

# 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

# 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

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

# 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

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

- Multiplication

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

# Motivation

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

# Motivation

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



# Motivation

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

# Motivation

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

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

$$\frac{xy+y+z}{xy+y+z}$$

# Example proof

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

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

$$\frac{xy + y + z}{xy + y + z}$$

- We now want to subtract  $y$

# Example proof

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

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

$$\frac{xy + y + z}{xy + y + z}$$

- 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  $z$

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

- 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

$$xy + y + z$$

# Algebraic view of proofs

- $V$  are polynomials we can prove
- $\Delta$  are leading terms of ones we cannot prove

$$xy + y + z$$

$$y$$



# Algebraic view of proofs

- $V$  are polynomials we can prove
- $\Delta$  are leading terms of ones we cannot prove
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V$

$$xy + y + z$$

$$y$$

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

# Algebraic view of proofs

- $V$  are polynomials we can prove
- $\Delta$  are leading terms of ones we cannot prove
- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V$
- $R$  is the projection onto  $\Delta$

$$xy + y + z$$

$$y$$

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

$$R(xy + z) = y$$

# Algebraic view of proofs

- $V$  are polynomials we can prove
- $\Delta$  are leading terms of ones we cannot prove

$$xy + y + z$$

- $S_n(\mathbb{K}) \cong \mathbb{K}\Delta \oplus V$

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

- $R$  is the projection onto  $\Delta$

$$R(xy + z) = y$$

- Similarly:

$V_d, \Delta_d, R_d$  for polynomials up to degree  $d$

$V_I, \Delta_I, R_I$  for polynomials using variables for pigeons in  $I$

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

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

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



# Main result

## Theorem

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

# Main result

## Theorem

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

- Characterize  $R_d$  semantically

# Main result

## Theorem

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

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

# Main result

## Theorem

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

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

# Main result

## Theorem

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

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

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

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

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

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

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

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

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



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

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

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

- Polynomials are evaluated to 0 if they allow the assignment

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

$$a(x_{1,1}x_{3,1}) = a(x_{1,2}x_{2,2}) = 0$$

# Characterizing $R_I$

- $M_I$  is the set of all assignments corresponding to injections  $I \hookrightarrow [m]$
- $V_I$  is polynomials that  $M_I$  evaluates to 0
- Define  $\Delta_I, R_I$  to be the restrictions of  $\Delta, R$  onto  $I$
- Note: this definition completely ignores degrees

## Combining $R_I$

- We want a characterization of  $R_d$ , not  $R_I$

Combining  $R_I$ 

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

# Combining $R_I$

- We want a characterization of  $R_d$ , not  $R_I$
- $V_d := \bigcup_{|I| \leq d} V_I$
- $R_d := R_{\text{dom}(t)}(t)$

Combining  $R_I$ 

- We want a characterization of  $R_d$ , not  $R_I$
- $V_d := \bigcup_{|I| \leq d} V_I$
- $R_d := R_{\text{dom}(t)}(t)$
- Does this definition actually work?

Combining  $R_I$ 

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

## Idea

- Goal: define  $R_I(t)$  so that it is independent of  $I \setminus \text{dom}(t)$



## Idea

- Goal: define  $R_I(t)$  so that it is independent of  $I \setminus \text{dom}(t)$
- We first define  $\Delta_I$  using the pigeon dance

## Idea

- Goal: define  $R_I(t)$  so that it is independent of  $I \setminus \text{dom}(t)$
- We first define  $\Delta_I$  using the pigeon dance
- The first pigeon flies to an unoccupied hole to its right

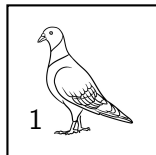
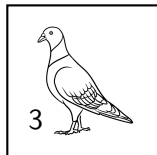
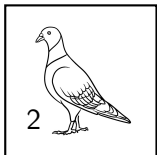
## Idea

- Goal: define  $R_I(t)$  so that it is independent of  $I \setminus \text{dom}(t)$
- We first define  $\Delta_I$  using the pigeon dance
- The first pigeon flies to an unoccupied hole to its right
- Repeat until all pigeons have moved once

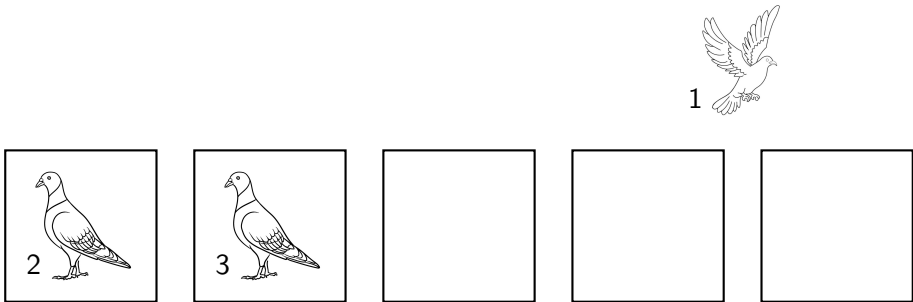
## Idea

- Goal: define  $R_I(t)$  so that it is independent of  $I \setminus \text{dom}(t)$
- We first define  $\Delta_I$  using 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

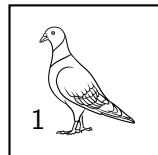
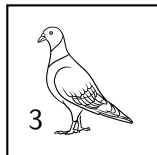
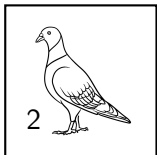
# Example



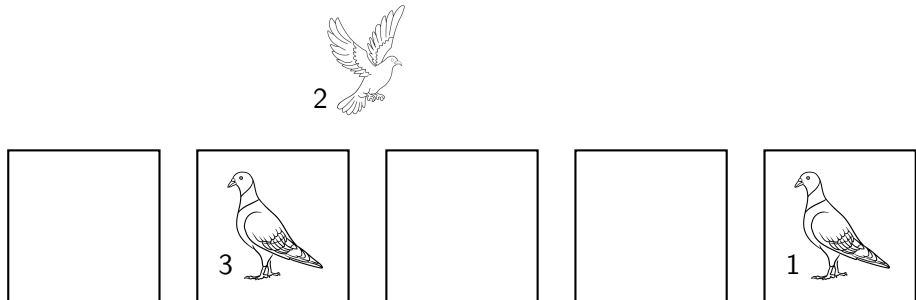
# Example



# Example



# Example

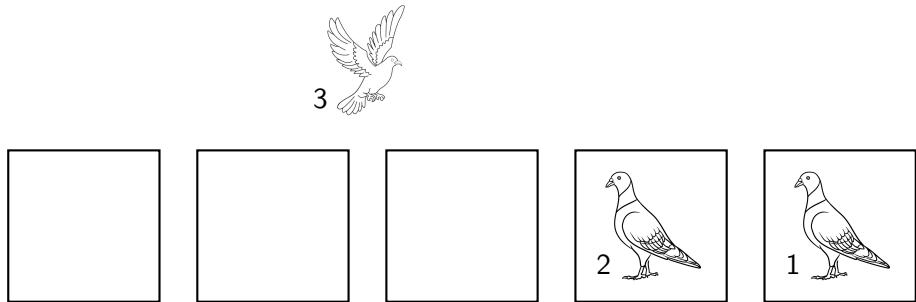




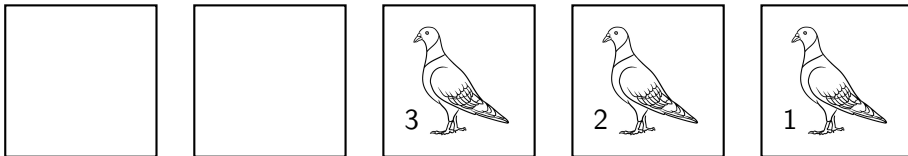
# Example



# Example



# Example



# Formalization

- Consider terms  $x_{i_1j_1} \cdots x_{i_dj_d}$  with all  $i$  and  $j$  pairwise different

# Formalization

- Consider terms  $x_{i_1j_1} \cdots x_{i_dj_d}$  with all  $i$  and  $j$  pairwise different
- Variables occurring in term correspond to pigeon positions

# Formalization

- Consider terms  $x_{i_1j_1} \cdots x_{i_dj_d}$  with all  $i$  and  $j$  pairwise different
- Variables occurring in term correspond to pigeon positions
- Define  $\Delta_I$  to be the set of terms that let pigeons complete the dance

# Formalization

- Consider terms  $x_{i_1j_1} \cdots x_{i_dj_d}$  with all  $i$  and  $j$  pairwise different
- Variables occurring in term correspond to pigeon positions
- Define  $\Delta_I$  to be 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

Defining  $R_I$ 

- We need  $R_I(t) = f$  with  $\text{LT}(f) \preceq t$  and  $t = f \pmod{V_I}$



Defining  $R_I$ 

- We need  $R_I(t) = f$  with  $\text{LT}(f) \preceq t$  and  $t = f \pmod{V_I}$
- If  $t \in \Delta_I$ , then  $f := t$

Defining  $R_I$ 

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

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

Defining  $R_I$ 

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

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

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

Defining  $R_I$ 

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

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

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

Defining  $R_I$  (cont.)

- Remaining terms have  $i > i_1$ ,  $j' > j_1$ , and  $j' \notin \{j_2, \dots, j_d\}$

Defining  $R_I$  (cont.)

- Remaining terms have  $i > i_1$ ,  $j' > j_1$ , and  $j' \notin \{j_2, \dots, j_d\}$
- Repeat the same process with all of them

Defining  $R_I$  (cont.)

- Remaining terms have  $i > i_1$ ,  $j' > j_1$ , and  $j' \notin \{j_2, \dots, j_d\}$
- Repeat the same process with all of them
- At each step the next  $i$  has  $x_{ij}$  replaced with  $x_{ij'}$  for some unused  $j' > j$

Defining  $R_I$  (cont.)

- Remaining terms have  $i > i_1$ ,  $j' > j_1$ , and  $j' \notin \{j_2, \dots, j_d\}$
- Repeat the same process with all of them
- At each step the next  $i$  has  $x_{ij}$  replaced with  $x_{ij'}$  for some unused  $j' > j$
- This is the pigeon dance!



Defining  $R_I$  (cont.)

- Remaining terms have  $i > i_1$ ,  $j' > j_1$ , and  $j' \notin \{j_2, \dots, j_d\}$
- Repeat the same process with all of them
- At each step the next  $i$  has  $x_{ij}$  replaced with  $x_{ij'}$  for some unused  $j' > j$
- This is the pigeon dance!
- Since  $t \notin \Delta_I$  the dance cannot be completed

Defining  $R_I$  (cont.)

- Remaining terms have  $i > i_1$ ,  $j' > j_1$ , and  $j' \notin \{j_2, \dots, j_d\}$
- Repeat the same process with all of them
- At each step the next  $i$  has  $x_{ij}$  replaced with  $x_{ij'}$  for some unused  $j' > j$
- This is the pigeon dance!
- Since  $t \notin \Delta_I$  the dance cannot be completed
- Process terminates with  $\text{LT}(f) \prec t$  and  $t = f \pmod{V_I}$

# 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
- $\text{Kill}(x_{i_1 j_1} \cdots x_{i_d j_d}) = x_{i_2 j'_2} \cdots x_{i_d j'_d}$  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  $\text{Kill}(x_{i_1 j'} \cdots x_{i_d j_d}) \in \Delta_I$ .

## 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. □

Closure of  $\Delta_I$ 

## Theorem

$\Delta_I$  is closed under Kill.

Closure of  $\Delta_I$ 

## Theorem

$\Delta_I$  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  $\text{dom}(t)$ , then there exists a  $j \in [n]$  such that  $\text{Kill}(x_{ij}t) \in \Delta_I$ .*

# The lower bound

## Theorem

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

## Proof sketch

At most

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

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

## Putting things together

- Show that the two operators are identical

## Putting things together

- Show that the two operators are identical
- Induction over  $|I|$  providing an  $a \in M_I$  with  $a(f) \neq 0$  for any  $f \in \mathbb{K}\Delta_I$

## Putting things together

- Show that the two operators are identical
- Induction over  $|I|$  providing an  $a \in M_I$  with  $a(f) \neq 0$  for any  $f \in \mathbb{K}\Delta_I$
- Remove variables  $x_{ij}$  for minimal  $i \in I$  from  $f$

## Putting things together

- Show that the two operators are identical
- Induction over  $|I|$  providing an  $a \in M_I$  with  $a(f) \neq 0$  for any  $f \in \mathbb{K}\Delta_I$
- 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

- Show that the two operators are identical
- Induction over  $|I|$  providing an  $a \in M_I$  with  $a(f) \neq 0$  for any  $f \in \mathbb{K}\Delta_I$
- 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  $\text{Kill}(x_{ij}t) \in \Delta_I$

## Putting things together

- Show that the two operators are identical
- Induction over  $|I|$  providing an  $a \in M_I$  with  $a(f) \neq 0$  for any  $f \in \mathbb{K}\Delta_I$
- 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  $\text{Kill}(x_{ij}t) \in \Delta_I$
- 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  $R_I(t) = R_{\text{dom}(t)}(t)$

# 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  $R_I(t) = R_{\text{dom}(t)}(t)$
- $V_d$  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  $R_I(t) = R_{\text{dom}(t)}(t)$
- $V_d$  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  $R_I(t) = R_{\text{dom}(t)}(t)$
- $V_d$  is precisely polynomials identically zero on  $M_I$
- $R_d \neq 0$
- There is no refutation of  $\neg \mathcal{PHP}_n^m$  with  $d \leq n/2 + 1$