

(See figure 11:VI)

Consider bipartite graph with set $\mathcal{M}$ of distinct monomials in $\mathbb{P}$ on left-hand side ($|\mathcal{M}| \le Sp(\mathbb{P})$) and commitments in $\mathcal{A}$ on right-hand side. Draw edge between $m \in \mathcal{M}$ and $C \in \mathcal{A}$ if there is a pigeon p mentioned in both (i.e. variable $x[p,i_1]^{b} \in Vars(m)$ and $x[p,i']^{b'} \in Vars(C)$.

Let $\mathcal{T} \subseteq \mathcal{M}$ be set of max size s.t. $|N(\mathcal{T})| \le 2|\mathcal{T}|$. Note that such a set exists — $\mathcal{T} = \emptyset$ if nothing else. If $\mathcal{T} = \mathcal{M}$ we can take $\mathcal{B} = N(\mathcal{T})$, and we're done. So suppose $\mathcal{T} \neq \mathcal{M}$.

Then for all $S \subseteq \mathcal{M} \setminus \mathcal{T}$ it holds that $|N(S) \setminus N(\mathcal{T})| > 2|S|$ since otherwise could add S to $\mathcal{T}$ to get larger set $\mathcal{T}$. By Hall's theorem, this means that there is a matching of every $m \in \mathcal{M} \setminus \mathcal{T}$ to two commitments $C', C'' \in \mathcal{A} \setminus N(\mathcal{T})$ such that every m gets two distinct commitments.

Fix such m with C', C''. Suppose

$$C' = x[p',i']^{b'} \vee x[q',j']^{c'}$$
$$C'' = x[p'',i'']^{b''} \vee x[q'',j'']^{c''}$$

where m mentions pigeons p' & p''.
(It can be that m also mentions q' and/or q'', but by construction we are guaranteed that m mentions at least one pigeon in each commitment.

Suppose $x[p', i_1]^{b_1} \in m$
$x[p'', i_2]^{b_2} \in m$

Then we construct a new ~~assig~~ commitment C for m to be $C = x[p', i_1]^{b_1} \vee x[p'', i_2]^{b_2}$
Do this for every $m \in M / N(\mathcal{F})$

Let $\mathcal{B}$ be the union of all these new assignments with $N(\mathcal{F})$.
$\mathcal{B}$ is a commitment set since all $\underbrace{\text{pigeons}}_{\text{mentioned in } \mathcal{B}}$ are different
Clearly $|\mathcal{B}| \leq 2|M| \leq 2 \cdot Sp(\mathbb{P})$. We claim that $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments. That is, we claim that any β that is well-behaved on and satisfies $\mathcal{B}$ must satisfy $\mathbb{P}$. We will prove this in a slightly roundabout way by finding α s.t.

1) $\mathbb{P}(\alpha) = \mathbb{P}(\beta)$
2) α is well-behaved on and satisfies $\mathcal{A}$

By (2) it follows (from the inductive hypothesis) that α satisfies $\mathbb{P}$. But if so, then β also satisfies $\mathbb{P}$ by (1).

Let S be the set of pigeons in $dom(\mathcal{B})$
T — " — $dom(\mathcal{A}) \setminus dom(\mathcal{B})$
(Notice $dom(\mathcal{B}) \subseteq dom(\mathcal{A})$).

Let $\mathcal{X}$ be the set of literals that for each $p \in T$ includes the (unique) literal $x[p,i]^b$ associated with p appearing in $\mathcal{A}$. Note that each commitment in $\mathcal{A} \setminus N(\mathcal{T})$ will have at least one literal in $\mathcal{X}$ (some commitments will potentially have both literals in $\mathcal{X}$)

Since $|\mathcal{A}| \leq n/4$ we have $|S \cup T| \leq n/2$.
Apply Cor 7 to β to get α which is
- well-behaved on $S \cup T$
- agrees with β on pigeons outside T
- satisfies $\mathcal{X}$

No monomial in $\mathcal{T}$ mentions pigeons in T (by construction) so α and β agree on $\mathcal{T}$.

For $m \in \mathcal{M} \setminus \mathcal{T}$, any β satisfying $\mathcal{B}$ must zero m – this is how the new commitments were constructed. Reassigning pigeons in T can change variables in m, but there is still at least one variable that is set to zero, zeroing the whole monomial. So for all $m \in \mathcal{M}$, α gives same value to m as does β. Hence $\mathbb{P}(\alpha) = \mathbb{P}(\beta)$

By Cor 7, α is well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$. Also, since α satisfies $\mathcal{X}$ as well as $N(\mathcal{T})$, α satisfies $\mathcal{A}$. Hence $\mathbb{P}(\alpha) = 0$.

Thus, any β that is well-behaved on and satisfies $\mathcal{B}$ must also satisfy $\mathbb{P}$. The lemma follows. $\boxed{\not{\square}}$

Let us make same kind of summary as for resolution in Lec 6

For PC/PCR, we have studied size, space and degree. Proved size and space LB

<u>Size vs degree</u>

Analogue of length vs width in resolution

Small degree ⇒ small size [CEI '96]

Small size ⇒ (reasonably) small degree [IPS '99]

Trade-offs ?

<u>Space vs degree</u>

Are there any nontrivial relations?

Is there an [AD08] style connection?

Nothing known. ?

<u>Size vs space</u>

Does small space imply small size as in resolution?

Does small size imply anything about space?

Are there any trade-offs?

Pretty much nothing known ?

But recent paper by [Huynh & Nordström '11] giving some indications as to what we might expect to hold.