Time-space trade-offs in proof complexity
Lecture 4

Jakob Nordström

KTH Royal Institute of Technology

17th Estonian Winter School in Computer Science
Palmse, Estonia
February 26 – March 2, 2012

Agenda for Final Lecture

- Finish proof of polynomial calculus space lower bound
- First spend quite some time recalling definitions and approach
- Then do proof modulo key technical result: Locality lemma
- Finally prove Locality lemma
- Wrap up course with some concluding remarks (if we're not desperately out of time)

Polynomial Calculus Resolution (PCR)

- Last time started studying polynomial calculus (PC)
- Annoying encoding problems led to introducting special variables for negated literals — polynomial calculus resolution (PCR)
- Axiom clauses of F interpreted as multilinear polynomials over variables $x, y, z, \ldots$ and (formally independent) $\overline{x}, \overline{y}, \overline{z}, \ldots$
- "Being true" corresponds to "evaluating to zero," so natural to flip convention and think of 0 as true and 1 as false
- Example: clause $x \vee y \vee \overline{z}$ gets translated to monomial $xy\overline{z}$
- To get unique representation, write polynomials as sums of monomials
- Prove F unsatisfiable by deriving 1 from monomials encoding axioms

Polynomial Calculus Resolution: Inference Rules

Lines in PCR refutation: multivariate polynomials $p \in \mathbb{F}[x, \overline{x}, y, \overline{y}, z, \overline{z}, \ldots]$ for some fixed field $\mathbb{F}$ (typically finite)

Derivation rules ($\alpha, \beta \in \mathbb{F}$, $p \in \mathbb{F}[x, \overline{x}, y, \overline{y}, z, \overline{z}, \ldots]$, x any variable):

Boolean axioms $\dfrac{}{x^2 - x}$

Complementarity axioms $\dfrac{}{x + \overline{x} - 1}$

Linear combination $\dfrac{p \qquad q}{\alpha p + \beta q}$

Multiplication $\dfrac{p}{xp}$

PCR-refutation ends when 1 is derived

All polynomials multilinear w.l.o.g. (follows from Boolean axioms)

Polynomial Calculus Resolution: Complexity Measures

PCR measures we cared about yesterday (and still care about today):

- **Size**
  Total # monomials in the refutation counted with repetitions
  (Analogue of length in resolution)

- **(Monomial) space**
  Maximal # monomials in any configuration counted with repetitions
  (Analogue of clause space in resolution)

In the best of worlds we want to:

- Prove upper bounds for PC (no variables $\overline{x}, \overline{y}, \overline{z}, \ldots$)
- Prove (matching) lower bounds for PCR

Size and Space Bounds for PC/PCR

$N =$ size of formula

Size: at most $\exp(\mathcal{O}(N))$ for PC for k-CNF formulas [Filmus et al. '12]
Matching lower bounds for PCR up to constant factors in exponent
e.g. [Alekhnovich & Razborov '01]

Space: at most $\mathcal{O}(N)$ for PC for k-CNF formulas [Filmus et al. '12]
No matching lower bounds!
Currently best bounds $\Omega\left(\sqrt[3]{N}\right)$ (for PC and PCR)

- Space lower bounds for wide formulas in [Alekhnovich et al. '00]
- Only recently shown for k-CNF formulas

For number of reasons (some of which we briefly mentioned),
prefer k-CNF formulas

PCR Space Lower Bounds for k-CNFs

Today, would like to prove first space lower bound for k-CNFs in polynomial calculus:

Theorem (Filmus, Lauria, Nordström, Thapen & Zewi '12)

There are k-CNF formulas F_N of size N s.t. $Sp_{\mathcal{PCR}}(F_N \vdash \perp) = \Omega(\sqrt[3]{N})$

Actually, will prove slightly weaker result:

Theorem (Filmus, Lauria, Nordström, Thapen & Zewi '12)

There are CNF formulas F_N of size N with clauses of width $\mathcal{O}(\log N)$ s.t. $Sp_{\mathcal{PCR}}(F_N \vdash \perp) = \Omega(\sqrt[3]{N/\log N})$

(But all key ingredients will be there in proofs)

PCR Space Lower Bounds for k-CNFs

Today, would like to prove first space lower bound for k-CNFs in polynomial calculus:

Theorem (Filmus, Lauria, Nordström, Thapen & Zewi '12)

There are k-CNF formulas F_N of size N s.t. $Sp_{\mathcal{PCR}}(F_N \vdash \bot) = \Omega\left(\sqrt[3]{N}\right)$

Actually, will prove slightly weaker result:

Theorem (Filmus, Lauria, Nordström, Thapen & Zewi '12)

There are CNF formulas F_N of size N with clauses of width $\mathcal{O}(\log N)$ s.t. $Sp_{\mathcal{PCR}}(F_N \vdash \bot) = \Omega\left(\sqrt[3]{N/\log N}\right)$

(But all key ingredients will be there in proofs)

Bitwise Pigeonhole Principle Formula $BPHP^m_n$

$$x^b = \begin{cases} x & \text{if } b = 0 \\ \overline{x} & \text{if } b = 1 \end{cases}$$ (x^b is true if and only if $x = b$)

$[0, j) = \{0, 1, \ldots, j-1\}$ (will index pigeons and holes starting from 0)

$n = 2^\ell$ (only consider even powers of 2 for # holes)

Variables $x[p, i]$ for each $p \in [0, m)$ and $i \in [0, \ell)$

Pigeon p sent to hole $x[p, \ell-1] \cdots x[p, 1]x[p, 0]$ (in binary encoding)

For all $p \neq q \in [0, m)$, $h = h_{\ell-1} \cdots h_0 \in [0, n)$, hole axiom

$$H(p, q, h) = \bigvee_{i=0}^{\ell-1} x[p, i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q, i]^{1-h_i}$$

"Have $m > n$ integers between 0 and $n - 1$ and they're all distinct"

Bitwise Pigeonhole Principle Formula $BPHP^m_n$

$$x^b = \begin{cases} x & \text{if } b = 0 \\ \overline{x} & \text{if } b = 1 \end{cases}$$ (x^b is true if and only if $x = b$)

$[0, j) = \{0, 1, \ldots, j-1\}$ (will index pigeons and holes starting from 0)

$n = 2^\ell$ (only consider even powers of 2 for # holes)

Variables $x[p, i]$ for each $p \in [0, m)$ and $i \in [0, \ell)$

Pigeon p sent to hole $x[p, \ell-1] \cdots x[p, 1]x[p, 0]$ (in binary encoding)

For all $p \neq q \in [0, m)$, $h = h_{\ell-1} \cdots h_0 \in [0, n)$, hole axiom

$$H(p, q, h) = \bigvee_{i=0}^{\ell-1} x[p, i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q, i]^{1-h_i}$$

"Have $m > n$ integers between 0 and $n-1$ and they're all distinct"

Bitwise Pigeonhole Principle Formula $BPHP^m_n$

$$x^b = \begin{cases} x & \text{if } b = 0 \\ \overline{x} & \text{if } b = 1 \end{cases} \qquad (x^b \text{ is true if and only if } x = b)$$

$[0, j) = \{0, 1, \ldots, j - 1\}$ (will index pigeons and holes starting from 0)

$n = 2^\ell$ (only consider even powers of 2 for # holes)

Variables $x[p, i]$ for each $p \in [0, m)$ and $i \in [0, \ell)$

Pigeon p sent to hole $x[p, \ell-1] \cdots x[p, 1] x[p, 0]$ (in binary encoding)

For all $p \neq q \in [0, m)$, $h = h_{\ell-1} \cdots h_0 \in [0, n)$, hole axiom

$$H(p, q, h) = \bigvee_{i=0}^{\ell-1} x[p, i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q, i]^{1-h_i}$$

"Have $m > n$ integers between 0 and $n - 1$ and they're all distinct"

Outline of Proof of PCR Space Lower Bound

Theorem

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

Proof method: For $\pi = \{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ with $Sp(\pi) \leq n/8$, construct "auxiliary configurations" $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_\tau$ such that

- $\mathcal{A}_t$ highly structured, so easier to understand than $\mathbb{P}_t$
- but still gives information about $\mathbb{P}_t$

Maintain invariants for $\mathcal{A}_t$:

1. $\mathcal{A}_t$ implies $\mathbb{P}_t$ (i.e., $\mathcal{A}_t$ "stronger" than $\mathbb{P}_t$)
2. $\mathcal{A}_t$ is satisfiable (so, in particular, $\mathbb{P}_t$ also satisfiable)
3. For $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$, can do update $\mathcal{A}_t \rightsquigarrow \mathcal{A}_{t+1}$ if $Sp(\mathbb{P}_t) \leq n/8$

So small-space derivation doesn't derive contradiction

Outline of Proof of PCR Space Lower Bound

Theorem

$Sp_{\mathcal{PCR}}(BPHP^m_n \vdash \bot) > n/8$

Proof method: For $\pi = \{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ with $Sp(\pi) \leq n/8$, construct "auxiliary configurations" $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_\tau$ such that

- $\mathcal{A}_t$ highly structured, so easier to understand than $\mathbb{P}_t$
- but still gives information about $\mathbb{P}_t$

Maintain invariants for $\mathcal{A}_t$:

1. $\mathcal{A}_t$ implies $\mathbb{P}_t$ (i.e., $\mathcal{A}_t$ "stronger" than $\mathbb{P}_t$)
2. $\mathcal{A}_t$ is satisfiable (so, in particular, $\mathbb{P}_t$ also satisfiable)
3. For $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$, can do update $\mathcal{A}_t \rightsquigarrow \mathcal{A}_{t+1}$ if $Sp(\mathbb{P}_t) \leq n/8$

So small-space derivation doesn't derive contradiction

Outline of Proof of PCR Space Lower Bound

Theorem

$Sp_{\mathcal{PCR}}(BPHP^m_n \vdash \bot) > n/8$

Proof method: For $\pi = \{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ with $Sp(\pi) \leq n/8$, construct "auxiliary configurations" $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_\tau$ such that

- $\mathcal{A}_t$ highly structured, so easier to understand than $\mathbb{P}_t$
- but still gives information about $\mathbb{P}_t$

Maintain invariants for $\mathcal{A}_t$:

1. $\mathcal{A}_t$ implies $\mathbb{P}_t$ (i.e., $\mathcal{A}_t$ "stronger" than $\mathbb{P}_t$)
2. $\mathcal{A}_t$ is satisfiable (so, in particular, $\mathbb{P}_t$ also satisfiable)
3. For $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$, can do update $\mathcal{A}_t \rightsquigarrow \mathcal{A}_{t+1}$ if $Sp(\mathbb{P}_t) \leq n/8$

So small-space derivation doesn't derive contradiction

Outline of Proof of PCR Space Lower Bound

Theorem

$Sp_{\mathcal{PCR}}(BPHP^m_n \vdash \perp) > n/8$

Proof method: For $\pi = \{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ with $Sp(\pi) \leq n/8$, construct "auxiliary configurations" $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_\tau$ such that

- $\mathcal{A}_t$ highly structured, so easier to understand than $\mathbb{P}_t$
- but still gives information about $\mathbb{P}_t$

Maintain invariants for $\mathcal{A}_t$:

1. $\mathcal{A}_t$ implies $\mathbb{P}_t$ (i.e., $\mathcal{A}_t$ "stronger" than $\mathbb{P}_t$)
2. $\mathcal{A}_t$ is satisfiable (so, in particular, $\mathbb{P}_t$ also satisfiable)
3. For $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$, can do update $\mathcal{A}_t \rightsquigarrow \mathcal{A}_{t+1}$ if $Sp(\mathbb{P}_t) \leq n/8$

So small-space derivation doesn't derive contradiction

Outline of Proof of PCR Space Lower Bound

Theorem

$Sp_{\mathcal{PCR}}(BPHP^m_n \vdash \bot) > n/8$

Proof method: For $\pi = \{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ with $Sp(\pi) \leq n/8$, construct "auxiliary configurations" $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_\tau$ such that

- $\mathcal{A}_t$ highly structured, so easier to understand than $\mathbb{P}_t$
- but still gives information about $\mathbb{P}_t$

Maintain invariants for $\mathcal{A}_t$:

1. $\mathcal{A}_t$ implies $\mathbb{P}_t$ (i.e., $\mathcal{A}_t$ "stronger" than $\mathbb{P}_t$)
2. $\mathcal{A}_t$ is satisfiable (so, in particular, $\mathbb{P}_t$ also satisfiable)
3. For $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$, can do update $\mathcal{A}_t \rightsquigarrow \mathcal{A}_{t+1}$ if $Sp(\mathbb{P}_t) \leq n/8$

So small-space derivation doesn't derive contradiction

Outline of Proof of PCR Space Lower Bound

Theorem

$Sp_{\mathcal{PCR}}(BPHP^m_n \vdash \bot) > n/8$

Proof method: For $\pi = \{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ with $Sp(\pi) \leq n/8$, construct "auxiliary configurations" $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_\tau$ such that

- $\mathcal{A}_t$ highly structured, so easier to understand than $\mathbb{P}_t$
- but still gives information about $\mathbb{P}_t$

Maintain invariants for $\mathcal{A}_t$:

1. $\mathcal{A}_t$ implies $\mathbb{P}_t$ (i.e., $\mathcal{A}_t$ "stronger" than $\mathbb{P}_t$)
2. $\mathcal{A}_t$ is satisfiable (so, in particular, $\mathbb{P}_t$ also satisfiable)
3. For $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$, can do update $\mathcal{A}_t \rightsquigarrow \mathcal{A}_{t+1}$ if $Sp(\mathbb{P}_t) \leq n/8$

So small-space derivation doesn't derive contradiction

Outline of Proof of PCR Space Lower Bound

Theorem

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

Proof method: For $\pi = \{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau\}$ with $Sp(\pi) \leq n/8$, construct "auxiliary configurations" $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_\tau$ such that

- $\mathcal{A}_t$ highly structured, so easier to understand than $\mathbb{P}_t$
- but still gives information about $\mathbb{P}_t$

Maintain invariants for $\mathcal{A}_t$:

1. $\mathcal{A}_t$ implies $\mathbb{P}_t$ (i.e., $\mathcal{A}_t$ "stronger" than $\mathbb{P}_t$)
2. $\mathcal{A}_t$ is satisfiable (so, in particular, $\mathbb{P}_t$ also satisfiable)
3. For $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$, can do update $\mathcal{A}_t \rightsquigarrow \mathcal{A}_{t+1}$ if $Sp(\mathbb{P}_t) \leq n/8$

So small-space derivation doesn't derive contradiction

Commitment Sets

(Disjunctive) commitment

- 2-clause of the form $C = x[p,i]^b \lor x[q,j]^c$
- Pigeons $p \neq q$ distinct
- No restrictions on $i, j \in [0, l)$, $b, c \in \{0, 1\}$
- Domain $\mathrm{dom}(C)$ = set of pigeons $\{p, q\}$ mentioned in C

Commitment set

- $\mathcal{A} = \{C_1, C_2, \ldots, C_s\}$ — think of $\mathcal{A}_t$ as 2-CNF formula
- For all $i \neq j$, $\mathrm{dom}(C_i) \cap \mathrm{dom}(C_j) = \emptyset$
  (i.e., all pigeons mentioned are distinct)
- $\mathrm{dom}(\mathcal{A}) = \bigcup_{C \in \mathcal{A}} \mathrm{dom}(C)$
- Size $|\mathcal{A}|$ = number of commitments in $\mathcal{A}$

Commitment Sets

(Disjunctive) commitment

- 2-clause of the form $C = x[p,i]^b \vee x[q,j]^c$
- Pigeons $p \neq q$ distinct
- No restrictions on $i, j \in [0, l)$, $b, c \in \{0, 1\}$
- Domain $\mathrm{dom}(C)$ = set of pigeons $\{p, q\}$ mentioned in C

Commitment set

- $\mathcal{A} = \{C_1, C_2, \ldots, C_s\}$ — think of $\mathcal{A}_t$ as 2-CNF formula
- For all $i \neq j$, $\mathrm{dom}(C_i) \cap \mathrm{dom}(C_j) = \emptyset$
  (i.e., all pigeons mentioned are distinct)
- $\mathrm{dom}(\mathcal{A}) = \bigcup_{C \in \mathcal{A}} \mathrm{dom}(C)$
- Size $|\mathcal{A}|$ = number of commitments in $\mathcal{A}$

Commitment Sets Implying PC-configurations

Any (total) assignment α to $Vars(BPHP_n^m)$ defines function $f_\alpha : [0, m) \to [0, n)$ — in what follows, identify α and f_α

A (total) assignment α to $Vars(BPHP_n^m)$ is well-behaved over set of pigeons $S \subseteq [0, m)$ if it sends pigeons in S to distinct holes

An assignment α is well-behaved on and satisfies commitment set $\mathcal{A}$ if

- α well-behaved on dom($\mathcal{A}$)
  (defines partial matching for all pigeons $\mathcal{A}$ mentions)
- α satisfies $\mathcal{A}$

Definition (Entailment)

$\mathcal{A}$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment α which is well-behaved on and satisfies $\mathcal{A}$ must also satisfy $\mathbb{P}$ (i.e., for every polynomial $P \in \mathbb{P}$ have $P(\alpha) = 0$)

Commitment Sets Implying PC-configurations

Any (total) assignment α to $Vars(BPHP_n^m)$ defines function $f_\alpha : [0, m) \to [0, n)$ — in what follows, identify α and f_α

A (total) assignment α to $Vars(BPHP_n^m)$ is well-behaved over set of pigeons $S \subseteq [0, m)$ if it sends pigeons in S to distinct holes

An assignment α is well-behaved on and satisfies commitment set $\mathcal{A}$ if

- α well-behaved on dom($\mathcal{A}$) (defines partial matching for all pigeons $\mathcal{A}$ mentions)
- α satisfies $\mathcal{A}$

Definition (Entailment)

$\mathcal{A}$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment α which is well-behaved on and satisfies $\mathcal{A}$ must also satisfy $\mathbb{P}$ (i.e., for every polynomial $P \in \mathbb{P}$ have $P(\alpha) = 0$)

Commitment Sets Implying PC-configurations

Any (total) assignment α to $Vars(BPHP^m_n)$ defines function $f_\alpha : [0, m) \to [0, n)$ — in what follows, identify α and f_α

A (total) assignment α to $Vars(BPHP^m_n)$ is well-behaved over set of pigeons $S \subseteq [0, m)$ if it sends pigeons in S to distinct holes

An assignment α is well-behaved on and satisfies commitment set $\mathcal{A}$ if

- α well-behaved on dom($\mathcal{A}$)
  (defines partial matching for all pigeons $\mathcal{A}$ mentions)
- α satisfies $\mathcal{A}$

Definition (Entailment)

$\mathcal{A}$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment α which is well-behaved on and satisfies $\mathcal{A}$ must also satisfy $\mathbb{P}$ (i.e., for every polynomial $P \in \mathbb{P}$ have $P(\alpha) = 0$)

Commitment Sets Implying PC-configurations

Any (total) assignment α to $Vars(BPHP^m_n)$ defines function $f_\alpha : [0, m) \to [0, n)$ — in what follows, identify α and f_α

A (total) assignment α to $Vars(BPHP^m_n)$ is well-behaved over set of pigeons $S \subseteq [0, m)$ if it sends pigeons in S to distinct holes

An assignment α is well-behaved on and satisfies commitment set $\mathcal{A}$ if

- α well-behaved on dom$(\mathcal{A})$
  (defines partial matching for all pigeons $\mathcal{A}$ mentions)
- α satisfies $\mathcal{A}$

Definition (Entailment)

$\mathcal{A}$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment α which is well-behaved on and satisfies $\mathcal{A}$ must also satisfy $\mathbb{P}$ (i.e., for every polynomial $P \in \mathbb{P}$ have $P(\alpha) = 0$)

Proof of Space Lower Bound for PCR

Fact: Any commitment set $\mathcal{A}_t$ satisfiable by well-behaved assignment (requires a proof; assume it for now)

Proof invariants:

- $\mathcal{A}_t$ entails $\mathbb{P}_t$ over well-behaved assignments
- $|\mathcal{A}_t| \leq 2 \cdot Sp(\mathbb{P}_t)$

Proof is by case analysis over derivation step $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$:

Download of polynomial encoding

1. Boolean or Complementarity axiom
2. axiom clause $H(p, q, h)$ of $BPHP^m_n$

Inference of polynomial Q from $\mathbb{P}_t$

Erasure of polynomial $Q \in \mathbb{P}_t$

Proof of Space Lower Bound for PCR

Fact: Any commitment set $\mathcal{A}_t$ satisfiable by well-behaved assignment (requires a proof; assume it for now)

Proof invariants:

- $\mathcal{A}_t$ entails $\mathbb{P}_t$ over well-behaved assignments
- $|\mathcal{A}_t| \leq 2 \cdot Sp(\mathbb{P}_t)$

Proof is by case analysis over derivation step $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$:

Download of polynomial encoding

1. Boolean or Complementarity axiom
2. axiom clause $H(p, q, h)$ of $BPHP^m_n$

Inference of polynomial Q from $\mathbb{P}_t$

Erasure of polynomial $Q \in \mathbb{P}_t$

Proof of Space Lower Bound for PCR

Fact: Any commitment set $\mathcal{A}_t$ satisfiable by well-behaved assignment (requires a proof; assume it for now)

Proof invariants:

- $\mathcal{A}_t$ entails $\mathbb{P}_t$ over well-behaved assignments
- $|\mathcal{A}_t| \leq 2 \cdot Sp(\mathbb{P}_t)$

Proof is by case analysis over derivation step $\mathbb{P}_t \rightsquigarrow \mathbb{P}_{t+1}$:

Download of polynomial encoding

1. Boolean or Complementarity axiom
2. axiom clause $H(p, q, h)$ of $BPHP^m_n$

Inference of polynomial Q from $\mathbb{P}_t$

Erasure of polynomial $Q \in \mathbb{P}_t$

Case 1: Download

Complementarity axiom $x + \overline{x} - 1$ or Boolean axiom $x^2 - x$:
Set $\mathcal{A}_{t+1} = \mathcal{A}_t$

Hole axiom $H(p,q,h) = \bigvee_{i=0}^{\ell-1} x[p,i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q,i]^{1-h_i}$:

1. $\{p,q\} \subseteq \mathrm{dom}(\mathcal{A}_t)$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t$; any well-behaved α sends pigeons p and q to distinct holes $\Rightarrow$ satisfies $H(p,q,h)$

2. $\{p,q\} \cap \mathrm{dom}(\mathcal{A}_t) = \emptyset$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$ for $C = x[p,0]^{1-h_0} \vee x[q,0]^{1-h_0}$

3. $p \in \mathrm{dom}(\mathcal{A}_t), q \notin \mathrm{dom}(\mathcal{A}_t)$: Pick "dummy" $p^* \notin \mathrm{dom}(\mathcal{A}_t) \cup \{q\}$; let $C = x[q,0]^{1-h_0} \vee x[p^*,0]^0$; set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$.
Well-behaved α gives p and q distinct holes $\Rightarrow$ satisfies $H(p,q,h)$

Space increases by ≥ 1 and never add more than $1 < 2$ commitments $\Rightarrow$ $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$

Case 1: Download

Complementarity axiom $x + \overline{x} - 1$ or Boolean axiom $x^2 - x$:
Set $\mathcal{A}_{t+1} = \mathcal{A}_t$

Hole axiom $H(p, q, h) = \bigvee_{i=0}^{\ell-1} x[p, i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q, i]^{1-h_i}$:

1. $\{p, q\} \subseteq \mathrm{dom}(\mathcal{A}_t)$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t$; any well-behaved α sends pigeons p and q to distinct holes $\Rightarrow$ satisfies $H(p, q, h)$
2. $\{p, q\} \cap \mathrm{dom}(\mathcal{A}_t) = \emptyset$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$ for $C = x[p, 0]^{1-h_0} \vee x[q, 0]^{1-h_0}$
3. $p \in \mathrm{dom}(\mathcal{A}_t), q \notin \mathrm{dom}(\mathcal{A}_t)$: Pick "dummy" $p^* \notin \mathrm{dom}(\mathcal{A}_t) \cup \{q\}$; let $C = x[q, 0]^{1-h_0} \vee x[p^*, 0]^0$; set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$. Well-behaved α gives p and q distinct holes $\Rightarrow$ satisfies $H(p, q, h)$

Space increases by ≥ 1 and never add more than $1 < 2$ commitments $\Rightarrow$ $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$

Case 1: Download

Complementarity axiom $x + \overline{x} - 1$ or Boolean axiom $x^2 - x$:
Set $\mathcal{A}_{t+1} = \mathcal{A}_t$

Hole axiom $H(p,q,h) = \bigvee_{i=0}^{\ell-1} x[p,i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q,i]^{1-h_i}$:

1. $\{p,q\} \subseteq \mathrm{dom}(\mathcal{A}_t)$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t$; any well-behaved α sends pigeons p and q to distinct holes $\Rightarrow$ satisfies $H(p,q,h)$
2. $\{p,q\} \cap \mathrm{dom}(\mathcal{A}_t) = \emptyset$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$ for $C = x[p,0]^{1-h_0} \vee x[q,0]^{1-h_0}$
3. $p \in \mathrm{dom}(\mathcal{A}_t), q \notin \mathrm{dom}(\mathcal{A}_t)$: Pick "dummy" $p^* \notin \mathrm{dom}(\mathcal{A}_t) \cup \{q\}$; let $C = x[q,0]^{1-h_0} \vee x[p^*,0]^0$; set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$. Well-behaved α gives p and q distinct holes $\Rightarrow$ satisfies $H(p,q,h)$

Space increases by ≥ 1 and never add more than $1 < 2$ commitments $\Rightarrow$ $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$

Case 1: Download

Complementarity axiom $x + \overline{x} - 1$ or Boolean axiom $x^2 - x$:
Set $\mathcal{A}_{t+1} = \mathcal{A}_t$

Hole axiom $H(p,q,h) = \bigvee_{i=0}^{\ell-1} x[p,i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q,i]^{1-h_i}$:

1. $\{p,q\} \subseteq \mathrm{dom}(\mathcal{A}_t)$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t$; any well-behaved α sends pigeons p and q to distinct holes $\Rightarrow$ satisfies $H(p,q,h)$
2. $\{p,q\} \cap \mathrm{dom}(\mathcal{A}_t) = \emptyset$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$ for $C = x[p,0]^{1-h_0} \vee x[q,0]^{1-h_0}$
3. $p \in \mathrm{dom}(\mathcal{A}_t), q \notin \mathrm{dom}(\mathcal{A}_t)$: Pick "dummy" $p^* \notin \mathrm{dom}(\mathcal{A}_t) \cup \{q\}$; let $C = x[q,0]^{1-h_0} \vee x[p^*,0]^0$; set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$. Well-behaved α gives p and q distinct holes $\Rightarrow$ satisfies $H(p,q,h)$

Space increases by ≥ 1 and never add more than $1 < 2$ commitments $\Rightarrow$ $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$

Case 1: Download

Complementarity axiom $x + \overline{x} - 1$ or Boolean axiom $x^2 - x$:
Set $\mathcal{A}_{t+1} = \mathcal{A}_t$

Hole axiom $H(p, q, h) = \bigvee_{i=0}^{\ell-1} x[p, i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q, i]^{1-h_i}$:

1. $\{p, q\} \subseteq \mathrm{dom}(\mathcal{A}_t)$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t$; any well-behaved α sends pigeons p and q to distinct holes $\Rightarrow$ satisfies $H(p, q, h)$
2. $\{p, q\} \cap \mathrm{dom}(\mathcal{A}_t) = \emptyset$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$ for $C = x[p, 0]^{1-h_0} \vee x[q, 0]^{1-h_0}$
3. $p \in \mathrm{dom}(\mathcal{A}_t), q \notin \mathrm{dom}(\mathcal{A}_t)$: Pick "dummy" $p^* \notin \mathrm{dom}(\mathcal{A}_t) \cup \{q\}$; let $C = x[q, 0]^{1-h_0} \vee x[p^*, 0]^0$; set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$. Well-behaved α gives p and q distinct holes $\Rightarrow$ satisfies $H(p, q, h)$

Space increases by ≥ 1 and never add more than $1 < 2$ commitments $\Rightarrow$ $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$

Case 1: Download

Complementarity axiom $x + \overline{x} - 1$ or Boolean axiom $x^2 - x$:
Set $\mathcal{A}_{t+1} = \mathcal{A}_t$

Hole axiom $H(p,q,h) = \bigvee_{i=0}^{\ell-1} x[p,i]^{1-h_i} \vee \bigvee_{i=0}^{\ell-1} x[q,i]^{1-h_i}$:

1. $\{p,q\} \subseteq \mathrm{dom}(\mathcal{A}_t)$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t$; any well-behaved α sends pigeons p and q to distinct holes $\Rightarrow$ satisfies $H(p,q,h)$
2. $\{p,q\} \cap \mathrm{dom}(\mathcal{A}_t) = \emptyset$: Set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$ for $C = x[p,0]^{1-h_0} \vee x[q,0]^{1-h_0}$
3. $p \in \mathrm{dom}(\mathcal{A}_t), q \notin \mathrm{dom}(\mathcal{A}_t)$: Pick "dummy" $p^* \notin \mathrm{dom}(\mathcal{A}_t) \cup \{q\}$; let $C = x[q,0]^{1-h_0} \vee x[p^*,0]^0$; set $\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}$.
   Well-behaved α gives p and q distinct holes $\Rightarrow$ satisfies $H(p,q,h)$

Space increases by ≥ 1 and never add more than $1 < 2$ commitments $\Rightarrow$ $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$

Case 2: Inference

- $\mathbb{P}_{t+1} = \mathbb{P}_t \cup \{Q\}$ for polynomial Q derived from $\mathbb{P}$
- Set $\mathcal{A}_{t+1} = \mathcal{A}_t$
- PCR is sound $\Rightarrow Q$ implied by $\mathbb{P}_t$
- I.e., if for all $P \in \mathbb{P}_t$ have that $P(\alpha) = 0$, then $Q(\alpha) = 0$ also holds
- All well-behaved α satisfying $\mathcal{A}_{t+1} = \mathcal{A}_t$ must satisfy $\mathbb{P}_t$ by the induction hypothesis and hence also Q, so all of $\mathbb{P}_{t+1}$ is satisfied
- Space increases but size of commitment set unchanged $\Rightarrow$ $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$

Case 3: Erasure

- $\mathbb{P}_{t+1} = \mathbb{P}_t \setminus \{Q\}$ for $Q \in \mathbb{P}_t$
- Know $\mathcal{A}_t$ entails $\mathbb{P}_{t+1} \subseteq \mathbb{P}_t$
- But $|\mathcal{A}_t|$ may be far too large if Q contains lots of monomials
- Need to find smaller commitment set that still entails $\mathbb{P}_{t+1}$
  (Was very easy for resolution; now not clear at all what to do)

Lemma (Locality lemma for PCR)

Suppose

- *$\mathcal{A}$ commitment set*
- *$\mathbb{P}$ PCR-configuration*
- *$\mathcal{A}$ entails $\mathbb{P}$ over well-behaved assignments*

Then $\exists$ 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

Case 3: Erasure

- $\mathbb{P}_{t+1} = \mathbb{P}_t \setminus \{Q\}$ for $Q \in \mathbb{P}_t$
- Know $\mathcal{A}_t$ entails $\mathbb{P}_{t+1} \subseteq \mathbb{P}_t$
- But $|\mathcal{A}_t|$ may be far too large if Q contains lots of monomials
- Need to find smaller commitment set that still entails $\mathbb{P}_{t+1}$
  (Was very easy for resolution; now not clear at all what to do)

Lemma (Locality lemma for PCR)

Suppose

- *$\mathcal{A}$ commitment set*
- *$\mathbb{P}$ PCR-configuration*
- *$\mathcal{A}$ entails $\mathbb{P}$ over well-behaved assignments*

Then $\exists$ 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

Case 3: Erasure

- $\mathbb{P}_{t+1} = \mathbb{P}_t \setminus \{Q\}$ for $Q \in \mathbb{P}_t$
- Know $\mathcal{A}_t$ entails $\mathbb{P}_{t+1} \subseteq \mathbb{P}_t$
- But $|\mathcal{A}_t|$ may be far too large if Q contains lots of monomials
- Need to find smaller commitment set that still entails $\mathbb{P}_{t+1}$
(Was very easy for resolution; now not clear at all what to do)

Lemma (Locality lemma for PCR)

Suppose

- *$\mathcal{A}$ commitment set*
- *$\mathbb{P}$ PCR-configuration*
- *$\mathcal{A}$ entails $\mathbb{P}$ over well-behaved assignments*

Then $\exists$ 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

Case 3: Erasure

- $\mathbb{P}_{t+1} = \mathbb{P}_t \setminus \{Q\}$ for $Q \in \mathbb{P}_t$
- Know $\mathcal{A}_t$ entails $\mathbb{P}_{t+1} \subseteq \mathbb{P}_t$
- But $|\mathcal{A}_t|$ may be far too large if Q contains lots of monomials
- Need to find smaller commitment set that still entails $\mathbb{P}_{t+1}$
  (Was very easy for resolution; now not clear at all what to do)

Lemma (Locality lemma for PCR)

Suppose

- *$\mathcal{A}$ commitment set*
- *$\mathbb{P}$ PCR-configuration*
- *$\mathcal{A}$ entails $\mathbb{P}$ over well-behaved assignments*

Then $\exists$ 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

Case 3: Erasure

- $\mathbb{P}_{t+1} = \mathbb{P}_t \setminus \{Q\}$ for $Q \in \mathbb{P}_t$
- Know $\mathcal{A}_t$ entails $\mathbb{P}_{t+1} \subseteq \mathbb{P}_t$
- But $|\mathcal{A}_t|$ may be far too large if Q contains lots of monomials
- Need to find smaller commitment set that still entails $\mathbb{P}_{t+1}$
  (Was very easy for resolution; now not clear at all what to do)

Lemma (Locality lemma for PCR)

Suppose

- *$\mathcal{A}$ commitment set*
- *$\mathbb{P}$ PCR-configuration*
- *$\mathcal{A}$ entails $\mathbb{P}$ over well-behaved assignments*

Then $\exists$ 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

End of Proof. . . Except for the Hard Part

- This completes the proof of the PCR space lower bound
- . . . modulo two assumptions
- Assumption 1: Commitment sets are satisfiable by well-behaved assignments (easy)
- Assumption 2: Locality lemma takes care of erasure case (harder)
- Let's stop beating around the bush and prove Locality lemma (and get satisfiability of commitment sets for free)

A Simple But Important Technical Lemma

Lemma

Given

- *any set* $S \subseteq [0, m), |S| < n/2$,
- *any assignment* β *well-behaved on* S,
- *any literal* $x[p, i]^b$ *associated to pigeon* $p \notin S$,

can modify β *to* α *by reassigning variables associated to pigeon* p *so that* α *is well-behaved on* $S \cup \{p\}$ *and satisfies* $x[p, i]^b$

Proof.

- Exactly half of n holes have binary expansion with ith bit $= b$
- Pigeons in S use less than $n/2$ holes (as assigned by β)
- Hence by counting $\exists$ hole h not assigned to any pigeon in S and having the right value of ith bit
- Modifying β by sending pigeon p to hole h satisfies $x[p, i]^b$ $\square$

A Simple But Important Technical Lemma

Lemma

Given

- *any set* $S \subseteq [0, m), |S| < n/2$,
- *any assignment* β *well-behaved on* S,
- *any literal* $x[p, i]^b$ *associated to pigeon* $p \notin S$,

can modify β *to* α *by reassigning variables associated to pigeon* p *so that* α *is well-behaved on* $S \cup \{p\}$ *and satisfies* $x[p, i]^b$

Proof.

- Exactly half of n holes have binary expansion with ith bit $= b$
- Pigeons in S use less than $n/2$ holes (as assigned by β)
- Hence by counting $\exists$ hole h not assigned to any pigeon in S and having the right value of ith bit
- Modifying β by sending pigeon p to hole h satisfies $x[p, i]^b$ □

A Simple But Important Technical Lemma

Lemma

Given

- *any set* $S \subseteq [0, m), |S| < n/2$,
- *any assignment* β *well-behaved on* S,
- *any literal* $x[p, i]^b$ *associated to pigeon* $p \notin S$,

can modify β *to* α *by reassigning variables associated to pigeon* p *so that* α *is well-behaved on* $S \cup \{p\}$ *and satisfies* $x[p, i]^b$

Proof.

- Exactly half of n holes have binary expansion with ith bit $= b$
- Pigeons in S use less than $n/2$ holes (as assigned by β)
- Hence by counting $\exists$ hole h not assigned to any pigeon in S and having the right value of ith bit
- Modifying β by sending pigeon p to hole h satisfies $x[p, i]^b$ □

An Even Simpler But Even More Important Corollary

Corollary

Given

- *any sets* $S, T \subseteq [0, m)$ *s.t.* $S \cap T = \emptyset$ *and* $|S \cup T| \leq n/2$,
- *any assignment* β *well-behaved on* S,
- *any set* X *of* **exactly** *one literal* $x[p, i_p]^{b_p}$ *for every* $p \in T$,

can modify β *to* α *by reassigning variables associated to pigeons in* T *so that* α *is well-behaved on* $S \cup T$ *and satisfies all literals in* X

Proof.

Consider pigeons in T one by one and apply Lemma □

In particular, proves that any commitment set $\mathcal{A}$ of size $|\mathcal{A}| \leq n/4$ is satisfiable by well-behaved assignment
(Let $S = \emptyset$, $T = \mathrm{dom}(\mathcal{A})$, $X = Lit(\mathcal{A})$ and apply Corollary)

An Even Simpler But Even More Important Corollary

Corollary

Given

- *any sets* $S, T \subseteq [0, m)$ *s.t.* $S \cap T = \emptyset$ *and* $|S \cup T| \leq n/2$,
- *any assignment* β *well-behaved on* S,
- *any set* X *of* **exactly** *one literal* $x[p, i_p]^{b_p}$ *for every* $p \in T$,

can modify β *to* α *by reassigning variables associated to pigeons in* T *so that* α *is well-behaved on* $S \cup T$ *and satisfies all literals in* X

Proof.

Consider pigeons in T one by one and apply Lemma □

In particular, proves that any commitment set $\mathcal{A}$ of size $|\mathcal{A}| \leq n/4$ is satisfiable by well-behaved assignment
(Let $S = \emptyset$, $T = \mathrm{dom}(\mathcal{A})$, $X = Lit(\mathcal{A})$ and apply Corollary)

An Even Simpler But Even More Important Corollary

Corollary

Given

- *any sets $S, T \subseteq [0, m)$ s.t. $S \cap T = \emptyset$ and $|S \cup T| \leq n/2$,*
- *any assignment β well-behaved on S,*
- *any set X of* **exactly** *one literal $x[p, i_p]^{b_p}$ for every $p \in T$,*

can modify β to α by reassigning variables associated to pigeons in T so that α is well-behaved on $S \cup T$ and satisfies all literals in X

Proof.

Consider pigeons in T one by one and apply Lemma □

In particular, proves that any commitment set $\mathcal{A}$ of size $|\mathcal{A}| \leq n/4$ is satisfiable by well-behaved assignment
(Let $S = \emptyset$, $T = \mathrm{dom}(\mathcal{A})$, $X = Lit(\mathcal{A})$ and apply Corollary)

An Even Simpler But Even More Important Corollary

Corollary

Given

- *any sets $S, T \subseteq [0, m)$ s.t. $S \cap T = \emptyset$ and $|S \cup T| \leq n/2$,*
- *any assignment β well-behaved on S,*
- *any set X of* **exactly** *one literal $x[p, i_p]^{b_p}$ for every $p \in T$,*

can modify β to α by reassigning variables associated to pigeons in T so that α is well-behaved on $S \cup T$ and satisfies all literals in X

Proof.

Consider pigeons in T one by one and apply Lemma $\square$

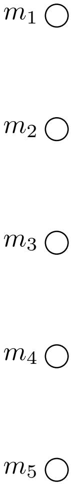
In particular, proves that any commitment set $\mathcal{A}$ of size $|\mathcal{A}| \leq n/4$ is satisfiable by well-behaved assignment
(Let $S = \emptyset$, $T = \mathrm{dom}(\mathcal{A})$, $X = Lit(\mathcal{A})$ and apply Corollary)

Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- $U =$ distinct monomials M in $\mathbb{P}$
- $V =$ commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\, S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow \exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)

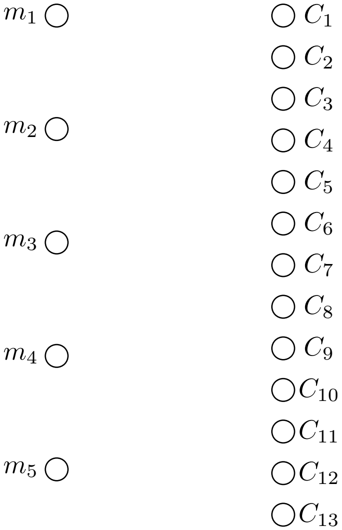
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\, S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow \exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



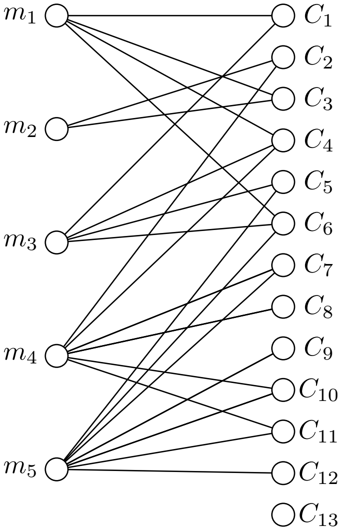
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow$ $\exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



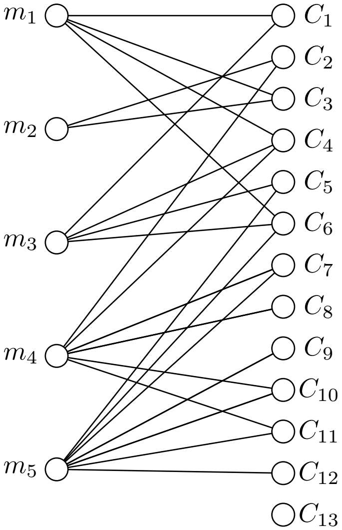
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow \exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



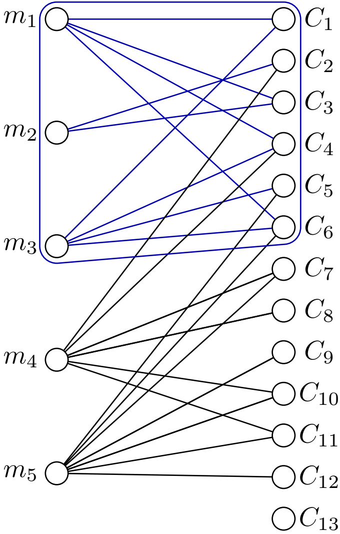
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- $U =$ distinct monomials M in $\mathbb{P}$
- $V =$ commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow \exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



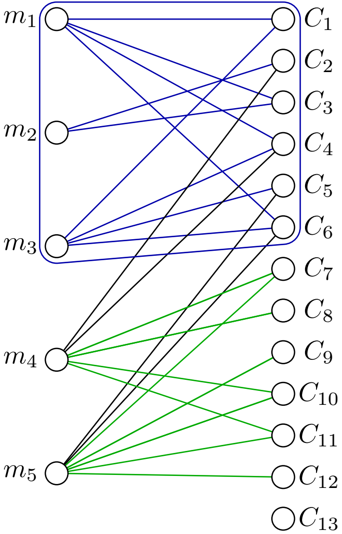
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- $U =$ distinct monomials M in $\mathbb{P}$
- $V =$ commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\, S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow$ $\exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



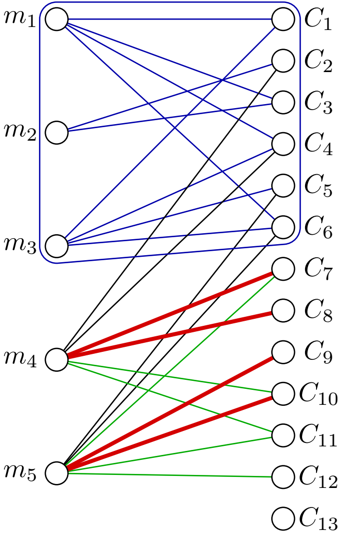
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow \exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



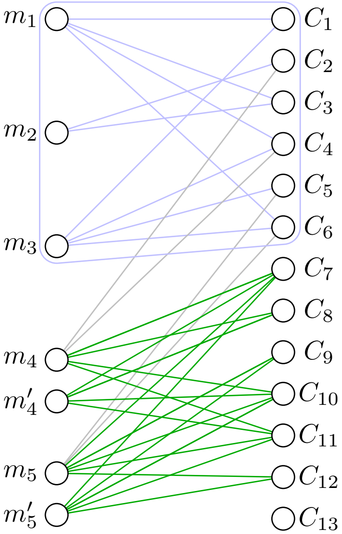
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\, S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow \exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



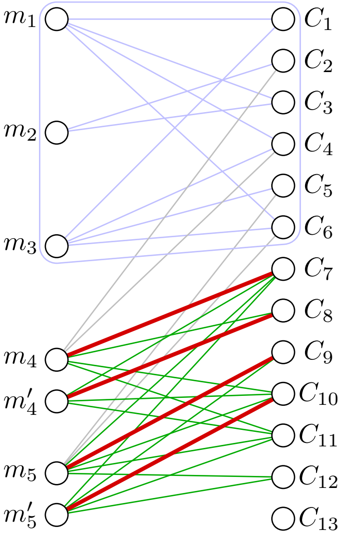
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- $U =$ distinct monomials M in $\mathbb{P}$
- $V =$ commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow$ $\exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



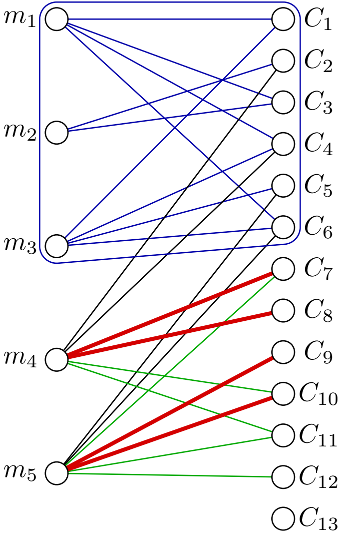
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow$ $\exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



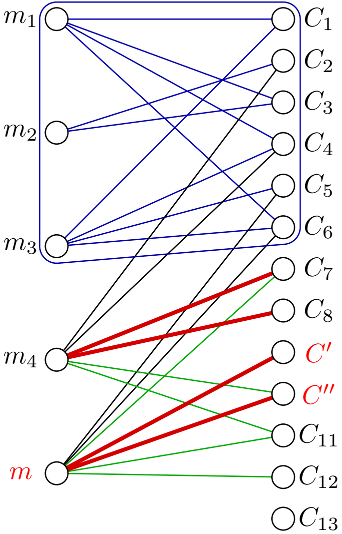
Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G=(U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow$ $\exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



Proof of Locality Lemma for PCR (1 / 4)

- Build bipartite graph $G = (U \cup V, E)$
- U = distinct monomials M in $\mathbb{P}$
- V = commitments in $\mathcal{A}$
- Edge between $m \in M$ and $C \in \mathcal{A}$ if $\exists$ pigeon p mentioned in both
- Let $\Gamma \subseteq M$ set of maximal size such that $|N(\Gamma)| \leq 2 \cdot |\Gamma|$
- Assume $\Gamma \neq M$ (else set $\mathcal{B} = N(\Gamma)$)
- $\forall\ S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow$ $\exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in \mathcal{A} \setminus N(\Gamma)$
- (Make 2 copies of each $m \in M \setminus \Gamma$ and apply Hall's theorem)



Proof of Locality Lemma for PCR (2 / 4)

Look at $m \in M \setminus \Gamma$

Matching commitments:

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

Suppose m mentions pigeons p' and p'' so that

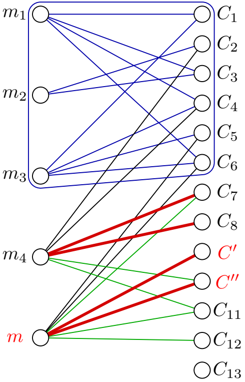
- $m = x[p', i_1]^{b_1} \cdot x[p'', i_2]^{b_2} \cdot m'$

(m can also mention q' and/or q'' — don't care)

Make new commitment $C_m = x[p', i_1]^{b_1} \lor x[p'', i_2]^{b_2}$

Let $\mathcal{B} = N(\Gamma) \cup \{C_m \mid m \in M \setminus \Gamma\}$

Done!



Proof of Locality Lemma for PCR (2 / 4)

Look at $m \in M \setminus \Gamma$

Matching commitments:

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

Suppose m mentions pigeons p' and p'' so that

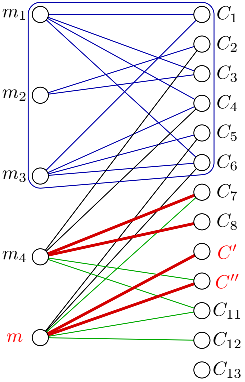
- $m = x[p', i_1]^{b_1} \cdot x[p'', i_2]^{b_2} \cdot m'$

(m can also mention q' and/or q'' — don't care)

Make new commitment $C_m = x[p', i_1]^{b_1} \vee x[p'', i_2]^{b_2}$

Let $\mathcal{B} = N(\Gamma) \cup \{C_m \mid m \in M \setminus \Gamma\}$

Done!



Proof of Locality Lemma for PCR (2 / 4)

Look at $m \in M \setminus \Gamma$

Matching commitments:

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

Suppose m mentions pigeons p' and p'' so that

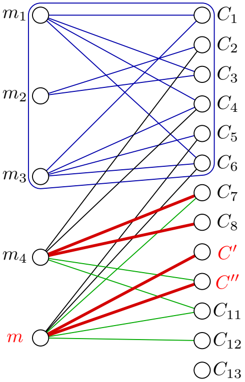
- $m = x[p', i_1]^{b_1} \cdot x[p'', i_2]^{b_2} \cdot m'$

(m can also mention q' and/or q'' — don't care)

Make new commitment $C_m = x[p', i_1]^{b_1} \lor x[p'', i_2]^{b_2}$

Let $\mathcal{B} = N(\Gamma) \cup \{C_m \mid m \in M \setminus \Gamma\}$

Done!



Proof of Locality Lemma for PCR (2 / 4)

Look at $m \in M \setminus \Gamma$

Matching commitments:

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

Suppose m mentions pigeons p' and p'' so that

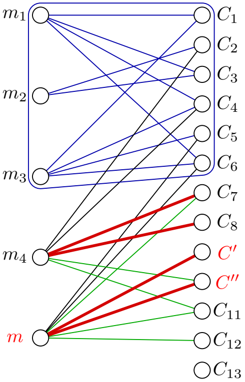
- $m = x[p', i_1]^{b_1} \cdot x[p'', i_2]^{b_2} \cdot m'$

(m can also mention q' and/or q'' — don't care)

Make new commitment $C_m = x[p', i_1]^{b_1} \vee x[p'', i_2]^{b_2}$

Let $\mathcal{B} = N(\Gamma) \cup \{C_m \mid m \in M \setminus \Gamma\}$

Done!



Proof of Locality Lemma for PCR (2 / 4)

Look at $m \in M \setminus \Gamma$

Matching commitments:

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

Suppose m mentions pigeons p' and p'' so that

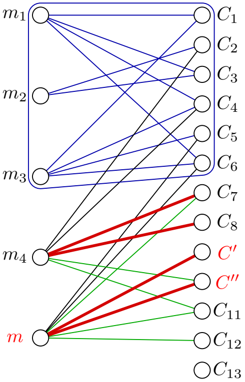
- $m = x[p', i_1]^{b_1} \cdot x[p'', i_2]^{b_2} \cdot m'$

(m can also mention q' and/or q'' — don't care)

Make new commitment $C_m = x[p', i_1]^{b_1} \vee x[p'', i_2]^{b_2}$

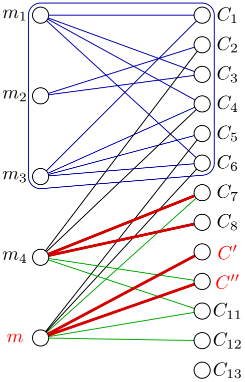
Let $\mathcal{B} = N(\Gamma) \cup \{C_m \mid m \in M \setminus \Gamma\}$

Done!



Need to prove three things:

1. $\mathcal{B}$ is a commitment set
   OK, all pigeons are distinct
2. $\mathcal{B}$ has the right size
   OK, since $|\mathcal{B}| \leq 2 \cdot |M| \leq 2 \cdot Sp(\mathbb{P})$
3. $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments
   Perhaps a priori not so clear...



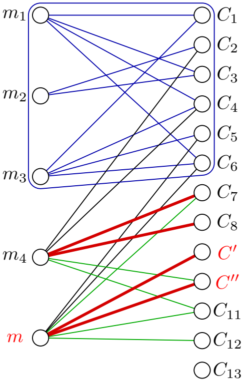
Prove entailment in slightly roundabout way:
Given any β well-behaved on and satisfying $\mathcal{B}$, find α such that

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

Proof of Locality Lemma for PCR (3 / 4)

Need to prove three things:

1. $\mathcal{B}$ is a commitment set
   OK, all pigeons are distinct
2. $\mathcal{B}$ has the right size
   OK, since $|\mathcal{B}| \leq 2 \cdot |M| \leq 2 \cdot Sp(\mathbb{P})$
3. $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments
   Perhaps a priori not so clear...



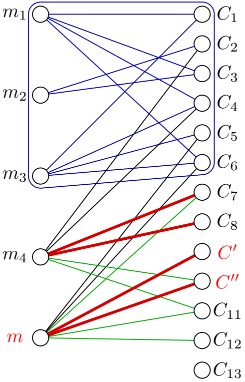
Prove entailment in slightly roundabout way:
Given any β well-behaved on and satisfying $\mathcal{B}$, find α such that

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

Proof of Locality Lemma for PCR (3 / 4)

Need to prove three things:

1. $\mathcal{B}$ is a commitment set
   OK, all pigeons are distinct
2. $\mathcal{B}$ has the right size
   OK, since $|\mathcal{B}| \leq 2 \cdot |M| \leq 2 \cdot Sp(\mathbb{P})$
3. $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments
   Perhaps a priori not so clear...

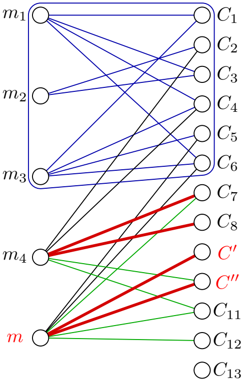


Prove entailment in slightly roundabout way:
Given any β well-behaved on and satisfying $\mathcal{B}$, find α such that

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

Need to prove three things:

1. $\mathcal{B}$ is a commitment set
   OK, all pigeons are distinct
2. $\mathcal{B}$ has the right size
   OK, since $|\mathcal{B}| \leq 2 \cdot |M| \leq 2 \cdot Sp(\mathbb{P})$
3. $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments
   Perhaps a priori not so clear...



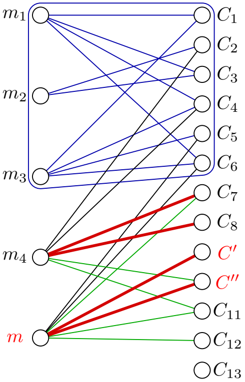
Prove entailment in slightly roundabout way:
Given any β well-behaved on and satisfying $\mathcal{B}$, find α such that

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

Proof of Locality Lemma for PCR (3 / 4)

Need to prove three things:

1. $\mathcal{B}$ is a commitment set
   OK, all pigeons are distinct
2. $\mathcal{B}$ has the right size
   OK, since $|\mathcal{B}| \leq 2 \cdot |M| \leq 2 \cdot Sp(\mathbb{P})$
3. $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments
   Perhaps a priori not so clear. . .

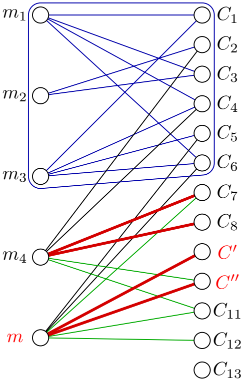


Prove entailment in slightly roundabout way:
Given any β well-behaved on and satisfying $\mathcal{B}$, find α such that

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

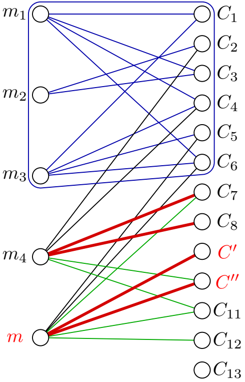
Proof of Locality Lemma for PCR (4 / 4)

- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$ $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.



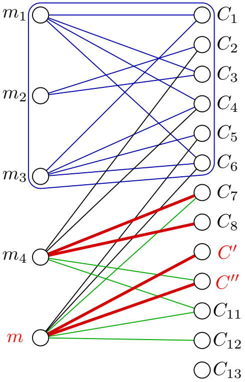
Proof of Locality Lemma for PCR (4 / 4)

- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p, i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$ $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.



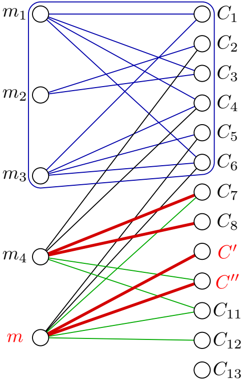
Proof of Locality Lemma for PCR (4 / 4)

- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$ $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.

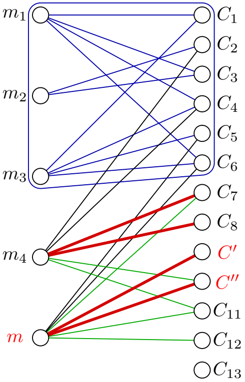


Proof of Locality Lemma for PCR (4 / 4)

- Let $S = \text{dom}(\mathcal{B})$ and $T = \text{dom}(\mathcal{A}) \setminus \text{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \text{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\text{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$ $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.

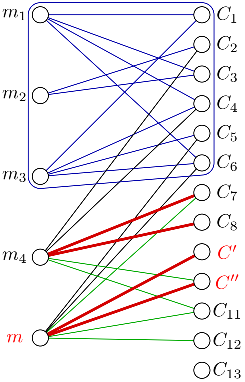


- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$ $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.



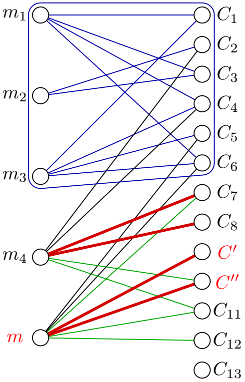
Proof of Locality Lemma for PCR (4 / 4)

- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ
  (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero
  (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$
  $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.

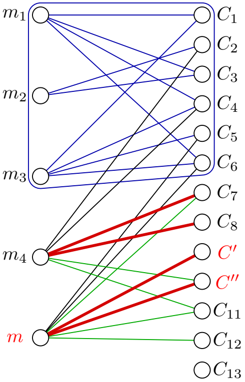


Proof of Locality Lemma for PCR (4 / 4)

- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ
  (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero
  (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$
  $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.



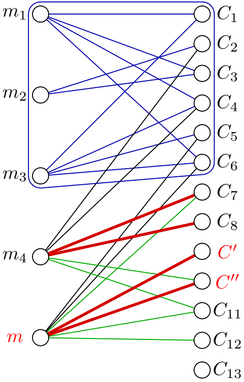
Proof of Locality Lemma for PCR (4 / 4)



- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ
  (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero
  (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$
  $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.

Proof of Locality Lemma for PCR (4 / 4)

- Let $S = \mathrm{dom}(\mathcal{B})$ and $T = \mathrm{dom}(\mathcal{A}) \setminus \mathrm{dom}(\mathcal{B})$
- Let $X = \{$for each $p \in T$ the literal $x[p,i]^b$ in $\mathcal{A}\}$
- Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has ≥ 1 literal in X
- $|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$
- Apply Corollary to S, T, $\beta \Rightarrow$ assignment α s.t.
  - α well-behaved on $S \cup T = \mathrm{dom}(\mathcal{A})$
  - α agrees with β on pigeons outside T
  - α satisfies all literals in X
- α and β agree on monomials in Γ
  (no $m \in \Gamma$ mentions $p \in T$ by construction)
- All β satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero
  (by construction of C_m)
- Hence α and β agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- α well-behaved on $\mathrm{dom}(\mathcal{A})$; satisfies $N(\Gamma) \cup X$
  $\Rightarrow$ satisfies $\mathcal{A} \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, Q.E.D.



Summing up the Course

- Brief overview of proof complexity in general
- Introduced resolution, polynomial calculus, and cutting planes
- Surveyed state of the art for resolution and polynomial calculus
- Proved some recent results for resolution and polynomial calculus
- Many open (and accessible) problems — now go solve them!

The Theory Group at KTH

The Theory Group at KTH (or: A Shameless Plug)

The Theory Group at KTH (or: A Shameless Plug)

- Strong research environment spanning e.g.
  - complexity theory
  - cryptography
  - computer and network security
  - formal methods
  - natural language processing
- Publish regularly in leading CS conferences and journals
- Numerous awards and research grants in recent years
- So we're expanding — and hiring!
  (PhD students, postdocs, and faculty)
- See www.csc.kth.se/tcs for more details