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

- V are polynomials we can prove $\qquad xy + y + z$
- Δ are leading terms of ones we cannot prove $\qquad y$
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V \qquad xy + z = -y + xy + y + z$
- R is the projection onto $\Delta \qquad R(xy + z) = y$
- Similarly:
  V_d, Δ_d, R_d for polynomials up to degree d
  V_I, Δ_I, R_I for polynomials using variables for subset of pigeons 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: $x_{ij}, i \in [m], n \in [n]$

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: $x_{ij}, i \in [m], n \in [n]$
- 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: $x_{ij}, i \in [m], n \in [n]$
- 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* $n/2+1$.

- Derived polynomials are constraints on pigeon assignments

Main result

Theorem

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

- Derived polynomials are constraints on pigeon assignments
- Locally valid assignments are possible

Main result

Theorem

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

- Derived polynomials are constraints on pigeon assignments
- Locally valid assignments are possible
- Polynomials need to have large degree to prove inconsitencies

Semantics of $\neg\mathcal{PHP}_n^m$

- Pigeons cannot share holes

Semantics of $\neg\mathcal{PHP}_n^m$

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

Semantics of $\neg\mathcal{PHP}_n^m$

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

Semantics of $\neg\mathcal{PHP}^m_n$

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

Semantics of $\neg\mathcal{PHP}_n^m$

- Pigeons cannot share holes
- Possible for pigeons $I \subseteq [m]$ with $|I| \leq n$
- Locally valid assignments are injections $I \hookrightarrow [n]$
- Corresponding varliable assignments are M_I
- V_I is the set of all polynomials with $a(f) = 0$ for all $a \in M_I$

Done?

- Not all polynomials are identically zero on M_I

Done?

- Not all polynomials are identically zero on M_I
- This definition completely ignores the degrees of the proofs!

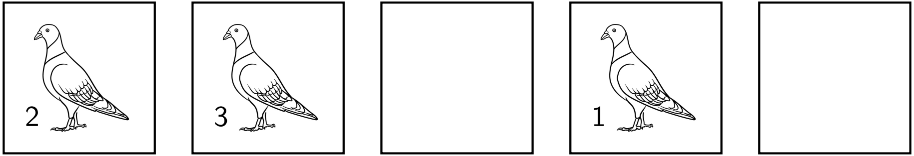
Done?

- Not all polynomials are identically zero on M_I
- This definition completely ignores the degrees of the proofs!
- It only works if $R_I(t)$ is independent of I

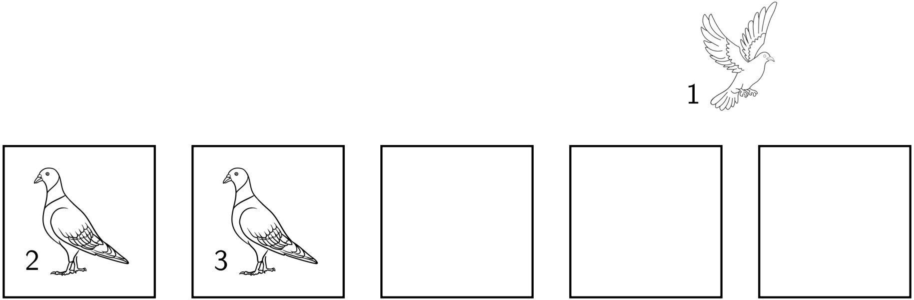
Done?

- Not all polynomials are identically zero on M_I
- This definition completely ignores the degrees of the proofs!
- It only works if $R_I(t)$ is independent of I
- Looks like this does not work at all

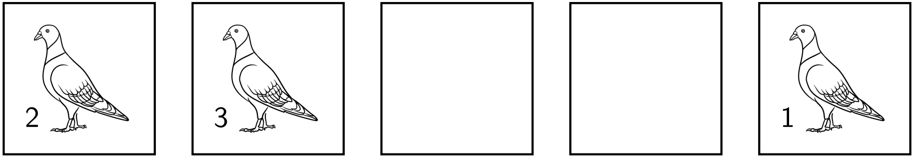
Example



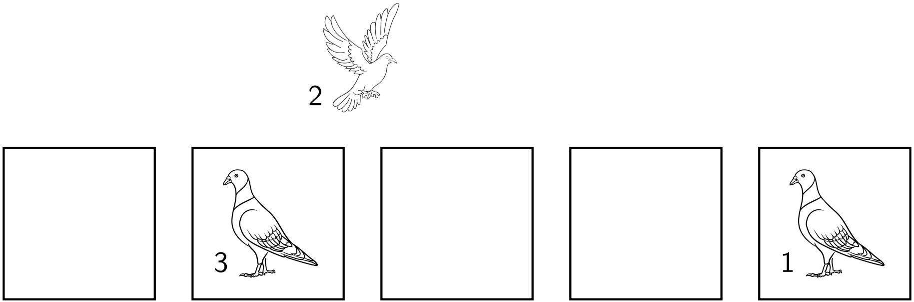
Example



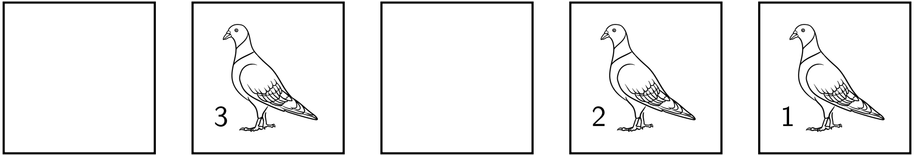
Example



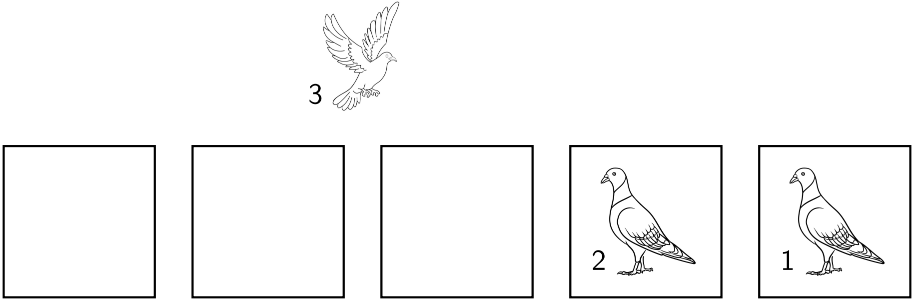
Example



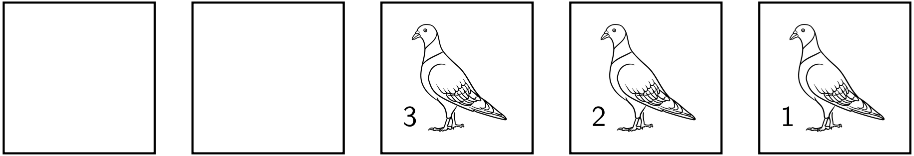
Example



Example



Example



The pigeon dance

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

The pigeon dance

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

The pigeon dance

- 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

The pigeon dance

- 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
- Encode pigeon positions as terms $(x_{1,4}x_{2,1}x_{3,2})$

The pigeon dance

- 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
- Encode pigeon positions as terms $(x_{1,4}x_{2,1}x_{3,2})$
- Δ_I is the set of terms that let pigeons complete the dance

The pigeon dance

- 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
- Encode pigeon positions as terms $(x_{1,4}x_{2,1}x_{3,2})$
- Δ_I is the set of terms that let pigeons complete the dance
- $t \in \Delta_I$ independent of I since pigeons not in the dance do not affect it

The Kill operator

- Idea: operator that lets us block specific holes

The Kill operator

- Idea: operator that lets us block specific holes
- The Kill operator kills the first pigeon and moves its hole to the left

The Kill operator

- Idea: operator that lets us block specific holes
- 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

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

The dance in terms 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 sketch

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

Proof sketch

At most

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

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, $\mathrm{Kill}(x_{ij}t)$ is the same as t since the only difference is j being moved to the left. $\square$

Putting things together

- Prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable

Putting things together

- Prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable
- Each f has a locally consistent assignment $a \in M_I$ with $a(f) \neq 0$

Putting things together

- Prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable
- Each f has a locally consistent assignment $a \in M_I$ with $a(f) \neq 0$
- Induction over $|I|$

Putting things together

- Prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable
- Each f has a locally consistent assignment $a \in M_I$ with $a(f) \neq 0$
- Induction over $|I|$
- Remove variables x_{ij} for minimal $i \in I$ from f

Putting things together

- Prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable
- Each f has a locally consistent assignment $a \in M_I$ 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 $a'(f') \neq 0$

Putting things together

- Prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable
- Each f has a locally consistent assignment $a \in M_I$ 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 $a'(f') \neq 0$
- Pick a j such that $\mathrm{Kill}(x_{ij}t) \in \Delta_I$

Putting things together

- Prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable
- Each f has a locally consistent assignment $a \in M_I$ 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 $a'(f') \neq 0$
- Pick a j such that $\mathrm{Kill}(x_{ij}t) \in \Delta_I$
- Extend assignment to I with $a(f) \neq 0$

Summary

Theorem

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

Summary

Theorem

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

- If the degree is small, pigeons can complete the dance

Summary

Theorem

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

- If the degree is small, pigeons can complete the dance
- You need to have $n/2 + 1$ pigeons to block enough holes

Summary

Theorem

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

- If the degree is small, pigeons can complete the dance
- You need to have $n/2+1$ pigeons to block enough holes
- Only polynomials corresponding to locally consistent assignments are derivable