Complexity of Positivstellensatz proofs for the knapsack

Dima Grigoriev

COMPLEXITY OF POSITIVSTELLENSATZ PROOFS FOR THE KNAPSACK

D. Grigoriev

Abstract. A lower bound is established on degrees of Positivstellensatz calculus refutations (over a real field) introduced in (Grigoriev & Vorobjov 1999; Grigoriev 1999), for the knapsack problem. The bound depends on the values of coefficients of an instance of the knapsack problem: for certain values the lower bound is linear and for certain values the upper bound is constant, while in the polynomial calculus the degree is always linear (regardless of the values of coefficients) (Impagliazzo *et al.* 1997). This shows that the Positivstellensatz calculus can be strictly stronger than the polynomial calculus from the point of view of the complexity of the proofs.

Keywords. polynomial calculus, Positivstellensatz proofs, complexity of the knapsack

Subject classification. 68Q25

Introduction

In recent years there has been an intensive activity in the research of algebraic proof systems (Beame *et al.* (1996); Buss *et al.* (1999, 1996/1997); Clegg *et al.* (1996); Grigoriev (1998); Impagliazzo *et al.* (1999); Razborov (1998)). The approach relies on Hilbert's Nullstellensatz and treats the problem of feasibility of a system of polynomial equations

$$f_1 = \cdots = f_k = 0,$$

where among the polynomials $f_1, \ldots, f_k \in F[X_1, \ldots, X_n]$, there appear the polynomials $X_1^2 - X_1, \ldots, X_n^2 - X_n$ (the so-called, Boolean case). Note that this problem is, in general, NP-complete.

The Nullstellensatz proof system (NS) was first considered in (Beame *et al.* 1996). The aim of the system is to find the polynomials $g_1, \ldots, g_k \in F[X_1, \ldots, X_n]$ such that $1 = g_1 f_1 + \cdots + g_k f_k$. The latter representation is sometimes called a *Nullstellensatz refutation.* The number $\max_{1 \leq i \leq k}\{\deg(g_i f_i)\}$ is called the *Nullstellensatz degree.* A linear upper bound $O(n)$ on the Nullstellensatz degree is evident, in (Beame *et al.* 1996) a non-constant lower bound was proved, while after a series of improvements in (Grigoriev 1998) a *linear* (and thus sharp) lower bound was proved.

In (Clegg *et al.* 1996) a stronger proof system — polynomial calculus (PC) was introduced. Starting from axioms $f_1, \dots, f_k$, PC allows one to derive new polynomials from two given polynomials $a, b \in F[X_1, \dots, X_n]$, according to the following two rules:

1. (additive) $a, b \vdash \alpha a + \beta b$, where $\alpha,\ \beta \in F$;
2. (multiplicative) $a \vdash X_i a$ for $1 \leq i \leq n$.

The aim of a derivation is to achieve 1.

The *degree* of a PC derivation is defined as the maximum of the degrees of all intermediately derived polynomials. The first lower bound on the degrees of PC derivations was obtained in (Razborov 1998) (see also (Impagliazzo *et al.* 1999) and (Buss *et al.* 1996/1997)). A linear lower bound for PC for Tseitin's tautologies was proved in Buss *et al.* (1999, 2001). Note that the latter bound is sharp.

In (Grigoriev & Vorobjov 2001), for the case of input polynomials $f_1, \dots, f_k \in \mathbf{R}[X_1, \dots, X_n]$ with real coefficients, derivations of inequalities as well as equalities were considered. The case of *linear* inequalities with added conditions $X_i^2 = X_i$ (Boolean programming) was widely studied by means of cutting planes proofs, for which an exponential lower bound on the length was obtained (a survey and references can be found in (Pudlák 1999)). Another approach to systems of *linear* inequalities was undertaken in Lovász (1994); Lovász & Schrijver (1991); Stephen & Tunçel (1999), where a derivation system was introduced which, given *any* linear polynomial e, allows one to derive $e^2 \geq 0$, given any *already derived* linear inequalities $a_1 \geq 0, a_2 \geq 0$, allows one to derive $a_1 + a_2 \geq 0$, $a_1 a_2 \geq 0$, and, given any *already derived* quadratic inequalities $p_1 \geq 0, p_2 \geq 0$, allows one to derive $p_1 + p_2 \geq 0$. In (Pudlák 1999) one can find some remarks on the complexity of this (called Lovász-Schrijver) procedure, in particular, an upper bound for the Pigeon Hole Principle (written as a system of linear inequalities).

More precisely, following (Grigoriev & Vorobjov 2001), let a system of equations and inequalities

$$(0.1) \qquad f_1 = \cdots f_k = 0,\ h_1 \geq 0, \dots, h_m \geq 0.$$

be given. Dealing with systems of inequalities one could get profit from using the axiom that any square is non-negative, and the rules of adding or multiplying inequalities. This is formalized in the following notion of the cone (which replaces the role of ideals for systems of equations) and in two proof systems described below for refuting systems of inequalities, they extend the systems NS and PC, respectively.

Definition 0.2. *The* cone $c(h_1, \dots, h_m)$ *generated by polynomials* $h_1, \dots, h_m \in \mathbf{R}[X_1, \dots, X_n]$ *is the smallest family of polynomials containing* $h_1, \dots, h_m$ *and satisfying the following rules:*

(a) $e^2 \in c(h_1, \dots, h_m)$ *for any* $e \in \mathbf{R}[X_1, \dots, X_n]$*;*

if $a, b \in c(h_1, \dots, h_m)$*, then*
(b) $a + b \in c(h_1, \dots, h_m)$*;*
(c) $ab \in c(h_1, \dots, h_m)$*.*

Remark 0.3. *The minimal cone* $c(\emptyset)$ *consists of all sums of squares of polynomials.*

Remark 0.4. *Any element of* $c(h_1, \dots, h_m)$ *can be represented in a form*

$$\sum_{I \subset \{1, \dots, m\}} \left(\prod_{i \in I} h_i \right) \left(\sum_j e_{I,j}^2 \right)$$

for some polynomials $e_{I,j} \in \mathbf{R}[X_1, \dots, X_n]$.

The two proof systems introduced in (Grigoriev & Vorobjov 2001) (which could be viewed as *static* and *dynamic*, respectively), rely on the following Positivestellensatz (see Bochnak *et al.* (1998); Stengle (1974)).

Positivstellensatz. *A system (0.1) has no common solutions in* $\mathbf{R}^n$ *if and only if for a suitable polynomial* $f \in \mathbf{R}[X_1, \dots, X_n]$ *from the ideal* $(f_1, \dots, f_k)$ *and a polynomial* $h \in c(h_1, \dots, h_m)$ *we have:* $f + h = -1$.

The first (static) proof system is stronger than NS refutations and could be viewed as its Positivstellensatz analogue.

Definition 0.5. *A pair of polynomials*

$$(f, h) = \left(\sum_{1 \le s \le k} f_s g_s, \quad \sum_{I \subset \{1, \dots, m\}} \left(\prod_{i \in I} h_i \right) \left(\sum_j e_{I,j}^2 \right) \right)$$

with $f + h = -1$ *where* $g_i, e_{I,j} \in \mathbf{R}[X_1, \dots , X_n]$ *we call a* Positivstellensatz refutation *for (0.1) (we denote it by* $PS_>$*). The* degree *of the refutation is*

$$\max_{s,I,j}\{\deg(f_s g_s),\ \deg(e_{I,j}^2 \prod_{i\in I} h_i)\}.$$

The second (dynamic) proof system is stronger than PC and could be viewed as its Positivstellensatz analogue.

Definition 0.6. *Let a polynomial* $f \in (f_1, \dots , f_k)$ *be derived in PC from the axioms* $f_1, \dots , f_k$*, and let a polynomial* $h \in c(h_1, \dots , h_m)$ *be derived, applying the rules (a), (b), (c) from Definition 0.2, from the axioms* $h_1, \dots , h_m$*. Suppose that* $f + h = -1$*. This pair of derivations we call a* Positivstellensatz calculus refutation *for (0.1) (we denote it by* $PC_>$*). By its* degree *we mean the maximum of the degrees of intermediate polynomials from both derivations. The* length *of the refutation we define as the total number of steps in both derivations.*

In the present paper we consider just the systems of equations $f_1 = \cdots = f_n = 0$ (the polynomials $h_1, \dots, h_m$ are absent). In this case a polynomial h is just a sum of squares $\sum_j h_j^2$ (cf. Remark 0.3).

In (Grigoriev & Vorobjov 2001) a so-called telescopic system of equations due to Lazard-Mora-Philippon is considered and an exponential lower bound on the degree of any its $PS_>$ refutation (see Definition 0.5) is proved. On the other hand it is shown a linear upper bound for the telescopic system on the degree of PC, being sharp because a linear lower bound is proved in (Grigoriev & Vorobjov 2001) for the stronger system of the $PC_>$ refutations (see Definition 0.6), and for the latter one also an exponential lower bound on the lengths of proofs is established.

However, the telescopic system is not Boolean, whereas the main interest in the proof theory is just in the Boolean systems. In (Grigoriev 2001) a linear lower bound on the degree of $PC_>$ refutations is established for the Tseitin's tautologies and for the parity principle, the proofs extend the argument from Buss *et al.* (1999, 2001) and similar lower bounds for PC.

In the present paper as in (Impagliazzo *et al.* 1999) we consider the following system which is a particular case of the knapsack problem

$$(0.7) \qquad f_i = X_i^2 - X_i = 0, 1 \le i \le n, f = X_1 + \cdots + X_n - r = 0$$

We note that throughout the paper $r \in \mathbf{R}$ denotes a real number.

The $PS_>$ (see Definition 0.5) and $PC_>$ (see Definition 0.6) degrees of (0.7) depend essentially on the value of r. If either $r < 0$ or $r > n$ then the following obvious identities

$$-f_1 - \cdots - f_n - f + X_1^2 + \cdots + X_n^2 = r$$

and respectively,

$$-f_1 - \cdots - f_n + f + (X_1 - 1)^2 + \cdots + (X_n - 1)^2 = n - r$$

show that both $PS_>$ and $PC_>$ degrees of (0.7) are 2. On the other hand, theorem 5.1 of Impagliazzo *et al.* (1999) establishes a lower bound of $\lceil n/2 \rceil + 1$ on the PC degree of (0.7) regardless of the value of r. Thus, $PC_>$ can be strictly stronger than PC and $PS_>$ can be strictly stronger than PS. The main result of the present paper is the following lower bound on the $PS_>$ and $PC_>$ degrees of (0.7).

Theorem. *Let k be a non-negative integer and suppose that $k < r < n - k$.*

(i) When $0 \le k \le (n-3)/2$ the Positivstellensatz refutation degree of (0.7) is greater or equal to $2k + 4$. For $k \ge (n-2)/2$ the degree is greater or equal to $n + 1$;

(ii) when $0 \le k \le \lceil n/4 \rceil - 2$ the Positivstellensatz calculus refutation degree of (0.7) is greater or equal to $2k + 4$. For $k > \lceil n/4 \rceil - 2$ the degree is greater or equal to $\lceil n/2 \rceil + 1$.

Remark 0.8. *Actually one could rephrase the theorem invoking the following stairs-form function δ which equals to 2 outside the interval $(0, n)$ and which equals to $2k+4$ on the intervals $(k, k+1)$ and $(n-k-1, n-k)$ for all integers $0 \le k < n/2$. Then the bound in a) on the degree is $\min\{\delta, n+1\}$ and the bound in b) is $\min\{\delta, \lceil n/2 \rceil + 1\}$. The values of the function δ at the integer points $0, \ldots, n$ does not matter since system (0.7) has a solution at precisely these values of r. Observe also that both degrees in the theorem as functions in m are symmetric with respect to the point $n/2$, taking into account the transformation $X_i \to 1 - X_i, 1 \le i \le n$.*

In section 1 we show how to reduce the proof of the theorem to the non-negativity of a relevant quadratic form which in its turn is proved in section 2.

In the theorem we establish lower bounds on the degrees of $PS_>$ and $PC_>$ refutations. It would be interesting to learn how close are they to upper bounds (we know this for $r < 0$ or $r > n$ due to the identities above and also when $k \ge (n-2)/2$ in case (i) and when $k > \lceil n/4 \rceil - 2$ in case (ii)).

1. Reduction to the non-negativity of a quadratic form

As in Impagliazzo *et al.* (1999) we consider a factor-algebra

$$A = \mathbf{R}[X_1, \dots, X_n]/(X_1^2 - X_1, \dots, X_n^2 - X_n)$$

which has a canonical basis of the multilinear monomials $\{X^I\}$ where $I \subset \{1, \dots n\}$. For a polynomial $g \in \mathbf{R}[X_1, \dots, X_n]$ denote by $\overline{g} \in A$ the multilinear polynomial that is the canonical image of g in A.

Lemma 5.2 of Impagliazzo *et al.* (1999) states that $deg(\overline{fg}) = deg(\overline{g}) + 1$, provided that $deg(\overline{g}) < \lceil n/2 \rceil$. This implies (theorem 5.1 of Impagliazzo *et al.* (1999)) the lower bound $\lceil n/2 \rceil$ on the degree of PC refutations of (0.7). This bound is sharp (theorem 4.2 Impagliazzo *et al.* (1999)). Moreover, it is claimed in the proof of theorem 5.1 of Impagliazzo *et al.* (1999) that if a polynomial h is deducible in PC from (0.7) with a degree of the refutation at most $\lceil n/2 \rceil$ then $h = f_1 g_1 + \cdots + f_n g_n + fg$ for suitable $g_1, \dots, g_n, g$ such that $\overline{g} = g, deg(\overline{h}) = deg(g) + 1$ and $deg(f_i g_i) \leq deg(h), 1 \leq i \leq n$ (this claim is verified in Impagliazzo *et al.* (1999) by induction along a deduction of h in PC relying on lemma 5.2 of Impagliazzo *et al.* (1999)). For a weaker system of NS one can prove a better (also sharp) lower bound (which holds, in fact, over any field of characteristic either zero or greater than n).

Proposition 1.1. *The Nullstellensatz degree of (0.7) equals to $n + 1$.*

Proof. The upper bound $n+1$ on the degree was established in Beame *et al.* (1996). Indeed, there is a polynomial g such that $\overline{g} = g$ and $\overline{fg} = 1$. Then the polynomial $fg - 1$ belongs to the ideal generated by $f_1, \dots, f_n$. Now we proceed to the lower bound.

Denote by $S = \frac{1}{n!} \sum_{\sigma \in S_n} \sigma$ the operator of symmetrization. Fix an NS refutation $1 = f_1 g_1 + \cdots \underline{f_n} g_n + fg$, one can assume without loss of generality that $g = \overline{g}$ and so $deg(\overline{fg}) = deg(g) + 1$, provided that $deg(g) < n$. After applying S to the NS refutation one could assume that $S(g) = g$, indeed, $S(g)$ is a linear combination of elementary symmetric functions $s_0 = 1, s_1 = X_1 + \cdots + X_n, \dots, s_n = X_1 \cdots X_n$, assuming that $k = \deg(g) < n$, for the highest terms in the product $\overline{fg}$ we have $\overline{s_1 s_k} = (k+1) s_{k+1} + k s_k$ since $f = s_1 - r$. □

Now we proceed to the proof of the theorem. Suppose that there is a $PS_>$ refutation of (0.7) in case (i) and a $PC_>$ refutation of (0.7) in case (ii), respectively, of degree d being less than a respective bound in the theorem. Note that $d \leq n$ in case (i) and $d \leq \lceil n/2 \rceil$ in case (ii) (see also the Remark 0.8 after the theorem). Definitions Definition 0.5, Definition 0.6, respectively, imply that for appropriate polynomials h_j we have an equality

$$1+\sum_j h_j^2 = f_1g_1+\cdots+f_ng_n+fg \tag{1.2}$$

where $deg(f_ig_i), deg(fg) \leq d, 1 \leq i \leq n$ in case (i), and in case (ii) the right-hand side is deducible in the PC within the degree d. Observe that $deg(h_j^2) \leq deg(f_1g_1+\cdots+f_ng_n+fg) \leq d$. Indeed, consider among all the monomials occurring in all h_j the highest one with respect to the *deglex* monomial ordering, then the coefficient of the square of this monomial in the sum $1+\sum_j h_j^2$ should be positive. In case (ii) the (already mentioned at the beginning of the section) claim in the proof of theorem 5.1 of Impagliazzo *et al.* (1999) states that $deg(fg), deg(f_ig_i) \leq d, 1 \leq i \leq n$ for $g, g_1, \ldots, g_n$ chosen in a suitable way.

Define a linear mapping $B: A \to \mathbf{R}$ by letting $B(X^I) = B_k = \frac{r(r-1)\cdots(r-k+1)}{n(n-1)\cdots(n-k+1)}$ for the basis elements X^I of A corresponding to any set I with $|I| = k$ and extending linearly. Further, extend B to all of $\mathbf{R}[X_1, \ldots, X_n]$ by defining $B(g) = B(\overline{g})$. Observe that the mapping B is symmetric and that $B(1) = B_0 = 1$.

Lemma 1.3. *For a polynomial* $g_0 \in \mathbf{R}[X_1, \ldots, X_n]$ *with* $deg(g_0) < n$ *we have* $B(fg_0) = 0$.

Proof. It suffices for a multilinear monomial X^I with $|I| = k < n$ to verify that $B(fX^I) = 0$, which is valid since $B(fX^I) = (n-k)B_{k+1} + (k-r)B_k$. □

Denote by $P_k \subset A, 0 \leq k \leq n$ the linear hull of all the monomials X^I of degree $|I| = k$. Then $A = \oplus_{0 \leq k \leq n} P_k$.

We introduce a quadratic form Q in the space $\oplus_{0 \leq k \leq \lfloor n/2 \rfloor} P_k$ with the entry in the place (X^I, X^J) being equal to $B(X^I X^J)$. By $Q_l, l \leq \lfloor n/2 \rfloor$ we denote the restriction of Q onto the subspace $\oplus_{0 \leq k \leq l} P_k$, in particular, $Q_{\lfloor n/2 \rfloor} = Q$. In the sequel we often identify a quadratic form with the symmetric matrix of its coefficients and we identify a polynomial with the vector of its coefficients.

Lemma 1.4. *The quadratic form* Q_l *is non-negative when* $l-1 < r < n-l+1$.

The proof of the Lemma 1.4 is contained in the next section, and now we show how to deduce the theorem from the Lemma 1.4.

End of the proof of the theorem. We apply the mapping B to both sides of (1.2). In the right-hand side we obtain $B(fg) = 0$ due to Lemma 1.3 because $deg(fg) \leq d \leq n$ in both cases (i), (ii). On the other hand let $h_j =$

$\sum_I h_j^{(I)} X^I$, then $B(h_j^2) = \sum_{I,J} h_j^{(I)} h_j^{(J)} B(X^I X^J) = h_j Q_{\lfloor d/2 \rfloor} h_j^T \geq 0$ according to Lemma 1.4, taking into the account that $deg(h_j^2) \leq d$ (see above) and that in case (i) when $0 \leq k \leq (n-3)/2$ or in case (ii) when $0 \leq k \leq \lceil n/4 \rceil - 2$ we have $\lfloor d/2 \rfloor \leq k+1$ by the adopted supposition that the theorem is wrong, and in case (i) when $k \geq (n-2)/2$ we have $k+1 \geq n/2 \geq d/2$, and finally in case (ii) when $k > \lceil n/4 \rceil - 2$ we have $k+1 \geq \lfloor \frac{\lceil n/2 \rceil}{2} \rfloor \geq \lfloor d/2 \rfloor$ (here h_j^T denotes the transposed vector of coefficients of h_j). Since $B(1) = 1$ we get a contradiction. □

Note that one can obtain another proof of the Proposition 1.1 just applying the mapping B to any NS refutation and making use of Lemma 1.3.

2. Non-negativity of the quadratic form Q

Now we proceed to the proof of Lemma 1.4. The plan is to describe the kernel of Q_l and its eigenspaces, and to prove that non-zero eigenvalues are positive.

First observe that the vector $fX^I, |I| \leq l-1$ belongs to the kernel $\ker Q_l$. Indeed, the product of the row of the matrix Q_l which corresponds to a monomial X^J by the vector fX^I, equals to $B(fX^I X^J) = B(fX^{I \cup J})$ which vanishes since $|J| \leq l$, hence $|I \cup J| \leq 2l-1 \leq n-1$ and we apply Lemma 1.3. Actually, we'll show in the sequel that $\ker Q_l$ is the linear hull of these vectors.

In the sequel for a vector $v \in P_k$ we utilize a notation $v = (v_I)$ where v_I is I-component of v, i.e. the coefficient of X^I in v. Consider a linear mapping $C_k : P_k \to P_{k+1}$ where for a vector $v = (v_I) \in P_k$ its image $(C_k(v))_J = \sum_{I \subset J} v_I$, here and below $I, J \subset \{1, \dots, n\}; |J| = k+1, |I| = k$. Also consider a linear mapping $D_k : P_{k+1} \to P_k$ under which the image of a vector $w = (w_J) \in P_{k+1}$ is a vector whose I-component equals to $(D_k(w))_I = \sum_{J \supset I} w_J$.

Denote by $P_{k+1}^{(0)} \subset P_{k+1}$ a subspace $\{(u_J) : \forall |I| = k \quad (\sum_{J \supset I} u_J = 0)\}$. For $t > k$ denote a subspace $P_{k+1}^{(t-k)} = C_t \cdot C_{t-1} \cdots C_{k+1}(P_{k+1}^{(0)}) \subset P_{t+1}$ and besides, for any vector $w = (w_J) \in P_{k+1}$ and any $L \subset \{1, \dots, n\}; |L| = t+1$ we have

$$((C_t \cdot C_{t-1} \cdots C_{k+1})(w))_L = (t-k)! (\sum_{J \subset L} w_J) \tag{2.1}$$

For a vector $u \in P_{k+1}^{(0)}$ one can represent (in algebra A defined in section 1 above) the polynomial

$$\overline{s_1^t \sum_J u_J X^J} = \sum_{|K|=k+t+1} (C_{k+t} \cdots C_{k+1}(u))_K X^K + \tag{2.2}$$
$$\eta_{k,t}^{(k+t)} \sum_{|K|=k+t} (\sum_{J \subset K} u_J) X^K + \cdots + \eta_{k,t}^{(k+1)} \sum_{|K|=k+1} u_K X^K$$

for appropriate constants $\eta_{k,t}^{(p)}$, by means of opening the parenthesis in s_1^t and taking into the account (2.1), provided that $k+t+1 \leq n$ (in fact, this equality holds for any vector $w \in P_{k+1}$). The vectors of coefficients of the polynomials $\overline{s_1 - r}, \overline{s_1(s_1 - r)}, \overline{s_1^2(s_1 - r)}, \ldots, \overline{s_1^{l-1}(s_1 - r)}$ (of the degrees $1, 2, \ldots, l$, respectively) belong to the $\ker Q_l$ (see the beginning of the present section), the same holds for the polynomials (or more precisely, the elements of A)

$$\overline{(s_1 - r)\sum_J u_J X^J}, \overline{s_1(s_1 - r)\sum_J u_J X^J}, \tag{2.3}$$
$$\overline{s_1^2(s_1 - r)\sum_J u_J X^J}, \ldots, \overline{s_1^{l-k-2}(s_1 - r)\sum_J u_J X^J}$$

Thus, using (2.2) we summarize the properties of the polynomials (2.3) in the following proposition.

Proposition 2.4. *The vectors of coefficients of polynomials (2.3) belong to the kernel* $\ker Q_l$ *and the leading homogeneous forms of (2.3) are*

$$C_{k+1}(u), C_{k+2} \cdot C_{k+1}(u), \ldots, C_{l-1} \cdots C_{k+2} \cdot C_{k+1}(u)$$

of the degrees $k+2, k+3, \ldots, l$, *respectively. The polynomials (2.3) lie in* $(l-k)$*-dimensional subspace* $P(u)$ *with the basis*

$$u^{(k+1)} = (u), u^{(k+2)} = C_{k+1}(u), u^{(k+3)} = \frac{1}{2!} C_{k+2} \cdot C_{k+1}(u), \ldots, \tag{2.5}$$
$$u^{(l)} = \frac{1}{(l-k-1)!} C_{l-1} \cdots C_{k+2} \cdot C_{k+1}(u) \in P_{k+1} \oplus P_{k+2} \oplus \cdots \oplus P_l$$

Due to (2.1) for $|K| = t$ the coordinate of the vector $(u^{(t)})_K = \sum_{J \subset K} u_J$. For a subset $T' \subseteq \{1, \ldots, n\}, |T'| \leq k$ we have (recall that $|J| = k+1$)

$$\sum_{J\supset T'} u_J = 0 \tag{2.6}$$

because up to a constant (positive) factor it equals to $\sum_{I\supseteq T',|I|=k}\sum_{J\supset I} u_J = 0$.

For fixed subsets $K\subseteq\{1,\dots,n\}, |K|=i$ and $T\subseteq K, |T|\leq k+1$ we prove the following identity:

$$\sum_{J\cap K=T} u_J = (-1)^{k+1-|T|}\sum_{T\subseteq J\subseteq K} u_J \tag{2.7}$$

The proof goes by induction on $k+1-|T|$. The base when $i\geq k+1$ for $|T|=k+1$ is trivial since both sides of (2.7) in this case equal to u_T. Respectively, when $i\leq k$ we put for the base $T=K$, then the both sides of (2.7) in this case vanish due to (2.6). For the inductive step from (2.6) we get

$$0=\sum_{J\supset T} u_J = \sum_{J\cap K=T} u_J + \\ \sum_{J\supset T,|J\cap K|=|T|+1} u_J + \sum_{J\supset T,|J\cap K|=|T|+2} u_J + \cdots + \sum_{J\supset T,|J\cap K|=k+1} u_J =$$

(in case when $i\leq k$ all the sums in the latter line vanish by the inductive hypothesis, hence the sum $\sum_{J\cap K=T} u_J = 0$ vanishes as well, which proves the inductive step, thus we continue the chain of equalities assumming that $i\geq k+1$)

$$= \sum_{J\cap K=T} u_J + \sum_{H\supset T,|H|=|T|+1} (-1)^{k+1-(|T|+1)}\sum_{H\subseteq J\subseteq K} u_J + \\ \sum_{H\supset T,|H|=|T|+2} (-1)^{k+1-(|T|+2)}\sum_{H\subseteq J\subseteq K} u_J + \cdots + \sum_{H\supset T,|H|=k+1} u_H =$$

due to the inductive hypothesis (where in the double sums the external summation ranges over H while the internal one ranges over J); in its turn continuing the chain of equalities we get

$$= \sum_{J\cap K=T} u_J + \sum_{T\subseteq J\subseteq K} (1 - \binom{k+1-|T|}{1} + \binom{k+1-|T|}{2} - \cdots +$$

$$(-1)^{k-|T|}\binom{k+1-|T|}{k-|T|})u_J = \sum_{J\cap K=T} u_J - (-1)^{k+1-|T|}\sum_{T\subseteq J\subseteq K} u_J$$

that proves (2.7).

Next we prove the following proposition.

Proposition 2.8. *The composition of the operators $D_t \cdot C_t$ restricted on the subspace $C_{t-1}\cdots C_{k+1}(P_{k+1}^{(0)})$ equals to a multiple $(n-t-k-1)(t-k)E$ of the identity operator E, provided that $n-t-k-1>0$.*

Proof of the proposition. Let $M \subseteq \{1,\dots,n\}; |M| = t$ and $u \in P_{k+1}^{(0)}$, we obtain the following chain of inequalities

$$\frac{1}{(t-k)!}(D_t C_t \cdots C_{k+1}(u))_M = \sum_{L\supset M, |L|=t+1}\ \sum_{J\subseteq L} u_J =$$

(due to (2.1))

$$= (n-t)\sum_{J\subseteq M} u_J + \sum_{|J\cap M|=k} u_J = (n-t)\sum_{J\subseteq M} u_J - \sum_{I\subset M, |I|=k}\ \sum_{I\subset J\subseteq M} u_J =$$

(see (2.7))

$$= (n-t)\sum_{J\subseteq M} u_J - (k+1)\sum_{J\subseteq M} u_J = (n-t-k-1)\sum_{J\subseteq M} u_J =$$

$$\frac{n-t-k-1}{(t-k-1)!}(C_{t-1}\cdots C_{k+1}(u))_M$$

(again due to (2.1)). This proves Proposition 2.8. □

We prove by induction on t that P_t is the direct sum of its subspaces

$$P_t^{(0)} \oplus C_{t-1}P_{t-1}^{(0)} \oplus C_{t-1}\cdot C_{t-2}P_{t-2}^{(0)} \oplus \cdots \oplus C_{t-1}\cdot C_{t-2}\cdots C_0 P_0^{(0)} \tag{2.9}$$

The base case for $t=0$ is obvious. Assuming (2.9) as the inductive hypothesis, we obtain that the image under the operator C_t of (2.9) is also a direct sum (due to Proposition 2.8 applied to each item of the direct sum (2.9), observe that $n-2t-1>0$ since $t<l\le\lfloor n/2\rfloor$):

$$C_tP_t = C_tP_t^{(0)} \oplus C_t \cdot C_{t-1}P_{t-1}^{(0)} \oplus C_t \cdot C_{t-1} \cdot C_{t-2}P_{t-2}^{(0)} \oplus \cdots \oplus C_t \cdot C_{t-1} \cdots C_0P_0^{(0)} \subset P_{t+1}$$

and $D_t \cdot C_tP_t = P_t$, moreover $D_t \cdot C_t$ is an automorphism of P_t. Apart from that, the kernel $\ker D_t = P_{t+1}^{(0)}$. Therefore, $P_{t+1} = P_{t+1}^{(0)} \oplus C_tP_t$ that proves the inductive hypothesis and (2.9).

Partition the matrix Q_l into the blocks $Q^{(i,j)} : P_j \to P_i, 0 \leq i, j \leq l$. Our next purpose is to calculate the vector $Q^{(i,k+1)}(u) \in P_i$, recall that $u \in P_{k+1}^{(0)}, |J| = k+1$. Let $|K| = i$, we have using the definition of the mapping B from section 1

$$(Q^{(i,k+1)}(u))_K = \sum_{T, T \subseteq K} \sum_{J, K \cap J = T} B(X^K X^J)u_J = \sum_{T \subseteq K} B_{i+k+1-|T|} \sum_{K \cap J = T} u_J$$

The latter sum vanishes when $i \leq k$ since $\sum_{K \cap J = T} u_J = 0$ due to (2.7).

Now when $i \geq k+1$ we obtain using (2.7)

$$\begin{aligned} (2.10) \quad & (Q^{(i,k+1)}(u))_K \\ &= B_i \sum_{J \subseteq K} u_J + B_{i+1} \sum_{|J \cap K| = k} u_J \\ &\quad + B_{i+2} \sum_{|J \cap K| = k-1} u_J + \cdots + B_{i+k+1} \sum_{|J \cap K| = 0} u_J \\ &= B_i \sum_{J \subseteq K} u_J - B_{i+1} \binom{k+1}{k} \sum_{J \subseteq K} u_J + B_{i+2} \binom{k+1}{k-1} \sum_{J \subseteq K} u_J - \cdots \\ &\quad + (-1)^{k+1} B_{i+k+1} \binom{k+1}{0} \sum_{J \subseteq K} u_J \\ &= (B_i - B_{i+1} \binom{k+1}{k} + B_{i+2} \binom{k+1}{k-1} - \cdots \\ &\quad + (-1)^{k+1} B_{i+k+1} \binom{k+1}{0}) \sum_{J \subseteq K} u_J \end{aligned}$$

Thus, $(Q^{(i,k+1)}(u)) = \mu_{i,k+1}u^{(i)}$ (see (2.5)) where

$$(2.11) \qquad \mu_{i,k+1} = \sum_{i \leq j \leq i+k+1} (-1)^{j-i} \binom{k+1}{j-i} B_j, l \geq i \geq k+1$$

(we recall that $k+1$ is fixed for the time being). In particular, for $i = k+1$ the vector $u^{(k+1)} = u$ is an eigenvector of the operator $Q^{(k+1,k+1)}$.

Because

$$0 = (Q^{(i,k+1)} \quad Q^{(i,k+2)}) \cdot \overline{(s_1 - r)\sum_J u_J X^J}$$

for all $i \leq l$, taking into the account Proposition 2.4, we get that $Q^{(i,k+2)} \cdot u^{(k+2)} = \mu_{i,k+2} u^{(i)}$ for appropriate constant $\mu_{i,k+2}$ when $i \geq k+1$ and $Q^{(i,k+2)} \cdot u^{(k+2)} = 0$ when $i \leq k$. In a similar way,

$$0 = (Q^{(i,k+1)} \quad Q^{(i,k+2)} \quad Q^{(i,k+3)}) \cdot \overline{s_1(s_1 - r)\sum_J u_J X^J},$$

this implies that $Q^{(i,k+3)} \cdot u^{(k+3)} = \mu_{i,k+3} u^{(i)}$ for appropriate constants $\mu_{i,k+3}$ when $i \geq k+1$ and $Q^{(i,k+3)} \cdot u^{(k+3)} = 0$ when $i \leq k$ and so on. Thus, the operator Q_l acts on the subspace $P(u)$ (see (2.5)), in other words $P(u)$ is invariant under Q_l, and $(\mu_{i,j})$ is the matrix of its action with respect to the basis (2.5) if in addition we set $\mu_{i,j} = 0$ when $j < k+1$. Since the polynomials (2.3) belong to $\ker Q_l$ due to Proposition 2.4, the rank of $(\mu_{i,j})$ is at most 1. We have already calculated the first (possibly) non-zero column of the matrix $(\mu_{i,j}), 0 \leq i, j \leq l$ (the index of this column is $k+1$).

Our next purpose is to calculate the first (possibly) non-zero row of this matrix (its index is also $k+1$ as was just proved).

So, we need to calculate the coordinate of the vector $(Q^{(k+1,i)} u^{(i)})_{J_0}$ for a fixed $|J_0| = k+1$. This coordinate equals to

$$\sum_{i \leq j \leq i+k+1} B_j \sum_{|K \cap J_0| = k+1-j+i} \sum_{J \subseteq K} u_J \tag{2.12}$$

where the second summation ranges over K and the third (internal) one ranges over J.

Now we transform one item of the sum (2.12):

$$\sum_{|K \cap J_0| = k+1-j+i} \sum_{J \subseteq K} u_J =$$

$$\sum_{0 \leq t \leq k+1-j+i} \binom{k+1-t}{k+1-t-j+i} \binom{n-2k-2+t}{j-2k-2+t} \Big(\sum_{|J \cap J_0| = t} u_J \Big) \tag{2.13}$$

where the first binomial coefficient $\binom{k+1-t}{k+1-t-j+i}$ counts the number of possibilities (for fixed J, J_0) to choose a subset $(J_0 - J) \cap K$ in the set $J_0 - J$ (note that $|J_0 - J| = k + 1 - t$, $|(J_0 - J) \cap K| = k + 1 - t - j + i$); while the second binomial coefficient $\binom{n-2k-2+t}{j-2k-2+t}$ counts the number of possibilities to choose a subset $K - J - J_0$ in the set $\{1, \dots, n\} - J - J_0$ (note that $|K - J - J_0| = j - 2k - 2 + t$, $|\{1, \dots, n\} - J - J_0| = n - 2k - 2 + t$). Thereby, the product of these two binomial coefficients provides the numbers of possibilities for K from the left-hand side.

Because of (2.7) we obtain that $\sum_{|J\cap J_0|=t} u_J = (-1)^{k+1-t}\binom{k+1}{t} u_{J_0}$. Therefore, (2.13) equals to

$$(\sum_{0\le t\le k+1-j+i} (-1)^{k+1-t}\binom{k+1}{t}\binom{k+1-t}{k+1-t-j+i}\binom{n-2k-2+t}{n-j})u_{J_0} =$$

$$(\sum_{0\le t\le k+1-j+i} (-1)^{k+1-t}\frac{(k+1)!}{t!(k+1-t-j+i)!(j-i)!}\binom{n-2k-2+t}{n-j})u_{J_0} =$$

$$\binom{k+1}{j-i}(\sum_{0\le t\le k+1-j+i} (-1)^{k+1-t}\binom{k+1-j+i}{t}\binom{n-2k-2+t}{n-j})u_{J_0} =$$

$$(-1)^{j-i}\binom{k+1}{j-i}\binom{n-2k-2}{i-k-1}u_{J_0}$$

.

To prove the latter equality denote by Ξ, Υ some sets of the cardinalities $k + 1 - j + i, n - 2k - 2$, respectively. Observe that the sum in the second-to-last line in the chain of the equalities

$$\sum_{0\le t\le k+1-j+i} (-1)^{k+1-t}\binom{k+1-j+i}{t}\binom{n-2k-2+t}{n-j}$$

coincides with the weighted sum of the number of choices of first, a subset Λ of Ξ of the cardinality t and subsequently a subset Δ of the cardinality $n - j$ of the union $\Lambda \cup \Upsilon$, taken with the weight $(-1)^{k+1-t}$. On the other hand, if Δ does not contain Ξ the contribution of Δ into the weighted sum vanishes since this contribution equals the weighted sum of occurances of Λ, i.e.

$$\sum_{\Xi\cap\Delta\subseteq\Lambda\subseteq\Xi} (-1)^{k+1-|\Lambda|} = \sum_{0\le\tau\le\tau_0} (-1)^{\tau}\binom{\tau_0}{\tau}$$

where $\tau_0 = |\Xi - \Delta|$. Else when Δ contains Ξ, the contribution (for the unique $\Lambda = \Xi$) equals $(-1)^{j-i}$. In order to finish this proof notice that the number of such Δ equals the number of subsets $\Delta \cap \Upsilon$ of the cardinality $(n-j)-(k+1-j+i)$ of the set Υ, i.e. $\binom{n-2k-2}{n-k-i-1}$.

Thus, (2.12) equals to

$$\binom{n-2k-2}{i-k-1}\Big(\sum_{i \le j \le i+k+1} (-1)^{j-i}\binom{k+1}{j-i}B_j\Big)u_{J_0},$$

hence

$$\text{(2.14)}\quad \mu_{k+1,i} = \binom{n-2k-2}{i-k-1}\Big(\sum_{i \le j \le i+k+1} (-1)^{j-i}\binom{k+1}{j-i}B_j\Big) = \binom{n-2k-2}{i-k-1}\mu_{i,k+1}$$

Therefore, the matrix $(\mu_{i,j})$ (being of the rank at most 1) is non-negative if and only if its entry $\mu_{k+1,k+1} > 0$, provided that $\mu_{k+1,k+1} \neq 0$. Indeed, each diagonal entry $\mu_{i,i}$ of the matrix $(\mu_{i,j})$ is non-negative (respectively, each one is non-positive) if and only if $\mu_{k+1,k+1} > 0$ (respectively, $\mu_{k+1,k+1} < 0$) since due to (2.14) the signs of $\mu_{k+1,i}$ and $\mu_{i,k+1}$ coincide and taking into account that $\mu_{i,i}\mu_{k+1,k+1} = \mu_{i,k+1}\mu_{k+1,i}$; furthermore, the only non-zero eigenvalue of the rank 1 matrix $(\mu_{i,j})$ equals to its trace, the latter is thereby positive if and only if $\mu_{k+1,k+1} > 0$.

Suppose that we have proved already that the matrices $(\mu_{i,j})$ (let us underline that the matrix $(\mu_{i,j})$ was defined for a fixed $k+1$) are non-negative for all $0 \le k+1 \le l$. This would imply that the matrix Q_l is non-negative as well since $(\mu_{i,j})$ is the action of Q_l on the subspace $P(u)$ (see above), hence the unique non-zero eigenvalue of the matrix $(\mu_{i,j})$ is the eigenvalue of Q_l as well, actually, this eigenvalue depends only on $k+1$ and does not depend on a particular vector $u \in P_{k+1}^{(0)}$. Moreover, these eigenvalues for all $0 \le k+1 \le l$ exhaust all the eigenvalues of Q_l. Indeed, the subspace

$$\text{(2.15)}\qquad P_{k+1}^{(0)} \oplus C_{k+1}P_{k+1}^{(0)} \oplus C_{k+2}C_{k+1}P_{k+1}^{(0)} \oplus \cdots \oplus C_{l-1}\cdots C_{k+1}P_{k+1}^{(0)}$$

equals the direct sum of subspaces of the form $P(u)$ where u ranges over the elements of an arbitrary basis of the subspace $P_{k+1}^{(0)}$, and on the other hand, the direct sum of all these subspaces of the form (2.15) for $0 \le k+1 \le l$ coincides with the whole space $P_0 \oplus \cdots \oplus P_l$ due to (2.9). Thus, Q_l is non-negative.

So, to complete the proof of Lemma 1.4 it remains to verify that $\mu_{k+1,k+1} > 0$ for all $0 \leq k+1 \leq l$.

Denote $B_i^{(k+1)} = \mu_{i,k+1}, l \geq i \geq k+1$ where $\mu_{i,k+1}$ is taken from (2.11). We prove by induction on k that

$$B_i^{(k+1)} = \frac{(\prod_{1 \leq j \leq i}(r+1-j))(\prod_{0 \leq t \leq k}(n-r+t))}{n(n-1)\cdots(n-i-k)} \tag{2.16}$$

For the base of induction $k = -1$ we have $B_i^{(0)} = B_i$ (see section 1).

For the inductive step we observe that $B_i^{(k+1)} = B_i^{(k)} - B_{i+1}^{(k)}$ and apply the inductive hypothesis, that proves (2.16).

Finally, the diagonal entry $\mu_{k+1,k+1} = B_{k+1}^{(k+1)}$ is positive for $k < r < n-k$ because of (2.16), that proves Lemma 1.4 since $k+1 \leq l$. □

Acknowledgements

The author would like to take this opportunity to thank anonymous referees whose remarks have conduced to improve the exposition.

References

P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi & P. Pudlák (1996). Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc.* **73**, 1–26.

J. Bochnak, M. Coste & M.-F.Roy (1998). *Real algebraic geometry.* Springer-Verlag.

S. Buss, D. Grigoriev, R. Impagliazzo & T. Pitassi (1999). Linear gaps between degrees for polynomial calculus modulo distinct primes. In *31st Ann. ACM Symp. on Theory of Computing*, 547–556.

S. Buss, D. Grigoriev, R. Impagliazzo & T. Pitassi (2001). Linear gaps between degrees for polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.* **62**, 267–289.

S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. Razborov & J. Sgall (1996/1997). Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity* 256–298.

M. Clegg, J. Edmonds & R. Impagliazzo (1996). Using the Groebner basis algorithm to find proofs of unsatisfiability. In *28th Ann. ACM Symp. on Theory of Computing,*, 174–183.

D. Grigoriev (1998). Nullstellensatz lower bounds for Tseitin tautologies. In *39th Ann. IEEE Symp. on Foundations of Computer Science*, 648–652.

D. Grigoriev (2001). Linear Lower Bound on Degrees of Positivstellensatz Calculus Proofs for the Parity. *Theor. Comput. Sci* **259**, 613–622.

D. Grigoriev & N. Vorobjov (2001). Complexity of Null- and Positivstellensatz proofs. *Ann. Pure Appl. Logic* .

Impagliazzo, P. Pudlák & J. Sgall (1999). Lower bounds for polynomial calculus and the Groebner basis algorithm. *Computational Complexity* **8**, 127–144.

L. Lovász (1994). Stable sets and polynomials. *Discrete Mathematics* **124**, 137–153.

L. Lovász & A. Schrijver (1991). Cones of matrices and set-functions and 0–1 optimization. *SIAM J. Optimization* **1**, 166–190.

P. Pudlák (1999). On the complexity of the propositional calculus. In *Proceedings of Logic Colloquium '97*, 197–218. Cambridge Univ.Press.

A. Razborov (1998). Lower bounds for the polynomial calculus. *Computational Complexity* **7**, 291–324.

G. Stengle (1974). A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Math. Ann.* **207**, 87–97.

T. Stephen & L. Tunçel (1999). On representation of the matching polytope via semidefinite liftings. *Mathematics of Operations Research* **24**, 1–7.

Manuscript received

D.Grigoriev
IRM Université de Rennes-1
Campus de Beaulieu, 35042 Rennes
France
dima@maths.univ-rennes1.fr
http://www.maths.univ-rennes1.fr