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 introducing 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 $x \lor y \lor \overline{z}$ 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**

\[
\frac{x^2 - x}{x^2 - x}
\]

**Complementarity axioms**

\[
\frac{x + \overline{x} - 1}{x + \overline{x} - 1}
\]

**Linear combination**

\[
\frac{p + q}{\alpha p + \beta q}
\]

**Multiplication**

\[
\frac{p}{xp}
\]

PCR-refutation ends when 1 is derived

All polynomials multilinear w.l.o.g. (follows from Boolean axioms)
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
\( N \) = size of formula

**Size:** at most \( \exp(O(N)) \) 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 \( O(N) \) for PC for \( k \)-CNF formulas [Filmus et al. ’12]

No matching lower bounds!
Currently best bounds \( \Omega\left(\frac{3}{\sqrt{N}}\right) \) (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. $Sp_{\mathsf{PCR}}(F_N \vdash \bot) = \Omega\left(\sqrt[3]{N}\right)$

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 $O(\log N)$ s.t. $Sp_{\mathsf{PCR}}(F_N \vdash \bot) = \Omega\left(\sqrt[3]{N / \log N}\right)$

(But all key ingredients will be there in proofs)
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. $S_{p_{PCR}}(F_N \vdash \bot) = \Omega(3\sqrt[3]{N})$

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 $O(\log N)$ s.t. $S_{p_{PCR}}(F_N \vdash \bot) = \Omega(3\sqrt[3]{N}/\log N)$

(But all key ingredients will be there in proofs)
Bitwise Pigeonhole Principle Formula $BPHP^m_n$

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

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

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

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

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

"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

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

“Have $m > n$ integers between 0 and $n - 1$ and they’re all distinct”
Bitwise Pigeonhole Principle Formula $BPHP^n_m$

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

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

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

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

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

"Have $m > n$ integers between 0 and $n - 1$ and they’re all distinct"
Outline of Proof of PCR Space Lower Bound

**Theorem**

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

**Proof method:** For \( \pi = \{P_0, P_1, \ldots, P_\tau\} \) with \( Sp(\pi) \leq n/8 \), construct “auxiliary configurations” \( A_0, A_1, \ldots, A_\tau \) such that

- \( A_t \) highly structured, so easier to understand than \( P_t \)
- but still gives information about \( P_t \)

**Maintain invariants for \( A_t \):**

1. \( A_t \) implies \( P_t \) (i.e., \( A_t \) “stronger” than \( P_t \))
2. \( A_t \) is satisfiable (so, in particular, \( P_t \) also satisfiable)
3. For \( P_t \rightsquigarrow P_{t+1} \), can do update \( A_t \rightsquigarrow A_{t+1} \) if \( Sp(P_t) \leq n/8 \)

So small-space derivation doesn’t derive contradiction
Outline of Proof of PCR Space Lower Bound

**Theorem**

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

**Proof method:** For \( \pi = \{P_0, P_1, \ldots, P_\tau\} \) with \( Sp(\pi) \leq n/8 \), construct "auxiliary configurations" \( A_0, A_1, \ldots, A_\tau \) such that

- \( A_t \) highly structured, so easier to understand than \( P_t \)
- but still gives information about \( P_t \)

**Maintain invariants for \( A_t \):**

1. \( A_t \) implies \( P_t \) (i.e., \( A_t \) “stronger” than \( P_t \))
2. \( A_t \) is satisfiable (so, in particular, \( P_t \) also satisfiable)
3. For \( P_t \sim P_{t+1} \), can do update \( A_t \sim A_{t+1} \) if \( Sp(P_t) \leq n/8 \)

So small-space derivation doesn’t derive contradiction
Outline of Proof of PCR Space Lower Bound

Theorem

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

Proof method: For $$\pi = \{P_0, P_1, \ldots, P_\tau\}$$ with $$Sp(\pi) \leq n/8$$, construct “auxiliary configurations” $$A_0, A_1, \ldots, A_\tau$$ such that

- $$A_t$$ highly structured, so easier to understand than $$P_t$$
- but still gives information about $$P_t$$

Maintain invariants for $$A_t$$:

1. $$A_t$$ implies $$P_t$$ (i.e., $$A_t$$ “stronger” than $$P_t$$)
2. $$A_t$$ is satisfiable (so, in particular, $$P_t$$ also satisfiable)
3. For $$P_t \leadsto P_{t+1}$$, can do update $$A_t \leadsto A_{t+1}$$ if $$Sp(P_t) \leq n/8$$

So small-space derivation doesn’t derive contradiction
Outline of Proof of PCR Space Lower Bound

Theorem
\[ \text{Sp}_{PCR}(BPHP^m \vdash \bot) > n/8 \]

Proof method: For \( \pi = \{P_0, P_1, \ldots, P_\tau\} \) with \( \text{Sp}(\pi) \leq n/8 \), construct “auxiliary configurations” \( A_0, A_1, \ldots, A_\tau \) such that
- \( A_t \) highly structured, so easier to understand than \( P_t \)
- but still gives information about \( P_t \)

Maintain invariants for \( A_t \):

1. \( A_t \) implies \( P_t \) (i.e., \( A_t \) “stronger” than \( P_t \))
2. \( A_t \) is satisfiable (so, in particular, \( P_t \) also satisfiable)
3. For \( P_t \leadsto P_{t+1} \), can do update \( A_t \leadsto A_{t+1} \) if \( \text{Sp}(P_t) \leq n/8 \)

So small-space derivation doesn’t derive contradiction
Outline of Proof of PCR Space Lower Bound

Theorem

\[ \text{Sp}_{PCR}(BPHP^m_n \vdash \bot) > n/8 \]

Proof method: For \( \pi = \{P_0, P_1, \ldots, P_\tau\} \) with \( \text{Sp} \leq n/8 \), construct “auxiliary configurations” \( A_0, A_1, \ldots, A_\tau \) such that

- \( A_t \) highly structured, so easier to understand than \( P_t \)
- but still gives information about \( P_t \)

Maintain invariants for \( A_t \):

1. \( A_t \) implies \( P_t \) (i.e., \( A_t \) “stronger” than \( P_t \))
2. \( A_t \) is satisfiable (so, in particular, \( P_t \) also satisfiable)
3. For \( P_t \leadsto P_{t+1} \), can do update \( A_t \leadsto A_{t+1} \) if \( \text{Sp}(P_t) \leq n/8 \)

So small-space derivation doesn’t derive contradiction
Outline of Proof of PCR Space Lower Bound

**Theorem**

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

**Proof method:** For \( \pi = \{P_0, P_1, \ldots, P_\tau\} \) with \( Sp(\pi) \leq n/8 \), construct “auxiliary configurations” \( A_0, A_1, \ldots, A_\tau \) such that

- \( A_t \) highly structured, so easier to understand than \( P_t \)
- but still gives information about \( P_t \)

Maintain invariants for \( A_t \):

1. \( A_t \) implies \( P_t \) (i.e., \( A_t \) “stronger” than \( P_t \))
2. \( A_t \) is satisfiable (so, in particular, \( P_t \) also satisfiable)
3. For \( P_t \leadsto P_{t+1} \), can do update \( A_t \leadsto A_{t+1} \) if \( Sp(P_t) \leq n/8 \)

So small-space derivation doesn’t derive contradiction
Outline of Proof of PCR Space Lower Bound

**Theorem**

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

**Proof method:** For \( \pi = \{P_0, P_1, \ldots, P_\tau\} \) with \( Sp(\pi) \leq n/8 \), construct "auxiliary configurations" \( A_0, A_1, \ldots, A_\tau \) such that
- \( A_t \) highly structured, so easier to understand than \( P_t \)
- but still gives information about \( P_t \)

**Maintain invariants for \( A_t \):**

1. \( A_t \) implies \( P_t \) (i.e., \( A_t \) “stronger” than \( P_t \))
2. \( A_t \) is satisfiable (so, in particular, \( P_t \) also satisfiable)
3. For \( P_t \dashv \vdash P_{t+1} \), can do update \( A_t \dashv \vdash A_{t+1} \) if \( Sp(P_t) \leq n/8 \)

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 $\text{dom}(C) = \text{set of pigeons } \{p, q\} \text{ mentioned in } C$

Commitment set

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

Commitment set

- $\mathcal{A} = \{C_1, C_2, \ldots, C_s\}$ — think of $\mathcal{A}_t$ as 2-CNF formula
- For all $i \neq j$, $\text{dom}(C_i) \cap \text{dom}(C_j) = \emptyset$
  (i.e., all pigeons mentioned are distinct)
- $\text{dom}(\mathcal{A}) = \bigcup_{C \in \mathcal{A}} \text{dom}(C)$
- Size $|\mathcal{A}| = \text{number of commitments in } \mathcal{A}$
Any (total) assignment $\alpha$ to $\text{Vars}(BPHP^m_n)$ defines function $f_\alpha : [0, m) \rightarrow [0, n)$ — in what follows, identify $\alpha$ and $f_\alpha$

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

An assignment $\alpha$ is well-behaved on and satisfies commitment set $A$ if

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

**Definition (Entailment)**

$A$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment $\alpha$ which is well-behaved on and satisfies $A$ 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 $\alpha$ to $\text{Vars}(\text{BP} \text{PHP}_m^n)$ defines function $f_\alpha : [0, m) \rightarrow [0, n)$ — in what follows, identify $\alpha$ and $f_\alpha$

A (total) assignment $\alpha$ to $\text{Vars}(\text{BP} \text{PHP}_m^n)$ is well-behaved over set of pigeons $S \subseteq [0, m)$ if it sends pigeons in $S$ to distinct holes

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

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

**Definition (Entailment)**

$\mathcal{A}$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment $\alpha$ 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 $\alpha$ to $\text{Vars}(BPHP^m_n)$ defines function $f_\alpha : [0, m) \to [0, n)$ — in what follows, identify $\alpha$ and $f_\alpha$.

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

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

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

**Definition (Entailment)**

$\mathcal{A}$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment $\alpha$ 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 $\alpha$ to $\text{Vars}(BPHP^m_n)$ defines function $f_\alpha : [0, m) \rightarrow [0, n)$ — in what follows, identify $\alpha$ and $f_\alpha$

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

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

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

**Definition (Entailment)**

$\mathcal{A}$ entails PCR-configuration $\mathbb{P}$ over well-behaved assignments if every assignment $\alpha$ 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 $A_t$ satisfiable by well-behaved assignment (requires a proof; assume it for now)

**Proof invariants:**
- $A_t$ entails $P_t$ over well-behaved assignments
- $|A_t| \leq 2 \cdot S_P(P_t)$

Proof is by case analysis over derivation step $P_t \leadsto P_{t+1}$:
- Download of polynomial encoding
  - Boolean or Complementarity axiom
  - axiom clause $H(p, q, h)$ of $BPHP_n^m$
- Inference of polynomial $Q$ from $P_t$
- Erasure of polynomial $Q \in P_t$
Proof of Space Lower Bound for PCR

**Fact:** Any commitment set $A_t$ satisfiable by well-behaved assignment (requires a proof; assume it for now)

**Proof invariants:**
- $A_t$ entails $P_t$ over well-behaved assignments
- $|A_t| \leq 2 \cdot Sp(P_t)$

Proof is by case analysis over derivation step $P_t \leadsto P_{t+1}$:

1. Download of polynomial encoding
2. Boolean or Complementarity axiom
3. Axiom clause $H(p, q, h)$ of $BPHP_n^m$
4. Inference of polynomial $Q$ from $P_t$
5. Erasure of polynomial $Q \in P_t$
Fact: Any commitment set $A_t$ satisfiable by well-behaved assignment (requires a proof; assume it for now)

Proof invariants:
- $A_t$ entails $P_t$ over well-behaved assignments
- $|A_t| \leq 2 \cdot Sp(P_t)$

Proof is by case analysis over derivation step $P_t \rightsquigarrow P_{t+1}$:
- Download of polynomial encoding
  - Boolean or Complementarity axiom
  - axiom clause $H(p, q, h)$ of $BPHP^n_m$
- Inference of polynomial $Q$ from $P_t$
- Erasure of polynomial $Q \in P_t$
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**

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

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

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

3. \(p \in \text{dom}(\mathcal{A}_t), q \notin \text{dom}(\mathcal{A}_t)\): Pick “dummy” \(p^* \notin \text{dom}(\mathcal{A}_t) \cup \{q\}\);
   let \(C = x[q, 0]^{1-h_0} \lor x[p^*, 0]^0\); set \(\mathcal{A}_{t+1} = \mathcal{A}_t \cup \{C\}\).

Well-behaved \(\alpha\) gives \(p\) and \(q\) distinct holes \(\Rightarrow\) satisfies \(H(p, q, h)\)

Space increases by \(\geq 1\) 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 $A_{t+1} = A_t$

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

1. $\{p, q\} \subseteq \text{dom}(A_t)$: Set $A_{t+1} = A_t$; any well-behaved $\alpha$ sends pigeons $p$ and $q$ to distinct holes $\Rightarrow$ satisfies $H(p, q, h)$

2. $\{p, q\} \cap \text{dom}(A_t) = \emptyset$: Set $A_{t+1} = A_t \cup \{C\}$ for $C = x[p, 0]^{1-h_0} \lor x[q, 0]^{1-h_0}$

3. $p \in \text{dom}(A_t), q \notin \text{dom}(A_t)$: Pick “dummy” $p^* \notin \text{dom}(A_t) \cup \{q\}$; let $C = x[q, 0]^{1-h_0} \lor x[p^*, 0]^0$; set $A_{t+1} = A_t \cup \{C\}$. Well-behaved $\alpha$ gives $p$ and $q$ distinct holes $\Rightarrow$ satisfies $H(p, q, h)$

Space increases by $\geq 1$ and never add more than $1 < 2$ commitments $\Rightarrow |A_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1})$
Case 1: Download

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

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

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

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

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

Space increases by \( \geq 1 \) and never add more than \( 1 < 2 \) commitments \( \Rightarrow \)
\( |\mathcal{A}_{t+1}| \leq 2 \cdot Sp(P_{t+1}) \)
Case 1: Download

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

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

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

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

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

Space increases by $\geq 1$ 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 \( A_{t+1} = A_t \)

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

1. \( \{p, q\} \subseteq \text{dom}(A_t) \): Set \( A_{t+1} = A_t \); any well-behaved \( \alpha \) sends pigeons \( p \) and \( q \) to distinct holes \( \Rightarrow \) satisfies \( H(p, q, h) \)

2. \( \{p, q\} \cap \text{dom}(A_t) = \emptyset \): Set \( A_{t+1} = A_t \cup \{C\} \) for \( C = x[p, 0]^{1-h_0} \lor x[q, 0]^{1-h_0} \)

3. \( p \in \text{dom}(A_t), q \notin \text{dom}(A_t) \): Pick \( \text{“dummy” } p^* \notin \text{dom}(A_t) \cup \{q\}; \) let \( C = x[q, 0]^{1-h_0} \lor x[p^*, 0]^{1-h_0} \); set \( A_{t+1} = A_t \cup \{C\} \).
   Well-behaved \( \alpha \) gives \( p \) and \( q \) distinct holes \( \Rightarrow \) satisfies \( H(p, q, h) \)

Space increases by \( \geq 1 \) and never add more than \( 1 < 2 \) commitments \( \Rightarrow \)
\( |A_{t+1}| \leq 2 \cdot Sp(\mathbb{P}_{t+1}) \)
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 $H(p, q, h) = \bigvee_{i=0}^{\ell-1} x[p, i]^{1-h_i} \lor \bigvee_{i=0}^{\ell-1} x[q, i]^{1-h_i}$:

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

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

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

Space increases by $\geq 1$ and never add more than $1 < 2$ commitments \implies $|\mathcal{A}_{t+1}| \leq 2 \cdot Sp(P_{t+1})$
Case 2: Inference

- $P_{t+1} = P_t \cup \{Q\}$ for polynomial $Q$ derived from $P$
- Set $A_{t+1} = A_t$
- PCR is sound $\Rightarrow$ $Q$ implied by $P_t$
- I.e., if for all $P \in P_t$ have that $P(\alpha) = 0$, then $Q(\alpha) = 0$ also holds
- All well-behaved $\alpha$ satisfying $A_{t+1} = A_t$ must satisfy $P_t$ by the induction hypothesis and hence also $Q$, so all of $P_{t+1}$ is satisfied
- Space increases but size of commitment set unchanged $\Rightarrow$ $|A_{t+1}| \leq 2 \cdot Sp(P_{t+1})$
Case 3: Erasure

- $P_{t+1} = P_t \setminus \{Q\}$ for $Q \in P_t$

- Know $A_t$ entails $P_{t+1} \subseteq P_t$

- But $|A_t|$ may be far too large if $Q$ contains lots of monomials

- Need to find smaller commitment set that still entails $P_{t+1}$
  (Was very easy for resolution; now not clear at all what to do)

Lemma (Locality lemma for PCR)

Suppose

- A commitment set
- $P$ PCR-configuration
- $A$ entails $P$ over well-behaved assignments

Then $\exists$ commitment set $B$ of size $|B| \leq 2 \cdot Sp(P)$ s.t. $B$ entails $P$ over well-behaved assignments
Case 3: Erasure

- $P_{t+1} = P_t \setminus \{Q\}$ for $Q \in P_t$
- Know $A_t$ entails $P_{t+1} \subseteq P_t$

- But $|A_t|$ may be far too large if $Q$ contains lots of monomials
- Need to find smaller commitment set that still entails $P_{t+1}$
  (Was very easy for resolution; now not clear at all what to do)

Lemma (Locality lemma for PCR)

Suppose

- $A$ commitment set
- $P$ PCR-configuration
- $A$ entails $P$ over well-behaved assignments

Then $\exists$ commitment set $B$ of size $|B| \leq 2 \cdot Sp(P)$ s.t. $B$ entails $P$ over well-behaved assignments
Case 3: Erasure

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

Lemma (Locality lemma for PCR)

**Suppose**

- $A$ commitment set
- $P$ PCR-configuration
- $A$ entails $P$ over well-behaved assignments

**Then** $\exists$ commitment set $B$ of size $|B| \leq 2 \cdot Sp(P)$ s.t. $B$ entails $P$ over well-behaved assignments
Case 3: Erasure

- $\mathbb{P}_{t+1} = \mathbb{P}_t \setminus \{Q\}$ for $Q \in \mathbb{P}_t$
- Know $A_t$ entails $\mathbb{P}_{t+1} \subseteq \mathbb{P}_t$
- But $|A_t|$ 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

- $A$ commitment set
- $\mathbb{P}$ PCR-configuration
- $A$ 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

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

Lemma (Locality lemma for PCR)

Suppose

- A commitment set
- $P$ PCR-configuration
- $A$ entails $P$ over well-behaved assignments

Then $\exists$ commitment set $B$ of size $|B| \leq 2 \cdot Sp(P)$ s.t. $B$ entails $P$ over well-behaved assignments
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 \( \beta \) well-behaved on \( S \),
- any literal \( x[p, i]^b \) associated to pigeon \( p \notin S \),

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

**Proof.**

- Exactly half of \( n \) holes have binary expansion with \( i \)th bit = \( b \)
- Pigeons in \( S \) use less than \( n/2 \) holes (as assigned by \( \beta \))
- Hence by counting \( \exists \) hole \( h \) not assigned to any pigeon in \( S \) and having the right value of \( i \)th bit
- Modifying \( \beta \) 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 $\beta$ well-behaved on $S$,
- any literal $x[p, i]^b$ associated to pigeon $p \notin S$,

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

Proof.

- Exactly half of $n$ holes have binary expansion with $i$th bit = $b$
- Pigeons in $S$ use less than $n/2$ holes (as assigned by $\beta$)
- Hence by counting $\exists$ hole $h$ not assigned to any pigeon in $S$ and having the right value of $i$th bit
- Modifying $\beta$ 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 \( \beta \) well-behaved on \( S \),
- any literal \( x[p, i]^b \) associated to pigeon \( p \notin S \),

can modify \( \beta \) to \( \alpha \) by reassigning variables associated to pigeon \( p \) so that \( \alpha \) is well-behaved on \( S \cup \{p\} \) and satisfies \( x[p, i]^b \)

Proof.

- Exactly half of \( n \) holes have binary expansion with \( i \)th bit = \( b \)
- Pigeons in \( S \) use less than \( n/2 \) holes (as assigned by \( \beta \))
- Hence by counting \( \exists \) hole \( h \) not assigned to any pigeon in \( S \) and having the right value of \( i \)th bit
- Modifying \( \beta \) 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 \( \beta \) well-behaved on \( S \),
- any set \( X \) of **exactly** one literal \( x[p, i_p]^{b_p} \) for every \( p \in T \),

can modify \( \beta \) to \( \alpha \) by reassigning variables associated to pigeons in \( T \) so that \( \alpha \) 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 \( A \) of size \( |A| \leq n/4 \) is satisfiable by well-behaved assignment

(Let \( S = \emptyset \), \( T = \text{dom}(A) \), \( X = \text{Lit}(A) \) 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 $\beta$ well-behaved on $S$,
- any set $X$ of exactly one literal $x[p, i_p]^{b_p}$ for every $p \in T$,

can modify $\beta$ to $\alpha$ by reassigning variables associated to pigeons in $T$ so that $\alpha$ 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 $A$ of size $|A| \leq n/4$ is satisfiable by well-behaved assignment.

(LET $S = \emptyset$, $T = \text{dom}(A)$, $X = \text{Lit}(A)$ 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 $\beta$ well-behaved on $S$,
- any set $X$ of exactly one literal $x[p, i_p]^{b_p}$ for every $p \in T$,

**can modify $\beta$ to $\alpha$ by reassigning variables associated to pigeons in $T$ so that $\alpha$ 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 $A$ of size $|A| \leq n/4$ is satisfiable by well-behaved assignment

(Let $S = \emptyset$, $T = \text{dom}(A)$, $X = \text{Lit}(A)$ 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 $\beta$ well-behaved on $S$,
- any set $X$ of exactly one literal $x[p, i_p]^{b_p}$ for every $p \in T$,

can modify $\beta$ to $\alpha$ by reassigning variables associated to pigeons in $T$ so that $\alpha$ 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 $S = \emptyset$, $T = \text{dom}(\mathcal{A})$, $X = \text{Lit}(\mathcal{A})$ and apply Corollary)
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
  \[ \exists \text{ pigeon } p \text{ mentioned in both} \]

- 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
  \[ |N(S) \setminus N(\Gamma)| > 2 \cdot |S| \]

- $\implies \exists$ 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 $A$
- Edge between $m \in M$ and $C \in A$ 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 $B = N(\Gamma)$)
- $\forall S \subseteq M \setminus \Gamma$ by maximality $|N(S) \setminus N(\Gamma)| > 2 \cdot |S|$
- $\Rightarrow \exists$ matching of each $m \in M \setminus \Gamma$ to 2 distinct $C', C'' \in A \setminus N(\Gamma)$
- (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 $G = (U ∪ V, E)$
- $U =$ distinct monomials $M$ in $P$
- $V =$ commitments in $A$

**Edge between** $m ∈ M$ and $C ∈ A$ **if**

$∃$ pigeon $p$ mentioned in both

**Let** $Γ ⊆ M$ set of maximal size such

that $|N(Γ)| ≤ 2 \cdot |Γ|$

**Assume** $Γ \neq M$ (else set $B = N(Γ)$)

$∀ S ⊆ M \setminus Γ$ by maximality

$|N(S) \setminus N(Γ)| > 2 \cdot |S|$

$⇒ ∃$ matching of each $m ∈ M \setminus Γ$

to 2 distinct $C', C'' ∈ A \setminus N(Γ)$

$(Make 2 copies of each $m ∈ M \setminus Γ$

and apply Hall’s theorem)$
Proof of Locality Lemma for PCR (1 / 4)

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

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

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

\( (m \text{ can also mention } q' \text{ and/or } q'' \text{ — don’t care}) \)

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

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

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

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

Done!
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

- \( m = x[p', i_1]^{b_1} \cdot x[p'', i_2]^{b_2} \cdot m' \)  
  \((m \text{ can also mention } q' \text{ and/or } q'' \text{ — don't care})\)

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

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

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 \( |\mathcal{B}| \leq 2 \cdot |\mathcal{M}| \leq 2 \cdot Sp(\mathcal{P}) \)

3. \( \mathcal{B} \) entails \( \mathcal{P} \) over well-behaved assignments
   Perhaps a priori not so clear...

Prove entailment in slightly roundabout way:

Given any \( \beta \) well-behaved on and satisfying \( \mathcal{B} \), find \( \alpha \) such that

- \( \mathcal{P}(\alpha) = \mathcal{P}(\beta) \)
- \( \alpha \) well-behaved on and satisfies \( \mathcal{A} \)
Need to prove three things:

1. $B$ is a commitment set
   OK, all pigeons are distinct

2. $B$ has the right size
   OK, since $|B| \leq 2 \cdot |M| \leq 2 \cdot Sp(P)$

3. $B$ entails $P$ over well-behaved assignments
   Perhaps a priori not so clear...

Prove entailment in slightly roundabout way:
Given any $\beta$ well-behaved on and satisfying $B$, find $\alpha$ such that
- $P(\alpha) = P(\beta)$
- $\alpha$ well-behaved on and satisfies $A$
Need to prove three things:

1. \( B \) is a commitment set
   OK, all pigeons are distinct

2. \( B \) has the right size
   OK, since \( |B| \leq 2 \cdot |M| \leq 2 \cdot Sp(\mathbb{P}) \)

3. \( B \) entails \( \mathbb{P} \) over well-behaved assignments
   Perhaps a priori not so clear...

Prove entailment in slightly roundabout way:
Given any \( \beta \) well-behaved on and satisfying \( B \), find \( \alpha \) such that

- \( \mathbb{P}(\alpha) = \mathbb{P}(\beta) \)
- \( \alpha \) well-behaved on and satisfies \( A \)
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 $|\mathcal{B}| \leq 2 \cdot |M| \leq 2 \cdot \mathcal{S}_p(\mathbb{P})$

3. $\mathcal{B}$ entails $\mathbb{P}$ over well-behaved assignments
   Perhaps a priori not so clear...

Prove entailment in slightly roundabout way:
Given any $\beta$ well-behaved on and satisfying $\mathcal{B}$, find $\alpha$ such that
- $\mathbb{P}(\alpha) = \mathbb{P}(\beta)$
- $\alpha$ 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 \( \beta \) well-behaved on and satisfying \( \mathcal{B} \), find \( \alpha \) such that

- \( \mathbb{P}(\alpha) = \mathbb{P}(\beta) \)
- \( \alpha \) well-behaved on and satisfies \( \mathcal{A} \)
Let $S = \text{dom}(\mathcal{B})$ and $T = \text{dom}(\mathcal{A}) \setminus \text{dom}(\mathcal{B})$.

Let $X = \{\text{for each } p \in T \text{ the literal } x[p, i]^b \text{ in } \mathcal{A}\}$

Notice each $C \in \mathcal{A} \setminus N(\Gamma)$ has $\geq 1$ literal in $X$

$|\mathcal{A}| \leq n/4 \Rightarrow |S \cup T| \leq n/2$

Apply Corollary to $S$, $T$, $\beta \Rightarrow$ assignment $\alpha$ s.t.

$\alpha$ well-behaved on $S \cup T = \text{dom}(\mathcal{A})$

$\alpha$ agrees with $\beta$ on pigeons outside $T$

$\alpha$ satisfies all literals in $X$

$\alpha$ and $\beta$ agree on monomials in $\Gamma$
(no $m \in \Gamma$ mentions $p \in T$ by construction)

All $\beta$ satisfying $\mathcal{B}$ must set all $m \in M \setminus \Gamma$ to zero
(by construction of $C_m$)

Hence $\alpha$ and $\beta$ agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$

$\alpha$ 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 $S = \text{dom}(B)$ and $T = \text{dom}(A) \setminus \text{dom}(B)$

Let $X = \{\text{for each } p \in T \text{ the literal } x[p, i]^b \text{ in } A\}$

Notice each $C \in A \setminus N(\Gamma)$ has $\geq 1$ literal in $X$

$|A| \leq n/4 \Rightarrow |S \cup T| \leq n/2$

Apply Corollary to $S$, $T$, $\beta \Rightarrow$ assignment $\alpha$ s.t.

- $\alpha$ well-behaved on $S \cup T = \text{dom}(A)$
- $\alpha$ agrees with $\beta$ on pigeons outside $T$
- $\alpha$ satisfies all literals in $X$

$\alpha$ and $\beta$ agree on monomials in $\Gamma$
(no $m \in \Gamma$ mentions $p \in T$ by construction)

All $\beta$ satisfying $B$ must set all $m \in M \setminus \Gamma$ to zero
(by construction of $C_m$)

Hence $\alpha$ and $\beta$ agree on all $m \in M \Rightarrow P(\alpha) = P(\beta)$

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

Let $X = \{\text{for each } p \in T \text{ the literal } x[p, i]^b \text{ in } A\}$.

Notice each $C \in A \setminus N(\Gamma)$ has $\geq 1$ literal in $X$.

$|A| \leq n/4 \Rightarrow |S \cup T| \leq n/2$.

Apply Corollary to $S$, $T$, $\beta \Rightarrow$ assignment $\alpha$ s.t.
- $\alpha$ well-behaved on $S \cup T = \text{dom}(A)$.
- $\alpha$ agrees with $\beta$ on pigeons outside $T$.
- $\alpha$ satisfies all literals in $X$.

$\alpha$ and $\beta$ agree on monomials in $\Gamma$ (no $m \in \Gamma$ mentions $p \in T$ by construction).

All $\beta$ satisfying $B$ must set all $m \in M \setminus \Gamma$ to zero (by construction of $C_m$).

Hence $\alpha$ and $\beta$ agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$.

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

Let \( S = \text{dom}(B) \) and \( T = \text{dom}(A) \setminus \text{dom}(B) \).

Let \( X = \{\text{for each } p \in T \text{ the literal } x[p, i]^b \text{ in } A\} \).

Notice each \( C \in A \setminus N(\Gamma) \) has \( \geq 1 \) literal in \( X \).

\(|A| \leq n/4 \Rightarrow |S \cup T| \leq n/2\)

Apply Corollary to \( S, T, \beta \Rightarrow \) assignment \( \alpha \) s.t.
  \( \quad \alpha \) well-behaved on \( S \cup T = \text{dom}(A) \)
  \( \quad \alpha \) agrees with \( \beta \) on pigeons outside \( T \)
  \( \quad \alpha \) satisfies all literals in \( X \)

\( \alpha \) and \( \beta \) agree on monomials in \( \Gamma \)
  (no \( m \in \Gamma \) mentions \( p \in T \) by construction)

All \( \beta \) satisfying \( B \) must set all \( m \in M \setminus \Gamma \) to zero
  (by construction of \( C_m \))

Hence \( \alpha \) and \( \beta \) agree on all \( m \in M \Rightarrow P(\alpha) = P(\beta) \)
\( \alpha \) well-behaved on \( \text{dom}(A) \); satisfies \( N(\Gamma) \cup X \)
\( \Rightarrow \) satisfies \( A \Rightarrow P(\alpha) = 0 \Rightarrow P(\beta) = 0 \), Q.E.D.
Let $S = \text{dom}(B)$ and $T = \text{dom}(A) \setminus \text{dom}(B)$

Let $X = \{\text{for each } p \in T \text{ the literal } x[p,i]^b \text{ in } A\}$

Notice each $C \in A \setminus N(\Gamma)$ has $\geq 1$ literal in $X$

Since $|A| \leq n/4$ $\Rightarrow$ $|S \cup T| \leq n/2$

Apply Corollary to $S$, $T$, $\beta \Rightarrow$ assignment $\alpha$ s.t.

- $\alpha$ well-behaved on $S \cup T = \text{dom}(A)$
- $\alpha$ agrees with $\beta$ on pigeons outside $T$
- $\alpha$ satisfies all literals in $X$

$\alpha$ and $\beta$ agree on monomials in $\Gamma$

(no $m \in \Gamma$ mentions $p \in T$ by construction)

All $\beta$ satisfying $B$ must set all $m \in M \setminus \Gamma$ to zero
(by construction of $C_m$)

Hence $\alpha$ and $\beta$ agree on all $m \in M \Rightarrow P(\alpha) = P(\beta)$

$\alpha$ well-behaved on $\text{dom}(A)$; satisfies $N(\Gamma) \cup X$

$\Rightarrow$ satisfies $A$ $\Rightarrow P(\alpha) = 0$ $\Rightarrow P(\beta) = 0$, Q.E.D.
Proof of Locality Lemma for PCR (4 / 4)

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

Let $X = \{\text{for each } p \in T \text{ the literal } x[p, i]^b \text{ in } A\}$

Notice each $C \in A \setminus N(\Gamma)$ has $\geq 1$ literal in $X$

$|A| \leq n/4 \Rightarrow |S \cup T| \leq n/2$

Apply Corollary to $S, T, \beta \Rightarrow$ assignment $\alpha$ s.t.

$\alpha$ well-behaved on $S \cup T = \text{dom}(A)$

$\alpha$ agrees with $\beta$ on pigeons outside $T$

$\alpha$ satisfies all literals in $X$

$\alpha$ and $\beta$ agree on monomials in $\Gamma$
(no $m \in \Gamma$ mentions $p \in T$ by construction)

All $\beta$ satisfying $B$ must set all $m \in M \setminus \Gamma$ to zero
(by construction of $C_m$)

Hence $\alpha$ and $\beta$ agree on all $m \in M \Rightarrow \mathbb{P}(\alpha) = \mathbb{P}(\beta)$

$\alpha$ well-behaved on $\text{dom}(A)$; satisfies $N(\Gamma) \cup X$
⇒ satisfies $A \Rightarrow \mathbb{P}(\alpha) = 0 \Rightarrow \mathbb{P}(\beta) = 0$, 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

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!

See www.csc.kth.se/tcs for more details

Jakob Nordström (KTH)
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
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](http://www.csc.kth.se/tcs) for more details