Imogen Hergeth

January 2023

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

- Introduction
- 2 The Pigeonhole Principle
- The Pigeon Dance
- 4 Conclusion

Introduction ••••••

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

The Pigeon Dance

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

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

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

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

Multiplication

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

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

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

- 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

- 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
- ullet Proving 1 from them is a refutation

Introduction 0000•0

Example proof

Introduction

Example proof

$$x + 1$$

Example proof

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

000000

Example proof

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

Example proof

• Try to prove xy + z from x + 1 and z

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

ullet We now want to subtract y

Example proof

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

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

Example proof

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

- 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

- ullet V are polynomials we can prove
- \bullet \triangle are leading terms of ones we cannot prove
- $S_n(\mathbb{K}) \cong \mathbb{K} \Delta \oplus V$
- Similarly V_I, Δ_I using subset of variables I

$$xy + y + z$$

u

$$xy + z = -y + xy + y + z$$

The pigeonhole principle

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

The pigeonhole principle

- ullet 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

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

Overviev

The pigeonhole principle

- ullet 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

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

$$Q_i \coloneqq 1 - \sum_{i \in [n]} x_{ij}$$

$$\text{ for each } i \in [m]$$

$$Q_{i_1,i_2,j} \coloneqq x_{i_1j} x_{i_2j}$$

for each
$$i_1 \neq i_2 \in [m], j \in [n]$$

Overviev

Main result

Theorem

Overviev

Main result

Theorem

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

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

Main result

Theorem

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

Pigeon Dance

Overviev

Main result

Theorem

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

Main result

Theorem

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

Pigeons cannot share holes

Overviev

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

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

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

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

Overviev

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

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

 \bullet V_I is the set of all polynomials with a(f)=0 for all $a\in M_I$

Overviev

- ullet V_I is the set of all polynomials with a(f)=0 for all $a\in M_I$
- ullet Not all polynomials are identically zero on M_I

- ullet V_I is the set of all polynomials with a(f)=0 for all $a\in M_I$
- ullet Not all polynomials are identically zero on M_I
- But, this definition completely ignores the degrees of the proofs!

- ullet V_I is the set of all polynomials with a(f)=0 for all $a\in M_I$
- ullet Not all polynomials are identically zero on M_I
- But, this definition completely ignores the degrees of the proofs!
- It still works, but only if $t \in \Delta_I$ is independent of I

- ullet V_I is the set of all polynomials with a(f)=0 for all $a\in M_I$
- ullet Not all polynomials are identically zero on M_I
- But, this definition completely ignores the degrees of the proofs!
- It still works, but only if $t \in \Delta_I$ is independent of I
- Use pigeon dance to see this













































































The pigeon dance

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

Idea

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

- 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 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 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 $(x_{1,4}, x_{2,1}, x_{3,2})$
- \bullet Δ_I is the set of terms that let pigeons complete the 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 $(x_{1,4} x_{2,1} x_{3,2})$
- ullet Δ_I is the set of terms that let pigeons complete the dance
- ullet $t \in \Delta_I$ 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
- $\operatorname{Kill}(x_{i_1j_1}\cdots x_{i_d,j_d})=x_{i_2j'_2}\cdots x_{i_dj'_d}$ with

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

Simulating the pigeon dance with Kill

Simulating the pigeon dance with Kill

Theorem

 $x_{i_1j_1}\cdots x_{i_dj_d}\in \Delta_I$ if and only if there is a $j'>j_1$ such that $\mathrm{Kill}(x_{i_1j'}\cdots x_{i_dj_d})\in \Delta_I$.

Simulating the pigeon dance with Kill

Theorem

 $x_{i_1j_1}\cdots x_{i_dj_d}\in \Delta_I$ if and only if there is a $j'>j_1$ such that $\mathrm{Kill}(x_{i_1j'}\cdots x_{i_dj_d})\in \Delta_I$.

Proof sketch

 $\operatorname{Kill}(x_{i_1j'}\cdots x_{i_dj_d})$ 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.

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.

The lower bound

Theorem

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

Propertie:

The lower bound

Theorem

If $|I| \le (n+1)/2$ 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

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

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.

• Goal: prove polynomials $f \in \mathbb{K}\Delta_I$ are not derivable

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

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

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

- Goal: 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 $a'(f') \neq 0$

- Goal: 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 $Kill(x_{ij}t) \in \Delta_I$

- Goal: 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 $Kill(x_{ij}t) \in \Delta_I$
- Extend assignment to I with $a(f) \neq 0$

Summary

• Proven a lower bound for polynomial calculus proofs

Summary

- Proven a lower bound for polynomial calculus proofs
- If the degree is small, pigeons can complete the dance

Summary

- Proven a lower bound for polynomial calculus proofs
- If the degree is small, pigeons can complete the dance
- ullet You need to have n/2+1 pigeons to force a contradiction