Lower Bounds for the Polynomial Calculus via the "Pigeon Dance"

Imogen Hergeth

January 2023

Overview

We will present the result from A.A. Razborov, "Lower Bounds for the Polynomial Calculus", in: Computational Complexity 7.4 (Dec. 2, 1998).

1. Introduction
2. The Pigeonhole Principle
3. The Pigeon Dance
4. Conclusion

Background

- Lower bounds for proofs in various systems

Background

- Lower bounds for proofs in various systems
- In particular for the pigeonhole principle

Background

- Lower bounds for proofs in various systems
- In particular for the pigeonhole principle
- Polynomial calculus is a strong proof system

Background

- Lower bounds for proofs in various systems
- In particular for the pigeonhole principle
- Polynomial calculus is a strong proof system
- Provide a lower bound for it with the pigeonhole principle

Definition

- Similar to sequent calculus, but lines are polynomials

Definition

- Similar to sequent calculus, but lines are polynomials
- We use multilinear polynomials $S_n(\mathbb{K})$
  $(xy + xz + v \equiv x^2y + x^3z^5 + v)$

Definition

- Similar to sequent calculus, but lines are polynomials
- We use multilinear polynomials $S_n(\mathbb{K})$
  $(xy + xz + v \equiv x^2y + x^3z^5 + v)$
- Addition

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

Definition

- Similar to sequent calculus, but lines are polynomials
- We use multilinear polynomials $S_n(\mathbb{K})$
  $(xy + xz + v \equiv x^2y + x^3z^5 + v)$
- Addition

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

- Multiplication

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

Refutations

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

Refutations

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

Refutations

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

Refutations

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

Example proof

- Try to prove $xy + z$ from $x + 1$ and z

Example proof

- Try to prove $xy + z$ from $x + 1$ and z

$$x + 1$$

Example proof

- Try to prove $xy + z$ from $x + 1$ and z

$$(\cdot y)\,\frac{x+1}{xy+y}$$

Example proof

- Try to prove $xy + z$ from $x + 1$ and z

$$\dfrac{(\cdot y)\,\dfrac{x+1}{xy+y} \qquad z}{xy+y+z}\,(+)$$

Example proof

- Try to prove $xy + z$ from $x + 1$ and z

$$\dfrac{(\cdot y)\,\dfrac{x+1}{xy+y} \qquad z}{xy+y+z}\,(+)$$

- We now want to subtract y

Example proof

- Try to prove $xy + z$ from $x + 1$ and z

$$\dfrac{(\cdot y)\,\dfrac{x+1}{xy+y} \qquad z}{xy+y+z}\,(+)$$

- We now want to subtract y
- There is no way to prove y from $x + 1$ and z

Example proof

- Try to prove $xy + z$ from $x + 1$ and z

$$\dfrac{(\cdot y)\,\dfrac{x+1}{xy+y} \qquad z}{xy+y+z}\ (+)$$

- We now want to subtract y
- There is no way to prove y from $x + 1$ and z
- Closest to $xy + z$ we can prove is $xy + y + z$

Algebraic view of proofs

Algebraic view of proofs

- Think of polynomials not just as lines but as elements of a $\mathbb{K}$-algebras

Algebraic view of proofs

- Think of polynomials not just as lines but as elements of a $\mathbb{K}$-algebras
- V are polynomials we can prove

$xy + y + z$

Algebraic view of proofs

- Think of polynomials not just as lines but as elements of a $\mathbb{K}$-algebras
- V are polynomials we can prove $xy + y + z$
- Δ are leading terms of ones we cannot prove y

Algebraic view of proofs

- Think of polynomials not just as lines but as elements of a $\mathbb{K}$-algebras
- V are polynomials we can prove $\quad xy + y + z$
- Δ are leading terms of ones we cannot prove $\quad y$
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V \quad xy + z = -y + xy + y + z$

Algebraic view of proofs

- Think of polynomials not just as lines but as elements of a $\mathbb{K}$-algebras
- V are polynomials we can prove $\quad xy + y + z$
- Δ are leading terms of ones we cannot prove $\quad y$
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V \quad xy + z = -y + xy + y + z$
- Similarly V_I, Δ_I using subset of variables I

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: $x_{ij}, i \in [m], j \in [n]$

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: $x_{ij}, i \in [m], j \in [n]$
- 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: $x_{ij}, i \in [m], j \in [n]$
- Assignment of $x_{3,5}$ corresponds to pigeon 3 being in hole 5

Definition ($\neg\mathcal{PHP}^m_n$)

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

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

Main result

Theorem

Every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ *must have degree at least* $n/2+1$.

Main result

Theorem

Every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ *must have degree at least* $n/2 + 1$.

- $\neg\mathcal{PHP}_n^m$ are constraints on pigeon assignments

Main result

Theorem

Every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ *must have degree at least* $n/2+1$.

- $\neg\mathcal{PHP}_n^m$ are constraints on pigeon assignments
- Proofs combine them into more complex ones

Main result

Theorem

Every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ *must have degree at least* $n/2+1$.

- $\neg\mathcal{PHP}_n^m$ are constraints on pigeon assignments
- Proofs combine them into more complex ones
- Can only derive local constraints with small degrees

Main result

Theorem

Every polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ *must have degree at least* $n/2+1$.

- $\neg\mathcal{PHP}_n^m$ are constraints on pigeon assignments
- Proofs combine them into more complex ones
- Can only derive local constraints with small degrees
- Pigeons can fly away to escape local contradictions

$\neg\mathcal{PHP}_n^m$ constraints

$\neg\mathcal{PHP}_n^m$ constraints

- Pigeons cannot share holes

$\neg\mathcal{PHP}_n^m$ constraints

- Pigeons cannot share holes
- Possible for pigeons $I \subseteq [m]$ with $|I| \leq n$

$\neg\mathcal{PHP}_n^m$ constraints

- Pigeons cannot share holes
- Possible for pigeons $I \subseteq [m]$ with $|I| \leq n$
- Locally valid assignments are injections $I \hookrightarrow [n]$

$\neg\mathcal{PHP}^m_n$ constraints

- Pigeons cannot share holes
- Possible for pigeons $I \subseteq [m]$ with $|I| \leq n$
- Locally valid assignments are injections $I \hookrightarrow [n]$
- Corresponding variable assignments are M_I

Locally valid assignments

- Characterize V_I as the set of all polynomials with $a(f) = 0$ for all $a \in M_I$

Locally valid assignments

- Characterize V_I as the set of all polynomials with $a(f) = 0$ for all $a \in M_I$
- We're done! Clearly not all polynomials are identically zero on M_I

Locally valid assignments

- Characterize V_I as the set of all polynomials with $a(f) = 0$ for all $a \in M_I$
- We're done! Clearly not all polynomials are identically zero on M_I
- This definition completely ignores the degrees of the proofs!

Locally valid assignments

- Characterize V_I as the set of all polynomials with $a(f) = 0$ for all $a \in M_I$
- We're done! Clearly not all polynomials are identically zero on M_I
- This definition completely ignores the degrees of the proofs!
- Only works if whether $t \in \Delta_I$ is independent of $I \supseteq \mathrm{dom}(t)$

Overview

- Goal:

Overview

- Goal:
  - Use pigeon dance to characterize Δ_I

Overview

- Goal:
  - Use pigeon dance to characterize Δ_I
  - Prove this Δ_I is exaclty the leading terms of underivable polynomials

Overview

- Goal:
  - Use pigeon dance to characterize Δ_I
  - Prove this Δ_I is exaclty the leading terms of underivable polynomials
- Start with pigeons sitting in their holes

Overview

- Goal:
  - Use pigeon dance to characterize Δ_I
  - Prove this Δ_I is exaclty the leading terms of underivable polynomials
- Start with pigeons sitting in their holes
- The first pigeon flies to an unoccupied hole to its right

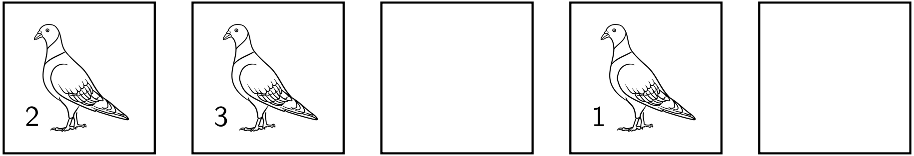
Overview

- Goal:
  - Use pigeon dance to characterize Δ_I
  - Prove this Δ_I is exaclty the leading terms of underivable polynomials
- Start with pigeons sitting in their holes
- The first pigeon flies to an unoccupied hole to its right
- Repeat until all pigeons have moved once

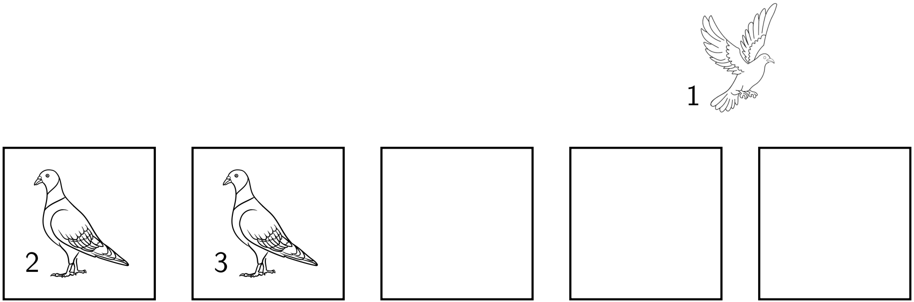
Overview

- Goal:
  - Use pigeon dance to characterize Δ_I
  - Prove this Δ_I is exaclty the leading terms of underivable polynomials
- Start with pigeons sitting in their holes
- The first pigeon flies to an unoccupied hole to its right
- Repeat until all pigeons have moved once
- If a pigeon cannot find an empty hole, the dance is aborted

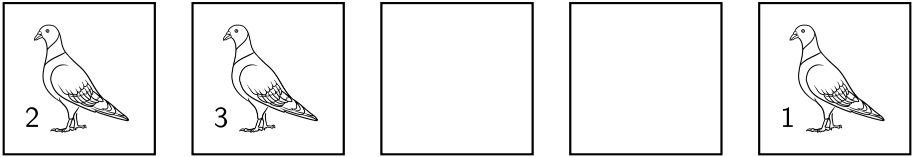
Example



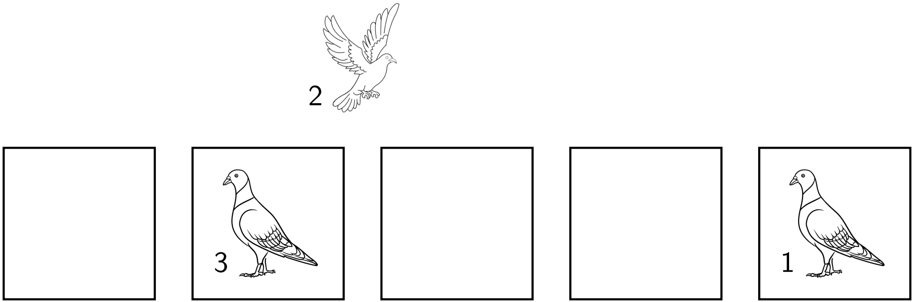
Example



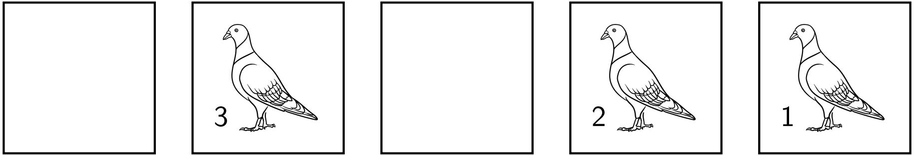
Example



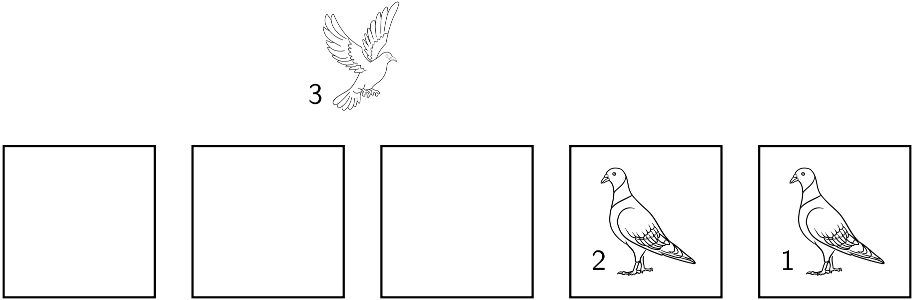
Example



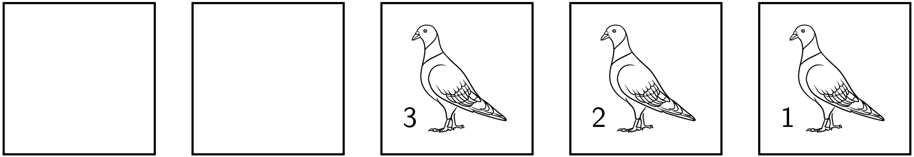
Example



Example



Example



Formalization

- Consider partial injections $I \hookrightarrow [m]$ $\qquad (1 \mapsto 4,\ \ 2 \mapsto 1,\ \ 3 \mapsto 2)$

Formalization

- Consider partial injections $I \hookrightarrow [m]$ $\quad (1 \mapsto 4,\ 2 \mapsto 1,\ 3 \mapsto 2)$
- Encode pigeon positions as terms $\quad (x_{1,4}\, x_{2,1}\, x_{3,2})$

Formalization

- Consider partial injections $I \hookrightarrow [m]$ $\quad (1 \mapsto 4,\ 2 \mapsto 1,\ 3 \mapsto 2)$
- Encode pigeon positions as terms $\quad (x_{1,4}\, x_{2,1}\, x_{3,2})$
- Δ_I is the set of terms that let pigeons complete the dance

Formalization

- Consider partial injections $I \hookrightarrow [m]$ $\qquad (1 \mapsto 4,\ 2 \mapsto 1,\ 3 \mapsto 2)$
- Encode pigeon positions as terms $\qquad (x_{1,4}\, x_{2,1}\, x_{3,2})$
- Δ_I is the set of terms that let pigeons complete the dance
- Whether $t \in \Delta_I$ is independent of I since pigeons not in the dance do not affect it

The Kill operator

- We need to further understand the dance to prove it correct

The Kill operator

- We need to further understand the dance to prove it correct
- Idea: a way to block specific pigeon holes

The Kill operator

- We need to further understand the dance to prove it correct
- Idea: a way to block specific pigeon holes
- Kill the first pigeon and moves its hole to the left

The Kill operator

- We need to further understand the dance to prove it correct
- Idea: a way to block specific pigeon holes
- Kill 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

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

Simulating the pigeon dance with Kill

Simulating the pigeon dance with 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* $\mathrm{Kill}(x_{i_1 j'} \cdots x_{i_d j_d}) \in \Delta_I$.

Simulating the pigeon dance with 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 sketch

$\mathrm{Kill}(x_{i_1 j'} \cdots x_{i_d j_d})$ effectively moves the first pigeon to an empty hole to its right 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. $\square$

Closure of Δ_I

Theorem

Δ_I *is closed under* Kill.

Closure of Δ_I

Theorem

Δ_I *is closed under* Kill.

Proof sketch

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 $|I| \leq (n+1)/2$ *and pigeons can complete the dance, then we can introduce a new pigeon such that* $\mathrm{Kill}(x_{ij}t) \in \Delta_I$.

The lower bound

Theorem

If $|I| \leq (n+1)/2$ *and pigeons can complete the dance, then we can introduce a new pigeon such that* $\mathrm{Kill}(x_{ij}t) \in \Delta_I$.

Proof sketch

At most

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

pigeons involved in the dance, each occupying two holes. Place pigeon at unused hole and kill it there. The remaining pigeons can complete the dance since the moved hole was not used. □

Putting things together

- Goal: show pigeon dance correctly characterizes underivable polynomials

Putting things together

- Goal: show pigeon dance correctly characterizes underivable polynomials
- Formally: each $f \in \mathbb{K}\Delta_I$ has an $a \in M_I$ with $a(f) \neq 0$

Putting things together

- Goal: show pigeon dance correctly characterizes underivable polynomials
- Formally: each $f \in \mathbb{K}\Delta_I$ has an $a \in M_I$ with $a(f) \neq 0$
- Induction over $|I|$

Putting things together

- Goal: show pigeon dance correctly characterizes underivable polynomials
- Formally: each $f \in \mathbb{K}\Delta_I$ has an $a \in M_I$ with $a(f) \neq 0$
- Induction over $|I|$
- Remove variables x_{ij} for minimal $i \in I$ from f

Putting things together

- Goal: show pigeon dance correctly characterizes underivable polynomials
- Formally: each $f \in \mathbb{K}\Delta_I$ has an $a \in M_I$ with $a(f) \neq 0$
- Induction over $|I|$
- Remove variables x_{ij} for minimal $i \in I$ from f
- Inductive assumption gives us $a' \in M_{I\setminus\{i\}}$ with $a'(f') \neq 0$ closure of Δ_I

Putting things together

- Goal: show pigeon dance correctly characterizes underivable polynomials
- Formally: each $f \in \mathbb{K}\Delta_I$ has an $a \in M_I$ with $a(f) \neq 0$
- Induction over $|I|$
- Remove variables x_{ij} for minimal $i \in I$ from f
- Inductive assumption gives us $a' \in M_{I \setminus \{i\}}$ with $a'(f') \neq 0$ closure of Δ_I
- Pick a j such that $\mathrm{Kill}(x_{ij}t) \in \Delta_I$ lower bound

Putting things together

- Goal: show pigeon dance correctly characterizes underivable polynomials
- Formally: each $f \in \mathbb{K}\Delta_I$ has an $a \in M_I$ with $a(f) \neq 0$
- Induction over $|I|$
- Remove variables x_{ij} for minimal $i \in I$ from f
- Inductive assumption gives us $a' \in M_{I \setminus \{i\}}$ with $a'(f') \neq 0$ closure of Δ_I
- Pick a j such that $\mathrm{Kill}(x_{ij}t) \in \Delta_I$ lower bound
- Extend assignment to I with $a(f) \neq 0$

Summary

- Proven a lower bound $d \geq n/2 + 1$ for polynomial calculus refutations of $\neg\mathcal{PHP}_n^m$

Summary

- Proven a lower bound $d \geq n/2 + 1$ for polynomial calculus refutations of $\neg\mathcal{PHP}_n^m$
- Characterize derivable polynomials V_I through locally consistent assignments M_I

Summary

- Proven a lower bound $d \geq n/2 + 1$ for polynomial calculus refutations of $\neg\mathcal{PHP}_n^m$
- Characterize derivable polynomials V_I through locally consistent assignments M_I
- This only works if membership in Δ_I is independent of I

Summary

- Proven a lower bound $d \geq n/2 + 1$ for polynomial calculus refutations of $\neg\mathcal{PHP}_n^m$
- Characterize derivable polynomials V_I through locally consistent assignments M_I
- This only works if membership in Δ_I is independent of I
- Characterize Δ_I through pigeon dance

Summary

- Proven a lower bound $d \geq n/2 + 1$ for polynomial calculus refutations of $\neg\mathcal{PHP}_n^m$
- Characterize derivable polynomials V_I through locally consistent assignments M_I
- This only works if membership in Δ_I is independent of I
- Characterize Δ_I through pigeon dance
- This works since Δ_I is linearly independent over M_I