Linear Lower Bound on Degrees of Positivstellensatz Calculus Proofs for the Parity

Dima Grigoriev*

Abstract

It is established a linear (thereby, sharp) lower bound on degrees of Positivstellensatz calculus refutations over a real field introduced in [GV99], for the Tseitin tautologies and for the parity (the *mod 2* principle). We use the machinery of the Laurent proofs developped for binomial systems in [BuGI 98], [BuGI 99].

keywords: Positivstellensatz calculus proofs, boolean binomial system, Tseitin tautologies

Introduction

In recent years there was an intensive activity in the research of algebraic proof systems ([BIK 96], [BuGI 98], [BuGI 99], [BuIK 96], [CEI 96], [G 98], [IPS 97]). The approach relies on the 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 $X_1^2 - X_1, \ldots, X_n^2 - X_n$ (so-called, Boolean case). Note that this problem is, in general, NP-complete.

*IRMAR, Université de Rennes, Campus de Beaulieu, 35042 Rennes, cedex France

The Nullstellensatz proof system (NS) was first considered in [BIK 96]. The aim of the system is to find the polynomials $g_1, \dots, g_k \in F[X_1, \dots, X_n]$ such that $1 = g_1 f_1 + \dots + g_k f_k$. 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 [BIK 96] a non-constant lower bound was proved, while in [G 98] a *linear* (and thus sharp) lower bound was proved.

In [CEI 96] a stronger proof system — polynomial calculus (PC) was introduced. Starting from axioms $f_1, \dots, f_k$, PC allows to derive from the already obtained polynomials $a, b \in F[X_1, \dots, X_n]$ more polynomials, 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 reach 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 [R 96] (see also [IPS 97] and [BuIK 96]). A linear lower bound for PC was proved in [BuGI 99]. Note that the latter bound is sharp.

In [GV 99] inequalities were involved along with equations into proof systems, in particular we assume that the input polynomials $f_1, \dots, f_k$ belong to $\mathbf{R}[X_1, \dots, X_n]$. 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 [P 98]). Another approach to systems of *linear* inequalities was undertaken in [LS 91], [L 94], [ST 98], where a derivation system was introduced which allows from *any* linear polynomial e, *already derived* linear inequalities $a_1 \geq 0, a_2 \geq 0$ and quadratic inequalities $p_1 \geq 0, p_2 \geq 0$, to derive quadratic inequalities $e^2 \geq 0,\ a_1 + a_2 \geq 0,\ a_1 a_2 \geq 0,\ p_1 + p_2 \geq 0$. In [P 98] one can find some remarks on the complexity of this Lovász-Schrijver procedure, in particular, an upper bound for the Pigeon Hole Principle which demonstrates an exponential gap between the complexity of cutting planes proofs and the Lovász-Schrijver procedure.

More precisely, following [GV 99], let a system of equations and inequalities

$$f_1 = \cdots f_k = 0,\ h_1 \geq 0, \ldots, h_m \geq 0. \tag{1}$$

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

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

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

Remark 1 *The minimal cone* $c(\emptyset)$ *consists of all sums of squares of polynomials.*

Remark 2 *Any element of* $c(h_1, \ldots, h_m)$ *can be represented in a form*

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

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

Two proof systems (which could be viewed as *static* and *dynamic*, respectively) introduced in [GV 99] rely on the following Positivestellensatz (see [BCR 87], [S 74]).

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

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

Definition 2 *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 *(denote it by $PS>$) for (1). 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 3 *Let a polynomial $f \in (f_1, \dots, f_k)$ be derived in PC from the axioms $f_1, \dots, f_k$, and a polynomial $h \in c(h_1, \dots, h_m)$ be derived, applying the rules (a), (b), (c) (see Definition 1), from the axioms $h_1, \dots, h_m$. Suppose that $f + h = -1$. This pair of derivations we call a* Positivstellensatz calculus refutation *(denote it by $PC>$) for (1). 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 1).

In [GV 99] a so-called telescopic system of equations due to Lazard-Mora-Philippon (see [Br 87]) is considered and an exponential lower bound on the degree of any its $PS>$ refutation (see definition 2) 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 [GV 99] for the stronger system of the $PC>$ refutations (see definition 3), 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 the present paper we prove a linear lower bound on the degree of $PC>$ refutations for the Tseitin tautologies (see Corollary 1 in section 3) and for the parity (see Corollary 2 in section 3), the proofs extend the argument from [BuGI 98], [BuGI 99]. They follow from the theorem in section 2 in which a lower bound on the degree of the $PC>$ refutations is established for Boolean binomial systems in terms of the Laurent proofs (see [BuGI 98], [BuGI 99] and also section 1 below). Let us mention that unlike the results of [BuGI 98], [BuGI 99] being valid over an arbitrary field F, the results of the present paper involving inequalities, make sense just over real fields.

1 Laurent proofs for Boolean Thue systems

Let F be a field.

A product of variables $m = X_1^{i_1} \cdots X_n^{i_n}$ is called a monomial, and am is called a term where a coefficient $a \in F^* = F - \{0\}$.

Definition 4 *(cf. [G 98], [BuGI 98], [BuGI 99]). A Boolean (multiplicative) Thue system over F in variables $X_1, \dots, X_n$ is a family $T = \{(a_1m_1, a_2m_2)\}$ of pairs of terms such that $(X_i^2, 1) \in T$ for any $1 \leq i \leq n$.*

Throughout first two sections we fix a Boolean Thue system T.

As in [BuGI 98], [BuGI 99] we consider *Laurent monomials* $l = X_1^{i_1} \cdots X_n^{i_n}$ with (possibly negative) integer exponents $i_1, \dots, i_n$. A product al where $a \in F^*$ is called a *Laurent term*. Laurent terms constitute a multiplicative group L. We define the degree $deg(l) = max\{\sum_{i_j>0} i_j, -\sum_{i_j<0} i_j\}$.

Definition 5 *(cf. [BuGI 98], [BuGI 99]). For any natural number d we construct recursively a subset $L_d \subset L$ of the terms of degrees at most d. As a base we include in L_d any term $a_1a_2^{-1}m_1m_2^{-1}$ from T (see definition 4), provided that its degree does not exceed d. As a recursive step for two Laurent terms $l_1, l_2 \in L_d$ we adjoin the product l_1l_2 in L_d if $deg(l_1l_2) \leq d$. Along with each $l_1 \in L_d$ we include $l_1^{-1} \in L_d$. Keep doing the recursion while augmenting L_d.*

Definition 6 *(cf. [BuGI 98], [BuGI 99]). Two terms t_1, t_2 are d-equivalent if $t_1 = lt_2$ for a certain $l \in L_d$.*

Lemma 1 *(cf. [BuGI 98], [BuGI 99]). (i) If t_1 is d-equivalent to t_2 then t_1X_j is d-equivalent to t_2X_j, $1 \leq j \leq n$.*

(ii) d-equivalence is a relation of equivalence on any subset of the set of all the terms of degrees at most d.

Definition 7 *(cf. [BuGI 98], [BuGI 99]). The refutation degree $D = D(T)$ is the minimal d such that L_d contains some $1 \neq a \in F^*$.*

By a support of a class of d-equivalence of terms we mean the set of their monomials. The following lemma comprises few properties of classes of d-equivalence of all the terms of degrees at most d.

Lemma 2 *(cf. [BuGI 98], [BuGI 99]). Let $d < D$. The supports of two classes of d-equivalence either coincide or disjoint. Two classes with the same support are obtained from one another by simultaneous multiplication of all the terms by an appropriate factor $b \in F^*$. Thus, any class could be represented by a vector $\{c_m\}_m$ where $c_m \in F^*$ and m runs over the support. Moreover, two classes with the same support has collinear corresponding vectors.*

As usual (cf. [G 98], [BuGI 98], [BuGI 99]) to each Thue system T one can attach a binomial ideal $P_T \subset F[X_1, \dots, X_n]$ generated by the binomials $a_1m_1 - a_2m_2$ (see definition 4).

Lemma 3 *(cf. [BuGI 98], [BuGI 99]). Let $d < D$. Assume that one can express a certain $f \in F[X_1, \dots, X_n]$ as a F-linear combination of binomials $t_1 - t_2$ where $t_1 = b_1m_3$, $t_2 = b_2m_4$ are d-equivalent and $deg(t_1), deg(t_2) \leq d$. Then such a linear combination could be chosen in a way that both monomials m_3, m_4 occur in f (this holds for all occurring binomials $t_1 - t_2$).*

Proof. Take any term am occurring in f. The vector of coefficients of a binomial $t_1 - t_2$ (which has just two nonzero coordinates) is orthogonal to the vector $\{1/c_m\}_m$ for the support of every class of d-equivalence (see lemma 2). Hence the vector of the coefficients of f is also orthogonal to the vector $\{1/c_m\}_m$. Therefore, there exists another term a_0m_0 occurring in f with m_0 from the support of the same class of d-equivalence as am. Due to lemma 2 am is d-equivalent to a suitable term $a_0^{'}m_0$. Then the polynomial $f - (am - a_0^{'}m_0)$ has less terms than f does, and we complete the proof of the lemma by induction on the number of terms in a polynomial. □

Lemma 4 *(cf. [BuGI 98], [BuGI 99]). If a polynomial f is deduced from P_T in the fragment of the polynomial calculus of a degree at most $d < D$ then f can be expressed as a suitable F-linear combination of binomials of the form*

t_1-t_2 for d-equivalent $t_1=b_1m_3, t_2=b_2m_4$ where $deg(t_1), deg(t_2) \leq d$. Moreover, such a linear combination could be chosen in a way that both monomials m_3, m_4 occur in f for any binomial t_1-t_2 from the linear combination.

The proof of the lemma proceeds by a direct induction along the inference of f in the PC. Herein after each inference step $g_1, g_2 \rightarrow g_1+g_2$ we apply lemma 3. For justifying any inference step $g_1 \rightarrow aX_ig_1$ we apply lemma 1(i). □

The previous lemmas are valid for an arbitrary (not necessary Boolean) Thue system (see [BuGI 98], [BuGI 99]), from now on we take into the account that T is just a Boolean Thue system.

Lemma 5 *Let $d < D/2$ and a Laurent term $al \in L_d$. Then $a \in \{-1, +1\}$.*

Proof. Since $al \in L_d \subset L_{D-1}$ we obtain $(al)^2 \in L_{D-1}$ because $deg(l^2) < D$. Let $l = X_1^{i_1} \cdots X_n^{i_n}$. Taking into the account that $X_1^2, \dots, X_n^2 \in L_{D-1}$, we conclude that $l^2 \in L_{D-1}$, hence $a^2 \in L_{D-1}$, i.e. $a^2 = 1$ by definition 7. □

2 Positivstellensatz calculus proofs for Boolean binomial systems

The results of the previous section are valid for an arbitrary field F (actually, over a commutative ring, with some modifications [BuGI 98], [BuGI 99]). In the sequel we suppose that F is a real field [BCR 87] (in particular, -1 cannot be represented as a sum of squares).

Assume now that we are given a $PC>$ refutation (see definition 3 and the remark after it) of a Boolean binomial ideal P_T (taking into account remark 1 from the introduction):

$$1+\sum_j h_j^2 = \sum_i f_i g_i \tag{2}$$

where the binomials $f_i = a_1m_1 - a_2m_2 \in P_T$ (cf. definition 4).

The main purpose of this section is to prove the following lower bound on the degree of the $PC>$ refutations.

Theorem. *The degree of any $PC >$ refutation of a Boolean binomial ideal P_T (over a real field) is greater or equal to $D/2$.*

Suppose that the right-hand side $\sum_i f_i g_i$ of (2) is deduced in the PC within a degree $d_0 < D/2$. Therefore, d_0 is an upper bound on the degree of $PC >$ refutations of P_T since $deg(h_j^2) \leq deg(\sum_i f_i g_i)$ (to show the latter inequality consider the highest with respect to the *deglex* monomial ordering term from all the polynomials h_j, then the coefficient at the square of this monomial in the sum $1 + \sum h_j^2$ should be positive).

Due to lemma 4 one can represent

$$\sum_i f_i g_i = \sum (b_1 m_3 - b_2 m_4) \tag{3}$$

where in each summand from the right-hand side the terms $b_1 m_3$ and $b_2 m_4$ are d_0-equivalent and occur in the left-hand side $\sum_i f_i g_i$, in particular, $deg(m_3), deg(m_4) \leq d_0$.

We introduce the following linear mapping ϕ from the space of polynomials of the degree at most d_0 to F. It suffices to define ϕ for all the monomials of the degree at most d_0. If a monomial is d_0-equivalent to a certain element $b \in F^*$ then ϕ sends this monomial to b, otherwise ϕ sends the monomial to zero. The mapping ϕ is correctly defined because b is unique, provided it does exist, due to lemma 1(ii) and to definition 7. Now let us consider the result of application of ϕ to the polynomial $\sum_i f_i g_i$. It can be calculated in two different ways: denote by $\Sigma_{(2)}$ the result of the evaluation of ϕ at the polynomial $1 + \sum_j h_j^2$ and by $\Sigma_{(3)}$ the result of evaluation of ϕ at the polynomial $\sum (b_1 m_3 - b_2 m_4)$. Evidently, $\Sigma_{(2)} = \Sigma_{(3)}$. If $b_1 m_3$ is d_0-equivalent to a certain $b \in F^*$ (see (3)) then $b_2 m_4$ is also d_0-equivalent to b (again due to lemma 1(ii)). Therefore, $\Sigma_{(3)} = 0$.

On the other hand, we will prove the following

Lemma 6 $\Sigma_{(2)} \geq 1$

which would lead to a contradiction with the supposition $d_0 < D/2$ and complete the proof of the theorem.

Proof of lemma 6. Fix for a time being one of the items $h = h_j = \sum_I a_I X^I$ (see (2)) where the latter sum contains q terms of the form $a_I X^I, a_I \in F^*, I \in \mathbf{Z}^n$ being a multiindex. Then $deg(X^I) \leq (1/2) deg(\sum f_i g_i)$; indeed, to show the latter again as above consider the highest (with respect to the *deglex* monomial ordering) term in all polynomials h_j, see (2). Hence $deg(X^I) \leq d_0/2 < D/4$.

Introduce an (undirected) graph Q with q vertices which correspond to the monomials X^I occurring in h (we identify a vertex with the corresponding I). The graph Q contains an edge (I, J) if and only if $bX^I X^J \in L_{d_0}$ for a pertinent $b \in F^*$. Since $(X^I)^2 \in L_{d_0}$ for any vertex I (cf. the proof of lemma 5), we treat also the loop (I, I) as an edge of Q.

Observe that after opening the parenthesis in the square $h^2 = h_j^2$, just the terms $2a_I a_J X^I X^J$ (in addition to the terms $(a_I X^I)^2$), where (I, J) is an edge of Q not being a loop, give contribution to the sum $\Sigma_{(2)}$ under consideration.

Let us show that the graph Q is a (disjoint) union of cliques. Indeed, assume that (I, J) and (J, K) are two edges of Q. Then $b_1 X^I X^J, b_2 X^J X^K \in L_{d_0}$ for suitable $b_1, b_2 \in F^*$. We have $(b_2 X^J X^K)^{-1} \in L_{d_0}$ and $b_1(b_2)^{-1} X^I (X^K)^{-1} \in L_{d_0}$ (see definition 5), hence $b_1(b_2)^{-1} X^I X^K \in L_{d_0}$ because $(X^K)^2 \in L_{d_0}$ and $deg(X^I X^K) \leq d_0$. Thus, (I, K) is also an edge of Q.

Fix for a time being a clique C of Q. Our next purpose is to prove that the contribution Σ_C of the terms corresponding to the egdes of C into the sum $\Sigma_{(2)}$ is non-negative. Note that the contribution of the term $(a_I X^I)^2$ into $\Sigma_{(2)}$ equals to a_I^2 since $(X^I)^2 \in L_{d_0}$. For every edge (I, J) of C either $X^I X^J \in L_{d_0}$ holds (in this case we label (I, J) by 1) or $-X^I X^J \in L_{d_0}$ holds (in this case we label (I, J) by -1) due to lemma 5. For each triple of vertices I, J, K of C the product of the labels of three edges $(I, J), (J, K), (K, I)$ equals to 1 (see definition 5). Therefore, one can partition the vertices of C into two parts V_1, V_2: if an edge links two vertices from the same part then it is labeled by 1, otherwise it is labeled by -1. Hence $\Sigma_C =$

$$\sum_{I \in V_1 \cup V_2} (a_I)^2 + 2 \sum_{I_1, J_1 \in V_1} a_{I_1} a_{J_1} + 2 \sum_{I_2, J_2 \in V_2} a_{I_2} a_{J_2} - 2 \sum_{I_1 \in V_1, I_2 \in V_2} a_{I_1} a_{I_2}$$

$$= (\sum_{I_1 \in V_1} a_{I_1})^2 + (\sum_{I_2 \in V_2} a_{I_2})^2 - 2(\sum_{I_1 \in V_1} a_{I_1})(\sum_{I_2 \in V_2} a_{I_2}) \geq 0.$$

Thus, the contribution into the sum $\Sigma_{(2)}$ of each h_j from the left-hand side of (2) is non-negative. □

3 Lower bounds on Positivstellensatz calculus refutations for the Tseitin tautologies and the parity

The purpose of this section is to prove lower bounds on the degrees of $PC_>$ refutations for Tseitin tautologies (see [T 68], [U 95], [G 98], [BuGI 98], [BuGI 99]) and for the parity (or *mod 2* principle, see [BuGI 98], [BuGI 99]).

To describe Tseitin tautologies *mod 2* (following [BuGI 98], [BuGI 99] we denote them by $TS_k(2)$) we start with an (undirected) graph G. To each its node v a charge $u_v \in \{-1, 1\}$ is assigned with the property that $\prod_v u_v = -1$. Besides, we assign to each edge e of G a variable X_e.

We construct a Boolean Thue system $T = T_G$ (see definition 4) according to these data. The system T_G contains a pair of terms (for each node v) $(X(v) = u_v \prod X_e, 1)$ where the product ranges over all the edges e incident to v (apart from the Boolean pairs $(X_e^2, 1)$).

One can obviously deduce in T that $\prod_v u_v = 1$ and thereby in the PC the element $1 - \prod_v u_v \in F^*$ (which actually equals to 2) from the binomial ideal P_T (see section 2).

Any Laurent monomial in the variables $\{X_e\}_e$ could be reduced using the Boolean pairs to the (uniquely defined) multilinear monomial (we call it reduced). By the *pseudo-degree* of a monomial we mean the number of variables which occur in its reduction. Observe that the pseudo-degree of a Laurent monomial does not exceed the double degree of this Laurent monomial (see section 1).

From now on we assume that $G = G_k$ is an *expander* [LPS 88], [M 88] with k nodes and being r-regular (r will be a constant, one could take, say $r = 6$ [LPS 88], [M 88]). That means that for any subset S of the set of the nodes of G the number of adjacent to S nodes in G is at least $(1 + \epsilon(1 - |S|/k))|S|$ for an appropriate constant $\epsilon > 0$. The corresponding to G_k Boolean Thue system we denote by $TS_k(2)$.

Any Laurent monomial in $\{X_e^2\}_e, \{X(v)\}_v$ could be also (uniquely) reduced invoking the Boolean pairs, to a multilinear monomial in $\{X(v)\}_v$ (obviously, this reduction does not change the pseudo-degree). By a *weight* of such a Laurent monomial we mean the number of $X(v)$ which occur in the reduced product.

The following lemma is similar to lemma 2 [G 98] (see also [BuGI 98], [BuGI 99]) and its item (i) justifies the correctness of the described reduction and of the weight because $\prod_v X(v) = -1 \neq 1$.

Lemma 7 *(i) Any reduced monomial in $\{X_e^2\}_e, \{X(v)\}_v$ which is equal to an element of the form am^2 where $a \in F^*$ and m is a monomial, is either* 1 *or $\prod_v X(v) = -1$;*

(ii) For any $1/2 \geq \epsilon_1 > 0$ there exists $\epsilon_0 > 0$ such that any reduced monomial in $\{X_e^2\}_e, \{X(v)\}_v$ with the weight between $\epsilon_1 k$ and $(1-\epsilon_1)k$ has the pseudo-degree at least $\epsilon_0 k$.

Proof. (i) If not all $X(v)$ occur in the reduced (non-empty) product U then (due to the connectedness of expanders) there is an edge $e = (v_1, v_2)$ of G such that $X(v_1)$ occurs in U and $X(v_2)$ does not occur in U. Hence U contains X_e with the exponent 1 and thereby, could not be of the form am^2.

(ii) Denote by S the set of nodes v of G such that $X(v)$ occurs in U. Then applying to S the property of the expanders, we conclude that there are at least $\epsilon_0 k$ edges of G with one endpoint in S and another endpoint not in S for a suitable ϵ_0. These edges give a contribution to the pseudo-degree of U. □

The following lemma is similar to lemma 5.9 [U 95] and to lemma 4 [G 98] (see also [BuGI 98], [BuGI 99]).

Lemma 8 *The refutation degree $D = D(TS_k(2))$ is greater than $\Omega(k)$.*

Proof. By definition 7 there exists a chain of Laurent monomials $l_1, \dots, l_N$ in $\{X_e^2\}_e, \{X(v)\}_v$ such that $1 \neq l_N \in F^*$ and that each l_j is either one of $\{X_e^2\}_e, \{X(v)\}_v$, either $l_{j_1}^{-1}$ or $l_{j_1} l_{j_2}$ for some $j_1, j_2 < j$, moreover the degree of each l_j does not exceed D. Then the pseudo-degrees of l_j do not exceed $2D$ (see above). Due to lemma 7(i) $l_N = -1$ and the weight $w(l_N) = k$. Since $w(X(v)) = 1$ and $w(l_j) \leq w(l_{j_1}) + w(l_{j_2})$, we conclude that there exists $1 < j_0 < N$ for which $(1/3)k \leq w(l_{j_0}) \leq (2/3)k$. Then lemma 7(ii) implies that the pseudo-degree of l_{j_0} is greater or equal to $\epsilon_0 k$. □

Lemma 8 and the theorem (see section 2) entail the following linear (thereby, sharp) lower bound on the degree of $PC >$ refutations for the Boolean binomial system corresponding to Tseitin tautologies.

Corollary 1 *The degree of any $PC >$ refutation of the Boolean binomial system $P_{TS_k(2)}$ is greater than $\Omega(k)$.*

Following [BuGI 98], [BuGI 99] we consider (the negation of) *mod 2* principle (or the parity) as a system of equations in $\binom{n}{2}$ variables X_e where $e \subset \{1, \dots, n\}, |e| = 2$, denoted by MOD_2^n:

$X_e^2 = X_e; X_e X_f = 0$ for every e, f such that $e \neq f, e \cap f \neq \emptyset$;

$1 = \sum_{i \in e} X_e$ for each $i \in \{1, \dots, n\}$.

Obviously, MOD_2^n is feasible if and only if n is even.

Note that MOD_2^n is not a binomial system unlike $P_{TS_k(2)}$.

Definition 8 *(see [BuGI 98], [BuGI 99]). Let $P = P(x_1, \dots, x_n), Q = Q(y_1, \dots, y_m)$ be two sets of polynomials. Then P is (d_1, d_2)-reducible to Q if for every $1 \leq i \leq m$ there exists a polynomial $s_i(x_1, \dots, x_n)$ of a degree at most d_1 such that there exists a degree d_2 derivation in the PC of the polynomials $Q(s_1, \dots, s_m)$ from the polynomials P.*

Lemma 9 *(cf. [BuGI 98], [BuGI 99]). Suppose that P is (d_1, d_2)-reducible to Q. Then if there is a degree d_3 $PC>$ refutation of Q then there is a degree $max\{d_2, d_3 d_1\}$ $PC>$ refutation of P.*

Lemma 10 *(see [BuGI 98], [BuGI 99]). For all k the Boolean binomial system $P_{TS_k(2)}$ is $(4r, 4r)$-reducible to $MOD_2^{k(1+2r)}$ (where r denotes the valency of the expander G_k, one could take $r = 6$, see above).*

Lemmas 9, 10 and Corollary 1 imply the following linear (thereby, sharp) lower bound on the degree of $PC>$ refutations for the parity.

Corollary 2 *(cf. [BuGI 98], [BuGI 99]). The degree of any $PC>$ refutation of MOD_2^k is greater than $\Omega(k)$.*

References

[BIK 96] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák *"Lower bounds on Hilbert's Nullstellensatz and propositional proofs,"* Proc. London Math. Soc., V. 73, 1996, 1–26.

[BCR 87] J. Bochnak, M. Coste, and M.-F.Roy *"Real algebraic geometry,"* Springer-Verlag, 1998.

[Br 87] D. Brownawell *"Bounds for the degrees in the Nullstellensatz,"* Ann. Math., 1987, V. 126, 577–591.

[BuGI 98] S. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi *"Linear gaps between degrees for polynomial calculus modulo distinct primes,"* Proc. 31st Ann. ACM Symp. on Theory of Computing, 1999, 547–556.

[BuGI 99] S. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi *"Linear gaps between degrees for polynomial calculus modulo distinct primes,"* To appear in J. Comput. Syst. Sci.

[BuIK 96] S. R. Buss, R. Impagliazzo, J. Krajíček, and P. Pudlák, A. Razborov, and J. Sgall *"Proof complexity in algebraic systems and bounded depth Frege systems with modular counting,"* Computational Complexity, 6, 1996/1997, 256–298.

[CEI 96] M. Clegg, J. Edmonds, and R. Impagliazzo *"Using the Groebner basis algorithm to find proofs of unsatisfiability,"* Proc. 28th Ann. ACM Symp. on Theory of Computing, 1996, 174–183.

[G 98] D. Grigoriev *"Nullstellensatz lower bounds for Tseitin tautologies,"* Proc. 39th Ann. IEEE Symp. on Foundations of Computer Science, 1998, 648–652.

[GV99] D. Grigoriev and N. Vorobjov *"Complexity of Null- and Positivstellensatz proofs,"* submitted to Ann. Pure Appl. Logic

[IPS 97] R. Impagliazzo, P. Pudlák, and J. Sgall *"Lower bounds for polynomial calculus and the Groebner basis algorithm,"* Computational Complexity, V. 8, 1999, 127–144.

[L 94] L. Lovász *"Stable sets and polynomials,"* Discrete Mathematics, V. 124, 1994, 137–153.

[LS 91] L. Lovász and A. Schrijver *"Cones of matrices and set-functions and 0–1 optimization,"* SIAM J. Optimization, V. 1, 1991, 166–190.

[LPS 88] A. Lubotzky, R. Phillips and P. Sarnak *"Ramanujan graphs,"* Combinatorica, V. 8, 1988, 261–277.

[M 88] G. Margulis *"Explicit group-theoretical construction of combinatorial schemes and their applications to the design of expanders and concentrators,"* Problems Inform. Transm., V. 24, 1988, 39–46.

[P 98] P. Pudlák *"On the complexity of the propositional calculus,"* Preprint, 1998.

[R 96] A. Razborov *"Lower bounds for the polynomial calculus,"* Computational Complexity, V. 7, 1998, 291–324.

[S 74] G. Stengle *"A Nullstellensatz and a Positivstellensatz in semialgebraic geometry,"* Math. Ann., V. 207, 1974, 87–97.

[ST 98] T. Stephen and L. Tunçel *"On representation of the matching polytope via semidefinite liftings,"* Preprint, 1998.

[T 68] G. Tseitin *"On the complexity of derivations in propositional calculus,"* in: Studies in mathematics and mathematical logic, V. 2, 1968, 115–125.

[U 95] A. Urquhart *"The complexity of propositional proofs,"* Bull. Symb. Logic, V. 1, 1995, 425–467.