DIMACS Series in Discrete Mathematics
and Theoretical Computer Science

Lower Bounds on Nullstellensatz Proofs via Designs

Samuel R. Buss

Abstract. The Nullstellensatz proof system is a proof system for propositional logic based on algebraic identities in fields. Prior work has proved lower bounds of the degree Nullstellensatz refutations using combinatorial constructions called designs. This paper surveys the use of designs for Nullstellensatz lower bounds. We give a new, more general definition of designs. We present an explicit construction of designs which give a linear lower bound on the degree of Nullstellensatz proofs of the housesitting principle. Our designs for the housesitting principle work over any ring.

1. Introduction

The Nullstellensatz proof system is a propositional proof system which establishes the truth of tautologies using reasoning about polynomials over a field, based on the Hilbert Nullstellensatz. The original definition of the Nullstellensatz proof system was by [**2**]. and many of the basic properties of Nullstellensatz proofs can be found in [**3**] and in the survey [**6**]. We begin with a review of the the Nullstellensatz.

In Nullstellensatz refutations, the Boolean values *True* and *False* are identified with the algebraic values 1 and 0 respectively. Boolean operations can be expressed as ring operations; e.g., $\neg x$ is the same as $1 - x$, a conjunction $x \wedge y$ is the same as the product xy, and a disjunction $x \vee y$ is the same as $x + y - xy$. In this way, one converts an arbitrary propositional formula $\varphi(\vec{x})$ into an algebraic term $t(\vec{x})$ such that $\varphi(\vec{x})$ and $t(\vec{x})$ have the same value for all assignments of 0/1 values to the variables $\vec{x}$. We shall always fix some underlying ring R and assume that all algebraic operations occur

1991 *Mathematics Subject Classification.* Primary 03F20, 03B05, 03G99, 68R05.

Key words and phrases. propositional proofs, nullstellensatz, design, housesitting principle.

Supported in part by NSF grant DMS-9503247 and US-Czech Science and Technology grant 93-025.

in that ring. Note that the translation from propositional logic to algebraic expressions works over an arbitrary ring. However, in most interesting cases, the ring is actually a field.

The central difficult computational problem of propositional logic is, given a propositional formula $\varphi(\vec{x})$ with $\vec{x} = x_1, \ldots, x_n$ the variables in φ, to determine if $\varphi(\vec{x})$ is satisfiable. If $t(\vec{x})$ is an algebraic expression which computes the same function as $\varphi(\vec{x})$ for all Boolean inputs, then φ is satisfiable if and only if $t(\vec{a}) = 1$ for some 0/1 assignment of values $\vec{a}$ to the variables $\vec{x}$. If our algebraic structure R is a field, then the formula $x_i^2 - x_i = 0$ is satisfied exactly when x_i is assigned a Boolean value 0 or 1. Therefore φ is unsatisfiable if and only if it is not possible to assign field elements to the variables $\vec{x} = x_1, \ldots, x_n$ which simultaneously satisfy the $n + 1$ equations

$$\begin{aligned} t(\vec{x}) - 1 &= 0 \\ x_i^2 - x_i &= 0 \qquad 1 \leq i \leq n. \end{aligned}$$

If the algebraic structure R is only a ring, it is still true that φ is unsatisfiable if and only if the $n + 1$ equations cannot be simultaneously satisfied in R. However, the statement is harder to prove for rings, since an equation $x^2 - x = 0$ may have many non-0/1 solutions in a ring. However it still holds for rings, since an assignment which satisfies the equations will also satisfy them in the field R/M for M a maximal ideal of R.

It is often convenient to work with terms t that are not obtained from a propositional formula φ by the above canonical method. Further it is often convenient to work with multiple terms instead of a single term t. This leads to the following generalization of the propositional satisfiability problem: given polynomials $t_1, \ldots, t_m$ over a ring R, is there a assignment of 0/1 values to the variables in the terms that makes all the terms simultaneously equal to zero. If R is a field this is equivalent to asking whether the $m + n$ equations

$$\begin{aligned} t_i(\vec{x}) &= 0 \qquad \text{for } i = 1, 2, \ldots, m \\ x_j^2 - x_j &= 0 \qquad \text{for } j = 1, 2, \ldots, n \end{aligned}$$

can be simultaneously satisfied. It is an easy consequence of the Hilbert Nullstellensatz that this question is equivalent to asking whether there are polynomials $F_i(\vec{x})$ and $G_j(\vec{x})$ such that the polynomial identity

$$\begin{aligned} 1 = {} & F_1(\vec{x})t_1(\vec{x}) + F_2(\vec{x})t_2(\vec{x}) + \cdots + F_m(\vec{x})t_m(\vec{x}) + \\ & G_1(\vec{x})(x_1^2 - x_1) + G_2(\vec{x})(x_2^2 - x_2) + \cdots + G_m(\vec{x})(x_n^2 - x_n) \end{aligned} \tag{1}$$

holds in $R[\vec{x}]$.

Definition A *Nullstellensatz refutation* of $t_1, \ldots, t_m$ is a set of polynomials $F_1, \ldots, F_m$, $G_1, \ldots, G_n$ such that the polynomial identity (1) holds. The *degree* of the Nullstellensatz refutation is

$$\max\{deg(F_i) + deg(t_i) \,:\, 1 \leq i \leq m\}.$$

It can be shown that $\max_j\{deg(G_j)+2\} \leq \max_i\{deg(F_i t_i)\}$, and this justifies the fact that the definition of 'degree' does not depend on the degrees of the G_j's.

The purpose of a Nullstellensatz refutation is to prove that the terms $t_1, \ldots, t_m$ cannot be simultaneously satisfied by 0/1 values.

THEOREM 1. *(Soundness of Nullstellensatz) If $t_1, \ldots, t_n$ have a Nullstellensatz refutation, then there is no assignment of 0/1 values to variables that makes $t_1, \ldots, t_n$ simultaneously equal to zero.*

The soundness theorem is readily proven by noting that any assignment of 0/1 values that made each t_i equal to zero would also make each polynomial $x_i^2 - x_i$ equal to zero; but this would contradict the equality (1).

Conversely, the Nullstellensatz proof system is adequate (complete), provided the algebraic structure is a field:

THEOREM 2. *(Completeness of Nullstellensatz refutations). Let the algebraic structure R be a field. Suppose there is no assignment of 0/1 values to variables that makes $t_1, \ldots, t_m$ simultaneously zero. Then $t_1, \ldots, t_n$ have a Nullstellensatz refutation.*

PROOF. Simple proofs of the completeness theorem have been given by [**3, 6**]. Alternatively, the completeness theorem is a simple corollary of the Hilbert Nullstellensatz; namely, if $t_1 = 0, \ldots, t_m = 0$ have no 0/1 satisfying assignment, then there is no solution to these equations plus the n equations $x_i^2 - x_i = 0$, even in the algebraic closure of R. Therefore the Hilbert Nullstellensatz implies the existence of polynomials F_i and G_j over R that satisfy (1). □

When the algebraic structure R is not a field, then the completeness theorem does not always hold in general. However, there are some notable cases in which is does holds; for instance, when the polynomials $\vec{t}$ take only 0/1 values on 0/1 inputs. This fact and some counterexamples are discussed in the appendix to this paper.

2. Designs

2.1. Designs and the degrees of refutations. We are interested in obtaining exact upper and lower bounds on the degrees of Nullstellensatz refutations of particular sets of polynomials. Upper bounds are generally best obtained by explicit construction of Nullstellensatz refutations. For lower bounds, the most useful tool so far has been the use of combinatorial constructions called designs. A general definition of a design, that applies to Nullstellensatz refutations of arbitrary sets of polynomials, is as follows.

Definition Fix an algebraic structure R and a set of polynomials $\mathcal{F} = \{F_i\}_i$. Let $d \geq 0$. A d-design for $\mathcal{F}$ is a mapping D from R-polynomials of degree $\leq d$ to R such that the following conditions hold:

(1): $D(1) = 1$. The polynomial 1 is mapped to the constant 1.

(2): D is linear. So $D(\alpha P) = \alpha D(P)$ and $D(P+Q) = D(P)+D(Q)$, for all $\alpha \in R$ and all R-polynomials P and Q.
(3): $D(Q \cdot F_i) = 0$ for all polynomials $F_i \in \mathcal{F}$ and all polynomials Q such that $deg(F_i) + deg(Q) \leq d$.
(4): $D(x^2 Q) = D(xQ)$ for all variables x and all polynomials Q of degree less than $d-1$.

A d-design is also called a design of degree d.

A *monomial* (sometimes referred to as a *power product*) is an expression of the form $x_1^{a_1} \cdots x_n^{a_n}$. A monomial is *multilinear* if the exponents a_i are all in $\{0,1\}$. A couple of easy observations about designs are:

(a): Since D is linear, D is completely determined by its values $D(Q)$ for all monomials Q.
(b): Likewise by linearity, it suffices that (3) and (4) hold for all *monomials* Q.
(c): The property of D being a d-design is completely independent of D's values on monomials of degree $> d$.
(d): By virtue of (4), the values of D are completely determined by its values on multilinear monomials. Alternatively, we could have included the polynomials $x_j^2 - x_j$ in the set $\mathcal{F}$ and then condition (4) would have been a consequence of (3).

We therefore will frequently find it convenient to define designs by specifying their values only on the multilinear monomials of degree $\leq d$. This viewpoint leads to the construction of designs as combinatorial objects; namely, the multilinear monomials can be viewed as conjunctions of the atomic statements represented by the (propositional) variables in the monomial.

The next theorem provides the basis for using designs to obtain lower bounds on the degrees of Nullstellensatz refutations.

THEOREM 3. *If $\mathcal{F}$ has a d-design, then $\mathcal{F}$ does not have a Nullstellensatz refutation of degree $\leq d$.*

PROOF. Suppose there exists a Nullstellensatz refutation

$$1 \;=\; \sum_i P_i \cdot F_i \;+\; \sum_j Q_j \cdot (x_j^2 - x_j)$$

of degree $\leq d$. Applying D to both sides, we have

$$\begin{aligned} 1 \;=\; D(1) \;&=\; D(\sum_i P_i \cdot F_i + \sum_j Q_j \cdot (x_j^2 - x_j)) \\ &=\; \sum_i D(P_i \cdot F_i) + \sum_j (D(x_j^2 Q_j) - D(x_j Q_j)) \\ &=\; 0 \end{aligned}$$

which is a contradiction. □

A converse to the above theorem also holds:

THEOREM 4. *Suppose the algebraic structure R is a field. If $\mathcal{F}$ does not have a Nullstellensatz refutation of degree d, then there is a d-design for $\mathcal{F}$.*

PROOF. The essential idea of the proof is to restate the question of whether a degree d refutation exists to a problem of finding a solution to a linear programming problem. The question of whether a design exists turns out to be the dual problem. Since it involves only elementary concepts from linear algebra, we give only a sketch of the proof.

Let δ be the number of monomials of degree $\leq d$; i.e., $\delta = \sum_{i=0}^{d} \binom{n+i-1}{i}$. Any polynomial H of degree $\leq d$ can be viewed as a column vector $\mathbf{v}_H$ of dimension δ by letting the entries in the vector equal the coefficients of the the monomials in H. We order the entries so that the last entry of $\mathbf{v}_H$ is the constant term of H.

Let $\mathcal{G}$ be the set of polynomials of the forms $Q \cdot F$ for Q a monomial, for F in $\mathcal{F}$ or of the form $x^2 - x$, and where $deg(QF) \leq d$. Let $\mathbf{v}_1$ be the vector with last entry equal to 1 and all other entries zero. Clearly, there is a Nullstellensatz refutation of degree $\leq d$ if only if the vector $\mathbf{v}_1$ can be expressed as an R-linear combination of the vectors $\mathbf{v}_{G_i}$ for $G_i \in \mathcal{G}$. Letting $\mathbf{M}$ be the $\delta \times |\mathcal{G}|$ matrix which has columns $\mathbf{v}_{G_i}$, this is equivalent to having solution $\mathbf{w}$ to the linear equation

$$\mathbf{M}\,\mathbf{w} = \mathbf{v}_1, \tag{2}$$

where $\mathbf{w}$ is a vector of dimension $|G|$. Let $\mathbf{M}^-$ be the matrix obtained by deleting the last row from $\mathbf{M}$. Since the first $\delta - 1$ entries of $\mathbf{v}_1$ are zero, any solution $\mathbf{w}$ to (2) must be in the nullspace (the kernel) of the mapping $\mathbf{M}^-$. If the last row of $\mathbf{M}$ is in the span of the row vectors of $\mathbf{M}^-$, $\mathbf{M}^-\mathbf{w} = \mathbf{0}$ implies $\mathbf{M}\mathbf{w} = 0$. On the other hand, if the final row is not in their span, then is it possible to find $\mathbf{w}$ satisfying (2). Therefore, there is a Nullstellensatz refutation of degree $\leq d$ if and only if the last row of $\mathbf{M}$ is linearly independent of the rest of the row vectors.

So suppose that the last row of $\mathbf{M}$ is a linear combination of the first $\delta - 1$ rows of $\mathbf{M}$. We must prove that there exists a d-design. Each row in $\mathbf{M}$ corresponds to a monomial Q of degree $\leq d$; we denote that row $\mathbf{u}_Q$. So we have

$$\sum_{deg(Q) \leq d} \alpha_Q \mathbf{u}_Q \;=\; 0,$$

where $\alpha_Q \in R$ and where $\alpha_1 = 1$. Define the design D by letting $D(Q) = \alpha_Q$ for all monomials Q. It is not difficult to check that D is a valid d-design. □

Remark: It is not entirely clear who was the original discoverer of designs. This author first heard about designs for the special case of tautologies expressing mod m tautologies in a communication from P. Pudlák, who certainly knew the corresponding special cases of Theorems 3 and 4. In any event, the next section discusses all the published work known to us.

2.2. Prior constructions of designs. Designs have been used to obtain several degree lower bounds for Nullstellensatz refutations.

First, [**1**] gave designs of degree $\sqrt{n}$ for polynomials which express a version of the pigeonhole principle. This thereby established a $\sqrt{n}$ lower bound on the degree of Nullstellensatz refutations of the pigeonhole principle. It is still open whether this lower bound can be improved substantially, although we conjecture that the correct lower bound is $\Omega(n)$.

Second, [**5**] gave linear degree designs for the housesitting principle over the field $\mathbb{Z}_2$. The housesitting principle is a form of strong induction. We describe the housesitting principle below and give a new construction of designs for the housesitting principle: our construction shows that the designs work over *any* ring R.

Third, [**4**] proved logarithmic upper and lower bounds on the degree of Nullstellensatz proofs of the induction principle. Their proof uses a complicated, explicit construction of designs for the induction principle. A simpler derivation of the degree bounds has very recently been obtained by Clegg and Impagliazzo based on the generation of Gröbner basis for the induction principle polynomials; their method does not explicitly construct the design however.

Recently, [**3**] has given explicit constructions of designs for the mod m matching principles of size n^ϵ. This establishes corresponding lower bounds on the degrees of Nullstellensatz refutations and thereby, using a result from [**2**], gives exponential lower bounds on the size of constant depth Frege proofs of the mod m matching principle in the presence of mod q counting axioms (with q and m relatively prime).

2.3. Designs for the Gröbner proof system? Designs have been an important tool for obtaining lower bounds on the degrees of Nullstellensatz refutations. A generalization of Nullstellensatz proofs, called "Gröbner proof systems," has been recently proposed by Clegg, Edmonds and Impagliazzo [**5**]; so far, no non-trivial degree lower bounds for Gröbner proofs have been obtained. (See also [**3**] for Gröbner proof systems.)

This raises the question of whether designs can be generalized to give degree lower bounds on Gröbner proofs. For this, we define a *Gröbner-design* just as we defined design, but we add an extra condition:

(5): If $D(P) = 0$ and if $\deg(P) + \deg(Q) \leq d$, then $D(Q \cdot P) = 0$.

Of course, with this extra condition present, then conditions (3) (4) can be weakened to state that $D(F_i) = 0$ for all $F_i \in \mathcal{F}$ and that $D(x^2 - x) = 0$ for all variables x.

The following theorem follows easily from the definition of Gröbner designs and the Gröbner proof system:

THEOREM 5. *If there is a Gröbner design of degree d, then there is no Gröbner proof of degree $\leq d$.*

We do not know if the converse to this theorem holds.

3. The Housesitting Principle

The rest of this paper discusses designs for a propositional tautology known as the housesitting principle. The construction of these designs provides a simple, instructive example of the construction of designs.

For the sequel, we let $I = \{0, \ldots, n\}$ and $J = \{1, \ldots, n\}$. For an intuitive picture, we think of J as a linearly ordered set of houses and of I as a set of people who occupy houses. Each person $i \in I$ either stays at home in house i, or housesits for some house $j > i$ for which person j is not at home. Since $0 \notin J$, person 0 must housesit. It is allowed that two people housesit for the same house. The housesitting principle states that these properties cannot be satisfied for all $i \in I$ simultaneously.

The housesitting principle can be viewed as a form of the complete induction principle. That is, let $A(k)$ be the assertion that every person $i \geq n-k$ is at home (i.e., in house i). Then trivially $A(0)$ holds, and it is easy to note that $A(k)$ implies $A(k+1)$. But $A(n)$ is a contradiction since person 0 must housesit some house in J.

Alternatively, the housesitting principle is a form of the infinite descent principle, except that our ordering is reversed so it becomes an infinite *ascent* principle. Namely, let $j_0 = 0$ and let j_{i+1} be the house occupied by person j_i. Then if the housesitting conditions were all met, $j_0, j_1, j_2, \ldots$ would be infinite, strictly increasing sequence of integers less than n.

3.1. The Nullstellensatz formulation. The set of polynomials used to express (the negation of) the housesitting principle in the Nullstellensatz proof setting are constructed as follows.

There are variables $x_{i,j}$, for all $0 \leq i \leq j \leq n$, $1 \leq j$, which intuitively express the condition that person i is in house j (a value of 1 denotes *True* and a value of 0 denotes *False*). There are linear polynomials F_i which state that person i is in some house numbered at least i:

$$F_i \;=\; x_{i,i} + x_{i,i+1} + \cdots + x_{i,n} - 1.$$

There are degree 2 polynomials $F'_{i,j}$, for $i < j$, which state that persons i and j are not both in house j:

$$F'_{i,j} \;=\; x_{i,j}x_{j,j}.$$

Finally there are the usual propositional polynomials, $F''_{i,j} = x_{i,j}^2 - x_{i,j}$.

Let $\mathcal{F}$ be the set of polynomials $\{F_i, F'_{i,j}\}$. Since the polynomials cannot be simultaneously equal to zero under propositional assignments to the variables (since otherwise the housesitting principle would be falsified), there must be a Nullstellensatz refutation of $\mathcal{F}$. We shall construct below an n-design which proves that any Nullstellensatz refutation must have degree at least $n+1$, over an arbitrary ring R.

Actually, we will do a little better: let $F^{(3)}_{i,k,\ell}$ be the polynomials

$$F^{(3)}_{i,k,\ell} \;=\; x_{i,k}x_{i,\ell}$$

for $k \neq \ell$, and let $F^{(4)}_{i,j,k,\ell}$ be the polynomials

$$F^{(4)}_{i,j,k,\ell} \;=\; x_{i,k}x_{j,\ell}$$

for $i < j < k, \ell$ and $k \neq \ell$. If we include these polynomials in $\mathcal{F}$, then the design we construct below is still a valid n-design for the enlarged set of polynomials.[1] Therefore any Nullstellensatz of the enlarged set of polynomials also requires degree $n+1$.

Theorem 3 and the design from Theorem 7 below imply the following lower bound on the degrees of Nullstellensatz refutations:

THEOREM 6. *Let R be an arbitrary ring. Then any Nullstellensatz refutation of the housesitting principle polynomials requires degree $n+1$.*

It is not difficult to see that degree $n+1$ suffices for Nullstellensatz refutations of the housesitting principle, so Theorem 6 is optimal. Clegg, Edmonds and Impagliazzo [**5**] already proved Theorem 6 for $R = \mathbb{Z}_2$.

3.2. Construction of the housesitting designs. As discussed above, it suffices to specify an n-design D by defining its values on multilinear monomials of degree $\leq n$. In our setting, a multilinear monomial is a product of the form

$$T \;=\; x_{i_1,j_1} \cdot x_{i_2,j_2} \cdot \cdots \cdot x_{i_d,j_d}$$

in which no variable occurs more than once. We can identify such a monomial with the conjunction of the propositional assertions, that for $k = 1, \ldots, n$, person i_k is in house j_k. If $i_k = i_\ell$ for some $k \neq \ell$, then this assertion puts some person into two houses: in this case, we will always make $D(T) = 0$. On the other hand, if the person numbers $i_1, \ldots, i_d$ are distinct, then we can also identify the term T with a partial mapping π such that $\pi(i_k) = j_k$ for $k = 1, \ldots, d$. Here, a *partial mapping* π is a mapping with domain a subset of I and range a subset of J. We use T_π to denote the term which is identified with the partial mapping π.

It will therefore suffice to define the values of the design D on terms which correspond to partial mappings. We will identify partial mappings with the terms to which they correspond and therefore can talk about the value, $D(\pi)$, of D on the partial mapping π.

Before we define the designs, we need some definitions and to state some technical conditions. We write $\pi(i)\uparrow$ (respectively, $\pi(i)\downarrow$) to represent the conditions that $\pi(i)$ is undefined (respectively, defined). We write $dom(\pi)$ to denote the domain of π, i.e., the set $\{i : \pi(i)\downarrow\}$. The *partial mapping conditions* are:

(α): For all $i \in dom(\pi)$, $\pi(i) \geq i$.
(β): For all $i \in dom(\pi)$, if $\pi(i) \neq i$, then $\pi(\pi(i))\uparrow$ or $\pi(\pi(i)) \neq \pi(i)$.

[1] This is because our designs will equal zero on terms which do not represent partial mappings or which do not satisfy condition (γ) below.

Note that the housesitting principle states that there is no total π which satisfies (α) and (β) for all values of i. Given a partial mapping π, let $r(\pi)$ be the least value r_0 such that $\pi(r_0)\uparrow$. There are two more partial mapping conditions that we also use:

(γ): Let $i < j$ be in I. Suppose $\pi(i) > j$ and $\pi(j) \neq j$. Then $\pi(i) = \pi(j)$. In particular, if $\pi(i) > j > i$, then $\pi(j)\downarrow$.

(δ): For all $i > r(\pi)$, if $\pi(i)\downarrow$, then $\pi(i) = i$.

The *degree*, $|\pi|$, of a partial mapping π is the cardinality of its domain. The unique partial mapping of degree 0 is denoted $\emptyset$.

Definition We now fix a value for n and we define the design D_n for the housesitting principle. The subscript n is henceforth suppressed and we let D denote D_n. For all π of degree $\leq n$, $D(\pi)$ is defined as follows:

(i): If π does not satisfy the four conditions (α)-(δ), then $D(\pi) = 0$.

(ii): Otherwise, if π does satisfy the four conditions, then let p be the number of $j \leq r(\pi)$ which are *not* in the range of π. Then $D(\pi) = (-1)^p$.

The main result of this section is:

THEOREM 7. *D is a degree n design over $\mathbb{Z}$ (and hence over every ring).*

LEMMA 8. *If $D(\pi) \neq 0$, then $r(\pi) \in range(\pi)$.*

PROOF. (of lemma). Suppose $D(\pi) \neq 0$. Let $r = r(\pi)$. We prove by induction on $i < r$ that

$$\left|\pi^{-1}\{1, \ldots, i\}\right| \ \leq \ i. \tag{3}$$

The base case is trivial of course. To prove the induction step, first note that, by condition (α),

$$\pi^{-1}\{1, \ldots, i\} \subseteq \{0, 1, \ldots, i\}.$$

Thus if $\pi(i) > i$, (3) holds. Otherwise, by (α), we have $\pi(i) = i$. Now, by condition (β), there is no $i' < i$ such that $\pi(i') = i$. So,

$$\pi^{-1}\{1, \ldots, i\} \ = \ \{i\} \cup \pi^{-1}\{1, \ldots, i-1\}.$$

By the induction hypothesis, $|\pi^{-1}\{1, \ldots, i-1\}| \leq i-1$ and thus equation (3) holds.

Now we prove that the $i = r-1$ case of equation (3) immediately implies the lemma. This is because there are r domain values $\leq r-1$, so there is some value $i_0 \leq r-1$ such that $\pi(i_0) \geq r$. By condition (γ) applied to i_0 and r, $\pi(i_0) = r$; hence r is in the range of π. □

A consequence of Lemma 8 and condition (γ) is that if $D(\pi) \neq 0$ and if $i < r$, then $\pi(i) \leq r$.

PROOF. (of theorem). We must establish that D satisfies properties (1)-(4) of being a design. Properties (2) and (4) automatically hold from the way we are defining D in terms of its values on monomials. Property (1) states that $D(1) = 1$: restating this in terms of partial mappings, this means

that $D(\emptyset) = 1$. Now, $r(\emptyset) = 0$, so $D(\emptyset) = 1$ as desired. Property (3) holds for the polynomials $F'_{i,j} \in \mathcal{F}$ because D maps non-partial mappings to 0; i.e., for any monomial T, $D(T \cdot F'_{i,j}) = 0$ since condition (β) is violated when $\pi(i) = \pi(j) = j$. Likewise, $D(T \cdot F^{(3)}_{i,k,\ell})$ must equal zero. In addition, condition (γ) implies that $D(T \cdot F^{(4)}_{i,j,k,\ell}) = 0$.

So it remains to establish property (3) for the polynomials $F_i \in \mathcal{F}$. For this, we must show that $D(T \cdot F_s) = 0$ for all s and all monomials T of degree $< n$. Since D is non-zero only for monomials which represent partial mappings, we may assume w.l.o.g. that T is a partial mapping, T_π, identified with a partial mapping π. By the linearity of D and the definitions of D and F_s, it will suffice to prove that

$$D(T_\pi) = \sum_{t \geq s} D(T_\pi x_{s,t}),$$

i.e., that $D(\pi) = \sum_{t \geq s} D(\pi \cup \{(s,t)\})$, where $\pi \cup \{(s,t)\}$ means the extension of π that sends s to t. For s in the domain of π, this is easy to show, so we assume henceforth that $s \notin dom(\pi)$.

We write $\pi' \supset_s \pi$ to denote the condition that π' is an extension of π and that $\{s\} = dom(\pi') \setminus dom(\pi)$. Therefore we can reexpress the previous equation as:

$$D(\pi) \;=\; \sum_{\pi' \supset_s \pi} D(\pi'). \tag{4}$$

Fix an an arbitrary matching π of degree $< n$. Let $s \notin dom(\pi)$. Let $r = r(\pi)$. We need to establish that equation (4) holds.

Case (1): $D(\pi) \neq 0$.

- ***Case (1.a):*** If $s > r$, then, by condition (δ), the only $\pi' \supset_s \pi$ with $D(\pi') \neq 0$, is the one with $\pi'(s) = s$. Also, for this π', $D(\pi') = D(\pi)$ by the definition of D.
- ***Case (1.b):*** If $s = r$, let r' be the least value greater than r not in the domain of π. By the lemma, if $\pi' \supset_s \pi$ and $D(\pi') \neq 0$, then $\pi'(s) = r'$. Also, since $D(\pi) \neq 0$ and by condition (δ), we have $\pi(i) = i$ for all $r < i < r'$. Therefore, for the π' such that $\pi'(s) = r'$, we have $D(\pi') = D(\pi)$, by the definition of D.

Case (2): $D(\pi) = 0$. This case splits into subcases based on the reason that $D(\pi) = 0$. In each case we show that $\sum_{\pi' \supset_s \pi} D(\pi') = 0$. We start with the cases that imply that $D(\pi') = 0$ for all $\pi' \supset \pi$.

- ***Case (2.a):*** Suppose condition (α) or (β) is violated by π. In this case, it is clear that the same condition is violated by any $\pi' \supset_s \pi$, so $D(\pi') = 0$ for all $\pi' \supset_s \pi$.
- ***Case (2.b):*** Suppose π satisfies conditions (α) and (β) and that $s > r$. In this case, $r(\pi') = r(\pi)$. First, if condition (δ) fails for π, then any $\pi' \supset_s \pi$ also fails to satisfy (δ). Second, suppose (γ) fails for π for the values $i < j < \pi(i)$. If $j \neq s$, then the same condition fails for any $\pi' \supset_s \pi$. If $j = s$, then $\pi' \supset_s \pi$

could satisfy (γ) only if $\pi'(s) = \pi(i) > s$, which would cause condition (δ) to be violated for $\pi\prime$ since $s > r(\pi')$. In any event, $D(\pi') = 0$ for all $\pi' \supset_s \pi$.

Case (2.c): Suppose $s = r$ and there is some $i < j < \pi(i)$ which cause condition (γ) to be violated for π. Clearly the same condition is violated for any $\pi' \supset_s \pi$.

Case (2.d): Suppose $s = r$ and there an $i > r(\pi')$ such that $\pi(i) \neq i$ which causes condition (δ) to fail for π. Obviously this also causes (δ) to fail for any $\pi' \supset_s \pi$.

Now we treat the cases where there is a $\pi' \supset_s \pi$ with $D(\pi') \neq 0$. Therefore none of the above cases hold and $s = r$. From Lemma 8, there must be an $i_0 < s \leq \pi(i_0)$.

Case (2.e): Suppose $\pi(i_0) > s$. Condition (δ) implies that any other $i < s$ with $\pi(i) \geq s$, must satisfy $\pi(i) = \pi(i_0)$. Also, condition (γ) implies that if $s \leq i < \pi(i_0)$, then $\pi'(i) \in \{i, \pi(i_0)\}$. In particular, $\pi'(s) \in \{s, \pi(i_0)\}$. Thus there are two possible $\pi' \supset_s \pi$ such that $S(\pi') \neq 0$:

$$\pi'_1 = \pi \cup \{(s, s)\}$$

and

$$\pi'_2 \ = \ \pi \cup \{(s, \pi(i_0))\}.$$

It is easily checked that they both satisfy all the conditions (α)-(δ) and that $D(\pi'_1) = -D(\pi'_2)$ since s is in the range of π'_1, but not in the range of π'_2. Thus

$$D(\pi) \ = 0 \ = \ D(\pi'_1) + D(\pi'_2) \ = \ \sum_{\pi' \supset_s \pi} D(\pi').$$

Case (2.f): Suppose $\pi(i_0) = s$. Since $D(\pi) = 0$ and since the conditions of cases (2.a)-(2.d) have been ruled out, there must be a least $i_1 > s$ such that $i_1 < r(\pi')$ and $i_1 < \pi(i_1)$, which causes condition (δ) to fail for π. In this case, for $D(\pi')$ to be non-zero, condition (γ) implies that $\pi'(s) \in \{i_1, \pi(i_1)\}$. Thus there are two possible $\pi' \supset_s \pi$ with $D(\pi') \neq 0$, namely,

$$\pi'_1 = \pi \cup \{(s, i_1)\}$$

and

$$\pi'_2 \ = \ \pi \cup \{(s, \pi(i_1))\}.$$

By similar reasoning to the previous case, $D(\pi'_1) = -D(\pi'_2)$, and the desired result follows as before.

□

4. Appendix: (non)completeness over rings

In section 1, we stated the completeness theorem for Nullstellensatz refutation for fields. When working over rings, the completeness theorem

may not always hold. However, the following completeness theorems do apply to rings.

THEOREM 9. *Let R be a commutative ring. Suppose there is no assignment of 0/1 values to variables that make $t_1, \ldots, t_m$ simultaneously equal to zero.*

(a): *Further suppose that R does not have any zero divisors. Then there is a nonzero $a \in R$ and polynomials F_i and G_j so that*

$$\sum_i F_i \cdot t_i + \sum_j G_j \cdot (x_j^2 - x_j) \ = a. \tag{5}$$

(b): *Now suppose instead that $t_1, \ldots, t_n$ assume only 0/1 values for all assignments of 0/1 values to the variables. That is to say, suppose each t_i is equivalent to a propositional formula. Then $t_1, \ldots, t_m$ have a Nullstellensatz refutation.*

We leave the proof of the above theorem to the reader. Note that the situation of part (a) does not quite give a Nullstellensatz refutation since a may not equal 1. However, since $a \neq 0$, (5) can be viewed as a refutation since it implies that there is no propositional assignment that makes the t_i's simultaneously zero.

We conclude with a couple of examples of situations where the Nullstellensatz completeness theorem fails. Both examples use the ring $R = \mathbb{Z}_6$. First consider solutions of

$$\begin{aligned} y + 1 &= 0 \\ y^2 - y &= 0 \end{aligned}$$

From these, one can use a Nullstellensatz refutation to derive 0, 2 or 4; e.g.,

$$(2 - y)(y + 1) + (y^2 - y) = 2.$$

However, there are no polynomials such that $F(y)(y+1)+G(y)(y^2-y) = 1$ over $\mathbb{Z}_6$. Second, consider solutions of

$$\begin{aligned} y + 2 &= 0 \\ y^2 - y &= 0 \end{aligned}$$

Here the situation is worse, the only value $a \in \mathbb{Z}_6$ for which

$$F(y)(y + 1) + G(y)(y^2 - y) \ = \ a$$

is possible is $a = 0$. To prove this last fact, note that $y = 4$ is a solution to the two equations.

References

[1] P. BEAME, S. COOK, J. EDMONDS, R. IMPAGLIAZZO, AND T. PITASSI, *The relative complexity of NP search problems*, in Proceedings of the 27th ACM Symposium on Theory of Computing, 1995, pp. 303–314.

[2] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák, *Lower bounds on Hilbert's Nullstellensatz and propositional proofs*, in Thirty-fifth Annual Symposium on Foundations of Computer Science, IEEE Press, 1994, pp. 794–806. Revised version to appear in Proceedings of the London Mathematical Society.

[3] S. R. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall, *Proof complexity in algebraic systems and constant depth Frege systems with modular counting*. To appear in *Computational Complexity*, 199?

[4] S. R. Buss and T. Pitassi, *Good degree lower bounds on nullstellensatz refutations of the induction principle*, in Proceedings of the Eleventh Annual Conference on Structure in Complexity Theory, IEEE Computer Society, 1996, pp. 233–242. Revised version to appear in *J. Computer and System Sciences*.

[5] M. Clegg, J. Edmonds, and R. Impagliazzo, *Gröbner proofs*, in Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing, Association for Computing Machinery, 1996, pp. 174–183.

[6] T. Pitassi, *Algebraic propositional proof systems*. To appear in the proceedings volume of the DIMACS workshop on *Finite Models and Descriptive Complexity, January 14-17, 1996*, 1995.

Department of Mathematics, University of California, San Diego
E-mail address: sbuss@ucsd.edu