On the asymptotic Nullstellensatz and Polynomial Calculus proof complexity

Søren Riis
Department of Computer Science
Queen Mary, University of London
United Kingdom
smriis@dcs.qmul.ac.uk

Abstract

We show that the asymptotic complexity of uniformly generated (expressible in First-Order (FO) logic) propositional tautologies for the Nullstellensatz proof system (NS) as well as for Polynomial Calculus, (PC) has four distinct types of asymptotic behavior over fields of finite characteristic. More precisely, based on some highly non-trivial work by Krajicek, we show that for each prime p there exists a function $l(n) \in \Omega(\log(n))$ for NS and $l(n) \in \Omega(\log(\log(n))$ for PC, such that the propositional translation of any FO formula (that fails in all finite models), has degree proof complexity over fields of characteristic p, that behave in 4 distinct ways:

(i) The degree complexity is bound by a constant.

(ii) The degree complexity is at least $l(n)$ for all values of n.

(iii) The degree complexity is bound by a constant on an infinite set S, and is at least $l(n)$ on the complement $N \setminus S$. Furthermore, membership $n \in S$ is for some $k \in N$ determined uniquely by the value of n modulo q^k.

(iv) The degree complexity fluctuates between constant and $l(n)$ (and possibly beyond) in a very particular way.

We leave it as an open question whether the classification remains valid for $l(n) \in n^{\Omega(1)}$ or even for $l(n) \in \Omega(n)$. Finally, we show that for any non-empty proper subset $A \subseteq \{(i), (ii), (iii), (iv)\}$ the decision problem of whether a given input FO formula ψ has type belonging to A - is undecidable.

1. Introduction

1.1 Weak propositional proof systems

A large number of problems in computer science including verification, knowledge representation, planning and automated theorem proving are linked to the following decision problem: Given a propositional formula ψ in m boolean variables as input, decide if the formula is a tautology. Mathematically this problem is trivial since essentially we can decide the question by exhaustively testing each of the 2^m possible $0/1$ truth assignments. However, from a practical computational point of view this is not feasible if m is large, so it is important to find methods that are more efficient than exhaustive search. In the case where the formula ψ is a tautology we would like this to be verified by some feasible and reliable procedure. This could be done, for example, by providing a proof of ψ in a suitable proof system. Such approach is, however, only feasible if there exists a 'short' proof (or in general a short 'certificate') that proves (or in general 'witnesses') the fact that Ψ is a tautology. A key problem in propositional proof complexity concerns this issue. The big open question is whether it is *in general* possible to do better than exhaustive testing. Is there a propositional proof system where, for example, it is always possible to provide proofs (certificates) that contain less than $p(m)$ symbols for some fixed polynomial p?

Cook and Recknows [6] put forward a program (for proving NP $\neq$ co-NP) where the idea is to obtain super-polynomial for stronger and stronger propositional proof systems. Cook and Recknow noticed that showing NP $\neq$ co-NP is equivalent to proving super polynomial lower bounds for *any* propositional proof system (where the axioms and rules are given in a manner that can be computed in Polynomial time).

Proof systems where proving super-polynomial lower bounds seems to be well beoynd current techniques are often refered to a "strong" propositional proof systems [12]. On the other hand propositional proof systems (like resolution) for which super-polynomial (or exponential) lower bounds are known - are referred to as "weak" propositional proof systems. Examples of strong propositional proof systems include proof systems like Natural deduction (tree-like or dag-like), Gentzen's system LK (with cuts) as well as the so called Frege-proof systems.

Despite being inefficient for some classes of tautologies, weak propositional proof systems play a very important role in many areas of computer science. The resolution proof system, for example, is quite a weak system, however many theorem provers and algorithms are based on this proof system (usually in the form of the Davis-Putnam algorithm). The main reason for this success of weak proof systems is that although strong propositional proof systems sometimes allow shorter proofs than the weak propositional system, in general it seems to be computationally hard to find these shorter proofs. In fact, in general, for some classes of tautologies it might (asymptotically) be computationally harder to find short proofs of the propositions in some given strong system, than to find the proofs of the propositions in a weak proof system.

Weak systems often allow us to get quite a clear idea about what are sensible (and what are less sensible) proof strategies. However, in many cases it seems very unclear how one can algorithmically (in a feasible manner) utilise the strength of the strong propositional system.

An important part of our motivation for studying weak systems (especially after a good lower bound have already been obtained for the system) is to understand - in as clear terms as possible - the proof systems' ability (or lack of ability) to handle various general classes of tautologies.

1.2 Related results

In [13, 15] Krajicek initiated the study of how particular weak propositional proof systems are coping with uniform systems of tautologies (or unsatisfiable propositions). In [16] Paris and Wilkie had already introduced a general method of converting statements of Bounded Arithmetic (and first oder logic) into propositional logic. This method allows us to convert any first order (FO) predicate formula ψ into a sequence ψ_n of propositional propositions. The method of translation can be seen as a special case of the translation methods discussed in [5], where various classes of formula in logic are translated into a uniform sequence of propositional logic. In the general translation each Σ_0^B FO-formula η is translated into a sequence $\eta[n]$ of propositional propositions. Our main result is not valid with this general translation, that allows "build-in" relation and functions (i.e. has certain relations and function symbols that play a special role in the translation). Informally, our translation can be viewed as similar to the Σ_0^B-translation for FO formula, but restricted to the case where there is no reference to any special symbols (of bounded arithmetic) that are translated such that the indices $1, 2, \ldots, n$ on the proposition variables are interpreted as representing the natural numbers $1, 2, \ldots, n$

Let Θ denote the class of FO formulae that have no finite models. Then the translation of each $\psi \in \Theta$ leads to a sequence ψ_n of unsatisfiable proposition formulae. Informally, the proposition ψ_n states that ψ has no model of size n.

For a given propositional refutation system $\mathcal{R}$, Krajicek's approach was to provide a general model theoretic criteria that together with a general increasing function $f : N \to N$ (e.g. a function of super polynomial growth rate), would insure that any FO sentence $\psi \in \Theta$ that satisfies the model theoretic criteria would lead to a sequence ψ_n of unsatisfiable propositions, that for n sufficiently large would require any $\mathcal{R}$-refutation to have complexity at least $f(n)$.

Maybe the most basic model theoretic principle is that a given FO formula $\psi \in \Theta$ is valid in some infinite model. In [20] Riis showed that the fact that ψ_n is unsatisfiable (represented as a statement expressed in undefined relational symbols) cannot be proven in the system $T_2^1(\alpha)$ of bounded arithmetic if and only if ψ holds in some infinite model.

From a combinatorial perspective (disregarding certain technical issues related to Bounded Arithmetic) the if-direction was later improved by Krajicek [13], when he showed that any FO-sentence $\psi \in \Theta$ that holds in some infinite model, leads to a sequence ψ_n that requires exponential size tree-like resolution refutations.

The pigeonhole principle is violated in some infinite models, thus Krajicek's criteria immediately made it possible to "explain" why various versions of the pigeonehole principle are hard for tree-resolution. For a fix field characteristic, Krajicek showed in [15, 14] that if there is an infinite model equipped with a suitable Euler structure (which depends on the characteristic of the field) in which ψ is valid, then ψ_n requires Nullstellensatz (NS) refutations of degree $\Omega(\log(n))$ and requires Polynomial Calculus (PC) refutations of degree $\Omega(\log\log(n))$.

Informally Kraijcek's criteria capture in some sense the class of first order sentences that lead to such hard tautologies with respect to the propositional system in focus. This informal interpretation is reflected in Krajicek's terminology where he says that his model theoretic criterion (different for different propositional proof systems) "corresponded" to the proof system. It should be emphasised that in general the correspondences established by Krajicek are not "exact" (and were not claimed it to be so).

A related, but different approach was introduced by Riis [21] suggesting that (weak) propositional proof systems in general might have so-called complexity gaps. Riis showed that a tree-resolution have a complexity gap and that Krajicek's model theoretic criterion for tree-resolution is in fact a characterisation. More specifically, for any formula ψ in predicate logic that there are two disjoint possibilities *either* the sequence ψ_n has polynomial size tree-resolution refutations *or* the sequence ψ_n requires full exponential size tree-resolution refutations. Furthermore, case (2) applies if and only if ψ is valid in some infinite model (the refutations tree-resolution complexity is set to ∞ if the formula ψ_n is satisfiable).

Notice, that the number of boolean variables in ψ generally is n^c for some $c > 1$ and it is possible for the refutation complexity to be as bad as 2^{n^c} for any $c > 0$. Danchev and Riis showed in [9] that for tree-like resolution there are no complexity gaps above $2^{cn \log n}$. In the same paper Riis and Danchev tried - with limited success - to improve this result. Based on our effort we conjectured that in fact for any formula ψ in predicate logic there are three distinct cases: (1) ψ_n has polynomial size tree-resolution refutations (2) for some constant $0 < c < d$ ψ_n has size 2^{dn} tree-resolution refutations, but has (except for finitely many expections) no refutations of size 2^{cn} (3) for some constant $c > 0$ ψ_n requires size $2^{cn \log(n)}$- tree-resolution refutations. This conjecture is still open.

It follows from [3] that the FO statement ψ that some binary relation R which defines a total ordering without a smallest element (i.e. a violation of the least number principle) has polynomial size resolution refutations. Since ψ is satisfiable in some infinite models (e.g. $(Z, <)$) it follows that if there is a model theoretic criterion for full sequential (dag-like) resolution it must be different from that for three-resolution. However, Danchev and Riis showed in [10] that the characterisation for tree-resolution remains valid for full dag-like resolution provided we consider "relativised" FO formula ψ in predicate logic (for definition see [10]) . This answered an open question by Krajicek and showed that for each relativised FO formula ψ there are two disjoint possibilities: (1) the sequence ψ_n has polynomial size resolution refutations (2) the sequence ψ_n requires full exponential size resolution refutations. Furthermore, case (2) applies if and only if ψ is valid in some infinite model.

It is an open question whether for any ψ in predicate logic there are two disjoint possibilities: (1) the sequence ψ_n has polynomial size resolution refutations OR (2) the sequence ψ_n requires exponential size resolution refutations. If this question can be answered positively we expect this to be difficult to prove since an exponential lower bound for the weak-pigeon hole principle (stating there is no map from n to $2n$) would follow just from a non-polynomial lower bound. So far one of the deepest and technically most involved theorems in resolution proof complexity has been the exponential lower bound on the weak pigeon-hole principle [18]. Also another difficulty is that it is not clear that there is a simple model theoretic criterion that exactly captures the class of ψ for which ψ_n requires exponential size resolution refutations.

More recently two new dichotomy results have been published. To give the flavor of these theorems we state them, but ask the reader to consult [7, 8] for precise definitions of the involved concepts.

Theorem A : (S. Dantchev and B. Martin) (Improvement of [7])

Given a FO sentence ψ which fails in all finite structures, consider its translation into a propositional CNF contradiction $C_{\psi,n}$, where n is the size of the finite universe. Then either 1 or 2 holds:

(1) There exists a constant r such that $C_{\psi,n}$ has rank-r Lovasz-Schrijver refutation for every n.

(2) There exists a positive constant a such that for every n, every Sherali-Adams refutation of $C_{\psi,n}$ is of rank at least n^a.

Furthermore, 2 holds if and only if ψ has an infinite model.

To fully appreciate this gap, one should notice that each rank k Lovasz-Schrijver refutation can be converted into a rank k Sherali-Adams refutation.

In Danchev's original paper only a poly-logarithmic bound were given for this result.

Theorem B : (S. Dantchev, B. Martin, S. Szeider)([8])

Given a FO sentence ψ, which fails in all finite models. Consider the sequence of parametrised contradictions $(C_{\psi,n,k})_{n \in N}$ is a translation of ψ. Then exactly of one the following three alternatives is valid:

(1) $C_{\psi,n,k}$ has a polynomial size tree-like resolution refutations of a size bound by a polynomial independent in n that does not depend on k.

(2a) $C_{\psi,n,k}$ has a parametrisised tree-like resolution refutation of size $\beta^k n^\alpha$ for some constants α and β which depends of ψ only.

(2b) There exists a constant γ, $0 < \gamma < 1$ such that for every $n > k$, every parametrised tree-like resolution refutation of $C_{\psi,n,k}$ is of size at least n^{k^γ}.

Furthermore, case (2) (i.e. case (2a) or case (2b)) occur if ψ holds in some infinite model. Furthermore, (2b) holds if and only if ψ has an infinite model whose induced hyper-graph has no finite dominating set.

1.3 Algebraic proof complexity

The Nullstellensatz proof system [1] and Polynomial Calculus [4] are two of the most popular weak algebraic proof systems. These systems have been studied quite intensively since their introduction in the mid 1990s.

Let F be a fixed (algebraically closed) field, and let $u \in N$. Given a (finite) collection $\Gamma = \{p_1, p_2, \ldots, p_\lambda\}$ of polynomials $p \in F[x_1, x_2, \ldots, x_u]$, the task is to show that the polynomials have no common root, i.e that there is no $(a_1, a_2, \ldots, a_u) \in F^u$ such that $p(a_1, a_2, \ldots, a_u) = 0$ for each $p \in \Gamma$.

One version of Hilbertz Nullstellensatz states that the polynomials in Γ have no common root if and only if the identity polynomial 1 belongs to the ideal generated by the polynomials in Γ. In other worlds there exists for each polynomial $p_j \in \Gamma$ a polynomial $r_j \in F[x_1, x_2, \ldots, x_u]$ such that $1 = \Sigma_{j=1}^{\lambda} r_j p_j$. The expression $1 = \Sigma_{j=1}^{\lambda} r_j p_j$ constitutes a Nullstellensatz proof. The degree of the proof is defined as the maximal degree of the polynomials $r_j p_j$, $j = 1, 2, \ldots, \lambda$.

We can think about each polynomial in Γ as a premise and as 1 representing the contradiction. From this perspective a Nullstellensatz proof is then an "indirect" proof (a refutation) that shows that the premises (which state that the polynomials $p \in \Gamma$ have a common zero), lead to a contradiction ($= 1$).

In most applications in propositional logic each variable $x_1, x_2, \ldots, x_n$ is assumed to take $0/1$-values, in which case for each variable x the equation $x^2 - x$ is assumed to belong to Γ. Occasionally, the fourier basis is used and the variables are assumed to take $-1/1$ values (and the underlying field is assumed to have characteristic $\neq 2$). In this case for each variable x the equation $x^2 - 1$ is assumed to belong to Γ. In both cases (the $0/1$ case as well as the $-1/1$ case) we can drop the assumption that the F is algebraically closed. In this paper we will not consider the fourier basis since the natural translation of a FO sentence in general does not lead to a polynomials of constant degree.

The polynomial calculus (PC) resembles more a traditional proof system. The idea behind PC is to show that 1 belongs to the ideal generated by the polynomials in Γ. This is done in a logic style derivation using the following two rules $\frac{q \quad p}{q+p}$ (cut) and $\frac{q}{rq}$ (weakening). We have adopted the terminology "cut" and "weakening" since these are the logical operations that naturally corresponds to these rules.

Given the set Γ of polynomials, a PC refutation of Γ is a sequences $q_1, q_2, \ldots, q_s = 1$ of polynomials where each polynomial is either a premise (i.e. belongs to Γ) or can be deduced by an application of either a cut or a weakening. The degree of the proof is the maximal degree of the polynomials $q_1, q_2, \ldots, q_s$.

Finally, we would like to pay attention to the $\mathcal{F}$-PC refutation system defined in [11] partly based on a suggestion in [17]. As noticed by a number of authors, the definition of PC does not constitute a Cook-Recknow proof system since no specific rules are given for how one is allowed to handle the polynomial expressions. This can be mended by considering the $\mathcal{F}$-PC refutation system that P-simulate any Frege propositional proof system [11] and is thus a strong refutation system. The degree of a $\mathcal{F}$-PC proof (defined as the largest degree of a polynomial that appear in the derivation), remains unchanged if we consider the PC refutation as taken part in the $\mathcal{F}$-PC system.

2 The main result

To state the main result in larger generality we define the refutation degree complexity of a system of satisfiable polynomial equations as infinite. This allows us to discuss the refutation degree complexity of a sequence ψ_n without requiring that each ψ_n is unsatisfiable.

The main result can be stated as follows:

Theorem 1 : *For each prime p and for each FO formula ψ there exists a function $l(n) \in \Omega(\log(n))$ for NS and $l(n) \in \Omega(\log(\log(n))$ for PC, such that the propositional translation of ψ (a collection of polynomial equations) leads to sequence ψ_n of polynomial equations with a refutation degree refutation complexity $d(n)$ over fields of characteristic p, that behaves in one of 4 distinct ways:*

1) The degree refutation complexity $d(n)$ is bound by a constant $c < \infty$ (with possible finitely many exceptions where the degree complexity is ∞).

2) The degree refutation complexity d(n) is at least $l(n)$ for all values of n.

3) The degree refutation complexity $d(n)$ is bound by a constant $c < \infty$ on an infinite set S, and is at least $l(n)$ on the complement $N \setminus S$. Furthermore, membership $n \in S$ is for some $k \in N$ determined uniquely by the value of n modulo q^k (with possibly finitely many exceptions).

4) The degree refutation complexity $d(n)$ fluctuates between constant and $l(n)$ (and possibly beyond) in a very particular way. More, specifically if $d(n)$ is strictly less than $l(n)$ then $d(m) = d(n)$ for all $m > n$ with $m = n$ modulo p^r for some r with $p^r \leq l(n)$.

For any non-empty proper subset $A \subseteq \{(i), (ii), (iii), (iv)\}$, the decision problem of whether a given input FO formula ψ has type belonging to A, is undecidable. This undecidablity result remains valid if we consider the promise decision problem where each ψ is selected such that it is unsatisfiable in all finite models.

The undecidable part implies trivially that each of the 4 possibilities can occur.

The theorem shows that for a fixed field F of finite characteristic p (and for a suitable choice of the function l) the class of first order formulae can be divided into 4 disjoint classes. We will later show (Theorem 10) that the type of a FO-formula does not depend on whether we consider NS-refutations or PC-refutations.

It turns out that a first order formula ψ that is unsatisfiable in all models (including infinite models) is always of type 1 (Lemma 7). Furthermore, it turns out that a first order formula ψ with even a slight irregular spectrum (i.e. where the set S for which ψ has a model of size n cannot be determined by properties of n modulo some powers of p) are always of type 2. Formulae of type 3 and 4, have always a very regular spectrum where the membership $n \in S$ of the spectrum of ψ is in general uniquely determined by properties of n modulo powers of p.

Finally, let us point out that the classification in Theorem 1 is highly robust with respect to the choice of the growth-rate of the function l (at least as long as it satisfies the general bounds stated in the theorem). If we replace, for example, l with any non-decreasing function $l' \in O(\log(n))$ for the NS-case [or $l' \in O(\log(\log(n)))$ for the PC-case] that is not bound from above by a constant $c < \infty$ each FO formula ψ translates to a sequence ψ_n that has the same type with respect to l' as it has with respect to l.

3 Proof of the main theorem

The main result heavily uses the following general principle that can be extracted from Krajicek's Theorem 3.5 in [15]. We suppress some of the parameters since they are not needed for our purpose. The actual choice of the parameters depends purely on the syntactical properties of the given FO formula ψ (as well the underlying field F).

Let ψ be a system of generating polynomials that generates a sequence ψ_n of polynomial equations over a field F of characteristic p. There exists $c = c(\psi, p)$ such that for each $d \in N$ there exists $N = N(d) \leq 2^{cd}$
$[N = N(d) \leq 2^{2^{cd}}$ for the PC-case] and $l \leq cd$
$[l \leq 2^{cd}$ for the PC-case] such that for each $n_1, n_2 \geq N$ with $n_1 = n_2$ modulo q^l, ψ_{n_1} has a NS-refutation [PC-refutation in the PC-case] of degree d if and only ψ_{n_2} has a NS-refutation [PC-refutation] of degree d

Let $h : N \rightarrow N \cup \{\infty\}$ and let $l, r : N \rightarrow N$ be general functions with l and r non-decreasing. Assume that the functions satisfy the following condition:

($\triangle$) *For each d if for some $n > l(d)$ we have $h(n) = d$, then for all m with $m > l(d)$ and $m = n$ modulo $q^{r(d)}$ we have $h(n) = h(m)$.*

Notice that since l and r are non-decreasing functions, if $h(n) < d$ for some $n > l(d)$, then $h(m) < d$ for all $m > l(d)$ with $n = m$ modulo $q^{r(d)}$.

Now let us increase d and ask what can happen asymptotically when d tends to infinity. The next lemma help link Kraijcek's results with Theorem 1.

Lemma 2 : *Let $h : N \rightarrow N \cup \{\infty\}$ and let $l, r : N \rightarrow N$ be general functions with l and r non-decreasing, that satisfy ($\triangle$). Then exactly one of the following 4 possibilities holds:*

1) $\{h(n) < \infty : n \in N\}$ is finite

2) $\{h(n) < \infty : n \in N\}$ is infinite and
$\{h(n) < \infty : n > l(h(n))\}$ is empty

3) $\{h(n) < \infty : n \in N\}$ is infinite and
$\{h(n) < \infty : n > l(h(n))\}$ is finite and non-empty

4) $\{h(n) < \infty : n \in N\}$ is infinite and
$\{h(n) < \infty : n > l(h(n))\}$ is infinite

Each of the four cases corresponds to the four cases in Theorem 1. This link follows by spelling out the concrete consequences (in conjunction the conditions in $\triangle$) of each of the four cases:

Lemma 2A : *Let $h, l, r : N \rightarrow N$ be function that satisfies ($\triangle$). Then exactly one of the following four mutually exclusive cases occurs.*

1) There exits $d_0 \in N$ such that $h(n) < d_0$ holds for all $n \in N$ with $n > l(d_0)$.

2) For all values of $d \in N$ if $n > l(d)$ then $h(n) > d$ for all $n \in N$.

3) $N = S_1 \cup S_2$ can be written as a disjoint union of two infinite sets S_1 and S_2 such that there exists $d_0 \in N$ with $h(n) < d_0$ for all $n \in S_1$ with $n > l(d_0)$ and for all $d \in N$ and $n \in S_2$ with $n > l(d)$, $h(n) > d$.

4) For arbitrarily large values of $d \in N$, $h(n) = d$ holds for some $n \in N$ with $n > l(d)$.

Proof: Directly from Lemma 2A using the properties of $\triangle$ ♣

Let $h(n)$ denote the minimal degree of a NS (or PC) refutation of ψ_n where ψ is a general FO formula. Then according to Krajicek's results h satisfies $\triangle$ with $l(n)$ and $r(n)$ having $l(n), q^{r(n)} \in \Omega(\log(n))$ for the NS case, and having $l(n), q^{r(n)} \in \Omega(\log(\log(n)))$ for the PC case. This shows the major part of Theorem 1.

4 Case 1,2 and 3

We will now show that each of the four possibilities in Theorem 1 can appear. We will illustrate this by choosing variant's of the pigeonhole principle and the counting modulo p principle. Cases $1, 2$ and 3 can be illustrated by numerous examples. Currently various versions of the weak pigeonhole principle are (essentially) the only cases we have found with fluctuating complexity, though we conjecture that there are many other (natural) examples. Most sequences of propositional formula that so far have been considered in the literature have type 1) or 2).

As an example, the bijective pigeonhole principle stating that there is no bijective map from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n-1\}$ - is of type 2. The negation of the pigeonhole principle has NS-refutation degree $n/2$ according to Razborov [19]. Let us consider this example from our perspective. The violation of the pigeonhole principle can be written as the conjunction of:

- $\forall x \exists y (y \neq n \wedge R(x,y))$

  and

- $\forall x, y, z ((R(x,y) \wedge R(x,z)) \rightarrow y = z)$

We refer to this conjunction as PHP_n^{n-1}. This statement says that there exits a point n, and a binary relation R that defines an injective map from the universe to the universe except for n. Translated into polynomial equations we get (after a few cosmetic changes) the following system of polynomial equations:

- $Q_i^1 := \Sigma_{j=1}^n x_{ij} - 1 = 0$ for $i \in \{1, 2, \ldots, n\}$

- $Q_{ijk}^2 := x_{ij} x_{ik} = 0$ for $i, j \neq k \in \{1, 2, \ldots, n\}$

These polynomial equations have no common solution. However, the equations do not have NS-refutations of degree complexity in $O(\log(n))$
[and do not have PC-refutations of degree $O(\log(\log(n)))$]. Thus the system of equations has NS-refutation degree complexity (PC-refutation degree complexity) of type 2.

Consider the conjunction of PHP_n^{n-1} with the following two FO-sentences:

- $\forall y \exists x R(x,y)$

- $\forall x_1, x_2, y ((R(x_1,y) \wedge R(x_2,y)) \rightarrow x_1 = x_2)$

The resulting statement says that there exits a point n, and a binary relation R that defines be bijection from the universe to the universe except for n. Translated into polynomial equations we get after a few cosmetic changes the following system of polynomial equations:

- $Q_i^1 := \Sigma_{j=1}^n x_{ij} - 1 = 0$ for $i \in \{1, 2, \ldots, n\}$

- $Q_j^2 := \Sigma_{i=1}^{n-1} x_{ij} - 1 = 0$ for $j \in \{1, 2, \ldots, n\}$

- $Q_{ijk}^3 := x_{ij} x_{ik} = 0$ for $i, j \neq k \in \{1, 2, \ldots, n\}$

- $Q_{i_1 i_2 j}^4 := x_{i_1,j} x_{i_2,j} = 0$ for $i_1 \neq i_2, j \in \{1, 2, \ldots, n\}$

- $Q_{ij}^5 := x_{ij}^2 - x_{ij} = 0$ for $i, j \in \{1, 2, \ldots, n\}$

This system of polynomial equations has no solution since a solution would define a bijection from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n-1\}$. The system has a NS-refutation of degree 2 (see [2]). Thus the system of equations has NS-refutation degree complexity (PC-refutation degree complexity) of type 1.

For a problem of type 3 consider the negation of the counting modulo p principle (where p is the characteristic of the underlying field) in conjunction with the negation of the pigeonhole principle for arbitrary functions (the two principle are expressed using two disjoint set of variables). More specifically the translation of the violation of the counting modulo p principle can be stated as follows [15]:

Let $n \geq p \geq 2$. For each p-element subset $e \subset \{1, 2, \ldots, n\}$ introduce a variable z_e. Then consider the polynomial equations:

- $Q_e := z_e^2 - z_e = 1$ for each variable z_e

- $Q_{e,f} := z_e z_f = 0$ for every e, f such that $e \cap f \neq \emptyset$ and $e \neq f$.

- $Q_i := \Sigma_{e \ni i} z_e - 1$ for each $i \in \{1, 2, \ldots, n\}$

In conjunction with these equations we add the equations

- $Q_i^1 := \Sigma_{j=1}^n x_{ij} - 1 = 0$ for $i \in \{1, 2, \ldots, n\}$

- $Q_{ijk}^2 := x_{ij} x_{ik} = 0$ for $i, j \neq k \in \{1, 2, \ldots, n\}$

For all values for n where $n \neq 0$ modulo p, there is NS-refutation (PC-refutation) of a very low degree over field of characteristic p that refutes the polynomial equations $Q_e = 0, Q_{e,f} = 0$ and $Q_i = 0$. When $n = 0$ modulo p the modulo p equations has a solution and can thus be refuted. The pigeonhole principle require even PC refutation degree $n/2$ according to Razborov [19].

This suggest that the combined principle has degree complexity $n/2$ when $n = 0$ modulo p, and has constant degree complexity for $n \neq 0$ modulo p. That this is indeed the case follows from lemma (we also need for the undecidability result).

Lemma 3 : *Let Γ and Δ be two collections of polynomials in disjoint set of variables. Assume that Γ is unsatisfiable (i.e. that the polynomials in Γ have no common zero) and assume that Δ is satisfiable (i.e. that the polynomials in Δ have a common zero). Then the collection Γ has a NS-refutation (PC-refutation) of degree d if and only if $\Gamma \cup \Delta$ has a NS-refutation (PC-refutation) of degree d.*

Proof: Assume $\Sigma_{P_\gamma \in \Gamma} Q_\gamma P_\gamma + \Sigma_{P_\delta \in \Delta} Q_\delta P_\delta = 1$ is a NS-derivation of degree d. The polynomials in Δ has a common zero $\vec{\eta}$. Since the set of variables are disjoint, it follows that $\Sigma_{P_\gamma \in \Gamma} Q_\gamma P_\gamma + \Sigma_{P_\delta \in \Delta} Q_\delta P_\delta(\vec{\eta}) = \Sigma_{P_\gamma \in \Gamma} Q_\gamma P_\gamma$ defines the 1 polynomial in the variables associated to Γ. In other words $\Sigma_{P_\gamma \in \Gamma} Q_\gamma P_\gamma = 1$. This shows the "if" direction for NS-refutations.

Assume $P_1, P_2, \ldots, P_j, \ldots, 1$ is a PC-derivation $\Gamma \cup \Delta \vdash_d 1$. Let $\vec{\eta}$ be a common zero of the polynomials in Γ, and substitute $\vec{\eta}$ into the variables associated with Γ. We get a PC-derivation of polynomials in the variables associated with Δ of the formal 1 polynomial. This derivation has degree $\leq d$. This shows the "if" direction for PC-refutations.

The "only if" case is trivial for NS-refutations (let $Q_\gamma = 0$ for each $P_\gamma \in \Gamma$). The "only if" case is even more trivial for PC-refutations (view a PC-refutation of Δ as a PC-refutation of $\Delta \cup \Gamma$). ♣

5 The fluctuating case

We now show that case 4, the fluctuating case is nonempty. The idea is to consider a weak version of the bijective pigeonhole principle that states that there is no bijection from n to $2n$. The violation of this principle can be written as a conjunction of the following propositions:

- $\forall x \exists y R(x, y) \vee S(x, y)$
- $\forall y \exists x R(x, y)$
- $\forall y \exists x S(x, y)$
- $\forall x, y, z (y \neq z \rightarrow \neg R(x, y) \vee \neg R(x, z))$
- $\forall x, y, z (y \neq z \rightarrow \neg S(x, y) \vee \neg S(x, z))$
- $\forall x, y, z (y \neq z \rightarrow \neg R(x, y) \vee \neg S(x, y))$
- $\forall x_1, x_2, y (x_1 \neq x_2 \rightarrow \neg R(x_1, y) \vee \neg R(x_2, y))$
- $\forall x_1, x_2, y (x_1 \neq x_2 \rightarrow \neg S(x_1, y) \vee \neg S(x_2, y))$

The translation of this system of propositions leads after a few cosmetic changes to the following system of polynomial equations:

- $Q^1_i := \Sigma_j x_{ij} + \Sigma_j y_{ij} - 1 = 0$ for $i \in \{1, 2, \ldots n\}$
- $Q^2_j := \Sigma_i x_{ij} - 1 = 0$ for $j \in \{1, 2, \ldots n\}$
- $Q^3_j := \Sigma_i y_{ij} - 1 = 0$ for $j \in \{1, 2, \ldots n\}$
- $Q^4_{ijk} := x_{ij} x_{ik} = 0$ for $i, j \neq k \in \{1, 2, \ldots n\}$
- $Q^5_{ijk} := y_{ij} y_{ik} = 0$ for $i, j \neq k \in \{1, 2, \ldots n\}$
- $Q^6_{ijk} := x_{ij} y_{ik} = 0$ for $i, j, k \in \{1, 2, \ldots n\}$
- $Q^7_{ijk} := x_{ji} x_{ki} = 0$ for $i, j \neq k \in \{1, 2, \ldots n\}$
- $Q^8_{ijk} := y_{ji} y_{ki} = 0$ for $i, j \neq k \in \{1, 2, \ldots n\}$

The equations $x^2_{ij} - x_{ij} = 0$ and $y^2_{ij} - y_{ij}$ that are a part of the translation procedure are superfluous since they follow by a (constant degree) NS-derivation (PC-derivation) from the other equations. In order to see this consider for each $i, j \in \{1, 2, \ldots, n\}$ the equations $x_{ij} Q^2_j = 0$ and $y_{ij} Q^3_j = 0$, combined with the equations $Q^7_{ijk} = 0$ and Q^8_{ijk} where $i, j, k \in \{1, 2, \ldots, n\}$.

We will show that over any field F of finite characteristic p, this system of equations has NS-refutation (PC-refutation) degree complexity that is asymptotically of the fluctuating type.

Notice, that there are $5n^3 - 4n^2 + 3n$ equations. These equations have no solution since a solution could be used to define a bijection from $\{1, 2, \ldots n\}$ to $\{1, 2, \ldots 2n\}$ violating a 'weak' version of the pigeonhole principle. Thus for each n the constant polynomial 1 belongs to the ideal generated by polynomials $Q^1_i, Q^2_j, \ldots Q^8_{ijk}$. Further, there exist polynomials $P^1_i, P^2_j, \ldots P^8_{ijk}$ such that $\Sigma_i P^1_i Q^1_i + \Sigma_j P^2_j Q^2_j + \ldots + \Sigma_{ijk} P^8_{ijk} Q^8_{ijk} = 1$. Let $d_P(n)$ denote the maximal degree of a summand in this expression, and let $d_{NS}(n)$ denote the equations NS-degree complexity i.e. the smallest value of $d_n(n)$ when P range over all possible choices of polynomials $P^1_i, P^2_j, \ldots P^8_{ijk}$.

The equations can be simplified by relabeling the variables! Consider the equations:

- $\Sigma^m_{j=1} x_{ij} - 1 = 0$ for $i = 1, 2, \ldots n$
- $\Sigma^n_{i=1} x_{ij} - 1 = 0$ for $j = 1, 2, \ldots m$
- $x_{ij} x_{ik} = 0$ for $i = 1, 2, \ldots n$
  and $j < k \in \{1, 2, \ldots m\}$
- $x_{ji} x_{ki} = 0$ for $i = 1, 2, \ldots m$
  and $j \neq k \in \{1, 2, \ldots n\}$

Now since $xy = yx$ the system of equations remains essentially unchanged if we drop the requirement $j < k$ and replace the third set of equations with:

- $x_{ij} x_{ik} = 0$ for $i = 1, 2, \ldots n$
  and $j \neq k \in \{1, 2, \ldots m\}$

The new slightly modified system has the same set of solutions. The new system contains $6n^3 - 4n^2 + 3n$ equations. This system of equations has already been analyzed in [2].

If we let $m = 2n$ and let $x_{i,n+j} := y_{ij}$ we notice that this system of equations is identical to the former system (still of course containing $5n^3 - 4n^2 + 3n$ equations). If we modify the original system by adding the equations

- $Q^9_{ijk} := y_{ij} x_{ik} = 0$ for $i, j, k \in \{1, 2, \ldots n\}$

to the original system of equations, we get a new system of equations that is equivalent to the original system, but contains same $6n^3 - 4n^2 + 3n$ equations as belong to the "$\mathrm{PHP}^m_n(onto)$".

Let F_p denote a fixed field of characteristic $p \neq 0$. Then the system of polynomial equations in [2] for the bijective pigeonhole principle $\mathrm{PHP}^{n+p^l}_n(bij)$ that states that there is no bijection from a set D with n elements to the set R with $n + p^l$ elements.

Proposition (Beame, Riis) *Let F be any field of characteristic p. If $p^l < n$, there is a NS-refutation of $PHP^{n+p^l}_n(bij)$ of degree $p^l - 1$. On the other hand if $n \geq ((p+2)^l - p^l)/2$ then any Nullstellensatz refutation of $PHP^{n+p^l}_n(bij)$ must have degree at least $2^l - 1$.*

Proof: The first part is Lemma 16 in [2] while the second part is Theorem 12 in [2]. ♣

We need a slight variation (and in many ways a weaker version) of this proposition

Lemma 4 : *Let F be any field of characteristic p. If $p^l < n$, for each $r \neq 0$ modulo p with $rp^l < n$ there is a NS-refutation of $PHP^{n+rp^l}_n(bij)$ of degree $p^l - 1$. On the other hand any Nullstellensatz refutation of $PHP^{n+rp^l}_n(bij)$ must have NS-refutation degree in $\Omega(\log(n))$*

Proof: The proof follows very closely the argument in [2] with minor changes. Better bounds can be achieved using , however for our application we only need relatively weak NS-degree lower bounds. For more details see the technical report [22]. ♣

From Lemma 4 it follows that the translation of the FO-formula ψ leads to a sequence ψ_n that has NS-degree refutation complexity of the fluctuating type. It follows from Theorem 10 (that is a simple consequence of a result by Krajicek (lemma 9)), that ψ_n also has PC-degree refutation complexity of the fluctuating type.

6 Undecidability of the asymptotic behavior

We have shown that a given FO formula ψ, translates into a sequence ψ_n of polynomial equations that has a NS-refutation complexity [PC-refutation complexity] that has exactly one of four types of behaviors, $1, 2, 3$ and 4. Let $A \subset \{1, 2, 3, 4\}$ be a proper non-empty subset. In this section we will show that the problem of deciding if a given first order formula ψ leads to a sequence ψ_n that has a complexity behavior of a type belonging to A - is undecidable.

Lemma 5 : *Let ψ be a FO-formula.*

If ψ is of type 1 i.e. if ψ_n has constant degree complexity for all but finitely n (where the degree complexity is ∞), then for any formula η (irrespective of its type), $\psi \wedge \eta$ is also of type 1.

If ψ is of type 2 i.e. if ψ_n has degree complexity $\geq l(n)$ for all n, then for any η the formula $\psi \wedge \eta$ has the same type as η.

Proof: Obvious given lemma 3. ♣

Lemma 6 : *There is a class Θ of FO formulae such that membership of Θ is recursive. For each $\psi \in \Theta$ there are two exclusive possibilities:*

i) ψ is valid in all finite models

ii) ψ is invalid in all sufficiently large finite models as well as in all infinite models.

Furthermore, there is no decision procedure that in general decides whether case i) or case ii) applies to a given $\psi \in \Theta$.

Proof (brief outline): For a more detailed outline see [22]. Consider the collection of FO sentences that contains a conjunction of the axioms of Robinson's Q modified so these define a general unspecified initial seqment of the natural numbers (like in Paris' and Wilkie's definition of an initial segment with a "top" element). These axioms force any finite model of propositions in Θ to define an initial segment of the set of the natural numbers). For each pair of polynomials S and R (with coefficients in the natural numbers) add axioms $\eta_{S,R}$ that define the polynomials S and R on the initial segment. Finally in conjunction to this add the FO proposition that states that the equation $S = R$ has no (integer) solutions in the initial segment $\{1, 2, \ldots, n\}$. Let $\psi_{S,R}$ denote the resulting FO formula and let Θ consist of the class of all such $\psi_{S,R}$.

Now the point is that the FO formula $\psi_{S,R}$ has a model of size n if and only if $S = R$ has no solution where all variables have values in $\{1, 2, \ldots, n\}$. Consequently the diophantine equation $S = R$ has no solution in the natural numbers if and only if $\psi_{S,R}$ is valid in all finite models. According to a variant of the unsolvability of Hilbert's 10th problem this decision problem is unsolvable. (the variant states that the decision problem whether a given polynomial with integer coefficients has a zero in the natural numbers is undecidable).

If $\psi_{S,R}$ is invalid (i.e. if the equation $S = R$ has a solution over the natural numbers), the formula $\psi_{S,R}$ is also invalid in infinite (non-standard) models, since these models contain the standard natural numbers. ♣

Lemma 7 : *If ψ is an FO-formula such that ψ is unsatisfiable in all models (finite as well as infinite), then there exists for each field F a number $d \in N$ such that each ψ_n has a degree d NS-refutation.*

Proof: The proof is somewhat similar to the proof that such formula ψ leads to sequences ψ_n of propositional formula that have polynomial tree-resolution refutations [21]. And it is similar to the proof that the such ψ has constant rank Lovasz-Schrijver refutation [7]. Please see the technical report [22] for the details. ♣

Lemma 8 : *The decision problem whether a given first order formula ψ leads to a sequence ψ_n that has a complexity behavior in A - is undecidable.*

Proof: Given a non-empty proper subset $A \subset \{1, 2, 3, 4\}$, without loss of generality we can assume that $1 \in A$ (otherwise replace A with $\{1, 2, 3, 4\} \setminus A$).

Since A is a proper subset, at least one of $2, 3$ or 4 does not belong to A. Pick a FO formula ψ of a type not in A (i.e. type $2, 3$ or 4). Now for each $\theta_{S,R} \in \Theta$ consider the FO formula $\theta_{S,R} \wedge \psi$. Now according to lemma 6 and lemma 7 any $\theta_{S,R} \in \Theta$ is either of type 1 (if it is unsatisfiable for some $n \in N$) or of type 2 (if it is satisfiable for all $n \in N$). Thus, according to lemma 5, $\theta_{S,R} \wedge \psi$ is of type 1 if and only if $\theta_{S,R}$ is of type 1, which happens if and only if the equation $S = R$ has a solution on N. ♣

7 NS versus PC

In general the exists a sequence of polynomial equations that have constant PC-refutation degree complexity, while the sequence have linear NS-refutation degree complexity. If however, we restrict ourself to the uniform sequences generated by a FO formula, Krajicek [15] have shown that such a situation cannot occur.

Lemma 9 : [Krajicek] [15] *Let $S \subseteq N$ be a fixed infinite set. Assume that ψ_n has degree d PC-refutations for each $n \in S$. Then there exists a constant $d' \geq d$ such that each ψ_n with $n \in S$, has a degree d' NS-refutation.*

Theorem 10 : *For an FO-formula ψ, the type of ψ with respect to the NS-refutation complexity behavior of ψ_n is identical to the type of ψ with respect to the PC-refutation complexity behavior of ψ_n.*

Proof: A direct application of lemma 9, shows that a FO-formulae of type 1,2 or 3 with respect to to NS-refutations (PC-refutations) has the same type with respect to PC-refutations (NS-refutations). It follow then from Theorem 1 that a first order formula ψ is of type 4 with respect to NS-refutation complexity if and only if it is of type 4 with respect to PC-refutation complexity. ♣

8 Final remarks

The big question is whether the main result remain valid for faster growth rates. We conjecture - in fact spend some considerable effort in trying to prove this - that the main theorem remains valid if l has growth rate n^{ϵ} for some sufficiently small $\epsilon > 0$ for the NS-case (and possibly for the PC-case). Such a result would be important as it would unify many known results.

One consequence of Theorem 1 is that the translation of any FO formula ψ leads to a sequence ψ_n that *asymptotically* has worst case refutation degree complexity that *either* is constant (case 1) *or* has growth rate $\Omega(l(n))$ (case 2,3,4). Thus according to the current version of Theorem 1, any non-constant lower bound on the NS-refutation degree [PC-refutation degree] automatically "lifts" to an $\Omega(l(n))$ lower bound NS-refutation degree [PC-refutation degree]. If Theorem 1, could be shown to be valid for $l \in n^{\Omega(1)}$ by the same argument, any non-constant lower bound could be lifted to a $n^{\Omega(1)}$-degree lower bound.

Another interesting question is if it possible to extend Krajicek's model theoretic approach to include model theoretical criteria that correspond to the fluctuating NS-degree (PC-degree) refutation complexity.

References

[1] P. Beame, R. Impagliazzo, J. Krajicek, T. Pitassi, and P. Pudlak. Lower bounds on hilbert's nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73(3):1–26, 1996.

[2] P. Beame and S. Riis. More on the relative strength of counting principles. *DIMACS Series in Discrete Maths. and Theoretical Computer Science*, 39:13–35, 1998.

[3] M. Bonet and N. Galesi. Optimality of size-width tradeoffs for resolution. Technical Report 10(4), Computational Complexity, 2001. 261-276.

[4] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the groebner basis algorithm to find proofs of unsatisfiability. *Proceedings of the 28th ACM STOC*, pages 174–183, 1996.

[5] S. Cook and P. Nguyen. Foundations of proof complexity: Bounded arithmetic and propositional translations. Technical report, Book (Draft version), 2008.

[6] S. Cook and R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[7] S. Danchev. Complexity gap for sherali-adams and lovsz-schrijver proof systems. *STOC*, 2007.

[8] S. Dantchev, B. Martin, and S. Szeider. Parameterized proof complexity. *FOCS*, 2007.

[9] S. Dantchev and S. Riis. Tree resolution proofs of the weak pigeon-hole principle. *The 16th annual IEEE Conference on Computational Complexity*, pages 69–75, June 2001.

[10] S. Dantchev and S. Riis. On complexity gaps for resolution-based proof systems. *The 12th Annual Conference on the*

EACSL, Computer Science Logic, LNCS 2803, Springer, pages 142–154, August 2003.

[11] D. Grigoriev and E. Hirsch. Algebraic proof systems over formulas. *Theoretical Computer Science*, 3:83–102, 2003.

[12] J. Krajicek. Lower bounds on the size of constant-dept propositional proofs. *Journal of Symbolic Logic*, 59(3):73–86, 1994.

[13] J. Krajicek. *Bounded arithmetic, propositional logic and complexity theory*, volume 60, chapter Encyclopefia of Mathematics and its applications, pages 1–772. Cambridge University Press, 1995.

[14] J. Krajicek. Uniform families of polynomial equations over a finite field and structures admitting euler characteristic of definable sets. *Proc. London Mathematical Society,*, 81(3):257–284, 2000.

[15] J. Krajicek. On the degree of ideal membership proofs from uniform families of polynomials over a finite field. *Illinois J. of Mathematics*, 45(1):41–73, 2001.

[16] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. *Methods in Mathematical logic, Springer-Verlag*, LNM 1130:317–340, 1985.

[17] T. Pitassi. Algebraic propositional proof systems. *Dimacs Discrete Mathematics and Theoretical Computer Science (Vol 31)*, 10:179–209, 1997.

[18] R. Raz. Resolution lower bounds for the weak pigeonhole principle. *Journal of Association for Computing Machinery 51(2)*, 51(2):115–138, 2004.

[19] R. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7:291–324, 1998.

[20] S. Riis. *Arithmetic, proof and complexity*, chapter Making infinite structures finite in models of bounded arithmetic, pages 289–319. Oxford University Press, 1993.

[21] S. Riis. A complexity gap for tree-resolution. *Computational Complexity*, 10:179–209, 2001.

[22] S. Riis. On the asymptotic nullstellensatz and polynomial calculus proof complexity. Technical report, www.dcs.qmul.ac.uk/ smriis, 2008.