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

Imogen Hergeth

January 2023

1 Introduction

A major open question in complexity theory is that of $\mathsf{NP} \stackrel{?}{=} \mathsf{coNP}$. A possible avenue to prove $\mathsf{NP} \neq \mathsf{coNP}$ is showing that no proof system admits a polynomial size refutation of some infinite class of unsatisfiable formulae. So far research towards this goal has only succeeded showing much weaker lower bounds for particular proof systems. In this article, we will discuss one such result as first presented in [**raz**], a linear bound on the pigeonhole principle in polynomial calculus.

The proof system we use is the *polynomial calculus*. Similar to proofs in the sequence calculus or Frege systems, these consist of a directed acyclic graph where the vertices are lines and edges are inferences. The difference to the other two systems is that lines are polynomials and the two rules of inference are addition

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

and multiplication

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

A polynomial calculus proof of g from $f_1, \ldots, f_m$ contains $f_1, \ldots, f_m$ as axioms and ends in g. And a refutation of $f_1, \ldots, f_m$ is a proof of $g = 1$ from $f_1, \ldots, f_m$. It is easy to see that some g can be proven from $f_1, \ldots, f_m$ if and only if it is in the ideal generated by $f_1, \ldots, f_n$. Further, theorem 5.2 in [**buss**] shows that $f_1, \ldots, f_n$ are refutable if and only if there are no 0–1 solutions to $f_0 = \cdots = f_m = 0$. From this the motivation of the polynomial calculus becomes clear: a set of ordinary propositional logic formulae can be converted into a set of polynomials whose common zeros correspond to satisfying assignments of the formula. Thus, a refutation of such a set of polynomials amounts to a proof of unsatisfiablity of the set of formulae.

2 The pigeonhole principle

The pigeonhole principle is a simple idea that is commonly used in mathematical reasoning which also lends itself to reasoning about proof systems. Figuratively speaking it says that if m pigeons occupy n pigeonholes and $m > n$ then at least two pigeons need to share one hole. We will now take the steps necessary to formalize this.

Definition 2.1. Let T_n be the set of *multilinear terms* of variables $x_1, \ldots, x_n$, i.e. $t = x_{i_1} \cdots x_{i_d}$ with $1 \leq i_1 < \cdots < i_d \leq n$. We say that $\deg(t) = d$ is the *degree* of t. The terms of some maximal degree d are $T_{n,d} \coloneqq \{t \in T_n \mid \deg(t) \leq d\}$.

There are two orders of T_n that are of interest to us, $\subseteq$ and $\preceq$. The former is simply the usual subset relation when viewing terms as the sets of variables occurring within them. The latter is the total degree lexicographic ordering, i.e., for some fixed arbitrary order of variables $x_1 < \cdots < x_n$ any terms $t_1, t_2 \in T_n$ with different degrees $\deg(t_1) < \deg(t_2)$ have $t_1 < t_2$ and otherwise $t_1 < t_2$ if t_1 occurs before t_2 using the usual lexicographic ordering.

Definition 2.2. Let $S_n(\mathbb{K})$ be the $\mathbb{K}$-algebra $S_n(\mathbb{K}) = \mathbb{K}[x_1, \ldots, x_n]/\{(x_i^2 - x_i) \mid i \in [n]\}\mathbb{K}[x_1, \ldots, x_n]$, i.e. the ring of multilinear polynomials with n indeterminates over some fixed field $\mathbb{K}$.

Polynomials in $S_n(\mathbb{K})$ have a unique representation as linear combinations of terms in T_n, so $S_n(\mathbb{K}) \cong \mathbb{K}T_n$.

Definition 2.3. The *leading term* LT of a polynomial is the largest (w.r.t. $\prec$) term of its representation as a linear combination over T_n. The *degree* of it is $\deg(f) = \deg(\mathrm{LT}(f))$. The set of polynomials with degree at most d is $S_{n,d}(\mathbb{K})$. Note $S_{n,d}(\mathbb{K}) \cong \mathbb{K}T_{n,d}$.

The *degree* of a polynomial calculus proof is the largest degree of a polynomial occurring within it.

With this, we can now formalize the pigeonhole principle, stating that m pigeons can not be placed in n holes, as a system of polynomial equations:

Definition 2.4 ($\neg\mathcal{PHP}_n^m$)**.** The set of polynomials in $S_{nm}(\mathbb{K})$ over variables x_{ij} with $i \in [m]$ and $j \in [n]$ denoted by $\neg\mathcal{PHP}_n^m$ is:

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

$$Q_{i_1,i_2,j} \coloneqq x_{i_1 j} x_{i_2 j} \qquad \text{for each } i_1 \neq i_2 \in [m], j \in [n] \tag{2}$$

Intuitively, $Q_i = 0$ expresses that pigeon i is in precisely one hole j, and $Q_{i_1,i_2,j} = 0$ says that two different pigeons can not occupy the same hole. We can immediately see that $\neg\mathcal{PHP}_n^m$ is refutable if $m > n$ since the corresponding system of equations is unsatisfiable.

The proof makes heavy use of three families of polynomials, terms, and linear operators, denoted by V, Δ, and R respectively, each indexed appropriately. These are derived from:

Definition 2.5. Define $V_{n,d}(f_1, \dots f_m)$ to be the set of all polynomials in $S_{n,d}(\mathbb{K})$ provable from $f_1, \dots, f_m$ with a proof of degree at most d. We say that a term $t \in T_{n,d}$ is *reducible* if $t = \mathrm{LT}(f)$ for some $f \in V_{n,d}(f_1, \dots f_m)$. Further define $\Delta_{n,d}(f_1, \dots f_m) \subseteq T_{n,d}$ to be the set of irreducible terms. And finally, let $R_{n,d,f_1,\dots f_m}$ be the linear operator taking any $f \in S_{n,d}(\mathbb{K})$ to some $f' \in \Delta_{n,d}(f_1, \dots f_m)$ such that $f - f' \in V_{n,d}(f_1, \dots f_m)$.

This reduction process $R_{n,d,f_1,\dots f_m}$ is the same as the one in the construction of Gröbner bases, though that algorithm is not relevant to us. What is important is that $\Delta_{n,d}(f_1, \dots f_m)$ are linearly independent modulo $V_{n,d}(f_1, \dots f_m)$ and that $S_{n,d}(\mathbb{K})$ can be written as the direct sum $\mathbb{K}\Delta_{n,d}(f_1, \dots f_m) \oplus V_{n,d}(f_1, \dots f_m)$ with $R_{n,d,f_1,\dots f_m}$ being the projection of $S_{n,d}(\mathbb{K})$ onto $\mathbb{K}\Delta_{n,d}(f_1, \dots f_m)$.

Of particular importance to us are the versions of these objects applied to the pigeonhole principle: $\Delta_d \coloneqq \Delta_{mn,d}(\neg\mathcal{PHP}^m_n)$, $V_d \coloneqq V_{mn,d}(\neg\mathcal{PHP}^m_n)$, and $R_d \coloneqq R_{mn,d,\neg\mathcal{PHP}^m_n}$.

We will mainly concern ourselves with variables that correspond to a subset of pigeons $I \subseteq [m]$, denoted by $X_I \coloneqq \{x_{ij} \mid i \in I, j \in [n]\}$. Let T_I be the terms over variables in X_I and extend these linearly to $S_I(\mathbb{K})$. Similarly define $T_{I,d}$ and $S_{I,d}(\mathbb{K})$ to be such terms and polynomials of degree at most d. Also, let $\mathrm{dom}(f) \coloneqq \{i \in [m] \mid x_{ij} \in f \text{ for some } j \in [n]\}$ be the set of pigeons that occur in f. Finally, let M_I be the set of all assignments to variables in X_I that correspond to injective total functions $I \to [n]$, i.e. assignments that for each $i \in I$ set precisely one x_{ij} to 1 (and all others to 0) and for each $j \in [n]$ set only one x_{ij} to 1.

3 A lower bound for polynomial calculus refutations of $\neg\mathcal{PHP}^m_n$

We now have the language needed to discuss the main result:

Theorem 3.1. For any $m > n$, every polynomial calculus refutation of $\neg\mathcal{PHP}^m_n$ must have degree at least $n/2 + 1$.

By definition, such a refutation of degree d exists if and only if $1 \in V_d$, which then implies $V_d = S_{n,d}(\mathbb{K})$ and thus $R_d = 0$. The goal of the proof is to disprove this by showing $R_d \neq 0$. The strategy we use is to first define R^{sem}_d, which we claim is identical to R_d and clearly has $R^{\mathrm{sem}}_d \neq 0$. To then we verify that R^{sem}_d is in fact the same operator as R_d we need to further change our perspective by splitting it into operators R^{sem}_I, which each act similar to R^{sem}_d but only on polynomials using variables in X_I.
The biggest challenge is to then show that each R^{sem}_I behaves as needed, in

particular that they all agree with each other at the intersections of their domains. We achieve this by again providing a different definition which clearly has the needed property and then showing that the two operators equal each other.

3.1 Valid pigeon arrangements

The idea behind the definition of R_d^{sem} comes from the indented semantics of the polynomials we use, i.e., from the variables encoding which hole each pigeon occupies. So the goal is for it to capture injectivity of the functions $\text{dom}(f) \to [m]$ induced by f.
Formally, let $I \subseteq [m]$ with $|I| \leq n$ be some subset of pigeons that can be properly placed into holes $[m]$. Then M_I as defined above is the set of all such possible arrangements. We define V_I to be the ideal in $S_I(\mathbb{K})$ that is identically zero on all assignments in M_I. We can now define $\Delta_I^{\text{sem}} \coloneqq \Delta_{|I|\cdot n,|I|\cdot n}(V_I)$ and $R_I^{\text{sem}} \coloneqq R_{|I|\cdot n,|I|\cdot n,V_I}$. That is, Δ_I^{sem} is all terms in T_I that do not occur as a leading term of any polynomial that is identically zero on assignments in M_I. And R_I^{sem} is the projection of $S_I(\mathbb{K})$ onto these, which is exactly the common Gröbner reduction process.
In order to obtain such a semantic description of R_d, we now join all Δ_I^{sem} and R_I^{sem} together. So $\Delta_d^{\text{sem}} \coloneqq \cup_{|I|\leq d}\Delta_I^{\text{sem}}$ and define $R_d^{\text{sem}}(t) \coloneqq R_{\text{dom}(t)}^{\text{sem}}(t)$ for $t \in T_d$ and extend it to $S_d(\mathbb{K})$ by linearity.

Our goal now is to show that this R_d^{sem} is equal to R_d and that its image is nonzero. The latter is easily done:

Lemma 3.2. $R_d^{\text{sem}} \neq 0$.

Proof. Let $I \subseteq [m]$ with $|I| \leq n$ and $f \in V_I$. Then $f + 1$ is identically 1 on M_I, so $f + 1 \notin V_I$. By construction $S_I(\mathbb{K}) = \mathbb{K}\Delta_I^{\text{sem}} \oplus V_I$ and R_I^{sem} is the projection onto the first component, so $R_d^{\text{sem}}(f + 1) = R_I^{\text{sem}}(f + 1) \neq 0$. □

In order to prove $R_d^{\text{sem}} = R_d$, we provide a characterization of $R_{n,d,f_1,\ldots,f_m}$ as a linear operator on $S_{n,d}(\mathbb{K})$:

Theorem 3.3. Let $f_1, \ldots, f_m \in S_{n,d}(\mathbb{K})$ and $R : S_{n,d}(\mathbb{K}) \to S_{n,d}(\mathbb{K})$ be a linear operator.

1. If

$$\begin{aligned} R(f_i) &= 0 && \text{for all } i \in [m], && (3)\\ \deg(R(f)) &\leq \deg(f) && \text{for all } f \in S_{n,d}(\mathbb{K}), && (4)\\ R(f \cdot x_i) &= R(R(f) \cdot x_i) && \text{for all } f \in S_{n,d-1}(\mathbb{K}), i \in [n] && (5) \end{aligned}$$

   then

$$V_{n,d}(f_1, \ldots, f_m) \subseteq \text{Ker}(R).$$

2. If additionally

$$f - R(f) \in V_{n,d}(f_1, \ldots, f_m) \text{ for all } f \in S_{n,d}(\mathbb{K}) \quad (6)$$

then

$$V_{n,d}(f_1, \ldots, f_m) = \mathrm{Ker}(R). \tag{7}$$

3. If (7) holds, $\mathrm{Im}(R) = \mathbb{K}\Delta$ for some $\Delta \subseteq T_{n,d}$, R is a projection onto Δ, i.e.,

$$R(f) = f \text{ for all } f \in \mathbb{K}\Delta, \tag{8}$$

and it also satisfies

$$\mathrm{LT}(R(f)) \preceq \mathrm{LT}(f) \text{ for all } f \in S_{n,d}(\mathbb{K}), \tag{9}$$

then $\Delta = \Delta_{n,d}(f_1, \ldots, f_m)$ and $R = R_{n,d}(f_1, \ldots, f_m)$.

Proof. See [**raz**] lemma 3.2. □

Of this characterization part 3 is the most important. We can use it here to show $R_d^{\mathrm{sem}} = R_d$ and we will use it again later to show $R_I^{\mathrm{sem}} = R_I^{\mathrm{syn}}$. But in order to use it we first need to show (7), which is easiest to do by proving (3) through (6).

Properties (4), (6), (8), and (9) follow directly from the construction of R_d^{sem} (a more complete explanation can be found in [**raz**]). Property (3) holds since all $Q \in \neg\mathcal{PHP}_n^m$ are identically zero on $M_{\mathrm{dom}(Q)}$ and thus are in $V_{\mathrm{dom}(Q)}$, so $R_d^{\mathrm{sem}}(Q) = R_{\mathrm{dom}(Q)}^{\mathrm{sem}}(Q) = 0$. We show (5) for terms $t \in T_d$, the proof extends to all $f \in S_d(\mathbb{K})$ by linearity. First rearrange:

$$\begin{aligned}
& R_d^{\mathrm{sem}}(t \cdot x_{ij}) = R_d^{\mathrm{sem}}(R_d^{\mathrm{sem}}(t) \cdot x_{ij}) \\
\Leftrightarrow\ & R_d^{\mathrm{sem}}(t \cdot x_{ij}) - R_d^{\mathrm{sem}}(R_d^{\mathrm{sem}}(t) \cdot x_{ij}) = 0 \\
\Leftrightarrow\ & R_d^{\mathrm{sem}}((t \cdot x_{ij}) - (R_d^{\mathrm{sem}}(t) \cdot x_{ij})) = 0 \\
\Leftrightarrow\ & R_d^{\mathrm{sem}}((t - R_d^{\mathrm{sem}}(t)) \cdot x_{ij}) = 0.
\end{aligned}$$

Observe that if $i \in \mathrm{dom}(t)$, (5) holds since $t - R_d^{\mathrm{sem}}(t) = t - R_{\mathrm{dom}(t)}^{\mathrm{sem}}(t) = f$ is some polynomial that is identically zero on M_I by definition, so the same must be true for $f \cdot x_{ij}$ and thus $f \cdot x_{ij} \in V_d$ and $R_d^{\mathrm{sem}}(f \cdot x_{ij}) = 0$.
The difficulty in proving (5) comes from showing that this still holds even if $i \notin \mathrm{dom}(t)$. Specifically what we need is that all R_I^{sem} behave identically on their intersection, i.e., that for any $t \in T_d, I \subseteq [m]$ with $\mathrm{dom}(t) \subseteq I$

$$R_I^{\mathrm{sem}}(t) = R_{\mathrm{dom}(t)}^{\mathrm{sem}}(t). \tag{10}$$

Then we can simply set $I = \mathrm{dom}(t) \cup \{x_{ij}\}$ in order to write

$$R_d^{\mathrm{sem}}((t - R_d^{\mathrm{sem}}(t)) \cdot x_{ij}) = R_I^{\mathrm{sem}}((t - R_{\mathrm{dom}(t)}^{\mathrm{sem}}(t)) \cdot x_{ij}) = R_I^{\mathrm{sem}}((t - R_I^{\mathrm{sem}}(t)) \cdot x_{ij})$$

and conclude similarly as above that this is 0.

3.2 The pigeon dance

What we have seen so far is that if (10) holds, then $R_d^{\text{sem}} = R_d$ and since $R_d^{\text{sem}} \neq 0$ there ca not be a polynomial calculus refutation of $\neg\mathcal{PHP}_n^m$ with degree at most d. The strategy for proving that (10) holds if $d \leq n/2 + 1$ is to describe R_I^{sem} through what is called the pigeon dance.

Given some partial assignment of pigeons to holes, the *pigeon dance* is a process where, starting with the leftmost pigeon, each one flies to a free hole to its right. We say the dance is *aborted* if any pigeon has no free hole to its right when it starts its flight, and *completed* otherwise.
Formally, we define $\tilde{T}_I$ to be those elements of T_I that correspond to partial injections $I \to [n]$, i.e. terms of the form $x_{i_1 j_1} \cdots x_{i_d j_d}$ where all i and all j are pairwise different. Then Δ_I^{syn} is defined to be the set of all such $\tilde{T}_I$ that let the pigeons complete their dance. We can already see that $t \in \Delta_I^{\text{syn}}$ does not depend on I since the pigeons not occurring in t play no role in the dance. Finally we define $R_I^{\text{syn}}(t)$ to be some polynomial $f \in \mathbb{K}\Delta_I^{\text{syn}}$ such that $\mathrm{LT}(f) \preceq t$ and $t - f \in V_I$.

Theorem 3.4. $R_I^{\text{syn}}(t)$ is well defined. That is, for every $t \in T_I$ there exists a $f \in \mathbb{K}\Delta_I^{\text{syn}}$ such that $\mathrm{LT}(f) \preceq t$ and $t - f \in V_I$.

Proof. If $t \notin \tilde{T}_I$ then let $f \coloneqq 0$. Trivially, $0 \preceq t$, and $t \in V_I$ since t contains some x_{ij_1} and x_{xij_2}, one of which always is zero on all assignments in M_I, thus t also is.
If $t \in \Delta_I^{\text{syn}}$, then let $f \coloneqq t$. Clearly, $t \preceq t$ and $t - f = 0 \in V_I$.
If $t \in \tilde{T} \setminus \Delta_I^{\text{syn}}$, write $t = x_{i_1 j_1} \cdots x_{i_d j_d}$ with $i_1 < \cdots < i_d$. Since $Q_{i_1} \in V_I$ we can use $Q_{i_1} = 0$ to derive equations modulo V_I:

$$\begin{aligned} t &= (x_{i_1 j_1} - 0) x_{i_2 j_2} \cdots x_{i_d j_d} \\ &= \left(x_{i_1 j_1} - \sum_{j \in [n]} x_{i_1 j} \right) x_{i_2 j_2} \cdots x_{i_d j_d} \mod V_I \\ &= x_{i_2 j_2} \cdots x_{i_d j_d} - \sum_{j' < j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} \\ &\quad - \sum_{j' > j_1} x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d} \mod V_I. \end{aligned}$$

Any terms $x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d}$ with $j' \in \{j_2, \ldots, j_d\}$ are equal to 0 and thus can be removed from the polynomial. The terms in either of the first two summands are strictly smaller than t (w.r.t. $\prec$) and thus can remain in the constructed polynomial. The remaining terms are larger than t, but we can iteratively apply the same construction to them, which again yields some 0 terms, some smaller terms, and potentially some larger terms.
To see that this will eventually remove all larger terms, notice that this construction is simulating the pigeon dance. At each step, the leftmost pigeon that has not moved yet moves to a different hole. The 0 terms are potential moves

that would lead to it flying to an already occupied hole. The ignored terms are ones where it would fly to the left. The larger terms are all the legal moves, where it flies to a previously unoccupied hole to its right. Since $t \notin \Delta_I^{\mathrm{syn}}$ the pigeon dance gets aborted for any strategy of the pigeons, i.e., when continually expanding terms all will be cancelled out eventually.
This lets us construct a polynomial $f' \in S_I(\mathbb{K})$ with $f' = t \mod V_I$ and $f' \prec t$. In order to obtain $f \in \mathbb{K}\Delta_I^{\mathrm{syn}}$, we recursively apply this process to all terms in f' not in Δ_I^{syn}. This eventually terminates since the newly constructed terms are always strictly smaller. And because $t = f \mod V_I$, we have $t - f \in V_I$. □

We can now extend R_I^{syn} to $S_I(\mathbb{K})$ by linearity to obtain the final characterization of the reduction process.

The goal of this construction was to prove (10), since we already know $R_I^{\mathrm{syn}} = R_{\mathrm{dom}(t)}^{\mathrm{syn}}$ we only need to verify $R_I^{\mathrm{sem}} = R_I^{\mathrm{syn}}$. Because of

$$R_I^{\mathrm{sem}} = R_{|I|\cdot n, |I|\cdot n, \{Q \in \neg\mathcal{PHP}_n^m \mid \mathrm{dom}(Q) \subseteq I\}},$$

we can use part 3 of Theorem 3.3 for this with $d = |I| \cdot n$ and

$$f_i \in \{Q \in \neg\mathcal{PHP}_n^m \mid \mathrm{dom}(Q) \subseteq I\}.$$

By construction, R_I^{syn} is a projection onto Δ_I^{syn}, we have $\mathrm{Im}(R_I^{\mathrm{syn}}) = \Delta_I^{\mathrm{syn}}$, $\mathrm{LT}(R_I^{\mathrm{syn}}(f)) \preceq \mathrm{LT}(f)$, and $\mathrm{Ker}(R_I^{\mathrm{syn}}) \subseteq V_I$. So the only property left to check is $\mathrm{Ker}(R_I^{\mathrm{syn}}) \supseteq V_I$. Since $S_I(\mathbb{K}) = \mathbb{K}\Delta_I^{\mathrm{syn}} \oplus \mathrm{Ker}(R_I^{\mathrm{syn}})$ we can rephrase this as $\mathbb{K}\Delta_I^{\mathrm{syn}} \cap V_I = \emptyset$, and further as Δ_I^{syn} being linearly independent when viewed as functions $M_I \to \mathbb{K}$.

To do this we need to define a new operator $\mathrm{Kill} : T_I \to \tilde{T}_I$ that represents removing the leftmost pigeon from its hole and moving the hole to the leftmost position. Formally, if $t \in \tilde{T}_I$ then $t = x_{i_1 j_1} \cdots x_{i_d j_d}$ with $i_1 < \cdots < i_d$ and $\mathrm{Kill}(t) = x_{i_2 j_2'} \cdots x_{i_d j_d'}$ with

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

Otherwise we set $\mathrm{Kill}(t) = 0$.

Theorem 3.5. For $t = x_{i_1 j_1} \cdots x_{i_d j_d} \in \tilde{T}_I$, $t \in \Delta_I^{\mathrm{syn}}$ if and only if there is a $j' > j_1$ such that $\mathrm{Kill}(x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d}) \in \Delta_I^{\mathrm{syn}}$.

Proof. By definition t is in Δ_I^{syn} if and only if there is an unoccupied hole j' for pigeon i_1 to fly to such that the rest of the pigeons can complete the dance. After i_1's flight the only effect it has on the dance is blocking hole j'. This results in the same configuration of available holes as removing i_1 and making hole j' inaccessible to the others by moving it all the way to the left, which is precisely what $\mathrm{Kill}(x_{i_1 j'} x_{i_2 j_2} \cdots x_{i_d j_d})$ does. □

Theorem 3.6. Δ_I^{syn} is closed downward w.r.t. $\subseteq$. That is, if $t \in \Delta_I^{\text{syn}}$ and $t' \subseteq t$, then $t' \in \Delta_I^{\text{syn}}$.

Theorem 3.7. Δ_I^{syn} is closed under Kill. That is, if $t \in \Delta_I^{\text{syn}}$ then $\text{Kill}(t) \in \Delta_I^{\text{syn}}$.

Proof. A formal proof for both theorems can be found in [**raz**], claim 3.7. Intuitively, removing pigeons can only make it easier for the others to complete the dance since the missing ones won't be there to block any holes. So if pigeons $\text{dom}(t)$ can successfully complete the dance, so can a subset of them. This still is true even if you remove a pigeon and also the hole it was occupying since any pigeon that wanted to fly to it can instead just fly to the hole the missing one would have flown to. □

Theorem 3.8. If $|I| \leq (n+1)/2$, $t \in \Delta_I^{\text{syn}}$, and the minimal element i of I is not in $\text{dom}(t)$, then there exists a $j \in [n]$ such that $\text{Kill}(x_{ij}t) \in \Delta_I^{\text{syn}}$.

Proof. There are at most

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

pigeons involved in the dance, and each will occupy 2 holes. So the total number of holes is at most $n-1$, meaning that there is at least one hole j not used at all. $\text{Kill}(x_{ij}t)$ results in the same arrangement of holes and pigeons as t modulo the missing hole j. Since j was not used during the successful dance the pigeons can perform the same dance for $\text{Kill}(x_{ij}t)$ and successfully complete it. □

We finally are ready to put all the pieces together and prove the crucial missing link:

Theorem 3.9. For $|I| \leq (n+1)/2$, terms in Δ_I^{syn} are linearly independent as functions on M_I.

Proof. By induction on $|I|$:
Base case: If $|I| = 0$ then $\Delta_I^{\text{syn}} = \emptyset$ and the claim vacuously holds.
Inductive step: Let i_1 be the smallest element of I and assume the claim has already been proved for $I \setminus \{i_1\}$. Given some non-trivial linear combination of terms in Δ_I^{syn} we can write it as:

$$\sum_{t \in \Gamma} t A_t \tag{11}$$

with $\Gamma \subseteq \tilde{T}_{I \setminus \{i_1\}}$ and $A_t \in \mathbb{K}\tilde{T}_{\{i_1\}} \setminus \{0\}$. This works because each term t in the linear combination contains at most one variable in $X_{\{i_1\}}$, so we can factor out common terms $t \in \tilde{T}_{I \setminus \{i_1\}}$ and be left with a factor that is a non-zero affine polynomial with variables in X_I. By construction each $t \in \Gamma$ has $t \subseteq t'$ for some

term t' in the linear combination, so $\Gamma \subseteq \Delta^{\text{syn}}_{I\setminus\{i_1\}}$ by Theorem 3.6. Let t_1 be the largest term in Γ (w.r.t. $\preceq$), and

$$A_{t_1} = \alpha_0 + \sum_{j\in[n]} \alpha_j x_{i_1 j}.$$

Finally, define $\rho_{i_1 j_1}$ to be the restriction that sends $x_{i_1 j_1}$ to 1 and all other x_{ij} with $i = i_1$ or $j = j_1$ to 0. Note that the effect of $\rho_{i_1 j_1}$ on $\tilde{T}_{I\setminus\{i_1\}}$ is the effectively the same as that of $t \mapsto \text{Kill}(x_{i_1 j_1} t)$, intuitively they both prevent hole j from being used by the pigeons.

Our goal now is to find a j_1 such that $\rho_{i_1 j_1}(A_t) \neq 0$ and $\text{Kill}(x_{i_1 j_1} t) \in \Delta^{\text{syn}}_I$. We distinguish two cases:
$\alpha_{\mathbf{0}} = \mathbf{0}$:
Since A_t is non-zero there is some summand with $\alpha_j \neq 0$, choose j_1 to be one of them. Because $\alpha_{j_1} x_{i_1 j_1} t_1$ is a term in (11), we have $x_{i_1 j_1} t_1 \in \Delta^{\text{syn}}_I$ and thus $\text{Kill}(x_{i_1 j_1} t_1) \in \Delta^{\text{syn}}_{I\setminus\{i_1\}}$ by Theorem 3.7. Clearly, $\rho_{i_1 j_1}(A_t) = \alpha_{j_1} \neq 0$ since all other summands are 0.
$\alpha_{\mathbf{0}} \neq \mathbf{0}$:
By Theorem 3.8 there are j's satisfying $\text{Kill}(x_{i_1 j_1} t) \in \Delta^{\text{syn}}_I$, let j_1 be the largest of them. Then $x_{i_1 j_1} t_1 \notin \Delta^{\text{syn}}_I$ by Theorem 3.5 and thus $x_{i_1 j_1} t_1$ can not be in (11). So $\alpha_{j_1} = 0$ and thus $\rho_{i_1 j_1}(A_t) = \alpha_0 \neq 0$.

If we now apply $\rho_{i_1 j_1}$ to (11) we obtain

$$\begin{aligned}\rho_{i_1 j_1}\left(\sum_{t\in\Gamma} t A_t\right) &= \rho_{i_1 j_1}(t_1 A_{t_1}) + \rho_{i_1 j_1}\left(\sum_{t\in\Gamma\setminus\{t_1\}} t A_t\right)\\ &= \alpha \cdot \rho_{i_1 j_1}(t_1) + f.\end{aligned}$$

By definition $\rho_{i_1 j_1}(t_1) \in \Delta^{\text{syn}}_{I\setminus\{i_1\}}$, so $g = \alpha \cdot \rho_{i_1 j_1}(t_1) + R^{\text{syn}}_{I\setminus\{i_1\}}(f)$ is a linear combination from $\Delta^{\text{syn}}_{I\setminus\{i_1\}}$. It is non-trivial because $\text{LT}(R^{\text{syn}}_{I\setminus\{i_1\}}(f)) \prec t_1$, by construction and Theorem 3.4. By the inductive assumption there exists some assignment $a \in M_{I\setminus\{i_1\}}$ evaluating g to some $k \in \mathbb{K}$. We extend this to a' by setting $a(x_{i_1 j_1}) \coloneqq 1$ and $a(x_{ij}) \coloneqq 0$ for all other x_{ij} with $i = i_1$ or $j = j_1$.
We have $a(f) = a(R^{\text{syn}}_{I\setminus\{i_1\}}(f))$ since $f = R^{\text{syn}}_{I\setminus\{i_1\}}(f) \mod V_I$ by Theorem 3.4 and all $h \in V_I$ have $a(h) = 0$ by definition. So $a'(g) = k$ and thus a' also evaluates (11) to $k \neq 0$. □

With $|I| = d \leq (n+1)/2$ this tells us that $\text{Ker}(R^{\text{syn}}_I) = V_I$ and thus $R^{\text{syn}}_I = R^{\text{sem}}_I$ holds. So we observe that $R^{\text{syn}}_I(t)$ is independent of I (as long as $\text{dom}(t) \subseteq I$) since pigeons not participating in the dance do not affect its success. This in turn implies that R^{sem}_d satisfies all properties (3) through (9) and thus $R^{\text{sem}}_d = R_{nm,d,\neg\mathcal{PHP}^m_n}$. Since $R^{\text{sem}}_d \neq 0$, the same is true for $R_{nm,d,\neg\mathcal{PHP}^m_n}$, which means that $V_{nm,d,\neg\mathcal{PHP}^m_n} \neq S_{nm,d}(\mathbb{K})$. This implies $1 \notin V_{nm,d}(\mathbb{K})$ and thus Theorem 3.1.