On the strength of Sherali-Adams and Nullstellensatz as propositional proof systems

Ilario Bonacina
bonacina@cs.upc.ecu
UPC Universitat Politècnica de Catalunya
Barcelona, Spain

Maria Luisa Bonet
bonet@cs.upc.edu
UPC Universitat Politècnica de Catalunya
Barcelona, Spain

ABSTRACT

We characterize the strength of the algebraic proof systems Sherali-Adams (SA) and Nullstellensatz (NS) in terms of Frege-style proof systems. Unlike bounded-depth Frege, SA has polynomial-size proofs of the pigeonhole principle (PHP). A natural question is whether adding PHP to bounded-depth Frege is enough to simulate SA.

We show that SA, with unary integer coefficients, lies strictly between tree-like depth-1 Frege + PHP and tree-like Resolution. We introduce a weighted version of PHP (wPHP) and we show that SA with integer coefficients lies strictly between tree-like depth-1 Frege + wPHP and Resolution.

Analogous results are shown for NS using the bijective (i.e. onto and functional) pigeonhole principle and a weighted version of it.

CCS CONCEPTS

• **Theory of computation → Proof complexity**.

KEYWORDS

bounded-depth Frege, Nullstellensatz, Pigeonhole Principle, Sherali-Adams

ACM Reference Format:

Ilario Bonacina and Maria Luisa Bonet. 2022. On the strength of Sherali-Adams and Nullstellensatz as propositional proof systems. In *37th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) (LICS '22), August 2–5, 2022, Haifa, Israel.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3531130.3533344

1 INTRODUCTION

This paper connects logic based proof systems with algebraic ones. While logic based proof systems work directly with propositional formulas, the algebraic ones work with polynomials, including polynomial translations of Boolean formulas.

For instance, in the *Nullstellensatz proof system* (NS) [5], a CNF formula is shown unsatisfiable by first translating it into a set of polynomial equations, and a proof of the unsatisfiability is a sum of multiples of those equations that, after simplifications, reduces to the trivial contradiction $1 = 0$ (Definition 2.5). NS with coefficients over $\mathbb{Z}_2$ was first studied in connection with a major (and yet open) problem in proof complexity: the problem of proving superpolynomial size lower bounds for bounded-depth Frege systems with parity gates ([4, 6, 11] among others). Moreover, lower bounds in NS can be lifted to lower bounds for stronger proof systems [26–28].

Sherali-Adams (SA) [29] is similar to NS but instead of equations we first produce polynomial inequalities and a proof of unsatisfiability is a sum of positive multiples of the inequalities together with sums of positive monomials. In this case the trivial contradiction is $-1 \geq 0$ (Definition 2.6). The interest in studying SA relies primarily on its connections to approximation algorithms for important **NP**-hard optimization problems, see for instance the survey [16].

Frege is the standard textbook logic proof system. Restricting the depth of the formulas in Frege, we obtain proof systems like *Resolution* or *bounded-depth Frege*. SA is known to simulate Resolution, and it is stronger, since SA can prove the pigeonhole principle efficiently, unlike Resolution or even bounded-depth Frege [21, 25]. Hence, natural questions are the following.

"*Which axioms do we need to add to constant-depth Frege to simulate* SA *or* NS*?*"

"*What is the minimal depth of constant-depth Frege (plus the extra axiom) needed to simulate* SA *or* NS*?*"

The axioms we want to add should be "natural", in the sense that they should have some clear combinatorial meaning. For instance, constant-depth Frege with *counting MOD_2* axioms simulates NS with coefficients over $\mathbb{Z}_2$ [19].

The *pigeonhole principle* (PHP, Definition 4.1) is a natural combinatorial principle, which informally says that $n + 1$ pigeons cannot all fly to n holes without any two of them sharing a hole. The *bijective* pigeonhole principle, i.e. onto and functional, is denoted by ofPHP (Definition 4.1). In this work we use propositional encodings of these principles.

We use principles generalizing PHP and ofPHP. The *weighted pigeonhole principles* wPHP and $w$ofPHP (Definition 5.1) informally capture similar combinatorial principles, where the pigeons have some "mass" and the holes have some "capacity". The mass of the ith pigeon is the same as the capacity of the ith hole, but there is an extra pigeon with positive mass. Each pigeon can fly once with the whole mass or twice with half mass. Each hole can accept either one pigeon filling the full capacity or two pigeons filling half capacity each. SA efficiently proves wPHP but the proof seems to require coefficients encoded in binary (Theorem 5.2).

In this article we answer the questions above for NS and SA with coefficients in $\mathbb{Z}$. A bit unexpectedly, their strength seems to depend on whether the coefficients of the polynomials are encoded in unary

LICS '22, August 2–5, 2022, Haifa, Israel

ACM ISBN 978-1-4503-9351-5/22/08…$15.00
https://doi.org/10.1145/3531130.3533344

or binary. Unary NS and unary SA refer to having coefficients encoded in unary.

Before we answer the questions, let us mention that, informally, *bounded-depth Frege + principle* means that the principle is given as an extra tautology. Also, a *tree-like* proof system means that each Boolean formula can only be used once.

We visually summarize our results, although the formal statements of the cited theorems are slightly stronger than what is shown in the figures, since they also take into account the degree of the polynomials.

As you can see in Fig. 1, tree-like depth-1 Frege + wPHP is strictly stronger than SA and SA is strictly stronger than Resolution. On the other hand, tree-like depth-1 Frege + PHP is strictly stronger than unary SA and unary SA is strictly stronger than tree-like Resolution.

Prior to our work, it was not clear at all if SA was able to prove efficiently any combinatorial principle significantly different from PHP (in addition to what Resolution can prove). This work shows this is not the case. At best, SA can prove just principles easily reducible to wPHP (in addition to what Resolution can prove).

Fig. 1 also states some equivalences between SA and unary SA and other proof systems based on Boolean formulas, in particular weighted Resolution ([10, 23, 24], Definition 3.1) and circular Resolution [2].

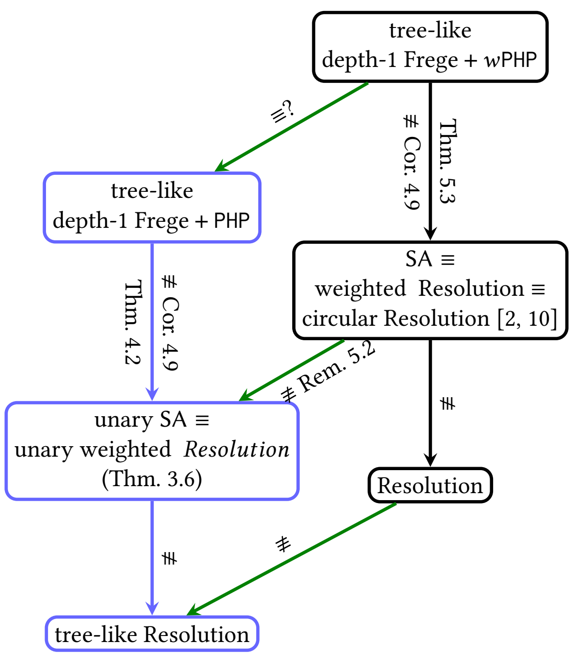

Figure 1: The p-simulations for SA. The notation $P \rightarrow Q$ means that the proof system P p-simulates the proof system Q. The p-simulations are annotated with "≢" if the p-simulation is known to be strict, or with "≡?" whenever it is an open question if the p-simulation is strict or not. An arrow → means the p-simulation is trivial. The color • is used to visually differentiate the results for the proof systems with unary weights/coefficients.

Informally, *weighted Resolution* is a proof system where clauses have weights that can be positive or negative. The positive weight of a clause is the number of times we are allowed to use it as a premise of some inference, while the negative weight is the number of times we used it as an assumption and hence are required to justify it by deriving it. Clauses with positive weights might appear out of nothing as long as the same clauses appears also with negative weights. A proof starts with the initial clauses with some chosen positive weights and produces, using a small modification of the rules of Resolution, an empty clause with positive weight and all the clauses with negative weights have been justified.

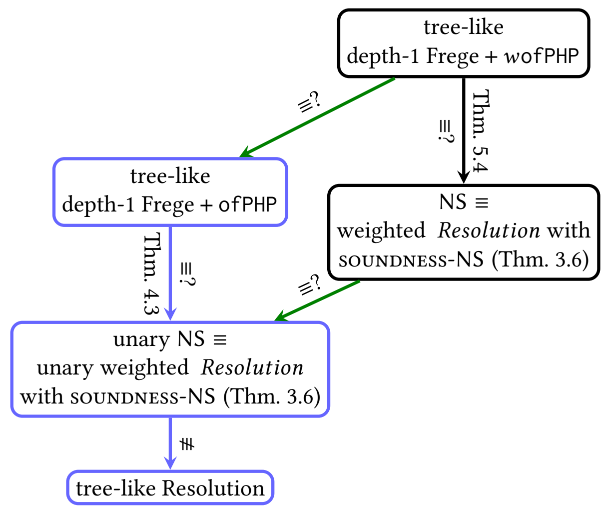

Figure 2: The p-simulations for NS.

As you can see in Fig. 2, tree-like depth-1 Frege + $w$ofPHP is stronger than NS. On the other hand, tree-like depth-1 Frege + ofPHP is stronger than unary NS and unary NS is strictly stronger than tree-like Resolution. We also show that NS and unary NS are p-equivalent to other proof systems based on Boolean formulas (Theorem 3.6).

The notion of weighted Resolution can be extended naturally to formulas of higher depth producing the system *weighted depth-d Frege* (see Definition 3.1). As weighted Resolution corresponds to SA, weighted depth-d Frege corresponds to a generalization of SA handling algebraic expressions of higher depth.[1] Fig. 3 shows the results we have for weighted depth-d Frege. Basically the same results as in Fig. 1 but lifted from formulas of depth 0, i.e. clauses, to formulas of depth d. Tree-like depth-$(d+1)$ Frege + wPHP is strictly stronger than weighted depth-d Frege and weighted depth-d Frege is strictly stronger than depth-d Frege. On the other hand, tree-like depth-$(d+1)$ Frege + PHP is strictly stronger than unary weighted depth-d Frege, and unary weighted depth-d Frege is strictly stronger than tree-like depth-d Frege.

The PHP is the most studied principle in proof complexity and, for instance, we know that depth-d Frege + PHP is strictly weaker than Frege, at least for $d = o\left(\frac{\log\log n}{\log\log\log n}\right)$ [6], hence unary weighted depth-d Frege is also *strictly* weaker than Frege for the same d (Corollary 4.7). To the best of our knowledge, the weighted pigeonhole principle wPHP is a completely new generalization of PHP. This

[1] We leave the formal definition of SA on algebraic expressions of higher depth, and the connections with circular depth-d Frege and weighted depth-d Frege, to a full version of this work.

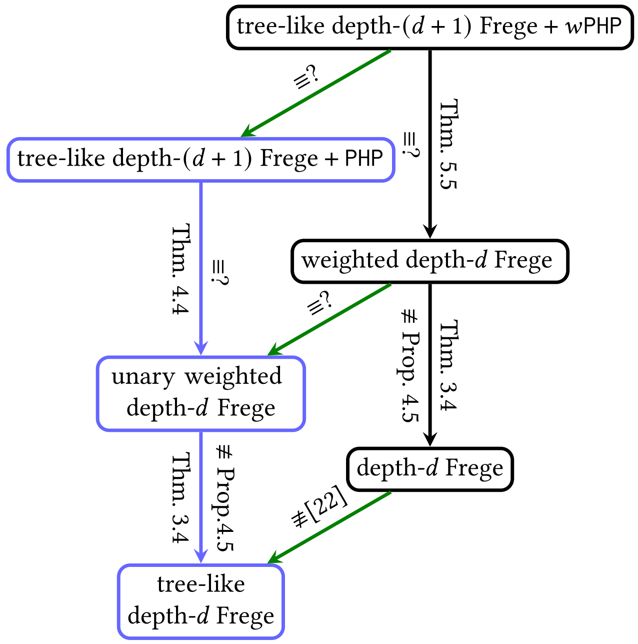

Figure 3: The p-simulations for weighted depth-d Frege.

naturally leaves several open questions about it. Including the obvious one of proving that depth-d Frege + wPHP is strictly weaker than Frege (see Section 6 for a list of open problems).

1.1 Connections with previous work

This article originated in the context of proof systems for MaxSAT extending MaxSAT Resolution, such as, for instance, DRMaxSAT [8]. Such systems, when seen as usual propositional proof systems, are stronger than Resolution, since they able to prove some versions of PHP. We were interested to see if they could also prove some different natural combinatorial principles. These proof systems are simulated by weighted Resolution (previously called *MaxSAT Resolution with Extension* in [23, 24]).

Since SA and weighted Resolution are equivalent, the question about MaxSAT proof systems morphed into asking whether SA was actually able to prove something significantly different from PHP (in addition to what Resolution can prove).

In this article, we give a first answer to the questions of the strength of SA and NS. SA can, at best, prove principles easily reducible to wPHP (in addition to what Resolution can prove). Similarly, NS can, at best, prove principles easily reducible to $w$ofPHP, in addition to what Resolution can prove (with a small increase in depth).

The starting point of our work is [8], where the authors prove that DRMaxSAT is simulated by bounded-depth Frege + PHP. The simulations upper-bounding the strength of SA, NS and weighted depth-d Frege in this article widely generalize the simulation in [8].

This was possible via the language of weighted Resolution and weighted depth-d Frege, a new way of looking at SA and NS (and other semi-algebraic proof systems).

1.2 Organization of the paper

Section 2 contains all the basic definitions: the notion of depth-d Frege, depth-d Frege + ϕ, and the semi-algebraic proof systems NS and SA.

Section 3 introduces the proof system weighted depth-d Frege with two soundness conditions, proves some basic facts about them, and the connection to semi-algebraic proof systems.

Section 4 contains the definition of the pigeonhole principle PHP and the simulation of unary SA (resp. unary NS) by depth-1 Frege + PHP (resp. depth-1 Frege + ofPHP).

Section 5, builds on the previous section and introduces a *weighted* version of the pigeonhole principle wPHP. We show how to refute it in SA and how to simulate SA by depth-1 Frege + wPHP.

Section 6 briefly recaps some aspects of this article and suggests some open problems.

2 PRELIMINARIES

For $n \in \mathbb{N}$, let $[n] = \{1, \ldots, n\}$. A *propositional proof system* is a polynomial time function $P\colon \{0,1\}^* \to \{0,1\}^*$ whose range is exactly the set TAUT of propositional tautologies in the DeMorgan language [12]. The notion we use to compare the strength of two propositional proof systems is the notion of *p-simulation*. Given two propositional proof systems P, Q we say that P *p-simulates* Q if there exist a polynomial time function $f\colon \{0,1\}^* \to \{0,1\}^*$ such that for all strings x, $Q(x) = P(f(x))$. If P p-simulates Q and Q p-simulates P we say that P and Q are *p-equivalent*. If P p-simulates Q and they are not p-equivalent we say that the p-simulation is *strict*.

2.1 Constant depth Frege systems

We follow the notation and definitions of [7] with minor changes. Propositional formulas are constructed from *literals*, i.e. Boolean variables x_i or negated variables $\neg x_i$, and unbounded fan-in conjunctions $\bigwedge$ and disjunctions $\bigvee$.

All formulas are either literals, $\bigvee$*-formulas* or $\bigwedge$*-formulas*. They are defined inductively:

- If Φ is a finite set of literals and $\bigvee$-formulas, then $\bigwedge \Phi$ is a $\bigwedge$-formula.
- If Φ is a finite set of literals and $\bigwedge$-formulas, then $\bigvee \Phi$ is a $\bigvee$-formula.

The point of this definition is that an $\bigwedge$-formula cannot be the argument of an $\bigwedge$, hence intuitively, adjacent $\bigwedge$ (resp. $\bigvee$) must be collapsed.

Definition 2.1 (depth-d formulas). Let $d \in \mathbb{N}$. The classes of formulas Θ_d over a set of variables X are defined inductively as follows:

(1) $\phi \in \Theta_0$ iff ϕ is a *literal*, i.e. either x or the negation $\neg x$ of some variable $x \in X$.
(2) $\phi \in \Theta_{d+1}$ iff $\phi \in \Theta_d$ or $\phi = \bigwedge \Psi$ or $\phi = \bigvee \Psi$, where Ψ is a finite subset of Θ_d.

We refer to $\phi \in \Theta_d$ as ϕ *being of depth d*.

For $\phi \in \Theta_d$ we denote by $\neg\phi$ the formula in Θ_d obtained from ϕ by interchanging $\bigvee$ and $\bigwedge$ and interchanging variables and their negations.

A Θ_d*-cedent* is a finite multiset of formulas of depth d. A Θ_0-cedent is a *clause*. The intended meaning of a cedent Γ is $\bigvee \Gamma$. A

CNF formula F is a set of clauses. The intended meaning of F is the conjunction of its members. We sometimes abuse notation by writing a cedent $\Gamma \cup \Phi$ simply as Γ, Φ.

Definition 2.2 (depth-d Frege). Let $\mathcal{F}$ be a set Θ_d-cedents. A depth-d Frege *derivation* of a Θ_d-cedent Γ is a tree T in which each node is labelled with a Θ_d-cedent, the root has label Γ, each leaf has label either the empty cedent or a cedent from $\mathcal{F}$, and for each node in the tree the label it gets is a consequence of the labels of its parents via one of the following inference rules

$$\frac{\Gamma, \phi, \phi}{\Gamma, \phi}\ (\text{CONTRACTION}) \qquad \frac{}{\phi, \neg\phi}\ (\text{EXCLUDED MIDDLE})$$

$$\frac{\Gamma, \phi \qquad \text{for } \phi \in \Phi}{\Gamma, \bigwedge \Phi}\ (\bigwedge\text{-INTRODUCTION})$$

$$\frac{\Gamma, \neg\phi \qquad \Gamma, \phi}{\Gamma}\ (\text{SYMMETRIC CUT}) \qquad \frac{\Gamma}{\Gamma,\ \Gamma'}\ (\text{WEAKENING})$$

$$\frac{\Gamma, \Phi}{\Gamma, \bigvee \Phi}\ (\bigvee\text{-INTRODUCTION}) \qquad \frac{\Gamma, \bigvee \Phi}{\Gamma, \Phi}\ (\bigvee\text{-ELIMINATION})$$

where the cedents Γ, Γ', Φ are Θ_d-cedents and $\bigvee \Phi, \bigwedge \Phi, \phi, \neg\phi$ are formulas of depth d. The *size* of T is the number of symbols of distinct cedents in the derivation. If we count the number of symbols in *all* occurrences of cedents we use the adjective *tree-like*. A depth-d Frege *refutation* of $\mathcal{F}$ is a derivation of the empty cedent.

The definition of depth-d Frege in [7] is essentially the one given above with the CONTRACTION rule given implicitly, since their cedents are sets. For us, it is more convenient to consider multisets and to have the rule given explicitly. The propositional proof system *Resolution* is depth-0 Frege. In this system, the $\bigwedge$ and $\bigvee$ rules cannot be applied.

Given $\boldsymbol{\phi} = (\phi_n)_{n\in\mathbb{N}}$ a family of unsatisfiable cedents, for instance ϕ_n being the pigeonhole principle PHP_n^{n+1} (see Section 4 for the definition of PHP_n^{n+1}), the notion of depth-d Frege + $\boldsymbol{\phi}$ has been considered for instance in [1, 6], and it is also very common in the context of bounded arithmetic (see for instance [20]).

Informally, depth-d Frege + $\boldsymbol{\phi}$ is depth-d Frege where we have the extra power to reduce the formula we want to refute to a substitution instance of some ϕ_n, and ϕ_n is given for free in the sense that we already know it is unsatisfiable. In some sense, in the system depth-d Frege + $\boldsymbol{\phi}$ we allow the formulas ϕ_n to be used only once. Formally, the definition is the following.

Definition 2.3 (depth-d Frege + $\boldsymbol{\phi}$). Let $\boldsymbol{\phi} = (\phi_n)_{n\in\mathbb{N}}$, where ϕ_n is a set of s many Θ_d-cedents in n variables. A refutation of a set of Θ_d-cedents F in depth-d Frege + $\boldsymbol{\phi}$ is a set of depth-d Frege derivations $\Gamma_1, \ldots, \Gamma_s$ of $G_1, \ldots, G_s$ such that: either (1) $G_1 = \emptyset$, i.e. Γ_1 is a refutation of F and $s = 1$, or (2) there is a $n \in \mathbb{N}$ such that the set of cedents $\{G_1, \ldots, G_s\}$ is a substitution instance of ϕ_n.[2] The *height* of the refutation is the maximum height of $\Gamma_1, \ldots, \Gamma_s$. The *size* of the refutation is the sum of the sizes of $\Gamma_1, \ldots, \Gamma_s$.

Even though we know that tree-like depth-$(d+1)$ Frege is equivalent to depth-d Frege [20], tree-like depth-$(d+1)$ Frege + ϕ is not the same as depth-d Frege + ϕ, since in the first system we allow to derive substitution instances of ϕ that are formulas of depth $d+1$.

[2] Let ψ_n be in the variables $x_1, \ldots, x_n$. The cedent $\{G_1, \ldots, G_s\}$ is a substitution instance of ϕ_n if there are depth-d formulas $\psi_1, \ldots, \psi_n$ s.t. once we substitute in ϕ_n all the x_is with the ψ_is we get exactly $\{G_1, \ldots, G_s\}$.

Definition 2.4 (Res(k)). Let $d, k \in \mathbb{N}$. The system $\mathrm{Res}(k)$ is the restriction of depth-1 Frege where the $\bigwedge$-INTRODUCTION rule in Definition 2.2 is limited to Θ_0-cedents (i.e. sets of clauses) Φ of size at most k. Let $\boldsymbol{\phi} = (\phi_n)_{n\in\mathbb{N}}$, where ϕ_n is a set of s many Θ_0-cedents in n variables. $\mathrm{Res}(k) + \boldsymbol{\phi}$ is then defined in an analogous way as depth-d Frege + $\boldsymbol{\phi}$ in Definition 2.3.

2.2 Algebraic and semi-algebraic proof systems

In this section, we define formally the proof systems Nullstellensatz [5] and Sherali-Adams [29]. Let X be the set of variables $x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n$. Given the ordered ring of the integers $\mathbb{Z}$, by $\mathbb{Z}[X]$ we denote the set of polynomials in the variables X and coefficients in $\mathbb{Z}$.

Definition 2.5 (Nullstellensatz, NS). Given polynomials $p_0, \ldots, p_\ell$ in $\mathbb{Z}[X]$, a *Nullstellensatz proof over* $\mathbb{Z}$ ($\mathsf{NS}_\mathbb{Z}$) of the equality $p_0 = 0$ from the equalities $p_1 = 0, \ldots, p_\ell = 0$ is a polynomial identity of the form

$$p_0 = \sum_{i=1}^{\ell} q_i p_i + \sum_{j=1}^{n} r_j (x_j^2 - x_j) + \sum_{j=1}^{n} r'_j (x_j + \bar{x}_j - 1)\,, \tag{1}$$

where q_i, r_j, r'_j are polynomials in $\mathbb{Z}[X]$. A *refutation* of the set of equalities $\{p_1 = 0, \ldots, p_\ell = 0\}$ is a derivation of the equality $c = 0$ where $c \in \mathbb{Z} \setminus \{0\}$. The *size* of the polynomial identity in (1) is the length of a bit-string representing the polynomials q_i, r_j, r'_j, including the coefficients. The *degree* of the polynomial identity in (1) is the maximum degree of the polynomials q_i, r_j, r'_j.

Definition 2.6 (Sherali-Adams, SA). Given a set of polynomials $p_0, \ldots, p_\ell \in \mathbb{Z}[X]$, a *Sherali-Adams proof over* $\mathbb{Z}$ ($\mathsf{SA}_\mathbb{Z}$) *of* $p_0 \geq 0$ *from* $p_1 \geq 0, \ldots, p_\ell \geq 0$ is a polynomial identity of the form

$$p_0 = \sum_{i=1}^{\ell} q_i p_i + \sum_{j=1}^{n} r_j (x_j^2 - x_j) + \sum_{j=1}^{n} r'_j (x_j + \bar{x}_j - 1) + q_0\,, \tag{2}$$

where r_j, r'_j are polynomials in $\mathbb{Z}[X]$ and the q_is are polynomials with positive coefficients. A *refutation* of a set of polynomial inequalities $p_1 \geq 0, \ldots, p_\ell \geq 0$ is a derivation of $c \geq 0$ where $c \in \mathbb{Z}$ and negative. The *size* of the polynomial identity in (2) is the length of a bit-string representing the polynomials q_i, r_j, r'_j, including the coefficients. The *degree* of the polynomial identity in (2) is the maximum degree of the polynomials q_i, r_j, r'_j.

In the Definitions 2.5 and 2.6, if we don't allow the variables $\bar{x}_1, \ldots, \bar{x}_n$, and hence the polynomials r'_j are identically 0, the resulting systems are known to be exponentially weaker [14], with respect to size. The degree of the two versions of the systems is obviously the same.

In this paper, we consider only Nullstellenstatz and Sherali-Adams over the ring $\mathbb{Z}$, resp. $\mathsf{NS}_\mathbb{Z}$ and $\mathsf{SA}_\mathbb{Z}$, hence from now we refer to them simply as NS and SA omitting the reference to $\mathbb{Z}$. When we restrict all the polynomials appearing in NS and SA derivations to have coefficients ± 1, we refer to those systems as unary NS and unary SA.

Theorem 2.7 (Normal form for NS/SA proofs). *Given a (unary)* NS *derivation* π *of* p_0 *as in eq.* (1)*, there is a (unary)* NS *derivation* *of p_0 of the form*

$$p_0 = \sum_{i=1}^{\ell} cp_i + \sum_{j=1}^{n} r_j(x_j^2 - x_j) + \sum_{j=1}^{n} r_j''(x_j + \bar{x}_j - 1) - \sum_{i=1}^{\ell} q_i' p_i \quad (3)$$

with size only polynomially larger than π, a constant $c > 0$ and all polynomials q_i' with positive coefficients. Similarly, given a (unary) SA *derivation π of p_0 as in eq.* (2)*, if all the p_is have negative coefficients, there is a (unary)* SA *derivation of p_0 of the form*

$$p_0 = \sum_{i=1}^{\ell} cp_i + \sum_{j=1}^{n} r_j(x_j^2 - x_j) + \sum_{j=1}^{n} r_j''(x_j + \bar{x}_j - 1) + q_0 - \sum_{i=1}^{\ell} q_i' p_i \quad (4)$$

with size only polynomially larger than π, a constant $c > 0$ and all polynomials q_i' with positive coefficients.

An analogous result appeared in [15, Theorem 1.5].

Proof. Let ax_jm be a monomial in q_i. If $a < 0$ consider this monomial to be part of q_i' (this case can only happen in NS). If $a > 0$ then we can rewrite amx_jp_i as

$$amx_jp_i = amp_i(x_j + \bar{x}_j - 1) - am\bar{x}_jp_i + amp_i\,,$$

where the polynomial amp_i is going to be part of r_j'' and the polynomial $am\bar{x}_j$ is going to be part of q_i'. We then rewrite amp_i in an analogous way, variable by variable. We repeat this for all the monomials in all the q_is. This way the sum $\sum_{i\in[\ell]} q_ip_i$ is rewritten as $\sum_{i\in[m]} c_ip_i$ for some constants $c_i > 0$ at the cost of adding monomials to the r_j''s and q_i's. Let $c = \max_{i\in[\ell]} c_i$. We can then further rewrite $\sum_{i\in[\ell]} c_ip_i$ as

$$\sum_{i\in[\ell]} c_ip_i = \sum_{i\in[\ell]} cp_i - \sum_{i\in[\ell]} (c - c_i)p_i\,.$$

To conclude, we just consider all monomials in $(c - c_i)p_i$ as part of q_i'. □

Notice that, if all the coefficients in $p_1, \ldots, p_\ell$ are negative, then the Normal Form for SA in the theorem above (i.e. eq. (4)) gets further simplified to

$$p_0 = \sum_{i=1}^{m} cp_i + \sum_{j=1}^{n} r_j(x_j^2 - x_j) + \sum_{j=1}^{n} r_j''(x_j + \bar{x}_j - 1) + q_0'\,,$$

for some polynomial q_0' with positive coefficients, since all monomials in $-\sum_{i=1}^{\ell} q_i'p_i$ have positive coefficients.

This is exactly what happens for the natural encoding of sets of clauses in the context of (semi-)algebraic proof systems. A clause $C = \{x_i, \neg x_j : i \in I,\ j \in J\}$ is represented as the monomial $-\prod_{i\in I} \bar{x}_i \prod_{j\in J} x_j$, intended to be $= 0$ in NS, and ≥ 0 in SA. In the algebraic context, we follow the common convention that a variable being 0 means it is true. In the propositional context it is the opposite, 0 means false and 1 means true. A set of clauses is then represented by the set of the (in)equalities corresponding to its clauses.

Under this natural representation it is well-known that SA p-simulates Resolution (see for instance [3, Lemma 3.5]) and NS with unary coefficients p-simulates tree-like Resolution. Moreover, both p-simulations are known to be strict.

3 WEIGHTED DEPTH-d FREGE AND (SEMI)-ALGEBRAIC PROOF SYSTEMS

A *weighted Θ_d-cedent over $\mathbb{Z}$* is a pair $[\Gamma; w]$ where Γ is a Θ_d-cedent and $w \in \mathbb{Z}$. Given two weighted cedents $[\Gamma; w]$ and $[\Delta; z]$ we say that $[\Gamma; w]$ is a *weakening* of $[\Delta; z]$ if $\Gamma \supseteq \Delta$.

In this paper we only consider proof systems handling weighted depth-d formulas over $\mathbb{Z}$, although the definitions can be extended easily to weighted polynomials, linear inequalities, etc.

$$\frac{[\Gamma, \phi, \phi; w]}{[\Gamma, \phi; w]}\ (\textsc{contraction}) \qquad \frac{}{[\phi, \neg\phi; w]}\ (\textsc{excluded middle})$$

$$\frac{[\Gamma, \phi_1; w] \quad [\Gamma, \phi_2; w]}{[\Gamma, \phi_1 \wedge \phi_2; w], \quad [\Gamma, \phi_1, \phi_2; w]}\ (\textstyle\bigwedge\textsc{-introduction})$$

$$\frac{[\Gamma, \neg\phi; w],\ [\Gamma, \phi; w]}{[\Gamma; w]}\ (\textsc{symmetric cut}) \qquad \frac{[\Gamma; u],\ [\Gamma; w]}{[\Gamma; u + w]}\ (\textsc{fold})$$

$$\frac{[\Gamma; w]}{[\Gamma, \neg\phi; w],\ [\Gamma, \phi; w]}\ (\textsc{split}) \qquad \frac{[\Gamma; u + w]}{[\Gamma; u],\ [\Gamma; w]}\ (\textsc{unfold})$$

$$\frac{[\Gamma, \Phi; w]}{[\Gamma, \bigvee \Phi; w]}\ (\textstyle\bigvee\textsc{-introduction}) \qquad \frac{}{[\Gamma; u],\ [\Gamma; -u]}\ (\textsc{introduction})$$

$$\frac{[\Gamma, \bigvee \Phi; w]}{[\Gamma, \Phi; w]}\ (\textstyle\bigvee\textsc{-elimination}) \qquad \frac{[\Gamma; u],\ [\Gamma; -u]}{}\ (\textsc{removal})$$

Figure 4: Inference rules of weighted depth-d Frege. The cedents $\Gamma, \Phi, \bigvee \Phi, \bigwedge \Phi, \phi, \neg\phi$ all are Θ_d-cedents, $u, w \in \mathbb{Z}$.

Definition 3.1 (weighted depth-d Frege). A *weighted depth-d Frege* derivation (over $\mathbb{Z}$) of a Θ_d-cedent Γ from a set of Θ_d-cedents $\mathcal{F} = \{\Gamma_1, \ldots, \Gamma_m\}$ is a sequence $\mathcal{L}_1, \ldots, \mathcal{L}_s$ of multisets of weighted Θ_d-cedents over $\mathbb{Z}$ such that:

(1) $\mathcal{L}_1 = \{[\Gamma_1; w], \ldots [\Gamma_m; w]\}$ where $w \in \mathbb{N}$,
(2) $[\Gamma; z] \in \mathcal{L}_s$ for some $z > 0$,
(3) all cedents in $\mathcal{L}_s \setminus \{[\Gamma; z]\}$ have positive weights.
(4) each $\mathcal{L}_i$ is obtained from $\mathcal{L}_{i-1}$ by applying one of the inference rules in Fig. 4 as substitution rules, i.e. removing the premises from $\mathcal{L}_{i-1}$ and adding the conclusions.

A weighted depth-d Frege *refutation* of $\mathcal{F}$ is a weighted depth-d Frege derivation of the empty cedent. The *size* of a weighted depth-d Frege derivation $\mathcal{L}_1, \ldots, \mathcal{L}_s$ is the total number of occurrences of symbols in $\mathcal{L}_1, \ldots, \mathcal{L}_s$ including the weights. Unless explicitly stated, the weights are assumed to be encoded in binary. If the weights are restricted to $-1, 1$ then we call the system unary weighted depth-d Frege. In the system with weights in unary there are no applications of the fold/unfold rules and the weighted cedents in $\mathcal{L}_1$ are given as a multiset, instead of $[\Gamma_i; w]$ we have a multiset consisting in w many copies of $[\Gamma_i; 1]$ if $w > 0$ or a multiset consisting in $-w$ many copies of $[\Gamma_i; -1]$ if $w < 0$.

The system *weighted Resolution* is weighted depth-0 Frege. It comes essentially from [10, 24].

Definition 3.2 (weighted depth-d Frege with soundness*-NS).* A *weighted depth-d Frege with soundness-*NS derivation (over $\mathbb{Z}$) of a Θ_d-cedent Γ from a set of Θ_d-cedents $\mathcal{F} = \{\Gamma_1, \ldots, \Gamma_m\}$ is a sequence $\mathcal{L}_1, \ldots, \mathcal{L}_s$ of multisets of weighted Θ_d-cedents over $\mathbb{Z}$

with the same requirement as in Definition 3.1 with the condition (3) substituted by the condition

(3′) all cedents in $\mathcal{L}_s \setminus \{[\Gamma; z]\}$ have positive weights and, moreover, they are also weakenings of cedents in $\mathcal{F}$ (soundness-NS condition).

The intuition, behind the definition of weighted proof systems, is that we are allowed to make assumptions (via the introduction rule) and the weights are a way to have some control over them. If we need to use an assumption k times, we also need to justify it with weight k. At some point, the assumptions must end-up being justified, via the removal rule. The system then needs to keep track of the weights in a consistent way, and this is done using inference rules as substitution rules.

Notice that the rules in Fig. 4 are weighted versions of the inference rules of depth-d Frege (see Definition 2.2) with two exceptions: the split and the $\bigwedge$-introduction. Those rules are defined in this way to have the property that, for any assignment α, the total weight of the falsified premises equals the total weight of the falsified conclusions. This property is true for all the inference rules in Fig. 4, and it is essentially what is used to prove the soundness of weighted depth-d Frege. The simple proof will appear in the full version of this paper.

Lemma 3.3. *For every $d \in \mathbb{N}$, the proof system weighted depth-d Frege is sound. The same is true for weighted depth-d Frege with the soundness-NS condition.*

Notice that the rules in Fig. 4 are redundant, e.g. the split rule can be simulated using the others. Moreover, only one among fold/unfold is enough. We don't use a minimal set of rules just to highlight the natural symmetry among the rules and to have more freedom to write down weighted Resolution proofs.

Remark 3.1. Restricting weighted depth-d Frege to have negative weights only in the intro./removal rules results in a system p-equivalent to weighted depth-d Frege. Moreover, weighted depth-d Frege is also p-equivalent to weighted depth-d Frege with all weights restricted to be powers of 2.

Remark 3.2. In the definition of weighted depth-d Frege (with the soundness-NS/SA condition) the first property required is that $\mathcal{L}_1 = \{[\Gamma_1; w], \dots [\Gamma_m; w]\}$ where $w \in \mathbb{N}$. We could have required instead

(1) $\mathcal{L}_1 = \{[\Gamma_1; w_1], \dots [\Gamma_m; w_m]\}$ where $w_1, \dots, w_m \in \mathbb{N}$ or even
(2) $\mathcal{L}_1 = \{[\Delta_1; w_1], \dots [\Delta_m; w_m]\}$ with $w_1, \dots, w_m \in \mathbb{N}$ and for all $i \in [m]$, $[\Delta_i; w_i]$ weakening of $[\Gamma_i; w_i]$.

All the three possibilities above would have resulted in p-equivalent systems. The reason is that, in the first case, we can always take $w = \max_{i\in[m]} w_i$. In the second case, given cedents Γ_i, Δ'_i, it is immediate to see that it is possible to infer in depth-d Frege from the weighted cedent $[\Gamma_i; w_i]$ a set S of weighted cedents containing $[\Gamma_i, \Delta'_i; w_i]$. Moreover, all cedents in S are weakening of $[\Gamma_i; w_i]$. This proof is just a sequence of $|\Delta'_i|$ applications of the split rule.

We now prove the p-equivalences and some p-simulations summarized in Fig. 1, 2 and 3. The following is a generalization of SA p-simulates Resolution.

Theorem 3.4. *For every $d \in \mathbb{N}$, weighted depth-d Frege p-simulates depth-d Frege.*

Proof. (sketch) The inference rules of weighted depth-d Frege (if we forget for a moment about the weights) produce the same consequences as the rules of depth-d Frege (and possibly some extra cedents). Since the rules of weighted depth-d Frege are substitution rules, to p-simulate depth-d Frege we take into account the number of times the premises are used, to assign the proper weights to the initial cedents.

To assign weights to Θ_d-cedents, the idea is to set $[\emptyset; 1]$ and then proceed bottom-up in π setting the weight of any Θ_d-cedent Γ looking at all the times it is used and summing the weights of those weighted cedents (similarly as in [9, Lemma 31], for instance). □

Theorem 3.5. *For all $d \in \mathbb{N}$, unary weighted depth-d Frege, with the soundness-NS condition, p-simulates tree-like depth-d Frege.*

This result is a generalization of the proof that NS p-simulates tree-like Resolution. In particular, since tree-like depth-1 Frege p-simulates Resolution [20, Lemma 3.4.2], the theorem implies that unary weighted depth-1 Frege with the soundness-NS condition p-simulates Resolution. The proof of Theorem 3.5 will appear in the full version of this paper.

One of the reasons we introduced weighted proofs is that, varying the soundness condition, it gives a characterization of distinct (semi)-algebraic proof systems in a more logic language.

Theorem 3.6.

(1) *(Unary)* SA *is p-equivalent to (unary) weighted Resolution.*
(2) *(Unary)* NS *is p-equivalent to (unary) weighted Resolution, with the soundness-*NS *condition.*

Moreover, degree-d proofs in SA/NS *correspond to width-d weighted proofs, where the width of a proof is the maximum number of literals in a clause of the proof.*

The part of this theorem for SA is already known: weighted Resolution is p-equivalent to circular Resolution [10] and circular Resolution is p-equivalent to SA [2]. As far as we know, there is no natural restriction of circular Resolution characterizing unary SA nor (unary) NS. Refutations in the systems NS/SA and refutations in weighted Resolution (with the appropriate soundness condition) are two different ways of looking at the same thing. The multisets $\mathcal{L}_1, \dots, \mathcal{L}_s$ in a weighted Resolution refutation are in a correspondence with partial sums of SA/NS refutations. The binomials $m(x_j^2 - x_j)$ correspond to applications of the contraction rule, and the trinomials $m(x_j + \bar{x}_j - 1)$ correspond to applications of the split/symm. cut rules. The proof uses these intuitions, together with the Normal Form Theorem for SA/NS refutations (Theorem 2.7). The proof of Theorem 3.6 will appear in the full version of this paper.

4 THE PIGEONHOLE PRINCIPLE AND UNARY NS/SA

In this section we prove the p-simulations relative to the *unary* parts of Fig. 1, 2 and 3.

Definition 4.1 (pigeonhole principle). Let $m, n \in \mathbb{N}$ with $m > n$ and let $p_{i,j}$ be Boolean variables with $i \in [m]$ and $j \in [n]$. The *pigeonhole principle* is the set of clauses

$$\mathsf{PHP}^m_n = \{\{p_{i,1},\dots,p_{i,n}\} : i \in [m]\} \cup \{\{\neg p_{i,j}, \neg p_{i',j}\} : i,i' \in [m] \text{ distinct}, j \in [n]\}.$$

The *onto-functional* pigeonhole principle ofPHP^m_n is the formula PHP^m_n together with the set of cedents

$$\{\{\neg p_{i,j}, \neg p_{i,j'}\} : i \in [m] \quad j,j' \in [n] \text{ distinct}\}, \tag{5}$$

the *functionality* axioms, and the set

$$\{\{p_{i,j} : i \in [m]\} : j \in [n]\}, \tag{6}$$

the *onto* axioms. Given a bipartite graph $G = (P \cup H, E)$ with $|P| = m$ and $|H| = n$, the *graph* pigeonhole principle $\mathsf{PHP}^m_n(G)$ is the formula PHP^m_n restricted by a partial assignment mapping $p_{i,j} = \bot$ for all $(i,j) \notin E$, i.e. we remove the literal $p_{i,j}$ from every clause of PHP^m_n where it appears and remove all clauses of PHP^m_n containing $\neg p_{i,j}$. The onto-functional *graph* pigeonhole principle $\mathsf{ofPHP}^m_n(G)$ is defined in the same way.

It is well-known that PHP^{n+1}_n has polynomial size unary SA refutations and ofPHP^{n+1}_n has polynomial size unary NS refutations. Let's recall briefly the argument. To refute PHP^{n+1}_n in SA first derive

$$\sum_{j\in[n+1]} \sum_{i\in[n]} p_{i,j} - (n+1) \geq 0 \tag{7}$$

$$n - \sum_{i\in[n]} \sum_{j\in[n+1]} p_{i,j} \geq 0\,. \tag{8}$$

Then, sum the two inequalities to get $-1 \geq 0$. The same argument can be easily adapted to show the results for unary NS. Moreover, for a bipartite graph G with maximum degree d, $\mathsf{PHP}^{n+1}_n(G)$ has degree-d unary SA refutations and $\mathsf{ofPHP}^{n+1}_n(G)$ has degree-d unary NS refutations.

We now show some sort of converse of the previous results: depth-1 Frege + $\mathsf{PHP}^{n+1}_n(G)$ p-simulates unary SA and depth-1 Frege + $\mathsf{ofPHP}^m_n(G)$ p-simulates unary NS.

Theorem 4.2. *For every d, tree-like Res(d)+$\mathsf{PHP}^{n+1}_n(G)$ p-simulates degree-d unary* SA*, where G is restricted to bipartite graphs of degree at most* 3 *and the height of the tree-like Res(d) + $\mathsf{PHP}^{n+1}_n(G)$ derivations is* 5.

Notice that tree-like Res(n) is tree-like depth-1 Frege. The proof of this result is loosely inspired by the proof of [8, Theorem 4].

Proof. We use the characterization of SA given by Theorem 3.6. Let $(\mathcal{L}_1,\dots,\mathcal{L}_s)$ be a weighted Resolution refutation of some set of clauses $F = \{C_1,\dots,C_m\}$. Since the weights are in unary, all the weights in π are just ±1. In this proof, there will be no application of the fold/unfold rules. Without loss of generality, we can assume that all the weights in the contraction/symm.cut/split/excl. middle rules are +1 (see Remark 3.1).

Let $\mathcal{L}_{s+1} = \{[\emptyset;1]\}$ and let P be the multiset given by the disjoint union of the multisets $\mathcal{L}_1,\dots,\mathcal{L}_{s+1}$ and H be the multiset given by the disjoint union of the multisets $\mathcal{L}_1,\dots,\mathcal{L}_s$. In particular, $|P| = |H| + 1$. The multiset P will represent the pigeons and H the holes.

Now for each $\alpha \in P$ and each $\beta \in H$ we want to define $p_{\alpha,\beta}$ as conjunctions of a set of at most d literals, such that we have small tree-like Res(d) derivations of the cedents $\{p_{\alpha,\beta} : \beta \in H\}$ for all $\alpha \in P$, and $\{\neg p_{\alpha,\beta}, \neg p_{\alpha',\beta}\}$ for all $\beta \in H$, and distinct $\alpha,\alpha' \in P$. We also want that $p_{\alpha,\beta} \neq \bot$ for at most 3 values of β and $p_{\alpha,\beta} \neq \bot$ for at most 3 values of α.

Given $\alpha \in P$, let $\alpha = [C_\alpha; w_\alpha]$ and let i_α be the index of the level to which α belongs, i.e. the unique i_α such that $\alpha \in \mathcal{L}_{i_\alpha}$; similarly for $\beta \in H$. Given α,β as above, we say that β is a *contraction/symm.cut/split-premise* of α if $i_\alpha = i_\beta + 1$ and between the layers $\mathcal{L}_{i_\beta}$ and $\mathcal{L}_{i_\alpha}$ there is an application of the contraction/symm.cut/split rule of weighted Resolution with β one of the premises and α one of the conclusions. There are no applications of the fold/unfold rules, so the only rule having two premises is the symmetric cut. We say that α is a *copy* of β if $i_\alpha = i_\beta + 1$ and between the layers $\mathcal{L}_{i_\alpha}$ and $\mathcal{L}_{i_\beta}$, the inference rule applied does not involve α or β. In particular, $[\emptyset;1]$ in $\mathcal{L}_{s+1}$ is a copy of some element in $\mathcal{L}_s$. Moreover, if α is a copy of β, then $C_\alpha = C_\beta$ and $w_\alpha = w_\beta$. If $w_\alpha = 1$ we say that α is a *positive-copy* of β, if $w_\alpha = -1$ we say that α is a *negative-copy* of β. Finally, we say that α,β are *appearing (resp. disappearing) siblings* if $i_\alpha = i_\beta$ and α and β are the result of an introduction rule on the layer $\mathcal{L}_{i_\alpha}$ (resp. α and β are used as premises of a removal rule on the layer $\mathcal{L}_{i_\alpha+1}$).

Informally, we want the formulas $p_{\alpha,\alpha}$ to express that if the clause C_α is true, then α flies to itself (as a hole). That is, we set $p_{\alpha,\alpha}$ to be the formula $\bigvee C_\alpha$ (see (10) below). The notion of a clause being true or false is under a hypothetical assignment satisfying all the initial clauses.

If C_α is an initial clause α always flies to itself. So we set $p_{\alpha,\alpha} = x \vee \neg x$ (see (9)).

If C_α is false and its weight is +1, it flies to the false premise C_β used to derive it or to its appearing sibling. The way to say that C_α and C_β are false is to use the formula $\neg\bigvee C_\alpha \wedge \neg\bigvee C_\beta$, but this is redundant, since it is always the case that either C_α contains C_β (see (13)) or the opposite (see (11)).

If C_α is false and the weight of C_α is -1 then α flies to its copy C_β in the direction of the proof, or to its disappearing sibling (see (12)). The way to define $p_{\alpha,\beta}$ is analogous as before.

Formally, $p_{\alpha,\beta}$ is the formula

$$x \vee \neg x \quad \text{if } \alpha = \beta \text{ and } \alpha \in \mathcal{L}_1\,, \tag{9}$$

$$\bigvee C_\alpha \quad \text{if } \alpha = \beta \text{ and } \alpha \notin \mathcal{L}_1\,, \tag{10}$$

$$\neg\bigvee C_\beta \ \text{ if } \begin{cases} \beta \text{ is a } \textsc{symm.cut}\text{-premise of } \alpha \\ \beta \text{ is a } \textsc{contraction}\text{-premise of } \alpha \\ \alpha,\beta \text{ appearing siblings}, w_\alpha = 1 \\ \alpha \text{ is a positive-copy of } \beta \end{cases} \tag{11}$$

$$\neg\bigvee C_\beta \ \text{ if } \begin{cases} \alpha,\beta \text{ disappearing siblings}, w_\alpha = -1 \\ \beta \text{ is a negative-copy of } \alpha \end{cases} \tag{12}$$

$$\neg\bigvee C_\alpha \quad \text{if } \beta \text{ is a } \textsc{split}\text{-premise of } \alpha\,, \tag{13}$$

$$\bot \quad \text{otherwise}\,.$$

The totality axioms $\{p_{\alpha,\beta} : \beta \in H\}$ are easily derivable in tree-like Res(d) from the initial clauses $C_1,\dots,C_m$. We need to check several cases.

If C_α is one of the initial clauses $C_1,\dots,C_m$ or an instance of the excluded middle rule, in both cases $\{p_{\alpha,\beta} : \beta \in H\} = \{p_{\alpha,\alpha}\}$. The cedent $\{p_{\alpha,\alpha}\}$ can be obtained by the EXCLUDED MIDDLE rule and $\bigvee$-INTRODUCTION RULE.

If C_α is the result of the application of a CONTRACTION rule on C_β

$$\{p_{\alpha,\gamma} : \gamma \in H\} = \{\bigvee C_\alpha, \neg \bigvee C_\beta\}\,.$$

If C_α is the result of the application of a SPLIT rule on C_β or α is a copy of β or α, β are appearing/disappearing siblings then

$$\{p_{\alpha,\gamma} : \gamma \in H\} = \{\bigvee C_\alpha,\ \neg \bigvee C_\alpha\}$$

is an instance of the EXCLUDED MIDDLE rule of Res(d), the height to derive it is 1.

The only remaining case is when α is the conclusion of a SYMMETRIC CUT with premises β, β'. Then, $\bigvee C_\beta = \bigvee C_\alpha \vee x$ and $\bigvee C_{\beta'} = \bigvee C_\alpha \vee \neg x$, and the totality axiom for the pigeon α is

$$\{p_{\alpha,\gamma} : \gamma \in H\} = \{\bigvee C_\alpha,\ \neg \bigvee C_\alpha \wedge \neg x,\ \neg \bigvee C_\alpha \wedge x\}\,.$$

This formula can be derived by first deriving by EXCLUDED MIDDLE

$$\{\bigvee C_\alpha \vee x,\ \neg \bigvee C_\alpha \wedge \neg x\} \quad \text{and} \quad \{\bigvee C_\alpha \vee \neg x,\ \neg \bigvee C_\alpha \wedge x\}\,,$$

then by SYMMETRIC CUT on weakening of the previous two cedents we derive

$$\{\bigvee C_\alpha,\ \neg \bigvee C_\alpha \wedge \neg x,\ \neg \bigvee C_\alpha \wedge x\}\,.$$

This derivation has height 5.

The injectivity axioms $\{\neg p_{\alpha,\beta},\ \neg p_{\alpha',\beta}\}$ are also easily derivable from the initial clauses $C_1, \ldots, C_m$. As before, we have several cases.

Case $\alpha' = \beta$.

- If $\beta \notin \mathcal{L}_1$, then $\{\neg p_{\alpha,\beta},\ \neg p_{\beta,\beta}\}$ is either $\{\bigvee C_\beta, \neg \bigvee C_\beta\}$ or $\{\bigvee C_\alpha, \neg \bigvee C_\beta\}$ if β is a SPLIT-premise of α. In both cases, these are easy tautologies derivable in small height.
- If $\beta \in \mathcal{L}_1$, then $\{\neg p_{\alpha,\beta},\ \neg p_{\beta,\beta}\}$ is either $\{\bigvee C_\beta,\ \neg(x \vee \neg x)\}$ or $\{\bigvee C_\alpha,\ \neg(x \vee \neg x)\}$ if β is a SPLIT-premise of α. In both cases they are derivable from C_β, a clause that is a weakening of an initial clause from $C_1, \ldots, C_m$, in small height.

Case $\alpha, \alpha' \neq \beta$.

- If $w_\beta = -1$, then there are no axioms of the form $\{\neg p_{\alpha,\beta},\ \neg p_{\alpha',\beta}\}$ since in β can only fly two pigeons, β itself and the copy of β from the previous layer (or its disappearing sibling).
- If $w_\beta = 1$, having the variables $p_{\alpha,\beta}$ and $p_{\alpha',\beta}$ distinct from $\bot$ means in particular that $i_\alpha = i_{\alpha'} = i_\beta + 1$ and β is a premise of both α and α'. That is, at level $\mathcal{L}_{i_\beta}$ we applied a SPLIT rule on β obtaining α, α'. I.e. $\bigvee C_\alpha = \bigvee C_\beta \vee x$ and $\bigvee C_{\alpha'} = \bigvee C_\beta \vee \neg x$ for some variable x. Hence,

$$\begin{aligned}\{\neg p_{\alpha,\beta},\ \neg p_{\alpha',\beta}\} &= \{\neg(\neg \bigvee C_\beta \wedge \neg x),\ \neg(\neg \bigvee C_\beta \wedge x)\}\\ &= \{\bigvee C_\beta \vee x, \bigvee C_\beta \vee \neg x\}\,,\end{aligned}$$

which is a tautology derivable in small height in Res(d) being a weakening of $x \vee \neg x$.

We showed that from the clauses $C_1, \ldots, C_m$ in tree-like Res(d) it is possible to derive all the clauses of the formula $\mathsf{PHP}^{n+1}_n(p_{\alpha,\beta})$, which is a $\mathsf{PHP}^{n+1}_n(G)$ for some graph G of degree at most 3. This concludes the refutation in tree-like Res(d) + $\mathsf{PHP}^{n+1}_n(G)$. It is a refutation of height 5. ◻

The construction of the formulas $p_{\alpha,\beta}$ in the previous proof does not satisfy the *onto* axioms but it clearly satisfies the *functionality axioms* of $\mathsf{ofPHP}^{n+1}_n(G)$, which means that the substitution instance of the functionality axioms is a tautology easily derivable. The reason the construction does not satisfy the onto axioms is the following. The last layer $\mathcal{L}_s$ might contain arbitrary weighted clauses $[C_\beta; w_\beta]$ that, if true, are mapped to themselves. Therefore, they receive a pigeon. If they are false, they are mapped to some hole in $\mathcal{L}_{s-1}$, and hence they, as a hole, don't receive a pigeon. Therefore, we have no guarantee that the holes in $\mathcal{L}_s$ receive some pigeon. If $\mathcal{L}_s$ satisfies the SOUNDNESS-NS condition we can adapt the definition of $p_{\alpha,\beta}$ in the proof of Theorem 4.2 to satisfy the *onto* axioms of the pigeonhole principle.

THEOREM 4.3. *For every d, tree-like Res(d)+$\mathsf{ofPHP}^m_n(G)$ p-simulates degree-d unary NS, where G is restricted to bipartite graphs of degree at most 3 and the height of the tree-like Res(d) + $\mathsf{ofPHP}^m_n(G)$ derivations is 5.*

PROOF. (sketch) We use the characterization of unary NS given by Theorem 3.6, and we argue basically as in Theorem 4.2. We know that the problematic clauses in $\mathcal{L}_s$ are weakening of initial axioms or several copies of $[\emptyset; 1]$. We can define the formula $p_{\alpha,\beta}$ as in Theorem 4.2. Now, the onto axioms for the holes in $\mathcal{L}_s$ become weakening of initial clauses, except for the holes corresponding to the copies of $[\emptyset; 1]$. Those, as in the case of SA, are copied in the layer $\mathcal{L}_{s+1}$. With the exception that for the argument in SA we only needed to copy one of the $[\emptyset; 1]$, here we need to copy all of them. Hence instead of $\mathsf{PHP}^{n+1}_n(G)$ we use $\mathsf{ofPHP}^m_n(G)$. ◻

The proof of Theorem 4.2 will generalize, almost without changes, if instead of clauses we consider Θ_d-cedents. This will appear in the full version of this paper.

THEOREM 4.4. *For every $d \in \mathbb{N}$, tree-like depth-($d+1$) Frege + $\mathsf{PHP}^{n+1}_n(G)$ p-simulates unary weighted depth-d Frege, where G is restricted to bipartite graphs of degree at most 3.*

We conclude this section with a couple of separations and lower-bounds.

PROPOSITION 4.5. *For every $d = o\left(\frac{\log\log n}{\log\log\log n}\right)$, depth-$d$ Frege does not p-simulate unary weighted depth-d Frege.*

PROOF. Any refutation of PHP^{n+1}_n in depth-d Frege must have size at least $2^{n^{(1/6)^d}}$ (see for instance [30]). PHP^{n+1}_n has polynomial size unary SA refutations, and hence it has polynomial size refutations in unary weighted depth-d Frege. ◻

Definition 4.6 (MOD$_2$ principle). Given $n \in \mathbb{N}$, the *MOD$_2$-principle* is the set of cedents in the variables $x_{i,j}$ for $i \neq j \in S$

$$\begin{aligned}\mathsf{MOD}^n_2 = &\{\{x_{i,1}, \ldots, x_{i,i-1}, x_{i,i+1}, \ldots, x_{i,2n+1}\} : i \in [2n+1]\}\\ &\cup \{\{\neg x_{i,j}, \neg x_{i',j}\} : i, i' \in [2n+1] \text{ distinct}, j \in [2n+1]\}\,.\end{aligned}$$

COROLLARY 4.7. *Given $n \in \mathbb{N}$ and $d = o\left(\frac{\log\log n}{\log\log\log n}\right)$, MOD^n_2 has no polynomial-size unary weighted depth-d Frege refutations.*

PROOF. Any refutation of MOD^n_2 in depth-d Frege + PHP must require size at least $\exp(n^{\Omega(1/d4^d)})$ [6, Theorem 4]. By Theorem

4.4 depth-$(d+1)$ Frege + PHP p-simulates unary weighted depth-d Frege. The lower bound follows: the formula MOD_2^n requires unary weighted depth-d Frege refutations of size $\exp(n^{\Omega(1/(d+1)4^d)})$. ☐

Definition 4.8 (bit-pigeonhole principle, [13] for instance). Let $n = 2^k$. The formula $\texttt{bit-PHP}_n$ has variables $b_{i\ell}$ for each $i \in [n+1]$ and $\ell \in [k]$. The variables $b_{i1}, \dots, b_{ik}$ represent the binary expansion of a hole, the hole i is mapped to. Then $\texttt{bit-PHP}_n$ only needs to enforce injectivity. The formula $\texttt{bit-PHP}_n$ is

$$\left\{ \{b_{i1}^{1-h_1}, \dots, b_{ik}^{1-h_k}, b_{i'1}^{1-h_1}, \dots, b_{i'k}^{1-h_k}\} : \begin{array}{c} i \neq i' \in [n+1] \\ h \in [n] \end{array} \right\},$$

where $h_1, \dots, h_k$ is the binary expansion of the hole h and $b_{ij}^{h_j} = b_{ij}$ if $h_j = 1$ and $b_{ij}^{h_j} = \neg b_{ij}$ if $h_j = 0$.

Corollary 4.9. SA *does not p-simulate tree-like depth-*1 *Frege* + PHP_n^{n+1}.

Proof. $\texttt{bit-PHP}_n$ does not have polynomial-size SA refutations [13]. To prove $\texttt{bit-PHP}_n$ in tree-like depth-1 Frege + PHP_n^{n+1}, we use the substitution $p_{ij} = b_{i1}^{j_1} \wedge \cdots \wedge b_{ik}^{j_k}$ where $j = (j_1, \dots, j_k)_2$. For $i \neq i' \in [n+1]$ and $j \in [n]$, $\{\neg p_{ij}, \neg p_{i'j}\}$ is immediately derivable from the axioms of $\texttt{bit-PHP}_n$ by $\bigvee$-introduction. For every $i \in [n+1]$, the cedent $\{p_{i1}, \dots, p_{in}\}$ is tautological, and it has $k = \log n$ variables. By excluded middle, derive all the $\{p_{ij}, \neg p_{ij}\}$ and then with weakening and 2^k applications of symm. cut it is easy to obtain $\{p_{i1}, \dots, p_{in}\}$. ☐

5 THE *WEIGHTED* PIGEONHOLE PRINCIPLE AND SHERALI-ADAMS

In this section, we generalize the constructions given for unary SA/NS and unary weighted depth-d Frege to systems with binary weights/coefficients. We prove all remaining p-simulations in Fig. 1, 2 and 3.

The starting point of this section is that, it is not clear at all whether it is possible to adapt Theorem 4.4 to show that tree-like depth-1 Frege + $\mathsf{PHP}_n^{n+1}(G)$ p-simulates SA. It seems we need a stronger version of the pigeonhole principle. For this reason, we introduce a new combinatorial principle, the *weighted* PHP.

The weighted pigeonhole principle maps n^2+1 pigeons into n^2 holes. First, we partition both sets of pigeons and holes into n parts. The partition of the holes consists of n sets $H_1, \dots, H_n$ given by $H_\ell = \{(\ell-1)n+1, \dots, \ell n\}$. Let $H_0 = H_{n+1} = \emptyset$. For the partition of the pigeons we set, for some $j \in [n]$, $P_j = H_j \cup \{n^2+1\}$ and for the remaining $\ell \in [n] \setminus \{j\}$, $P_\ell = H_\ell$. Let $P_0 = P_{n+1} = \emptyset$.

*Definition 5.1 (weighted pigeonhole principle, w*PHP*).* The *weighted* pigeonhole principle has variables x_{ij} for each $i \in [n^2+1]$ and each $j \in [n^2]$. The formula $w\mathsf{PHP}_{n^2}^{n^2+1}$ has the following clauses. For every $\ell \in [n]$, every pigeon $p \in P_\ell$ we have clauses

$$\{x_{p1}, \dots, x_{pn^2}\}, \tag{14}$$

$$\{\neg x_{pj}\} \quad \text{for all } j \notin H_{\ell-1} \cup H_\ell \cup H_{\ell+1}, \tag{15}$$

$$\{\neg x_{pj},\ x_{pj'} : j' \in H_{\ell-1} \setminus \{j\}\} \ \text{ for all } \ j \in H_{\ell-1}, \tag{16}$$

$$\{\neg x_{pj_1},\ \neg x_{pj_2},\ \neg x_{pj_3}\} \ \text{ for all distinct } j_1, j_2, j_3 \in H_{\ell-1} \tag{17}$$

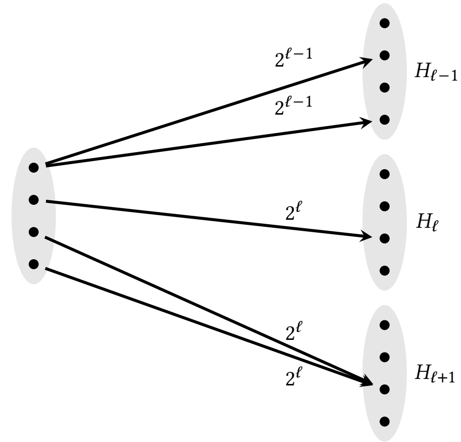

Figure 5: Possible ways pigeons in P_ℓ can fly.

and every hole $h \in H_\ell$, we have clauses

$$\{\neg x_{ih},\ \neg x_{i'h}\} \quad \text{for all distinct } i \in P_\ell \cup P_{\ell+1} \text{ and } i' \in [n^2+1], \tag{18}$$

$$\{\neg x_{i_1h},\ \neg x_{i_2h},\ \neg x_{i_3h}\} \quad \text{for all distinct } i_1, i_2, i_3 \in P_{\ell-1}. \tag{19}$$

Intuitively, $p \in P_\ell$ means that p has mass 2^ℓ, and $h \in H_\ell$ means h has capacity 2^ℓ, see Fig. 5. The pigeon $p \in P_\ell$ has to fly somewhere (eq. (14)) and moreover, it can only fly to holes in $H_{\ell-1}$ or H_ℓ or $H_{\ell+1}$ (eq. (15)). The pigeon has to fly with either full or half-mass. If $p \in P_\ell$ flies to $H_{\ell-1}$, it flies with half-mass and hence it should fly to two distinct holes in $H_{\ell-1}$ (eq. (16)) but not to three holes in $H_{\ell-1}$ (eq. (17)). If $p \in P_\ell$ flies to H_ℓ, we assume it flies with full mass, hence completely filling the capacity of a hole in H_ℓ (eq. (18)). If $p \in P_\ell$ flies to $H_{\ell+1}$, we also assume it flies with full mass, but now it only fills half of the capacity of a hole in $H_{\ell+1}$. Therefore, to fill the capacity of a hole $h \in H_{\ell+1}$ we will need another pigeon from P_ℓ flying to h but not two more (eq. (19)).

The intended meaning of the variable x_{ij} for $i \in P_\ell$ is: for $j \in H_\ell \cup H_{\ell+1}$, $x_{ij} = 1$ means "*the pigeon i flies to j with mass* 2^ℓ"; for $j \in H_{\ell-1}$, $x_{ij} = 1$ means "*i flies to j with mass* $2^{\ell-1}$". If $j \notin H_{\ell-1} \cup H_\ell \cup H_{\ell+1}$ then $x_{ij} = \bot$.
Similar to the PHP case, given a bipartite graph $G = (P \dot\cup H, E)$ with $|P| = n^2+1$ and $|H| = n^2$, the *graph* weighted pigeonhole principle $w\mathsf{PHP}_{n^2}^{n^2+1}(G)$ is the formula $w\mathsf{PHP}_{n^2}^{n^2+1} \restriction_\alpha$ where α is a partial restriction mapping $x_{i,j} = \bot$ for all $(i,j) \notin E$.

If we add to $w\mathsf{PHP}_{n^2}^{n^2+1}$ the following *onto-functional* axioms, we obtain the formula $w\mathsf{ofPHP}_{n^2}^{n^2+1}$. The axioms we add are: for every $\ell \in [n]$ and every pigeon $p \in P_\ell$ the clauses

$$\{\neg x_{pj},\ \neg x_{pj'}\} \quad \text{for all distinct } j \in H_\ell \cup H_{\ell+1} \text{ and } j' \in [n^2],$$

and every hole $h \in H_\ell$ the clauses

$$\{x_{1h}, \dots, x_{n^2+1,h}\},$$
$$\{\neg x_{ih},\ x_{i'h} : i' \in P_{\ell-1} \setminus \{i\}\} \ \text{ for all } \ i \in P_{\ell-1}.$$

The clauses in eq. (17) are not needed to have an unsatisfiable formula but they are useful to have a short proof in SA. When considering $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$, the graphs G we need to consider, turn out to always have at most 2 edges of the form $(p, j), (p, j')$ with $p \in P_\ell$ and $j, j' \in H_{\ell-1}$. Hence, for those graphs G, the axioms in eq. (17) are always satisfied: one of the variables x_{pj_1}, x_{pj_2}, x_{pj_3} is always set to $\bot$.

Remark 5.1. We defined $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ for a very specific fixed partitions $H_1, \dots H_n$, and $P_1, \dots, P_n$, all of size n except for one P_j of size $n+1$. We could also allow $P_1, P_2, \dots, P_n$ to be disjoint sets of size possibly smaller than n (at most $n+1$ for one P_j). This would not give a more general definition of $w\mathsf{PHP}^{n^2+1}_{n^2}$, as long as for every $\ell \in [n]$, $H_\ell = P_\ell \setminus \{n^2+1\}$. Basically, we could add some padding to all P_js and H_js, until they have size n and change G to a graph that forces the new vertices in each part P_j to be mapped to the corresponding new vertex in H_j. In Theorem 5.3 we will use the $w\mathsf{PHP}^{n^2+1}_{n^2}$ with partition sets possibly smaller than n and we will not use the padding.

It may be not immediately clear why $w\mathsf{PHP}^{n^2+1}_{n^2}$ is unsatisfiable. Informally, a way to see this is to notice that for every pigeon p (say $p \in P_\ell$) the axioms of $w\mathsf{PHP}^{n^2+1}_{n^2}$ can be interpreted to state that the weight flying away from p is at least 2^ℓ and, for every hole h (say $h \in H_\ell$), the weight it can accommodate is at most 2^ℓ. So the holes can, in total, accommodate a total weight of at most $\sum_{\ell\in[n]} n2^\ell$ which is strictly smaller than the total weight of the pigeons flying, that is $2^j + \sum_{\ell\in[n]} n2^\ell$ for some $j \in [n]$.

Next, we formalize this argument in SA.

Theorem 5.2. *The formula $w\mathsf{PHP}^{n^2+1}_{n^2}$ has polynomial-size SA refutations. Also, for every bipartite graph $G = (P\dot\cup H, E)$ with $|P| = n^2+1$, $|H| = n^2$ and degree d, $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ has SA-refutations of degree d.*

Proof. (sketch) First observe that the axioms imply, for every $i \in [n^2+1]$ with $i \in P_\ell$, the inequality

$$2\sum_{j\in H_\ell\cup H_{\ell+1}} x_{ij} + \sum_{j\in H_{\ell-1}} x_{ij} - 2 \geq 0\,, \tag{20}$$

and, for each $j \in [n^2]$ with $j \in H_\ell$, the inequality

$$2 - 2\sum_{i\in P_\ell\cup P_{\ell+1}} x_{ij} - \sum_{i\in P_{\ell-1}} x_{ij} \geq 0\,. \tag{21}$$

Eq. (20) says that the pigeon i must fly at least once into the set $H_\ell \cup H_{\ell+1}$ or at least twice into the set $H_{\ell-1}$.

Eq. (21) says that the hole j can receive at most one pigeon from the set $P_\ell \cup P_{\ell+1}$, or at most two pigeons from $P_{\ell-1}$.

The proof of the two inequalities will appear in the full version of this paper. To conclude, we want to sum appropriate multiples of eq. (20) and eq. (21), in a way that all variables from (20) cancel with variables in (21), and after all the cancellations we just get some negative constant:

$$\sum_{\substack{\ell\in[n]\\ i\in P_\ell}} 2^\ell\left(2\sum_{j\in H_\ell\cup H_{\ell+1}} x_{ij} + \sum_{j\in P_{\ell-1}} x_{ij} - 2\right) + \sum_{\substack{\ell\in[n]\\ j\in H_\ell}} 2^\ell\left(2 - 2\sum_{i\in P_\ell\cup P_{\ell+1}} x_{ij} - \sum_{i\in P_{\ell-1}} x_{ij}\right) \geq 0\,. \tag{22}$$

Consider a variable x_{ij} in (22), with $i \in P_\ell$.

If $j \in H_\ell$, the coefficient of x_{ij} is $2^\ell \cdot 2 - 2^\ell \cdot 2 = 0$.

If $j \in H_{\ell+1}$, the coefficient of x_{ij} is $2^\ell \cdot 2 - 2^{\ell+1} = 0$.

If $j \in H_{\ell-1}$, the coefficient of x_{ij} is $2^\ell - 2 \cdot 2^{\ell-1} = 0$.

That is, all the variables x_{ij} cancel out in (22). The constants in (22) sum to

$$-2\sum_{\substack{\ell\in[n]\\ i\in P_\ell}} 2^\ell + 2\sum_{\substack{\ell\in[n]\\ j\in H_\ell}} 2^\ell = -2^{j+1}\,,$$

if the pigeon n^2+1 was in the set P_j, since $|P_\ell| = |H_\ell|$ for all ℓ except for j where $|P_j| = |H_j| + 1$. That is, the sum in (22), after cancellations, reduces to the trivial contradiction $-2^{j+1} \geq 0$. ◻

Via a similar argument, it is easy to see that $w\mathsf{ofPHP}^{n^2+1}_{n^2}$ has polynomial-size NS refutations.

Remark 5.2. Notice that there is also a different way to infer a contradiction from (20) and (21). This results in a system of polynomial inequalities that does not have polynomial-size unary SA refutations, and hence separating SA and unary SA. This can be seen by a minor modification of the techniques in [18]. Recently, a preprint was submitted to ArXiv showing that unary SA does not p-simulate Resolution [17]. As a corollary, they show that SA and unary SA are not p-equivalent using polynomials encoding propositional formulas.

It is easy to see that depth-1 Frege + wPHP proves PHP in polynomial size. We don't know whether the opposite is true, but we suspect it is not (see Section 6), even using higher constant depth. This would imply not only that $w\mathsf{PHP}^{n^2+1}_{n^2}$ is hard to refute in unary SA, via Theorem 4.2, but even in unary weighted depth-d Frege, via Theorem 4.4.

We now prove the remaining p-simulations from Fig. 1, Fig. 2, and Fig. 3.

Theorem 5.3. *For every $d \in \mathbb{N}$, the proof system tree-like Res(d) + $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ p-simulates degree-d SA, where G is restricted to bipartite graphs of degree at most 3 and the tree-like Res(d) + $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ derivations have height 5.*

Proof. The structure of the proof is similar to the proof of Theorem 4.2. By Theorem 3.6 it is enough to prove the result for weighted Resolution. Let $\pi = \mathcal{L}_1, \dots, \mathcal{L}_s$ be a weighted Resolution refutation of a set of clauses $\{C_1, \dots, C_m\}$. W.l.o.g. we can assume that no weighted cedent in π has weight 0 and, by Remark 3.1, we can assume that all the weights appearing in π are powers of 2, and all the rules have positive weights, except for introduction/removal. Moreover, since π is a refutation, we can assume

$[\emptyset; 1] \in \mathcal{L}_s$. If the last layer of π had $[\emptyset; 2^z]$ for some $z \geq 0$, we can obtain a new last layer containing $[\emptyset; 1]$, using the UNFOLD rule.

We define a substitution instance of $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ without padding (see Remark 5.1) such that we have shallow $\mathrm{Res}(d)$ derivations of it.

Let $\mathcal{S}+1$ be the size of π, let $\mathcal{L}_{s+1} = \{[\emptyset; 1]\}$ and let $P_1, \ldots, P_{\mathcal{S}}$ be a partition of the multiset $\mathcal{L}_1 \cup \cdots \cup \mathcal{L}_{s+1}$ according to the weight of the weighted clauses, i.e. all the weighted clauses in P_j have weight 2^{j-1} or -2^{j-1}. By assumption, all those multisets have size at most $\mathcal{S}$, except P_1 that has size at most $\mathcal{S}+1$. Let $P_0 = P_{\mathcal{S}+1} = \emptyset$. Let $H_1, \ldots, H_{\mathcal{S}}$ be defined as $H_1 = P_1 \setminus \mathcal{L}_{s+1}$, and for all $\ell \in \{2, \ldots, \mathcal{S}\}$, $H_\ell = P_\ell$. Let $H_0 = H_{\mathcal{S}+1} = \emptyset$.

Let P be the multiset given by the disjoint union of the multisets $P_1, \ldots, P_{\mathcal{S}}$ and similarly, let H be the disjoint union of the multisets $H_1, \ldots, H_{\mathcal{S}}$. Now, for all $\ell \in [S]$, $\alpha \in P_\ell$, and $\beta \in H_\ell$ we want to define $\bigwedge$-formulas $x_{\alpha,\gamma}$ and $x_{\gamma',\beta}$ such that we can easily derive from $C_1, \ldots, C_m$ the cedents

$$\{x_{\alpha\gamma} : \gamma \in H\} \tag{23}$$

$$\{\neg x_{\alpha\beta}\} \quad \text{for all } \beta \notin H_{\ell-1} \cup H_\ell \cup H_{\ell+1} \tag{24}$$

$$\{\neg x_{\alpha\gamma}, x_{\alpha\gamma'} : \gamma' \in H_{\ell-1} \setminus \{\gamma\}\} \quad \text{for all } \gamma \in H_{\ell-1} \tag{25}$$

$$\{\neg x_{\alpha\gamma_1},\ \neg x_{\alpha\gamma_2},\ \neg x_{\alpha\gamma_3}\} \quad \text{for all distinct } \gamma_1, \gamma_2, \gamma_3 \in H_{\ell-1}\,, \tag{26}$$

$$\{\neg x_{\gamma\beta},\ \neg x_{\gamma'\beta}\} \quad \text{for all distinct } \gamma \in P_\ell \cup P_{\ell+1}\,, \gamma' \in P \tag{27}$$

$$\{\neg x_{\gamma_1\beta},\ \neg x_{\gamma_2\beta}, \neg x_{\gamma_3\beta}\} \quad \text{for all distinct } \gamma_1, \gamma_2, \gamma_3 \in P_{\ell-1}\,. \tag{28}$$

Informally, the idea is very similar to Theorem 4.2. We want the $\bigwedge$-formulas $x_{\alpha,\beta}$ to express that if the clause C_α is true then α flies to itself (as a hole), if it is false and its weight is positive, it flies to *all* the false premises used to derive it (i.e. two in the case of the FOLD and one in all remaining cases) or to its appearing sibling. If C_α is a weakening of an initial clause, it flies to itself. If the weight of C_α is negative, then α flies to its copy in the direction of the proof, or to its disappearing sibling. If we define a mapping from pigeons to holes in this way, there might be collisions due to the UNFOLD rules. Those types of collisions are exactly the ones allowed to have in the $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ principle, since they correspond to mapping two pigeons with mass 2^j to one hole with capacity 2^{j+1}.

Given $\alpha \in \pi \cup \mathcal{L}_{s+1}$, let i_α be the unique index of the level where α belongs, i.e. $\alpha \in \mathcal{L}_{i_\alpha}$, and let w_α be the weight of α. Recall that given α, β in π we say that β is a *premise* of α if $i_\alpha = i_\beta + 1$, and between the layers $\mathcal{L}_{i_\beta}$ and $\mathcal{L}_{i_\alpha}$ we apply one of the inference rules of Fig. 4, with β one of the premises and α one of the conclusions. β is an *UNFOLD-premise* of α if β is a premise of α and the rule applied is the UNFOLD rule. The rest of the terminology is the same as in the proof of Theorem 4.2.

Using the terminology from Theorem 4.2, the definition of $x_{\alpha,\beta}$ is the same as the definition of $p_{\alpha,\beta}$, with just two more cases. The formula $x_{\alpha,\beta}$ is

$$
\begin{cases}
x \vee \neg x & \text{if } \alpha = \beta \text{ and } \alpha \in \mathcal{L}_1\,,\\
\bigvee C_\alpha & \text{if } \alpha = \beta \text{ and } \alpha \notin \mathcal{L}_1\,,\\
\neg \bigvee C_\beta & \text{if } \begin{cases} \beta \text{ is a SYMM.CUT-premise of } \alpha\\ \beta \text{ is a CONTRACTION-premise of } \alpha\\ \beta \text{ is a FOLD/UNFOLD-premise of } \alpha\\ \alpha,\beta \text{ are appearing siblings and } w_\alpha > 0\\ \alpha \text{ is a positive-copy of } \beta \end{cases}\\
\neg \bigvee C_\beta & \text{if } \begin{cases} \alpha,\beta \text{ are disappearing siblings and } w_\alpha < 0\\ \beta \text{ is a negative-copy of } \alpha \end{cases}\\
\neg \bigvee C_\alpha & \text{if } \beta \text{ is a SPLIT-premise of } \alpha\,,\\
\bot & \text{otherwise}\,.
\end{cases}
$$

The axioms that require a slightly different argument from the proof of Theorem 4.2 are (25)–(28). The axiom (25) is a weakening of $\top$ in all cases, except when α is the conclusion of a FOLD rule and γ is one of its premises. Let 2^ℓ be the weight of α, i.e. both its FOLD premises β, γ have weights $2^{\ell-1}$ and

$$\{\neg x_{\alpha\gamma}, x_{\alpha\gamma'} : \gamma' \in W_{\ell-1} \setminus \{\gamma\}\} = \{\bigvee C_\alpha, \neg \bigvee C_\alpha\}\,.$$

The axiom (26) is always a weakening of $\top$, since all inference rules have at most 2 premises and none of the $\gamma_1, \gamma_2, \gamma_3$ can be α, since $\alpha \in P_\ell$ and the γ_is are in $H_{\ell-1}$. Hence, at least one among the variables $x_{\alpha\gamma_1}, x_{\alpha\gamma_2}, x_{\alpha\gamma_3}$ is $\bot$ and its negation is true, i.e. $\top$. Similarly, the axiom (28) is always a weakening of $\top$, since all the rules have at most two conclusions and the γ_is cannot be β, for the same reason as before. Hence, one among the variables $x_{\gamma_1\beta}, x_{\gamma_2\beta}, x_{\gamma_3\beta}$ is always $\bot$.

To check the axioms in (27) we proceed exactly as in the cases of the injectivity in Theorem 4.2. Notice that the cedents $\{\neg x_{\gamma\beta}, \neg x_{\gamma'\beta}\}$ for β an UNFOLD premise of γ and γ' are <u>not</u> part of the cedents in eq. (26).

We showed that from the clauses $C_1, \ldots, C_m$ in tree-like $\mathrm{Res}(d)$ it is possible to derive all the clauses of the formula $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ in the formulas $x_{\alpha,\beta}$, which is a $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$ for some graph G of degree at most 3. □

The construction of the formulas $x_{\alpha,\beta}$ in the previous proof does not satisfy the *onto/functional* axioms of wofPHP. The reason is the same we had for PHP and unary SA: the last layer $\mathcal{L}_s$ might contain arbitrary weighted clauses $[C_\beta; w_\beta]$. If they are true, they are mapped to themselves. If they are false, they are mapped to some hole in $\mathcal{L}_{s-1}$. We have no guarantees that the holes in $\mathcal{L}_s$ receive some pigeon, but if $\mathcal{L}_s$ satisfies the SOUNDNESS-NS condition we can adapt the definition of $x_{\alpha,\beta}$ in the proof of Theorem 5.3 to satisfy the *onto/functional* axioms of the weighted pigeonhole principle.

THEOREM 5.4. *For every d, tree-like $\mathrm{Res}(d)$ + $\mathsf{wofPHP}^{n^2+1}_{n^2}(G)$ p-simulates degree-d NS, where G is restricted to bipartite graphs of degree at most 3 and the height of the tree-like $\mathrm{Res}(d)$ + $\mathsf{wofPHP}^{n^2+1}_{n^2}(G)$ derivations is 5.*

PROOF. (sketch) We use the characterization of NS given by Theorem 3.6 and we reason basically as in Theorem 4.3. We know that the problematic clauses in $\mathcal{L}_s$ are weakening of initial axioms or a single instance of $[\emptyset; z]$. We copy $[\emptyset; z]$ to a $\mathcal{L}_{s+1}$, and we define the formula $x_{\alpha,\beta}$ as in Theorem 5.3. Now the onto axioms for the holes in $\mathcal{L}_s$ become weakening of initial clauses except for the hole $[\emptyset; z]$, which receive a pigeon flying there from the layer $\mathcal{L}_{s+1}$. □

It is immediate to generalize Theorem 5.3 from clauses to Θ_d-cedents. The argument for this generalization is the same as in Theorem 4.4.

Theorem 5.5. *For all $d \in \mathbb{N}$, weighted depth-d Frege is p-simulated by tree-like depth-$(d+1)$ Frege + $w\mathsf{PHP}^{n^2+1}_{n^2}(G)$, where G is restricted to bipartite graphs of degree at most* 3.

6 OPEN QUESTIONS

In addition to the open questions left in Fig. 1, 2 and 3, we conclude this article with a list of open problems.

(1) Prove that depth-d Frege + $w\mathsf{PHP}$ is strictly weaker than Frege, say for at least d constant.
(2) Refining on the problem above, prove that the formula MOD_2 (see Definition 4.6) does not have polynomial size refutations in depth-d Frege + $w\mathsf{PHP}$, say for at least d constant.
(3) Does depth-d Frege + PHP, say for constant d, have polynomial size refutations of $w\mathsf{PHP}$? A negative answer, together with Theorem 5.5, would imply super-polynomial size lower bounds for weighted depth-d Frege.

ACKNOWLEDGMENTS

We would like to thank Albert Atserias, Massimo Lauria, Sam Buss, Neil Thapen and Moritz Müller for very fruitful conversations that simplified and improved this paper.

This work is supported by the grants PID2019-109137GB-C21, PID2019-109137GB-C22 and IJC2018-035334-I funded by MCIN/AEI/ 10.13039/501100011033.

REFERENCES

[1] M. Ajtai. 1990. *Parity and the Pigeonhole Principle*. Birkhäuser Boston, Boston, MA, 1–24.
[2] Albert Atserias and Massimo Lauria. 2019. Circular (Yet Sound) Proofs. In *Theory and Applications of Satisfiability Testing - SAT 2019 - 22nd International Conference, SAT 2019, Lisbon, Portugal, July 9-12, 2019, Proceedings (Lecture Notes in Computer Science)*, Mikolás Janota and Inês Lynce (Eds.), Vol. 11628. Springer, 1–18.
[3] Albert Atserias and Joanna Ochremiak. 2018. Proof Complexity Meets Algebra. *ACM Trans. Comput. Logic* 20, 1 (Dec. 2018), 1–46.
[4] Paul Beame, Stephen Cook, Jeff Edmonds, Russell Impagliazzo, and Toniann Pitassi. 1998. The Relative Complexity of NP Search Problems. *J. Comput. System Sci.* 57, 1 (1998), 3 – 19.
[5] P. Beame, R. Impagliazzo, J. Krajicek, T. Pitassi, and P. Pudlak. 1994. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 794–806.
[6] Paul Beame and Toniann Pitassi. 1996. An Exponential Separation between the Parity Principle and the Pigeonhole Principle. *Ann. Pure Appl. Log.* 80 (10 1996), 195–228.
[7] Arnold Beckmann and Sam Buss. 2019. On transformations of constant depth propositional proofs. *Ann. Pure Appl. Log.* 170, 10 (2019), 1176–1187.
[8] Maria Luisa Bonet, Sam Buss, Alexey Ignatiev, João Marques-Silva, and António Morgado. 2018. MaxSAT Resolution With the Dual Rail Encoding. In *AAAI*. 6565–6572.
[9] Maria Luisa Bonet, Sam Buss, Alexey Ignatiev, Antonio Morgado, and Joao Marques-Silva. 2021. Propositional proof systems based on maximum satisfiability. *Artificial Intelligence* 300 (2021), 103552.
[10] Maria Luisa Bonet and Jordi Levy. 2020. Equivalence Between Systems Stronger Than Resolution. In *Theory and Applications of Satisfiability Testing – SAT 2020*. Springer International Publishing, Cham, 166–181.
[11] Samuel R. Buss. 1998. Lower bounds on Nullstellensatz proofs via designs. In *Proof complexity and feasible arithmetics (Rutgers, NJ, 1996)*. DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Vol. 39. Amer. Math. Soc., Providence, RI, 59–71.
[12] Stephen A. Cook and Robert A. Reckhow. 1979. The Relative Efficiency of Propositional Proof Systems. *The Journal of Symbolic Logic* 44, 1 (1979), 36–50.
[13] Stefan S. Dantchev, Abdul Ghani, and Barnaby Martin. 2020. Sherali-Adams and the Binary Encoding of Combinatorial Principles. In *LATIN 2020: Theoretical Informatics - 14th Latin American Symposium, São Paulo, Brazil, January 5-8, 2021, Proceedings (Lecture Notes in Computer Science)*, Yoshiharu Kohayakawa and Flávio Keidi Miyazawa (Eds.), Vol. 12118. Springer, 336–347.
[14] Susanna F. de Rezende, Massimo Lauria, Jakob Nordström, and Dmitry Sokolov. 2021. The Power of Negative Reasoning. In *36th Computational Complexity Conference (CCC 2021) (Leibniz International Proceedings in Informatics (LIPIcs))*, Valentine Kabanets (Ed.), Vol. 200. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 40:1–40:24.
[15] Noah Fleming, Stephan Grosser, Mika Göös, and Robert Robere. 2022. On Semi-Algebraic Proofs and Algorithms. *Electron. Colloquium Comput. Complex.* (2022), TR22–003.
[16] Noah Fleming, Pravesh Kothari, and Toniann Pitassi. 2019. Semialgebraic Proofs and Efficient Algorithm Design. *Foundations and Trends® in Theoretical Computer Science* 14, 1-2 (2019), 1–221.
[17] Mika Göös, Alexandros Hollender, Siddhartha Jain, Gilbert Maystre, William Pires, Robert Robere, and Ran Tao. 2022. Separations in Proof Complexity and TFNP. *CoRR* abs/2205.02168 (2022). https://doi.org/10.48550/arXiv.2205.02168 arXiv:2205.02168
[18] Tuomas Hakoniemi. 2021. Monomial size vs. Bit-complexity in Sums-of-Squares and Polynomial Calculus. In *36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, Rome, Italy, June 29 - July 2, 2021*. IEEE, 1–7.
[19] Russell Impagliazzo and Nathan Segerlind. 2006. Constant-Depth Frege Systems with Counting Axioms Polynomially Simulate Nullstellensatz Refutations. *ACM Trans. Comput. Logic* 7, 2 (April 2006), 199–218.
[20] Jan Krajíček. 2019. *Proof Complexity*. Cambridge University Press.
[21] Jan Krajíček, Pavel Pudlák, and Alan Woods. 1995. An exponential lower bound to the size of bounded depth frege proofs of the pigeonhole principle. *Random Structures and Algorithms* 7, 1 (Aug. 1995), 15–39.
[22] Jan Krajiček. 1994. Lower Bounds to the Size of Constant-Depth Propositional Proofs. *The Journal of Symbolic Logic* 59, 1 (1994), 73–86.
[23] Javier Larrosa and Emma Rollon. 2020. Augmenting the Power of (Partial) MaxSat Resolution with Extension. *Proceedings of the AAAI Conference on Artificial Intelligence* 34, 02 (Apr. 2020), 1561–1568.
[24] Javier Larrosa and Emma Rollon. 2020. Towards a Better Understanding of (Partial Weighted) MaxSAT Proof Systems. In *Theory and Applications of Satisfiability Testing – SAT 2020*, Luca Pulina and Martina Seidl (Eds.). Springer International Publishing, Cham, 218–232.
[25] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. 1993. Exponential lower bounds for the pigeonhole principle. *Computational Complexity* 3, 2 (Jun 1993), 97–140.
[26] Toniann Pitassi and Robert Robere. 2017. Strongly Exponential Lower Bounds for Monotone Computation. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2017)*. Association for Computing Machinery, New York, NY, USA, 1246–1255.
[27] Toniann Pitassi and Robert Robere. 2018. Lifting Nullstellensatz to Monotone Span Programs over Any Field. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2018)*. Association for Computing Machinery, New York, NY, USA, 1207–1219.
[28] Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A. Cook. 2016. Exponential Lower Bounds for Monotone Span Programs. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*. 406–415.
[29] Hanif D. Sherali and Warren P. Adams. 1990. A Hierarchy of Relaxations between the Continuous and Convex Hull Representations for Zero-One Programming Problems. *SIAM Journal on Discrete Mathematics* 3, 3 (1990), 411–430.
[30] Alasdair Urquhart and Xudong Fu. 1996. Simplified Lower Bounds for Propositional Proofs. *Notre Dame Journal of Formal Logic* 37, 4 (1996), 523–544.