Electronic Colloquium on Computational Complexity, Report No. 17 (2013)

A Short Excursion into Semi-Algebraic Hierarchies

Pratik Worah

January 23, 2013

Abstract

This brief survey gives a (roughly) self-contained overview of some complexity theoretic results about semi-algebraic proof systems and related hierarchies and the strong connections between them. The article is not intended to be a detailed survey on "Lift and Project" type optimization hierarchies (cf. Chlamtac and Tulsiani [12]) or related proof systems (cf. Grigoriev et al. [16]).

1 Introduction and Motivation

In the past decade a lot of work has been done on hierarchies based on Linear and Semidefinite Programs (LPs and SDPs) in areas as diverse as Proof Complexity, Approximation Algorithms and even Probability Theory. In this section we briefly mention some recent highlights which will motivate further exploration of the limitations of such optimization based hierarchies or (propositional) proof systems[1].

A *propositional proof system* is any polynomial time computable function

$$P : \{0,1\}^* \xrightarrow{onto} TAUT,$$

where $TAUT$ is the set of boolean tautologies (or a subclass of boolean tautologies). If $P(x) = \varphi$ for any string x then x is called a P-proof of φ. Cook and Reckhow showed that $NP = coNP$ if and only if there exists a proof system for $TAUT$, such that every input x has a polynomial sized proof. Therefore it is a natural question to show that weaker proof systems, for example Resolution, do not have subexponential sized refutations for some unsatisfiable families of formulae. It is known that PHP and Tseitin Tautologies do not have subexponential sized refutations in Resolution [6] and Polynomial Calculus [5]. However, it turns out that both these principles have polynomial sized proofs in the Lovász-Schrijver (LS) type proof systems.

Theorem 1.1 ((informal) Pudlák) *PHP_n^{n+1} has polynomial sized refutations in LS.*

Theorem 1.2 ((informal) [16]) *There is a polynomial sized refutation of Tseitin Tautologies on d-regular graphs in LS^{d+2}. LS^{d+2} is a generalization of the usual LS proof system to allow degree $d+2$ polynomials instead of just quadratic polynomials.*

Such strong results provide one reason to explore the limitations of LS and related proof systems or hierarchies.

[1] We use the words hierarchy and proof system interchangeably since they are roughly synonymous when dealing with a boolean k-CSP - the running example in this article.

ISSN 1433-8092

However, size is not the only important parameter for such hierarchies. For 0-1 optimization problems (like MAX-CSP) one can design approximation algorithms based on encoding the problem as an Integer Program (IP), solve its LP/SDP relaxation to obtain an optimal fractional solution and then round the fractional solution to an integer solution. While we know approximating MAX-3-CSPs is NP-hard, a recent SDP rounding algorithm by Barak et al [4] uses the Lasserre hierarchy, which is stronger than the basic LS hierarchy, to approximate the optimal value of some MAX-2-CSPs.

Theorem 1.3 ((informal) [4]) *Given a MAX-2-CSP instance F on alphabet $[k]$, let r_τ denote the number of eigenvalues greater than τ for the normalized adjacency matrix of the constraint graph of F. There exists a constant c such that for every $\varepsilon > 0$ and $r \geq \frac{k}{\varepsilon^c} r_\tau$, the optimal value of the objective function for the r^{th} level Lasserre relaxation of F is within ε of the the optimal value of F. Moreover there is a polynomial time rounding algorithm that finds the assignment corresponding to the approximate optimum given the Lasserre SDP solution.*

Such rounding algorithms and the the papers that build upon it [3, 19] give another reason to study the limitations of such hierarchies. The reasonable way to proceed here is to lower bound the worst case integrality gap i.e., the maximum of the ratio between the optimal fractional and integer solution over all problem instances, of the Lasserre relaxation of the encoded LP / SDP - since it is unreasonable to expect that one would always know the value of the optimal integer solution in advance. Such lower bounds are now well studied for most LP and some SDP hierarchies [9, 1, 24, 11, 7] and we will sketch their relation to lower bounds for proof systems via the MAX-CSP problem.

2 Preliminaries and Definitions

In this section we briefly remind the reader of some relevant basic definitions and provide a brief overview of the type of lower bound problems which we will discuss later.

A polytope is a set of the form $\{x \in \mathbb{R}^n : Ax \geq b, A \in \mathbb{R}^{m \times n}, b \in \mathbb{R}^n\}$. Throughout we assume that the matrix A has size polynomial in n and is explicitly given. A Linear Program optimizes a linear objective function $c^T x$ over some polytope P and therefore is of the form:

$$\max_x \; c^T x \quad s.t.\; Ax \geq b.$$

In addition we will always assume that the polytope P lies in the unit cube of appropriate dimension. The feasibility of a linear program can be decided in polynomial time and therefore the optimization problem can be solved in polynomial time. A Semidefinite Program is of the form:

$$\max_X \; C \cdot X \quad s.t.\; A_i \cdot X \geq b_i \; \forall i \in [k],\; X \succeq 0,$$

where $A_i, X \in \mathbb{R}^{n \times n}$ and $\cdot$ denotes the usual inner product. Hence an SDP reduces to an LP whenever the matrix X is diagonal. There is no known algorithm to decide the feasibility of a SDP in polynomial time but one can find the optimal solution to a SDP in polynomial time upto any given level of accuracy.

2.1 CSPs and their Representations

Definition 2.1 *Given a boolean predicate $f : \{0,1\}^k \to \{0,1\}$ we define MAX-k-CSP(f) as the following optimization problem F:*

$$\max_{x\in\{0,1\}^n} \sum_{i\in[m]} f_i(x), \tag{2.1}$$

where f_i denotes an instance of f on some k variables chosen from the n 0-1 variables such that some of the input variables of f may be negated.

Throughout we will assume $k \geq 3$. We will encode the above optimization problem as a LP or SDP in the next section. For the purpose of proving integrality gaps F will usually consist of randomly chosen instances of f_i. It is known that such random instances are very unsatisfiable as long as the number of constraints m exceeds a certain threshold δn. It is therefore natural to study the complexity of refuting the CSP(f) formula corresponding to F:

$$\bigwedge_{i\in[m]} f_i(x). \tag{2.2}$$

We will soon see that lower bounds for the later problem imply integrality gaps for the former problem and the converse will also hold in some cases. In the remainder of this subsection we consider the example of MAX-k-SAT and show how to encode it as set of contradicting axioms to a proof system which manipulates inequalities or equalities.

A MAX-k-SAT instance F consists of a conjunction of clauses each of the form $\bigvee_{i\in[k]} l_i$. Hence to encode the axioms for F it suffices to provide an encoding for the clauses.

Encoding with *linear inequalities* or simply the *linear encoding:* Given a clause $C := \bigvee_{i\in[k]} l_i$ we encode it as the inequality $L_C := \sum_{i\in[k]} \ell_i \geq 1$, where $\ell_i := 1 - x_i$ if $l_i = \neg x_i$ and $\ell_i := x_i$ otherwise. The ℓ_i are variables in $\mathbb{R}$. Observe that both C and L_C have the same set of satisfying solutions in $\{0,1\}^k$.

Encoding with *polynomial equalities* or simply the *product encoding:* Given a clause $C := \bigvee_{i\in[k]} l_i$ we encode it as the equality $P_C := \Pi_{i\in[k]}\ell_i = 0$, where $\ell_i := x_i$ if $l_i = \neg x_i$ and $\ell_i := 1 - x_i$ otherwise. Usually, for our purposes, the ℓ_i are variables in $\mathbb{R}$. Observe that both C and P_C have the same set of satisfying solutions in $\{0,1\}^k$.

Semialgebraic proof systems, like LS, manipulate inequalities starting from the linear encoding of the axioms. The closely related algebraic proof systems - the Nullstellensatz and Polynomial Calculus (PC) manipulate equalities starting from a product encoding of the axioms. See the survey by Pitassi [20] for a review of proof complexity results related to the later.

2.2 Hierachies and Proof Systems

In this subsection we briefly review "lift and project" hierarchies and proof systems based on them. Given a polytope P in $[0,1]^n$ with m facets, it is sometimes possible to introduce more variables and obtain another polytope Q, the *extension* (also lift) of P, such that Q lies in $[0,1]^N$ $(N > n)$ but has M facets for some $M < n$, and the *projection* of Q to the original n dimensions is P. The number of facets of Q is the extension complexity of Q and some recent papers [14, 8] also study lower bounds on extension complexity.

Lovász and Schrijver made an important observation when the polytope P corresponds to an LP relaxation of some 0-1 integer polytope P_I. Given any polytope P they define a hierarchy of nested

polyopes, via their systematic lift and project operations, which always converges to P_I in at most n such operations. Moreover they constructed separation oracles for the intermediate polytopes in their hierarchy which allows one to efficiently optimize LPs over the nested polytopes obtained within a few lift and project steps (for details see [12]).

Definition 2.2 (see [12]) *Given a polytope $P^r \subseteq P$ obtained after r rounds of LS lift and project, inductively define P^{r+1} as the polytope bounded by* linear *inequalities of the form:*

$$\sum_{i=1}^{n} \alpha_i h^{(r)}(x) x_i + \sum_{i=1}^{n} \beta_i g^{(r)}(x)(1 - x_i) + \sum_{i=1}^{n} \gamma_i (x_i^2 - x_i) \geq 0, \tag{2.3}$$

where $h^{(r)}(x) \geq 0$ and $g^{(r)}(x) \geq 0$ are linear inequalities valid for P^r, $\alpha_i, \beta_i \in \mathbb{R}^+$ and $\gamma_i \in \mathbb{R}$.

Note that $P^0 = P$ and r is the *rank* of P^r. It is known that $P^r = P_I$ for some $r \leq n$. By restricting the final form of the inequality in Equation 2.3 to be linear, we have implicitly defined P^{r+1} as the projected polytope obtained from P^r after one step of lift and project. If we map products of variables $x_i x_j \to x_{ij}$ then any quadratic inequality which can be expressed in the form of Equation 2.3 corresponds to a linear inequality (in $\binom{n}{2}$ variables) of the (LS) lifted polytope Q^r obtained from P^r. The corresponding LS proof system may be formally defined as follows.

Definition 2.3 ([16]) *Given a set P of linear inequalities on the variables $\{x_1, ..., x_n\}$ and axioms $x_i^2 - x_i = 0$, we have the following inference rules for LS:*

1. $\frac{p \geq 0}{p \cdot q \geq 0}$ *where $deg(pq) \leq 2$ and $q \in \{x_i, 1 - x_i : i \in [n]\}$.*
2. $\frac{p \geq 0 \quad q \geq 0}{\alpha p + \beta q \geq 0}$ *for $\alpha, \beta \in \mathbb{R}^+$.*

A valid refutation of P must obtain the contradiction $-1 \geq 0$.

Various strengthenings of the LS hierachy have been defined. The LS_+ hierarchy works with SDP relaxations and Equation 2.3 is modified to allow addition of squares of arbitrary linear forms. Another strengthening of LS is the Sherali-Adams (SA) hierarchy in which there are no intermediate projection steps i.e., one is allowed to multiply the original inequalities with multipliers $\Pi_I x_i \Pi_J (1 - x_j)$, to obtain the SA lifted polytope in one shot. The SA (also static-LS) proof system[2] may be defined as:

Definition 2.4 ([16]) *Given a set P of linear inequalities on the variables $\{x_1, ..., x_n\}$ and axioms $x_i^2 - x_i = 0$. A valid SA refutation consists of positive linear combination of the terms $\varphi_{I,J} = s_{I,J} \cdot \Pi_{i \in I} x_i \Pi_{j \in J} (1 - x_j)$ where I and J are multisets of variable indices and $s_{I,J}$ is an axiom. A valid refutation is obtained by deriving*

$$\sum_{l} \omega_l \cdot \varphi_{I_l, J_l} \quad = \quad -1 \tag{2.4}$$

where each $\omega_l \in \mathbb{R}^+$.

[2]Formally SA (equivalently static-LS) may not even be a proof system since even a simple verification of validity of the certificate may require exponential time [16]. But for lower bound purposes these systems are no less interesting.

Remark 2.5 *Observe that the LS is a* dynamic *proof system since it derives a refutation in a step by step manner (like Resolution and Polynomial Calculus), while SA is a* static *proof system since it derives the refutation in one shot (like the Nullstellensatz). The division into dynamic and static seems to play some role as far as lower bound methods are concerned.*

Similar to LS one can strengthen static-LS to static-LS_+. We will define the stronger Lasserre hierarchy and Positivstellensatz Calculus in the upcoming sections.

2.3 Measures of Complexity

We have already defined *rank* for the LS hierarchy. The *rank* of an LS refutation is analogously defined as the maximum number of applications of the first inference rule along any path in the proof DAG. Note that for any linear encoding of an unsatisfiable MAX-k-CSP instance the LS hierarchy rank and LS proof system rank are equivalent by Farkas' lemma and similarly for LS_+. The *rank* of a static-LS refutation is just the maximum degree of summands in Equation 2.4. Like other dynamic proofs, the *size* of an LS refutation is just the number of lines in the refutation and the *size* of a static-LS refutation is the number of summands in Equation 2.4. The surveys [16] and [12] have a more detailed discussion on this.

Each of these measures has some physical significance. For example, optimization over the rank r polytope in the LS, SA (and other similar hierarchies) takes $n^{O(r)}$ time. The LS rank lower bounds the static-LS rank and also the logarithm of LS (and static-LS) size. No relation seems to be known between LS and static-LS size. Since the size lower bounds would hold against any optimization algorithm captured by the model, as opposed to the fixed $n^{O(r)}$ algorithms, they are more difficult to obtain. The same measures can also be defined for LS_+ and static-LS_+.

3 Overview of Proof Techniques in the Area

We now provide an overview of techniques in the lower bounds for the MAX-k-CSP(P) problem (Equation 2.1), where $P : \{0,1\}^k \to \{0,1\}$ is a boolean predicate, and the closely related problem of proving lower bounds for random instances of CSP(P) (Equation 2.2). As far as basic techniques in the proofs of integrality gaps and rank lower bounds for SA and Lasserre hierachies are concerned, the proofs for just the case of MAX-k-XOR provide a fairly complete picture. While we do know some gaps for problems like finding the maximum independent set or the minimum vertex cover in graphs, much can be shown via involved reductions from gaps of MAX-k-XOR (see [1, 23, 26] and exceptions in [11]).

3.1 Resolution and Polynomial Calculus

We take a short detour through two techniques previously used for weaker proof systems - Resolution and Polynomial Calculus, for their influence on lower bound proofs for static proof systems.

The Resolution refutations have propositional clauses as lines and a valid refutation uses the inference rule:

$$\frac{C_1 \vee \neg x \quad x \vee C_2}{C_1 \vee C_2}$$

to derive an empty clause. The *size* (S) of a refutation is the number of lines in it and the *width* (w) of a refutation is the maximum number of variables in a clause in the refutation. Ben-Sasson

and Wigderson [6] related size and width of a refutation π as follows:

$$w(\pi) \leq w_0(\pi) + \sqrt{n \log S},$$

where w_0 is the maximum of the width of the axioms and n the number of variables. Therefore lower bounding the width of a Resolution refutation also serves to lower bound its size. In the case of random instances of CNF-SAT they prove a linear lower bound on the width of any Resolution refutation by showing that high (boundary) expansion of the constraint graph of the instance i.e. the natural variable vs constraint bipartite graph, implies the refutation has a wide clause. They generalized their proof to random instances of CSP(P), where $P : \{0,1\}^k \to \{0,1\}$ is any *sensitive* predicate (For eg. XOR, which can be satisfied by flipping only a few bits of any unsatisfying assignment). Immediately afterwards Ben-Sasson and Impagliazzo [5] used a similar technique to prove linear lower bounds for the degree in the algebraic proof system - Polynomial Calculus. The Polynomial Calculus (PC) [13] is a dynamic version of the Nullstellensatz, where the lines are polynomial equalities from the ring $S_n(\mathbb{F}) = \mathbb{F}[x_1, .., x_n]/\{x_i^2 - x_i : i \in [n]\}$. Sometimes the rule $x_i^2 - 1 = 0$ may be substituted for $x_i^2 - x_i = 0$ and these axioms allow us to ignore issues about the completeness of the underlying field $\mathbb{F}$. The inference rules for PC are:

$$\frac{p = 0 \quad q = 0}{\alpha p + \beta q = 0}, \qquad \frac{p = 0}{x \cdot p = 0},$$

where $p, q \in S_n(\mathbb{F})$ and $\alpha, \beta \in \mathbb{F}$. A valid refutation shows $1 = 0$. The *degree* (d) of a refutation is the maximum degree among the lines of the refutation and the *size* (S) of a refutation is number of monomials in the refutation. Size vs degree trade-offs are also known for PC [13] and they chronologicaly preceeded the size-width trade-offs for Resolution. For an instance of CSP(P), PC encodes the axioms in the product encoding, typically over $\mathbb{R}$ in relation to semialgebraic proof systems. In [5], the authors use the ideas from [6] to show linear lower bounds for the degree in any PC refutation of random instances of CNF-SAT over $\mathbb{F} \neq \mathbb{F}_2$. They actually show the lower bound when the axioms lead to binomials[3] and from it deduce the lower bound for CNF-SAT by a simple reduction. We will illustrate the importance of these ideas for Lasserre rank lower bounds and integrality gaps in the next section.

The lower bounds for PC degree when the predicate P in CSP(P) does not translate to binomials were more involved and used different techniques [2]. Given a random instance F of a CSP(P), as in Equation 2.2, the f_i are polynomials in $S_n(\mathbb{F})$ derived from P which is assumed to be *immune* (a fairly general class of predicates) and suppose one wants to exhibit a degree d lower bound on PC refutations of F. The main idea in [2] is to construct an operator $R_d : S_{n,d}(\mathbb{F}) \to S_{n,d}(\mathbb{F})$ defined on monomials of degree at most d and linearly extended to the degree d fragment of the ring $S_n(\mathbb{F})$ such that:

1. $V_d(F) \subseteq Ker(R_d) \subset S_n(\mathbb{F})$, where $V_d(F)$ is a degree d pseudoideal of F (cf [13, 2]).
2. $R_d(x_j t) = R_d(x_j R_d(t))$, where t is a monomial of degree at most $d - 1$.

Intuitively, R_d would send the LHS of any degree d PC refutation to zero while the RHS of the refutation would remain non-zero thus giving us a contradiction to the existence of such a refutation. The operator R_d in [2] is constructed by restricting the classical reduction operator i.e $R_I : S_n(\mathbb{F}) \to S_n(\mathbb{F})$, which gives the unique remainder upon reduction by the Groebner basis of

[3] A *Binomial Ideal* is any ideal generated by binomials, which are polynomials consisting of a linear combination of two monomials. For example, the product encoding of the axioms of XOR with $x^2 = 1$ gives binomials.

the ideal $I := \langle \{f_i\}_{i=1,..,r} \rangle$, to the degree d fragment of S_n. Of course there are many ideals in S_n, and hence many R_Is, and to fix the value of $R_d(t)$ for a term $t \in S_n$ one has to choose which R_I to use. Using an involved argument relying on immunity and expansion properties of F, [2] get around this problem and show *local consistency* among the R_Is i.e.

$$R_{\langle \{f_i\}_{i_1,..,i_r} \rangle}(t) = R_{\langle \{f_i\}_{i_1,..,i_\nu} \rangle}(t)$$

when the monomial t has small enough, but still $\Omega(n)$, degree and the small set of generators $\{f_i\}_{i_1,..,i_\nu}$ depends only on the term t. Therefore $R_d(t)$ is chosen locally i.e. depending only on t, with respect to some small enough, in the number of generators, ideal I. The local consistency of R_Is will ensure properties 1 and 2 above for R_d. A similar, but somewhat simpler, approach works for proofs of rank lower bounds in static hierarchies. In particular, proofs of SA integrality gaps use a similar local consistency lemma but with functionals.

We conclude this subsection by noting that width in Resolution and degree in PC play a role analogous to rank in hierarchies and proof systems and such evidence is given by [25, 21]. However, we still do not know any size-rank trade-offs for LS type dynamic proof systems.

3.2 Static Hierachies and Proof Systems

We will consider the example of integrality gaps for a random instance F of MAX-k-XOR in the SA hierarchy [7]. For clarity we write down the SA LP correponding to MAX-k-XOR (Equation 2.1 instantiated with XOR) instance F consisting of variables $V = \{x_1, .., x_n\}$ and XOR constraints $C = \{C_i : \{0,1\}^k \to \{0,1\} : i \in [m]\}$. The variables of the LP obtained after r rounds of SA hierarchy are: $x_{S,A}$, where $S \subseteq V, |S| \leq r$ and $A \in \{0,1\}^r$. Intuitively, $x_{S,A}$ is 1 if $S \to A$ and 0 otherwise. Let S_{C_i} be the set of variables in constraint C_i then the LP after r rounds of SA is given below. Note that the usual definition of SA has variables of the form x_S but not $x_{S,A}$ but it is easier

Sherali-Adams LP for MAX-k-CSP(f)

$$\begin{aligned}
\text{maximize} \quad & \sum_{i=1}^{m} \sum_{A \in \{0,1\}^{T_i}} C_i(A) \cdot x_{(T_i,A)} & & \\
\text{subject to} \quad & x_{(\emptyset,\emptyset)} = 1 & & \\
& \sum_{j \in \{0,1\}} x_{(S \cup \{i\}, A \circ j)} = x_{(S,A)} & & \forall S \text{ s.t. } |S| < r,\ \forall i \notin S, A \in \{0,1\}^S \\
& x_{(S,A)} \geq 0 & & \forall S \text{ s.t. } |S| \leq r,\ \forall A \in \{0,1\}^S
\end{aligned}$$

to write the objective function of the LP in the above formulation. One can think of $x_S \rightsquigarrow x_{S,\{1,..,1\}}$ and use induction on the size of S to see that with respect to SA rank and integrality gaps the two translations are equivalent.

Theorem 3.1 ((informal) [7]) *For a random instance F of MAX-k-XOR, the SA LP (above) has an integrality gap of $2 - \varepsilon$ w.h.p. even after some $\Omega(n)$ rounds.*

For the sake of exposition we will illustrate the rank lower bound proofs with respect to SA i.e. static-LS, proof system and not with the LP formulation.

Remark 3.2 *A rank lower bound on SA for a linear encoding of F already implies an integrality gap of $2 - \varepsilon$ for F.*

This follows because at most $1/2 + \varepsilon$ of the constraints in F are simultaneously satisfiable by 0-1 assignments and (by Farkas lemma) the rank lower bound in the SA proof system implies that there is an obstruction, in the form of a fractional point, which satisfies all the lifted constraints of F after many rounds of SA lifts. Hence it will suffice to sketch a rank lower bound for F instead of an integrality gap for F.

3.2.1 Locally Consistent Measures

First we define families of locally consistent measures on 0-1 assignments to small sized sets of variables of F.

Definition 3.3 ([7, 11]) *Given an instance F of CSP(P) with variables $V := \{x_1, .., x_n\}$ and constraints $C := \{c_i : i \in [m]\}$, a family of distributions (i.e. discrete probability measures) m_T on* 0-1 *assignments to all $T \subseteq V$ such that $|T| \leq r$ is* r-locally consistent *if for any R, S and T, $R \subseteq S \subseteq T$, we have*

$$\forall A \in \{0,1\}^{|S|} : \sum_{B \in \{0,1\}^{|S \setminus R|}} m_T(A \circ B) = m_S(A). \tag{3.1}$$

Clearly, the definition above is inspired by the constraints in the SA LP. However, as promised, we will illustrate the proof technique in terms of proof systems to make the connections with PC and Resolution clearer.

3.2.2 Perfect and Imperfect Completeness

Definition 3.4 *Given a family of r-locally consistent measures on an instance F of MAX-k-XOR such that every measure in the family is positive only on the satisfying* 0-1 *partial assignments of F i.e. if a* 0-1 *partial assignment A_T violates a constraint supported on only the variables in T ($|T| \leq O(r)$) then $m_T(A_T) = 0$, then such a family of measures is said to have* perfect completness

The idea is that the measure fools the LP or SDP into thinking that the instance is perfectly satisfiable [4]. Now assume we had a rank/degree $d < r$ SA (static-LS) refutation of F (as in Equation 2.4) then we can obtain a contradiction as follows.

Define a funtional $\varphi : S_{n,d}(\mathbb{R}) \to \mathbb{R}$ on monomials in $S_{n,d}$ as $\Pi_{i \in I} x_i \mapsto \mathbb{E}_{m_I}\left[\Pi_{i \in I} \mathbb{1}_{\{I\}}\right]$, and φ is extended linearly to $S_{n,d}$. Now we apply φ to both sides of our degree d refuation and by using local consistency and perfect completeness of m_I (see for eg. [11, 28] for a similar proof) we will obtain $-1 \geq 0$ - a contradiction. Observe the similarities to the high level framework of [2]. However, the similarities do not end at the high level since the actual construction of these locally consistent measures with perfect completeness in [7], which we skip, relies on similar notions of boundary expansion and closures of constraints that have also been used by [2]. We will see more of such similarities between lower bounds for PC and integrality gaps / rank lower bounds for proof systems in the next sections. To summarize:

Remark 3.5 *The existence of r-locally consistent measures with perfect completeness implies degree must be $\geq r$ for any refutation of CSP(P) in the static proof system in question (SA, static-LS_+ etc). So far the constructions, for example [7, 23], of integrality gaps for SA (and also Lasserre) for MAX-k-CSPs rely on exhibiting locally consistent measures and all of them, except [11], additionally satisfy the perfect completeness property.*

[4] This terminology has its origins in PCP literature.

4 Lasserre Lower Bounds for Parity

Given a sequence $\{y_i : y_i \in [0,1]\}_{1,..,s(2t)}$, where $s(2t) = \binom{n}{\leq 2t}$, the 0-1 moment matrix $M_t(y)$ is a $\mathbb{R}^{s(t)\times s(t)}$ matrix indexed by t-subsets of $[n]$ such that $M_t(I,J) := y_{I\cup J}$. The r round Lasserre SDP for MAX-k-CSP in Equation 2.1 is defined as follows (see [18]).

$$\begin{aligned} \max \quad & \sum_{A\in\{0,1\}^k, C_i\in C} x_{S_i,A} C_i(A) \\ s.t. \quad & M_t(x) \succeq 0, \quad \forall t \leq r. \end{aligned}$$

Using the fact that any positive semidefinite matrix X can be written in the form YY^T, the above SDP can be rewritten in a form similar to the SA LP from the previous section.

Lasserre SDP for MAX-k-CSP(f)

$$\begin{aligned} \text{maximize} \quad & \mathop{\mathbb{E}}_{C_i\in F} \sum_{A\in\{0,1\}^{C_i}} C_i(\alpha)\cdot \left\|\mathbf{V}_{(S_{C_i},A)}\right\|^2 & \\ \text{subject to} \quad & \left\langle \mathbf{V}_{(S_1,A_1)}, \mathbf{V}_{(S_2,A_2)}\right\rangle = 0 & \forall\ A_1(S_1\cap S_2) \neq A_2(S_1\cap S_2) \\ & \left\langle \mathbf{V}_{(S_1,A_1)}, \mathbf{V}_{(S_2,A_2)}\right\rangle = \left\langle \mathbf{V}_{(S_3,A_3)}, \mathbf{V}_{(S_4,A_4)}\right\rangle & \forall\ S_1\cup S_2 = S_3\cup S_4,\ A_1\circ A_2 = A_3\circ A_4 \\ & \sum_{j\in\{0,1\}} \left\|\mathbf{V}_{(\{i\},j)}\right\|^2 = 1 & \forall i\in[n] \\ & \left\langle \mathbf{V}_{(S_1,A_1)}, \mathbf{V}_{(S_2,A_2)}\right\rangle \geq 0 & \forall S_1,S_2,A_1,A_2 \\ & \left\|\mathbf{V}_{(\emptyset,\emptyset)}\right\| = 1 & \end{aligned}$$

Theorem 4.1 ((informal) [23]) *Given a random instance F of MAX-k-XOR an integrality gap of $2-\varepsilon$ persists w.h.p. even after $\Omega(n)$ rounds of Lasserre.*

The proof in [23] explicitly constructs the vectors in the above Lasserre SDP for some $r = \Omega(n)$. We take some liberty with the notation in [23] to make the connections with PC degree lower bounds clearer. The proof is in two steps.

- Consider the refutation of F via Gaussian Elimination (GE) [5] over $R := \mathbb{F}_2[x_1,..,x_n]$. The width of such a refutation is the maximum number of variables in a line of the refutation. Let $L_{F,r}$ be the lines deducible via width r Gaussian Elimination starting from F. For linear forms $l_1, l_2 \in R$, we say $l_1 \sim_F l_2$ if $l_1 + l_2 \in L_{F,r}$. For $l \in L_{F,r}$, define $\pi(l) = 1$ if l has the form: $\sum_i x_i = 0$, and $\pi(l) = -1$ if l has the form: $\sum_i x_i + 1 = 0$.

  Remark 4.2 *It is shown in [5] that any such expanding instance of XORs needs width $\Omega(n)$ to deduce a valid GE refutation. Hence for some $r = \Omega(n)$, $\sim_F$ is an equivalence relation and π is well defined.*

- We now construct the SDP vectors using π and $\sim_F$. Each vector will have a coordinate I corresponding to the representative of an equivalence class $[I]$ of $\sim_F$. Define

$$v_{S,A}(I) := \sum_{J\in[I],\ Vars(J)\subseteq S} \pi(J)\frac{(-1)^{J(A)}}{2^{|S|}},$$

where $J \in R$, $Vars(J)$ denotes the variables in J, and $J(A)$ is simply J evaluated on assignment A.

Finally [23] verifies that the vectors $v_{S,A}$ defined above indeed satisfy satisfy the Lasserre SDP constraints and that $\sum_{A \in C_i^{-1}(1)} ||v_{S_i,A}||_2^2 = 1$, which implies the SDP optimum is 1. However, since the integer optimum is $1/2 - \varepsilon$ we have shown the required integrality gap of $2 - \varepsilon$.

The GE width and PC degree are equivalent upto a factor of 2 for their respective refutations of k-XOR [5], and note that the Lasserre SDP solution above has "perfect completeness" so we summarize this section with the following remark but without a formal justification.

Remark 4.3 *For the case of k-XOR we have shown that a linear lower bound on the degree of PC refutation together with high enough expansion implies a linear lower bound on the rank of the Lasserre SDP relaxation.*

5 Positivstellensatz Calculus and Binomial Ideals

In this section we sketch yet another lower bound for k-XOR type instances but this time for the degree in the stronger Positivstellensatz Calculus of Grigoriev. The technique of the proof will be reminiscent of [2]. The proof is from [15]. However, we will not use Laurent monomials as in [15], but stick to $S_n(\mathbb{R})$ in order to make the similarities with other lower bound proofs clearer.

Definition 5.1 ([15]) *Let $f \in S_{n,d}(\mathbb{R})$ be derived using degree d PC and $h \in S_{n,d}(\mathbb{R})$ be a sum of squares of multiinear polynomials. A degree d* Positivstellensatz Calculus (PZ) *refutation has the form:*

$$f + h = -1. \tag{5.1}$$

As noted before, the product encoding of k-XOR constitutes of binomials when we quotient with $\{x_i^2 - 1 : i \in [n]\}$ as opposed to $\{x_i^2 - x_i : i \in [n]\}$. Hence, when dealing with a random instance of k-XOR predicates one prefers to work in the quotient ring of the former. Let us denote this ring by $S'_n(\mathbb{R})$.

Theorem 5.2 ((informal) [15]) *Suppose any PC refutation of a k-CSP instance F requires degree $2d$, when encoded as binomials over $S'_n(\mathbb{R})$ with all coeffcients in $\{\pm 1, 0\}$[5], then any PZ refutation of F starting with the same encoding requires degree d.*

We provide a sketch of the proof from [15]. The idea is to construct a functional $\varphi : S'_{n,d}(\mathbb{R}) \to \mathbb{R}$ such that $\varphi(f) \mapsto 0$ in Equation 5.1 and $\varphi(h) \mapsto \alpha$ with $\alpha \geq 0$ thus giving a contradiction. When the axioms of F encode to binomials with all coeffcients in $\{\pm 1, 0\}$, the Groebner basis algorithm of [13] implies that the vector space of polynomials derived from a degree d PC on F i.e. the pseudoideal $V_{n,d}(F)$, is a $\mathbb{R}$-linear span of a subset of binomials with all coeffcients in $\{\pm 1, 0\}$. This property of binomials was also used in [5, 10]. We define $\varphi(m) \mapsto 0$ whenever neither $(m+1)$ nor $(m-1)$ belongs to $V_{n,d}(F)$. Otherwise, $\varphi(m) \mapsto \{\pm 1\}$ depending on whether $m+1$ or $m-1$ is in $V_{n,d}$. Since we already know that PC has no degree $2d$ refutation for F, φ is well defined. We linearly extend φ to $S'_{n,d}$. Clearly $\varphi(f) = 0$ for $f \in V_{n,d}(F)$. The argument that $\varphi(h) \geq 0$ is by elementary manipulation. One simply expands the squares in h, applies φ and after some

[5] This holds when F is a random instance of k-XOR as in [5].

simplification constructs a new sum of squares but this time over $\mathbb{R}$. We refer the reader to [15] for the remaining details.

Some concluding remarks are in order. The first is regarding if we can view φ as an instance of some R as in [2].

Remark 5.3 *It is possible that $\varphi(xm) \not\mapsto 0$ for some monomial m and yet $\varphi(m) \mapsto 0$ so the answer is negative. However, over monomials m such that $\varphi(m) \mapsto \{\pm 1\}$ one may think of φ as a remainder in the Groebner basis division (w.r.t. some appropriate ideal). It seems that the definition of φ escapes the complexities involved in defining R [2] because knowledge of the structure of the basis of $V_{n,d}(F)$ makes it easier to define non-trivial φ such that $V_{n,d}(F) \subseteq Ker(\varphi)$.*

The second remark is regarding the similarities between Lasserre and Positivstellensatz Calculus lower bounds for CSPs. For example, both the Lasserre integrality gap in Section 4 and the PZ degree lower bound above define maps from subsets of variables to $\{\pm 1\}$ i.e. π and φ respectively, we note that $\pi = \varphi$.

Remark 5.4 *The Positivstellensatz (PS) [15] is the static version of PZ. The dual of the rank r Lasserre SDP has the same structure as a degree r PS refutation (Section 4.2 in [18]). If we use the product encoding over S_n (or S'_n) for Lasserre then the SDP objective function for MAX-k-CSP remains unchanged. Although there maybe some subtleties about SDP duality that may prevent a black-box relationship between the degree lower bound for the PS and integrality gaps with perfect completeness for Lasserre, it is likely that the ideas involved in the lower bounds for k-CSP in PZ would be helpful for proving Lasserre integrality gaps with perfect completeness.*

6 Dynamic Hierarchies and Proof Systems

The integrality gaps and rank lower bounds for dynamic hierarchies like LS and LS_+ have used a different proof framework [9, 1, 24]. For MAX-CSPs most of the LS rank lower bounds are now subsumed by the corresponding SA rank lower bounds. The LS_+ rank lower bounds were not implied by static-LS_+ lower bounds(cf. [27]). The LS (and LS_+) integrality gaps or rank lower bounds follow via intricrate induction arguments which are framed as a Prover-Adversary game to make them more readable. The game involves construction of protection matrices since this approach was inspired from the orginal definition of LS hierarchy, which is repeated below for completeness.

Definition 6.1 (see [12]) *Given homogenized convex cones $\tilde{K_1}, \tilde{K_2}$ in $\mathbb{R}^{n+1}$ corresponding to polytopes K_1 and K_2, define the cone $M(\tilde{K_1}, \tilde{K_2})$ (the lifted LS cone) as the cone consisting of all $(n+1) \times (n+1)$ matrices Y in $\mathbb{R}$ satisfying the conditions:*

1. *Y is symmetric*
2. *$Y_{ii} = Y_{i0}$*
3. *$\tilde{K_1}^* Y \tilde{K_2}^* \geq 0$.*

Let $N(\tilde{K_1}, \tilde{K_2})$ denote the projection Ye_0 of $M(\tilde{K_1}, \tilde{K_2})$. Let Q_n denote the unit cube $[0,1]^n$. Define $N(\tilde{K}, \tilde{Q_n})$ (or simply $N(K)$) as the cone (polytope) obtained after a single LS lift and project step.

The rank r polytope is obtained by applying N for r times. The matrices in M are typically referred to as Protection matrices in the lower bound proofs. LS_+ additionally requires elements of $M(K,Q)$ be positve semidefinite. We illustrate this method next with a much simpler example. Consider the Symmetric Knapsack polytope defined as:

$$\sum_{i=1}^{2n+1} x_i = n + 1/2,$$
$$\forall i \in [2n+1] : x_i \in [0,1].$$

The polytope has no 0-1 vertices and so LS will derive a refutation in $2n$ rounds. The LS rank lower bound of $n/2$ (due to [16][6]) actually proves the stronger static-LS lower bound via defining a functional - as expected for the case for static proof systems. However, a direct rank lower bound for LS using the game method would likely amount to an inductive proof of the claim: The LS polytope of rank $\leq k$ would contain all the points of the form:

$$\{\pi(\langle \vec{1}^{n-k}, \vec{0}^{n-k}, \frac{\vec{1}^{2k+1}}{2} \rangle) : \pi \in \mathcal{S}_{2n+1}\}.$$

Using an involved argument [24] prove the following statement.

Theorem 6.2 ((informal) [24]) *For a random instance F of MAX-k-XOR, a gap of $2-\varepsilon$ persists w.h.p. even after $\Omega(n)$ rounds of LS_+.*

The proof constructs protection matrices as mentioned before using the Prover-Adversary game framework. The expansion of the underlying constraint graph of F is used to ensure positive semidefiniteness and also prove that the protection matrices exist even after many rounds of LS_+.

7 Some Open Problems

Several important open problems remain as far as lower bounds for such hierarchies and proof systems are concerned. We list some of the less well known questions below.

1. It is known that a random instance of MAX-k-XOR ($k \geq 3$) [7, 23] almost always has an integrality gap with perfect completeness even after linear number of rounds of Lasserre and the corresponding degree lower bounds for the Positvstellensatz are also known. However, it is not known for which predicates other than k-XOR can one can show similar lower bounds. There is modest progress in this direction in [27] which shows rank lower bounds for the static-LS_+ hierarchy, which is at least as strong as the mixed hierarchy. It would be interesting to see if one can define a reduction operator similar to Alekhnovich and Razborov [2] and generalize their lower bound for the degree of any polynomial calculus refutation of immune predicates to show similar positivstellensatz type lower bounds for (say) immune predicates.

2. As far as just the question of integrality gaps is concerned i.e., one is even satisfied with hard instances which have *imperfect completeness*, it would be interesting to answer for which predicates P does MAX-k-CSP(P) have large integrality gap even in strong hierarchies. Of course we know some such results with perfect completeness here [23, 26, 7, 27] and such

[6] The lower bound in [16] is actually for the positivstellensatz.

questions have also been explored for weak proof systems like Resolution [6] and Polynomial Calculus [2]. But we know very few results with imperfect completeness for MAX-k-CSPs. Moreover, one may go a step further and ask for algorithms which beat the random assignment in case existence of lower bounds is suspect. Such a question essentially asks for dichotomy type results but with respect to weaker models of computation. There is modest progress in this direction in [17] but still many questions remain open.

3. Integrality gaps for the Unique Games type of problems remain elusive in SDP hierarchies and since the Sum of Squares type derivations can refute known hard instances, any progress would be very interesting. However, is the full power of SOS derivations necessary for non-trivial approximation algorithms or could we use fewer rounds of fancier "lift and project" type derivations. For example, could dynamic hierachies (for eg. the LS_* hierarchy) be used to show non-trivial rank bounds for such questions. While there is some progress in [28] for this question as far as the LS_* hierarchy is concerned, there are likely a couple of obvious weak (non-SOS) hierarchies which are left to be ruled out.

4. Finally, all lower bounds mentioned so far essentially show that some fixed algorithms based on LP and SDP relaxations can not approximate or refute certain hard instances. However, the question of size lower bounds in dynamic hierarchies [16, 22] goes beyond fixed algorithms and we do not know any size vs rank tradeoffs in dynamic hierachies. Moreover, we also do not know size vs rank tradeoffs for the static positivstellensatz. Such size lower bounds for static hierarchies may also be interesting simply because they would imply a lower bound on the number of lifted inequalities needed to deduce the empty polytope and as a consequence also imply corresponding rank lower bounds.

References

[1] Michael Alekhnovich, Sanjeev Arora, and Iannis Tourlakis. Towards Strong Non-Approximability Results in the Lovász-Schrijver Hierarchy. In *STOC*, pages 294–303, 2005.

[2] Michael Alekhnovich and Alexander Razborov. Lower Bounds for Polynomial Calculus: Non-Binomial Case. In *FOCS*, pages 190–199, Washington, DC, USA, 2001. IEEE Computer Society.

[3] Boaz Barak, Fernando G. S. L. Brandão, Aram Wettroth Harrow, Jonathan A. Kelner, David Steurer, and Yuan Zhou. Hypercontractivity, Sum-of-Squares Proofs, and their Applications. *CoRR*, abs/1205.4484, 2012.

[4] Boaz Barak, Prasad Raghavendra, and David Steurer. Rounding Semidefinite Programming Hierarchies via Global Correlation. In *FOCS*, pages 472–481, 2011.

[5] Eli Ben-Sasson and Russell Impagliazzo. Random CNFs are Hard for the Polynomial Calculus. *Comput. Complex.*, 19(4):501–519, December 2010.

[6] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow – resolution made simple. *J. ACM*, 48(2):149–169, March 2001.

[7] Siavosh Benabbas, Konstantinos Georgiou, Avner Magen, and Madhur Tulsiani. SDP Gaps from Pairwise Independence. In *Theory of Computing*, To appear.

[8] Gábor Braun, Samuel Fiorini, Sebastian Pokutta, and David Steurer. Approximation limits of linear programs (beyond hierarchies). *CoRR*, abs/1204.0957, 2012.

[9] Joshua Buresh-Oppenheim, Nicola Galesi, Shlomo Hoory, Avner Magen, and Toniann Pitassi. Rank Bounds and Integrality Gaps for Cutting Planes Procedures. In *FOCS*, pages 318–, Washington, DC, USA, 2003. IEEE Computer Society.

[10] Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.*, 62(2):267–289, 2001.

[11] Moses Charikar, Konstantin Makarychev, and Yury Makarychev. Integrality Gaps for Sherali-Adams Relaxations. In *STOC*, pages 283–292, New York, NY, USA, 2009. ACM.

[12] Eden Chlamatac and Madhur Tulsiani. Convex Relaxations and Integrality Gaps. In *Handbook on Semidefinite, Cone and Polynomial Optimization*, 2010.

[13] Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the groebner basis algorithm to find proofs of unsatisfiability. In *STOC*, pages 174–183, 1996.

[14] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf. Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds. In *STOC*, pages 95–106, 2012.

[15] Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theor. Comput. Sci.*, 259(1-2):613–622, 2001.

[16] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Complexity of Semi-Algebraic Proofs. *ECCC*, (103), 2001.

[17] Subhash Khot, Madhur Tulsiani, and Pratik Worah. The Complexity of Somewhat Approximation Resistant Predicates. *ECCC*, (151), 2012.

[18] Jean Bernard Lasserre. *Moments, Positive Polynomials and Their Applications*. Imperial College Press, 2009.

[19] Ryan O'Donnell and Yuan Zhou. Approximability and Proof Complexity. *CoRR*, abs/1211.1958, 2012.

[20] Toniann Pitassi. Propositional Proof Complexity and Unsolvability of Polynomial Equations. *Proc. of the Intl. Cong. of Mathematicians*, pages 451–460, 1998.

[21] Toniann Pitassi and Nathan Segerlind. Exponential Lower Bounds and Integrality Gaps for Tree-like Lovász-Schrijver Procedures. In *SODA*, pages 355–364, 2009.

[22] Pavel Pudlák. Lower Bounds for Resolution and Cutting Plane Proofs and Monotone Computations. *J. Symb. Log.*, 62(3):981–998, 1997.

[23] Grant Schoenebeck. Linear Level Lasserre Lower Bounds for Certain k-CSPs. In *FOCS*, pages 593–602, Washington, DC, USA, 2008. IEEE Computer Society.

[24] Grant Schoenebeck, Luca Trevisan, and Madhur Tulsiani. A Linear Round Lower Bound for Lovász-Schrijver SDP Relaxations of Vertex Cover. In *IEEE Conference on Computational Complexity*, pages 205–216, 2007.

[25] Stefan Dantchev and Barnaby Martin and Mark Rhodes. Tight Rank Lower Bounds for the Sherali-Adams Proof System. *Theoretical Computer Science*, 410(21-23):2054 – 2063, 2009.

[26] Madhur Tulsiani. CSP gaps and Reductions in the Lasserre Hierarchy. In *STOC*, pages 303–312, 2009.

[27] Madhur Tulsiani and Pratik Worah. LS+ Lower Bounds from Pairwise Independence. *ECCC*, (105), 2012.

[28] Pratik Worah. Rank Bounds fo a Hierarchy of Lovász and Schrijver. *ECCC*, (003), 2012.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de