

# On the asymptotic Nullstellensatz and Polynomial Calculus proof complexity

Søren Riis \*

February 4, 2009

## 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 Krajíček, 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 mutually 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 at least  $l(n)$  except in a finite number of regular subsequences of infinite size, where the degree is constant.
- (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  $\psi$  has type belonging to  $A$  - is undecidable.

---

\*Department of Electro Engineering and Computer Science,  
Queen Mary, University of London  
Email: smriis@dcs.qmul.ac.uk

# 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*  $\psi$  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  $\psi$  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  $\psi$  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  $\Psi$  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 Reckhow [14] put forward a program (for proving  $\text{NP} \neq \text{co-NP}$ ) where the idea is to obtain super-polynomial lower bounds for stronger and stronger propositional proof systems. Cook and Reckhow noticed that showing  $\text{NP} \neq \text{co-NP}$  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 beyond current techniques are often referred to as *strong* propositional proof systems [22]. 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). In fact the DLL-algorithm - the undisputed most popular sat solving algorithm - is based on an even weaker proof system: *regular resolution*. It has been shown that regular resolution for some classes of tautologies is performing exponentially worse than resolution (for a recent result in this direction see [36]).

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 (longer) 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 [12] Cook introduced a general method of translating statements of Bounded Arithmetic into polynomial size families of propositional formulas, in such a way that theorems translate into tautology families with small proofs in a particular proof system (extended Frege). Later in [27] Paris and Wilkie introduced the idea of basing the translation on an uninterpreted function (relation) symbol, while fixing an interpretation of all the other symbols. The Paris-Wilkie translation can be seen as a special case of the translation of  $\Sigma_0^B$  formulas that Cook and Nguyen introduce in [13].

The method of translation we consider in this paper can be viewed as a special case of the Paris-Wilkie translation where *all* relations and symbols are uninterpreted. In the general translation each  $\Sigma_0^B$  formula  $\eta$  of Bounded Arithmetic is translated into a sequence  $\eta[n]$  of propositional propositions. Our main result is not valid in this general translation. *It is crucial for our*

result that function and relation symbols are all uninterpreted, and that there are no special build-in relations (functions) with a predefined interpretation.

Let  $\Theta$  denote the class of first order formulae in predicate logic (FO formulae <sup>1</sup>) that have no finite models. Then the translation of each  $\psi \in \Theta$  leads to a sequence  $\psi[n]$  of unsatisfiable proposition formulae. Informally, the proposition  $\psi[n]$  states that  $\psi$  has no model of size  $n$ . The general idea is for a given weak propositional system to characterize the class of  $\psi$  for which the sequence  $\psi[n]$  has short (or requires long) proofs.

In [23, 25] Krajicek initiated the study of how particular weak propositional proof systems are coping with uniform systems of polynomial equations corresponding to unsatisfiable propositions. For a given propositional proof system  $\mathcal{R}$  (commonly presented as a *refutation system* where the aim is to refute a proposition), Krajicek's approach was to provide a general model theoretic criteria that together with a general increasing function  $f : N \rightarrow N$  (e.g. a function of super polynomial growth rate), would ensure that any FO sentence  $\psi \in \Theta$  that satisfies the model theoretic criteria would lead to a sequence  $\psi[n]$  of unsatisfiable propositions, that asymptotically 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 sentence  $\psi \in \Theta$  is valid in some infinite model. In [31] Riis showed that  $\psi$  is valid in some infinite model if and only if  $\psi[n]$  (represented as a statement expressed in uninterpreted relational symbols) is independent (i.e. without proof or refutation) in the system  $T_2^1(\alpha)$  of bounded arithmetic.

From a combinatorial perspective (disregarding certain technical issues related to forcing in non-standard models of Bounded Arithmetic) the if-direction was later improved by Krajicek [23], when he showed that any FO sentence  $\psi \in \Theta$  that holds in some infinite model, leads to a sequence  $\psi[n]$  that requires exponential size ( $2^{\Omega(\sqrt{n})}$ ) 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 pigeonhole principle are hard for tree-resolution.

For a fixed field  $F$ , Krajicek showed in [25, 24] that if there is an infinite model equipped with a suitable Euler structure in which  $\psi$  is valid, then  $\psi[n]$  requires *Nullstellensatz* (NS) refutations of degree  $\Omega(\log(n))$  and requires

---

<sup>1</sup>We use the notions *FO formulae* and *FO sentence* interchangeable since we adopt the common convention that a formula with free variables is valid in a model when its valid for all interpretations of the free variables

*Polynomial Calculus* (PC) refutations of degree  $\Omega(\log \log(n))$ .

Informally Krajíček's criteria capture in some sense the class of FO sentences that lead to such hard tautologies with respect to the propositional system in focus. This informal interpretation is reflected in Krajíček's terminology when he in [26] says that his model theoretic criterion (different for different propositional proof systems) "corresponded" to the proof system. Krajíček's showed in [26, 24] that the NS and PC refutation systems over a finite prime field  $F_p$  has a covering class of Euler structures with a suitable Grothendieck ring (Krajíček's terminology). It should be emphasised that this correspondence is not "exact" in the sense that the notion exactly identify the class of FO formula  $\psi$  for which  $\psi[n]$  has constant degree NS-refutations (PC-refutations).

A related, but different approach was introduced by Riis [32] suggesting that (weak) propositional proof systems in general might have so-called complexity gaps. Riis showed that the tree-resolution propositional proof system have a complexity gap and that Krajíček's model theoretic criterion for tree-resolution is in fact a characterisation. More specifically, for any formula  $\psi$  in predicate logic there are two disjoint possibilities: *Either* the sequence  $\psi[n]$  has polynomial size tree-resolution refutations *or* the sequence  $\psi[n]$  requires full exponential size  $2^{\Omega(n)}$  tree-resolution refutations. Furthermore, case (2) applies if and only if  $\psi$  is valid in some infinite model (the refutations tree-resolution complexity is set to  $\infty$  if the formula  $\psi[n]$  is satisfiable).

Notice, that the number of boolean variables in  $\psi$  generally is  $n^c$  for some  $c > 1$  that depends on  $\psi$ . Thus it is possible for the refutation complexity to be as bad as  $2^{n^c}$ . Danchev and Riis showed in [17] that for tree-like resolution there are no complexity gaps above  $2^{\Omega(n \log n)}$ . 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  $\psi$  in predicate logic there are three distinct cases: (1)  $\psi[n]$  has polynomial size tree-resolution refutations (2) the sequence  $\psi[n]$  has size  $2^{O(n)}$  tree-resolution refutations but require tree-resolutions of  $2^{\Omega(n)}$  (3)  $\psi[n]$  requires size  $2^{\Omega(n \log(n))}$ - tree-resolution refutations. This conjecture is still open.

In [35] it was shown that the statement  $GT_n$  that (falsely) asserts that *there is a directed acyclic ordering on  $n$  nodes* has size  $n^2$  (dag-like) resolution refutations. Contrary to that in [5] it was shown that  $GT_n$  require exponential tree-resolution refutation. This last statement also follows from [32], since there exists an infinite linear ordering (e.g.  $(\mathbb{Z}, <)$ ) with no minimal element. From this difference between resolution and tree-resolution it follows that *if*

there is a model theoretic criterion for full sequential (dag-like) resolution it must be *different* from that for tree-resolution. However, Danchev and Riis showed in [18] that the characterisation for tree-resolution remains valid for full dag-like resolution provided we consider "relativised" FO formula  $\psi$  in predicate logic (for definition see [18]). This answered an open question by Krajicek and showed that for each relativised FO formula  $\psi$  there are two disjoint possibilities: (1) the sequence  $\psi[n]$  has polynomial size resolution refutations (2) the sequence  $\psi[n]$  requires full exponential size resolution refutations. Furthermore, case (2) applies if and only if  $\psi$  is valid in some infinite model.

It is an open question whether for any FO-formula  $\psi$  are two disjoint possibilities: (1) the sequence  $\psi[n]$  has polynomial size resolution refutations OR (2) the sequence  $\psi[n]$  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 [29]. Also another difficulty is that it is not clear that there is a simple model theoretic criterion that exactly captures the class of  $\psi$  for which  $\psi[n]$  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 [15, 16] for precise definitions of the involved concepts.

**Theorem A** : (S. Danchev and B. Martin) (Improvement of [15])

*Given a FO sentence  $\psi$  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  $\psi$  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)([16])

*Given a FO sentence  $\psi$ , which fails in all finite models. Consider the sequence of parametrised contradictions  $(C_{\psi,n,k})_{n \in \mathbb{N}}$  is a translation of  $\psi$ . 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 parametrised tree-like resolution refutation of size  $\beta^k n^\alpha$  for some constants  $\alpha$  and  $\beta$  which depends of  $\psi$  only.

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

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

### 1.3 Algebraic proof complexity

The Nullstellensatz (NS) proof system [3] and Polynomial Calculus (PC) [11] are two of the most popular algebraic proof systems. These systems have been studied quite intensively since their introduction in the mid 1990s. Both systems are used to establish the truths of tautologies using reasoning about polynomials over a field, based on Hilberts Nullstellensatz. One nice feature of algebraic proofs is that small degree proofs can be found quickly by for example using a modification of the Grobner basis algorithm [28].

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

One version of Hilbertz Nullstellensatz states that the polynomials in  $\Gamma$  have no common root if and only if the identity polynomial 1 belongs to the ideal generated by the polynomials in  $\Gamma$ . In other worlds there exists for each

polynomial  $p_j \in \Gamma$  a polynomial  $r_j \in F[x_1, x_2, \dots, x_u]$  such that

$$\sum_{j=1}^{\lambda} r_j p_j = 1$$

The expression  $\sum_{j=1}^{\lambda} r_j p_j = 1$  constitutes a Nullstellensatz proof. The degree of the proof is defined as the maximal degree of the polynomials  $r_j p_j$ ,  $j = 1, 2, \dots, \lambda$  before terms in  $r_j p_j$  are cancelled out [i.e. the degree is  $\max_j(\deg(r_j) + \deg(p_j))$ ].

The question of the degree of the polynomials  $r_i$  has been studied in the context of the *efficient Nullstellensatz* by Brownawell [6], Kollar [21] and Caniglia et. al. [10]. The general optimal degree bounds are doubly exponential in the number of variables. In the context of propositional proof complexity we can think of each polynomial in  $\Gamma$  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 ( $1 = 0$ ).

In most applications in propositional logic each variable  $x_1, x_2, \dots, x_n$  is assumed to be boolean i.e. to take 0/1-values. From this perspective true is 1, false is 0,  $\neg x$  is the same as  $1 - x$ , a conjunction  $x \wedge y$  is the same as the product  $xy$  and a disjunction  $x \vee y$  is the same as  $x + y - xy$ . As explained in [7] each propositional formula  $\psi(\vec{x})$  then corresponds to an algebraic term  $t(\vec{x})$  such that  $\psi(\vec{x})$  and  $t(\vec{x})$  has the same assignments of 0/1-values to the variables  $\vec{x}$ . For each boolean variable  $x$  the equation  $x^2 - x$  is assumed to belong to  $\Gamma$ <sup>2</sup>. In general if all solutions are 0/1-solutions we do not need to assume that  $F$  is algebraically closed. In fact Buss noticed (Theorem 9 in [7]) that when the polynomials  $\vec{t}$  take only 0/1 values on 0/1 inputs, all results valid over commutative rings.

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  $\Gamma$ . This is done in a logic style derivation using the following

---

<sup>2</sup>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  $\Gamma$ . 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



two rules

$$\frac{q \quad p}{q + p} \quad (\text{cut})$$

and

$$\frac{q}{rq} \quad (\text{weakening})$$

where  $q, p$  are polynomials and  $r$  is any monomial. We have adopted the terminology *cut* and *weakening* since these are the logical inference rules that naturally corresponds to these rules. Given the set  $\Gamma$  of polynomials, a PC refutation of  $\Gamma$  is a sequences  $q_1, q_2, \dots, q_s = 1$  of polynomials where each polynomial is either a premise (i.e. belongs to  $\Gamma$ ) 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  $q_1, q_2, \dots, q_s$ . It does not affect the validity or degree of derivations if we allow  $r$  to be a proper polynomial in the weakening rule, but in this case the degree of  $rq$  has to be calculated before terms are cancelled out.

The NS proof system as well as PC are *sound* over any commutative ring and in the case polynomials that takes 0/1 values on 0/1 inputs the NS proof system as well as PC are *complete* over any commutative ring [7].

Finally, we would like to pay attention to the  $\mathcal{F}$ -PC refutation system defined in [19] partly based on a suggestion in [28]. As noticed by a number of authors, the definition of PC does not constitute a Cook-Reckhow 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 [19] 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.

## 1.4 The translation procedure

The translation of a FO formula  $\psi$  to a sequence of  $\psi[n]$  of propositional formula (polynomial equations) is carried out in two steps.

The first step is to convert  $\psi$  into a *special* quantifier free formula  $\psi'$  on conjunctive normal form (i.e. as a conjunction of disjunctions).

The second step is to use the Paris-Wilkie translation and translate  $\psi'$  to a sequence  $\psi[n]$  of propositions in propositional logic. Each function and relation symbol in  $\psi'$  is uninterpreted. In our setting where we consider algebraic proof systems, so the translation is modified to a sequence of polynomial equations.

Let  $L = L(f_1, f_2, \dots, f_k, \dots, R_1, R_2, \dots, R_l, \dots)$  be a fixed first order language with an unlimited (i.e. countable infinite) number of function symbols of each arity, as well as an unlimited number of relation symbols of each arity. We let  $Var_{FO} = \{x_1, x_2, \dots, x_r, \dots\}$  denote a countable infinite set of variables and let  $FO(L, Var_{FO})$  denote the class of first order formula in the language  $L$  and (free) variables in  $Var_{FO}$ .

We consider a special subset  $S$  ( $S$  for special) of  $FO(L, Var_{FO})$  formulae that is a conjunction of disjunctions that each is an atomic (or negation of an atomic) formula on one of the following two forms:

$$\begin{aligned} R(v_1, v_2, \dots, v_k) \text{ for some } k\text{-ary relation symbol } R \in L \\ \text{with } k \in \{1, 2, \dots\} \text{ and } v_1, v_2, \dots, v_k \in Var_{FO} \end{aligned} \quad (\text{I})$$

$$\begin{aligned} v_{k+1} = f(v_1, v_2, \dots, v_k) \text{ for some } k\text{-ary function symbol } f \in L \\ \text{with } k = \{0, 1, 2, \dots\} \text{ and } v_1, v_2, \dots, v_k, v_{k+1} \in Var_{FO} \end{aligned} \quad (\text{II})$$

As usual 0-ary function symbols are called constants and an atomic formula involving a constant  $c$  is of the form  $v = c$  for some  $v \in Var_{FO}$ . Atomic formula of the form  $v_i = v_j$  are also included in (II).

Using the Paris-Wilkie translation it is straight forward to translate any quantifier free formula in  $S$  into a sequence of polynomial equations. The degree of the polynomial equations is bound from above by a constant that is independent of  $n$ . The conversion of a general FO-formula into a quantifier free formula in  $S$  and the point that this translation procedure leads to polynomial equations of bounded degree was discussed in [34] as well as in [26].

### Example

Consider the unsatisfiable FO-sentence

$$\psi \equiv: \forall x \exists y \forall z R(x, y, z) \wedge \exists x \forall y \exists z \neg R(x, y, z) \quad (\text{C1})$$

This example was also considered in [32]. The first step in the translation is to convert  $\psi$  into a quantifier free formula that belongs to  $S$ . To this end, we introduce Skolem Functions and get

$$\psi' \equiv: R(x, f(x), z) \wedge \neg R(c, y, g(y)) \quad (\text{C2})$$

This formula is still not in  $S$  so we modify it further and get

$$\psi'' \equiv: (\neg y = f(x) \vee R(x, y, z)) \wedge (\neg u = c \vee \neg w = g(v) \vee \neg R(u, v, w)) \quad (\text{C3})$$

that is the required formula in  $S$ .

The second step is for each  $n \in N$  to convert the formula  $\psi''$  into a propositional formula (system of polynomial equations) that states that essentially claim (incorrectly) that  $\psi'$  is satisfiable in a model of size  $n$ . The polynomial equations  $\psi[n]$  has variables in  $f_{i,j}$   $i, j \in \{1, 2, \dots, n\}$ ,  $c_j$   $j \in \{1, 2, \dots, n\}$ ,  $g_{i,j}$   $i, j \in \{1, 2, \dots, n\}$  and  $r_{ijk}$   $i, j, k \in \{1, 2, \dots, n\}$  (i.e. consists of polynomials that each contains potentially  $n^3 + 2n^2 + n$  distinct variables). The formula  $\psi''$  translate into the polynomial equations:

$$f_{i_1, i_2}(1 - r_{i_1, i_2, i_3}) = 0 \text{ for } i_1, i_2, i_3 \in \{1, 2, \dots, n\} \quad (\text{Eq 1})$$

$$c_{i_4} g_{i_5, i_6} r_{i_4, i_5, i_6} = 0 \text{ for } i_4, i_5, i_6 \in \{1, 2, \dots, n\} \quad (\text{Eq 2})$$

$$\left(\sum_j c_j\right) - 1 = 0 \quad (\text{Eq 3})$$

$$\left(\sum_j f_{i,j}\right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{Eq 4})$$

$$\left(\sum_j g_{i,j}\right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{Eq 5})$$

$$r_{i_1, i_2, i_3}^2 - r_{i_1, i_2, i_3} = 0 \text{ for } i_1, i_2, i_3 \in \{1, 2, \dots, n\} \quad (\text{Eq 6})$$

$$f_{ij} f_{ik} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{Eq 7})$$

$$g_{ij} g_{ik} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{Eq 8})$$

$$c_i c_j = 0 \text{ for } i \neq j \in \{1, 2, \dots, n\} \quad (\text{Eq 9})$$

The FO-formula  $\psi$  (as well as  $\psi'$  and  $\psi''$ ) fail in ALL models (finite as well as infinite). We will show (Proposition A and Lemma 7) that this ensures that the system of polynomial equations has constant (independent of  $n$ )

degree NS-refutations. As it happens the system  $\psi[n]$  of equations in the example has a degree 4 NS-refutation for each value of  $n$ :

$$\begin{aligned} & \sum_{i,j,k} (c_i g_{jk}) [f_{ij}(1 - r_{ijk})] + \sum_{i,j,k} (f_{i,j}) [c_i g_{j,k} r_{i,j,k}] + \sum_{i,j} (-c_i f_{i,j}) [(\sum_k g_{j,k}) - 1] \\ & + \sum_i (-c_i) [(\sum_j f_{i,j}) - 1] + (-1) [(\sum_i c_i) - 1] = 1 \end{aligned} \quad (\text{D1})$$

Notice that only Eq1-Eq5 were needed for this derivation.

## 2 The main result

To state the main result in more 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  $\psi[n]$  without requiring that each  $\psi[n]$  is unsatisfiable.

The main result can be stated as follows:

**Theorem 1** : *For each prime  $p$  and for each FO formula  $\psi$  there exists a non-decreasing 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  $\psi$  (a collection of polynomial equations) leads to sequence  $\psi[n]$  of polynomial equations with a refutation degree refutation complexity  $d(n)$  over fields of characteristic  $p$ , that behaves in one of 4 distinct ways:*

**T1)** *The degree refutation complexity  $d(n)$  is bound by a constant  $c < \infty$  (with possible finitely many exceptions where the degree complexity is  $\infty$ ).*

**T2)** *The degree refutation complexity  $d(n)$  is at least  $l(n)$  for all values of  $n$ .*

**T3)** *The degree complexity  $d(n)$  is at least  $l(n)$  except in a finite number of regular subsequences of infinite size, where the degree is constant. Furthermore, membership of each subsequence is uniquely (with possible finitely many exceptions) determined the value of  $n$  modulo  $p^k$  for some  $k$ .*

**T4)** *The degree refutation complexity  $d(n)$  assumes arbitrary big values with  $d(n) < l(n)$  and for each specific  $n$  where  $d(n)$  is strictly less than*

$l(n)$ , there exists  $r$  such that  $d(m) = d(n)$  for all  $m > n$  with  $m = n$  modulo  $p^r$ .

*For any non-empty proper subset  $A \subseteq \{(i), (ii), (iii), (iv)\}$ , the decision problem of whether a given input FO formula  $\psi$  has type belonging to  $A$ , is undecidable. This undecidability result remains valid if we consider the promise decision problem where each  $\psi$  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  $\psi$  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  $\psi$  with even a slight irregular spectrum (i.e. where the set  $S$  for which  $\psi$  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  $\psi$  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  $\psi$  translates to a sequence  $\psi[n]$  that has the same type with respect to  $l'$  as it has with respect to  $l$ .

### 3 Background in the representation theory of the symmetric group

In [1, 2] Ajtai considered of a prime number  $p$  and a finite set  $A$  with  $n$  elements. For each sequence  $a = (a_1, a_2, \dots, a_k)$  of length  $k$  from the elements of  $A$  he introduced a variable  $x_a$ . In general if  $k_1, k_2, \dots, k_s$  is a finite collection

of natural numbers Ajtai introduced for each  $j = 1, 2, \dots, s$  and for each sequence  $a = (a_1, a_2, \dots, a_{k_j})$  a variable  $x_{a,j}$ . Ajtai considered systems of linear equations modulo  $p$  of the form

$$\sum_a u_a^{(i)} x_a \equiv b_i \text{ modulo } p \quad (\text{A1})$$

for  $i = 1, 2, \dots, l$ . More generally in [2] Ajtai considered systems of linear equations modulo  $p$  of the form

$$\sum_{j=1}^s \sum_a u_{a,j}^{(i)} x_{a,j} \equiv b_i \text{ modulo } p \quad (\text{A2})$$

for  $i = 1, 2, \dots, l$ . The system *symmetric* if for each permutation  $\pi$  of the set  $A$  and for each  $i = 1, 2, \dots, l$  the equation

$$\sum_a u_{\pi(a)}^{(i)} x_a = b_i \quad (\text{A3})$$

and in general

$$\sum_{j=1}^s \sum_a u_{\pi(a),j}^{(i)} x_{a,j} = b_i \quad (\text{A4})$$

is also an equation of the system. Ajtai also introduced the notion of a uniform sequence of linear equations (definition given below).

Ajtai showed that if we for  $n \geq n_0$ ,  $n \in N$  consider *uniform* sequences  $L[n]$  of such linear equations, then the question of whether  $L[n]$  has a solution is *not* a matter of the magnitude of  $n$ , but rather a question of the value of  $n$  modulo  $p^r$  for some constant  $r$  (provided  $n$  is sufficiently large). Ajtai obtained this result by showing that the representation theory of the symmetric group developed by James [20] could be modified to fit the setup where one is given an uniform sequence of linear equations (rather than just a single system of linear equations).

### Uniform sequence of linear equations

In many examples of systems of polynomial equations e.g. (Eq1)-(Eq9), the equations are given in a way that is intuitively quite uniform. Ajtai, captured this notion formally as follows: Suppose that  $A_0 \subseteq A_1$  and assume

that  $|A_1 \setminus A_0| > k$ . Suppose that  $u_1$  is a  $F$ -valued function defined on  $A_1^k \times \Gamma \times \{1, 2, \dots, l\}$  and  $b$  is a  $F$ -valued function defined on  $\{1, 2, \dots, l\}$  (the values of  $b$  will be denoted by  $b_1, b_2, \dots, b_l$ ). Then Ajtai would say (and so would Krajicek [25]) then say that a system of linear equations

$$\sum_{a \in A_1^k, \gamma \in \Gamma} u_{a, \gamma}^{(i)} x_{a, \gamma} = b_i \quad (\text{A5})$$

for  $i = 1, 2, \dots, l$  is based on the quadruplet  $u_1, A_1, A_0, b$  if the following holds for each  $A \supseteq A_1$ : For all  $i = 1, 2, \dots, l$  and  $(a, \gamma) \in A^k \times \Gamma$  if  $\pi$  is a permutation of  $A$  which fixes each element of  $A_0$  and  $\pi(a) \in A_1^k$ , then

$$u_{a, \gamma}^{(i)} = u_1((\pi(a), \gamma, i)) \quad (\text{A6})$$

Finally, Ajtai would say that a symmetric system  $E$  of linear equations is induced by the quadruplet  $u_1, A_0, A_1, b$  (over  $A$ ) if  $E$  is the *symmetric hull* (or *the closure under  $S_n$* ) of a system based on this quadruplet.

Instead of this somewhat technical definition we will give an alternative but equivalent definition that we think is more natural.

Consider a system of equations

$$\sum_{a \in A_1^k, \gamma \in \Gamma} u_{a, \gamma}^{(i)} x_{a, \gamma} = b_i \quad (\text{A7})$$

for  $i = 1, 2, \dots, l$  and for some set  $A_1$ . Let  $A_0 \subseteq A_1$ . We say that the system of equations in (A7) is invariant under permutations in  $S_{A_1 \setminus A_0}$  (i.e. permutations  $\pi : A_1 \rightarrow A_1$  that fixes  $A_0$  point wise), if each such permutation maps the equation to itself.

It can be shown (see [1]) that if  $|A_1 \setminus A_0| > k$ , then a system of equations  $L(n_1)$  (with  $n_1 = |A_1|$ ) where each equation is invariant under permutations in  $S_{A_1 \setminus A_0}$  (we also will refer to as permutations in  $S_{n_1 - n_0}$  where  $|A_0| = n_0$  and  $|A_1| = n_1$ ) for each  $A \supseteq A_1$  naturally lifts (via condition (A6)) to a system  $L(n)$  of equations of the form

$$\sum_{a \in A^k, \gamma \in \Gamma} u_{a, \gamma}^{(i)} x_{a, \gamma} = b_i \quad (\text{A8})$$

for  $i = 1, 2, \dots, l$ . Instead of defining uniformity by a quadruplet, we simply notice that a specific system  $L(n_1)$  of linear equations, that is  $S_{k+1}$ -invariant for each  $n \geq n_0$  uniquely lifts to a system  $L(n)$  of linear generating equations. This system of generators is defined by a quadruplet. And if we are given a system of generators by a quadruplet the system is also given by a specific

## Theorems underlying our results

Like Ajtai and Krajicek we consider a set  $A$  with  $n$  elements. For each sequence  $a = (a_1, a_2, \dots, a_k)$  of length  $k$  we introduce a variable  $x_a$  and more generally if  $k_1, k_2, \dots, k_s$  is a finite collection of natural numbers we introduce for each  $j = 1, 2, \dots, s$  and for each sequence  $a = (a_1, a_2, \dots, a_{k_j})$  variables  $x_{a,j}$ . For natural numbers  $k_1, k_2, \dots, k_s$  we let  $\Lambda_n = \Lambda_n(k_1, k_2, \dots, k_s)$  denote such a set of variables. There are  $\sum_{j=1}^s n^{k_j}$  variables in  $\Lambda_n(k_1, k_2, \dots, k_s)$ .

Let  $F[\Lambda_n]$  denote the polynomial ring over the variables in  $\Lambda_n$  and let  $F[\Lambda_n]_d$  denote the set of polynomials in  $F[\Lambda_n]$  of degree  $\leq d$ . We consider  $F[\Lambda_n]_d$  a vector space over  $F$ . In this view the one polynomial 1 is a vector (not a scalar). The symmetric group  $S_n$  acts naturally on the set of variables in  $\Lambda_n$  via the action

$$\pi(x_{a,j}) = \pi(x_{(a_1, a_2, \dots, a_{k_j}), j}) := x_{(\pi(a_1), \pi(a_2), \dots, \pi(a_{k_j})), j}$$

This action of the symmetric group is extended by linearity to an action on  $F[\Lambda_n]$  as well as on  $F[\Lambda_n]_d$ . The space  $F[\Lambda_n]_d$  (and  $F[\Lambda_n]$ ) can then be viewed as a  $FS_n$ -module. The representation theory of the symmetric group provides some general structure theorems about finite  $FS_n$  modules like  $F[\Lambda_n]_d$ . The (partial) ring structure combined with the vector space and the  $FS_n$ -module structure, make mathematical structures like  $F[\Lambda_n]_d$  very rich and interesting.

From a formal perspective [1, 2] Ajtai initiated the study of submodules that in our notation are of the form  $F[\Lambda_n]_1$ , however Ajtai's analysis applies with very few minor changes to  $F[\Lambda_n]_d$  for  $d > 1$ . In [25] Krajicek investigated  $F[\Lambda_n]_d$  for general  $d$  and gave explicit bounds on some of the parameters in Ajtai's results. Our application relies on these bounds. Direct application of Ajtai's results would give only a weak non-constructive version of Theorem 1. In this version we could only conclude that the non-decreasing function  $l(n)$  has  $\lim_{n \rightarrow \infty} l(n) = \infty$  (i.e. it could be arbitrarily slow growing).

Ajtai showed that if  $Q[n] \subseteq F[\Lambda_n]_1$  is a uniform sequence of *linear* equations (given by a quadruplet as described in the previous section) with the property that the set  $Q[n]$  of linear equations for each  $n$  is closed under the action of the symmetric group  $S_n$ , then the question of whether the system of equations has a solution or not, depends on  $n$  modulo  $p^r$  for some constant  $r$  and for  $n$  sufficiently large. Krajicek's proved in [25] an efficient version of this result by Ajtai [1, 2]. The following Theorem that can be extracted from Krajicek's Theorem 3.5 in [25] combined with the remark of how to



get rid of an exponential factor in the NS-case. 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  $\psi$  (as well the underlying field  $F$ ). In our terminology Krajicek's efficient version of Ajtai's result can be stated.

**Theorem X1 :** (Krajicek [25]) *Let  $F$  be an algebraic closed field of characteristic  $p$ . Let  $Q[n] \subseteq F[\Lambda_n]$  be a sequence of polynomials generated by a quadruplet. Then there exist non-decreasing functions  $l_{NS}, l_{PC} : N \rightarrow N$  with  $l_{NS}(n) \in \Omega(\log(n))$  and  $l_{PC}(n) \in \Omega(\log(\log(n)))$ , and constant  $c$  such that:*

*If  $Q[n]$  for some  $d = d(n)$  with  $d \leq l_{NS}(n)$  has a NS-refutation of degree  $d$ , then there exist  $r \in N$  such that  $p^r \leq cd(n)$  and  $d(n) = d(m)$  for all  $m \geq n$  with  $n = m$  modulo  $p^r$ .*

*If  $Q[n]$  for some  $d = d(n)$  with  $d \leq l_{PC}(n)$  has a PC-refutation of degree  $d$ , then there exist  $r \in N$  such that and  $d(n) = d(m)$  for all  $m \geq n$  with  $n = m$  modulo  $p^r$ .*

From this we get:

**Theorem X2 :** *Let  $F$  be a fixed field of characteristic  $p$ . Let  $\psi$  be a FO-formula and consider a propositional translation of  $\psi$  into a sequence  $\psi[n]$  of polynomial equations. The polynomial equations express that  $\psi$  has no model of size  $n$ . There exists non-decreasing functions  $l_{NS}, l_{PC} : N \rightarrow N$  with  $l_{NS}(n) \in \Omega(\log(n))$  and  $l_{PC}(n) \in \Omega(\log(n))$  and a constant  $c$  such that:*

*If  $\psi[n]$  for some  $d = d(n)$  with  $d \leq l_{NS}(n)$  has a NS-refutation of degree  $d$ , then there exist  $r \in N$  such that  $d(n) = d(m)$  for all  $m \geq n$  with  $n = m$  modulo  $p^r$ .*

*If  $\psi[n]$  for some  $d = d(n)$  with  $d \leq l_{PC}(n)$  has a NS-refutation of degree  $d$ , then there exist  $r \in N$  such that  $d(n) = d(m)$  for all  $m \geq n$  with  $n = m$  modulo  $p^r$ .*

**Proof:** The translation of a given FO-formula  $\psi$  leads for each  $n$  to a system  $\psi[n]$  of polynomial equations in  $F[\Lambda_n]$  where  $\Lambda_n = \Lambda_n(k_1, k_2, \dots, k_r)$ . Given Theorem X1 it suffices to show that the sequence  $\psi[n]$  is generated by a

quadruplet. This follows since *the set* of polynomial equations in  $\psi[n]$  is closed under the action of  $S_n$  and we can choose generators (for each  $n$  with  $|A| = n$ ) that are closed under the action of  $S_{A \setminus A_0}$ . Thus by an earlier remark for  $|A \setminus A_0| > k = \max_j k_j$  the sequence  $\psi[n]$  is generated by a quadruplet.

♣

## 4 Proof of the main theorem (part 1)

In this section we will show how the first part of the theorem follows from Theorem X1 and Theorem X2. For a specific uniform sequence  $\psi[n]$  (or  $Q[n]$ ) of polynomial equations we let  $h : N \rightarrow N \cup \{\infty\}$  denote the NS-refutation (PC-refutation) degree complexity of  $\psi[n]$  ( $Q[n]$ ) as a function of  $n$ . Let  $l, r : N \rightarrow N$  be general functions with  $l$  and  $r$  non-decreasing. Assume that the functions  $h, l$  and  $r$  satisfy the following condition:

( $\Delta$ ) *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  $p^{r(d)}$  we have  $h(m) = d$ .*

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  $p^{r(d)}$ .

Now let us increase  $d$  and ask what can happen asymptotically when  $d$  tends to infinity. The next lemma help link Theorem X1 and Theorem X2 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 ( $\Delta$ ). Then exactly one of the following 4 possibilities holds:*

$$\{h(n) < \infty : n \in N\} \text{ is finite} \tag{T1'}$$

$$\begin{aligned} &\{h(n) < \infty : n \in N\} \text{ is infinite and} \\ &\{h(n) < \infty : n > l(h(n))\} \text{ is empty} \end{aligned} \tag{T2'}$$

$$\begin{aligned} &\{h(n) < \infty : n \in N\} \text{ is infinite and} \\ &\{h(n) < \infty : n > l(h(n))\} \text{ is finite and non-empty} \end{aligned} \tag{T3'}$$

$$\begin{aligned} \{h(n) < \infty : n \in N\} & \text{ is infinite and} \\ \{h(n) < \infty : n > l(h(n))\} & \text{ is infinite} \end{aligned} \quad (\text{T4}')$$

The four cases corresponds to the four cases in Theorem 1. Theorem 1 follows by spelling out the concrete consequences of each of the four cases in conjunction with the conditions in  $(\Delta)$ :

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

$$\begin{aligned} & \text{There exists } d_0 \in N \text{ such that} \\ & h(n) < d_0 \text{ holds for all } n \in N \text{ with } n > l(d_0) \end{aligned} \quad (\text{T1}'')$$

$$\begin{aligned} & \text{For all values of } d \in N \\ & \text{if } n > l(d) \text{ then } h(n) > d \text{ for all } n \in N \end{aligned} \quad (\text{T2}'')$$

$$\begin{aligned} & N = S_1 \cup S_2 \text{ can be written as a disjoint union} \\ & \text{of two infinite sets } S_1 \text{ and } S_2 \text{ such that there exists} \\ & d_0 \in N \text{ with } h(n) < d_0 \text{ for all } n \in S_1 \text{ with } n > l(d_0) \\ & \text{and for all } d \in N \text{ and } n \in S_2 \text{ with } n > l(d), h(n) > d \end{aligned} \quad (\text{T3}'')$$

$$\begin{aligned} & \text{For arbitrarily large values of } d \in N, \\ & h(n) = d \text{ holds for some } n \in N \text{ with } n > l(d) \end{aligned} \quad (\text{T4}'')$$

**Proof:** Directly from Lemma 2A using the properties of  $(\Delta)$ . ♣

Let  $h(n)$  denote the minimal degree of a NS (or PC) refutation of  $\psi_n$  where  $\psi$  is a general FO formula. Then according to Krajicek's results  $h$  satisfies  $\Delta$  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.

## 5 Case 1,2 and 3

We will now show that each of the four possibilities in Theorem 1 can appear. Most sequences of propositional formula that so far have been considered in the literature have been of type T1 or type T2.

### Type T1

In example 1, calculation D1 showed that a specific predicate contradiction had a propositional translation of NS-refutation degree 4 i.e. a complexity behaviour of type T1.

It turns out (Lemma 7) that:

**Proposition A :** *A predicate formula  $\psi$  that fails in all sufficiently large finite models as well as in all infinite models, always translate to a sequence  $\psi_n$  of propositional formula that has NS-refutation (PC-refutation) degree complexity of type T1 ( i.e. that has constant degree NS-refutations (PC-refutations)).*

For a detailed example illustrating this proposition see section 7.

The converse of Proposition A is not valid:

**Proposition B :** *There exists propostions of type T1 that are satisfiable in infinite models.*

An example of this the bijective pigeonhole principle stating that there is no bijective map from  $\{1, 2, \dots, n\}$  to  $\{1, 2, \dots, n - 1\}$  is valid in some infinite models yet the principle is of type T1. This version of the pigeon-hole consists of the conjunction of the following four FO-sentences that together claim that there exists a point  $n$ , and a binary relation  $R$  that defines a bijection from the universe to the universe except for some point  $c$ .

$$\forall x \exists y (y \neq c \wedge R(x, y)) \tag{PHP1}$$

$$\forall x, y, z ((R(x, y) \wedge R(x, z)) \rightarrow y = z) \tag{PHP2}$$

$$\forall y \exists x R(x, y) \tag{PHP3}$$

$$\forall x_1, x_2, y ((R(x_1, y) \wedge R(x_2, y)) \rightarrow x_1 = x_2) \tag{PHP4}$$

Translated into polynomial equations we get after a few cosmetic changes (and letting  $c = n$ ) the following system of polynomial equations:

$$Q_i^1 := \left( \sum_{k=1}^{n-1} r_{i,k} \right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{T1.1})$$

$$Q_j^2 := \left( \sum_{k=1}^n r_{k,j} \right) - 1 = 0 \text{ for } j \in \{1, 2, \dots, n-1\} \quad (\text{T1.2})$$

$$Q_{ijk}^3 := r_{ij}r_{ik} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{T1.3})$$

$$Q_{i_1 i_2 j}^4 := r_{i_1, j} x_{i_2, j} = 0 \text{ for } i_1 \neq i_2, j \in \{1, 2, \dots, n\} \quad (\text{T1.4})$$

$$Q_{ij}^5 := r_{ij}^2 - r_{ij} = 0 \text{ for } i, j \in \{1, 2, \dots, n\} \quad (\text{T1.5})$$

This system of polynomial equations has no solution since a solution would define a bijection from  $\{1, 2, \dots, n\}$  to  $\{1, 2, \dots, n-1\}$ . The system has a NS-refutation of degree 2

$$\sum_{i=1}^n Q_i^2 - \sum_{j=1}^n Q_j^1 = \sum_{j=1}^{n-1} \left[ \left( \sum_{k=1}^n r_{k,j} \right) - 1 \right] - \sum_{i=1}^n \left[ \left( \sum_{k=1}^{n-1} r_{i,k} \right) - 1 \right] = 1 \quad (\text{D2})$$

Notice that the derivation only uses (T1.1) and (T1.2). The calculation show that the system of equations has constant NS-refutation degree complexity (PC-refutation degree complexity) i.e. is of type T1.

## Type T2

Satisfiable formula (by definition) always leads to propositions of degree complexity  $\infty$  i.e propositions of type T2. The pigeon-hole principle can be used as a "genuine" example that leads to a sequence of unsatisfiable propositions of NS-refutation (PC-refutation) degree complexity of type T2. To see this consider the conjunction of PHP1 and PHP2

$$\forall x \exists y (y \neq c \wedge R(x, y)) \quad (\text{PHP1})$$

$$\forall x, y, z ((R(x, y) \wedge R(x, z)) \rightarrow y = z) \quad (\text{PHP2})$$

We get (after a few cosmetic changes where we let  $n = c$ ) the following system of polynomial equations:

$$Q_i^1 := \left( \sum_{j=1}^{n-1} x_{ij} \right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{T2.1})$$

$$Q_{ijk}^2 := x_{ij}x_{ik} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{T2.2})$$

$$Q_{ij}^3 := x_{ij}^2 - x_{ij} = 0 \text{ for } i, j \in \{1, 2, \dots, n\} \quad (\text{T2.3})$$

The polynomial equations in T2.3 are not needed since they have a constant NS-derivation from equations in T2.1 and T2.2. The polynomial equations in T2.1, T2.2 and T2.3 have no common solution since a common zero would violate the Pigeon-hole principle. According to Razborov [30] these equations require NS-refutation degree (PC-refutation degree)  $n/2$ . Thus the system of equations has NS-refutation degree complexity (PC-refutation degree complexity) of type T2.

The class T2 is very rich and many distinct problems belongs to this class. The Spectrum  $S_\psi$  of a FO-formula  $\psi$  is defined as

$$S_\psi := \{n \in N : \psi \text{ has a model of size } n\}$$

It is well know that any set  $U \subseteq N$  with complexity that belongs to NEXP, is the spectrum of some FO-formula  $\psi$ . Any FO-formula  $\psi$  with irregular spectrum is of type T2. More specifically, any FO-formula with a spectrum with a complement that does not contain a residue class modulo  $p^r$  is for type T2.

One way to construct a general sequence  $\psi[n]$  of unsatisfiable propositions of type T2, is to select a finite collection  $U_1, U_2, \dots, U_v$  of sets of complexity in NEXP and with  $\bigcap_{j=1}^v U_j = \emptyset$ , with each  $U_j$  being irregular (i.e. with no residue class modulo  $p^r$  in its complement). Then there exist FO-formula  $\psi_1, \dots, \psi_v$  with these spectra. Translation of the conjunction  $\psi := \bigwedge_j \psi_j$  leads to a sequence  $\psi[n]$  of unsatisfiable propositions that can be shown (see Lemma 3 below) to be of type T2.

### Type T3

For a problem of type T3 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 [25]:

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

$$Q_e := z_e^2 - z_e = 0 \text{ for each variable } z_e \quad (\text{T3.1})$$

$$Q_{e,f} := z_e z_f = 0 \text{ for every } e, f \text{ such that } e \cap f \neq \emptyset \text{ and } e \neq f \quad (\text{T3.2})$$

$$Q_i := \left( \sum_{e \ni i} z_e \right) - 1 = 0 \text{ for each } i \in \{1, 2, \dots, n\} \quad (\text{T3.3})$$

For  $n = k$  modulo  $p$  with  $k \neq 0$  and  $k \in \{1, 2, \dots, p-1\}$  we have:

$$\begin{aligned} \sum_i -k^{-1} \left[ \left( \sum_{e \ni i} z_e \right) - 1 \right] &= -k^{-1} \left( \sum_i \left( \sum_{e \ni i} z_e \right) - n \right) = \\ -k^{-1} \left( p \left( \sum_e z_e \right) - k \right) &= -k^{-1} (0 - k) = 1 \end{aligned} \quad (\text{D3})$$

Thus for each  $n \neq 0$  modulo  $p$  the polynomial equations in (T3.3) (the equations in (T3.1) and (T3.2) are not needed) has a NS-refutation (PC-refutation) of degree 1 over field of characteristic  $p$  that refutes the polynomial equations  $Q_e = 0, Q_{e,f} = 0$  and  $Q_i = 0$ . Notice that the derivation (D3) in fact only use the equations in (T3.3). The equations are satisfiable for  $n = 0$  modulo  $p$  i.e. they have refutation degree complexity  $\infty$ .

If we want an example of a sequence of type T3, where the polynomial equations are unsatisfiable for all values of  $n$  we can add to (T3.1),(T3.2) and (T3.3) the equations:

$$Q_i^1 := \left( \sum_{j=1}^n x_{ij} \right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{T3.4})$$

$$Q_{ijk}^2 := x_{ij} x_{ik} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{T3.5})$$

The pigeonhole principle require PC refutation degree  $n/2$  according to Razborov [30]. This suggest that when the conjunction of the counting modulo  $p$  principle and the general pigeonhole principle are combined, the resulting system has complexity of type T3.

To show this we need to observe/show that combining two systems of polynomial equations in disjoint set of variables, cannot lead to a composed system with refutation degree complexity strictly lower than the maximal degree complexity of each of the system on their own. This follows the next Lemma. We also use this lemma for the undecidability result.

**Lemma 3 :** *Let  $\Gamma$  and  $\Delta$  be two collections of polynomials in disjoint set of variables. Assume that  $\Gamma$  is unsatisfiable (i.e. that the polynomials in  $\Gamma$  have no common zero) and assume that  $\Delta$  is satisfiable (i.e. that the polynomials in  $\Delta$  have a common zero). Then the collection  $\Gamma$  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  $\sum_{P_\gamma \in \Gamma} Q_\gamma P_\gamma + \sum_{P_\delta \in \Delta} Q_\delta P_\delta = 1$  is a NS-derivation of degree  $d$ . The polynomials in  $\Delta$  has a common zero  $\vec{\eta}$ . Since the set of variables are disjoint, it follows that  $\sum_{P_\gamma \in \Gamma} Q_\gamma P_\gamma + \sum_{P_\delta \in \Delta} Q_\delta P_\delta(\vec{\eta}) = \sum_{P_\gamma \in \Gamma} Q_\gamma P_\gamma$  defines the 1 polynomial in the variables associated to  $\Gamma$ . In other words  $\sum_{P_\gamma \in \Gamma} Q_\gamma P_\gamma = 1$ . This shows the "if" direction for NS-refutations.

Assume  $P_1, P_2, \dots, P_j, \dots, 1$  is a PC-derivation  $\Gamma \cup \Delta \vdash_d 1$ . Let  $\vec{\eta}$  be a common zero of the polynomials in  $\Gamma$ , and substitute  $\vec{\eta}$  into the variables associated with  $\Gamma$ . We get a PC-derivation of polynomials in the variables associated with  $\Delta$  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  $\Delta$  as a PC-refutation of  $\Delta \cup \Gamma$ ). ♣

## 6 The fluctuating case

We now show that case 4, the fluctuating case is non-empty. 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:

$$\forall x \exists y R(x, y) \vee S(x, y) \tag{F1}$$

$$\forall y \exists x R(x, y) \tag{F2}$$

$$\forall y \exists x S(x, y) \tag{F3}$$



$$\forall x, y, z (y \neq z \rightarrow \neg R(x, y) \vee \neg R(x, z)) \quad (\text{F4})$$

$$\forall x, y, z (y \neq z \rightarrow \neg S(x, y) \vee \neg S(x, z)) \quad (\text{F5})$$

$$\forall x, y, z (y \neq z \rightarrow \neg R(x, y) \vee \neg S(x, y)) \quad (\text{F6})$$

$$\forall x_1, x_2, y (x_1 \neq x_2 \rightarrow \neg R(x_1, y) \vee \neg R(x_2, y)) \quad (\text{F7})$$

$$\forall x_1, x_2, y (x_1 \neq x_2 \rightarrow \neg S(x_1, y) \vee \neg S(x_2, y)) \quad (\text{F8})$$

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

$$Q_i^1 := \left( \sum_j x_{ij} \right) + \left( \sum_j y_{ij} \right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{T4.1})$$

$$Q_j^2 := \left( \sum_i x_{ij} \right) - 1 = 0 \text{ for } j \in \{1, 2, \dots, n\} \quad (\text{T4.2})$$

$$Q_j^3 := \left( \sum_i y_{ij} \right) - 1 = 0 \text{ for } j \in \{1, 2, \dots, n\} \quad (\text{T4.3})$$

$$Q_{ijk}^4 := x_{ij}x_{ik} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{T4.4})$$

$$Q_{ijk}^5 := y_{ij}y_{ik} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{T4.5})$$

$$Q_{ijk}^6 := x_{ij}y_{ik} = 0 \text{ for } i, j, k \in \{1, 2, \dots, n\} \quad (\text{T4.6})$$

$$Q_{ijk}^7 := x_{ji}x_{ki} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{T4.7})$$

$$Q_{ijk}^8 := y_{ji}y_{ki} = 0 \text{ for } i, j \neq k \in \{1, 2, \dots, n\} \quad (\text{T4.8})$$

The equations  $x_{ij}^2 - x_{ij} = 0$  and  $y_{ij}^2 - y_{ij} = 0$  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  $i, j \in \{1, 2, \dots, n\}$  the equations  $x_{ij}Q_j^2 = 0$  and  $y_{ij}Q_j^3 = 0$ , combined with the equations  $Q_{ijk}^7 = 0$  and  $Q_{ijk}^8$  where  $i, j, k \in \{1, 2, \dots, n\}$ .

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  $\{1, 2, \dots, n\}$  to  $\{1, 2, \dots, 2n\}$  violating a ‘weak’ version of the pigeonhole principle. Thus

for each  $n$  the constant polynomial 1 belongs to the ideal generated by polynomials  $Q_i^1, Q_j^2, \dots, Q_{ijk}^8$ . Further, there exist polynomials  $P_i^1, P_j^2, \dots, P_{ijk}^8$  such that  $\sum_i P_i^1 Q_i^1 + \sum_j P_j^2 Q_j^2 + \dots + \sum_{ijk} P_{ijk}^8 Q_{ijk}^8 = 1$ . 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  $P_i^1, P_j^2, \dots, P_{ijk}^8$ .

The equations can be simplified by relabeling the variables! Let  $D$  and  $R$  be two finite sets with  $n$  and  $m$  elements. The equations can then be written as:

$$Q_i^D(\vec{x}) := \left( \sum_{j \in R} x_{i,j} \right) - 1 = 0 \text{ for each } i \in D \quad (\text{Eq 1})$$

$$Q_j^R(\vec{x}) := \left( \sum_{i \in D} x_{i,j} \right) - 1 = 0 \text{ for each } j \in R \quad (\text{Eq 2})$$

$$Q_{i,j,k}(\vec{x}) := x_{ij}x_{ik} = 0 \text{ for each } i \in D, \text{ and } j < k \in R \quad (\text{Eq 3'})$$

$$Q_{ij,k}(\vec{x}) := x_{i,k}x_{j,k} = 0 \text{ for each } i \neq j, i, j \in D, j \in R \quad (\text{Eq 4})$$

where the variables  $x_{i,j}$  have  $i \in D$  and  $j \in R$ .

Since  $xy = yx$  the system of equations remains equivalent if we drop the requirement  $j < k$  and replace the third set of equations with:

$$Q_{i,j,k}(\vec{x}) := x_{i,j}x_{i,k} = 0 \text{ for each } i \in D, j, k \in R, j \neq k \quad (\text{Eq 3})$$

We denote the system of equations i.e. (Eq 1), (Eq 2), (Eq 3) and (Eq 4), by  $\text{PHP}_D^R(\text{bij})$  or sometimes by  $\text{PHP}_n^m(\text{bij})$ .

The system  $\text{PHP}_D^R(\text{bij})$  contains  $6n^3 - 4n^2 + 3n$  equations. This system of equations has already been analyzed in Beame and R is [4].

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

$$Q_{ijk}^9 := y_{ij}x_{ik} = 0 \text{ for } i, j, k \in \{1, 2, \dots, n\} \quad (\text{T4.9})$$

to the original system of equations, we get a new system of equations that is equivalent to the original system, but contains the very same  $6n^3 - 4n^2 + 3n$  equations as  $\text{PHP}_n^m(\text{bij})$ .

Let  $F_p$  denote a fixed field of characteristic  $p \neq 0$ . Then the system of polynomial equations in [4] for the bijective pigeonhole principle  $\text{PHP}_n^{n+p^l}(\text{bij})$  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  $PHP_n^{n+p^l}(\text{bij})$  of degree  $p^l - 1$ . On the other hand if  $n \geq ((p+2)^l - p^l)/2$  then any Nullstellensatz refutation of  $PHP_n^{n+p^l}(\text{bij})$  must have degree at least  $2^l - 1$ .*

**Proof:** The first part is Lemma 16 in [4] while the second part is Theorem 12 in [4]. ♣

We need a slight variation of this proposition. We prove an upper fluctuating bound and as well as a Lower fluctuating bound and notice that these bounds ensure a fluctuating NS-refutation degree complexity.

### Fluctuating upper NS-degree bound

Consider the equations (Eq1)-(Eq4). For  $k \in N$  we have the following identities over a field of characteristic  $p$ :

$$\begin{aligned}
& \sum_{d_1 < d_2 < \dots < d_k \in D} \left( \sum_{r_1, r_2, \dots, r_{k-1} \in R} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_{k-1}, r_{k-1}} \left[ \left( \sum_{r_k \in R} x_{d_k, r_k} \right) - 1 \right] + \right. \\
& \sum_{r_1, r_2, \dots, r_{k-2} \in R} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_{k-2}, r_{k-2}} \left[ \left( \sum_{r_{k-1} \in R} x_{d_{k-1}, r_{k-1}} \right) - 1 \right] + \dots + \\
& \sum_{r_1, r_2, \dots, r_{j-1} \in R} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_{j-1}, r_{j-1}} \left[ \left( \sum_{r_j \in R} x_{d_j, r_j} \right) - 1 \right] + \dots + \left. \left[ \left( \sum_{r_1 \in R} x_{d_1, r_1} \right) - 1 \right] \right) \\
& = \sum_{d_1 < d_2 < \dots < d_k \in D} \left( \sum_{r_1, r_2, \dots, r_k \in R} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_k, r_k} - 1 \right) \tag{F1}
\end{aligned}$$

Furthermore, notice that:

$$\begin{aligned}
& \sum_{d_1 < d_2 < \dots < d_k} \left( \left( \sum_{r_1, r_2, \dots, r_k} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_k, r_k} \right) - 1 \right) = \\
& \left( \sum_{d_1 < d_2 < \dots < d_k} \sum_{r_1, r_2, \dots, r_k} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_k, r_k} \right) - \binom{|D|}{k} \text{ modulo } p \tag{F2}
\end{aligned}$$

Similarly,

$$\sum_{r_1 < r_2 < \dots < r_k \in R} \left( \sum_{d_1, d_2, \dots, d_{k-1} \in D} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_{k-1}, r_{k-1}} \left[ \left( \sum_{d_k \in D} x_{d_k, r_k} \right) - 1 \right] + \right.$$

$$\begin{aligned}
& \sum_{d_1, d_2, \dots, d_{k-2} \in D} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_{k-2}, r_{k-2}} \left[ \left( \sum_{d_{k-1} \in D} x_{d_{k-1}, r_{k-1}} \right) - 1 \right] + \dots + \\
& \sum_{d_1, d_2, \dots, d_{j-1} \in D} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_{j-1}, r_{j-1}} \left[ \left( \sum_{d_j \in D} x_{d_j, r_j} \right) - 1 \right] + \dots + \left[ \left( \sum_{d_1 \in D} x_{d_1, r_1} \right) - 1 \right] \\
& = \sum_{r_1 < r_2 < \dots < r_k \in R} \left( \sum_{d_1, d_2, \dots, d_k \in D} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_k, r_k} - 1 \right) \tag{F3}
\end{aligned}$$

Notice that

$$\begin{aligned}
& \sum_{r_1 < r_2 < \dots < r_k} \left( \sum_{d_1, d_2, \dots, d_k} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_k, r_k} \right) - 1 = \\
& \left( \sum_{r_1 < r_2 < \dots < r_k} \sum_{d_1, d_2, \dots, d_k} x_{d_1, r_1} x_{d_2, r_2} \dots x_{d_k, r_k} \right) - \binom{|R|}{k} \text{ modulo } p \tag{F4}
\end{aligned}$$

Subtracting (F2) from (F4) we notice that all the monomials cancel out so we get:

$$\text{Equation(F2)} - \text{Equation(F4)} = \binom{|R|}{k} - \binom{|D|}{k} \text{ modulo } p \tag{F5}$$

This show that there is a degree  $k$  refutation of  $\text{PHP}_D^R(\text{bij})$  if

$$\binom{|R|}{k} - \binom{|D|}{k} \neq 0 \text{ modulo } p \tag{F6}$$

Now it is well known (see [4] for more details) that for any prime  $p$ , for all  $l \in \mathbb{N}$ , for all  $n \geq p^l \in \mathbb{N}$  and for all  $r \neq 0$  modulo  $p$

$$\binom{n + rp^l}{p^l} - \binom{n}{p^l} = r \text{ modulo } p \tag{F7}$$

Thus if we for  $r \neq 0$  modulo  $p$  let  $|R| = n + rp^l$  and  $|D| = n$ , we have shown that over fields of chatacteristic  $p > 0$ ,  $\text{PHP}_n^{n+rp^l}(\text{bij})$  has a NS-refutation of degree  $p^l$ . More specifically we have show that:

**Proposition 4A :** Let  $F$  be a field of finite characteristic  $p$ . Then for  $m \geq n \geq p^{l(m-n)}$  the polynomial equations  $\text{PHP}_n^m(\text{bij})$  has a NS-refutation of degree  $p^{l(m-n)}$  where  $l(m-n)$  is the power of the prime factor  $p$  in the prime factorization of  $m-n$ .

This shows that we have a NS-degree upper bound for  $\text{PHP}_n^m(\text{bij})$  that has a fluctuating behavior as a function of  $m$ .

## Proving degree lower bound by designs

In this section we will briefly discuss a general method for proving degree lower bound for the NS-proof (NS-refutation) system. In an unpublished manuscript Pudlak introduced the method and the term “design” was chosen as a standard term for this type of objects. Later specific design were constructed and used for proving specific lower bounds in [7, 8, 9, 4].

Let  $\Lambda_n = \Lambda_n(k_1, k_2, \dots, k_r)$  be a set of variables and let  $F[\Lambda_n]$  be the set of polynomials over these variables. As in section 3, consider also  $F[\Lambda_n]_d$  the set of polynomials of degree  $\leq d$ .

Assume that we are given a set  $\Gamma \subseteq F[\Lambda_n]_d$ . Typically of degree of each polynomial  $p \in \Gamma$  is much smaller than  $d$ . For proving a degree lower bound we are concerned whether the set  $\Gamma$  of polynomials has NS-refutation of degree  $d$ . The idea is to prove this by constructing an object we will call a  $d$ -design  $\mathcal{D}$  for  $\Gamma$ . A design is a (linear) map  $\mathcal{D} : F[\Lambda_n]_d \rightarrow F$  that satisfies:

For  $p_1, p_2 \in F[\Lambda_n]_d$  and  $\lambda_1, \lambda_2 \in F$

$$\mathcal{D}(\lambda_1 p_1 + \lambda_2 p_2) = \lambda_1 \mathcal{D}(p_1) + \lambda_2 \mathcal{D}(p_2) \quad (\text{R1})$$

For each  $p \in \Gamma$  and for each monomial  $m$  for which  $mp$  has degree  $\leq d$

$$\mathcal{D}(mp) = 0 \quad (\text{R2})$$

$$\mathcal{D}(1) \neq 0 \quad (\text{R3})$$

The point in this definition is that if there exists a  $d$ -design  $\mathcal{D}$  for  $\Gamma$ , then polynomials in  $\Gamma$  does not have a degree  $d$  NS-refutation. To see this notice, that

$$\sum_{p \in \Gamma} q_p p = 1 \text{ implies that } 1 = \mathcal{D}(1) = \mathcal{D}\left(\sum_{p \in \Gamma} q_p p\right) = \sum_{p \in \Gamma} \mathcal{D}(q_p p) = 0$$

From an abstract perspective a design is just a certain vector in the dual vector space of  $F[\Lambda_n]_d$ .

Let  $U$  denote the linear vector space spanned by all weakenings of the axioms  $p \in \Gamma$ . Or more formally let

$$U := \text{span}\{mp : m \text{ is a monomial, } p \in \Gamma \text{ and } \deg(mp) \leq d\}$$

It is not hard to show that the vector “1” (the 1-polynomial is treated as a vector rather than a scalar) belongs to  $U \subseteq F[\Lambda_n]_d$  if and only if  $\Gamma$  has a

NS-refutation of degree  $\leq d$ . Let  $V = \text{span}\{1, V\}$ . In general  $\dim(V) = \dim(U)$  or  $\dim(V) = \dim(U) + 1$ . The first case occurs if and only if the vector 1 belongs to  $U$ .

Let  $U^\circ$  denote the dual space of  $U$  and let  $V^\circ$  denote the dual space of  $V$ . In general for any linear subspace  $W \subseteq F[\Lambda_n]_d$  (e.g.  $W = U$  or  $W = V$ ). It is well known that

$$\dim(W) + \dim(W^\circ) = \dim(F[\vec{x}]_d)$$

The system  $\Gamma$  has a degree NS-refutation if and only if  $V^\circ = U^\circ$ . In the case  $\Gamma$  has no NS-refutation of degree  $d$ ,  $\dim(U^\circ) = \dim(V^\circ) + 1$ . In this case notice that any vector  $\alpha \in U^\circ \setminus V^\circ$  has:

$$\alpha(p_1 + p_2) = \alpha(p_1) + \alpha(p_2) \tag{R1'}$$

$$\alpha(mp) = 0 \text{ for each weakening of the axiom } p \in \Gamma \tag{R2'}$$

$$\alpha(1) \neq 0 \tag{R3'}$$

Notice that the collection of  $\beta$  of the form  $\beta := \alpha + \gamma$  with  $\gamma \in V^\circ$  exactly is the space of designs for  $\Gamma$ . We will not need this, but notice the space of designs is a linear side-space and notice that if the space of designs is non-empty it has dimension identical to the dimension of the dual of  $U$  minus 1.

## A fluctuating lower NS-degree bound

In this section we show that there is a lower bound that fluctuates in a similar fashion as the upper bound i.e. that there is a NS-degree lower bound (of  $2^l$ ) that depend on the power  $l$  of  $p$  in the prime factorization of  $m - n$ .

We consider the specific situation of  $\text{PHP}_n^{n+rp^l}(\text{bij})$  where  $F[\vec{x}]$  is the polynomial ring of polynomials in the variables  $x_{i,j}$  with  $i \in D$  and  $j \in R$ . We follow [4] and define a  $d$ -design  $\mathcal{D}$  i.e. a linear map  $\mathcal{D} : F[\vec{x}]_d \rightarrow F$  which vanish on weakenings of the axioms and maps the 1-polynomial to a non-zero. Following [4] we relate monomials and sets of edges in  $D \times R$  as follows: Given a set of edges  $\pi \in D \times R$ , we define a monomial  $X_\pi := \prod_{(i,j) \in \pi} x_{i,j}$ , and given a monomial  $X = x_{i_1, j_1}^{e_1} x_{i_2, j_2}^{e_2} \dots x_{i_k, j_k}^{e_k}$  with  $e_1, e_2, \dots, e_k \geq 1$ , define  $\pi_X := \{(i_1, j_1), (i_2, j_2), \dots, (i_k, j_k)\}$ . The reader might find this identification of monomials as edges in  $D \times R$  useful.

A  $d$ -design  $\mathcal{D}$  for  $D \times R$  is a mapping from partial matchings (i.e. sets of disjoint edges in  $D \times R$ ) of size  $\leq d$  into  $F$  such that

$$\mathcal{D}(\emptyset) \neq 0 \tag{a}$$

For each partial matching  $\pi$  with  $|\pi| < d$  and  $i \in D \setminus \text{dom}(\pi)$

$$\sum_{j \in R \setminus \text{range}(\pi)} \mathcal{D}(\pi \cup (i, j)) = D(\pi) \text{ modulo } p \tag{b}$$

For each partial matching  $\pi$  with  $|\pi| < d$  and  $j \in R \setminus \text{range}(\pi)$

$$\sum_{i \in D \setminus \text{dom}(\pi)} \mathcal{D}(\pi \cup (i, j)) = D(\pi) \text{ modulo } p \tag{c}$$

In general  $\mathcal{D}$  vanish on set of edges that are not partial matchings (i.e. on sets of edges that contains edges that are not disjoint).  $\mathcal{D}$  is extended by linearity to include all polynomials in  $F[\vec{x}]_d$ . Notice that definition agree with the general definition of design.

**Lemma 4B** : *If there is a  $d$ -design  $\mathcal{D}$  for  $D \times R$  (over  $F$ ), there is for each  $c \in N$  a  $d$ -design  $\mathcal{D}'$  for  $D' \times R'$  (over  $F$ ) with  $|D'| = |D| + c$  and  $|R'| = |R| + c$ .*

**Proof:** With out loss of generality we can assume that  $D' = D \cup \{d'_1, d'_2, \dots, d'_c\}$  and that  $R' = R \cup \{r'_1, r'_2, \dots, r'_c\}$  are disjoint unions. We consider partial matching on  $D' \times R'$  that are consistent with the partial matching  $\{(d'_1, r'_1), (d'_2, r'_2), \dots, (d'_c, r'_c)\}$ . We define  $\mathcal{D}'$  of such consistent partial matching  $D' \times R'$  as  $\mathcal{D}$  of the restriction of the matching to  $D \times R$ .  $\mathcal{D}'$  vanish on partial partitions that are inconsistent with  $\{(d'_1, r'_1), (d'_2, r'_2), \dots, (d'_c, r'_c)\}$ . It is straight forward to check that  $\mathcal{D}'$  is a  $d$ -design on  $D' \times R'$  over  $F$ . ♣

**Lemma 4C** : *If there is a  $d$ -design  $\mathcal{D}$  for  $D \times R$  (over  $F$ ), there is for each  $c \in N$  a  $d$ -design  $\mathcal{D}'$  for  $D' \times R'$  (over  $F$ ) with  $D'$  ( $R'$ ) consisting of  $c$  disjoint copies of  $D$  ( $R$ ).*

**Proof:** Let  $D_1, D_2, \dots, D_c$  be  $c$  copies of  $D$  and let  $R_1, R_2, \dots, R_c$  be  $c$  copies of  $R$ . Without loss of generality we can assume that  $D' = D_1 \cup D_2 \cup \dots \cup D_c$  and  $R' = R_1 \cup R_2 \cup \dots \cup R_c$ .  $\mathcal{D}'$  is zero on all partial matchings, except partial matchings of  $D' \times R'$  which match elements in  $D_j$  with  $R_j$  for  $j = 1, 2, \dots, c$ .

For these matchings  $\mathcal{D}' = \mathcal{D}_1\mathcal{D}_2\dots\mathcal{D}_c$  i.e. the product (in the sense of the field  $F$ ) of the design evaluations on the partial matching restricted to the pairs.  $D_1 \times R_1, D_2 \times R_2, \dots, D_c \times R_c$ . It is straight forward to check that  $\mathcal{D}'$  is a  $d$ -design on  $D' \times R'$  over  $F$ . ♣

**Lemma 4D** : [4] *If there is a  $d$ -design for  $D \times R$  over a field  $F$  of characteristic  $p$ , then there is a  $2d + 1$ -design for  $D' \times R'$  with*

$$|D'| = (p + 1)|D| + |R| \text{ and } |R'| = |D| + (p + 1)|R|$$

**Proof:** This is far for obvious but was proved in [4] ♣

**Lemma 4E** : *Let  $F$  be a field of characteristic  $p > 0$ . Let  $d, r \in N$  and assume that*

$$|D| \geq r(p + 2)^{d-1} + p\left(\frac{p^{d-1} - 1}{p - 1}\right) \quad (\text{Assumption 1})$$

*and that*

$$|R| - |D| = rp^d. \quad (\text{Assumption 2})$$

*Then,*

$$\text{there exists a } 2^d - 1\text{-design for } D \times R \text{ over } F \quad (\text{Conclusion})$$

**Proof:** There is a 1-design with  $m - n = rp$  for  $n \geq 1$ . Then according to Lemma 4C, there is a 3-design for  $n \geq (p + 1) + (1 + rp) = (p + 2) + rp$  with  $m - n = rp^2$ . There is a 7-design for  $n \geq (p + 1)(p + 2) + ((p + 2) + rp + rp^2) = (p + 2)^2 + rp + rp^2$  with  $m - n = rp^3$ . In general there is a  $2^d - 1$ -design for  $n \geq (p + 2)^{d-1} + r(p + p^2 + \dots + p^{d-1})$  with  $m - n = rp^d$ . ♣

**Lemma 4F** : *Let  $F$  be a field of characteristic  $p > 0$ . For any  $r, l \in N$  and for any  $n \geq (p + 2)^l$   $\text{PHP}_n^{n+rp^l}(\text{bij})$  has no NS-refutation of degree  $< 2^l - 1$ .*

**Proof:** According to Lemma 4E, there exists a  $2^l - 1$ -design for  $D \times R$  with  $|D| \geq (p + 2)^l \geq r(p + 2)^{l-1} + p\left(\frac{p^{l-1} - 1}{p - 1}\right)$  and with  $|R| - |D| = rp^l$ . Thus  $\text{PHP}_D^R(\text{bij})$  i.e.  $\text{PHP}_n^{n+rp^l}(\text{bij})$  has no NS-refutation of degree  $\leq 2^l - 1$  ♣

**Proposition 4G** : *Let  $F$  be a field of finite characteristic  $p$ . Then for  $m \geq n \geq (p + 2)^{l(m-n)}$  any NS-refutation of the polynomial equations  $\text{PHP}_n^m(\text{bij})$  has degree  $\geq 2^{l(m-n)} - 1$  where  $l(m - n)$  is the power of the prime factor  $p$  in the prime factorization of  $m - n$ .*



## Combining the fluctuating lower and upper bounds

Combining Proposition 4A and Proposition 4G we see that for  $m \geq n$  and for  $n$  sufficiently large, the NS-refutation degree complexity of  $\text{PHP}_n^m(\text{bij})$  always is bound from below by  $2^{l(m-n)} - 1$  and from above by  $p^{l(m-n)}$  where  $l(m-n)$  is the power of the prime factor  $p$  in the prime factorization of  $m-n$ .

It follows that the the weak pigeon hole principle has fluctuating complexity:

**Proposition 4H :** Let  $F$  be a field of characteristic  $p > 0$ . Let  $l(n)$  denote the power of  $p$  in the prime factorization of  $n$ . Then for any  $n$  with  $n \geq (p+2)^{l(n)}$  any NS-refutation of  $\text{PHP}_n^{2n}(\text{bij})$  has a NS-refutation degree complexity at least  $2^{l(n)} - 1$  and at most  $p^{l(n)}$ .

It follows from Theorem 10 (that is a simple consequence of a result by Krajicek (lemma 9)), that  $\psi_n$  also has PC-degree refutation complexity of the fluctuating type.

## 7 Proof of the main theorem (part 2)

We have shown that a given FO formula  $\psi$ , translates into a sequence  $\psi[n]$  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 the remaining part of the paper we will consider the decision problem of deciding if a given first order formula  $\psi$  leads to a sequence  $\psi[n]$  that has a complexity behavior of a type belonging to  $A$ .

**Lemma 5 :** *Let  $\psi$  be a FO-formula.*

*If  $\psi$  is of type T1 i.e. if  $\psi_n$  has constant degree complexity for all but finitely  $n$  (where the degree complexity is  $\infty$ ), then for any formula  $\eta$  (irrespective of its type),  $\psi \wedge \eta$  is also of type T1.*

*If  $\psi$  is of type T2 i.e. if  $\psi_n$  has degree complexity  $\geq l(n)$  for all  $n$ , then for any  $\eta$  the formula  $\psi \wedge \eta$  has the same type as  $\eta$ .*

**Proof:** Obvious given Lemma 3. ♣

## Finite and infinitely unsatisfiable formula

In preparation for Lemma 6 (and to help construct examples of Lemma 7) consider the following versions of Robinson's Arithmetical system  $Q$  where the axioms have been modified so they define an initial segment  $(\{0, 1, 2, \dots, c\}, 0, c, s, +, \times)$  of natural numbers. As usual,  $s$  is the successor function and  $+$  and  $\times$  are the addition and multiplication defined the usual way when all numbers involved are strictly smaller than  $c$ . The number  $c$  behaves as an "absorbing" element.

$$s(x) \neq 0 \tag{Q1}$$

$$x \neq 0 \rightarrow \exists y(s(y) = x) \tag{Q2}$$

$$(x \neq c \wedge y \neq c) \rightarrow (s(x) = s(y) \rightarrow x = y) \tag{Q3}$$

$$x = x + 0 \tag{Q4}$$

$$(x + y \neq c) \rightarrow (x + s(y) = s(x + y)) \tag{Q5}$$

$$x \neq c \rightarrow x \times 0 = 0 \tag{Q6}$$

$$(c \neq x \times s(y) \wedge c \neq (x \times y) + x) \rightarrow x \times s(y) = (x \times y) + x \tag{Q7}$$

$$s(c) = c \wedge c \times x = c \wedge x \times c = c \wedge x + c = c \wedge c + x = c \tag{Q8-Q12}$$

If we introduce a Skolem function  $t$  (with  $s(t(x)) = x$ ) we can convert the FO formula  $Q$  into a quantifier free formula  $Q'$  of the special form  $S$ . In the conversion we replace  $v_1 + v_2$  with  $a(v_1, v_2)$  and replace  $v_1 \times v_2$  with  $m(v_1, v_2)$ . Then  $Q'$  is the conjunction of:

$$\neg z_2 = s(z_1) \vee \neg z_3 = 0 \vee \neg z_2 = z_3 \tag{Q1a}$$

$$z_1 = 0 \vee \neg z_2 = t(z_1) \vee z_1 = s(z_2) \tag{Q2a}$$

$$z_1 = c \vee z_2 = c \vee \neg z_3 = s(z_1) \vee \neg z_4 = s(z_2) \vee \neg z_3 = z_4 \vee z_1 = z_2 \tag{Q3a}$$

$$\neg z_2 = 0 \vee z_1 = a(z_1, z_2) \tag{Q4a}$$

$$z_1 = c \vee \neg z_3 = c \vee \neg z_4 = a(z_1, z_2) \vee z_3 = z_4 \vee \neg z_5 = a(z_1, z_6)$$

$$\vee \neg z_6 = s(z_2) \vee \neg z_7 = s(z_8) \vee \neg z_8 = a(z_1, z_2) \vee z_5 = z_8 \tag{Q5a}$$

$$\neg z_3 = m(z_1, z_2) \vee \neg z_2 = 0 \vee z_3 = z_2 \tag{Q6a}$$

$$\neg z_3 = c \vee \neg z_4 = s(z_2) \vee z_5 = m(z_1, z_4) \vee \neg z_3 = z_5 \vee z_6 = m(z_1, z_2) \vee$$

$$\neg z_3 = a(z_6, z_1) \vee \neg z_7 = m(z_2, z_4) \vee \neg z_8 = a(z_6, z_2) \vee z_7 = z_8 \quad (\text{Q7a})$$

$$\neg z_1 = c \vee \neg z_2 = s(z_1) \vee z_1 = z_2 \quad (\text{Q8a})$$

$$\neg z_1 = c \vee \neg z_2 = m(z_1, z_3) \vee z_1 = z_2 \quad (\text{Q9a})$$

$$\neg z_1 = c \vee \neg z_2 = m(z_3, z_1) \vee z_1 = z_2 \quad (\text{Q10a})$$

$$\neg z_1 = c \vee \neg z_2 = a(z_3, z_1) \vee z_1 = z_2 \quad (\text{Q11a})$$

$$\neg z_1 = c \vee \neg z_2 = a(z_1, z_3) \vee z_1 = z_2 \quad (\text{Q12a})$$

Converting this formula into polynomial equations, we get:

$$s_{i_1, i_2} 0_{i_3} = 0 \text{ for } i_2 \neq i_3, i_1, i_2, i_3 \in \{1, 2, \dots, n\} \quad (\text{Q1b})$$

$$(1 - 0_{i_1}) t_{i_1, i_2} (1 - s_{i_2, i_1}) = 0 \text{ for } i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{Q2b})$$

$$(1 - c_{i_1})(1 - c_{i_2}) s_{i_1, i_3} s_{i_2, i_3} = 0 \text{ for } i_1 \neq i_2, i_1, i_2, i_3 \in \{1, 2, \dots, n\} \quad (\text{Q3b})$$

$$0_{i_2} (1 - a_{i_1, i_2, i_1}) = 0 \text{ for } i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{Q4b})$$

$$(1 - c_{i_1}) c_{i_3} a_{i_1, i_2, i_4} a_{i_1, i_6, i_5} s_{i_2, i_6} s_{i_8, i_7} a_{i_1, i_2, i_8} = 0$$

$$\text{for } i_3 \neq i_4 \text{ and } i_5 \neq i_8 \text{ and } i_1, i_2, i_3, \dots, i_8 \in \{1, 2, \dots, n\} \quad (\text{Q5b})$$

$$m_{i_1, i_2, i_3} 0_{i_2} = 0 \text{ for } i_2 \neq i_3 \text{ and } i_1, i_2, i_3 \in \{1, 2, \dots, n\} \quad (\text{Q6b})$$

$$c_{i_3} s_{i_2, i_4} (1 - m_{i_1, i_4, i_3}) (1 - m_{i_1, i_2, i_6}) a_{i_6, i_1, i_3} m_{i_2, i_4, i_7} a_{i_6, i_2, i_8} = 0$$

$$\text{for } i_7 \neq i_8 \text{ and } i_1, i_2, i_3, \dots, i_8 \in \{1, 2, \dots, n\} \quad (\text{Q7b})$$

$$c_{i_1} s_{i_1, i_2} = 0 \text{ for } i_1 \neq i_2 \text{ and } i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{Q8b})$$

$$c_{i_1} m_{i_1, i_3, i_2} = 0 \text{ for } i_1 \neq i_2 \text{ and } i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{Q9b})$$

$$c_{i_1} m_{i_3, i_1, i_2} = 0 \text{ for } i_1 \neq i_2 \text{ and } i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{Q10b})$$

$$c_{i_1} a_{i_1, i_3, i_2} = 0 \text{ for } i_1 \neq i_2 \text{ and } i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{Q11b})$$

$$c_{i_1} a_{i_3, i_1, i_2} = 0 \text{ for } i_1 \neq i_2 \text{ and } i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{Q12b})$$

Besides this we have the axioms:

$$\left( \sum_j c_j \right) - 1 = 0 \quad (\text{Q13b})$$

$$\left( \sum_j s_{i, j} \right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{Q14b})$$

$$\left(\sum_j t_{i,j}\right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{Q15b})$$

$$\left(\sum_k a_{i,j,k}\right) - 1 = 0 \text{ for } i, j \in \{1, 2, \dots, n\} \quad (\text{Q16b})$$

$$\left(\sum_k m_{i,j,k}\right) - 1 = 0 \text{ for } i, j \in \{1, 2, \dots, n\} \quad (\text{Q17b})$$

$$c_j^2 - c_j = 0 \text{ for } j \in \{1, 2, \dots, n\} \quad (\text{Q18b})$$

$$s_{i,j}^2 - s_{i,j} = 0 \text{ for } i, j \in \{1, 2, \dots, n\} \quad (\text{Q19b})$$

$$a_{i,j,k}^2 - a_{i,j,k} = 0 \text{ for } i, j, k \in \{1, 2, \dots, n\} \quad (\text{Q20b})$$

$$m_{i,j,k}^2 - m_{i,j,k} = 0 \text{ for } i, j, k \in \{1, 2, \dots, n\} \quad (\text{Q21b})$$

$$c_i c_j = 0 \text{ for } i \neq j, \text{ and } i, j \in \{1, 2, \dots, n\} \quad (\text{Q22b})$$

$$s_{i,j} s_{i,k} = 0 \text{ for } j \neq k \text{ and } i, j, k \in \{1, 2, \dots, n\} \quad (\text{Q23b})$$

$$a_{i,j,k_1} a_{i,j,k_2} = 0 \text{ for } k_1 \neq k_2 \text{ and } i, j, k_1, k_2 \in \{1, 2, \dots, n\} \quad (\text{Q24b})$$

$$m_{i,j,k_1} m_{i,j,k_2} = 0 \text{ for } k_1 \neq k_2 \text{ and } i, j, k_1, k_2 \in \{1, 2, \dots, n\} \quad (\text{Q25b})$$

Let  $Q[n]$  denote the conjunction of Q1-Q12 and let  $Q_n$  denote the conjunction of the polynomials in Q1b-Q25b. The formula  $Q[n]$  has a model of size  $n$  for each  $n$  so the translation i.e. the polynomials in  $Q_n$  are solvable. And for each  $n \in \mathbb{N}$  each solution (zero) to  $Q_n$  corresponds to a model of Robinson's arithmetical  $Q$  modified to an initial segment  $\{0, 1, \dots, n-1\}$  with a special maximal element  $c$ . We need  $Q_n$  for the next lemma:

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

- i)  $\psi$  is valid in all finite models*
- ii)  $\psi$  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:** Consider the FO-formula  $Q$  that is the conjunction of the axioms  $Q1 - Q12$ . Any finite model of  $Q$  define an initial segment of the set of the natural numbers. For any pair  $s$  and  $t$  of terms (i.e. polynomials with coefficients in the natural numbers  $N$ ) add to  $Q$  the formula  $s = c \vee \neg s = t$ . Let  $\psi_{s,t}$  denote  $Q$  in conjunction with  $s = c \vee \neg s = t$ . Let  $\Theta$  consists of the class of all  $\psi_{s,t}$  where  $s, t$  are terms (polynomials) in the language of  $Q$ .

Now the FO formula  $\psi_{s,t}$  holds in a model of size  $n$  if and only if  $s = t$  has no solution where all variables have values in  $\{0, 1, \dots, n-2\}$ . Consequently the diophantine equation  $s = t$  has **no** solution in the natural numbers if and only if  $\psi_{s,t}$  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  $\psi_{s,t}$  is invalid in sufficiently large finite models (i.e. if the equation  $s = t$  has a solution over the natural numbers), the formula  $\psi_{s,t}$  is also invalid in infinite (non-standard) models, since these models contain the standard natural numbers. ♣

Consider the polynomial equations  $Q_n$  that is the conjunction of the equations  $Q1b - Q25b$ . For a given pair of polynomials  $s$  and  $t$  (expressed as terms in the language of  $Q$ ) we add a system of polynomial equations  $Q26b$  that ensures that  $s \neq t$  holds unless  $s = c$  (or  $t = c$ ). Let us call this system of polynomial equations  $Q_n(s, t)$ .

As we will show Lemma 6 allows us (by use of Lemma 7) to draw the following conclusion:

**Proposition :** *The polynomial equations  $Q_n(s, t)$  have for any pair  $s, t$  of polynomials has either NS-refutation (PC-refutation) degree complexity of type T1 or is satisfiable for sufficiently large values of  $n$  i.e. is of type T2 (with degree complexity  $\infty$  for all sufficiently large values of  $n$ ).*

*Furthermore,  $Q_n(s, t)$  has type T1 if and only if  $s = t$  has NO solution over the natural numbers.*

## A concrete example

It is currently an open question if the equation

$$x_1^5 + x_2^5 = x_3^5 + x_4^5 \quad (*)$$

has a solution for distinct positive integers  $x_1, x_2, x_3$  and  $x_4$ . Let  $\text{NE}(x_1, x_2, x_3, x_4)$  be shorthand for the proposition that  $x_1, x_2, x_3$  and  $x_4$  are distinct and consider the first order formula

$$\begin{aligned} &\text{NE}(x_1, x_2, x_3, x_4) \rightarrow \\ &a(m(m(m(x_1, x_1), m(x_1, x_1)), x_1), m(m(m(x_2, x_2), m(x_2, x_2)), x_2)) \neq \\ &a(m(m(m(x_3, x_3), m(x_3, x_3)), x_3), m(m(m(x_4, x_4), m(x_4, x_4)), x_4)) \end{aligned}$$

This can be translated into the following polynomial equations, where we for each choice of distinct  $j_1, j_2, j_3, j_4$  with  $j_1, j_2, j_3, j_4, i_1, i_2, \dots, i_{13} \in \{1, 2, \dots, n\}$  have a polynomial equation:

$$\begin{aligned} &m_{j_1, j_1, i_1} m_{i_1, i_1, i_2} m_{i_2, j_1, i_3} m_{j_2, j_2, i_4} m_{i_4, i_4, i_5} m_{i_5, j_2, i_6} \\ &m_{j_3, j_3, i_7} m_{i_7, i_7, i_8} m_{i_8, j_3, i_9} m_{j_4, j_4, i_{10}} m_{i_{10}, i_{10}, i_{11}} \\ &m_{i_{11}, j_4, i_{12}} a_{i_3, i_6, i_{13}} a_{i_9, i_{12}, i_{13}} (1 - c_{i_{13}}) = 0 \end{aligned} \tag{Q26b(*)}$$

The polynomial equations in Q1b-Q25b together with the special polynomial equations in Q26b(\*), has models of size  $n$  if (\*) has *no* solutions involving natural numbers strictly less than  $n - 1$ . In fact:

**Observation :** *The polynomial equations Q1b-Q25b and Q26b(\*) has a solution for  $n \in N$  if and only if the equations in (\*) has no solution involving numbers strictly less than  $n - 1$*

Thus since (\*) is know to have no solutions for fairly large values of  $n$  (at least  $n > 1.000.000.000$ ) we know that the system of polynomial equations in Q1b-Q26b(\*) has a solution for all  $n \leq 1.000.000.000$ .

If the diophantine equation (\*) has no solution over  $N$  the system Q1b-Q26b(\*) has a solution for arbitrarily large values of  $n$  and thus belong to type T2 in the classification. If on the other hand the system has a solution over  $N$ , the system Q1b-Q26b(\*) has no solution in sufficiently large models (finite as well as infinite), and thus the system has a constant degree NS-refutation (lemma 7) i.e. is of type T1.

Let us modify the equations in Q26b(\*) (obtaining a system Q26b(\*\*)) to express (the falsity) that

$$x_1^4 + x_2^4 \neq x_3^4 + x_4^4 \tag{**}$$

for distinct  $x_1, x_2, x_3$  and  $x_4$ . The following polynomial equations will do:

$$m_{j_1, j_1, i_1} m_{i_1, i_1, i_2} m_{j_2, j_2, i_3} m_{i_3, i_3, i_4} m_{j_3, j_3, i_5} m_{i_5, i_5, i_6}$$

$$m_{j_4, j_4, i_7} m_{i_7, i_7, i_8} a_{i_2, i_4, i_9} a_{i_6, i_8, i_9} (1 - c_{i_9}) = 0 \quad (\text{Q26b(**)})$$

It is known that  $133^4 + 134^4 = 59^4 + 158^4$  from which it follows that the polynomial equations Q1b-Q25b together with Q26b(\*\*) are unsatisfiable in models of size  $\geq 133^4 + 134^4 + 1 = 635.318.658$ . The equation (\*\*) is unsatisfiable in sufficiently large models (finite as well as infinite) that satisfies Robinson's arithmetical Q axiomatized as an initial segment. This is because each sufficiently large initial segment allow us to implement the calculation  $133^4 + 134^4 = 59^4 + 158^4$ . We will show that this fact guarantee that there exists a general calculation (like the calculations in D1 and D2) that constitute a constant degree NS-refutation of Q1b-Q25b combined with Q26b(\*\*).

### Implicit build-in axioms of equality

Before we state and show Lemma 7, we present a example that illustrate how the axioms of equality are nicely build into the translation. Consider as an example the FO-formula

$$\gamma := c^1 = c^2 \wedge c^2 = c^3 \wedge \neg c^1 = c^3 \quad (1)$$

in the FO language  $L$  containing the three constants  $c^1, c^2$  and  $c^3$ . This formula is NOT a contradiction in logic without equality where  $=$  is just treated as any other relation symbol. The presence of the basic equations for constants and function symbols ensure that the axioms of equality is taken properly care of.

The formula  $\gamma$  can be converted to an equivalent proposition in  $S$

$$(z_1 \neq c^1 \vee z_2 \neq c^2 \vee z_1 = z_2) \bigwedge (z_2 \neq c^2 \vee z_2 \neq c^3 \vee z_2 = z_3)$$

$$\bigwedge (z_1 \neq c^1 \vee z_3 \neq c^3 \vee z_1 \neq z_3) \quad (2)$$

This translate into the polynomial equations:

$$c_{i_1}^1 c_{i_2}^2 = 0 \text{ for } i_1 \neq i_2, i_1, i_2 \in \{1, 2, \dots, n\} \quad (\text{E1})$$

$$c_{i_2}^2 c_{i_3}^3 = 0 \text{ for } i_2 \neq i_3, i_2, i_3 \in \{1, 2, \dots, n\} \quad (\text{E2})$$

$$c_{i_1}^1 c_{i_3}^3 = 0 \text{ for } i_1 = i_3, i_1, i_3 \in \{1, 2, \dots, n\} \quad (\text{E3})$$

As usual we introduce some addition equations of each constant and function symbols:

$$\left(\sum_k c_k^1\right) - 1 = 0, \quad \left(\sum_k c_k^2\right) - 1 = 0 \text{ and } \left(\sum_k c_k^3\right) - 1 = 0 \quad (\text{E4})$$

These set of equations in (E1)-(E4) has the following NS-refutation:

$$\begin{aligned} & \sum_{i,j,k \text{ with } i \neq j} c_k^3 [c_i^1 c_j^2] + \sum_{j,k} c_j^1 [c_j^2 c_k^3] + \sum_i c_i^2 [c_i^1 c_i^3] \\ & - \sum_{i,j} (c_i^1 c_j^2) \left[ \left(\sum_k c_k^3\right) - 1 \right] - \sum_i c_i^1 \left[ \left(\sum_j c_j^2\right) - 1 \right] - \left[ \left(\sum_i c_i^1\right) - 1 \right] = 1 \quad (\text{D4}) \end{aligned}$$

### Example illustrating the general construction

This section is inserted as a benefit for readers that might find it useful to see how the main ideas in the proof of Proposition A (Lemma 7), plays out in a concrete example. The reader who is not interested in the guidance offered by the example, is welcome to *jump straight to the next section*.

In the example we consider the following inconsistent formula  $\eta_{1+2 \neq 3}$  that essentially states that  $1 + 2 \neq 3$ . Formally,

$$x = a(x, c) \wedge a(x, s(y)) = s(a(x, y)) \wedge \neg a(s(c), s(s(c))) = s(s(s(c))) \quad (\text{P1-P3})$$

These equations are contradictory since

$$a(s(c), s(s(c))) = s(a(s(c), s(c))) = s(s(a(s(c), c))) = s(s(s(c))).$$

To translate the FO-formula into a sequence of propositional formula first we convert  $\eta_{1+2 \neq 3}$  into a special FO-formula  $\tilde{\eta}_{1+2 \neq 3}$  that belongs to the special class  $S$  of FO-formula. The formula  $\tilde{\eta}_{1+2 \neq 3}$  is the conjunction of

$$z_1 \neq c \vee x = a(x, z_1) \quad (\text{P1a})$$

$$z_2 \neq s(y) \vee z_3 \neq a(x, y) \vee z_4 \neq s(z_3) \vee z_5 \neq a(x, z_2) \vee z_4 = z_5 \quad (\text{P2a})$$



$$z_6 \neq c \bigvee z_7 \neq s(z_6) \bigvee z_8 \neq s(z_7) \bigvee z_9 \neq s(z_8) \bigvee z_{10} \neq a(z_7, z_8) \bigvee z_9 \neq z_{10} \quad (\text{P3a})$$

The inequality symbol " $\neq$ " is not part of the language and for any choice of terms  $s, t$  the expression  $t \neq s$  is short hand for  $\neg t = s$ .

For each  $n \in N$  we convert the FO-formula  $\eta_{1+2 \neq 3}$  (i.e.  $\tilde{\eta}_{1+2 \neq 3}$ ) to a sequence  $\eta_{1+2 \neq 3}[n]$  of polynomial equations. The equation  $z_1 = c$  is replaced with a variable  $c_j$  for each  $j = 1, 2, \dots, n$ . And following the translation procedure we let  $c_{i_1}$  is 1 if and only if  $i_1 = c$ . Otherwise  $c_{i_1}$  is zero. The equation  $z_2 = s(z_1)$  is replaced with a variable  $s_{i_1, i_2}$  for each  $i_1, i_2 \in \{1, 2, \dots, n\}$ . According to the translation procedure  $s_{i_1, i_2}$  is 1 if and only if  $i_2 = s(i_1)$ . Otherwise  $s_{i_1, i_2}$  is zero. Finally, the equation  $z_3 = a(z_1, z_2)$  is replaced by a variable  $a_{i_1, i_2, i_3}$  for each  $i_1, i_2, i_3 \in \{1, 2, \dots, n\}$ . According to the translation procedure,  $a_{i_1, i_2, i_3}$  is 1 if and only if  $i_3 = a(i_1, i_2)$ . Otherwise  $s_{i_1, i_2, i_3}$  is zero.

$$p_{i_1, j_1}^{[1]} := c_{i_1} (1 - a_{j_1, i_1, j_1}) = 0 \text{ for } i_1, j_1 \in \{1, 2, \dots, n\} \quad (\text{P1b})$$

$$p_{j_1, j_2, i_2, i_3, i_4, i_5}^{[2]} := s_{j_2, i_2} a_{j_1, j_2, i_3} s_{i_3, i_4} a_{j_1, i_2, i_5} = 0 \\ \text{for } i_4 \neq i_5 \text{ and } j_1, j_2, i_2, i_3, i_4, i_5 \in \{1, 2, \dots, n\} \quad (\text{P2b})$$

$$p_{i_6, i_7, i_8, i_9, i_{10}}^{[3]} := c_{i_6} s_{i_6, i_7} s_{i_7, i_8} s_{i_8, i_9} a_{i_7, i_8, i_{10}} = 0 \\ \text{for } i_9 = i_{10} \text{ and } i_6, i_7, i_8, i_9, i_{10} \in \{1, 2, \dots, n\} \quad (\text{P3b})$$

Besides these polynomial equations we include:

$$p^{[4]} := \left( \sum_j c_j \right) - 1 = 0 \quad (\text{P4b})$$

$$p_{i, j}^{[5]} := c_i c_j = 0 \text{ for } i \neq j \text{ and } i, j \in \{1, 2, \dots, n\} \quad (\text{P5b})$$

$$p_i^{[6]} := \left( \sum_k s_{i, k} \right) - 1 = 0 \text{ for } i \in \{1, 2, \dots, n\} \quad (\text{P6b})$$

$$p_{i, k, m}^{[7]} := s_{i, k} s_{i, m} = 0 \text{ for } k \neq m \text{ and } i, k, m \in \{1, 2, \dots, n\} \quad (\text{P7b})$$

$$p_{i, j}^{[8]} := \left( \sum_k a_{i, j, k} \right) - 1 = 0 \text{ for } i, j \in \{1, 2, \dots, n\} \quad (\text{P8b})$$

$$p_{i, j, k, m}^{[9]} := a_{i, j, k} a_{i, j, m} = 0 \text{ for } k \neq m \text{ and } i, j, k, m \in \{1, 2, \dots, n\} \quad (\text{P9b})$$

The FO-formula  $\eta_{1+2\neq 3}$  (as well as  $\tilde{\eta}_{1+2\neq 3}$ ) fail in ALL models (finite as well as infinite). Thus Proposition A apply and there exist a constant degree NS-refutation of the polynomial equations P1b-P9b.

We will later in the paper show Proposition A (Lemma 7) by use of Herbrand's Theorem. As a preparation for this we will here illustrate how Herbrands Theorem can be used to construct the required NS-refutation of the polynomial equations P1b-P9b.

In general if a quantifier free formula  $\eta(\vec{x})$  with variables  $\vec{x}$  fails in all models, by the completeness theorem  $\eta$  is a logical contradiction in predicate logic with equality. There is finite collection  $E$  of term equations (instances of the equality axioms) such that  $\tilde{\eta} := \eta \wedge E$  is a logical contradiction of predicate logic (without axioms of equality). According to an obvious modification of Herbrand's theorem (switching from a valid disjunction to an invalid conjunction) there exists a finite conjunction

$$\tilde{\eta}(\vec{x}_1) \wedge \tilde{\eta}(\vec{x}_2) \wedge \dots \wedge \tilde{\eta}(\vec{x}_r)$$

(the variables  $\vec{x}_i$  for  $i = 1, 2, \dots, r$  are all distinct), together with a term unification (as introduced by Julia Robinson)

$$\Delta = \{\vec{t}_1 \rightarrow \vec{x}_1, \vec{t}_2 \rightarrow \vec{x}_2, \dots, \vec{t}_r \rightarrow \vec{x}_r\}$$

such that

$$\Delta(\tilde{\eta}(\vec{x}_1) \wedge \tilde{\eta}(\vec{x}_2) \wedge \dots \wedge \tilde{\eta}(\vec{x}_r)) \equiv \tilde{\eta}(\vec{t}_1) \wedge \tilde{\eta}(\vec{t}_2) \wedge \dots \wedge \tilde{\eta}(\vec{t}_r)$$

is a logical contradiction *in the sense of propositional logic*.

The following conjunctive normal form is contradictory in the sense of propositional logic (it follows from Herbrand's Theorem that such one exists).

$$a(s(c), s(s(c))) = s(a(s(c), s(c))) \tag{U1}$$

$$a(s(c), s(c)) = s(a(s(c), c)) \tag{U2}$$

$$s(c) = a(s(c), c) \tag{U3}$$

$$\neg a(s(c), s(s(c))) = s(s(s(c))) \tag{U4}$$

$$\neg a(s(c), s(c)) = s(a(s(c), c)) \vee s(a(s(c), s(c))) = s(s(a(s(c), c))) \tag{U5}$$

$$\neg s(c) = a(s(c), c) \vee s(s(s(c))) = s(s(a(s(c), c))) \tag{U6}$$

$$\neg s(s(s(c))) = s(s(a(s(c), c))) \bigvee s(s(a(s(c), c))) = s(s(s(c))) \quad (\text{U7})$$

$$\neg a(s(c), s(s(c))) = s(a(s(c), s(c))) \bigvee \neg s(a(s(c), s(c))) = s(s(a(s(c), c)))$$

$$\bigvee a(s(c), s(s(c))) = s(s(a(s(c), c))) \quad (\text{U8})$$

$$\neg a(s(c), s(s(c))) = s(s(a(s(c), c))) \bigvee \neg s(s(a(s(c), c))) = s(s(s(c)))$$

$$\bigvee a(s(c), s(s(c))) = s(s(s(c))) \quad (\text{U9})$$

The fact that there are 9 type of equations (P1)-(P9) as well as 9 conjuncts in (U1)-(U9) is just a coincidence. To convert this Herbrand formula into a NS-refutation, we first let

$$u_1 := c, \quad s(c) = u_2 = s(u_1), \quad s(s(c)) = u_3 = s(u_2), \quad s(s(s(c))) = u_4 = s(u_3)$$

$$a(s(c), c) = u_5 = a(u_2, u_1), \quad s(a(s(c), c)) = u_6 = s(u_5)$$

$$a(s(c), s(c)) = u_7 = a(u_2, u_2), \quad s(a(s(c), s(c))) = u_8 = s(u_7)$$

$$s(s(a(s(c), c))) = u_9 = s(u_6), \quad a(s(c), s(s(c))) = u_{10} = a(u_2, u_3)$$

We can express the term equations as:

$$u_{10} = u_8 \quad (\text{U1a})$$

$$u_7 = u_6 \quad (\text{U2a})$$

$$u_2 = u_5 \quad (\text{U3a})$$

$$\neg u_{10} = u_4 \quad (\text{U4a})$$

$$\neg u_7 = u_6 \bigvee u_8 = u_4 \quad (\text{U5a})$$

$$\neg u_2 = u_5 \bigvee u_4 = u_9 \quad (\text{U6a})$$

$$\neg u_4 = u_9 \bigvee u_9 = u_4 \quad (\text{U7a})$$

$$\neg u_{10} = u_8 \bigvee \neg u_8 = u_9 \bigvee u_{10} = u_9 \quad (\text{U8a})$$

$$\neg z_{10} = u_9 \bigvee \neg u_9 = u_4 \bigvee u_{10} = u_4 \quad (\text{U9a})$$

Let  $\delta(v \neq u)$  denote a version of Kroneker's  $\delta$  function defined as 1 if  $v \neq u$  and as 0 if  $v = u$ . As shorthand notation let  $Y_1 \leftarrow \delta(i_{10} \neq i_8)$ ,

$Y_2 \leftarrow \delta(i_7 \neq i_6)$ ,  $Y_3 \leftarrow \delta(i_2 \neq i_5)$ ,  $Y_4 \leftarrow \delta(i_{10} \neq i_4)$ ,  $Y_5 \leftarrow \delta(i_7 \neq i_9)$ ,  
 $Y_6 \leftarrow \delta(i_4 \neq i_9)$ ,  $Y_7 \leftarrow \delta(i_9 \neq i_4)$ ,  $Y_8 \leftarrow \delta(i_{10} \neq i_9)$ .

We can then write conditions (U1a)-(U9a) as:  $1 - Y_1 = 0$ ,  $1 - Y_2 = 0$ ,  
 $1 - Y_3 = 0$ ,  $Y_4 = 0$ ,  $Y_2(1 - Y_5) = 0$ ,  $Y_3(1 - Y_6) = 0$ ,  $Y_6(1 - Y_7) = 0$ ,  
 $Y_1Y_5(1 - Y_8) = 0$ ,  $Y_8Y_7(1 - Y_4) = 0$ . These equations can be converted into  
the following NS-refutation of the equations U1b-U8b.

$$\begin{aligned} & Y_5(1-Y_8)[1-Y_1] + [Y_1Y_5(1-Y_8)] + (1-Y_8)(1-Y_5)[1-Y_2] + (1-Y_8)[Y_2(1-Y_5)] \\ & + Y_8[1 - Y_3] + Y_8[Y_3(1 - Y_6)] + Y_3Y_8[Y_6(1 - Y_7)] \\ & + Y_3Y_6Y_8Y_7[Y_4] + Y_3Y_6[Y_8Y_7(1 - Y_4)] = 1 \end{aligned} \quad (W)$$

Our aim is to show how to convert this derivation into a derivation of 1 from  
the polynomial equations P1b-P9b.

Using this NS-refutation we get the required constant degree derivation  
of  $0 = 1$  from the polynomials equations in P1b-P9b. The derivation is based  
on the following identity:

$$\begin{aligned} & \sum_{u_1, u_2, u_3, \dots, u_{10}} (c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} Y_5(1-Y_8)[1-Y_1] + \\ & u_1 c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} Y_1 Y_5 [1 - Y_8] + \\ & c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} (1-Y_8)(1-Y_5)[1-Y_2] + \\ & c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} (1-Y_8)[Y_2(1-Y_5)] + \\ & c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} Y_8 [1 - Y_3] + \\ & c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} Y_8 [Y_3(1 - Y_6)] + \\ & c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} Y_3 Y_8 [Y_6(1 - Y_7)] + \\ & c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} Y_3 Y_6 Y_8 Y_7 [Y_4] + \\ & c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} a_{u_2, u_3, u_{10}} Y_3 Y_6 [Y_8 Y_7(1 - Y_4)]) \\ & - \sum_{u_1, u_2, \dots, u_9} c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} s_{u_8, u_9} [(\sum_{u_{10}} a_{u_2, u_3, u_{10}}) - 1] \\ & - \sum_{u_1, u_2, \dots, u_8} c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} s_{u_7, u_8} [(\sum_{u_9} s_{u_8, u_9}) - 1] \\ & - \sum_{u_1, u_2, \dots, u_7} c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} a_{u_2, u_2, u_7} [(\sum_{u_8} s_{u_7, u_8}) - 1] \end{aligned}$$

$$\begin{aligned}
& - \sum_{u_1, u_2, \dots, u_6} c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} s_{u_5, u_6} \left[ \left( \sum_{u_7} a_{u_2, u_2, u_7} \right) - 1 \right] \\
& - \sum_{u_1, u_2, \dots, u_5} c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} a_{u_2, u_1, u_5} \left[ \left( \sum_{u_6} s_{u_5, u_6} \right) - 1 \right] \\
& - \sum_{u_1, u_2, \dots, u_4} c_{u_1} s_{u_1, u_2} s_{u_2, u_3} s_{u_3, u_4} \left[ \left( \sum_{u_5} a_{u_2, u_1, u_5} \right) - 1 \right] \\
& - \sum_{u_1, u_2, u_3} c_{u_1} s_{u_1, u_2} s_{u_2, u_3} \left[ \left( \sum_{u_4} s_{u_3, u_4} \right) - 1 \right] \\
& - \sum_{u_1, u_2} c_{u_1} s_{u_1, u_2} \left[ \left( \sum_{u_3} s_{u_2, u_3} \right) - 1 \right] \\
& - \sum_{u_1} c_{u_1} \left[ \left( \sum_{u_2} s_{u_1, u_2} \right) - 1 \right] \\
& - \left[ \left( \sum_{u_1} c_{u_1} \right) - 1 \right] = 1 \tag{D5}
\end{aligned}$$

**To summarize:** Since the equations P1b-P9b are contradictory it follows from Hilbert Nullstellensatz that the polynomial equations (P1)-(P9) can be refuted i.e. 1 can be derived by a NS-derivation from these equations. The calculation D5 above shows that there is in fact a NS-derivation of 1 that involves only polynomials of a degree bound by a constant (= 10) independently of  $n$  (notice that only the equations P1,P2,P3,P4,P6 and P8 were used in the calculation D2). According to proposition A, the fact that the original term equations are contradictory (including in infinite models) implies that there exists such a constant degree derivation of 1. The proof of proposition A, proceed along very similar lines as the calculations above.

## Proof of Proposition A

**Lemma 7 :** (Proposition A) *If  $\psi$  is an FO-formula such that  $\psi$  is unsatisfiable in all sufficiently large finite models and is unsatisfiable in all infinite models, then there exists for each field  $F$  a number  $d \in \mathbb{N}$  such that each  $\psi[n]$  has a degree  $d$  NS-refutation.*

Before we prove this we will make some preperational definitions. Without loss of generality we can assume that  $\psi$  is a quantifier free formula in some finite FO-language  $L$  and is on the special form  $S$ . Assume  $L =$

$L(f^1, f^2, \dots, f^r, r^1, r^2, \dots, r^s)$  besides the relation symbols  $r^1, r^2, \dots, r^s$  also contain the function symbols  $f^1, f^2, \dots, f^r$ , where  $f^u$  has arity  $a_u \geq 0$ .

As we already explained in the translation procedure for each function symbol  $f^u$  of arity  $a_u$ , a collection

$$f_{i_1, i_2, \dots, i_{a_u}, j}^u \text{ where } i_1, i_2, \dots, i_{a_u}, j \in \{1, 2, \dots, n\} \quad (\text{H1})$$

of  $n^{a_u+1}$  a new (boolean) variables is introduced. As we already explained the idea is that if  $M = \{1, 2, \dots, n\}$  then

$$f_{i_1, i_2, \dots, i_{a_u}, j}^u = 1 \text{ exactly if } M \models f^u(i_1, i_2, \dots, i_{a_u}) = j \quad (\text{H2})$$

The equations

$$\left( \sum_j f^u(i_1, i_2, \dots, i_{a_u}, j) \right) - 1 = 0 \text{ for } i_1, i_2, \dots, i_{a_u} \quad (\text{H3})$$

and

$$f_{i_1, i_2, \dots, i_{a_u}, j}^u f_{i_1, i_2, \dots, i_{a_u}, k}^u = 0 \text{ for } j \neq k, i_1, i_2, \dots, i_{a_u}, j, k \in M \quad (\text{H4})$$

ensure that  $f^u$  has a unique value  $j \in M$  for each  $i_1, i_2, \dots, i_{a_u} \in M$ .

For each closed term  $t := f(t_1, t_2, \dots, t_r)$  we want to assign a monomial  $X_t$ , a "variable"  $v_t$  as well as a set of variables  $\text{Var}(t)$ . This assignment is done inductively such that  $v_t$  is a new variable, and such that

$$X_t = f_{v(t_1), v(t_2), \dots, v(t_r), v_t} X_{t_1} X_{t_2} \dots X_{t_r} \quad (\text{H5})$$

We define  $\text{Var}(t)$  inductively as

$$\text{Var}(t) = \text{Var}(t_1) \cup \text{Var}(t_2) \cup \dots \cup \text{Var}(t_r) \cup \{v_t\} \quad (\text{H6})$$

The variable  $v_t$  denote the value of the term  $t$  and  $\text{Var}(t)$  consists of all variables that denote values of sub-terms of  $t$ .

Let  $\Delta$  be a set of closed terms and assume that  $\Delta$  is closed under taking sub-formula i.e. if  $f(t_1, t_2, \dots, t_r) \in \Delta$  then  $t_1, t_2, \dots, t_r \in \Delta$ . Then we define a monomial

$$X_\Delta := \prod_{t \in \Delta} X_t \quad (\text{H7})$$

And we define

$$\text{Var}(\Delta) := \bigcup_t \text{Var}(t) \quad (\text{H8})$$

An evaluation  $E$  is a map  $E : \text{Var}(\Delta) \rightarrow M$ . The idea is that each evaluation  $E$  give each term in  $\Delta$  a specific value in  $M$ .

The equations

$$\left( \sum_{E \in M^{\text{Var}(\Delta)}} X_{\Delta}^E \right) - 1 = 0 \text{ and } \sum_{E \in M^{\text{Var}(\Delta)}} X_{\Delta}^E = 0 \quad (\text{H9})$$

will play an important role in our argument.

The first equation essentially says that *all the terms in  $\Delta$  has (at least) one value*. We will show (Lemma 7A) that this equation can be written as a NS-expression of degree  $|\Delta|$  from the axioms in (H3).

The second equation says that *if all the terms in  $\Delta$  are defined, then a contradiction occurs*. We will show (Lemma 7B) that if for some  $n_0 \in \mathbb{N}$  the FO-sentence  $\psi$  is contradictory in *all* models of size  $\geq n_0$  Herbrand's Theorem allows us to choose  $\Delta$  such that the second equation can be written as a NS-expression bounded by a constant that is independent of  $n$ .

Combining the two equations leads to the required constant degree refutation since

$$0 = 0 - 0 = \sum_{E \in M^{\text{Var}(\Delta)}} X_{\Delta}^E - \left( \left( \sum_{E \in M^{\text{Var}(\Delta)}} X_{\Delta}^E \right) - 1 \right) = 1 \quad (\text{H10})$$

**Lemma 7A :** *Let  $\Delta$  be a set of closed terms in the language  $L$ . Assume that  $\Delta$  contains all sub-terms of each term  $t \in \Delta$ . Then equation*

$$\left( \sum_{E \in M^{\text{Var}(\Delta)}} X_{\Delta}^E \right) - 1 = 0 \quad (\text{H11})$$

*has a NS-derivation of degree  $s = |\Delta|$  from the polynomial equations in (H3)*

**Proof:** For terms  $t, t'$  in the language of  $L$  we write  $t \prec t'$  if  $t$  is a sub-term of  $t'$ . The relation  $\prec$  is a partial ordering. Extend  $\prec$  to a total ordering. Assume  $\Delta = \{t_1, t_2, \dots, t_r\}$ . Without loss of generality we can assume that  $t_1 \prec t_2 \prec \dots \prec t_r$ . The Lemma now follows from the general identity:

$$\sum_{E \in M^{\text{Var}(\{t_1, t_2, \dots, t_r\})}} X_{\{t_1, t_2, \dots, t_r\}}^E - 1 =$$

$$\begin{aligned}
& \sum_{E \in M^{\text{Var}(\{t_1, t_2, \dots, t_{r-1}\})}} X_{\{t_1, t_2, \dots, t_{r-1}\}}^E [(\sum_{E \in M^{\text{Var}(t_r)}} X_{t_r}^E) - 1] + \\
& \sum_{E \in M^{\text{Var}(\{t_1, t_2, \dots, t_{r-2}\})}} X_{\{t_1, t_2, \dots, t_{r-2}\}}^E [(\sum_{E \in M^{\text{Var}(t_{r-1})}} X_{t_{r-1}}^E) - 1] + \dots + \\
& \sum_{E \in M^{\text{Var}(\{t_1, t_2, \dots, t_j\})}} X_{\{t_1, t_2, \dots, t_j\}}^E [(\sum_{E \in M^{\text{Var}(t_{j+1})}} X_{t_{j+1}}^E) - 1] + \dots + \\
& [(\sum_{E \in M^{\text{Var}(t_1)}} X_{t_1}^E) - 1] \tag{H12}
\end{aligned}$$

♣

**Lemma 7B :** *Assume  $\psi$  is a quantifier free FO-formula in  $L$  on the special form  $S$ . Assume further that  $\psi$  has no models of size  $\geq n_0 \in N$  i.e. that  $\psi$  is contradictory in all models of size  $\geq n_0$ . Then there exists a set  $\Delta$  of terms such that for each  $n \geq n_0$*

$$\sum_{E \in M^{\text{Var}(\Delta)}} X_{\Delta}^E = 0 \tag{H13}$$

*has a NS-derivation from the propositional translation  $\psi[n]$  of  $\psi$ . The degree of the NS-derivation can be chosen independently of  $n$ .*

**Proof: Case 1:**  $\psi = \psi(\vec{x})$  *is unsatisfiable in ALL models:* Assume  $\psi(\vec{x})$  has no models. According the the completeness theorem in this case  $\psi(\vec{x})$  has a refutation in predicate logic. Actually, we can apply Herbrand's theorem and conclude that there there exists  $r$  such that the formula

$$\psi(\vec{x}_1) \wedge \psi(\vec{x}_2) \wedge \dots \wedge \psi(\vec{x}_r) \tag{H14}$$

has a unification

$$\Delta(\vec{t}_1 \rightarrow \vec{x}_1, \vec{t}_2 \rightarrow \vec{x}_2, \dots, \vec{t}_r \rightarrow \vec{x}_r) \tag{H15}$$

Since we consider logic with equality, the resulting formula

$$\psi(\vec{x}_1/\vec{t}_1) \wedge \psi(\vec{x}_2/\vec{t}_2) \wedge \dots \wedge \psi(\vec{x}_r/\vec{t}_r) \tag{H16}$$




is not necessarily a contradiction in propositional logic (where as usual atomic sentences are viewed formally as propositional variables). However, for each interpretation of the terms in  $\Delta$  the resulting formula

$$\psi(\vec{v}_1) \wedge \psi(\vec{v}_2) \wedge \dots \wedge \psi(\vec{v}_r) \quad (\text{H17})$$

is a contradiction in propositional logic.


Let  $\Delta$  be the collection of all terms in the unifactaion as well as all sub-terms of these terms.

Now for each evaluation  $E : \text{Var} \rightarrow M$ , the monomial  $X_{\Delta}^E$  take the value 1 only if the evaluation  $E$  evaluate the terms in  $\Delta$  in  $M$ . But  $\Delta$  was chosen such that the proposition in (H17) is a contradiction in propositional logic. Assume the propositional formula in (H17) has a degree  $d$  NS-refutation (over the underlying field  $F$ ). This refutation allows us for each interpretation  $E$ , to derive  $X_{\Delta}^E$  by an expression of degree  $|\Delta| + d$  NS-derivation.

**Case 2:**  $\psi = \psi(\vec{x})$  is unsatisfiable in all models of size  $\geq n_0$ : Add new constants  $c^1, c^2, \dots, c^{n_0}$  to the models together with the conjunction  $\tau$  of  $c^i \neq c^j$  for  $i, j \in \{1, 2, \dots, n_0\}$  and  $i \neq j$ . The resulting formula  $\psi \wedge \tau$  has no models and thus Case 1, applies that the system  $(\psi \wedge \tau)[n]$  of polynomial equations that arise from the translation of  $\psi \wedge \tau$  has a constant degree NS-refutation. If we compare there polynomial equations in  $(\psi \wedge \tau)[n]$  with those in  $\psi[n]$  we notice that if we choose a specific assignment of the constants  $c^1, c^2, \dots, c^{n_0}$  in  $M$  such that they have distinct values (this require  $n \geq n_0$ ) the resulting NS-derivation of 1 from the polynomials in  $(\psi \wedge \tau)[n]$  become a NS-derivation of 1 from the polynomials in  $\psi[n]$ . 

**Lemma 8 :** *The decision problem whether a given first order formula  $\psi$  leads to a sequence  $\psi[n]$  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  $\psi$  of a type  $\tau$  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 *not* of type  $\tau$  if and only if  $\theta_{S,R} \wedge \psi$  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  $N$ . 

## 8 NS versus PC

In general there 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 ourselves to the uniform sequences generated by a FO formula, Krajicek [25] have shown that such a situation cannot occur.

**Lemma 9 :** (Theorem 5.5 [25]) *Let  $S \subseteq N$  be a fixed infinite set. Assume that  $\psi[n]$  has degree  $d$  PC-refutations for each  $n \in S$ . Then there exists a constant  $d' \geq d$  such that each  $\psi[n]$  with  $n \in S$ , has a degree  $d'$  NS-refutation.*

**Theorem 10 :** *For an FO-formula  $\psi$ , the type of  $\psi$  with respect to the NS-refutation complexity behavior of  $\psi[n]$  is identical to the type of  $\psi$  with respect to the PC-refutation complexity behavior of  $\psi[n]$ .*

**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 follows then from Theorem 1 that a first order formula  $\psi$  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.

♣

## 9 Final remarks

The big question is whether the main result remains 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  $n^\epsilon$  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. <sup>3</sup>

One consequence of Theorem 1 is that the translation of any FO formula  $\psi$  leads to a sequence  $\psi[n]$  that *asymptotically* has worst case refutation

---

<sup>3</sup>In the preprint [33] such a complexity gap from linear to  $n^\epsilon$  (in the worst case) was claimed. Unfortunately, the paper was rather obscure and it turned out that the "inducing down" argument contains a gap. Despite considerable effort we have not been able to fix this gap. We still conjecture that the main claim is valid, but it is now clear that new ideas are needed in the proof.

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] M. Ajtai. The independence of the modulo p counting principles. *Annual ACM Symposium on Theory of Computing (STOC)*, 26(6):402–411, 1994. ACM Press.
- [2] M. Ajtai. Symmetric systems of linear equations modulo p. *Preprint*, 8(TR94-015), 1994. <http://www.eccc.uni-trier.de/eccc>.
- [3] 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.
- [4] 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.
- [5] M. Bonet and N. Galesi. Optimality of size-width tradeoffs for resolution. Technical Report 10(4), Computational Complexity, 2001. 261-276.
- [6] D. Brownawell. Bounds for the degrees in the nullstellensatz. *Annals of Mathematics*, 126:577–591, 1987. (second Series).
- [7] S. Buss. Lower bounds on nullstellensatz proofs via designs. *in Proof Complexity and Feasible Arithmetics*, S. Buss and P. Beame, eds., pages 59–71, 1998. American Mathematical Society, Providence.
- [8] S. Buss, R. Impagliazzo, J. Krajicek, P. Pudlak, A. Razborov, and J. Sgall. Proof complexity in algebraic systems and bounded depth frege systems with modular counting. *Computational Complexity*, 6(3):256–298, 1997. Birkhauser Verlag.
- [9] S. Buss and T. Pitassi. Good degree lower bounds on nullstellensatz refutations of the induction principle. *Proceedings of the Eleventh Annual Conference on Structure in Complexity Theory*, pages 233–242, 1996. IEEE Computer Society.

- [10] L. Caniglia, A. Galligo, and J. Heintz. Some new effective bounds in computational geometry. *Proceedings 6th International Conferences on Applied Algebra, Algebraic Algorithms and error correcting codes*, 357, 1988. Lecture Springer Notes CS 357.
- [11] 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.
- [12] S. Cook. Feasibly constructive proofs and the propositional calculus. *Annual ACM Symposium on Theory of Computing (STOC)*, 7:83–97, 1975.
- [13] S. Cook and P. Nguyen. Foundations of proof complexity: Bounded arithmetic and propositional translations. Technical report, Book (Draft version), 2008.
- [14] S. Cook and R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.
- [15] S. Danchev. Complexity gap for sherali-adams and lovsz-schrijver proof systems. *STOC*, 2007.
- [16] S. Dantchev, B. Martin, and S. Szeider. Parameterized proof complexity. *FOCS*, 2007.
- [17] 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.
- [18] 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.
- [19] D. Grigoriev and E. Hirsch. Algebraic proof systems over formulas. *Theoretical Computer Science*, 3:83–102, 2003.
- [20] G. James. The representation theory of the symmetric groups. *Springer-Verlag*, 682, 1978. Lecture Notes in Mathematics.
- [21] J. Kollar. Sharp effective nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.
- [22] J. Krajicek. Lower bounds on the size of constant-dept propositional proofs. *Journal of Symbolic Logic*, 59(3):73–86, 1994.
- [23] J. Krajicek. *Bounded arithmetic, propositional logic and complexity theory*, volume 60, chapter Encyclopeda of Mathematics and its applications, pages 1–772. Cambridge University Press, 1995.
- [24] 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.
- [25] 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.

- [26] J. Krajicek. Combinatorics of first order structures and propositional systems. *Arkive for Mathematical logic*, 43(4):427–441, 2004.
- [27] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. *Methods in Mathematical logic*, Springer-Verlag, LNM 1130:317–340, 1985.
- [28] T. Pitassi. Algebraic propositional proof systems. *Dimacs Discrete Mathematics and Theoretical Computer Science (Vol 31)*, 10:179–209, 1997.
- [29] R. Raz. Resolution lower bounds for the weak pigeonhole principle. *Journal of Association for Computing Machinery* 51(2), 51(2):115–138, 2004.
- [30] R. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7:291–324, 1998.
- [31] S. Riis. *Arithmetic, proof and complexity*, chapter Making infinite structures finite in models of bounded arithmetic, pages 289–319. Oxford University Press, 1993.
- [32] S. Riis. A complexity gap for tree-resolution. *Computational Complexity*, 10:179–209, 2001.
- [33] S. Riis and M. Sitharam. Non-constant degree lower bounds imply linear degree lower bounds. *ECCC*, TR97-048:1–46, 1997. The inducing down argument contains a gap that cannot be repaired unless new ideas are introduced.
- [34] S. Riis and M. Sitharam. Generating hard tautologies using predicate logic and the symmetric group. *Logic Journal of the IGPL*, 8(6):787–795, 2000. Oxford University Press.
- [35] G. Stalmarck. Short resolution proofs for a sequence of tricky formulas. *Acta Informatica* 33 (1996) 277280, 33:277–280, 1996.
- [36] A. Urquhart. Regular and general resolution: An improved separation. Technical report, University of Toronto, 2008. Submitted.