Lower Bounds for the Polynomial Calculus via the “Pigeon Dance”

Imogen Hergeth

January 2023

Overview

- Overview of the needed background

Overview

- Overview of the needed background
- Ideas behind the proof and its structure

Overview

- Overview of the needed background
- Ideas behind the proof and its structure
- The proof in more detail

Definition

- Similar to sequent calculus, but lines are polynomials

Definition

- Similar to sequent calculus, but lines are polynomials
- Addition

$$\frac{f \qquad g}{af + bg}$$

Definition

- Similar to sequent calculus, but lines are polynomials
- Addition

$$\frac{f \qquad g}{af + bg}$$

- Multiplication

$$\frac{f}{f \cdot x}$$

Definition

- Similar to sequent calculus, but lines are polynomials
- Addition

$$\frac{f \qquad g}{af + bg}$$

- Multiplication

$$\frac{f}{f \cdot x}$$

- We use multilinear polynomials $S_n(\mathbb{K})$
  $(xy + xz + v \equiv x^2y + x^3z^5 + v)$

Motivation

- g is provable from $f_1, \ldots, f_n$ if and only if it is in the ideal generated by them

Motivation

- g is provable from $f_1, \ldots, f_n$ if and only if it is in the ideal generated by them
- A *refutation* of $f_1, \ldots, f_n$ is a proof of 1 from $f_1, \ldots, f_n$

Motivation

- g is provable from $f_1, \ldots, f_n$ if and only if it is in the ideal generated by them
- A *refutation* of $f_1, \ldots, f_n$ is a proof of 1 from $f_1, \ldots, f_n$
- A refutation exists if and only if $f_1, \ldots, f_n$ have no common zeroes

Motivation

- g is provable from $f_1, \ldots, f_n$ if and only if it is in the ideal generated by them
- A *refutation* of $f_1, \ldots, f_n$ is a proof of 1 from $f_1, \ldots, f_n$
- A refutation exists if and only if $f_1, \ldots, f_n$ have no common zeroes
- We construct polynomials such that their zeroes correspond to satisfying assignments

The pigeonhole principle

- If there are m pigeons, n pigeon holes, and $m > n$ then at least two pigeons have to share a hole

The pigeonhole principle

- If there are m pigeons, n pigeon holes, and $m > n$ then at least two pigeons have to share a hole
- Formally: if $m > n$ there is no injection $[m] \hookrightarrow [n]$

The pigeonhole principle

- If there are m pigeons, n pigeon holes, and $m > n$ then at least two pigeons have to share a hole
- Formally: if $m > n$ there is no injection $[m] \hookrightarrow [n]$
- Variables: $x_{i,j}, i \in [m], n \in [n]$

The pigeonhole principle

- If there are m pigeons, n pigeon holes, and $m > n$ then at least two pigeons have to share a hole
- Formally: if $m > n$ there is no injection $[m] \hookrightarrow [n]$
- Variables: $x_{i,j}, i \in [m], n \in [n]$
- Assignment of $x_{3,5}$ corresponds to pigeon 3 being in hole 5

The pigeonhole principle

- If there are m pigeons, n pigeon holes, and $m > n$ then at least two pigeons have to share a hole
- Formally: if $m > n$ there is no injection $[m] \hookrightarrow [n]$
- Variables: $x_{i,j}, i \in [m], n \in [n]$
- Assignment of $x_{3,5}$ corresponds to pigeon 3 being in hole 5

Definition ($\neg\mathcal{PHP}_n^m$)

$$Q_i := 1 - \sum_{j\in[n]} x_{ij} \qquad \text{for each } i \in [m]$$

$$Q_{i_1,i_2,j} := x_{i_1 j} x_{i_2 j} \qquad \text{for each } i_1 \neq i_2 \in [m], j \in [n]$$

Intuition

- Terms are potential pigeon assignments

Intuition

- Terms are potential pigeon assignments
- Multiplication and $Q_{i_1,i_2,j}$ let us remove ones we know are impossible

$$\frac{1 - x_{1,1}x_{2,2}x_{3,3} - x_{1,2}x_{2,2}x_{3,3} \qquad \frac{x_{1,2}x_{2,2}}{x_{1,2}x_{2,2}x_{3,3}}}{1 - x_{1,1}x_{2,2}x_{3,3}}$$

Intuition

- Terms are potential pigeon assignments
- Multiplication and $Q_{i_1,i_2,j}$ let us remove ones we know are impossible

$$\frac{1 - x_{1,1}x_{2,2}x_{3,3} - x_{1,2}x_{2,2}x_{3,3} \qquad \frac{x_{1,2}x_{2,2}}{x_{1,2}x_{2,2}x_{3,3}}}{1 - x_{1,1}x_{2,2}x_{3,3}}$$

- Strategy: pick some pigeon i, and show it can not fit regardless of other assignments

Intuition

- Terms are potential pigeon assignments
- Multiplication and $Q_{i_1,i_2,j}$ let us remove ones we know are impossible

$$\frac{1 - x_{1,1}x_{2,2}x_{3,3} - x_{1,2}x_{2,2}x_{3,3} \qquad \frac{x_{1,2}x_{2,2}}{x_{1,2}x_{2,2}x_{3,3}}}{1 - x_{1,1}x_{2,2}x_{3,3}}$$

- Strategy: pick some pigeon i, and show it can not fit regardless of other assignments
- Start with some Q_i, multiply with all other $x_{i',j}$, and remove all terms

Theorem

Theorem

For any $m > n$, every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ must have degree at least $n/2 + 1$.

Theorem

Theorem

For any $m > n$, every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ must have degree at least $n/2 + 1$.

- Pigeonhole principle is locally consistent

Theorem

Theorem

For any $m > n$, every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ must have degree at least $n/2 + 1$.

- Pigeonhole principle is locally consistent
- Polynomial calculus preserves local validity

Theorem

Theorem

For any $m > n$, every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ must have degree at least $n/2 + 1$.

- Pigeonhole principle is locally consistent
- Polynomial calculus preserves local validity
- Only large terms are always cancellable

Technical details

- $\prec$ orders variables and terms degree lexicographic $(x_{3,1} \prec x_{2,5} \prec x_{1,1}x_{1,2})$

Technical details

- $\prec$ orders variables and terms degree lexicographic $(x_{3,1} \prec x_{2,5} \prec x_{1,1}x_{1,2})$
- We use V to denote those polynomials that are provable

Technical details

- $\prec$ orders variables and terms degree lexicographic $(x_{3,1} \prec x_{2,5} \prec x_{1,1}x_{1,2})$
- We use V to denote those polynomials that are provable
- Δ are terms that do not appear as leading terms of polynomials in V

Technical details

- $\prec$ orders variables and terms degree lexicographic $(x_{3,1} \prec x_{2,5} \prec x_{1,1}x_{1,2})$
- We use V to denote those polynomials that are provable
- Δ are terms that do not appear as leading terms of polynomials in V
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V$

Technical details

- $\prec$ orders variables and terms degree lexicographic ($x_{3,1} \prec x_{2,5} \prec x_{1,1}x_{1,2}$)
- We use V to denote those polynomials that are provable
- Δ are terms that do not appear as leading terms of polynomials in V
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V$
- R is the projection onto Δ

Technical details

- $\prec$ orders variables and terms degree lexicographic $(x_{3,1} \prec x_{2,5} \prec x_{1,1}x_{1,2})$
- We use V to denote those polynomials that are provable
- Δ are terms that do not appear as leading terms of polynomials in V
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V$
- R is the projection onto Δ
- Index all of these with n, d, I

Technical details

- $\prec$ orders variables and terms degree lexicographic $(x_{3,1} \prec x_{2,5} \prec x_{1,1}x_{1,2})$
- We use V to denote those polynomials that are provable
- Δ are terms that do not appear as leading terms of polynomials in V
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V$
- R is the projection onto Δ
- Index all of these with n, d, I
- Important: R tells us what can not be proved ($R \neq 0 \Leftrightarrow V$ refutable)

Proof structure

- Characterize V_d semantically

Proof structure

- Characterize V_d semantically
- Problem: only works if R_I agree on their intersections

Proof structure

- Characterize V_d semantically
- Problem: only works if R_I agree on their intersections
- Characterize R_I syntactically

Proof structure

- Characterize V_d semantically
- Problem: only works if R_I agree on their intersections
- Characterize R_I syntactically
- Show the different operators are identical

Idea

- What polynomials are derivable from $\neg\mathcal{PHP}_n^m$?

Idea

- What polynomials are derivable from $\neg\mathcal{PHP}_n^m$?
- Pigeons can not share holes

Idea

- What polynomials are derivable from $\neg\mathcal{PHP}_n^m$?
- Pigeons can not share holes
- Pigeon assignments are variable assignments

$$\delta(x) = \begin{cases} 1, & \text{if } x \in \{x_{1,2}, x_{2,4}, x_{3,1}\} \\ 0, & \text{otherwise} \end{cases}$$

Idea

- What polynomials are derivable from $\neg\mathcal{PHP}_n^m$?
- Pigeons can not share holes
- Pigeon assignments are variable assignments

$$\delta(x) = \begin{cases} 1, & \text{if } x \in \{x_{1,2}, x_{2,4}, x_{3,1}\} \\ 0, & \text{otherwise} \end{cases}$$

- Polynomials are evaluated to 0 if they allow the assignment

$$\delta(1 - x_{1,1} - x_{1,2} - x_{1,3} - x_{1,4}) = 0$$
$$\delta(x_{1,1}x_{3,1}) = \delta(x_{1,2}x_{2,2}) = 0$$

Derivable Polynomials

- $I \subseteq [n]$ is a set of pigeons

Derivable Polynomials

- $I \subseteq [n]$ is a set of pigeons
- M_I is all assignments corresponding to injections $I \hookrightarrow [m]$

Derivable Polynomials

- $I \subseteq [n]$ is a set of pigeons
- M_I is all assignments corresponding to injections $I \hookrightarrow [m]$
- Polynomials in $\neg\mathcal{PHP}_n^m$ are identically zero on M_I

Derivable Polynomials

- $I \subseteq [n]$ is a set of pigeons
- M_I is all assignments corresponding to injections $I \hookrightarrow [m]$
- Polynomials in $\neg\mathcal{PHP}_n^m$ are identically zero on M_I
- Polynomials derivable from $\neg\mathcal{PHP}_n^m$ are identically zero on M_I

Derivable Polynomials

- $I \subseteq [n]$ is a set of pigeons
- M_I is all assignments corresponding to injections $I \hookrightarrow [m]$
- Polynomials in $\neg\mathcal{PHP}_n^m$ are identically zero on M_I
- Polynomials derivable from $\neg\mathcal{PHP}_n^m$ are identically zero on M_I

$\Rightarrow V_I$ are all polynomials identically zero on M_I

Combining V_I

- We want a characterization of V_d, not V_I

Combining V_I

- We want a characterization of V_d, not V_I
- Set $V_d := \bigcup_{|I| \leq d} V_I$ and R_d accordingly

Combining V_I

- We want a characterization of V_d, not V_I
- Set $V_d := \bigcup_{|I| \leq d} V_I$ and R_d accordingly
- Does this definition actually work?

Combining V_I

- We want a characterization of V_d, not V_I
- Set $V_d := \bigcup_{|I| \leq d} V_I$ and R_d accordingly
- Does this definition actually work?
- Yes it does! But only if $R_I(t) = R_{\mathrm{dom}(t)}(t)$

Overview

- Define $R_I(t)$ so that it is independent of pigeons not in t

Overview

- Define $R_I(t)$ so that it is independent of pigeons not in t
- Show that the two definitions are identical

Overview

- Define $R_I(t)$ so that it is independent of pigeons not in t
- Show that the two definitions are identical
- We will only show the broad steps

Example

Formalization

- The first pigeon flies to an unoccupied hole to its right

Formalization

- The first pigeon flies to an unoccupied hole to its right
- Repeat until all pigeons have moved once

Formalization

- The first pigeon flies to an unoccupied hole to its right
- Repeat until all pigeons have moved once
- If a pigeon can not find an empty hole, the dance is aborted

Formalization

- The first pigeon flies to an unoccupied hole to its right
- Repeat until all pigeons have moved once
- If a pigeon can not find an empty hole, the dance is aborted
- Define Δ_I to be the set of terms that let pigeons complete the dance

Formalization

- The first pigeon flies to an unoccupied hole to its right
- Repeat until all pigeons have moved once
- If a pigeon can not find an empty hole, the dance is aborted
- Define Δ_I to be the set of terms that let pigeons complete the dance
- $R_I(t) = R_{\mathrm{dom}(t)}(t)$ since pigeons not in the dance do not affect it

Defining R_I

- We need $R_I(t) = f$ with $\mathrm{LT}(f) \prec t$ and $t - f \in V_I$

Defining R_I

- We need $R_I(t) = f$ with $\mathrm{LT}(f) \prec t$ and $t - f \in V_I$
- If $t \in \Delta_I$ then $f = t$

Defining R_I

- We need $R_I(t) = f$ with $\mathrm{LT}(f) \prec t$ and $t - f \in V_I$
- If $t \in \Delta_I$ then $f = t$
- Otherwise we use $Q_{i_1} = 0$ to derive

$$\begin{aligned} t = x_{i_2 j_2} \cdots x_{i_d j_d} &- \sum_{j' < j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} \\ &- \sum_{j' > j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} \mod V_I. \end{aligned}$$

Defining R_I

- We need $R_I(t) = f$ with $\mathrm{LT}(f) \prec t$ and $t - f \in V_I$
- If $t \in \Delta_I$ then $f = t$
- Otherwise we use $Q_{i_1} = 0$ to derive

$$\begin{aligned} t = x_{i_2 j_2} \cdots x_{i_d j_d} - \sum_{j' < j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} \\ - \sum_{j' > j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} \mod V_I. \end{aligned}$$

- The first two summands are $\prec t$ and can be ignored

Defining R_I

- We need $R_I(t) = f$ with $\mathrm{LT}(f) \prec t$ and $t - f \in V_I$
- If $t \in \Delta_I$ then $f = t$
- Otherwise we use $Q_{i_1} = 0$ to derive

$$t = x_{i_2 j_2} \cdots x_{i_d j_d} - \sum_{j' < j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} - \sum_{j' > j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} \mod V_I.$$

- The first two summands are $\prec t$ and can be ignored
- Any terms with $j' \in \{j_2, \ldots, j_d\}$ are 0 and can be ignored

Defining R_I (cont.)

- Repeat the same process with all remaining terms

Defining R_I (cont.)

- Repeat the same process with all remaining terms
- At each step the first $x_{i,j}$ gets replaced with $x_{i,j'}$ with some unused $j' > j$

Defining R_I (cont.)

- Repeat the same process with all remaining terms
- At each step the first $x_{i,j}$ gets replaced with $x_{i,j'}$ with some unused $j' > j$
- This is the pigeon dance!

Defining R_I (cont.)

- Repeat the same process with all remaining terms
- At each step the first $x_{i,j}$ gets replaced with $x_{i,j'}$ with some unused $j' > j$
- This is the pigeon dance!
- Since $t \notin \Delta_I$ the dance can not be completed

Defining R_I (cont.)

- Repeat the same process with all remaining terms
- At each step the first $x_{i,j}$ gets replaced with $x_{i,j'}$ with some unused $j' > j$
- This is the pigeon dance!
- Since $t \notin \Delta_I$ the dance can not be completed
- Process terminates with $f \prec t$ and $t = f \mod V_I$

The Kill operator

- The Kill operator kills the first pigeon and moves its hole to the left

The Kill operator

- The Kill operator kills the first pigeon and moves its hole to the left
- $\mathrm{Kill}(x_{i_1,j_1}\cdots x_{i_d,j_d}) = x_{i_2,j'_2}\cdots x_{i_d,j'_d}$ with

$$j'_k := \begin{cases} j_k + 1, & \text{if } j_k < j_1 \\ j_k, & \text{if } j_k > j_1. \end{cases}$$

Properties of Kill

Theorem

$x_{i_1,j_1}\cdots x_{i_d,j_d} \in \Delta_I$ *if and only if there is a* $j' > j_1$ *such that* $\mathrm{Kill}(x_{i_1,j'}\cdots x_{i_d,j_d}) \in \Delta_I$.

Properties of Kill

Theorem

$x_{i_1,j_1} \cdots x_{i_d,j_d} \in \Delta_I$ if and only if there is a $j' > j_1$ such that $\mathrm{Kill}(x_{i_1,j'} \cdots x_{i_d,j_d}) \in \Delta_I$.

Proof

This operator effectively moves the first pigeon to an empty hole and then kills it. This is the same as each step in the dance, where the first pigeon flies to some free hole to its right and then occupies it. □

Properties of Kill (cont.)

Theorem

Δ_I *is closed under* Kill.

Properties of Kill (cont.)

Theorem

Δ_I *is closed under* Kill.

Proof

If $t \in \Delta_I$ then the pigeons can complete their dance. During this the first pigeon will start at j and fly to j'. Killing the pigeon frees up j' so any other pigeon that wanted to use j can use it instead. $\square$

The lower bound

Theorem

If $|I| \leq (n+1)/2, t \in D_I$ and the minimal element i of I is not in $\mathrm{dom}(t)$, then there exists a $j \in [n]$ such that $\mathrm{Kill}(x_{ij}t) \in \Delta_I$.

The lower bound

Theorem

If $|I| \leq (n+1)/2, t \in D_I$ *and the minimal element* i *of* I *is not in* $\operatorname{dom}(t)$, *then there exists a* $j \in [n]$ *such that* $\operatorname{Kill}(x_{ij}t) \in \Delta_I$.

Proof

At most

$$|\operatorname{dom}(t)| \leq |I \setminus \{i\}| \leq \frac{n-1}{2}$$

pigeons involved in the dance, each occupying two holes. Thus the total number of holes is $n-1$ and one hole j remains free. For the purposes of the dance, $\operatorname{Kill}(x_{ij} \cdot t)$ is the same as t since the only difference is j being moved to the left. □

Putting things together

- We now show that the two operators are identical

Putting things together

- We now show that the two operators are identical
- Equivalent to Δ_I being linearly independent as functions $M_I \to \mathbb{K}$

Putting things together

- We now show that the two operators are identical
- Equivalent to Δ_I being linearly independent as functions $M_I \to \mathbb{K}$
- Induction on $|I|$ gives us assignment $a \in M_{I \setminus \{i\}}$ with $a(f') \neq 0$

Putting things together

- We now show that the two operators are identical
- Equivalent to Δ_I being linearly independent as functions $M_I \to \mathbb{K}$
- Induction on $|I|$ gives us assignment $a \in M_{I \setminus \{i\}}$ with $a(f') \neq 0$
- Pick a j such that $\mathrm{Kill}(x_{i,j}t) \in \Delta_I$

Putting things together

- We now show that the two operators are identical
- Equivalent to Δ_I being linearly independent as functions $M_I \to \mathbb{K}$
- Induction on $|I|$ gives us assignment $a \in M_{I \setminus \{i\}}$ with $a(f') \neq 0$
- Pick a j such that $\mathrm{Kill}(x_{i,j}t) \in \Delta_I$
- Extend assignment to I with $a'(f) \neq 0$

Summary

- If $d \leq n/2 + 1$, then definition of R_I via the pigeon dance and via M_I are identical

Summary

- If $d \leq n/2 + 1$, then definition of R_I via the pigeon dance and via M_I are identical
- Pigeons not in the dance do not affect its success, so $R_I(t) = R_{\mathrm{dom}(t)}(t)$

Summary

- If $d \leq n/2 + 1$, then definition of R_I via the pigeon dance and via M_I are identical
- Pigeons not in the dance do not affect its success, so $R_I(t) = R_{\mathrm{dom}(t)}(t)$
- V_d is precisely polynomials identically zero on M_I

Summary

- If $d \leq n/2 + 1$, then definition of R_I via the pigeon dance and via M_I are identical
- Pigeons not in the dance do not affect its success, so $R_I(t) = R_{\mathrm{dom}(t)}(t)$
- V_d is precisely polynomials identically zero on M_I
- $R_d \neq 0$

Summary

- If $d \leq n/2 + 1$, then definition of R_I via the pigeon dance and via M_I are identical
- Pigeons not in the dance do not affect its success, so $R_I(t) = R_{\mathrm{dom}(t)}(t)$
- V_d is precisely polynomials identically zero on M_I
- $R_d \neq 0$
- There is no refutation of $\neg\mathcal{PHP}_n^m$ with $d \leq n/2 + 1$