# Sherali-Adams and the binary encoding of combinatorial principles

Stefan Dantchev[1], Abdul Ghani[1], and Barnaby Martin[1]

Department of Computer Science, Durham University, U.K.

**Abstract.** We consider the Sherali-Adams (SA) refutation system together with the unusual *binary* encoding of certain combinatorial principles. For the unary encoding of the Pigeonhole Principle and the Least Number Principle, it is known that linear rank is required for refutations in SA, although both admit refutations of polynomial size. We prove that the binary encoding of the Pigeonhole Principle requires exponentially-sized SA refutations, whereas the binary encoding of the Least Number Principle admits logarithmic rank, polynomially-sized SA refutations. We continue by considering a refutation system between SA and Lasserre (Sum-of-Squares). In this system, the unary encoding of the Least Number Principle requires linear rank while the unary encoding of the Pigeonhole Principle becomes constant rank.

**Keywords:** Proof Complexity · Lift-and-Project Methods · Binary encoding

## 1 Introduction

It is well-known that questions on the satisfiability of propositional CNF formulae may be reduced to questions on feasible solutions for certain Integer Linear Programs (ILPs). In light of this, several ILP-based proof (more accurately, refutation) systems have been suggested for propositional CNF formulae, based on proving that the relevant ILP has no solutions. Typically, this is accomplished by relaxing an ILP to a continuous Linear Program (LP), which itself may have (non-integral) solutions, and then modifying this LP iteratively until it has a solution iff the original ILP had a solution (which happens at the point the LP has no solution). Among the most popular ILP-based refutation systems are Cutting Planes [11, 6] and several proposed by Lovász and Schrijver [18].

Another method for solving ILPs was proposed by Sherali and Adams [22], and was introduced as a propositional refutation system in [7]. Since then it has been considered as a refutation system in the further works [9, 1]. The Sherali-Adams system (SA) is of significant interest as a static variant of the Lovász-Schrijver system without semidefinite cuts (LS). It is proved in [15] that the SA rank of a polytope is less than or equal to its LS rank; hence we may claim that SA is at least as strong as LS (though it is unclear whether it is strictly stronger).

Various fundamental combinatorial principles used in Proof Complexity may be given in first-order logic as sentences $\varphi$ with no finite models and in this article we will restrict attention to those in $\Pi_2$-form. Riis discusses in [21] how to generate from prenex $\varphi$ a family of CNFs, the $n$th of which encodes that $\varphi$ has a model of size $n$, which are hence contradictions. Following Riis, it is typical to encode the existence of the witnesses to an existentially quantified variable in longhand with a big disjunction, of the form $S_{\mathbf{a},1} \vee \ldots \vee S_{\mathbf{a},n}$, that we designate the *unary encoding*. Here the arity of $\mathbf{a}$ is the number of universally quantified variables preceding the existentially quantified variable, on which it might depend.

As recently investigated in the works [10, 3, 4, 17, 13, 8], it may also be possible to encode the existence of such witnesses *succinctly* by the use of a *binary encoding*. Essentially, the existence of the witness is now given implicitly as any propositional assignment to the relevant variables $S_{\mathbf{a},1}, \ldots, S_{\mathbf{a},\log n}$, which we call $S$ for Skolem, gives a witness; whereas in the unary encoding a solitary true literal tells us which is the witness. Combinatorial principles encoded in binary are interesting to study for Resolution-type systems since they still preserve the hardness of the combinatorial principle while giving a more succinct propositional representation. In certain cases this leads to obtain significant lower bounds in an easier way than for the unary case [10, 4, 17, 8].

The binary encoding also implicitly enforces an at-most-one constraint at the same time as it does at-least-one. When some big disjunction $S_{\mathbf{a},1} \vee \ldots \vee S_{\mathbf{a},n}$ of the unary encoding is translated to constraints for an ILP it enforces $S_{\mathbf{a},1} + \ldots + S_{\mathbf{a},n} \geq 1$. Were we to insist that $S_{\mathbf{a},1} + \ldots + S_{\mathbf{a},n} = 1$ then we encode immediately also the at-most-one constraint. We paraphrase this variant as being (the unary) *encoding with equalities* or "SA-with-equalities".

The Pigeonhole Principle (PHP), which essentially asserts that $n$ pigeons may not be assigned to $n-1$ holes such that no hole has more than one pigeon, and the Least Number Principle (LNP), which asserts that a partially-ordered $n$-set possesses a minimal element, are ubiquitous in Proof Complexity. Typically (and henceforth) we work under the same name with their negations, which are expressible in ($\Pi_2$) first-order logic as formulae with no finite models.

In [9] we have proved that the SA rank of (the polytopes associated with) (the unary encoding of) each of the Pigeonhole Principle and Least Number Principles is $n-2$ (where $n$ is the number of pigeons and elements in the poset, respectively). It is known that SA polynomially simulates Resolution (see e.g. [9]) and it follows there is a polynomially-sized refutation in SA of the Least Number Principle. That there is a polynomially-sized refutation in SA of the Pigeonhole Principle is noted in [20].

In this paper we consider the binary encodings of the Pigeonhole Principle and the Least Number Principle as ILPs. We additionally consider their (unary) encoding with equalities. We first prove that the binary encoding of the Pigeonhole Principle requires exponential size in SA. We then prove that the (unary) encoding of the Least Number Principle with equalities has SA rank 2 and polynomial size. This allows us to prove that the binary encoding of the Least Number Principle has SA rank at most $2 \log n$ and polynomial size.

The divergent behaviour of these two combinatorial principles is tantalising – while the Least Number Principle becomes easier for SA in the binary encoding (in terms of rank), the Pigeonhole Principle becomes harder (in terms of size). Such variable behaviour has been observed for the Pigeonhole Principle in Resolution, where the binary encoding makes it easier for treelike Resolution (in terms of size) [8].

We continue by considering a refutation system SA+Squares which is between SA and Lasserre (Sum-of-Squares) [14] (see also [15] for comparison between these systems). SA+Squares appears as Static $\mathrm{LS}_+$ in [12]. In this system one can always assume the non-negativity of (the linearisation of) any squared polynomial. In contrast to our system SA-with-equalities, we see that the rank of the unary encoding of the Pigeonhole Principle is 2, while the rank of the Least Number Principle is linear. We prove this by showing a certain moment matrix in positive semidefinite. Our rank results for the unary encoding can be contrasted in Table 1. Owing to space restrictions, many of our proofs are omitted.

| unary case | SA | SA-with-equalities | SA+Squares |
|---|---|---|---|
| PHP | linear | linear | constant |
| LNP | linear | constant | linear |

| binary case | SA |
|---|---|
| PHP | exponential |
| LNP | polynomial |

| unary case | SA | SA-with-equalities | SA+Squares |
|---|---|---|---|
| PHP | [9] | ([9]) | Theorem 4 ([12]) |
| LNP | [9] | Theorem 3 | Theorem 5 |

| binary case | SA |
|---|---|
| PHP | Theorem 2 |
| LNP | Corollary 2 |

**Table 1.** Rank based complexity for the unary encoding in different systems (on the left) and size based complexity for the binary encoding (on the right). The lower table shows where the corresponding result is proved.

## 2 Preliminaries

Let $[m]$ be the set $\{1, \ldots, m\}$. Let us assume, without loss of much generality, that $n$ is a power of 2. Cases where $n$ is not a power of 2 are handled in the binary encoding by explicitly forbidding possibilities.

If $P$ is a propositional variable, then $P^0 = \overline{P}$ indicates the negation of $P$, while $P^1$ indicates $P$. A *term* is a conjunction of propositional literals.

From a CNF formula $F := C_1 \wedge \ldots \wedge C_r$ in variables $v_1, \ldots, v_m$ we generate an ILP in $2m$ variables $Z_{v_\lambda}, Z_{\neg v_\lambda}$ $(\lambda \in [m])$. For literals $l_1, \ldots, l_t$ s.t. $(l_1 \vee \ldots \vee l_t)$ is a clause of $F$ we have the constraining inequality

$$(2.1) \quad Z_{l_1} + \ldots + Z_{l_t} \geq 1.$$

We also have, for each $\lambda \in [m]$, the equalities of negation

$$(2.2) \quad Z_{v_\lambda} + Z_{\neg v_\lambda} = 1$$

together with the bounding inequalities

$$(2.3) \quad 0 \leq Z_{v_\lambda} \leq 1 \quad \text{and} \quad 0 \leq Z_{\neg v_\lambda} \leq 1.$$

Let $\mathcal{P}_0^F$ be the polytope specified by these constraints on the real numbers. It is clear that this polytope contains integral points iff the formula $F$ is satisfiable. In general, $\mathcal{P}_0^F$ is non-empty; in fact, if $F$ is a contradiction that does not admit refutation by unit clause propagation, this is the case (we may use unit clause propagation to assign $0-1$ values to some variables, thereafter assigning $1/2$ to those variables remaining). Note that it follows that any unsatisfiable Horn CNF $F$ (i.e., where each clause contains at most one positive variable) has SA rank 0, since $F$ must then admit refutation by unit clause propagation (which may be used to demonstrate $\mathcal{P}_0^F$ empty).

Sherali-Adams (SA) provides a static refutation method that takes the polytope $\mathcal{P}_0^F$ defined by (2.1) – (2.3) and *r-lifts* it to another polytope $\mathcal{P}_r^F$ in $\sum_{\lambda=0}^{r+1} \binom{2m}{\lambda}$ dimensions. Specifically, the variables involved in defining the polytope $\mathcal{P}_r^F$ are $Z_{l_1 \wedge \ldots \wedge l_{r+1}}$ ($l_1, \ldots, l_{r+1}$ literals of $F$) and $Z_\emptyset$. Let us say that the term $Z_{l_1 \wedge \ldots \wedge l_{r+1}}$ has *rank* $r$. Note that we accept commutativity and idempotence of the $\wedge$-operator, e.g. $Z_{l_1 \wedge l_2} = Z_{l_2 \wedge l_1}$ and $Z_{l_1 \wedge l_1} = Z_{l_1}$. Also $\emptyset$ represents the empty conjunct (boolean true); hence we set $Z_\emptyset := 1$. For literals $l_1, \ldots, l_t$, s.t. $(l_1 \vee \ldots \vee l_t)$ is a clause of $F$, we have the constraining inequalities

$$(2.1') \quad Z_{l_1 \wedge D} + \ldots + Z_{l_t \wedge D} \geq Z_D,$$

for $D$ any conjunction of at most $r$ literals of $F$. We also have, for each $\lambda \in [m]$ and $D$ any conjunction of at most $r$ literals, the equalities of negation

$$(2.2') \quad Z_{v_\lambda \wedge D} + Z_{\neg v_\lambda \wedge D} = Z_D$$

together with the bounding inequalities

$$(2.3') \quad 0 \leq Z_{v_\lambda \wedge D} \leq Z_D \quad \text{and} \quad 0 \leq Z_{\neg v_\lambda \wedge D} \leq Z_D.$$

For $r' \leq r$, the defining inequalities of $\mathcal{P}_{r'}^F$ are consequent on those of $\mathcal{P}_r^F$. Equivalently, any solution to the inequalities of $\mathcal{P}_r^F$ gives rise to solutions of the inequalities of $\mathcal{P}_{r'}^F$, when projected on to its variables. If $D'$ is a conjunction of $r'$ literals, then $Z_{D \wedge D'} \leq Z_D$ follows by transitivity from $r'$ instances of (2.3′). We refer to the property $Z_{D \wedge D'} \leq Z_D$ as *monotonicity*. Finally, let us note that $Z_{v \wedge \neg v} = 0$ holds in $\mathcal{P}_1^F$ and follows from a single lift of an equality of negation.

The SA *rank* of the polytope $\mathcal{P}_0^F$ (formula $F$) is the minimal $i$ such that $\mathcal{P}_i^F$ is empty. Thus, the notation rank is overloaded in a consistent way, since $\mathcal{P}_i^F$ is specified by inequalities in variables of rank at most $i$. The largest $r$ for which $\mathcal{P}_r^F$ need be considered is $2m-1$, since beyond that there are no new literals to lift by. Even that is somewhat further than necessary, largely because, if the conjunction $D$ contains both a variable and its negation, it may be seen from the equalities of negation that $Z_D = 0$. In fact, it follows from [15] that the SA rank of $\mathcal{P}_0^F$ is always $\leq m-1$ (for a contradiction $F$).

The number of defining inequalities of the polytope $\mathcal{P}_r^F$ is exponential in $r$; hence a naive measure of SA size would see it grow more than exponentially in rank. However, not all of the inequalities $(2.1') - (2.3')$ may be needed to specify the empty polytope. We therefore define the SA *size* of the polytope $\mathcal{P}_0^F$ (formula $F$) to be the size (of an encoding) of a minimal subset of the inequalities $(2.1') - (2.3')$ of $\mathcal{P}_{2m}^F$ that specifies the empty polytope.

Let us now consider principles which are expressible as first-order formulae, with no finite models, in $\Pi_2$-form, i.e. as $\forall\vec{x}\exists\vec{w}\varphi(\vec{x},\vec{w})$ where $\varphi(\vec{x},\vec{w})$ is a formula built on a family of relations $\vec{R}$. For example the *Least Number Principle*, which states that a finite partial order has a minimal element is one of such principles. Its negation can be expressed in $\Pi_2$-form as:

$$\forall x,y,z\exists w\ \neg R(x,x) \wedge (R(x,y) \wedge R(y,z) \rightarrow R(x,z)) \wedge R(x,w).$$

This can be translated into a unsatisfiable CNF using a unary encoding of the witness, as shown below alongside the binary encoding.

| $\mathrm{LNP}_n$ : <u>*Unary encoding*</u> | | $\mathrm{LNP}_n$ : <u>*Binary encoding*</u> | |
|---|---|---|---|
| $\overline{P}_{i,i}$ | $\forall i \in [n]$ | $\overline{P}_{i,i}$ | $\forall x \in [n]$ |
| $\overline{P}_{i,j} \vee \overline{P}_{j,k} \vee P_{i,k}$ | $\forall i,j,k \in [n]$ | $\overline{P}_{i,j} \vee \overline{P}_{j,k} \vee P_{i,k}$ | $\forall i,j,k \in [n]$ |
| $\overline{S}_{i,j} \vee P_{i,j}$ | $\forall i,j \in [n]$ | $\bigvee_{i\in[\log n]} S_{i,j}^{1-a_i} \vee P_{j,a}$ | $\forall j,a \in [n]$ |
| $\bigvee_{i\in[n]} S_{i,j}$ | $\forall j \in [n]$ | where $a_1 \dots a_{\log n} = \mathrm{bin}(a)$ | |

Note that we placed the witness in the Skolem variables $S_{i,x}$ as the first argument and not the second, as we had in the introduction. This is to be consistent with the $P_{i,j}$ and the standard formulation of LNP as the least, and not greatest, number principle. A more traditional form of the (unary encoding of the) $\mathrm{LNP}_n$ has clauses $\bigvee_{i\in[n]} P_{i,j}$ which are consequent on $\bigvee_{i\in[n]} S_{i,j}$ and $\overline{S}_{i,j} \vee P_{i,j}$ (for all $i \in [n]$).

Indeed, one can see how to generate a binary encoding of C from any combinatorial principle C expressible as a first order formula in $\Pi_2$-form with no finite models. Exact details can be found in definition 4 in [8].

As a second example we consider the *Pigeonhole Principle* which states that a total mapping from $[m]$ to $[n]$ has necessarily a collision when $m$ and $n$ are integers with $m > n$. The negation of its relational form for $m = n+1$ can be expressed as a $\Pi_2$-formula as

$$\forall x,y,z\exists w\ \neg R(x,0) \wedge (R(x,z) \wedge R(y,z) \rightarrow x = y) \wedge R(x,w)$$

where 0 represents the object that is among the $[n+1]$ but not among the $[n]$. Its usual unary and binary propositional encoding are:

$$\text{PHP}^m_n : \underline{\textit{Unary encoding}}$$
$$\bigvee_{j=1}^{n} P_{i,j} \qquad \forall i \in [m]$$
$$\overline{P}_{i,j} \vee \overline{P}_{i',j} \qquad \forall i \neq i' \in [m], j \in [n]$$

$$\text{PHP}^m_n : \underline{\textit{Binary encoding}}$$
$$\bigvee_{j=1}^{\log n} P_{i,j}^{1-a_j} \vee \bigvee_{j=1}^{\log n} P_{i',j}^{1-a_j}$$
$$\forall a \in [n], i \neq i' \in [m]$$
$$\text{where } a_1 \dots a_{\log n} = \text{bin}(a)$$

where 0 no longer appears now $m$ and $n$ are explicit. Properly, the Pigeonhole Principle should also admit $S$ variables (as with the LNP) but one notices that the existential witness $w$ to the type *pigeon* is of the distinct type *hole*. Furthermore, pigeons only appear on the left-hand side of atoms $R(x, z)$ and holes only appear on the right-hand side. For the Least Number Principle instead, the transitivity axioms effectively enforce the type of $y$ appears on both the left- and right-hand side of atoms $R(x, z)$. This accounts for why, in the case of the Pigeonhole Principle, we did not need to introduce any new variables to give the binary encoding, yet for the Least Number Principle a new variable $S$ appears. However, our results would hold equally were we to have chosen the more complicated form of the Pigeonhole Principle. Note that our formulation of the Least Number Principle is symmetric in the elements and our formulation of the Pigeonhole Principle is symmetric in each of the pigeons and holes.

When we consider the Sherali-Adams $r$-lifts of, e.g., the Least Number Principle, we will identify terms of the form $Z_{P_{i,j} \wedge \overline{S}_{i',j'} \wedge \dots}$ as $P_{i,j}\overline{S}_{i',j'} \dots$. Thus, we take the subscript and use overline for negation and concatenation for conjunction. This prefigures the multilinear notation we will revert to in Section 5, but one should view for now $P_{i,j}\overline{S}_{i',j'} \dots$ as a single variable and not a multilinear monomial.

Finally, we wish to discuss the encoding of the Least Number Principle and Pigeonhole Principle as ILPs *with equality*. For this, we take the unary encoding but instead of translating the wide clauses (e.g. from the LNP) from $\bigvee_{i \in [n]} S_{i,x}$ to $S_{1,x} + \dots + S_{n,x} \geq 1$, we instead use $S_{1,x} + \dots + S_{n,x} = 1$. This makes the constraint at-least-one into exactly-one (which is a priori enforced in the binary encoding). A reader who doesn't wish to consult the long version of this paper should consider the Least Number Principle as the combinatorial principle of the following lemma.

**Lemma 1.** *Let* C *be any combinatorial principle expressible as a first order formula in* $\Pi_2$*-form with no finite models. Suppose the unary encoding of* C *with equalities has an* SA *refutation of rank* $r$ *and size* $s$*. Then the binary encoding of* C *has an* SA *refutation of rank at most* $r \log n$ *and size at most* $s$*.*

*Proof.* We take the SA refutation of the unary encoding of C with equalities of rank $r$, in the form of a set of inequalities, and build an SA refutation of the binary encoding of C of rank $r \log n$, by substituting terms $S_{x,a}$ in the former with $S_{x,1}^{a_1} \dots S_{x,\log n}^{a_{\log n}}$, where $a_1 \dots a_{\log n} = \text{bin}(a)$, in the latter. Note that the equalities of the form

$$\sum_{a_1 \dots a_{\log n} = \mathrm{bin}(a)} S_{x,1}^{a_1} \cdots S_{x,\log n}^{a_{\log n}} = 1$$

follow from the inequalities (2.2') and (2.3'). Further, inequalities of the form $S_{x,1}^{a_1} \dots S_{x,\log n}^{a_{\log n}} \leq P_{x,a}$ follow since $S_{x,j}\overline{S}_{x,j} = 0$ for each $j \in [\log n]$.

## 3 The lower bound for the binary Pigeonhole Principle

In this section we study the inequalities derived from the binary encoding of the Pigeonhole principle. We first prove a certain SA rank lower bound for a version of the binary PHP, in which only a subset of the holes is available.

**Lemma 2.** *Let $H \subseteq [n]$ be a subset of the holes and let us consider binary $\mathrm{PHP}^m_{|H|}$ where each pigeon can go to a hole in $H$ only. Any* SA *refutation of binary $\mathrm{PHP}^m_{|H|}$ involves a term that mentions at least $|H|$ pigeons.*

The proof of the size lower bound for the binary $\mathrm{PHP}^{n+1}_n$ then is by a standard random-restriction argument combined with the rank lower bound above. Assume w.l.o.g that $n$ is a perfect power of two. For the random restrictions $\mathcal{R}$, we consider the pigeons one by one and with probability $1/4$ we assign the pigeon uniformly at random to one of the holes still available. We first need to show that the restriction is "good" w.h.p., i.e. neither too big nor too small. The former is needed so that in the restricted version we have a good lower bound, while the latter will be needed to show that a good restriction coincides well any reasonably big term, in the sense that they have in common a sufficiency of pigeons. A simple application of a Chernoff bound gives the following

**Fact 1** *If $|\mathcal{R}|$ is the number of pigeons (or holes) assigned by $\mathcal{R}$,*

1. *the probability that $|\mathcal{R}| < \frac{n}{8}$ is at most $e^{-n/32}$, and*
2. *the probability that $|\mathcal{R}| > \frac{3n}{8}$ is at most $e^{-n/48}$.*

So, from now on, we assume that $\frac{n}{8} \leq |\mathcal{R}| \leq \frac{3n}{8}$. We first prove that a given wide term, i.e. a term that mentions a constant fraction of the pigeons, survives the random restrictions with exponentially small probability.

**Lemma 3.** *Let $T$ be a term that mentions at least $\frac{n}{2}$ pigeons. The probability that $T$ does not evaluate to zero under the random restrictions is at most $\left(\frac{5}{6}\right)^{n/16}$.*

*Proof.* An application of a Chernoff bound gives the probability that fewer than $\frac{n}{16}$ pigeons mentioned by $T$ are assigned by $\mathcal{R}$ is at most $e^{-n/64}$. For each of these pigeons the probability that a single bit-variable in $T$ belonging to the pigeon is set by $\mathcal{R}$ to zero is at least $\frac{1}{5}$. This is because when $\mathcal{R}$ sets the pigeon, and thus the bit-variable, there were at least $\frac{5n}{8}$ holes available, while at most $\frac{n}{2}$ choices set the bit-variable to one. The difference is $\frac{n}{8}$ which divided by $\frac{5n}{8}$ gives $\frac{1}{5}$. Thus $T$ survives under $\mathcal{R}$ with probability at most $e^{-n/64} + \left(\frac{4}{5}\right)^{n/16} < \left(\frac{5}{6}\right)^{n/16}$.

Finally, we can prove that

**Theorem 2.** *Any* SA *refutation of the binary* $\mathrm{PHP}_n^{n+1}$ *has to contain at least* $\left(\frac{6}{5}\right)^{n/16} - 1$ *terms.*

We now consider the so-called weak binary PHP, $\mathrm{PHP}_n^m$, where $m$ is potentially much larger than $n$. The weak unary $\mathrm{PHP}_n^m$ is interesting because it admits (significantly) subexponential-in-$n$ refutations in Resolution when $m$ is sufficiently large [5]. It follows that this size upper bound is mirrored in SA. However, as proved in [8], the weak binary $\mathrm{PHP}_n^m$ remains almost-exponential-in-$n$ for minimal refutations in Resolution. We will see here that the weak binary $\mathrm{PHP}_n^m$ remains almost-exponential-in-$n$ for minimally sized refutations in SA. In this weak binary case, the random restrictions $\mathcal{R}$ above do not work, so we apply quite different restrictions $\mathcal{R}'$ that are as follows: for each pigeon select independently a single bit uniformly at random and set it to 0 or 1 with probability of $1/2$ each.

We can easily prove the following

**Lemma 4.** *A term* $T$ *that mentions* $n'$ *pigeons does not evaluate to zero under* $\mathcal{R}'$ *with probability at most* $e^{-n'/2\log n}$.

*Proof.* For each pigeon mentioned in $T$, the probability that the bit-variable present in $T$ is set by the random restriction is $\frac{1}{\log n}$, and if so, the probability that the bit-variable evaluates to zero is $\frac{1}{2}$. Since this happens independently for all $n'$ mentioned pigeons, the probability that they all survive is at most $\left(1 - \frac{1}{2\log n}\right)^{n'}$.

Now, we only need to prove that in the restricted version of the pigeon-hole principle, there is always a big enough term.

**Lemma 5.** *The probability that an* SA *refutation of the binary* $\mathrm{PHP}_n^m$*, for* $m > n$*, after* $\mathcal{R}'$ *does not contain a term mentioning* $\frac{n}{2\log n}$ *pigeons is at most* $e^{-n/32\log^2 n}$.

We now proceed as in the proof of Theorem 2 to deduce that any SA refutation of the binary $\mathrm{PHP}_n^m$ must have size exponential in $n$.

**Corollary 1.** *Any* SA *refutation of the binary* $\mathrm{PHP}_n^m$*,* $m > n$*, has to contain at least* $e^{n/32\log^2 n}$ *terms.*

*Proof.* Assume for a contradiction, that there is a refutation with fewer terms of rank at most $\frac{n}{2\log n}$. By lemma 4 and a union-bound, there is a specific restriction that evaluates all these terms to zero. However, this contradicts lemma 5 .

## 4 The Least Number Principle with equality

Recall that the unary *Least Number Principle (*$\mathrm{LNP}_n$*) with equality* has the following set of SA axioms:

$$\begin{gathered}
\mathit{self} : P_{i,i} = 0 \quad \forall\, i \in n \\
\mathit{trans} : P_{i,k} - P_{i,j} - P_{j,k} + 1 \geq 0 \quad \forall\, i,j,k \in [n] \\
\mathit{impl} : P_{i,j} - S_{i,j} \geq 0 \quad \forall\, i,j \in [n] \\
\mathit{lower} : \textstyle\sum_{i \in [n]} S_{i,j} - 1 = 0 \quad \forall\, j \in [n]
\end{gathered}$$

Strictly speaking Sherali-Adams is defined for inequalities only. An equality axiom $a = 0$ is simulated by the two inequalities $a \geq 0, -a \geq 0$, which we refer to as the *positive* and *negative* instances of that axiom, respectively. Also, note that we have used $P_{i,j} + \overline{P}_{i,j} = 1$ to derive this formulation. We call two terms *isomorphic* if one term can be gotten from the other by relabelling the indices appearing in the subscripts by a permutation.

**Theorem 3.** *For $n$ large enough, the* SA *rank of the* $\mathrm{LNP}_n$ *with equality is at most* 2 *and* SA *size at most polynomial in $n$.*

**Corollary 2.** *The binary encoding of* $\mathrm{LNP}_n$ *has* SA *rank at most* $2 \log n$ *and* SA *size at most polynomial in $n$.*

*Proof.* Immediate from Lemma 1.

## 5 SA+Squares

In this section we consider a proof system, SA+Squares, based on inequalities of multilinear polynomials. We now consider axioms as degree-1 polynomials in some set of variables and refutations as polynomials in those same variables. Then this system is gotten from SA by allowing addition of (linearised) squares of polynomials. In terms of strength this system will be strictly stronger than SA and at most as strong as Lasserre (also known as Sum-of-Squares), although we do not at this point see an exponential separation between SA+Squares and Lasserre. See [14, 15, 2] for more on the Lasserre proof system and [16] for tight degree lower bound results.

Consider the polynomial $S_{i,j}P_{i,j} - S_{i,j}P_{i,k}$. The square of this is

$$S_{i,j}P_{i,j}S_{i,j}P_{i,j} + S_{i,j}P_{i,k}S_{i,j}P_{i,k} - 2S_{i,j}P_{i,j}S_{i,j}P_{i,k}.$$

Using idempotence this linearises to $S_{i,j}P_{i,j} + S_{i,j}P_{i,k} - 2S_{i,j}P_{i,j}P_{i,k}$. Thus we know that this last polynomial is non-negative for all 0/1 settings of the variables. A *degree-d* SA+Squares refutation of a set of linear inequalities (over terms) $q_1 \geq 0, \ldots, q_x \geq 0$ is an equation of the form

$$-1 = \sum_{i=1}^{x} p_i q_i + \sum_{i=1}^{y} r_i^2 \tag{1}$$

where the $p_i$ are polynomials with nonnegative coefficients and the degree of the polynomials $p_i q_i, r_i^2$ is at most $d$. We want to underline that we now consider a term like $S_{i,j}P_{i,j}P_{i,k}$ as a product of its constituent variables. This is opposed to the preceding sections in which we viewed it as a single variable $Z_{S_{i,j}P_{i,j}P_{i,k}}$. The translation from the degree discussed here to SA rank previously introduced may be paraphrased by "rank = degree − 1".

We show that the unary PHP becomes easy in this stronger proof system while the LNP remains hard. The following appears as Example 2.1 in [12].

**Theorem 4 ([12]).** *The unary* $\mathrm{PHP}_n^{n+1}$ *has an* SA + Squares *refutation of degree 2.*

We give our lower bound for the unary $\mathrm{LNP}_n$ by producing a linear function $v$ (which we will call a *valuation*) from terms into $\mathbb{R}$ such that

1. for each axiom $p \geq 0$ and every term $X$ with $deg(Xp) \leq d$ we have $v(Xp) \geq 0$, and
2. we have $v(r^2) \geq 0$ whenever $deg(r^2) \leq d$.
3. $v(1) = 1$.

The existence of such a valuation clearly implies that a degree-$d$ SA+Squares refutation cannot exist, as it would result in a contradiction when applied to both sides of eq. (1).
To verify that $v(r^2) \geq 0$ whenever $deg(r^2) \leq d$ we show that the so-called *moment-matrix* $\mathcal{M}_v$ is positive semidefinite. The degree-$d$ moment matrix is defined to be the symmetric square matrix whose rows and columns are indexed by terms of size at most $d/2$ and each entry is the valuation of the product of the two terms indexing that entry. Given any polynomial $\sigma$ of degree at most $d/2$ let $c$ be its coefficient vector. Then if $\mathcal{M}_v$ is positive semidefinite:

$$v(\sigma^2) = \sum_{deg(T_1), deg(T_2) \leq d/2} c(T_1)c(T_2)v(T_1T_2) = c^\top \mathcal{M}_v c \geq 0.$$

(For more on this see e.g. [14], section 2.)
Recall that the unary *Least Number Principle (*$\mathrm{LNP}_n$*)* has the set of SA axioms *self*, *trans*, *impl* but where the last axiom *lower* now has the form $\sum_{i\in[n]} S_{i,j} - 1 \geq 0$, for all $j \in [n]$.

**Theorem 5.** *There is no* SA + Squares *refutation of the unary* $\mathrm{LNP}_n$ *with degree at most* $(n-3)/2$.

An alternative formulation of the Least Number Principle asks that the order be total, and this is enforced with axioms *anti-sym* of the form $P_{i,j} \vee P_{j,i}$, or $P_{i,j} + P_{j,i} \geq 1$, for $i \neq j \in [n]$. Let us call this alternative formulation TLNP. Ideally, lower bounds should be proved for TLNP, because they are potentially stronger. Conversely, upper bounds are stronger when they are proved on the ordinary LNP, without the total order. Looking into the last proof, one sees that the lifts of *anti-sym* are satisfied as we derive our valuation exclusively from total orders. This is interesting because an upper bound in Lasserre of order $\sqrt{n}$ is known for $\mathrm{TLNP}_n$ [19]. It is proved for a slightly different formulation of $\mathrm{TLNP}_n$ from ours, but we believe it is straightforward to translate it to our formulation. Thus, Theorem 5, together with [19], shows a quadratic rank separation between SA+Squares and Lasserre.

## 6 Conclusion

Our result that the unary encoding of the Least Number Principle with equalities has SA rank 2 contrasts strongly with the fact that the unary encoding of the Least Number Principle has SA rank $n-2$ [9]. Now we know the unary encoding of the Pigeonhole Principle has SA rank $n-2$ also. This leaves one wondering about the unary encoding of the Pigeonhole Principle with equalities, which does appear in Figure 1. In fact, the valuation of [9] witnesses this still has SA rank $n-2$ (and we give the argument in the long version of this paper). That is, the Pigeonhole Principle does not drop complexity in the presence of equalities, whereas the Least Number Principle does.

**Acknowlegements**. We thank Nicola Galesi for collaboration on the binary encoding in Resolution-type systems. In particular, some of our definitions come from joint work with him in [8]. We thank several anonymous reviewers for careful reading of our paper and their insights.

## References

1. Atserias, A., Lauria, M., Nordström, J.: Narrow proofs may be maximally long. ACM Trans. Comput. Log. **17**(3), 19:1–19:30 (2016). https://doi.org/10.1145/2898435, https://doi.org/10.1145/2898435
2. Barak, B., Steurer, D.: Sum-of-squares proofs and the quest toward optimal algorithms. In: Proceedings of International Congress of Mathematicians (ICM). vol. IV, pp. 509–533 (2014)
3. Bonacina, I., Galesi, N.: A framework for space complexity in algebraic proof systems. J. ACM **62**(3), 23:1–23:20 (2015). https://doi.org/10.1145/2699438, http://doi.acm.org/10.1145/2699438
4. Bonacina, I., Galesi, N., Thapen, N.: Total space in resolution. SIAM J. Comput. **45**(5), 1894–1909 (2016). https://doi.org/10.1137/15M1023269, https://doi.org/10.1137/15M1023269
5. Buss, S.R., Pitassi, T.: Resolution and the weak pigeonhole principle. In: Computer Science Logic, 11th International Workshop, CSL '97, Annual Conference of the EACSL, Aarhus, Denmark, August 23-29, 1997, Selected Papers. pp. 149–156 (1997). https://doi.org/10.1007/BFb0028012, http://dx.doi.org/10.1007/BFb0028012
6. Chvátal, V.: Edmonds polytopes and a hierarchy of combinatorial problems. Discrete Math. **4**, 305–337 (1973)
7. Dantchev, S.S.: Rank complexity gap for Lovász-Schrijver and Sherali-Adams proof systems. In: STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing. pp. 311–317. ACM Press, New York, NY, USA (2007). https://doi.org/http://doi.acm.org/10.1145/1250790.1250837

8. Dantchev, S.S., Galesi, N., Martin, B.: Resolution and the binary encoding of combinatorial principles. In: 34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA. pp. 6:1–6:25 (2019). https://doi.org/10.4230/LIPIcs.CCC.2019.6, https://doi.org/10.4230/LIPIcs.CCC.2019.6, see http://arxiv.org/abs/1809.02843
9. Dantchev, S.S., Martin, B., Rhodes, M.N.C.: Tight rank lower bounds for the sherali-adams proof system. Theor. Comput. Sci. **410**(21-23), 2054–2063 (2009). https://doi.org/10.1016/j.tcs.2009.01.002, https://doi.org/10.1016/j.tcs.2009.01.002
10. Filmus, Y., Lauria, M., Nordström, J., Ron-Zewi, N., Thapen, N.: Space complexity in polynomial calculus. SIAM J. Comput. **44**(4), 1119–1153 (2015). https://doi.org/10.1137/120895950, https://doi.org/10.1137/120895950
11. Gomory, R.E.: Solving linear programming problems in integers. In: Bellman, R., Hall, M. (eds.) Combinatorial Analysis, Proceedings of Symposia in Applied Mathematics. vol. 10. Providence, RI (1960)
12. Grigoriev, D., Hirsch, E.A., Pasechnik, D.V.: Complexity of semi-algebraic proofs. In: STACS '02: Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science. pp. 419–430. Springer-Verlag, London, UK (2002)
13. Hrubes, P., Pudlák, P.: Random formulas, monotone circuits, and interpolation. In: Umans, C. (ed.) 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017. pp. 121–131. IEEE Computer Society (2017). https://doi.org/10.1109/FOCS.2017.20, https://doi.org/10.1109/FOCS.2017.20
14. Lasserre, J.B.: An explicit exact sdp relaxation for nonlinear 0-1 programs. In: Aardal, K., Gerards, B. (eds.) Proceedings of the 8th International Conference on Integer Programming and Combinatorial Optimization (IPCO0́1). Lecture Notes in Computer Science, vol. 2081, pp. 293–303. Springer, Berlin, Heidelberg (2001)
15. Laurent, M.: A comparison of the Sherali-Adams, Lovász-Schrijver and Lasserre relaxations for $0-1$ programming. Tech. Rep. PNA–R0108, Amsterdam (2001)
16. Lauria, M., Nordström, J.: Tight size-degree bounds for sums-of-squares proofs. computational complexity **26**(4), 911–948 (Dec 2017). https://doi.org/10.1007/s00037-017-0152-4, https://doi.org/10.1007/s00037-017-0152-4
17. Lauria, M., Pudlák, P., Rödl, V., Thapen, N.: The complexity of proving that a graph is ramsey. Combinatorica **37**(2), 253–268 (2017). https://doi.org/10.1007/s00493-015-3193-9, https://doi.org/10.1007/s00493-015-3193-9
18. Lovász, L., Schrijver, A.: Cones of matrices and set-functions and 0-1 optimization. SIAM J. Optimization **1**(2), 166–190 (1991)
19. Potechin, A.: Sum of squares bounds for the total ordering principle (2018)
20. Rhodes, M.: Rank lower bounds for the Sherali-Adams operator. In: Cooper, S.B., Löwe, B., Sorbi, A. (eds.) CiE. Lecture Notes in Computer Science, vol. 4497, pp. 648–659. Springer (2007)
21. Riis, S.: A complexity gap for tree resolution. Computational Complexity **10**(3), 179–209 (2001)
22. Sherali, H.D., Adams, W.P.: A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. SIAM J. Discrete Math. **3**(3), 411–430 (1990)