Non-constant Degree Lower Bounds imply linear Degree Lower Bounds.

Søren Riis[*] **Meera Sitharam**[†]

October 13, 1997

Abstract

The semantics of decision problems are always essentially independent of the underlying representation. Thus the space of input data (under appropriate indexing) is closed under action of the symmetrical group S_n (for a specific data-size) and the input-output relation is closed under the action of S_n. We show that symmetries of this nature (together with uniformity constraints) have profound consequences in the context of Nullstellensatz Proofs and Polynomial Calculus Proofs (Gröbner basis proofs).

Our main result states that for any co-NP (i.e. Universal Second Order) sentence ψ any non-constant degree lower bound on Nullstellensatz proofs of ψ_n immediately lifts to a linear-degree lower bound. This kind of "gap" theorem is new in this area of complexity theory.

The gap theorem is valid for Polynomial Calculus proofs as well, and allows us immediately to solve a list of open problems concerning degree lower bounds. We get a linear degree (linear in the model size) lower bounds for various matching principles. This solves an open problem first posed in [3]. The bounds also improves the degree lower bounds of $\Omega(n^\epsilon)$ achieved in [5] as well as the degree lower bounds achieved in [4].

Another corollary to our main technical result underlying the gap theorem is a *direct* linear degree lower bound on proving primality. This improves recent work by [13]. We also give a linear Polynomial Calculus degree lower bound on the onto-Pigeonhole principle answering a question from [16].

[*] The International PhD Research School at BRICS, Aarhus, Denmark.

[†] Mathematics and Computer Science, Kent State University, Kent, Ohio 44242, USA Supported in part by NSF Grant CCR 94-09809.

I Introduction

I.1 Automatizable proof systems

An abstract proof system can be viewed as a non-deterministic tool for 'certifying' facts. Some proof systems are more efficient than others in the sense that they in general allow shorter certificates (proofs) than other proof systems do. However, there is often a price to be paid for the efficiency.

Consider, for example, the usual natural-deduction style propositional proof systems used in textbooks. These proof systems are generally more efficient than resolution style proof systems. The advantage of resolution based proof systems lies in their determinism i.e. in the fact that it is not much harder to find a proof than to check it. This is the main reason why automated reasoning and other tools for AI much more widely is based on resolution rather than on natural-deduction [14].

Within the last years various algebraic proof systems have been studied intensively. In particular the Nullstellensatz proof system (NS) and the Polynomial Calculus (PC) (also sometimes referred to as the Gröber basis calculus) have got a lot of attention. At first, NS was merely introduced as a theoretical tool used to settle an open problem in the field of proof complexity [3]. Later, after PC had also been introduced, it became clear that both these systems have many merits [5], [7], [16]. As a start NS and PC have a good relationship between the search complexity (the number of algorithmic steps required to find a proof) and the proof complexity (number of symbols in the proof). This relationship is essentially* polynomial for both systems. Thus both proof systems are essentially *automatizable* in the sense of [7]. On the other hand, both NS and PC are (theoretically) more efficient than resolution. In addition, it is clear that all the known standard refinements and strengthenings of propositional resolution (like Lock Resolution, Linear Resolution and Hyper-resolution [14]) have counterparts in NS and PC proof systems. Conversely, however, there are extensions of NS and PC which do not easily transfer to the setting of resolution as shown in [24].

The idea behind NS and PC is to translate the given proposition ψ_n into an equivalent system of polynomial equations $\bar{Q}(\bar{x}) = 0$ over some field $\mathbb{F}$. Typically, the number of variables of this polynomial system grows polynomially with n, but its degree remains constant independent of n (which is crucial for our purposes). The task of proving ψ_n can thus be rephrased as the task of showing that $\bar{Q}(\bar{x}) = 0$ does not have a 0/1-solution over $\mathbb{F}$. Now according a weak version of Hilbert's Nullstellensatz, this is equivalent to showing that the ideal generated by $\bar{Q} \cup I$ (where $I := \{x^2 - x, x \text{ variable}\}$) contains the constant polynomial 1. An NS-proof is a list of polynomials $\bar{P}$ such that $\sum P_i Q_i = 1$, where $P_i \in \bar{P}$ and $Q_i \in \bar{Q} \cup I$. The degree of the proof is the maximum degree of the wittnesing polynomials $\bar{P}$. Notice that the number of variables in the system $\bar{Q}$ is a trivial upper bound on the degree of the NS proof since the polynomials $x^2 - x$ for each variable x have been added to $\bar{Q}$. A PC-proof (as refutation proof) is a sequence (like in Hilbert style proofs)

*Assuming that the complexity is measured by as number of monomials in a polynomial of degree d, where d is the degree lower bound of polynomials $q_1, ..., q_u \equiv 1$, such that each polynomial q_j is either a $Q_i \in \bar{Q} \cup I$, is $q_j = \lambda_1 q_{j'} + \lambda_2 q_{j''}$, $j', j'' < j$, $\lambda_1, \lambda_2 \in \mathbb{F}$ or is $q_j = x q_{j'}$ where x is a variable and $j' < j$. A nice feature of PC is the fact that there is a natural algebraic characterisation of degree d PC-provability [7].

I.2 Closure under S_n and lifting degree lower bounds

The semantics of a natural decision problem is usually independent of its representation. Thus, under appropriate indexing of the inputs, the set of inputs is closed under action of the symmetrical group S_n (for a specific input-index-size n) and the input-output relation is closed under the action of S_n. We show that symmetries of this nature (together with uniformity constraints) have some interesting consequences in the context of NS-proofs and PC-proofs. More specifically, we consider NS and PC proofs whose corresponding polynomial systems are closed under the action of S_n on variable indices.

The main result of this paper shows that non-constant lower bounds on the degrees of NS proofs of universal second order statements ψ_n in fact imply linear lower bounds. This yields a new "gap" theorem for proof complexity. This gap theorem also holds for PC proofs and allows us immediately to solve a list of open problems concerning degree lower bounds. We get a linear degree (linear in the model size) lower bounds for various matching principles. This solves an open problem first posed in [3]. The bounds also improve the degree lower bounds of $\Omega(n^{\epsilon})$ achieved in [5] as well as the degree lower bounds achieved in [4].

Finding both NS and PC proofs essentially reduces to deciding whether two given systems of linear equations, $\bar{L}_1(\bar{x}) = 0$ and $\bar{L}_2(\bar{x}) = 0$, have the same set of solutions. The closure under S_n links this kind of problem to the representation theory of the symmetric group. Ajtai [1] was the first who were able to relate and solve specific problems in logic by uses of the representation theory of the symmetric group. During a number of papers Ajtai proved various pioneering results. In [13] Krajicek tried to apply Ajtai's results directly to achieve degree lower bounds. Krajicek were able to use Ajtai's approach to give a non-constant degree lower bound on PC proofs of the proposition which encodes the primality of a number. A brief outline of our approach was presented by the first author at an open problem session at a workshop at DIMACS May 1996. Our main technical result allows us to draw much stronger conclusions. As a comparison, our result *directly* gives a linear (in the input-index-size) degree lower bound for the same set of equations as in [13]. We present (with heavy reference to [22] and [23]) a non-constant PC degree lower bound on the onto-Pigeonhole principle. Application of our main result immediately allows us to achieve a linear PC degree lower thus answer a question from [16].

We describe here the flavour and intuition of the main technical result underlying the gap theorem.

For fixed natural numbers n and k we consider the vector space $V_{n,k}$ which is spanned by the basis $e_{(i_1, i_2, ..., i_k)}$ where $i_1, i_2, ..., i_k \in \{1, 2, ..., n\}$. The dimension of

$V_{n,k}$ is n^k i.e. a polynomial in n. The group S_n operates naturally on $V_{n,k}$ via the identity

$$\pi \sum a_{(i_1,i_2,...,i_k)} e_{(i_1,i_2,...,i_k)} := \sum a_{(i_1,i_2,...,i_k)} e_{(\pi(i_1),\pi(i_2),...,\pi(i_k))}.$$

In more technical terms $V_{n,k}$ is an $\mathbb{F}S_n$-module. A $\mathbb{F}S_n$-submodule $W \subseteq V_{n,k}$ is a linear subspace of $V_{n,k}$ which is closed under the above action of S_n.

The intuition behind our proof becomes clear in the case $\mathbb{F}$ is a field of characteristic 0 and begins with the following theorem.

Theorem 1 *For any $k \in \mathbb{N}$ there exists a finite collection of polynomials $p_1, p_2, ..., p_{\tau(k)} \in \mathbb{Q}[x]$ such that: For any $n \in \mathbb{N}$ and for any linear subspace $W \subseteq V_{n,k}$ closed under S_n there exists $j \in \{1, 2, ..., \tau(k)\}$ such that* $\dim W = p_j(n)$. *The function $\tau(k)$ grows rapidly: $\tau(1) = 4, \tau(2) = 40, \tau(3) \geq 1500$ and $\tau(4) \geq 20,000,000$.*

This theorem is an easy consequence of the highly developed structure theory for irreducible representations of the symmetric group (over fields of characteristic 0). See Section VI (under 2) for a proof of this result.

Now consider the problem of lifting degree lower bounds: Suppose that we are given a non-constant degree lower bound for NS-proofs of ψ_n. Consider the system $\bar{Q} \cup I$ of polynomial equations corresponding to ψ_n. If ψ_n is a Universal Second Order statement, then it turns out that the polynomial system is closed under S_n. For each fixed d consider the 2 linear systems that solve for the coefficients of polynomials $\bar{P}$ of degree at most d satisfying $\sum P_i Q_i = 0$, and $\sum P_i Q_i = C$, for some $C \in \mathbb{F}$ (could be 0), where $P_i \in \bar{P}$ and $Q_i \in \bar{Q} \cup I$; Let U_n and W_n be the corresponding solution spaces of these two linear systems. Notice that clearly $U_n \subseteq W_n$. In addition, since $\bar{Q}$ is closed under the action of S_n, U_n and W_n are also closed under S_n. Moreover, since the system $\bar{Q}$ has *constant degree independent of* n, it turns out that U_n and W_n are submodules of $V_{n,k(d)}$, where $k(d)$ is some linear function of d.

Since we are given a non-constant degree lower bound for NS proofs of ψ_n, it follows that for any given degree d, for infinitely many values of n we must have $U_n = W_n$. In order to lift this to a linear lower bound, we need to show that if there is any n where $U_n = W_n$, then there always must be a small n (say bounded by $2k(d)$) where $U_n = W_n$.

How to prove $U_n = W_n$ for small values of n? Now Theorem 1 comes into play. We know $U_n \subseteq W_n$ for all values of n. We also know from Theorem 1 that the dimensions of U_n and W_n are polynomial - except it may well be that the polynomial expressing $\dim U_n$ (resp. $\dim W_n$) may vary with n. *If* we could strengthen Theorem 1 to show that $\dim U_n$ (resp. $\dim W_n$) is expressed by the *same* polynomial for each value of $n \geq 2k(d)$, then we would have the desired consequence that $U_n = W_n$ for the appropriate small values of n because two polynomials agreeing for infinitely many values must be identical. We show a slightly weaker result (Theorem 12) that has the same desired consequence. (It remains a conjecture (see Section VI) to show that $\dim U_n$ (resp. $\dim W_n$) is expressed as a single polynomial beyond a small value of n.)

We note that our proof does *not* make heavy use of methods from representation theory. The representation theory methods that were used to prove Theorem 1 generally only work for fields of characteristic 0. For example, the proof uses the fact that well-studied modules called Specht modules (whose dimensions are directly calculable using the so-called Hook's formulae) are exactly all the irreducible modules over fields of characteristic 0. This fails to hold, however, over fields of finite characteristic. In fact, we can explicitly prove that the submodules – obtained from the statements ψ commonly studied for NS degree lower bounds – contain irreducible components that are not Specht modules. Thus the representation theory known from the characteristic 0 case is not particularly applicable to most frontier problems in lower bounds proofs. Solving these problems (along the lines just outlined) would be tied up with some of the deepest open problems in the modular representation theory of S_n. Some of these links are examined more closely in [9].

The paper is organised as follows. Section 2 gives the required background in logic and algebraic proof systems. It describes how to transform a logic statement into a system of polynomial equations and explains why these systems are naturally S_n-closed for Universal Second Order statements. Section 3 describes a (somewhat tedious) first transformation of the main problem of lifting NS degree lower bounds to a problem about the equivalence of S_n-closed linear systems. Section 4 views the transformed problem from Section 3 as a problem about $\mathbb{F}S_n$ modules and contains the proof of the main result. Section 5 gives other applications of the main result, in particular the lifting of PC degree lower bounds. Section 6 gives open problems of independent interest in the representation theory of S_n that are moreover intimately linked to complexity lower bounds.

II Background in Logic

Given a Π^1_1-sentence (i.e. a co-NP sentence) η. For $n \in \mathbb{N}$ let ψ_n denote the sentence ψ relativised to a universe with n elements. Suppose $a_1 < a_2 < ...$ is a sequence of natural numbers. We say $< \eta, a_j >$ defines a sequence of tautologies if each η_{a_j} is a tautology. We also refer to the Π^1_1-tautology η with the understanding that we always restrict η to numbers n for which η_n is a tautology.

Clearly there is a straight forward way of translating Π^1_1-sentences into polynomial equations. However for our purpose it is crucial that the resulting sequence of systems of polynomial equations have a degree which is bounded by some constant independent of the model size n. We achieve this by introducing suitable Skolem functions which ensure that the first order part becomes purely existential. Our translation allows us to convert any given Σ^1_1-sentence ψ (which we take as the negation of the given Π^1_1-tautology under scrutiny) into a finite system $\bar{Q} = 0$ of polynomial equations such that:

- For each n the $S_n$closure $\bar{Q}_n = 0$ of the polynomial equations $\bar{Q} = 0$ forms a system of polynomial equations in some polynomial ring $\mathbb{F}[x_e : e \in \cup_i(\{1, 2, ..., n\}^{r_i})]$.
- The system $\bar{Q}_n$ have a root if and only if ψ has a model of size n.
- The degree of the polynomials $\bar{Q}_n$ is bounded by a constant independent of n.

First let

$$\psi := \exists U_1 .... \exists U_k \forall i_1 \exists j_1 \forall i_2 \exists j_2 .... \forall i_k \exists j_k \psi'(i_1, i_2, ..., i_k, j_1, j_2, ..., j_k).$$

We eliminate all first order existential quantifiers by introducing Skolem functions and replacing ψ by

$$\tilde{\psi} := \exists U_1 .... \exists U_k \exists f_1 \exists ... \exists f_k \forall i_1 ... \forall i_k \psi'(i_1, .., i_k, f_1(i_1), f_2(i_1, i_2), ..., f_k(i_1, ..., i_k)).$$

Notice that different Skolemisations in general might lead to different polynomial equations. In general we allow ψ to contain second order existential quantifiers ranging over sets, relations (of any arity) as well as functions (of any arity). We assume we have eliminated all first order existential quantifiers.

For each n we translate $\tilde{\psi}$ into polynomial equations as follows: First we introduce a collection of Boolean variables: For each r-ary relation symbol $R(i_1, i_2, ..., i_r)$ we introduce a variable x_e^R for each $e \in \{1, 2, ..., n\}^r$. For each function symbol f of arity r introduce variables x_e^f indexed by points in $\{1, 2, ..., n\}^{r+1}$.

Now we start specifying the collection of polynomials: in $\bar{Q}_n$.

- **(a)** For each variable z_e we define a polynomial

  $$Q_e^z :\equiv \ z_e^2 - z_e$$

  These polynomials ensure all common solutions to the polynomials become $0, 1$-solutions (see [3]).

- **(b)** For each function symbol f and for each $(i_1, i_2, ..., i_r) \in \{1, 2, ..., n\}^r$ we define a polynomial

  $$Q_{i_1, i_2, ..., i_r}^{f, tot} :\equiv \Sigma_j \ x_{i_1, i_2, ..., i_r, j}^f - 1$$

  These polynomials encodes the fact that f is a total function.

- (c) For each function symbol f and for each $(i_1, i_2, ..., i_r, i_{r+1}, i_{r+2}) \in \{1, 2, ..., n\}^{r+2}$ where $i_{r+1} \neq i_{i+2}$ we define a polynomial

  $$Q_{i_1, i_2, ..., i_r, i_{r+1}, i_{r+2}}^{f, fun} :\equiv x_{i_1, i_2, ..., i_r, i_{r+1}}^f \, x_{i_1, i_2, ..., i_r, i_{r+2}}^f .$$

  The polynomials encode the fact that f takes at most one function value.

Suppose that the matrix $\psi'(i_1, i_2, ..., i_k; i_{k+1}, i_{k+2}, ..., i_{2k})$ contain the relation symbols $R_1, R_2, ..., R_t$ of arity $r(1), r(2), ..., r(t)$. Then the matrix can be written as

$$\wedge_\alpha (\vee_{\beta \in I_\alpha} \ R_{\tau(\beta)}(i_{\eta_1(\beta)}, i_{\eta_2(\beta)}, \ldots, i_{\eta_{r(\tau(\beta))}(\beta)}) \vee$$

$$\vee_{\gamma \in J_\alpha} \ \neg R_{\tau(\gamma)}(i_{\eta_1(\gamma)}, i_{\eta_2(\gamma)}, \ldots, i_{\eta_r(\tau(\gamma))(\gamma)}))$$

where $\tau(\beta), \tau(\gamma) \in \{1, 2, ..., t\}, \eta_j(\beta), \eta_j(\gamma) \in \{i_1, i_2, ..., i_{2k}\}$. The index α run through a finite set and each set I_α and J_α are finite. Now clearly we can replace each $R_j(i_{\eta_1(\alpha,\beta)}, ..., i_{\eta_{r(\tau(\beta))}(\beta)})$ by the polynomial $p_\beta := x_{j,(i_{\eta_1(\beta)}, ..., i_{\eta_{r(\tau(\beta))}(\beta)})} - 1$ and each

$\neg R_{\tau(\gamma)}(i_{\eta_1(\gamma)}, i_{\eta_2(\gamma)}, ..., i_{\eta_r(\tau(\gamma))(\gamma)})$ by the polynomial $p_\gamma := x_{j,(i_{\eta_1(\gamma)},...,i_{\eta_{r(\tau(\gamma))}(\gamma)})}$. For each α replace the corresponding disjunction by the polynomial

$$Q_\alpha := 1 - \Pi_{\beta \in I_\alpha}(1 - p_\beta)\Pi_{\gamma \in J_\alpha}(1 - p_\gamma).$$

Notice each model $< U_1, U_2, ..., U_k, f_1, f_2, ..f_k >$ of ψ' induces a truth value assignment to the variables by letting $x_{j,(i_{\eta_1(\beta)},...,i_{\eta_{r(\tau(\beta))}(\beta)})} = 1$ if
$R_j(i_{\eta_1(\beta)}, ..., i_{\eta_r(\tau(\beta))(\beta)})$ and by letting $x_{j,(i_{\eta_1(\beta)},...,i_{\eta_{r(\tau(\beta))}(\beta)})} = 0$ otherwise.

Now it is straight forward (using the polynomials constructed under (a), (b) and (c)) to produce a system of polynomial equations $\bar{Q}$ which have a solution if and only if ψ have a model of size n.

Notice that each polynomial Q_α has degree bounded by $|I_\alpha| + |J_\alpha|$. Thus the degree of the polynomials in $\bar{Q}$ (also including the one constructed under (a),(b) and (c)) is bounded by a constant independent of n. Notice also that the system of polynomials $\bar{Q}$ is closed under S_n.

Clearly this translation works for arbitrary Universal Second Order propositions. Our approach show that every computational or deductive problem can be translated into an equivalent equational problem. Lot of extensive work have already been done on purely equational theories [15]. We would emphasise that equational reasoning is one of the few areas where the machines already are significantly superior to ordinary mathematicians. Our translation into equational theories introduce a lot of additional computational structure. We feel that these rich algebraic features makes our approach very promising. Clearly we can express any decision problem (in a feasible manner) as a problem concerning the existence of a solution to finitely generated (under S_n) systems of polynomial equations. Each solution $\bar{a}$ of the polynomial equations $\bar{Q}_n(\bar{a})$ uniquely corresponds to a model of size n of the proposition ψ. Such decision problems are of course undecidable if we are also searching for an appropriate n, while it is NEXPTIME-hard (i.e. the same complexity as the spectrum problem for first order logic) if n is given as part of the input [8]. This last observation easily show (reducing finding PC proofs to that of solving linear equations) that:

Theorem 2 *If* EXPTIME $\neq$ NEXPTIME *then there must be systems of polynomial equations $\bar{Q}_n(\bar{a})$ which do not have linear degree PC-proofs.*

The number of solutions to $\bar{Q}_n$ equals the number of models of the appropriate skolemisation of $\tilde{\psi}$. The closure under S_n ensures that different solutions (not isomorphic under S_n) corresponds to non-isomorphic models. Actually the number of non-isomorphic models $M \models \psi_n$ is negatively related to the size of the ideal $I_{\psi,n}$ generated by the polynomials in $\bar{Q}$. Knowledge of $I_{\psi,n}$ allows us uniquely to determine all models of ψ_n, and clearly there is a 1-1 correspondence between models of ψ_n and points on the algebraic variety defined by $I_{\psi,n}$. Notice that all ideals $I_{\psi,n}$ are closed under S_n and therefore it is natural to expect rich mathematical structures to follow from this symmetry. And indeed this will be borne out by the remainder of our discussion.

III Problem Transformation and the Main Result

Here we state the main problem and result about Nullstellensatz degree lower bounds, and transform it into a problem about S_n-closed, uniformly generated sequences of linear equation systems.

III.1 Notation

For each $e \in \{1 \dots n\}^r$ we introduce a variable x_e. We consider the ring $\mathbb{F}[x_e, e \in \{1 \dots n\}^r]$ of polynomials over some field $\mathbb{F}$. We display polynomials $P(x) \in \mathbb{F}[x_e, e \in \{1 \dots n\}^r]$ of degree d_P in a suitable **multi index** notation: x_E^α simply denotes a monomial $x_{e^1}^{\alpha_1} x_{e^2}^{\alpha_2} \dots x_{e^d}^{\alpha_d}$ where E is an *ordered* list of length at most $d \leq d_P$, of elements $e^j \in \{1, \dots, n\}^r$; and $\alpha \in \{1, \dots, d_P\}^{|E|}$ is a corresponding list of nonzero powers satisfying $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_d$ and $\sum_{e^j \in E} \alpha_d \leq d_P$. The constant term is denoted $x_\emptyset^0$.

Actually we need to consider a generalisation of the ring $\mathbb{F}[x_e, e \in \{1 \dots n\}^r]$. We denote this polynomial ring by $\mathbb{F}[x, n, r]$. The **ring parameters** of this polynomial ring are the field characteristic $q_\mathbb{F}$ and r. In $\mathbb{F}[x, n, r]$ we include other types of primitive terms besides monomials. In these terms, we permit the entries in e^j to be indeterminates which are then summed over $\{1, \dots, n\}$. More precisely, we include primitive terms that are generalisations of monomials of the following form. We start with a term $x_E^\alpha = x_{e^1}^{\alpha_1} x_{e^2}^{\alpha_2} \dots x_{e^d}^{\alpha_d}$ as before, but now we permit the e^j to additionally take values among a set of named indeterminates, under the condition that the different indeterminates that appear in any term x_E^α are all *distinct.* Note that the values in $\{1, \dots, n\}$ that appear in the e^j's i.e, the determinates, are not forced to be distinct and could contain repetitions.

Let $\{*^1, *^2, \dots *^m\}$ denote the set of indeterminates that appear among the indices of x_E^α. As observed before, these are all distinct, but there could be repetitions of indeterminates between different x_E^α's. The primitive terms are sums of the form $\sum_{*^1=1}^{n} \sum_{*^2=1}^{n} \dots \sum_{*^m=1}^{n} x_E^\alpha$, which we shall simply refer to, unambiguously, as x_E^α.

The **dimension** of a term is the number of summation signs that appear in it. For example, a term with no summation signs (a standard monomial) is called a **point** term, a term with one summation a **line**, with two summations a **plane**, etc.

In addition to the degree $d_{E,\alpha} = \sum_{e^i \in E} \alpha_i$, and the dimension $t_{E,\alpha}$ of a term x_E^α, the other parameter of importance is the set of *distinct* values in $\{1, \dots, n\}$ (determinates) that appear among all of the $e \in E$. We call this set, listed in, say ascending order, as the *support* of the term x_E^α, denote it $s_{E,\alpha}$. Its size is called the **support size** and denoted $l_{E,\alpha}$. The support size, degree and dimension are called the **defining parameters** of the term.

A polynomial $P(x) \in \mathbb{F}[x,n,r]$ is then written as

$$\sum_{E} \sum_{\alpha \in \{1 \dots d_P\}^{|E|}} c_E^{\alpha} \sum_{*^1=1}^{n} \cdots \sum_{*^{m_{E,\alpha}}=1}^{n} x_E^{\alpha},$$

where $c_E^{\alpha} \in \mathbb{F}$, and $m_{E,\alpha}$ is the number of indeterminates appearing in x_E^{α}. The support of a polynomial is the *union* (listed, say, in ascending order) of the supports of its terms and is denoted s_P with the support size denoted l_P. The defining parameters of a *set* of polynomials are the *maximum* degree and the *maximum* of the support sizes of its elements.

Example: For each $e := (i,j),\ i,j \in \{1,2,...,n\} \cup \{*\}$ introduce a variable $x_{(i,j)}$. Consider the polynomials $Q^1 := x_{(1,2)}^2 - x_{(1,2)}$, $Q^2 := x_{(1,*)}$ and $Q^3 := x_{(1,2)} - x_{(2,1)}$. For a fixed field $\mathbb{F}$ these 3 polynomials belongs to $\mathbb{F}[x,n,2]$. Note, for example, that the coefficients c_E^{α} here are: $c_{(1,2)}^{1,(1)}$ in the polynomial Q^1 is -1, $c_{(1,2)}^{1,(2)}$ in the polynomial Q^1 is 1, and $c_{(1,*)}^{2,(1)}$ in the polynomial Q^2 is 1.

The polynomial Q^1 is interpreted as $\sum_{*} x_{(1,*)}$. The closure of Q^1, Q^2 and Q^3 under S_n gives the following system of polynomials:

$x_{(i,j)}^2 - x_{(i,j)}$ for $i,j \in \{1,2,...,n\}$

$\sum_{j} x_{(i,j)} - 1$ for each $i \in \{1,2,...,n\}$

$x_{(i,j)} - x_{(j,i)}$ for $i,j \in \{1,2,...,n\}$.

A common solution to these polynomials can be viewed as an undirected graph of n-vertices where each out-degree is 1 modulo $q_{\mathbb{F}}$. Thus the polynomials only have a common root for n even. ♣

In general we actually need to consider polynomial expressions which are more general than those in $\mathbb{F}[x,n,r]$. In general we consider polynomials expressions in $\mathbb{F}[x^1, x^2, x^3, \dots, n, r]$, where x^1, x^2 are different **types** of variables. These polynomials consist of terms of the form $x_E^{1,\alpha} x_F^{2,\beta}$ etc. The degree of a term still denotes the total degree, i.e, the sum of all the degrees that appear in a term, and the support of a term includes the distinct indices that appear in the subscripts over *all* variable types that occur in the term. However, for convenience while explaining the notation and basic facts, restrict ourselves to polynomials in $\mathbb{F}[x,n,r]$ unless otherwise specified. Analogous facts apply to the more general polynomials with many variable types.

Notice that terms and polynomials in $\mathbb{F}[x,n,r]$ can be viewed as a *sequence* (in n) of polynomials. But the sequence is very simple with defining parameters independent of n. Really such a sequence should be subscripted by n, but we omit the subscript, and continue to refer to the elements of $\mathbb{F}[x,n,r]$ simply as polynomials.

The following fact describes simple properties of terms.

Fact 3 *The product of two terms $x_E^{\alpha}\ x_F^{\beta}$ in $\mathbb{F}[x,n,r]$ is obtained naturally as follows (an analogous process applies to terms containing many variable types). First, rename the indeterminates that appear in F, so that they are all distinct from the indeterminates that appear in E. The variables in both terms, with subscripts in*

$E \oplus F$ (symmetric difference) are retained in the product, together with their powers and summations over indeterminates. For variable subscripts $e^i \in E \cap F$ (which do not contain any indeterminates), the corresponding from the two terms are replaced by $x_{e^i}^{\alpha_i+\beta_i}$ in the product. Next, all the variables in the product are arranged so that their powers are in ascending order.

Primitive term (sequence)s T_n are asymptotically linearly independent, in the sense that no primitive term can be obtained from other primitive terms as a fixed linear combination (independent of n).

We say a set $\bar{Q}$ of polynomials in $\mathbb{F}[x,n,r]$ an S_m-**closed** set, for a fixed m, if for all permutations in $\pi \in S_m$, i.e, permutations applied to $\{1,\ldots,m\}$,

$$P \in \bar{Q} \iff \pi(P) \in \bar{Q}$$

where π acts on the polynomial

$$P(x) = \sum_E \sum_{\alpha \in \{1 \ldots d_P\}^{|E|}} c_E^\alpha x_E^\alpha$$

by its natural action on the elements in $\{1,\ldots,n\}$ that constitute the indices e_j in the lists E. The indeterminates appearing in the e_j and the summations over these indeterminates remain untouched. This is well-defined also for $n < m$.

For sets $\bar{Q}$ of polynomials that have more than one variable type, we say the set is S_m-closed if it is closed with respect to the action of S_m on the subscript indices of *each* variable type.

We say a set *sequence* $\bar{P}_n$ is S_n-closed, if for *every* m, the element $\bar{P}_m$ of the sequence is S_m-closed. Otherwise, the sets in the sequence might vary non-uniformly. We say an S_n-closed set sequence $\bar{Q}_n$ is **uniformly generated** in n if it is generated for all n, starting with a fixed set of **generating polynomials** in $\mathbb{F}[x,n,r]$, say $G = \{G^1,\ldots,G^{m_{\bar{Q}}}\}$, whose degree is bounded by $d_{\bar{Q}}$, and support sizes are bounded by $l_{\bar{Q}}$. I.e, we form the S_n-closed sets $\bar{Q}_n$ for any n, by letting the permutations in S_n act on the elements of G in the above described manner. As in the case of the elements of $\mathbb{F}[x,n,r]$, if the S_n-closed sets are uniformly generated, we omit the word "sequence" when referring to them. Notice that we still retain the subscript n in $\bar{Q}_n$ to distinguish from a *fixed* set of polynomials in $\mathbb{F}[x,n,r]$, which may even be S_m closed for some fixed m. Note that a fixed S_m-closed set of polynomials in $\mathbb{F}[x,n,r]$ is also well-defined for any n, but its size, for example, does not change with n; whereas the size of the sets in an S_n-closed uniformly generated set $\bar{Q}_n$ do change with n.

The polynomials in an S_n-closed, uniformly generated set $\bar{Q}_n$ can be indexed using elements of $\{1,\ldots,n\}^{l_{\bar{Q}}} \times \{1,\ldots,m_{\bar{Q}}\}$ for $d \leq d_{\bar{Q}}$ using the following scheme. Index a generating polynomial G^i not only by $i \in \{1,\ldots,m_{\bar{Q}}\}$ but also by the elements in $\{1,\ldots,n\}$ in its support s_{G^i}, listed in some fixed, say ascending, order. We will refer to this list as s_{G^i} as well. Any polynomial Q in $\bar{Q}_n$ is, without loss, obtained by the action of a permutation π_Q in S_n on a unique generating polynomial, say G^{i_Q}. This gives a natural method of indexing Q namely by i_Q and the list $\pi_Q(s_{G^{i_Q}})$, which is nothing but the support s_Q of Q listed in ascending order. So we think of the polynomial Q as $Q^{i_Q}_{s_Q}$. Note that Q's generating polynomial G^{i_Q} is indexed with the same superscript i_Q, but a possibly different subscript. I.e we think of G^{i_Q} as $Q^{i_Q}_{s_{G^{i_Q}}}$ where $s_{G^{i_Q}}$ is the same as $\pi_Q^{-1}(s_Q)$.

For set sequences $\bar{Q}_n$ consisting of polynomials with many variable types, the definitions of S_n-closed, uniformly generated, and the indexing scheme are the natural extensions of those described above, to each variable type.

An important thing to notice (even when there are many variable types) is that defining parameters of an S_n-closed, uniformly generated set $\bar{Q}_n$ are independent of n. Clearly, the degree bound $d_{\bar{Q}}$, and the support size bound $l_{\bar{Q}}$ apply to all the polynomials in $\bar{Q}_n$, independent of n, and therefore the the *size* of the names or index ascribed to each polynomial in $\bar{Q}_n$ (by the above described indexing scheme) is also independent of n.

III.2 Main Results

Clearly, S_n-closed, uniformly generated sets $\bar{Q}_n$ of polynomials are special. But they occur commonly, as shown in Section II. For such sets we prove two results about lifting non-constant degree lower bounds - on the the Nullstellensatz refutations (of common zeroes) - into linear lower bounds.

First, we consider the Nullstellensatz witnessing polynomials in a sequence $\bar{P}_n$ of lists, each list in the sequence consisting of polynomials in $\mathbb{F}[x, n, r]$: these lists show that the ideal generated by $\bar{Q}_n$ contains the constant polynomial. I.e, $\sum_{Q^i_s \in \bar{Q}_n} Q^i_s P^i_s = 1$. This is same as saying that the polynomials in $\bar{Q}_n$ do not have a common zero.

Note 4 *We assume through out this section that the set $\bar{Q}_n$ and the corresponding witnessing polynomials $\bar{P}_n$ consist of polynomials in $\mathbb{F}[x, n, r]$ of a single variable type. It can be easily verified that results extend to many variable types, as well. Note that the lists in the sequence $\bar{P}_n$ depend on $\bar{Q}_n$, but unlike $\bar{Q}_n$, the lists in $\bar{P}_n$ need not be S_n-closed, and even if they are, they need not be uniformly generated in n. However, for a fixed n, the indexing of the polynomials in $\bar{Q}_n$ (described in the previous subsection) transfers to a natural indexing on the polynomials in $\bar{P}_n$ as well.*

We are interested in lower bounds on the degree of the set of witnessing polynomials $\bar{P}_n$. We treat as constants the defining parameters of $\bar{Q}_n$, for example, the degree $d_{\bar{Q}}$, the support size $l_{\bar{Q}}$, and the ring parameters of $\mathbb{F}[x, n, r]$ namely r and the field characteristic $q_{\mathbb{F}}$; and we are interested in how the degree lower bounds for $\bar{P}_n$ depend on n. In particular we are interested in specific cases of S_n-closed, uniformly generated sets $\bar{Q}_n$ for which it has been shown that the corresponding degree $d_{\bar{P}_n}$ grows, perhaps very slowly, with n. Our aim is to show that *any* positive dependence of this degree on n automatically implies a *linear* dependence on n. More precisely, we show the following.

Theorem 5 *Assume we are given an uniformly generated set $\bar{Q}_n$, of polynomials in $\mathbb{F}[x, n, r]$. Assume $\bar{Q}_n$ is closed under S_n. Let $n(d)$ be a number so that there is no* *polynomials of degree d which witness the fact that the system $\bar{Q}_{n(d)}$ does not have a common zero.*

Then actually there is no witnessing polynomials of degree d which witness the that the system $\bar{Q}_n$ does not have a common zero for each $n \geq \max\{d_{\bar{Q}}r + 3l_{\bar{Q}} + 4dr, (7 + q_{\mathbb{F}}^2)(l_{\bar{Q}} + dr) - q_{\mathbb{F}}\}$ in the same residue class (modulo $q_{\mathbb{F}}^m$, $m := \mathrm{int}(\frac{\log(l_{\bar{Q}}+dr)+1}{\log(q_{\mathbb{F}})} + 1)$) as $n(d)$ (m is the smallest integer such that $q_{\mathbb{F}}^m \geq l_{\bar{Q}} + dr$.

Corollary 6 *Let ψ_n be a sentence which does not have constant degree Nullstellensatz refutation proofs for infinitely many values of n. Then for some n there is no degree $d \leq \min\{\frac{n+q_{\mathbb{F}}-(7+q_{\mathbb{F}}^2)l_{\bar{Q}}}{(7+q_{\mathbb{F}}^2)r}, \frac{n-d_{\bar{Q}}r-3l_{\bar{Q}}}{4r}\}$ Nullstellensatz refutation proof of ψ_n. The entries $r, q_{\mathbb{F}}$ and $l_{\bar{Q}}$ are constants and thus are independent of n and d.*

The proof of Theorem 5 consists of 2 parts. The first part is given by the following lemma.

Lemma 7 *Given an S_n-closed, uniformly generated set $\bar{Q}_n$, of polynomials in $\mathbb{F}[x,n,r]$, and any d, one can construct an S_n-closed, uniformly generated set $\bar{\Lambda}_{\bar{Q},n}$ of linear polynomials and a linear polynomial $T_{\bar{Q}}$ (depending on d), such that the following holds. Sets of degree d Nullstellensatz witnessing polynomials cannot show the nonexistence of a common zero for $\bar{Q}_n$, for $n \in N_d$, where N_d is any subset of $\mathbb{N}$ which could depend on d, if and only if the linear span (over $\mathbb{F}$) of $\bar{\Lambda}_{\bar{Q},n}$ includes a specific linear polynomial $T_{\bar{Q}}$ (the 1-polynomial) for $n \in N_d$.*

The polynomials in $\bar{\Lambda}_{\bar{Q},n}$ as well as $T_{\bar{Q}}$ contain many variable types and live in

$$\mathbb{F}[\lambda^{i,\alpha,\omega} : 1 \leq i \leq m_{\bar{Q}}, \alpha, \omega \subseteq \{1,\ldots,dr\}; n, dr + l_{\bar{Q}}],$$

where $m_{\bar{Q}}$ is the size of the (minimal) set of generating polynomials of $\bar{Q}_n$, and α runs over multi-index powers of any legal term of $\mathbb{F}[x,n,r]$ of degree at most $(d + d_{\bar{Q}})$, and $l_{\bar{Q}}$ is the bound on the support size of $\bar{Q}_n$.

The defining parameters of $\bar{\Lambda}_{\bar{Q},n}$ are: degree bounded by 1, and support size bounded by $(d + d_{\bar{Q}})r$). The polynomial $T_{\bar{Q}}$ has defining parameters: degree bounded by 1, and support-size 0.

Thus their defining parameters are independent of n, depending only on the defining parameters of $\bar{Q}_n$, and at most linearly on the degree bound d allowed for the witnessing polynomials.

Proof.

The idea of the proof is the following. It is easy to see that in order to solve for the coefficients of polynomials $P_j \in \mathbb{F}[x,n,r]$ of degree d that *do* satisfy $\sum\limits_j Q_jP_j = 1$, for a given, *fixed* set $\bar{Q}$ consisting of $Q_j \in \mathbb{F}[x,n,r]$, of degree bounded by $d_{\bar{Q}}$, one can instead solve a linear system whose variables are the coefficients of the desired P_j. All but one equation in this linear system correspond to non-constant terms in the sum $\sum\limits_j Q_jP_j = 1$, and each equation is homogeneous and asserts that the coefficient of a term in this sum is 0; these terms have degree at most $d + d_{\bar{Q}}$, which, together with the number of polynomials $Q_j \in \bar{Q}$, influences the defining parameters (such as support-size) of each of the corresponding linear equations. Let us denote this set of homogeneous linear equations as $\bar{\Lambda}_{\bar{Q}} = 0$. In addition to these homogeneous linear equations corresponding to non-constant terms, there is a *single* non-homogeneous linear equation corresponding to the constant term in the sum, $\sum_j Q_j P_j = 1$, which asserts that the constant term, say $T_{\bar{Q}}$ in the above sum is 1.

Therefore, in order to show that for any d, *no* polynomials P_j of degree bounded by d exist in $\mathbb{F}[x, n, r]$ that satisfy $\sum_j Q_j P_j = 1$, for $n \in N_d$, it is necessary and sufficient to show that for each d, the corresponding *homogeneous* equations in $\bar{\Lambda}_{\bar{Q}}$ in fact imply that $T_{\bar{Q}} = 0$, for $n \in N_d$ (it is well defined to talk about $\bar{Q}$, $\bar{\Lambda}_{\bar{Q}}$ etc. for varying n, since these sets consist of objects in $\mathbb{F}[x^1, x^2, \ldots, n, r]$ which are well defined for varying n). The last statement is equivalent to saying that for each d, the corresponding linear span of the linear polynomials in $\bar{\Lambda}_{\bar{Q}}$ in fact includes the polynomial T_Q, for $n \in N_d$. Moreover, as mentioned before, the defining parameters of $\bar{\Lambda}_{\bar{Q}}$ and T_Q depend only on d, $d_{\bar{Q}}$ and the number of polynomials in $\bar{Q}$.

One could extend the above argument to *sequences* of sets $\bar{Q}_n$ by which one can rephrase the result explained above, and show the following. For each d, there exist a sequence of sets of linear polynomials $\bar{\Lambda}_{\bar{Q},n}$ and a sequence of polynomials $T_{\bar{Q},n}$ such that there are no polynomials P_Q of degree bounded by d in $\mathbb{F}[x, n, r]$ that satisfy $\sum_{Q \in \bar{Q}_n} Q P_Q = 1$, for $n \in N_d$, if and only if the linear span of linear polynomials in $\bar{\Lambda}_{\bar{Q},n}$ in fact includes $T_{\bar{Q},n}$, for $n \in N_d$.

The *catch* is that while the defining parameters of $\bar{\Lambda}_{\bar{Q},n}$ and $T_{\bar{Q},n}$ depend only on d, $d_{\bar{Q}_n}$ and the number of polynomials in $\bar{Q}_n$, the latter two quantities could well depend on n.

In fact, even if $\bar{Q}_n$ is generated in a uniform way, while the degree $d_{\bar{Q}_n}$ stays independent of n, the number of polynomials in $\bar{Q}_n$ could grow tremendously with n, and therefore the defining parameters of $\bar{\Lambda}_{\bar{Q},n}$ and $T_{\bar{Q},n}$ could grow with n. Moreover, it is not clear that $\bar{\Lambda}_{\bar{Q},n}$ is generated in a uniform manner, just by the fact that $\bar{Q}_n$ is.

The lemma states, however, that in the case that $\bar{Q}_n$ is S_n-closed and uniformly generated, $\bar{\Lambda}_{\bar{Q},n}$ is also S_n-closed and uniformly generated, and its defining parameters do *not* depend on n, depend only linearly on d and moreover one can make do with a single polynomial $T_{\bar{Q}}$ instead of a sequence $T_{\bar{Q},n}$.

Therefore, the idea in the previous paragraphs for constructing $\bar{\Lambda}_{\bar{Q},n}$ and $T_{\bar{Q}}$ has to be refined and analyzed carefully for the case of $\bar{Q}_n$ that are S_n-closed and uniformly generated.

Fix d. We use the indexing scheme discussed in the previous subsection, for polynomials in an S_n-closed, uniformly generated set.

Consider solving for the coefficients of the multiplying polynomials $P^i_s \in \mathbb{F}[x, n, r]$ of degree d which *do* satisfy

$$\sum_{Q^i_s \in \bar{Q}_n} Q^i_s P^i_s = 1. \qquad (I)$$

Name the (variable) coefficient in P^i_s of the term $x^{\alpha}_{\bar{E}}$, as $\lambda^{i,\alpha}_{E,s}$ (note that this λ should be viewed as a *single* variable, i.e, a *linear* term in $\mathbb{F}[\lambda^{i,\alpha}, n, dr+l_{\bar{Q}}]$ and not a high degree term, say in $\mathbb{F}[\lambda, n, r]$, in multiindex notation). In addition, denote the (constant) coefficient of x_{E}^{α} in Q_s^i as $q_{E,s}^{i,\alpha}$.

As mentioned earlier we can now solve a linear system whose variables are the λ's. All but one equation in this linear system are homogeneous and assert that each nonconstant term x_E^α in the sum (I) has a 0 coefficient. Each nonconstant term x_E^α has degree $\sum_{e^i \in E} \alpha_i \leq d + d_{\bar{Q}}$. Let Π_E^α denote the set of all pairs $([E^1, \alpha^1], [E^2, \alpha^2])$ such that the product of $x_{E^1}^{\alpha^1}$ and $x_{E^2}^{\alpha^2}$ is x_E^α, (see Fact 3 on how to obtain products of terms), where the first element of the pair has degree at most d. The coefficient of x_E^α term in (I) can now be written as the following linear polynomial in the λ's.

$$\sum_i \sum_s \sum_{([E^1,\alpha^1],[E^2,\alpha^2]) \in \Pi_E^\alpha} \lambda_{E^1,s}^{i,\alpha^1} q_{E^2,s}^{i,\alpha^2}. \qquad (II)$$

Note that the above linear polynomial has several variable types, λ^{i,α^1}, and it is not quite a "legal" polynomial. There are two issues to be dealt with.

- The subscripts E^1 may contain "original" indeterminates (which are *not summed over* in (II)), because $\lambda_{E^1,s}^{i,\alpha^1}$ is the coefficient of a term $x_{E^1}^{\alpha^1}$ (of the polynomial P_s^i) which contains indeterminates and summations.
- The length of the subscripts E^1 in $\lambda_{E^1,s}^{i,\alpha^1}$, may vary between 0 and dr. Moreover, the support sizes, i.e, the length of s may vary between 1 and $l_{\bar{Q}}$.

In order to homogenize the subscipt lengths, we introduce $dr - |E^1|$ distinct indeterminates into E^1, to get $\bar{E}^1$ of length dr, and similarly introduce $l_{\bar{Q}} - |s|$ distinct indeterminates into s to get $\bar{s}$ of length $l_{\bar{Q}}$. Now we think of $\lambda_{E^1,s}^{i,\alpha^1}$ unambiguously as $\lambda_{\bar{E}^1,\bar{s}}^{i,\alpha^1}$, which includes sumations over these indeterminates. In order to deal with the indeterminates in $\bar{E}^1$ which are not summed over in (II), we simply create several more variable types, one for each subset of $\{1, \ldots, dr\}$. The subset $\omega_{\bar{E}^1}$ denotes those indeterminates in the subscript $\bar{E}^1$ which are "original" indeterminates that are not summed over in (II). Once the variable types have been thus distinguished, we sum over the original indeterminates as well. (See Example 8). Now we think of $\lambda_{\bar{E}^1,\bar{s}}^{i,\alpha^1,\omega_{\bar{E}^1}}$, unambiguously as including the summations over the indeterminates picked out by $\omega_{\bar{E}^1}$ as well.

The collection of all such linear polynomials corresponding to each term x_E^α of degree at most $d + d_{\bar{Q}}$ is denoted $\bar{\Lambda}_{\bar{Q},n}$. This (set) sequence is clearly S_n-closed.

To show that it is uniformly generated, we collect several terms in each linear polynomial as in (II) and replace them by terms that contain summation over indeterminates. More precisely, observe that the sum in (II) can be rewritten as

$$\sum_i \sum_{([E^1,\alpha^1],[E^2,\alpha^2]) \in \Pi_E^\alpha} \left(\sum_s q_{E^2,s}^{i,\alpha^2} \lambda_{\bar{E}^1,\bar{s}}^{i,\alpha^1,\omega_{\bar{E}^1}} \right). \qquad (III)$$

Since $\bar{Q}_n$ is uniformly generated, for fixed values of i, E^1, E^2, α^1 and α^2, the summation over s runs through all permutations π of some sublist s^i of $\{1, \ldots, n\}$, of constant size independent of n, which is the support of a particular generator G^i of $\bar{Q}_n$. As described earlier, $\bar{s}^i$ denotes s^i with indeterminates added to homogenise its length. The value of $q^{i,\alpha^2}_{E^2,s}$ thus remains constant for all s. Thus the sum in (III) can be written as

$$\sum_i \sum_{([E^1,\alpha^1],[E^2,\alpha^2])\in\Pi^{\alpha}_{\bar{E}}} q^{i,\alpha^2}_{E^2,s^i}\Big(\sum_{\pi} \lambda^{i,\alpha^1,\omega_{\bar{E}^1}}_{\bar{E}^1,\pi(\bar{s}^i)}\Big). \qquad (IV)$$

The summation over all permutations of s^i is itself not a "legal" term in $\mathbb{F}[\lambda^{i,\alpha^1,\omega_{\bar{E}^1}}, n, (d+d_{\bar{Q}})r + l_{\bar{Q}}]$ (fixed i, α^1, and $\omega_{\bar{E}^1}$ result in a single variable type); however it can be rewritten, using Lemma 9, (a form of inclusion-exclusion), as a linear combination of legal terms which contain all possible subsets of the $|S|$ distinct indeterminates, *all* summed from 1 to n. Once the linear polynomial in (IV) has been thus rewritten, it is clear that its support is obtained entirely from the subscripts E^1 (each of size at most dr) of the variables λ, since the remaining subscripts become indeterminates. Thus the support of the polynomial in (IV) is contained in $s_{E,\alpha}$, i.e, the support of the term $x^{\alpha}_{\bar{E}}$ of degree at most $d+d_{\bar{Q}}$. Thus the support size is at most $(d+d_{\bar{Q}})r$ which is independent of n.

Now consider the collection of those linear polynomials as in (IV), which correspond to (the coefficients of) those non-constant terms $x^{\alpha}_{\bar{E}}$ in (I), of degree at most $d+d_{\bar{Q}}$, whose support is restricted to $\{1,\ldots,(d+d_{\bar{Q}})r\}$. Clearly this collection is a generating set that generates all of (and exactly) $\bar{\Lambda}_{\bar{Q},n}$ under the action of S_n, thereby showing that $\bar{\Lambda}_{\bar{Q},n}$ is not only S_n-closed, but also uniformly generated, with defining parameters independent of n (degree obviously bounded by 1, and and support size bounded by $(d+d_{\bar{Q}})r$).

The linear polynomial $T_{\bar{Q}}$ i.e, the left hand side of the *single* non-homogeneous equation corresponding to the constant term in the sum (I), is obtained by a similar process, and its defining parameters are degree bounded by 1, and support-size 0.

Finally, it follows from the construction that the polynomials in $\bar{\Lambda}_{\bar{Q},n}$ as well as $T_{\bar{Q}}$ are in in

$$\mathbb{F}[\lambda^{i,\alpha,\omega} : 1 \le i \le m_{\bar{Q}}, \alpha, \omega \subseteq \{1,\ldots,dr\}; n, dr + l_{\bar{Q}}],$$

where $m_{\bar{Q}}$ is the size of the set of generating polynomials of $\bar{Q}_n$, and α runs over multi-index powers of any legal term of degree at most $(d+d_{\bar{Q}})$, and $l_{\bar{Q}}$ is the bound on the support size of $\bar{Q}_n$. It follows also from the construction that for any d, sets of degree d Nullstellensatz witnessing polynomials cannot show the nonexistence of a common zero for an S_n-closed, uniformly generated set $\bar{Q}_n$, for $n \in N_d$, where N_d is any subset of $\mathbb{N}$ depending on d, if and only if the linear span of $\bar{\Lambda}_{\bar{Q},n}$ whose linear span (over $\mathbb{F}$) includes $T_{\bar{Q}}$ for $n \in N_d$. (the sets $\bar{\Lambda}_{\bar{Q},n}$ and $T_{\bar{Q}}$ clearly depend on d). ■

The following example illustrates the construction in the above proof

Example 8 *Let $\bar{Q}$ be an S_n-closed, uniformly generated, set containing the following generating polynomials $Q^i_s \in \mathbb{F}[x,n,2]$: $Q^1_{1,2} = x^2_{1,2} - x_{1,2}$,*
$Q^2_1 = \sum_* x_{1,*} - 1$,
and

$$Q^3_{1,2} = x_{1,2} - x_{2,1}.$$

Elaboration. In the above example, the defining parameters of $\bar{Q}$ are $d_{\bar{Q}} = 2$; and $l_{\bar{Q}} = 2$. The coefficients $q^{i,\alpha}_{E,s}$ are: $q^{1,(2)}_{(1,2),\{1,2\}} = 1$; $q^{1,(1)}_{(1,2),\{1,2\}} = -1$; $q^{2,(1)}_{(1,*),\{1\}} = 1$; $q^{2,(0)}_{(\emptyset),\{1\}} = -1$; $q^{3,(1)}_{(1,2),\{1,2\}} = 1$; and $q^{3,(1)}_{(2,1),\{1,2\}} = -1$.

Fixing $d = 2$ to be the bound on the witnessing polynomials P^i_s of the Nullstellensatz, of the form: $\sum^{\alpha}_{E} \lambda^{i,\alpha}_{E,s} x^{\alpha}_{E}$. We obtain the S_n-closed, uniformly generated set, $\bar{\Lambda}_{\bar{Q}}$, of homogeneous linear equations, one corresponding to each non-constant primitive term of degree $d + d_{\bar{Q}} = 4$. The generating set of $\bar{\Lambda}_{\bar{Q}}$ is given by those equations corresponding to non-constant primitive terms of degree 4, whose support is also restricted to $\{1, \ldots, d + d_{\bar{Q}}\} = \{1, 2, 3, 4\}$. There are many terms in this set, for example: $x_{1,2}$, $x_{1,3}$, …, $x_{4,3}$, $\sum_{*} x_{1,*}$, …, $\sum_{*} x^3_{4,*}$, …, $\sum_{*} x_{*,4}$, $x^2_{1,2}x_{2,3}$, …, $\sum_{*^1,*^2} x_{1,*^1} x^3_{*^2,3}$ $\sum_{*^1,*^2} x_{1,*^1} x_{1,*^2}$ etc.

We consider one of these primitive terms, say $\sum_{*^1,*^2} x_{1,*^1} x^3_{*^2,3}$ and write the corresponding linear polynomial Λ for that term. First we find all the possible ordered pairs of terms $(x^{\alpha^1}_{E^1},\ x^{\alpha^2}_{E^2})$ whose product gives the above term. There are exactly 4 such pairs: $(\sum_{*^1,*^2} x^3_{*^2,3} x_{1,*^1}, 1)$, $(1, \sum_{*^1,*^2} x^3_{*^2,3} x_{1,*^1})$, $(\sum_{*^1} x_{1,*^1}, \sum_{*^2} x^3_{*^2,3})$, $(\sum_{*^2} x^3_{*^2,3}, \sum_{*^1} x_{1,*^1})$. Thus only the second polynomial in $\bar{Q}$, i.e, Q^2, contributes to this term. The linear polynomial Λ is given below. (We first introduce indeterminates in order to homogenise lengths of subscripts E^1 and s of the variables λ to total $dr + l_{\bar{Q}} = 6$, and introduce additional variable types or superscripts - which are subsets of $\{1, \ldots, dr\}$ - corresponding to different sets of "original" indeterminates.)

$$\sum_{\pi} (q^{2,(1)}_{(1,*),\{\pi(1)\}} = 1)[\sum_{*^2} \sum_{*^3} \sum_{*^4} \sum_{*^5} \lambda^{2,(3),\{1\}}_{(*^2,3),(*^3,*^4),\{\pi(1),*^5\}} +$$
$$(q^{2,(0)}_{(\emptyset),\{\pi(1)\}} = -1) \sum_{*^1} \sum_{*^2} \sum_{*^3} \lambda^{2,(3,1),\{1,4\}}_{(*^2,3),(1,*^1),\{\pi(1),*^3\}}]$$

(Note that we have not distinguished the indeterminate in $(q^{2,(1)}_{(1,*),\{\pi(1)\}} = 1)$ since it is unambiguous. Also note that the superscript $\{1\}$ on the first λ refers to the position of its subscript $*^2$ corresponding to an original indeterminate, and similarly the superscript $\{1, 4\}$ on the second λ refers to the position of the original indeterminates $*^2$ and $*^1$ in its subscript list.). Since there is only one permutation $\pi \in S_n$, namely the identity, for which $q^{2,(1)}_{(1,*),\{\pi(1)\}}$ $q^{2,(1)}_{(\emptyset),\{\pi(1)\}}$ are non-zero, in this particular case, the $\sum_{\pi}$ can be removed from the above polynomial (otherwise, one would have to employ the Lemma 9 to decompose this sum into "legal" sums). ■

The following lemma is a simple application of the inclusion-exclusion principle which has been used in the proof of Lemma 7.

Lemma 9 *For any term x^{α}_{E} in $\mathbb{F}[x, n, r]$, consider the summation $\sum_{\pi} x^{\alpha}_{\pi(E)}$ where π runs over all permutations of its support (the set of distinct elements of $\{1, \ldots, n\}$ that occur in E). Clearly, this summation is not a legal term in $\mathbb{F}[x, n, r]$. The following procedure expresses this summation as a linear combination of legal terms. Let m be the support size of x^{α}_{E}. Replace the elements in E by a set of m distinct indeterminates, $I = \{*^1, \ldots, *^m\}$, and denote the resulting expression (not yet a legal term) as $x^{\alpha}_{E^*}$. For each subset $S = \{*^{s_1}, *^{s_2}, \ldots, *^{s}\}$ of I, denote by $\sum^{S}$, the operator*

$$\sum_{\{(*^1,\ldots,*^m)\in\{1,\ldots,n\}^m : *^{s}1 = *^{s}2 = \ldots = *^{s}\}} .$$

Now

$$\sum_{\pi} x^{\alpha}_{\pi(E)} = \overset{\emptyset}{\sum} x^{\alpha}_{E^*} - \sum_{\{S \subseteq I : 2 \leq |S| \leq m\}} (-1)^{|S|-1}(|S|-1) \overset{S}{\sum} x^{\alpha}_{E^*}.$$

This holds in any field $\mathbb{F}$*, with the coefficients* $(-1)^{|S|-1}(|S|-1)$ *expressed* $\pmod{q}_{\mathbb{F}}$.

Given Lemma 7, for the second step of the proof of Theorem 5 it is sufficient to show that if the linear span of an S_n-closed, uniformly generated set of linear polynomials $\bar{\Lambda}_{\bar{Q},n}$ includes a specific linear polynomial $T_{\bar{Q}}$ whenever $n = n(d)$, for some increasing function $n(d)$, then in fact, this inclusion holds for all $n \geq \max\{(d + d_{\bar{Q}})r + 3(dr + l_{\bar{Q}}), (7 + q_{\mathbb{F}}^2)(dr + l_{\bar{Q}}) - q_{\mathbb{F}}\}$, in some residue class of $q_{\mathbb{F}}^m$ (where m is the smallest integer such that $q^m \geq l_{\bar{Q}} + dr$.

To prove the above statement, we first transform it into a statement about $\mathbb{F}S_n$ modules in Section IV, whose proof takes advantage of basic properties of these modules.

IV The Problem in the Context of $\mathbb{F}S_n$ modules

In this section, we view the span of the S_n-closed, uniformly generated set (sequence) $\tilde{\Lambda}_{\tilde{Q},n}$ of linear polynomials from the last section, as a uniformly generated $\mathbb{F}S_n$-module (sequence). Thus we view the question left open in the last section as a question concerning the inclusion of the linear polynomial $T_{\tilde{Q}}$ in the $\mathbb{F}S_n$-module $\tilde{\Lambda}_{\tilde{Q},n}$.

First we give a concise background on $\mathbb{F}S_n$ modules, followed by a description of the specific modules that we deal with. Finally, we state and prove the theorems that are needed to complete the proofs of the main results stated in the previous section.

IV.1 Background on $\mathbb{F}S_n$ modules

Let S_n be the symmetric group of permutations of n distinct letters, say $\{1, \ldots, n\}$ and let $\mathbb{F}$ be a field.

NOTE: In the following definitions, to maintain clarity, we subscript additions and multiplications by the algebraic object in which they operate. During the remainder of the discussion, however, we omit subscripts since the algebraic object where the operations take place is usually clear from the context.

The **group ring** $\mathbb{F}S_n$, consists of elements of the form $\sum_{\pi} a_\pi \pi$, where $a_\pi \in \mathbb{F}$ and $\pi \in S_n$, with addition and multiplication defined as:

$$(\sum_{\pi} a_\pi \pi) +_{\mathbb{F}S_n} (\sum_{\pi} b_\pi \pi) = \sum_{\pi} (a_\pi +_{\mathbb{F}} b_\pi)\pi;$$

$$(\sum_{\pi} a_\pi \pi)(\sum_{\delta} b_\delta \delta) = \sum_{\pi} \sum_{\delta} (a_\pi *_{\mathbb{F}} b_\delta)(\pi \circ_{S_n} \delta).$$

The group ring $\mathbb{F}S_n$ is also a the **group algebra** of S_n over $\mathbb{F}$, and hence we will also refer to it as the group algebra $\mathbb{F}S_n$.

An $\mathbf{\mathbb{F}S_n}$**-module** V is an additive Abelian group V together with a map M_V from $\mathbb{F}S_n \times V \to V$, such that for $r, s \in \mathbb{F}S_n$, and $A, B \in V$,

- $M_V(r,(A +_V B)) = M_V(r,A) +_V M_V(r,B)$;
- $M_V((r +_{\mathbb{F}S_n} s),A) = M_V(r,A) +_V M_V(r,A)$;
- $M_V(r, M_V(s,A)) = M_V(r *_{\mathbb{F}S_n} s, A)$.

A group V can support more than one $\mathbb{F}S_n$ module structure, depending on the chosen map M_V.

In this paper (roughly speaking), the $\mathbb{F}S_n$-modules V contain elements of the form $\sum\limits_u b_u u$, where $b_u \in \mathbb{F}^t$, for some field $\mathbb{F}$; and $u \in \{1,\ldots,n\}^k$, (recall our convention that $\{1,\ldots,n\}$ is just a set of n distinct letters on which the permutations in S_n will act), t and k are constants. Addition in the Abelian group V is defined as:

$$(\sum_u a_u u) +_V (\sum_u b_u u) = \sum_u (a_u +_{\mathbb{F}^t} b_u)u;$$

and the map M_V giving the module structure to V is the following: given an element $\sum_\pi a_\pi \pi$ of the group ring $\mathbb{F}S_n$ and an element $\sum_u b_u u$ of the Abelian group V,

$$M_V(\sum_\pi a_\pi \pi, \sum_u b_u u) = \sum_\pi \sum_u (a_\pi *_{\mathbb{F}} b_u)\pi(u),$$

where $\pi(u)$ is the natural action of a permutation $\pi \in S_n$ on $u \in \{1,\ldots,n\}^k$.

Notice that the $\mathbb{F}S_n$ modules V described in the above paragraph are in fact vector spaces over $\mathbb{F}$, spanned by basis elements $B_i \in V$ such that every $F \in V$ can be written as $\sum_i a_i B_i$, where $a_i \in \mathbb{F}$. In addition, due to their module structure, these vector spaces V are in fact closed under the natural action of S_n on its elements.

Thus in addition to being vector spaces over $\mathbb{F}$ spanned by basis elements, $\mathbb{F}S_n$ modules V are **generated** by a set of **generators** $E_i \in V$, such that every $F \in V$ can be written as $\sum_i r_i E_i$, where r_i is an element of the group algebra $\mathbb{F}S_n$.

Each $\mathbb{F}S_n$ module is a **representation** of S_n in the following sense. Viewing the $\mathbb{F}S_n$ modules (such as the modules V described earlier) as vector spaces over $\mathbb{F}$ that are closed under the natural action of permutations in S_n, it becomes clear that each permutation represents a linear transformation on V. In other words, each $\mathbb{F}S_n$ module provides a group of linear transformation matrices representing the group of permutations S_n. As a result, $\mathbb{F}S_n$ modules are studied extensively in the representation theory of S_n. Moreover, most of the interesting questions in the case of $\mathbb{F}$ being a field of finite characteristic are still unsolved.

In the current discussion, however, we avoid the use of much representation theory, and develop the machinery that we need, as we go. Several related, unsolved representation theory problems arise from the discussion in this paper, which are of independent interest. These we list in Section VI, and deal with in a separate paper [9].

IV.2 The modules $\tilde{V}[\mathbb{F}, n, k, t]$ and basic properties

The module $\tilde{V}[\mathbb{F}, n, k, t]$ consists of all module elements of the form: $\sum\limits_i \beta_i E_i$, where $\beta_i \in \mathbb{F}^t$. To describe the **primitive module elements** E: take a vector e (called the **defining vector** of E) in $\{1,\ldots,n,*^1,*^2,\ldots,*^k\}^k$ with the property that the indeterminates $*^j$ that appear in e are all distinct; let $*^1,\ldots,*^m$ be the indeterminates that appear in e; now E has the form $\sum_{*^1=1}^{n}\sum_{*^2=1}^{n}\ldots\sum_{*^m=1}^{n} e$. The **dimension** of a primitive module element (analogous to terms in Section III.1) is the number of indeterminates or summation signs that appear in it. For example, a primitive element with no summation signs is called a **point** element a term with one summation a **line**, with two summations a **plane**, etc. The **intersection** of two primitive elements E and F with defining vectors e and f is non-empty exactly if each pair of determinates – occurring at the same coordinate of e and f – coincide in value. The intersection in this case has dimension equal to the number of coordinates where the determinate pairs coincide. The new defining vector is identical to e where f has indeterminates and is identical to f where e has indeterminates. Where both have determinates they takes their common value.

Given an element E of $\tilde{V}[\mathbb{F},n,k,t]$, its **support**, s_E, is the list in say, ascending order, of *distinct* entries from $\{1,\ldots,n\}$ (determinates) that appear among the primitive elements in its expansion. Its **defining parameters** are the characteristic $q_{\mathbb{F}}$ of the field $\mathbb{F}$, its **universal dimension** k, and its **support-size** l_E. We say an element of $\tilde{V}[\mathbb{F},n,k,t]$ is **ultrasmall** if its support size is at most $2k$. All of these parameters are independent of n.

Note that a module element E of $\tilde{V}[\mathbb{F},n,k,t]$ can be viewed as a *sequence* of elements (that may change) as n increases; But since this sequence is straightforward, we will drop the word "sequence" and the subscript n, normally just refer to it as a module element. However, in some situations, to avoid confusion, we will refer to the nth module element in the sequence as E_n. Often, two module elements E and F of $\tilde{V}[\mathbb{F},n,k,t]$ are **equivalent** only for a certain value of n. For example, the element

$$C =< 3,3 > [1,1,2]+ < 3,3 > [2,1,2]$$

of $\tilde{V}[\mathbb{F}=\mathbb{R},n,k=3,t=2]$ is equivalent to the element

$$B =< 1,2 > \sum_{*}^{n}[*,1,2]+ < 2,1 > \sum_{*}^{n}[*,1,2]$$

at $n=2$. Whereas, we say that two elements E and F of $\tilde{V}[\mathbb{F},n,k,t]$ are **identical** if they are equivalent for *all* values of n. For example, the element B described above is identical to the element

$$A =< 3,3 > \sum_{*}^{n}[*,1,2].$$

Notice that two equivalent elements may have *different support-sizes*, even at the particular n where they are equivalent. Intuitively, the support-size represents the amount of non-periodic information in a module element. If two elements H and H' are equivalent at n, we say $\mathbf{H} \succ \mathbf{H}'$ if H has been obtained from H' by replacing some part of H of the form $P_1+\ldots+P_s$ where the $P_i's$ have dimension m, by an equivalent Q of dimension greater than m.

We treat sets of module elements similar to single elements. The defining parameters of a set are the same as those of its elements, except the support-size which is the *maximum* of the support-sizes of its elements.

We treat (sub)modules, including $\tilde{V}[\mathbb{F}, n, k, t]$ a little differently. In general, the support-size $l_{\tilde{W}}$ of a submodule $\tilde{W}$ of $\tilde{V}[\mathbb{F}, n, k, t]$ (for a fixed n), is the *minimum* of the support-sizes of all the generating sets for $\tilde{W}$, therefore, in general, the defining parameters of a submodule sequence $\tilde{W}_n$ *depends* on n, and hence we do not drop the subscript n when referring to the sequence. However, we will use the n in $\tilde{W}_n$ or in $\tilde{V}[\mathbb{F}, n, k, t]$ *both* to refer to the sequence, as well as to refer to the n^{th} module in the sequence, in order to distinguish it from a single module is defined for a fixed n.

A submodule sequence $\tilde{W}_n$ of $\tilde{V}[\mathbb{F}, n, k, t]$ is **uniformly generated**, if there is a set $\bar{G}$ of generating module elements in $\tilde{V}[\mathbb{F}, n, k, t]$, such that for each n, the submodule $\tilde{W}_n$ is the $\mathbb{F}S_n$ module generated by $\bar{G}_n$. Clearly, if a submodule sequence $\tilde{W}_n$ is uniformly generated, its defining parameters are independent of n. We drop the word "sequence" when referring to submodule (sequences) $\tilde{W}_n$ that are uniformly generated, however, as before, we will use the subscript n in $\tilde{W}_n$ both to refer to the sequence, as well as to refer to the n^{th} module in the sequence, in order to distinguish it from single module $\tilde{W}$ that is defined for a fixed n. We sometimes write $\tilde{W}_n$, uniformly generated from $\bar{G}$, as $[\bar{G}]_n$ when convenient.

Example: For $n \geq 10$ and $k = 3$ let

$$E := [123] + [132] + [213] + [231] + [312] + [321] + [445] + \\ [676] + [988] + [10, 10, 10] + \sum_i \sum_j \sum_k [ijk]$$

and let

$$F := [123] + [132] + [213] + [231] + [312] + [321] + [445] + [676] + [988] + [10, 10, 10].$$

Notice that $s_E = s_F = \{1, 2, ...10\}$, and that $l_E = l_F = 10$. The dimension of the primitive module element $\sum_i \sum_j \sum_k [ijk]$ is 3, while all other primitive module elements in E and F have dimension 0 (i.e. are points). We want to decide when E and F generates the same subspaces of $\tilde{V}[\mathbb{F}, n, k, 1]$. For $q \neq 3$ it is not hard to show that $[E]_n = [F]_n$ for all $n \geq 10$. To settle the case for $q = 3$ it is convenient to define an S_n-invariant inner product **(to be continued)**. ♣

Since a module is, among other things, a vector space, we can define an inner product between module elements. Let $\langle \beta, \gamma \rangle$ be the standard inner product between vectors β and γ in $\mathbb{F}^t$. The inner product $[[,]]_n$ between module elements of $\tilde{V}[\mathbb{F}, n, k, t]$ is defined as follows.

$$[[\sum_i \beta_i E_i, \sum_i \gamma_i F_i]]_n = \sum_{e \in \{1,\ldots,n\}^k} \langle \sum_{e \in E_{i,n}} \beta_i, \sum_{e \in F_{i,n}} \gamma_i \rangle.$$

All summations on the RHS are in $\mathbb{F}^t$. When $[[E_n, F_n]]_n = 0$, as usual, we say that $E_n \perp_n F_n$, and drop the subscript on $\perp$. The vector space (in fact, a module) that is orthogonal to a module $\tilde{W}_n$ (under $[[,]]_n$), is denoted $\tilde{W}_n^{\perp}$. Notice that the inner product is S_n-invariant i.e. $\forall \pi \in S_n$: $[[\pi E, F]]_n = [[E, \pi^{-1} F]]_n$. Or in other words, $\forall \pi \in S_n$: $[[E, F]]_n = [[\pi E, \pi F]]_n$.

Example, continued: For $q = 3$ we have $[E]_n \subseteq [F]_n$. We leave it to the reader to check that $[E]_n = [F]_n$ when $\binom{n}{3} \neq 2$ modulo 3, i.e. $n = 0, 1, 2, 3, 4, 5$ modulo 9, while $[E]_n \neq [F]_n$ when $\binom{n}{3} = 2$ modulo 3 i.e. $n = 6, 7, 8$ modulo 9 To show $[E]_n \neq [F]_n$ when $\binom{n}{3} = 2$ modulo 3 simply compare the inner products $[[\delta E, \sum_{i<j<k} [i, j, k]]]$ and $[[\delta F, \sum_{i<j<k} [i, j, k]]]$ for any $\delta \in S_n$). ♣

The following proposition gives a simple, but useful asymptotic property concerning the invariance of the orthogonality of module elements with small support. The fact that the orthogonality conditions only depend on the residue class modulo $q_{\mathbf{F}}$ show however that stronger methods are needed to prove our main result of Section III.2 where the residue class depends on k as well. In particular, For fixed q and k we write $\mathbf{n} \equiv_{\mathbf{q},\mathbf{k}} \mathbf{n}'$ provided $\binom{n}{j} = \binom{n'}{j}$ modulo q for $j = 1, 2, ..., k$. Notice that $n \equiv_{q,k} n'$ if and only if $n = n'$ mod q^u where $u := \min\{u : q^u \geq k\}$. the main technical result Theorem 12, applies to residue classes with respect to $\equiv_{q,k}$.

We only include the next proposition as an easier result with the same flavour as the main result.

Proposition 10 *Given two module elements E and F of $\tilde{V}[\mathbb{F}, n, k, t]$, of support-size bounded by l, $E_{n^*} \perp F_{n^*}$ for some $n^* \geq 2l$ if and only if $E_n \perp F_n$ for all $n \geq 2l$ in the same $q_{\mathbf{F}}$-residue class as n^*.*

Proof Since E and F have support at most l, without loss, we can assume that E and F together have support restricted to $\{1, \ldots, 2l\}^k$. Decompose E and F into their constituent points, lines, planes etc. Let E_i^0, F_i^0 represent the points, E_i^1, F_i^1 represent the lines, and in general E_i^k F_i^k represent the k-dimensional constituents of E and F respectively. Now $[[E, F]]_n$ is the sum of the all the inner products of the form $[[E_{i_1}^{j_1} F_{i_2}^{j_2}]]_n$. Clearly the inner products between a point and anything else remains the same for all $n \geq 2l$. Also, for two higher dimensional constituents that intersect on a point (dimension 0), the inner product remains the same for all $n \geq 2l$. Similarly for any two constituents that do not intersect at all, the inner product remains 0 always.

For two higher dimensional constituents whose intersection has dimension $m \geq 1$, (for $n \geq 2l$), the inner product depends only on the residue class of $n^m \text{mod} q_{\mathbf{F}}$.

Thus if $[[E, F]]_{n^*} = 0$ for any $n^* \geq 2l$, then $[[E, F]]_n = 0$ for any $n \geq 2l$, in the same $q_{\mathbf{F}}$-residue class as n^*. ■

IV.3 Module Versions of the Main Results

The main theorem in this subsection, Theorem 12 is a general result about the asymptotic behaviour of uniformly generated submodule sequences, which, together with the Proposition 11, completes the proof of the main results given in Section III.

This theorem additionally raises several related representation theory questions of independent interest which are listed in Section VI, and dealt with in a separate paper [9].

Proposition 11 *The linear span of an S_n-closed, uniformly generated set $\bar{\Lambda}$ of linear polynomials $\Lambda \in \mathbb{F}[\lambda^1, \ldots, \lambda^t, n, k]$ of support-size $l_{\bar{\Lambda}}$ is a uniformly generated submodule of $\tilde{V}[\mathbb{F}, n, k, t]$ whose support-size is at most $l_{\bar{\Lambda}}$.*

Proof Each linear polynomial Λ in $\bar{\Lambda}$ is of the form:

$$\sum_E \sum_i^t c_E^i \sum_{*^1=1}^n \cdots \sum_{*^{m_E}=1}^n \lambda_E^i,$$

where $c_E^i \in \mathbb{F}$, and E runs over elements of $\{1, \ldots, n, *^1, \ldots, *^k\}^k$ with m_E distinct indeterminates. Since we are only concerned with $\mathbb{F}$-linear spans of sets of linear polynomials, Λ can unambiguously be viewed as

$$\sum_E (c_E^1, \ldots, c_E^t)^T \sum_{*^1=1}^n \cdots \sum_{*^{m_E}=1}^n E$$

which is clearly a module element of $\tilde{V}[\mathbb{F}, n, k, t]$. Moreover, since the set $\bar{\Lambda}_n$ is S_n-closed, its linear span is clearly a submodule of $\tilde{V}[\mathbb{F}, n, k, t]$. Finally, since (the sequence) $\bar{\Lambda}$ is uniformly generated, its linear span is a uniformly generated submodule (sequence) with the same support-size. ■

Theorem 12 *Take a uniformly generated submodule $[\bar{G}]_n$ of $\tilde{V}[\mathbb{F}, n, k, t]$ and a module element H in $\tilde{V}[\mathbb{F}, n, k, t]$, both of support size bounded by l. For some $n^* \geq \max\{l + 3k, (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}\}$ let H' be a module element that is equivalent to H at n^*, with $H \succ H'$. Now if $H'_{n^*} \in [\bar{G}]_{n^*}$ (resp. $\notin$) if and only if $H_n \in [\bar{G}]_n$ (resp. $\notin$) for every $n \geq \max\{l + 3k, (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}\}$, with $n \equiv_{q_{\mathbb{F}},k} n^*$. In the case $\mathbb{F}$ has characteristic 0 the requirement $n \equiv_{q,k} n^*$ is dropped and the requirement on n^* (resp. n) is weakened to $n^* \geq 2l$ (resp. $n \geq 2l$).*

We divide the proof of Theorem 12 into two cases. The easier case when $\mathbb{F}$ has characteristic 0, and the more involved where $\mathbb{F}$ has finite characteristic, which requires several intermediate lemmas.

Proof (of Theorem 12 for $\mathbb{F}$ of characteristic 0)

Without loss, we assume that $\bar{G}$ and H have support exactly $\{1, \ldots, l\}$.

Inducing Down We first show that if $H_{n^*} \in [\bar{G}]_{n^*}$ for some $n^* \geq 2l$, then in fact $H_n \in [\bar{G}]_n$ for all $2l \leq n \leq n^*$. Clearly, it is sufficient to show that $H_{n^*-1} \in [\bar{G}]_{n^*-1}$, since $n^* \geq 2l$ is chosen arbitrarily.

Consider the expansion of H_{n^*} as a linear combination of permutations of elements (but not necessarily primitive) $\bar{G}_{n^*}$:

$$H_{n^*} = \sum_i \alpha_i G_{i,n^*} \qquad (I)$$

where each G_i is obtained by letting a permutation in S_{n^*} act on one of the generators in $\bar{G}$.

The idea of the proof is simple: we first show that a useful increment Δ_{n^*} can also be generated by $\bar{G}$ at n^*. Obtain H'_{n^*} by restricting to $n^* - 1$, all summation signs in the elements (i.e, lines, planes etc..) that appear in the G_{i,n^*} in (I). Obtain H''_{n^*} by viewing H_{n^*-1} as an element in $\tilde{V}[\mathbb{F}, n^*, k, t]$, which has zero coefficients attached to all vectors in $\{1, \ldots, n^*\}^k \setminus \{1, \ldots, n^* - 1\}^k$. Now $\Delta_{n^*} =_{def} H'_{n^*} - H''_{n^*}$. Notice that Δ_{n^*} has support restricted to $\{1, \ldots, n^*\}^k \setminus \{1, \ldots, n^* - 1\}^k$. Then we observe that $H_{n^*} - \Delta_{n^*}$ can be generated by $\bar{G}$ using only permutations that fix n^*. It follows immediately from these observations and from the definition of Δ_{n^*} that H_{n^*-1} can be generated by $\bar{G}$ at $n^* - 1$.

Let Π denote the subgroup of permutations in S_{n^*} that fix the the values in $\{1, \ldots, l\}$ and the value n^*. Clearly,

$$H_{n^*} = 1/|\Pi| \sum_{\pi \in \Pi} \sum_i \alpha_i \pi(G_{i,n^*}). \qquad (II)$$

Let $\bar{C}$ denote the set of all G_{i,n^*} in (II) that contain a vector (with a non-zero coefficient) in $\{1, \ldots, n^*\}^k \setminus \{1, \ldots, n^* - 1\}^k$. Note that higher dimensional module elements G_{i,n^*} may contain an entry m even if m is not in the support of G_{i,n^*} (See Section IV for the definition of support of a module element) and let $\bar{D}$ denote the set of all G_{i,n^*} in (II) that contain only vectors in $\{1, \ldots, n^* - 1\}^k$ (these are not only supported entirely in $\{1, \ldots, n^* - 1\}$, but are also linear combinations of zero dimensional elements, i.e, points alone).

For each $F_{n^*} \in \bar{C}$, Denote by $\Pi_F \subseteq S_{n^*}$ all the permutations in S_{n^*} that fix $\{1, \ldots, l\}$, do *not* fix n^* and do not map any value in the support of F_{n^*} to n^*. Clearly the size of Π_F differs depending on the size of support of F_{n^*}.

Consider the quantity:

$$1/|\Pi| \sum_{\pi \in \Pi} [\sum_{G_{i,n^*} \in \bar{D}} \alpha_i \pi(G_{i,n^*})] + \sum_{G_{i,n^*} \in \bar{C}} [1/|\Pi_{G_i}| \sum_{\pi \in \Pi_{G_i}} \alpha_i \pi(G_{i,n^*})] \qquad (III)$$

Notice that each permutation π in Π can be modified into a permutation in Π_F for any F, by inserting n^* into a cycle in π, making sure that it does not immediately follow (in the cycle), any value in the support of F_{n^*}. Using this process, each permutation $\pi \in \Pi$ yields exactly the same number of permutations in Π_F. Conversely, there is a surjective map from Π_F to Π that maps exactly the same number of permutations in Π_F to each permutation in Π.

Observe that (III) is identical to H_{n^*} on $\{1,\ldots,l\}^k$ (and thus to $H_{n^*} - \Delta_{n^*}$, due to the definition of (the support of) Δ_{n^*}); and is identical to $H_{n^*} - \Delta_{n^*}$ on $\{1,\ldots,n^*\}^k \setminus \{1,\ldots,n^*-1\}^k$. Moreover, for vectors v in $\{1,\ldots,n^*-1\}^k \setminus \{1,\ldots,l\}^k$, the coefficient value c_v in (III) is given as follows: let $c_{H,v}$ be the coefficient of v in H_{n^*} (or $H_{n^*} - \Delta_{n^*}$, which is the same); and let $c_{\Delta,v}$ be the coefficient, in Δ_{n^*}, of a vector v' obtained from v by using the permutation (b, n^*) on some entry-value b between $l+1$ and n^*-1 that occurs in v (notice that it does not matter which entry-value of v we choose to move). Now $c_v = c_{H,v} + \alpha c_{\Delta,v}$, where α is a *fixed* constant.

Notice that (III) is almost identical to $H_{n^*} - \Delta_{n^*}$ except on $\{1,\ldots,n^*-1\}^k \setminus \{1,\ldots,l\}^k$, where there is an extra contribution resulting from certain well-defined summands in the second term of (III). These summands correspond exactly to those G_{i,n^*} that contribute to the "Δ_{n^*} part" of of H_{n^*} in (I) and can therefore be isolated. Hence this extra contribution is removed by weighting all of these summands by $1/(1+\alpha)$ in (III).

Thus we have shown that $H_{n^*} - \Delta_{n^*}$ can be generated by $\bar{G}$ using (III), and and clearly all the summands in (III) have supports restricted to $\{1,\ldots,n^*-1\}$. Therefore we have completed the proof of the first part.

Inducing Up. Next, we show that if $H_{n^*} \in [\bar{G}]_{n^*}$ for some $n^* \geq 2l$, then in fact $H_{n^*+1} \in [\bar{G}]_{n^*+1}$.

The idea here is to "reverse" the process of inducing down, and in fact the reversed process is simpler to perform. Consider the expansion of H_{n^*} in (I) and its (identical) symmetrised version in (II). Denote by $H^e_{n^*+1}$ the element of $\tilde{V}[\mathbb{F}, n^*+1, k, t]$ obtained by extending all the summation signs (of lines, planes etc.) occurring in the RHS of (I) to n^*+1. Denote the resulting expression as (I'). Note that $H_{n^*+1} - H^e_{n^*+1}$ is exactly Δ_{n^*+1} as defined earlier. Note also that $H^e_{n^*}$ remains invariant when symmetrised by averaging over all permutations that fix $\{1,\ldots,l,n^*+1\}$. Clearly, $H^e_{n^*+1}$ is generated by $\bar{G}$. Similar to the process used to obtain (III), symmetrise each G_{i,n^*} that appears in the RHS of (I') by averaging over all permutations in S_{n^*+1} that fix $\{1,\ldots,l\}$. Call the new expression (III').

Notice that (III') is almost identical to the desired H_{n^*+1}; the difference is restricted to $\{1,\ldots,n^*+1\} \setminus \{1,\ldots,l\}$, and can be expressed, as before, by a fixed constant fraction α times a sum of permuted copies of Δ_{n^*+1}. Again, as before, this extra contribution is nullified by weighting a well-defined set of summands in (I') by $1/(1+\alpha)$.

■

IV.4 The Main Lemmas

The lemmas required to complete the proof of Theorem 3 in the finite characteristic case rely on the following phenomena: uniformly generated submodules of $\tilde{V}[\mathbb{F}, n, k, t]$ are in fact generated by ultrasmall generators. Furthermore, if an ultrasmall element F' equivalent to F with $F \succ F'$ is generated by a set $\bar{E}$ of ultrasmalls for some large n^*, then, in fact, F is generated from $\bar{E}$ at all n beyond a small constant in some residue class of n^*. Both the constant and the residue class depend only on $q_{\mathbf{F}}$ and (linearly) on k.

Compression

The first lemma shows that uniformly generated submodules (sequences) of $\tilde{V}(\mathbb{F}, n, k, t)$ that have generators of small support in fact have ultrasmall generators beyond a small value of n. We say we **compress** the collection of small objects into ultrasmall objects when we carry out this procedure.

Lemma 13 *Given an element E of $\tilde{V}(\mathbb{F}, n, k, t)$ of support l, there is a set $\bar{F}$ of ultrasmall generators such that for all $n \geq l + 3k$, $[\bar{F}]_n = [E]_n$.*

Proof The key idea in breaking down small elements to ultrasmall generators is quite simple in essence. We hope that the following pictures can be helpful for the reader to understand the underlying idea in many later arguments:

First let us consider a toy example which captures some of the general ideas in some of the later arguments. Consider figure 1 to figure 6 in the Appendix. In figure 1 we see a generator E. It have support $\{1, 2, ..., 6\}$ (assuming it has two horizontal lines with coefficients 5 and 3) In figure 2 we consider $(6, 7)E$. Any submodule containing E obviously also must contain $E_1 := (6, 7)E - E$. And any submodule containing E_1 must contain E_3 and E'. On the other hand $E = E' - E_3$ so the submodule $[E', E_3]_n$ and $[E]_n$ are identical for all $n \geq 8$. Notice that E' is slightly simpler than E because it contain one more 0 entry. And E_3 is ultra-small (support size $\leq 2k = 4$). In general, the situation is more complex, though in principle very similar. The complexity arises due to the following considerations.

- We have to consider the case $k > 2$.
- We also have to deal with lines, planes and other higher dimensional objects. This is not an entirely trivial generalisation because is some cases, in compressing higher dimensional objects, we will partly destroy some of the compression which we have achieved for smaller dimensional objects.
- All entries are vectors (in $\mathbb{F}^t$) not just field elements.

We now consider the general case: Pick a k-element tuple $[i_1^1, i_2^1, ..., i_k^1]$ where each $i_j^1 > l$. Let E be a generator support contained in $l := \{1, 2, ..., l\}, l \geq k$. Assume that $n \geq l + 3k$. For each k-element tuple $[i_1^0, i_2^0, ..., i_k^0] \in \{1, 2, ..., n\}^k$ we define an operator $\Gamma^0_{[i_1^0, i_2^0, ..., i_k^0; i_1^1, i_2^1, ..., i_k^1]}$ by

$$\Gamma^0_{[i_1^0, i_2^0, ..., i_k^0; i_1^1, i_2^1, ..., i_k^1]} := \sum_{(\alpha_1, ..., \alpha_k) \in \{0,1\}^k} (-1)^{\alpha_1 + ... + \alpha_k + k - 1} \; (i_1^0, i_1^{\alpha_1})(i_2^0, i_2^{\alpha_2}) .... (i_k^0, i_k^{\alpha_k}).$$

Here $(i_1^0, i_1^{\alpha_1})(i_2^0, i_2^{\alpha_2}) .... (i_k^0, i_k^{\alpha_k}) \in S_n$ is written in the usual cycle notation.

To better describe the action of Γ^0, define $\delta^0_{[i_1^2, i_2^2, ..., i_k^2]}([j_1, j_2, ..., j_k]) = 1$ if $i_1^2 = j_1, i_2^2 = j_2, ..., i_k^2 = j_k$ and 0 otherwise. Notice $\Gamma^0_{[i_1^0, ..., i_k^0; i_1^1, i_2^1, ..., i_k^1]} \delta^0_{[i_1^2, i_2^2, ..., i_k^2]}$ is zero except when $\{i_1^2, i_2^2, ..., i_k^2\} = \{i_1^0, ..., i_k^0\}$ (assuming that $\{i_1^1, i_2^1, ..., i_k^1\} \cap \{i_1^2, i_2^2, ..., i_k^2\} = \emptyset$). We

also consider $\delta's$ which instead of being supported in a point, are supported in an d-dimensional primitive module element. Such an object is denoted by $\delta^d_{[i^2_1,i^2_2,...,i^2_k]}$ where d of the variables $i^2_1, i^2_2, ..., i^2_k$ are indeterminates. Notice that for $d \geq 1$ $\Gamma^0_{[i^0_1,i^0_2,...,i^0_k;i^1_1,i^1_2,...,i^1_k]}\delta^d_{[i^2_1,i^2_2,...,i^2_k]} = 0$ for any choice of $i^2_1, i^2_2, ..., i^2_k$.
More generally for each $0 \leq d \leq k$, and for each $k-d$ tuples $i^0_1, i^0_2, ..., i^0_{k-d}$ and $i^1_1, i^1_2, ..., i^1_{k-d}$ we let

$$\Gamma^d_{[i^0_1,i^0_2,...,i^0_{k-d};i^1_1,...,i^1_{k-d}]} := \sum_{(\alpha_1,...,\alpha_{k-d})\in\{0,1\}^{k-d}} (-1)^{\alpha_1+...+\alpha_{k-d}+k-d-1}\ (i^0_1, i^{\alpha_1}_1)....(i^0_{k-d}, i^{\alpha_{k-d}}_{k-d}).$$

A crucial fact to note is that a $\Gamma^d\delta^{d'} = 0$ for $d' > d$, or in other words, operators Γ^d annihilate objects of dimension greater than d. Equally important: notice that $\Gamma^d E$ (any E) always has support size at most $2(k-d)$.

Now given $E = E_0 + E_1 + ... + E_d$ of support $S_E \subseteq \{1, 2, ..., l\}$ ($l \geq 2k$) (in general E_j consists of j-dimensional primitive elements), we want to show that if $n \geq l + 3k$ we can always "improve" these support sizes so they all eventually become at most $2k$.

The first step in this reduction is carried out as follows: Pick $[i^1_1, i^1_2, ..., i^1_k]$ such that $\{i^1_1, i^1_2, ..., i^1_k\} \subseteq \{l+1, ..., n\}$. Pick also $\{i^0_1, ..., i^0_k\}$ inside the support set of E_0. The operator $\Gamma^0 := \Gamma^0_{[i^0_1,...,i^0_k;i^1_1,i^1_2,...,i^1_k]}$ can now be used to increase the number of zeros at places with at least one coordinate outside $\{1, 2, ..., 2k\}$ as follows. Note that $\Gamma^0 E = \Gamma^0 E_0$ has support size at most $2k$. If a permutation π is chosen appropriately so it maps $\{i^1_1, i^1_2, ..., i^1_k\}$ onto $\{1, 2, ..., k\}$, the number of non-zeroes of $E_0 - \pi\Gamma^0 E_0$, at points with at least one coordinate outside $\{1, 2, ..., 2k\}$ has been reduced by at least 1. Now $E - \pi\Gamma^0 E$ can be written as $E_0 - \pi\Gamma^0 E_0 + E_1 + ... + E_d$. Notice that E is derivable from $E - \pi\Gamma^0 E$ and $\Gamma^0 E$. By continuing this process, we eventually get $E' = E'_0 + E_1 + ... + E_d$ where the support of E' is contained in $\{1, 2, ..., 2k\}$. Thus we have a general method by which $E = E_0 + E_1 + ... + E_d$ can be decomposed into $E' = E'_0 + E_1 + ... + E_d$ (where E'_0 has support contained in $\{1, 2, ..., 2k\}$) together with a finite number of ultrasmall generators.

Next we decompose the lines in E_1. This is done by use of an appropriate operator Γ^1 as before. Notice that $\Gamma^1 E'_0$ has support at most k, so in $E' - \pi\Gamma^1 E = (E'_0 - \pi\Gamma^1 E'_0)$ $+(E_1 - \pi\Gamma^1 E_1) + E_2 + ... + E_d$ the support of $E''_0 := E'_0 - \pi\Gamma^1 E'_0$ is at most $2k$. The support of $E_1 - \pi\Gamma^1 E_1$ is at most $\max(2(k-1), l-k)$. When we continue this process, by choosing a new Γ^1 at the next step to reduce the support of $E_1 - \pi\Gamma^1 E_1$ even further, the support-size of E'''_0 (the reduced part of E''_0) may now have support size $3k$. However, this can be reduced back to $2k$ by use of an appropriate Γ^0, provided $n \geq l + 3k$.

Eventually, after a finite number of steps (depending on l and k, but independent of n) we have produced a set of ultrasmalls $\bar{F}$ such that for any $n \geq l + 3k$ we have $[E]_n = [\bar{F}]_n$. ■

Notice that submodules of $\tilde{V}(\mathbb{F}, n, k, t)$ that are orthogonal (w.r.t $[[,]]_n$) to submodules generated by ultrasmall generators are themselves *not* necessarily generated by ultrasmalls. In other words, the class of modules generated by ultrasmall generators is not closed under the $\perp_n$ operation. This prevents the use of Proposition 10

A proof system for submodule membership First let us summerise the idea behind the following constructions. Our overall aim is to prove Theorem 12. Suppose that for some n there is a derivation of some ultrasmall object F from a collection $\{E_1, E_2, .., E_u\}$ of ultrasmalls. One could imagine that during this derivation some very nasty module elements $G, G', G'', ..$ are constructed. Nasty in the sense that they generate a FS_n-module which for example is not generated by ultrasmalls. The idea behind the following proof system is to show that such hypothetical nasty module elements $G, G', G'', ..$ can be avoided. It is an open question to what extend such nasty module elements exists at all. Now the fact F is ultrasmall allows us to show there indeed is a nice derivation of F. Intuitively the point is that the derivation is so well-behaved that the derivation actually can be lifted/lowered to other values of n. The following formal proof system captures all manipulations (for generating module elements) one could possible hope to be available in the FS_n-case.

Let F be and element and $\bar{E}$ a set of elements of $\tilde{V}(\mathbb{F}, n, k, t)$. Then a **formal derivation** of F from $\bar{E}$ is defined as follows.

The **formal proof system** $\mathcal{P}[\mathbb{F}, n, k, t]$ for proving submodule membership of $\tilde{V}[\mathbb{F}, n, k, t]$ contains the following rules for deriving new module elements: $\frac{A\ B}{A+B}$, $\frac{A}{\pi A}$ and $\frac{A}{cA}$ where $\pi \in S_n$ and $c \in \mathbb{F}$. This describes the proof system $\mathcal{P}[\mathbb{F}, n, k, t]$ completely. We say the module element F is derived (in $\mathcal{P}[\mathbb{F}, n, k, t]$) from $\bar{E}$, if starting from the elements of $\bar{E}$ and applying a series of the above rules, one obtains F. The **width** of the proof denotes the largest number m which was moved under some $\rho \in S_n$ during the proof.

Given $E \in \tilde{V}(\mathbb{F}, n, k, t)$, where $n \geq 2k$. The **formal compression** of E of support size l is a collection $U(E)$ of ultrasmall (i.e support size $\leq 2k$) elements which appear by taking $E_{n'}$ for some $n' \geq l + 3k$ (for instance $n' = n + 3k$) and applying the compression procedure to get a collection $E_1, E_2, ..., E_u \in \tilde{V}(\mathbb{F}, 2k, k, t)$ of ultrasmalls such that $[E]_{n'} = [E_1, E_2, ..., E_u]_{n'}$. We let $U(E) := \{E_1, E_2, ..., E_u\}$. For convenience we normally also assume $U(E)$ is closed under S_{2k} (i.e. $F \in U(E) \Rightarrow \pi F \in U(E)$ for $\pi \in S_{2k}$).

Lemma 14 *Given any module element F of $\tilde{V}(\mathbb{F}, n, k, t)$, with $F \in [\bar{E}]_n$, and a a formal derivation of F from $\bar{E}$ in $P(\mathbb{F}, n, k, t)$, we assign a collection of ultrasmalls $T(W)$ at each intermediate module element W in the derivation as follows. To each "axiom" $E_j \in \bar{E}$ we assign $\{\pi E_i, \pi \in S_{2k}\}$. The assignment of a conclusion $\frac{A}{\pi A}$ is unchanged (i.e. $T_{\pi A} = T_A$). The assignment of a conclusion $\frac{A}{cA}$ is given by: $T_{cA} := \{cE : E \in T_A\}$. The assignment T_{A+B} to conclusion of an application of $\frac{A\ B}{A+B}$ is obtained as follows: we have the assignments T_A and T_B, and we et*

$$T^{\text{aux}}_{A+B} := \{E :\ \exists \pi_1, \pi_2 \in S_{4k}, \exists E_A \in T_A, E_B \in T_B\ E = \pi_1 E_A + \pi_2 E_B\}.$$

Notice that all objects in T^{aux}_{A+B} have support size $\leq 4k$. Now let T_{A+B} consist of all ultrasmall objects which can be written as a linear combination of elements (possible moved by some $\pi \in S_{4k}$) in $U(T^{\text{aux}}_{A+B})$. Notice that each object in T_{A+B} has a derivation of width $\leq 7k (= 4k + 3k)$ from objects in T^{aux}_{A+B}. Thus in general each object in T_W can be derived by a proof of width $\leq 7k$. The claim is that for every module element W in the derivation, we have $U(W) \subseteq T_W$; and in particular $U(F) \subseteq T_F$.

Proof. We prove the claim by induction of the length of the derivation. Assume $U(A) \subseteq T_A$, $U(B) \subseteq T_B$, and consider a derivation step $\frac{A\ B}{A+B}$ (other derivation steps are trivial). We claim $U(A+B) \subseteq T_{A+B}$. Pick $E \in U(A+B)$. We have an expression:

$$E = A + B - \sum_{j=1}^{u} \pi_j \Gamma_j A - \sum_{j=1}^{u} \pi_j \Gamma_j B + \sum_{j} \sum_{k>j} \pi_k \Gamma_k \pi_j \Gamma_j A + \sum_{j} \sum_{k>j} \pi_k \Gamma_k \pi_j \Gamma_j B - ...$$

This expression splits naturally into two so we can write $E = E_A + E_B$. Now $E_A = \sum_j \pi_j^A E_{A,j}$ and $E_B = \sum_j \pi_j^B E_{B,j}$ where $E_{A,j} \in T_A$ and $E_{B,j} \in T_B$ and each π_j^A and π_j^B fixes the points outside $\{1, 2, ..., 7k\}$. Now $E_{A,j} + E_{B,j} \in T_{A+B}^{\text{aux}}$ for each j so E can be written as sum of objects (possible moved by $\pi \in S_{7k}$) in T_{A+B}^{aux}. Thus E can actually be written as sum of objects in T_{A+B}. This ensures $E \in T_{A+B}$ and thus completes the proof. ■

From Lemma 14, we immediately get the following lemma.

Lemma 15 *Let F and the set $\bar{E}$ consist of ultrasmalls. Then if $F_{n^*} \in [\bar{E}]_{n^*}$ for some $n^* \geq 7k$ then $F_n \in [\bar{E}]_n$ for all $n \geq 7k$.*

From Lemma 15, we obtain the following weaker version of Theorem 12 of independent interest, for fields $\mathbb{F}$ of any characteristic (including 0).

Theorem 16 *Take a uniformly generated submodule $[\bar{G}]_n$ of $\tilde{V}[\mathbb{F}, n, k, t]$ and a module element H in $\tilde{V}[\mathbb{F}, n, k, t]$, both of support size bounded by l. Now if $H_{n^*} \in [\bar{G}]_{n^*}$ (resp. $\notin$) for some $n^* \geq \max\{l + 3k, 7k\}$ then $H_n \in [\bar{G}]_n$ (resp. $\notin$) for every $n \geq \max\{l + 3k, 7k\}$.*

Proof. Since $H_{n^*} \in [\bar{G}]_{n^*}$, there is a derivation for H_{n^*} from $\bar{G}$. By Lemma 14 it follows that the ultrasmalls in $U(H)$ that form the formal compression of H can be derived from the ultrasmalls in $U(\bar{G})$ by a derivation of width at most $7k$. In other words, $[U(H)]_n \subseteq [U(\bar{G})]_n$ for all $n \geq 7k$. Since $\bar{G}$ and H have support size at most l, by Lemma 13, $H_n \in [U(H)]_n$ and $[U(\bar{G})]_n \in [\bar{G}]_n$ for $n \geq l + 3k$, and therefore the chain:

$$H_n \in [U(H)]_n \subseteq [U(\bar{G})]_n \subseteq [\bar{G}]_n$$

holds for $n \geq \max\{l + 3k, 7k\}$. ■

Now we prove a stronger version of Lemma 15, where F is replaced by F' that is only equivalent to F at n^*.

Lemma 17 *Let F and the set $\bar{E}$ consist of ultrasmalls. For some $n^* \geq (7+q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$, let F' be equivalent to F at n^*, with $F \succ F'$. Then if $F'_{n^*} \in [\bar{E}]_{n^*}$ then $F_n \in [\bar{E}]_n$ for all $n \geq (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ with $n \equiv_{q_{\mathbb{F}},k} n^*$.*

Proof.

We convert the derivation for F' into a derivation for F, moving top down and replacing intermediate module elements E, *whenever possible*, by appropriate, equivalent module elements $B \succ B'$. In the process of showing that a replacement is valid, one needs to show that the replacement can be carried out not only in the derivation tree at n^*, but more or less independent of n, i.e, for any $n \geq (7+q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ with $n \equiv_{q_{\mathbb{F}},k} n^*$.

Since relevant replacements are made whenever possible, and the axioms of the derivation $\bar{E}$ are ultrasmall, (and applying Lemma 14), we can assume that at any given step of the derivation where a replacement takes place, the old element $A+B'$ is replaced by an equivalent element $A+B \succ A+B'$, where B is ultrasmall. Note that A is not being replaced at the current step, and could have been partly replaced earlier, but may be inseparable from B in the derivation.

The proof is by induction on the number of replacements in the derivation of F'_{n^*} from $\bar{E}$ required to get a derivation of F from $\bar{E}$ as described above. The induction basis is Lemma 15. The induction step is carried out in 2 parts, analogous to the proof of Theorem 12 for the characteristic 0 case. Although F is itself ultrasmall, in the induction step, we need to consider intermediate replacements where $A+B'$ is replaced by $A+B$, where only B is ultrasmall.

Inducing Up Assume $n' \equiv_{q,k} n^*$ for some $n' > n^* \geq (7+q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$. We show that if $A+B'_{n^*} = A+B_{n^*}$ can be formally derived from $\bar{E}$, then $A+B_{n'}$ can be formally derived from $\bar{E}$.

We are given

$$A+B_{n^*} = \sum_{k=1}^{v} \sum_{a_j\pi_j} a_j \pi_j E_{kj}$$

where $a_j \in \mathbb{F}$ and we first assume that each π_j fixes points outside $\{1,2,...,n^*\}$. Let $7k \leq a \leq (7+q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ be an constant. We will specify its exact value later. For each (n^*-a)-element subset $W \subseteq \{a+1, a+2, ..., n'\}$ we let

$$(A+B_n^*)_W := \sum_{k=1}^{v} \sum_{a_j\pi_j} a_j \eta_W \pi_j E_{kj},$$

where $\eta_W : \{a+1, a+2, ..., n\} \to_{1-1} W \subset \{a+1, a+2, ..., n'\}$ is an arbitrary bijective (onto W) map. Notice that A might contain higher dimensional elements, but these have already been replaced and can thus be view as formal objects not depending on n.

We claim:

$$A+B_{n'} = \sum_{W \subseteq \{a+1,a+2,...,n'\}, |W|=n^*-a} (A+B_{n^*})_W.$$

To prove this, notice that:

$$\sum_{W \subseteq \{a+1,a+2,...,n'\}, |W|=n^*-a} (A+B_{n^*})_W = \binom{n'-a}{n^*-a} A + \sum_{W \subseteq \{a+1,a+2,...,n'\}, |W|=n^*-a} (B_{n^*})_W.$$

Consider a point $p = [i_1, i_2, ..., i_k] \in \{1,2,...,n'\}^k$. Assume p contains d' coordinates in $\{a+1, a+2, ..., n'\}$ and $k-d'$ coordinates in $\{1,2,...,a\}$. Let us compute the number of $W \subseteq \{a+1, a+2, ..., n'\}$ which have $p \in (B_{n^*})_W$.

Without loss of generality we can assume B_{n^*} is a single primitive element defined by:

$$\{(i_1, i_2, ..., i_{k-d}, j_1, j_2, ..., j_d) : j_1, j_2, ..., j_d \in \{1, 2, ..., n^*\}\}$$

for $i_1, i_2, ..., i_{k-d} \in \{1, 2, ..., 7k\}$. For general ultrasmalls B that are linear combinations of primitive elements, the proof extends straightforwardly. The point p lies on $(B_{n^*})_W$ if the first d coordinates of p is $i_1, i_2, ..., i_{k-d}$. The number of sets $W \subseteq \{a+1, a+2, ..., n'\}$ of size $n^* - a$ which contain d' points is $\binom{n'-a-d'}{n^*-a-d'}$. Now assume a was chosen such that $\binom{n'-a-j}{n^*-a-j} = 1$ modulo $q_{\mathbb{F}}$ for $j = 0, 1, 2, .., k$. Now there is an $s \in \mathbb{N}$ such that $n' - n^* = sq_{\mathbb{F}}^u$ where u is the smallest number with $q_{\mathbb{F}}^u \geq k$. It suffices to show we can always deal with the case where $n' = n^* + q_{\mathbb{F}}^u$. Thus it suffices to show there exists suitable a such that $\binom{n'-a-j}{q^u} = 1$ modulo $q_{\mathbb{F}}$ for $j = 0, 1, ..., k$.

Now clearly $\binom{q_{\mathbb{F}}^u}{j} = 0$ modulo $q_{\mathbb{F}}$ for $j = 1, 2, ..., q_{\mathbb{F}}^u - 1$. Thus $\binom{q_{\mathbb{F}}^u + j}{q_{\mathbb{F}}^u} = 1$ modulo $q_{\mathbb{F}}$ for $j = 0, 1, ..., q_{\mathbb{F}}^u - 1$ (to see this consider Pascal's triangle). The function $j \rightarrow \binom{j}{q_{\mathbb{F}}^u}$ has period $q_{\mathbb{F}}^{u+1}$ so for any $\tilde{l} \in \mathbb{N}$ we have $\binom{\tilde{l}q_{\mathbb{F}}^{u+1} + q_{\mathbb{F}}^u + j}{q_{\mathbb{F}}^u} = 1$ modulo $q_{\mathbb{F}}$ for $j = 0, 1, ..., q_{\mathbb{F}}^u - 1$. Now pick a such that $a = n' - \tilde{l}q_{\mathbb{F}}^{u+1} - q_{\mathbb{F}}^u - k$. We need $a \geq 7k$ so there always exists such an $a \leq (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ (note that $q_{\mathbb{F}}k - 1 \geq q_{\mathbb{F}}^u \geq k$, so $q_{\mathbb{F}}^2 k - q_{\mathbb{F}} \geq q_{\mathbb{F}}^{u+1} \geq q_{\mathbb{F}}k$). Thus if $n, n' \geq (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$, we can always choose $a \geq 7k$ such that $\binom{n'-j}{q^u} = 1$ modulo q for $j = 0, 1, ..., k(\leq q^u)$. ■

Inducing Down To complete the proof of the induction step, we need to show that the replacement of $A + B'$ by $A + B$ – where B is ultrasmall, equivalent to B' at n^* and $B \succ B'$ – can in fact be carried out at any n with $(7k + q_{\mathbb{F}}^2) - q_{\mathbb{F}} \leq n < n^*$, when $n \equiv_{q_{\mathbb{F}},k} n^*$. In other words, we need to show that if $A + B'_{n^*} = A + B_{n^*}$ can be derived from $\bar{E}$, and all replaceable (ultrasmall) module elements in the tree prior to $A + B'$ have been validly replaced – i.e, the Lemma holds for all of them, then in fact $A + B_{\tilde{n}} \in [\bar{E}]_{\tilde{n}}$, where $\tilde{n} < n^*$ is the largest number with $\tilde{n} \equiv_{q_{\mathbb{F}},k} n^*$.

We prove this by an inner induction on the dimension of B. This does not contradict the outer induction on the number of replacements in the derivation of $A + B'$: derivations of m dimensional ultrasmalls may theoretically contain replacements of intermediate elements of dimension greater than m, but as we shall see, the induction hypothesis is only applied to elements that depend on replacements that occurred prior to that of B.

The induction basis of the inner induction is if B contains no lines, planes, etc. and is proved by Lemma 15, since in this case, B' is in fact identical to B.

To prove the induction step of the inner induction, and complete the induction step of the outer induction, we first let $b = n^* - \tilde{n}$ and consider the derivation $\mathcal{T}_{n^*+b}$ of $A + B_{n^*+b}$, from $\bar{E}$. The existence of $\mathcal{T}_{n^*+b}$ has been proved by the "Inducing Up" part of the proof above. The derivation $\mathcal{T}_{n^*+b}$ contains $A + B'_{n^*+b}$ as an intermediate element, and its derivation $\mathcal{T}_{n^*}$ is a copy of the derivation $A + B'_{n^*}$ (which is being considered in the outer induction step). Since B itself is ultrasmall, notice that the difference $B_{n^*+b} - B'_{n^*+b}$ is equivalent to an ultrasmall Δ_{n^*+b} of dimension one less than that of B. Δ_{n^*+b} occurs as an intermediate node in $\mathcal{T}_{n^*+b}$, that depends (if at all) only on elements in $\mathcal{T}_{n^*}$ that occur prior to $A + B'_{n^*+b}$. Therefore, the (inner) induction hypothesis applies to Δ_{n^*+b}, and we can assume that Δ_{n^*} can be derived from $\bar{E}$. Moreover, Δ_{n^*} must appear as an intermediate node in $\mathcal{T}_{n^*}$.

Now we return to the derivation of $A+B'_{n^*} = A+B_{n^*}$ which is a copy of $\mathcal{T}_{n^*}$ (except that the summations in the non-zero dimensional elements or closed terms of A and B'_{n^*} now only go up to n^* instead of n^*+b). Now Δ_{n^*} and therefore $A+B'_{n^*} - \Delta_{n^*}$ which is equivalent to $A+B_{n^*} - \Delta_{n^*}$, must occur as elements prior to $A+B'_{n^*}$ in this derivation and hence the (outer) induction hypothesis applies to them. Thus Δ_{n^*-b} and $A+B_{n^*-b} - \Delta_{n^*-b}$ can be derived from $\bar{E}$, and hence $A+B_{n^*-b} = A+B_{\tilde{n}}$ can also be derived from $\bar{E}$.

■

Finally, we are ready to complete the proof of Theorem 12.

Proof (of Theorem 12 for fields $\mathbb{F}$ of finite characteristic).

The proof has the same structure as the proof of Theorem 16. Note that since H' (equivalent to H at n^*) can be generated from $\bar{G}$, it follows from Lemma 14 that some ultrasmall element equivalent (at n^*) to each element of $U(H)$ can be generated from $U(\bar{G})$. Now, by Lemma 17, it follows that each element of $U(H)$ can be generated from $U(\bar{G})$ for all $n \geq (7+q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ with $n \equiv_{q_{\mathbb{F}},k} n^*$.

The remainder of the proof is identical to that of Theorem 16. Since $\bar{G}$ and H have support size at most l, by Lemma 13, $H_n \in [U(H)]_n$ and $[U(\bar{G})]_n \in [\bar{G}]_n$ for $n \geq l+3k$, and therefore the chain:

$$H_n \in [U(H)]_n \subseteq [U(\bar{G})]_n \subseteq [\bar{G}]_n$$

holds for $n \geq \max\{l+3k, (7+q_{\mathbb{F}}^2)k - q_{\mathbb{F}}\}$, with $n \equiv_{q_{\mathbb{F}},k} n^*$. ■

V Other Applications

V.1 Lifting degree lower bounds for Polynomial Calculus

We now describe how to lift lower bounds on the degrees of Gröbner or Polynomial Calculus proofs of ideal membership of a target multi-linear polynomial in the ideal generated (modulo $x^2 = x$ for all variables x) by an S_n-closed, uniformly generated set of multi-linear polynomials in $\mathbb{F}[x,n,r]$. The PC case differ from the NS case in three important ways.

- The PS is dual to the NS in the following sense:

  In the NS case we showed that if two uniformly generated FS_n submodules $V_n \subseteq W_n$ are *different* for large n this also holds for small n. This followed from the inducing up, by showing that if the dual spaces V_n^o and W_n^o are identical from some small n^* then they must be identical for all large n with $n \equiv_{q_{\mathbb{F}},k} n^*$.

  In the PS case we have to show that if two uniformly generated FS_n submodules $V_n \subseteq W_n$ are *identical* for large n this also holds for small n. This (modulo some modifications) follows from the inducing down, without passing to dual spaces.

- In the NS case we had to consider linear subspaces closed under the group algebra $\mathbb{F}S_n$. In the PC case we have to prove that similar results are valid for linear subspaces which besides being closed under $\mathbb{F}S_n$ are closed under certain uniformly given, S_n-closed linear maps.
- In the PC-case it is an advantage to view on the appropriate FS_n-submodule as a subring of the polynomial ring.

These changes is relative minor and the corresponding result form the PC-case follows from the work we have already done.

Let $V_{n,\bar{r},d}$, $\bar{r} = (r_1, r_2, ..., r_u)$ denote the vector-space of multi-linear polynomials of degree $\leq d$ in the variables $x_{j,(i_1,i_2,...,i_{r_j})}$, $j = 1, 2, ..., u, i_1, i_2, ..., i_{r_j} \in \{1, 2, ..., n\}$. Given finitely many polynomials $Q_1, Q_2, ..., Q_v \in V_{n,\bar{r},d}$. The support size l_Q of a polynomial Q is the number of index in labels on variables in Q. The support $l_{\bar{Q}}$ is the support size of $Q_1, ..., Q_v$ added up. Let $r := max\{r_j : \ j = 1, 2, ..., u\}$. Let $k := rd$. Thus k still (like in section IV) denote the maximal number of index in module elements. An ultrasmall polynomial is a polynomial of support size $\leq 2k = 2dr$. A small polynomial has support size $l_{\bar{Q}}$ (typical larger than $2k$).

Our next major aim is to prove the following theorem:

Theorem 18 *A non-constant degree lower bound – for PC proofs of a multi-linear polynomial Q^*_n in the ideal generated by an S_n-closed, uniformly generated set of multi-linear polynomials (such as any set derived from a Universal Second Order sentence ψ) $\bar{Q}$ – lifts to a degree $d \geq \min\{\frac{n+q^2_{\mathbb{F}}}{(7+q^2_{\mathbb{F}})r}, \frac{n-l_{\bar{Q}}}{3}\}$ lower bound, where $l_{\bar{Q}}$ is the maximum of the support sizes of any of the polynomials in $\bar{Q}$, and that of Q^*.*

We depend on the following result of [7] (paraphrased).

Theorem 19 *(Clegg-Edmonds-Impagliazzo) There is a degree d PC proof of membership of a polynomial P^*_n in the ideal generated by $\bar{Q}_n$ (modulo $x^2 = x$ for all variables x) if and only if P^*_n belongs in a certain subspace $V_{n,d}(\bar{Q})$ defined as the smallest subspace of the space of degree d multi-linear polynomials that contains $\bar{Q}$ and is closed under the operations $M_{d,x}(P)$, acting on polynomials P and defined for each variable x: $M_{d,x}(P)$ maps P to the multi-linearisation of xP (under the rule $x^2 = x$) provided the resulting polynomial has degree at most d; otherwise $M_{d,x}(P)$ is undefined. It is assumed that P and P^* all have degree less than d.*

Suppose that an ultrasmall polynomial $P \in V_{n,\bar{r},d}$ can be derived (from FS_n-operations, and $M_{d,x}$-operations) from ultrasmall polynomials $Q_1, Q_2, ..., Q_u \in V_{n,\bar{r},d}$. We want to show that this ensures that there exists a controlled derivation of P which for example does not involve any pathological polynomials R, R', R''...

Lemma 20 *Given polynomials $Q_1, Q_2, ..., Q_v$ of support size $l_{\bar{Q}}$ and degree $\leq d'$. Then there is a collection $Q'_1, Q'_2, ..., Q'_{v'}$ of ultrasmall polynomials of degree $\leq d'$ such that for all $n \geq l_{\bar{Q}+3k}$ $[Q_1, Q_2, ..., Q_v]_n = [Q'_1, Q'_2, ..., Q'_{v'}]_n$.*

This lemma is almost identical to lemma 13. However in the PC-case we can express the result directly in term of multi-linear polynomials. We did not have that luxury in the NS case.

V.2 The Main Lemmas (the PC case)

In this section we briefly go through the similar lemma's from section 4. The lemmas required to complete the proof of Theorem 18 depend on the fact that uniformly generated submodules of $V_{n,\bar{r},d}$ are in fact generated by ultrasmall polynomials. Notice that the concept *generated* now also include closure under the operators $M_{d,x}$. Basically we continue the argument very similar to the NS-case. Once more we have to show that if an ultrasmall polynomial P' equivalent (this concept remain unchanged) to P with $P \succ P'$ generated by a set $\bar{Q}$ of ultrasmall polynomials for some large n^*, then, in fact, P is generated from $\bar{Q}$ at all n beyond a small constant in some residue class of n^*. Both the constant and the residue class depend only on $q_{\mathbb{F}}$ and (linearly) on k.

Compression (the PC case)

The next lemma shows that uniformly generated submodules (sequences) of $V_{n,\bar{r},d}$ that have generators of small support in fact have ultrasmall generators beyond a small value of n. We say we **compress** the collection of small objects into ultrasmall objects when we carry out this procedure.

Lemma 21 *Given an element Q of $V_{n,\bar{r},d}$ of support size l, there is a set $\bar{R}$ of ultrasmall generators such that for all $n \geq l + 3dr$, $[\bar{R}]_n = [Q]_n$.*

Proof More or less identical to the proof of lemma 13. ∎

A proof system for submodule membership

Let Q be and element and $\bar{R}$ a set of elements of $V_{n,\bar{r},d}$. Then a **formal derivation** of Q from $\bar{R}$ is defined as follows.

Given $Q \in V_{n,\bar{r},d}$, where $n \geq 2dr (= 2k)$. The **formal compression** of Q of support size l is a collection $U(Q)$ of ultrasmall (i.e support size $\leq 2k$) elements (i.e. polynomials) got by taking $Q_{n'}$ for some $n' \geq l + 3k$ (for instance $n' = n + 3k$) and then by applying the compression procedure to get a collection $R_1, R_2, ..., R_u \in V_{2k,\bar{r},d}$ of ultrasmalls such that $[Q]_{n'} = [R_1, R_2, ..., R_u]_{n'}$. We let $U(E) := \{R_1, R_2, ..., R_u\}$. For convenience we normally also assume $U(E)$ is closed under S_{2k} (i.e. $P \in U(Q) \Rightarrow \pi P \in U(Q)$ for $\pi \in S_{2k}$).

Now the argument continue almost identical to lemma 14. To make the behaviour of the operators $M_{d,x}$ more transparent we now express everything in terms of polynomials in $V_{n,\bar{k},d}$. Given any polynomial Q of $V_{n,\bar{k},d}$, with $P \in [\bar{Q}]_n$, and a formal derivation of P from $\bar{Q}$ in we assign a collection of ultrasmalls $T(W)$ at each intermediate module element W in the derivation as follows. To each "axiom" $Q_j \in \bar{Q}$ we assign $\{\pi Q_i, \pi \in S_{2k}\}$. The assignment of a conclusion $\frac{P}{\pi P}$ is unchanged (i.e. $T_{\pi P} = T_P$). The assignment of a conclusion $\frac{P}{cP}$ is given by: $T_{cP} := \{cR : R \in T_P\}$. The assignment $T_{P_1+P_2}$ to conclusion of an application of $\frac{P_1 \ P_2}{P_1+P_2}$ is obtained as follows: we have the assignments T_{P_1} and T_{P_2}, and we get

$$T^{\mathrm{aux}}_{P_1+P_2} := \{R : \exists \pi_1, \pi_2 \in S_{4k}, \exists R_1 \in T_{P_1}, R_2 \in T_{P_2} \ R = \pi_1 R_1 + \pi_2 R_2\}.$$

Notice that all objects in $T^{\mathrm{aux}}_{P_1+P_2}$ have support size $\leq 4k$. Now let $T_{P_1+P_2}$ consist of all ultrasmall polynomials which can be written as a linear combination of elements (possible moved by some $\pi \in S_{4k}$) in $U(T^{\mathrm{aux}}_{P_1+P_2})$. Notice that each object in $T_{P_1+P_2}$ has a derivation of width $\leq 7k (= 4k + 3k)$ from objects in $T^{\mathrm{aux}}_{P_1+P_2}$. Thus in general each object in T_W can be derived by a proof of width $\leq 7k$. The assignment T_{xP} to a conclusion of an application of $\frac{P}{xP}$ is obtained as follows: We have an assignment T_P of elements of support in $2k$. Let T^{aux}_{xP} be the collection of polynomials which appear by taking for each variable x of support in $\{1, 2, ..., 3k\}$ and each $R \in T_P$ the polynomial xR. Now let $T_{xP} := U(T^{\mathrm{aux}}_{xP})$.

Lemma 22 *For every polynomial W in the derivation, we have $U(W) \subseteq T_W$.*

Proof: Most of the lemma is proved exactly as lemma 14. The only new rule to consider is the rule $\frac{P}{xP}$. Assume $U(P) \subseteq T_P$. Then clearly $U(xP) \subseteq T^{\mathrm{aux}}_{xP}$. Now $U(xP) = U(U(xP)) \subseteq U(T^{\mathrm{aux}}_{xP}) = T_{xP}$. ■

From this lemma we immediately get the following:

Lemma 23 *Let P and the set $\bar{Q}$ consist of ultrasmall polynomials. Then if $P_{n^*} \in [\bar{Q}]_{n^*}$ for some $n^* \geq 7k$ then $P_n \in [\bar{Q}]_n$ for all $n \geq 7k$.*

Now we prove a stronger version of Lemma 23, where P is replaced by P' that is only equivalent to P at n^*.

Lemma 24 *Let P and the set $\bar{Q}$ consist of ultrasmalls. For some $n^* \geq (7+q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$, let P' be equivalent to P at n^*, with $P \succ P'$. Then if $P'_{n^*} \in [\bar{Q}]_{n^*}$ then $P_n \in [\bar{Q}]_n$ for all $n \geq (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ with $n \equiv_{q_{\mathbb{F}},k} n^*$.*

Proof As the proof of lemma 17. ■

This now proves Theorem 18 exactly like the final argument proving Theorem 12 in section IV.

V.3 Degree Lower bounds for proving Primality

Let ψ be a first order sentence which has a model of size n if and only if n is a composite number. For instance we can let ψ be the conjunction of the following sentences:

$\psi_1 :\equiv \forall z \exists! x, y\ A(x) \wedge B(y) \wedge f(x,y) = z$

$\psi_2 :\equiv \exists x, y\ x \neq y \wedge A(x) \wedge A(y)$

$\psi_3 :\equiv \exists x, y\ x \neq y \wedge B(x) \wedge B(y)$.

This system of sentences can (as we showed in Section 2) be translated into bounded degree polynomial equations. More specifically we get a system essentially similar to a system first considered in [13]:

For each $i, j \in \{1, 2, ..., n\}$ we have variables x_i, y_j and $v_{i,j}$. For each $i, j, k \in \{1, 2, ..., n\}$ we have a variable $z_{i,j,k}$.

The polynomials are:

(1) $Q^4_{i,j} :\equiv x_i y_j (1 - \sum\limits_k z_{ijk} - v_{i,j})$

(2) $Q^5_k :\equiv 1 - \sum\limits_{i,j} x_1 y_j z_{ijk}$

(3) $Q^6_{i_1,i_2,j_1,j_2,k} :\equiv x_{i_1} x_{i_2} y_{j_1} y_{j_2} z_{i_1,j_1,k} z_{i_2,j_2,k}$ for $i_1 \neq i_2$ or $j_1 \neq j_2$.

(4) $Q^7_{i,j,k_1,k_2} :\equiv x_i y_j z_{i,j,k_1} z_{i,j,k_2}$ for $k_1 \neq k_2$.

First using the conversion mechanism described in the proof of Theorem 18, we obtain a uniformly generated submodule sequence of $\tilde{V}[\mathbb{F}, n, k = 3d, 4]$ (k in this case is the maximum number of indices in any term, which is the number of indices of any variable ($r = 3$) times degree (d), and there are 4 variable types). The support size (l) of the generating elements is almost 5.

The following corollary of Theorem 12 improves the non-constant degree lower bound from [13] *directly* (i.e, without going through his non-constant degree lower bound and our lifting result Theorem 18):

Corollary 25 *For each n, there is no degree $\leq \min\{\frac{\mathrm{n+q_F}}{21+3\mathrm{q}_{\mathbb{F}}^2}, \frac{\mathrm{n-10}}{9}\}$ (i.e, $\leq \min\{\frac{\mathrm{n+q_F}}{(7+\mathrm{q}_{\mathbb{F}}^2)\mathrm{r}}, \frac{\mathrm{n-2l}}{3\mathrm{r}}\}$ Polynomial Calculus refutation proof of 'n is a prime'.*

Proof: The proposition 'n is a prime' fails (for any fixed m) for some n' in each residue class modulo $q^m_{\mathbb{F}}$. The proof follows from Theorem 12. ■

In Krajicek's encoding of primality (as a system of polynomial equations) is of course highly infeasible from a practical point of view. It would be interesting to consider degree lower bounds on proving primality when the number is represented in binary representation (rather than unary representation). Our methods does not settle this question.

An interesting problem

V.4 NS-degree and PC-degree lower bound on the onto-PHP

In this section we solve an open problem from [16]. First, however, we improve the n^ϵ NS-degree lower bound from [4].

Let P_{v,T_n}, $T_n \in \{1, 2, ..., n\}^k, v = 1, 2, ..u$ be a collection of uniformly generated polynomials closed under S_n. The describing variables in the polynomials P_{v,T_n}, $T = (i_1, i_2, ..., i_k)$ belongs to $\{i_1, i_2, ..., i_k\}$. Consider the question whether there is a sequence $\alpha_{T_n} \in \mathbb{F}$, such that $\sum\limits_{j,T_n} \alpha_{T_n}(1 + P_{v,T_n}) = 1$.

Example: Consider the polynomials $P_{(i_1,i_2,i_3)_n} := \sum\limits_j^n x_{i_1,i_2} x_{i_3,j} - x_{i_1,i_2} x_{i_3,i_3}$ for $i_1, i_2, i_3 \in \{1, 2, ..., n\}$ all different. Also consider the collection $P_{(i)_n} := \sum\limits_j^n x_{i,j} - x_{i,i}$. Each monomial corresponds to a branch in a decision tree like the ones introduced in [22]. The sum

$$\sum_{i_1}^{n}\sum_{i_2}^{n}\sum_{i_3}^{n} \alpha_{(i_1,i_2,i_3)}P_{(i_1,i_2,i_3)_n} + \sum_{i}^{n} \alpha_{(i)}P_{(i)_n} = 0$$

if and only if all monomials in the polynomial appears a number of times divisible by $\mathbb{F}$. Thus there is a sequence $\alpha_{(i_1,i_2,i_3)}, \alpha_{(i)}$ such that

$$\sum_{i_1}\sum_{i_2}\sum_{i_3} \alpha_{(i_1,i_2,i_3)}(1 + P_{(i_1,i_2,i_3)_n}) + \sum_{i} \alpha_{(i)}(1 + P_{(i)}) = 0$$

if and only if there exists an $q_{\mathbb{F}}$-exception forest of hight ≤ 2.

♣

We can rephrase Theorem 12 (using the fact that $l = k$, and thus $(7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}) \geq l + 3k)$ in the following form:

Theorem 26 *Let P_{v,T_n}, $T_n \in \{1, 2, ..., n\}^k, v = 1, 2, ..u$ be a uniformly given collection of polynomials closed under S_n. Let m denote the smallest integer such that $q^m \geq k$ and let $0 \leq r < q^m$.*

The the following are equivalent:

For some $n^* \geq (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ with $n^* = r$ modulo $q_{\mathbb{F}}^m$ there is a sequence $\alpha_{T_{n^*}} \in \mathbb{F}$, such that $\sum_{j,T_n} \alpha_T P_{v,T_n} = 0$, but such that $\sum_{j,T_n} \alpha_{j,T_n} \neq 0$.

For all $n \geq (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}$ with $n = r$ modulo $q_{\mathbb{F}}^m$ there is a sequence $\alpha_{T_n} \in \mathbb{F}$, such that $\sum_{j,T_n} \alpha_T P_{v,T_n} = 0$, but such that $\sum_{j,T_n} \alpha_{j,T_n} \neq 0$.

This immediately allows us to give improved NS-degree lower bounds on the following systems of equations which were considered in [4].

Let D and R be two finite sets. Let $D = \{1, 2, ..., d\}$ and let $R = \{1, 2, ..., r\}$. In [4] close upper and lower bounds on NS-refutations of onto-PHP_r^d are given:

Proposition 27 (Beame, Riis) *If p is prime and $p^\ell \leq N$, there is a Nullstellensatz refutation of* $\mathrm{onto} - \mathrm{PHP}_N^{N+p^\ell}$ *of degree $p^\ell - 1$.*

Proposition 28 (Beame, Riis) *If $N \geq ((p_{\mathbb{F}} + 2)^\ell - p_{\mathbb{F}}^\ell)/2$ then any Nullstellensatz refutation of* $\mathrm{onto} - \mathrm{PHP}_N^{N+p_{\mathbb{F}}^\ell}$ *over $\mathbb{F}$ must have degree at least $2^\ell - 1$.*

These propositions essentially reduces to giving upper and lower bounds for the degree of the NS proof for the following system of equations:

Let $D := \{1, 2, ..., N + p_{\mathbb{F}}^\ell\}$ and let $R := \{1, 2, ..., N\}$.

$Q_{d,r}^1 :\equiv x_{d,r}^2 - x_{d,r}$ for $d \in D, r \in R$.

$Q_d^2 :\equiv \sum_{r \in R} x_{d,r} - 1$ for $d \in D$.

$Q_{d,r_1,r_2}^3 :\equiv x_{d,r_1}x_{d,r_2}$ for $d \in D, r_1, r_2 \in R$ with $r_1 \neq r_2$.

$Q_{d_1,d_2,r}^4 :\equiv x_{d_1,r}x_{d_2,r}$ for $d_1, d_2 \in D, r \in R$ with $d_1 \neq d_2$.

$Q^5_r :\equiv \sum_{d \in D} x_{d,r} - 1$ for $r \in R$.

Now this system of equations is uniformly given (for fixed ℓ) with the group S_n operating on $\{1, 2, ..., N + p^{\ell}_{\mathbb{F}}\}$ by fixing the last $p^{\ell}_{\mathbb{F}}$ numbers. Now $r = 3$ so as a corollary to Theorem 12 we get a linear degree lower bound:

Corollary 29 *For $N \geq (21 + 3p^2_{\mathbb{F}})(2^{\ell} - 2) - p_{\mathbb{F}}$ any NS-degree refutation proof of* $\text{onto} - \text{PHP}^{N+p^{\ell}_{\mathbb{F}}}_N$ *must have degree at least $2^{\ell} - 1$ over $\mathbb{F}$.*

Now we show that the combinatorics developed in [22], [23] actually is sufficient to give a non-constant degree lower bound for Polynomial Calculus refutations of the onto-PHP. For this section we recomend to have [22] at hand.

We want to show that the constant polynomial 1 not can be generated from the polynomials Q^i_{α} we already have defined above. Now let I be the ideal generated by the polynomisals Q^3_{d,r_1,r_2} and $Q^4_{d_1,d_2,r}$.

Consider PC-degree lower bounds in $\mathbb{F}[\bar{x}]/I$. Now $M_{x_{s',r'}}(\sum_r x_{s,r} - 1) = \sum_r x_{s,r}x_{s',r'} - x_{s',r'}$. Continuing iterating M_x we see that anything which can be generated (including closure under $\frac{P}{xP}$) from $Q_1, Q_2, .., Q_u$ (modulo I) really is generated (as a $\mathbb{F}S_n$-module) by all expressions of one of the forms:

$Q :\equiv \sum_{r \in R} x_{d_1,r_1}x_{d_2,r_2}....x_{d_{h-1},r_{h-1}}x_{d_h,r} - x_{d_1,r_1}x_{d_2,r_2}....x_{d_{h-1},r_{h-1}}$

$Q' :\equiv \sum_{d \in D} x_{d_1,r_1}x_{d_2,r_2}....x_{d_{h-1},r_{h-1}}x_{d,r_h} - x_{d_1,r_1}x_{d_2,r_2}....x_{d_{h-1},r_{h-1}}$.

Now consider a **PU**-tree as it was defined in [22] or [23]. Such a tree corresponds to a polynomial P_T: The tree $T = (d_1, r_1)(d_2, r_2)...(d_{h-1}, r_{h-1})(r_h)$ contain labelled branches corresponding to the monomials in

$$P_T := \sum_{d \in D} x_{d_1,r_1}x_{d_2,r_2}...x_{d_{h-1},r_{h-1}}x_{d,r_h} + \sum_{r \in R, r \neq r_{h-1}} x_{d_1,r_1}x_{d_2,r_2}...x_{d_{h-2},r_{h-2}}x_{d_{h-1},r} +$$

$$+ ... + \sum_{r \in R, r \neq r_1} x_{d_1,r}.$$

Now both Q and Q' can be written on the form $P_T - P_{T'}$. More specifically we can write $Q \equiv P_{(d_1,r_1)(d_2,r_2)...(d_{h-1},r_{h-1})(d_h)} - P_{(d_1,r_1)(d_2,r_2)...(d_{h-1})}$. And $Q' \equiv P_{(d_1,r_1)(d_2,r_2)...(d_{h-1},r_{h-1})(r_h)} - P_{(d_1,r_1)(d_2,r_2)...(d_{h-1})}$. Thus we have:

Lemma 30 *For any polynomial R of degree $\leq \bar{d}$, and for any polynomial $Q^2_{(d)} \equiv \sum_{r \in R} x_{d,r} - 1$ (or $Q^5_{(r)} \equiv \sum_{d \in D} x_{d,r} - 1$) there exists two* **PU**-*trees T, T' of height $\leq \bar{d} + 1$ such that $P_T - P_{T'} = RQ^2_{(d)}$ (or $P_T - P_{T'} = RQ^5_{(r)}$) modulo I.*

Translating the main result on **PU**-trees from [23] into this setting we get:

Lemma 31 *Let D and R be two finite sets. Let $D = \{1, 2, ..., d\}$ and let $R = \{1, 2, ..., r\}$. Let $\tilde{T}_v(d, r)$ (or just $\tilde{T}_v$) denote the collection of D, R-labelled* **PU**-*trees of height $\leq v$. For each T let P_T denote the multi-linear polynomial corresponding to T. Suppose that $r = d + q^m$. Then there is no sequence $\{\lambda_T\}_{T \in \tilde{T}_{2m}}$ such that*

$$\sum_{T \in \tilde{T}_{2m}} (1 + P_T) = 1.$$

Lemma 32 *There is no sequence of constant degree Polynomial Calculus proofs P_n of* $\text{onto} - \text{PHP}_n^{n+q^m}$ *over a field $\mathbb{F}$ of characteristic q.*

Proof: We have to show 1 does not belong to $V_{d,\bar{r},n}$. Anything we generate is a collection polynomials P_T. If we could generate 1 we could generate a sequence λ_T, $T \in \tilde{T}_d$ such that $\sum_T \lambda_T \; P_T = 1$. Thus we would have a forest of **PU**-labelled trees where each branch appear 0 modulo $q_{\mathbb{F}}$ times and where the total number of trees would be 0. (To get the last claim notice that we alway generate a positive as well as a negative tree whenever we multiply something by Q_d^2 or Q_r^5). Thus $\sum_T \lambda_T \; (1 + P_T) = 1$ which would contradict lemma 31. ■

These gives us the main result in this subsection which answers an open question [16]:

Theorem 33 *For $N \geq (21 + 3p_{\mathbb{F}}^2)(2^\ell - 2) - p_{\mathbb{F}}$ any PC-degree refutation proof of* $\text{onto} - \text{PHP}_N^{N+p_{\mathbb{F}}^\ell}$ *must have degree at least $2^\ell - 1$ over $\mathbb{F}$.*

We can apply this result as in [23] and obtain a series of new PC-degree lower bounds on the relative strength between various versions of the matching principles.

VI Related Representation Theory Problems

Several natural theorems and conjectures on the asymptotic behavior of representations of S_n arise from the discussion of this paper. These are of independent interest, and related results appear in [9].

The following theorem has been proven by the results of this paper.

Theorem 34 *Let $[\bar{G}]_n$ and $[\bar{H}]_n$ be two uniformly generated submodule (sequence)s of $\tilde{V}[\mathbb{F}, n, k, t]$ with support size at most l. Then there is an $n^* \geq \max\{l + 3k, (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}\}$ with $[\bar{G}]_{n^*} = [\bar{H}]_{n^*}$ if and only if $[\bar{G}]_n = [\bar{H}]_n$ for all $n \geq \max\{l + 3k, (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}\}$ with $n \equiv_{q,k} n^*$.*

A stronger version of this theorem is the following conjecture. This statement can be viewed as a a stronger version of Theorem 34, where the uniformly generated module $[\bar{H}]_n$ is replaced by an arbitrary submodule of $\tilde{V}[\mathbb{F}, n, k, t]$.

Conjecture 1 *Let $[\bar{G}]_n$ be a uniformly generated submodule (sequence) of $\tilde{V}[\mathbb{F}, n, k, t]$, and let $[\bar{G}]_\infty$ be the union of this sequence. Let $\tilde{W}_n$ be $[\bar{G}]_\infty \cap \tilde{V}[\mathbb{F}, n, k, t]$ (Note that this module need not be identical to $[\bar{G}]_n$). Then, for $n \geq \max\{l + 3k, (7 + q_{\mathbb{F}}^2)k - q_{\mathbb{F}}\}$ with $n \equiv_{q,k} n^*$, $[\bar{G}]_n = \tilde{W}_n$.*

The following conjecture is easily shown to be true for $q_{\mathbb{F}} = 0$, see [9], and also see Theorem 1 in Section I, but remains unsolved for other characteristics.

Conjecture 2 *There is a finite set $\mathcal{D}_k$ of polynomials depending on k (of cardinality exponential in k), such that given any submodule $\tilde{W}$ of $\tilde{V}[\mathbb{F}, n, k, t]$, there is a polynomial $p_{\tilde{W}} \in \mathcal{D}_k$ such that the dimension of $\tilde{W}$ is $p_{\tilde{W}}(n)$.*

Proof (for characteristic 0): We only give an outline the proof which essentially follows from the representation theory of the symmetric group: Let $E(k)$ denote the class of equivalence relations on $\{1, 2, ..., k\}$. Let $\mathrm{Cl}(\approx)$ denote the number of equivalence classes in $\approx$. For each equivalence relation $\approx \in E(k)$, let $V_{n,k,\approx}$ denote the linear subspace ($\mathbb{F}S_n$-submodule) of $V_{n,k} := \tilde{V}[\mathbb{F}, n, k, 1]$, where $\mathbb{F}$ has characteristic 0. which is generated by the vectors $e_{(i_1, i_2, ..., i_k)}$ where $i_j = i_k$ if and only if $j \approx k$. Thus we have

$$V_{n,k} = \oplus_{\approx \in E(k)} \; V_{n,k,\approx}.$$

In the standard literature [11] on representation theory of S_n, the modules M^β usually denotes the vector space generated by the so-called β-tabloids. Clearly (having digested the underlying definitions)

$$V_{n,k,\approx} = M^{(n,1^{\mathrm{cl}(\approx)})}.$$

Now we employ the rich theory for decomposing modules of the form $M^{(n,1^j)}$ into their irreducible components. The irreducible components (for fields of characteristic 0) consists of the so-called Specht-modules S^λ. There are typically infinitely many different decompositions of $V_{n,k}$ into irreducible components. However all these decompositions are isomorphic so the multiplicities of each S^β is bounded by estimating its multiplicity in each $M^{(n,1^{\mathrm{cl}(\approx)}}$. Now this multiplicity is independent of n for $n \geq 2k$. Furthermore Hook's formula allows us to show that each irreducible component $S^{n-i_1, i_2, .., i_l}$, $n - i_1 \geq i_2 \geq ... \geq i_l$ has a dimension which is polynomial in n.

Thus for each partitioning $\lambda = (n - i_1, i_2, ..., i_l)$ there is a polynomial $p_\lambda(n) \in \mathbb{Q}[x]$ such that $\dim(S^\lambda) = p_\lambda(n)$. Suppose that the multiplicities of S^λ in the decomposition of $V_{n,k}$ is c_λ. Now for each assignment $\lambda \to b_\lambda$ (where $0 \leq b_\lambda \leq c_\lambda$), we introduce a polynomial $p(n) := \sum\limits_\lambda \; b_\lambda p_\lambda(n)$.

Each submodule $W \subseteq V_{n,k}$ can uniquely (up to isomorphism) be decomposed into Specth modules. Thus there exists a choice of multiplicities $0 \leq b_\lambda \leq c_\lambda$ such that

$$\dim(W) = \sum_\lambda \; b_\lambda p_\lambda(n).$$

The number of λ's which appear in the decomposition is bounded by the number of partitionings of $2k$. The total number $\tau(k)$ of polynomials is thus bounded by an expression which is independent of n. ■

The following conjecture will follow with additional work, from Conjecture 1, and would give an alternative, more elegant proof of the main technical result of this paper, i.e, Theorem 12.

Conjecture 3 *Given any uniformly generated submodule $[\bar{G}]_n$ of $\tilde{V}[\mathbb{F}, n, k, t]$, there is a single polynomial p_G such that for all $n \geq lin(k)$ in some residue class of $q_{\mathbf{F}}^m$, the dimension of $[\bar{G}]_n$ is $p_G(n)$. We would like that lin is a linear function and m is a small constant. We would expect different polynomials p_G for different residue classes.*

VII Appendix

8	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
6	2	1	4	3	7	1	0	0
5	2	5	1	4	8	3	0	0
4	1	7	2	5	5	5	5	5
3	1	0	6	3	3	3	3	3
2	3	1	6	4	2	4	0	0
1	1	2	7	2	4	1	0	0
	1	2	3	4	5	6	7	8

Figure 1: The generator E

xx

8	0	0	0	0	0	0	0	0
7	2	1	4	3	7	0	1	0
6	0	0	0	0	0	0	0	0
5	2	5	1	4	8	0	3	0
4	1	7	2	5	5	5	5	5
3	1	0	6	3	3	3	3	3
2	3	1	6	4	2	0	4	0
1	1	2	7	2	4	0	1	0
	1	2	3	4	5	6	7	8

Figure 2: $(6,7)E$

8	0	0	0	0	0	0	0	0
7	2	1	4	3	7	0	1	0
6	-2	-1	-4	-3	-7	-1	0	0
5	0	0	0	0	0	-3	3	0
4	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
2	0	0	0	0	0	-4	4	0
1	0	0	0	0	0	-1	1	0
	1	2	3	4	5	6	7	8

Figure 3: $E_1 := (6,7)E - E$

8	0	0	0	0	0	-1	1	0
7	0	1	4	3	7	0	1	2
6	0	-1	-4	-3	-7	-1	0	-2
5	0	0	0	0	0	-3	3	0
4	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
2	0	0	0	0	0	-4	4	0
1	0	0	0	0	0	0	0	0
	1	2	3	4	5	6	7	8

Figure 4: $E_2 := (1,8)E_1$

8	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
6	-2	2	0	0	0	0	0	0
5	2	-2	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
2	0	0	0	0	-1	1	0	0
1	0	0	0	0	1	-1	0	0
	1	2	3	4	5	6	7	8

Figure 5: $E_3 := (7,6,5)(E_2 - E_1)$

8	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
6	0	3	4	3	7	1	0	0
5	4	3	1	4	8	3	0	0
4	1	7	2	5	5	5	5	5
3	1	0	6	3	3	3	3	3
2	3	1	6	4	1	5	0	0
1	1	2	7	2	5	0	0	0
	1	2	3	4	5	6	7	8

Figure 6: $E' := E + E_3$

References

[1] Ajtai, M.: The independence of the modulo p counting principles. In Proceedings of the 26th ACM STOC, 402-411 (1994)

[2] Beame, P., Cook, S., Edmonds, R., Impagliazzo, R., Pitassi, T.: The relative complexity of NP search problems. In Procedings of the 27th ACM STOC, 303-314 (1995)

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

[4] Beame, P., Riis, S.: More on the relative strength of counting principles. In: Proceedings of the DIMACS workshop on Feasible Arithmetic and Complexity of Proofs, (1996)

[5] Buss, S., Krajicek, j,. Pitassi, T., Razborov, A., Sergal, J.: Polynomial bound on Nullstellensatz for counting principles. To appear in Computational Complexity (1997)

[6] Bonet, M., Pitassi, T., Raz, R.: No feasible interpolation for TC^0 Frege. In: Procedings of the 38th FOCS (1997)

[7] Clegg, M., Edmonds, j., Impagliazzo, R.: Using the Groebner basic algorithm to find proofs of unsatisfiability. In: Procedings of the 28th ACM STOC 174-183 (1996)

[8] Börger, E., Grädel, E., Gurevich, Y.: The Classical Decition Problem: Book in Series of Perspectives in Mathematical Logic, Springer (1996)

[9] Gagola, S., Lewis, M., Riis, S., Sitharam, M.: In progress.

[10] Iwama, k.: Complexity of Finding Short Resolution Proofs. In Proc. 22nd Symposium on Mathematical Foundation of Computer Sceince (MFCS'97) (to appear).

[11] James, G.: The Representation Theory of the Symmetic Groups. Lecture Notes in Mathematics., Vol. 682, Springer-Verlag, (1978)

[12] Krajicek, J.:Bounded Arithmetic, propositional logic, and complexity theory, Encyclopedia of Mathematics and Its Applications, Vol. 60, Cambridge University Press (1995)

[13] Krajicek, J.: On the degree of ideal membership proofs from uniform families of polynomials over a finite field (manuscript)

[14] Leitsch, A.: The resolution Calculus. Book in the series of Texts in Theoretical Computer Science, Ed. Brauer, W., Rozenberg, G., Salomaa, A. Springer / Heidelberg (1996)

[15] McCune, W., Padmanablan, R.: Automated deduction in equational logic and cubic curves. Lecture Notes in Computer Science, 1095 Springer-Verlag, Berlin (1996)

[16] Razborov, A.: Lower bounds for the polynomial calculus (manuscript)

[17] Razborov, A.: Unprovability of lower bounds on circuit size in certain fragments of Bounded Arithmetic Izvestiya: Mathematics 59:1 205-227 (1995)

[18] Razborov, A.: Lower bounds for propositional proofs and independence results in Bounded Arithmetic. In Proceedings of 23th ICALP Lecture Notes in Computer Science, 1099, 48-62 New Your/ Berlin, 1996. Springer-Verlag.

[19] Razborov, A. Widgerson, A., Yao, A.: Read-once brancing programs, rectangular proofs of the pigeonhole principle and transversal calculus. In Proceedings of the 29th ACM STOC (1997)

[20] Riis, S.: Making infinite structures finite in models of Second Order Bounded Arithmetic. In: Arithmetic, proof theory and computorial complexity, 289-319, Oxford: Oxford University Press 1993

[21] Riis, S.: Independence in Bounded Arithmetic. DPhil dissertation, Oxford University (1993)

[22] Riis, S.: Count(q) does not imply Count(p) to appear in Annals of Pure and Applied Logic.

[23] Riis, S.: Count(q) versus the pigeon-hole principle. Archive for Mathematical Logic **36** 157-188 (1997)

[24] Riis, S.: Automated Theorem Proving via Algebra and Representation Theory: In progress.

[25] Smolensky, R.: Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In the 19th ACM STOC, 77-82 (1987)