Uniform families of polynomial equations over a finite field and structures admitting an Euler characteristic of definable sets *†

Jan Krajíček‡

Mathematical Institute, Academy of Sciences
Žitná 25, Prague, 115 67, The Czech Republic
and
Mathematical Institute, Oxford University
24-29 St.Giles', Oxford, OX1 3LB, U.K.

Abstract

We consider families of polynomial equations $f_i(x_1, \ldots, x_{n_N}) = 0$, $i = 1, \ldots, k_N$, over a fixed finite field $\mathbf{F}_p$ that are uniformly determined by a parameter N. The notion of a uniform family is defined in terms of first-order logic.

We give a sense, using a notion of an abstract Euler characteristic, to a statement that the system has a solution for infinite N, and we prove a statement linking the solvability of a linear system for infinite N with its solvability for finite N.

Using this characterisation we formulate a criterion yielding degree lower bounds for various ideal membership proof systems (e.g., Nullstellensatz and the polynomial calculus).

Further we prove several results about Euler structures (structures with an abstract Euler characteristic) and investigate more closely, in particular, the case of fields.

*1991 Mathematics Subject Classification. Primary 03F20, 12L12, 15A06; Secondary 03C99, 12E12, 68Q15, 13L05.

†**Keywords:** finite fields, polynomial ideals, degree lower bounds, uniform polynomial systems, Euler characteristic, propositional proof complexity, Nullstellensatz, polynomial calculus, fields.

‡Partially supported by cooperative research grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech republic) and by the grant #A1019602 of the Academy of Sciences of the Czech Republic. Written while the author was funded by the EPSRC fellowship number GR/L01176.

Introduction

Consider the following system of polynomial equations over a finite prime field $\mathbf{F}_p$. Fix a parameter $N \geq 1$ (identified with $\{0, 1, \ldots, N-1\}$). The variables of the system $\neg PHP_N$ are x_{ij}, where $i \in N$ and $j \in N \setminus \{0\}$. The system consists of the following polynomials:

1. $Q_{ij} := x_{ij}^2 - x_{ij}$, all i, j.
2. $Q_{i_1,i_2,j} := x_{i_1 j} x_{i_2 j}$, all $i_1 \neq i_2$, j.
3. $Q_{i,j_1,j_2} := x_{ij_1} x_{ij_2}$, all i, $j_1 \neq j_2$.
4. $Q_i := 1 - \sum_j x_{ij}$, all i.

and the equations are stating that all these polynomials are zero. We identify a polynomial system $\{F_i\}_i$ with the system of equations $\{F_i = 0\}_i$.

The system is unsolvable for all N: by the first equations each x_{ij} is either 0 or 1, by the remaining equations the set $\{(i,j) \mid x_{ij} = 1\}$ is a graph of an injective mapping from N into $N \setminus \{0\}$, violating the pigeonhole principle (hence the name $\neg PHP_N$).

Now take for N an infinite set containing a constant 0. The definition of variables as well as of polynomials make a good sense: the equations are indexed by tuples of elements of N and the conditions defining which monomial occurs with which coefficient in a polynomial are defined in terms of equalities and inequalities among indices (making a sense over any set N). For infinite N however, $\neg PHP_N$ has intuitively a solution as there are injective maps from N into $N \setminus \{0\}$.

This appears to have nothing to do with equations but just with simple properties of infinite cardinalities. However, we shall consider N equipped with structures (most often with a field structure in this paper) and we only take those solutions (i.e., injective maps avoiding 0) that are definable in the structure. Furthermore we shall require that there is a consistent way of assigning "cardinalities" with values in $\mathbf{F}_p$ to definable sets so that one can verify using such a cardinality modulo p function that a solution indeed satisfies the equations. This leads to the notion of an abstract Euler characteristic on a first-order structure. An example of a structure admitting such an Euler characteristic (with values in $\mathbf{Z}$, in fact) is the real field $\mathbf{R}$ in the language of ordered rings (see Example 2.3).

We show that the solvability of a system of linear equations in $\mathbf{F}_p$ for N (finite or infinite) depends only on r modulo a fixed power p^ν of p, where r is the Euler characteristic given to (structure) N (in finite case this is just the cardinality modulo p^ν). The implicit connection between finite and infinite N is caused by the uniformity of the definition of the linear system. The notion of uniformity is defined in (simple) terms of first-order logic (or, equivalently, in a combinatorial way). The proof of this theorem is based on a generalisation (from finite sets to Euler structures) of some results on tabloid modules and Specht modules (cf.[25]) by [2, 28].

Our main motivation for this work was the question to establish degree lower bounds for various ideal membership proof systems (over various fields F). A proof system seeks to prove that $f_0 \in \langle f_1, \ldots, f_k \rangle$, given $f_i \in F[\overline{x}]$. A proof of the ideal membership in the so called *Nullstellensatz proof system* (cf.[5]), abbreviated NS, is a k-tuple $g_1, \ldots, g_k$ of polynomials from $F[\overline{x}]$ such that $\sum_{i \geq 1} g_i \cdot f_i = f_0$. A proof of the ideal membership in *polynomial calculus* (or Gröbner calculus as it is called in [11], cf. also [6]), abbreviated PC, is a sequence of polynomials $h_1, \ldots, h_t$ such that $h_t = f_0$, and such that every h_j is either one of $f_1, \ldots, f_k$, or is derived from earlier $h_1, \ldots, h_{j-1}$ by one of the two rules: g_1, g_2 entail any F-linear combination of g_1, g_2, and g entails any $x_i \cdot g$.[1]

A suitable measure of complexity of proofs turned out to be the maximum degree of a polynomial from the proof; $\max_{i \geq 1} deg(g_i f_i)$ in NS and $\max_i deg(h_i)$ in PC. Some bounds for NS and PC were established (cf.[5, 4, 6, 34, 28, 23]). If f_i's are given uniformly in N then the existence of a degree d NS or PC proof of the ideal membership is equivalent to the solvability of a linear system, also uniform in N (cf.[5], [28]). Thus our criterion, together with examples constructed here, yields new proofs for some of the known degree lower bounds, as well as some new bounds. It allows us to replace finite combinatorics by geometric considerations.

The study of algebraic proof systems such as NS or PC originated from a research in complexity of propositional logic and in related theory of bounded arithmetic (cf.[27]). In fact, the criterion we prove (Theorem 6.1) was first guessed from a somewhat analogous situation in bounded arithmetic. There is an infinitary criterion yielding independence results for bounded arithmetic theory $S^2_2(\alpha)$ and lower bounds for corresponding proof system and for particular search trees (cf.[35] and [27, Sec.11.3]). As it is not difficult to observe that NS over $\mathbf{F}_p$ corresponds to an extension of $S^2_2(\alpha)$ by the so called counting modulo p principle, one expects a similar criterion linking NS and infinite structures satisfying such a counting principle. We shall, however, not pursue this connection here as the proof we give does not use any bounded arithmetic.

Although our main motivation lies in ideal membership proof systems, we devote a large part of the paper to the development of the notion of Euler structures, a first-order structure M augmented by an abstract Euler characteristic χ of its definable sets. We give a sufficient condition on M guaranteeing that some (M, χ) is an Euler structure, and we show that the existence of such an expansion is a property of the theory of M rather than of M itself. Further we consider various classes of fields (real closed, algebraically closed, finite and pseudo-finite, p-adic) and prove several existence and non-existence theorems about Euler characteristics on them. We also consider definable dependence of

[1] The corresponding rule in the definition of PC in [6] allows to infer $g' \cdot g$, any $g' \in F[\overline{x}]$; as we are interested in the maximum degree of polynomials in a PC-proof, this makes no difference.

Euler characteristic on parameters.

The paper is organised as follows. The definition of uniform polynomial systems and some examples of these are given the first section. Euler structures are defined and studied in the second and the third sections. The solvability criterion is proved in the fourth section. The fifth section studies Euler structure properties of various fields. Degree lower bounds for NS and PC are considered in the sixth section. The last section concerns the definability of the Euler characteristic.

The reader interested only in degree lower bounds may skip Sections 3, 5 and 7, while the reader interested only in Euler structures may skip Sections 4 and 6.

Remarks on the notation: N is identified with $\{0, \ldots, N-1\}$ and $[N]^m$ denotes the set of m-element subsets of N. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ are the rings of integers, and the fields of rationals, reals and complex numbers respectively. Their language is the language of rings $0, 1, +, \cdot, =$ except for $\mathbf{R}$ whose language is the language of ordered rings containing also $<$. $\mathbf{F}_p$ is the p-element finite field, $\tilde{\mathbf{F}_p}$ is its algebraic closure. $\mathbf{Q}_p$ and $\mathbf{Z}_p$ are the p-adics and the p-adic integers. $\mathbf{Z}/m$ is the ring of integers modulo m. $\mathbf{F}_p G$ is a group algebra, M^μ and S^μ are the tabloid module and the Specht module ([25]). Finally, NS and PC are the ideal membership proof systems defined earlier.

1 Uniform systems of polynomials

Consider first two more polynomial systems, to have a few examples illustrating the general definition of a uniform system.

Example 1.1 *Let $N \geq m \geq 2$. The variables of the system $\neg Count_m^N$ are x_e, where e ranges over $[N]^m$. The system consists of the following polynomials:*

1. $Q_e \ := \ x_e^2 - x_e$ *, for each e.*
2. $Q_{e,f} \ := \ x_e \cdot x_f$ *, for every e, f such that $e \cap f \neq \emptyset$ but $e \neq f$.*
3. $Q_i \ := \ 1 - \sum_{e:\ i \in e} x_e$ *, for each $i \in N$.*

Assume that $x_e \ := \ a_e$ is a solution of the system $\neg Count_m^N$ in some integral domain. Then by equations $Q_e = 0$ all a_e are 0 or 1, and by the remaining equations the set

$$\{e \in [N]^m \mid a_e = 1\}$$

is a partition of N into m-element sets. Thus the system has a solution iff m divides N.

Now we shall construct another example of a uniform system. Take $\neg Count^N_m$ over a field F. By Nullstellensatz, for N not divisible by m, the ideal generated by the system is improper (the same holds for all N in the case of $\neg PHP_N$). Hence there are polynomials P_e, $P_{e,f}$ and P_i such that

$$\sum_e P_e Q_e + \sum_{e,f} P_{e,f} Q_{e,f} + \sum_i P_i Q_i = 1$$

holds in the ring $F[\overline{x}]$.

Fix $d \geq 2$ (2 is the maximum degree of polynomials in $\neg Count_m$) and for any monomial α (an unordered tuple of variables with repetitions) of degree at most d, identified with unordered tuples of not necessarily distinct elements of $[N]^m$, take variables $u_{\alpha,e}$, $v_{\alpha,e,f}$ and $w_{\alpha,i}$. Their intended meaning is to denote the coefficient of the monomial α in the polynomials P_e, $P_{e,f}$ and P_i respectively.

Example 1.2 *The following linear polynomial expresses the coefficient of β in the Nullstellensatz expression above:*

$$\sum_{\alpha,e:\beta=\alpha\cup\{e,e\}} u_{\alpha,e} - \sum_{\alpha,e:\beta=\alpha\cup\{e\}} u_{\alpha,e} + \sum_{\alpha,e,f:\beta=\alpha\cup\{e,f\},e\perp f} v_{\alpha,e,f} +$$

$$\sum_{\alpha,i:\beta=\alpha} w_{\alpha,i} - \sum_{\alpha,e,i:\beta=\alpha\cup\{e\},i\in e} w_{\alpha,i} \ .$$

Denote by $NS(d, \neg Count_m)^N$ the linear system consisting of the equations saying that all these polynomials are zero for all β of degree at most d, except for the constant monomial 1 (represented by $\beta = \emptyset$) for which the equations requires the value 1 (the right-hand side of the Nullstellensatz expression above).

$NS(d, \neg Count^N_m)$ is solvable iff there are polynomials P_e, $P_{e,f}$ and P_i such that the maximum degree of $P_e Q_e$, $P_{e,f} Q_{e,f}$ and $P_i Q_i$ is at most d satisfying the Nullstellensatz identity. Note that this system is intuitively also uniform in N, if d is fixed.

Now we give, in two steps, the definition of uniform systems. An equivalent combinatorial definition is provided by Lemma 1.7.

Definition 1.3 *Let $L(C)$ be the first-order language consisting only of the symbol $=$ for equality and of a finite set C of distinct constants. Let $L^*(C)$ be a first-order language extending $L(C)$ and having an element-sort and a set-sort, and consisting of an equality predicate $=$ in both sorts, of a membership relation $\in$ between elements and sets, and constants C. The set-sort can be used only as free variables; i.e., quantifiers may range only over element-sort.*

Any structure M containing C has a unique natural expansion M^* to an (expansion of the) $L^*(C)$-structure: it interprets the element-sort by its elements and the set-sort by its subsets. We shall always assume that all constants from C are different in M.

We shall, in fact, never substitute for set-variables other than finite sets.

Definition 1.4 *Let M be a first-order structure containing C.*

1. *$Index(M,k)$ is the set of k-tuples $i = (i_1, \ldots, i_k)$ of finite subsets of M such that $|i_j| \leq k$, all $j \leq k$. The elements of $Index(M,k)$ are called k-ary indices over M. The support of i is the set $supp(i) := \bigcup_j i_j$, and the support - size of i is the cardinality of $supp(i)$.*

2. *$Var(M,k)$ is the set of variables x_i indexed by elements i of $Index(M,k)$ different from $\overline{\emptyset} = (\emptyset, \ldots, \emptyset)$. (The index $\overline{\emptyset}$ will represent 1 in monomials.)*

3. *$Mon(M,k,d)$ is the set of all monomials formed from $Var(M,k)$ and of degree at most d. Monomials from $Mon(M,k,d)$ are identified with some indices from $Index(M,kd)$, utilising the index $\overline{\emptyset}$ for monomials of degree less than d: in particular, monomial $x_{i^1}x_{i^2}\ldots x_{i^\ell}$, $i^t = (i^t_1, \ldots, i^t_k)$, is identified with the kd -ary index $(i^1_1, \ldots, i^1_k, \ldots, i^\ell_1, \ldots, i^\ell_k, \emptyset, \ldots, \emptyset)$.*

   We sometimes also write x^i for the monomial i.

4. *A polynomial over M is an $L^*(C)$-definable function from $Mon(M,k,d)$ to $\mathbf{F}_p$. It is definable in $L^*(C)$ over $A \subseteq M$ if for each $a \in \mathbf{F}_p$ there is an $L^*(C)$-formula $\theta_a(\alpha)$ with free variables $\alpha = (\alpha_{1,1}, \ldots, \alpha_{1,k}, \ldots, \alpha_{d,1}, \ldots, \alpha_{d,k})$ and with parameters from $C \cup A$ such that the coefficient of the monomial $x_{j_{1,1},\ldots,j_{1,k}} \cdot \ldots \cdot x_{j_{d,1},\ldots,j_{d,k}}$ is a iff the formula $\theta_a(j)$ holds in M^*.*

   $Poly(M,k,d)$ is the set of polynomials of degree at most d with variables from $Var(M,k)$.

5. *A family F^M_i, $i \in Index(M,\ell)$ and M ranging over structures containing C, of polynomials with variables from $Var(M,k)$ and of degree at most d is* uniform *iff there are $L^*(C)$-formulas $\theta_a(\gamma,\alpha)$, $a \in \mathbf{F}_p$, with no parameters other than C, with free variables $\gamma = \gamma_1, \ldots, \gamma_\ell$, $\alpha = \alpha_{1,1}, \ldots, \alpha_{d,k}$ of the set-sort such that for every M and every $i \in Index(M,\ell)$ the polynomial F^M_i is defined in M^* by the formulas $\theta_a(i,\alpha)$.*

   We shall use the notation $F^M_{i,j}$ for the unique $a \in \mathbf{F}_p$ such that $\theta_a(i,j)$ holds in M^*, and we shall write $F^M_i = \sum_j F^M_{i,j} j$, where j also denotes the monomial corresponding to j.

The language $L^*(C)$ is introduced to allow as indices also unordered tuples (as in Example 1.1).

The reason for the somewhat unnatural representation of monomials of degree $\ell \leq d$ by kd -ary indices is that we shall later use the theory of tabloid modules and tabloids are ordered (it also allows us to use a fixed number of variables α_{ij} for formulas $\theta_a(\alpha)$ defining polynomials). More importantly, this representation of monomials by indices does not account for the commutativity of variables. We shall correct this situation, when studying degree $\leq d$ polynomials, by including in all families F a particular family $\mathrm{COMM}^{k,d}$.

Definition 1.5 *$COMM^{k,d}$ is a uniform family indexed by pairs i, j of elements of $Mon(M, k, d)$, with the polynomial $COMM^{k,d}_{i,j}$ being $x^i - x^j$, whenever i, j represent the same monomial.*

Hence, for finite M, $Poly(M, k, d)/\mathrm{COMM}^{k,d}$ is isomorphic to the $\mathbf{F}_p$-vector space of degree $\leq d$ polynomials over $\mathbf{F}_p$ with variables $Var(M, k)$. With this understanding we shall abuse the language and call elements of $Mon(M, k, d)$ and $Poly(M, k, d)$ monomials and polynomials respectively; there is never a danger of misunderstanding.

Note that the linear polynomials are simply functions $F : Index(M, k) \to \mathbf{F}_p$ such that each $F^{(-1)}(a)$, $a \in \mathbf{F}_p$, is $L^*(C)$-definable.

We need to link definability with the symmetric group. Permutations of N act also on the set of variables (and hence on polynomials) of the systems from Examples 1.1 and 1.2, and the systems are invariant under such actions. For a general uniform system over some M a similar fact holds.

Definition 1.6 *Let M be an $L(C)$-structure, $A \subseteq M$, and $i \in Index(M, r)$. $\mathbf{Sym}_C(M/A)$ is the group of permutations of M fixing point-wise the set $C \cup A$.*

The type of i over A, denoted $\mathbf{tp}_C(i/A)$, is the isomorphism type of the finite $L(C)$-structure

$$\langle C \cup supp(i) \cup A; \{c\}_{c \in C}, \{a\}_{a \in A}, i_1, \ldots, i_r \rangle$$

with the universe $C \cup supp(i) \cup A$.

Types of r-ary indices over A are in a bijective correspondence with orbits of $\mathbf{Sym}_C(M/A)$ acting on $Index(M, r)$. The following lemma is a simple model-theoretic fact (recall that we allow quantification only over the element-sort).

Lemma 1.7 *Let $L(C)$, the set A and r be fixed. Let $X^M \subseteq Index(M, r)$, M ranging over $L(C)$-structures containing A, be a family of sets of r-ary indices. Then the following two statements are equivalent:*

1. *There is an $L^*(C)$-formula $\psi(\alpha)$, $\alpha = (\alpha_1, \ldots, \alpha_r)$, with parameters from A such that for each $M \supseteq A$*

$$X^M = \{i \in Index(M, r) \mid M^* \models \psi(i)\} \ .$$

2. *There is a (necessarily finite) set S of types over A of r-ary indices such that for every $M \supseteq A$ and every $i \in Index(M, r)$*

$$i \in X^M \quad \textit{iff} \quad \mathbf{tp}_C(i/A) \in S \ .$$

In particular, a family F^M is uniform iff the value $F^M_{i,j} \in \mathbf{F}_p$ depends only on the type $\mathbf{tp}_C((i,j))$ of the pair of indices (i,j).

Let us conclude this section by an example of a system that is not uniform in our sense but that also occurred in proof complexity. It is the iteration principle considered in connection with bounded arithmetic in [7] (renamed as the house-sitting principle by various authors, cf. [4, 11]).

Example 1.8 *For $N \geq 1$, the system $Iter_N$ has variables x_{ij}, for $i,j \in N$, and polynomials:*

1. $x_{ij}^2 - x_{ij}$, *all* i,j.
2. $x_{ij}(1 - \sum_{k>j} x_{jk})$, *all* $i < j$.
3. $1 - \sum_{j>0} x_{0j}$.

By 1. and 3., $x_{0,j_0} = 1$ for some $j_0 > 0$. Then by 1. and 2., $x_{j_0,j_1} = 1$ for some $j_1 > j_0$, and $x_{j_1,j_2} = 1$ for some $j_2 > j_1$, etc., which is impossible.

The system is not uniform as its definition uses an ordering of N.

2 Euler structures and evaluation of polynomials

The following definition formalises properties of an Euler characteristic thought of as a cardinality function. I have come up with it while progressing towards Theorem 6.1, in a splendid ignorance of possibly related work. Papers, where such a cardinality function on possibly infinite structures is considered in order to extend validity of results for finite structures are the following: [37] considers a general problem of constructing an abstract Euler characteristic (and dimension) for distributive categories, and [41] uses Euler characteristic in the O-minimal context as a cardinality function. [1] studies the existence of a cardinality modulo p function for linearly ordered structures.

Definition 2.1 *Let M be a first-order structure. $Def^k(M)$ is the class of subsets of M^k definable in M (with parameters) and $Def^\infty(M)$ is the union $\bigcup_k Def^k(M)$.*

Let R be a commutative ring with unity. A function

$$\chi : Def^\infty(M) \longrightarrow R$$

is an abstract Euler characteristic *on M* over *R iff it satisfies the following conditions:*

1. $\chi(\{a\}) = 1$, *any* $a \in M^k$.

2. $\chi(A \cup B) = \chi(A) + \chi(B)$, *whenever* $A, B, A \cup B \in Def^\infty(M)$ *and* A, B *are disjoint.*

3. $\chi(A \times B) = \chi(A) \cdot \chi(B)$, *whenever* $A, B, A \times B \in Def^\infty(M)$.

4. $\chi(A) = \chi(B)$, *whenever* $A, B \in Def^\infty(M)$ *and there is a definable bijection between* A *and* B.

5. $\chi(A) = c \cdot \chi(B)$, *whenever* $c \in R$, $A, B \in Def^\infty(M)$ *and there is a definable map* f *with domain* A *and range* B *such that each its fiber* $f^{(-1)}(b)$, $b \in B$, *has Euler characteristic* $\chi(f^{(-1)}(b)) = c$.

Any pair $(M,\ \chi/R)$ *satisfying this conditions is called* Euler structure *and an* Euler expansion *of* M. *(We abuse the notation slightly as* $(M, \chi/R)$ *is not a first-order structure.)*

A function χ/R *satisfying all conditions but the last one is called* weak *abstract Euler characteristic and* $(M, \chi/R)$ *a* weak *Euler structure.*

The word *abstract* is meant to stress that χ is not assumed to arise from any particular cohomology theory, and we shall skip it for the sake of brevity. We shall also abbreviate the phrase that *M admits an (weak) Euler characteristic χ over R* to *M admits (weak) χ/R.*

Note that the conditions in Definition 2.1 are not independent. For example, conditions 3. and 4. follow from conditions 1. and 5. (the former is witnessed by a projection map, the later is trivial using 1.), and assuming a priori that χ is not identically zero and R is an integral domain, also 1. follows from 5. (there is a definable bijection between $\{a\}$ and $\{a\} \times \{a\}$ so $x := \chi(\{a\})$ satisfies $x^2 = x$ and thus $x = 0$ or $x = 1$, the former being excluded as it forces $\chi \equiv 0$). Hence, having a non-constant function χ from $Def^\infty(M)$ to an integral domain, it is enough to verify conditions 2. and 5. in order to certify that χ is an abstract Euler characteristic.

In the proof of Theorem 4.1 as well as in its applications to degree lower bounds (Section 6) we use Euler structures and not weak Euler structures. However, general existence theorems like Theorems 3.1, 3.4 or 3.7 seems to be valid only for weak Euler structures.

We note a simple but useful property of Euler structures.

Lemma 2.2 *Let* $(M, \chi/R)$ *be an Euler structure. Let* $R \subseteq A \times B$ *be a definable relation between definable sets. Assume that there are* $c_A, c_B \in R$ *such that*

$$\chi(\{b \in B \mid R(a, b)\}) = c_A, \quad \textit{for all } a \in A$$

and

$$\chi(\{a \in A \mid R(a, b)\}) = c_B, \quad \textit{for all } b \in B\ .$$

Then $\chi(A) \cdot c_A = \chi(B) \cdot c_B$.

Proof :

Let π_A and π_B be the two projections of R on A and B. By the assumption, all fibers of π_A as well as of π_B have the same value of the χ-characteristic (c_A and c_B respectively). So, by condition 5. of Definition 2.1

$$\chi(A) \cdot c_A = \chi(R) = \chi(B) \cdot c_B \ .$$

q.e.d.

We shall give now several examples of Euler structures.

Example 2.3 *Let* $\mathbf{R}$ *be the real field considered as a first-order structure in the language of ordered rings* $0, 1, +, \cdot, <$. *Definable sets are semi-algebraic sets (by Tarski-Seidenberg's theorem) and* $\mathbf{R}$ *admits* $\chi/\mathbf{Z}$ *(see [13, 14, 33, 37]).*

Note that this Euler characteristic is different from the one arising from the singular cohomology (the later one does not distinguish between an open and a closed interval which contradicts conditions of Definition 2.1).

Similar general construction of $\chi/\mathbf{Z}$ works over any O-minimal structure (cf.[13, 14, 33]). In particular, over expansions of $\mathbf{R}$ by the restricted analytic functions or exponentiation or Pfaffian functions (see [12, 16, 42, 43]).

A reduct of $\mathbf{R}$ whose definable sets are boolean combinations of polyhedra (semi-linear sets) is considered in connection with Euler characteristic in [40].

Example 2.4 *Let* $\mathbf{C}$ *be the complex field considered as a first-order structure in the language of rings* $0, 1, +, \cdot$. *Definable sets are boolean combinations of algebraic sets, i.e. constructible sets (by Chevalley, cf. [32, 30]) and* $\mathbf{C}$ *admits* $\chi/\mathbf{Z}$ *as* $\mathbf{C}$ *is definable in* $\mathbf{R}^2$.

In fact, all algebraically closed fields of characteristic 0 admit $\chi/\mathbf{Z}$.

Example 2.5 *A pseudo-finite field is an infinite field satisfying the theory of all finite fields (cf.[3, 8, 18] or the introduction to [22]). Any pseudo-finite field admits weak* χ/R *over any finite* R *(see Theorem 5.6).*

We remark that [9] provide a function μ defined on definable sets in pseudo - finite fields with values in $\mathbf{Q}^+$ (behaving like a measure). μ satisfies all the conditions of Definition 2.1 except condition 2. that holds only for sets of equal dimension.

Example 2.6 *The rings of integers and rationals do not admit weak* χ/R *over any non-trivial* R *as in both rings a bijection between a non-empty subset of the ring and the subset without one element is definable (this is trivial for integers, and integers are definable in rationals by [36]). That contradicts conditions 1., 2. and 4. of Definition 2.1.*

Our use of Euler structures is aimed chiefly at the following.

Definition 2.7 *Let $(M^*, \chi/\mathbf{F}_p)$ be an Euler structure and let*

$$f : Index(M, r) \to \mathbf{F}_p$$

be definable in M^*. For $a \in \mathbf{F}_p$, let

$$X_a := \{j \in Index(M, r) \mid M^* \models f(j) = a\} .$$

Then we define, for $b \in \mathbf{F}_p$:

$$(M^*, \chi/\mathbf{F}_p) \models \sum_j f(j) = b \quad \textit{iff} \quad \sum_{a \in \mathbf{F}_p} a \cdot \chi(X_a) = b .$$

In particular, as $F \in Poly(M, k, d)$ is definable in M^*, if there is a definable assignment a to $Var(M, k)$ giving the value a^j to monomial j, then the value of F at a is one of such sums: $\sum_j F_j^M a^j$. We leave it as an exercise to verify that this evaluation of polynomials is a homomorphism of the space of polynomials $Poly(M, k, d)$ to $\mathbf{F}_p$, fixing $\mathbf{F}_p$ and containing $\mathrm{COMM}^{k,d}$ in its kernel. We only summarise in one lemma some of the counting properties provable from Euler characteristic axioms used later (the proofs establish definable bijections between terms on both sides of the equalities).

Lemma 2.8 *Let $(M^*, \chi/\mathbf{F}_p)$ be an Euler structure. Let $f, g : Index(M, r) \to \mathbf{F}_p$ and $h : Index(M, r) \times Index(M, r) \to \mathbf{F}_p$ be functions definable in M^*. Then:*

1. $(\sum_{j_1} f(j_1))(\sum_{j_2} g(j_2)) = \sum_j (\sum_{j_1, j_2 : (j_1, j_2) = j} f(j_1) g(j_2))$,
   with j_1, j_2 ranging over $Index(M, r)$, j over $Index(M, 2r)$, and (j_1, j_2) being the concatenation of indices j_1, j_2.
2. $\sum_i (\sum_j h(i, j)) = \sum_j (\sum_i h(i, j))$,
   with j ranging over $Index(M, r)$.

Proof :
Consider the first part. By the definition $(\sum_{j_1} f(j_1))(\sum_{j_2} g(j_2))$ is equal to

$$(\chi(X_0) + \ldots + \chi(X_{p-1})) \ \cdot \ (\chi(Y_0) + \ldots + \chi(Y_{p-1}))$$

where X_a (resp. Y_a) is the set of j_1 (resp. j_2) such that $f(j_1) = a$ (resp. $g(j_2) = a$). Similarly, the right hand side of the equation is equal to

$$\chi(Z_0) + \ldots + \chi(Z_{p-1})$$

where Z_a is the set of triples $\langle j, j_1, j_2 \rangle$ such that $j = (j_1, j_2)$ and $f(j_1) g(j_2) = a$. The definable bijection sending pair $\langle j_1, j_2 \rangle$ to the triple $\langle (j_1, j_2), j_1, j_2 \rangle$, maps $\bigcup_{i=0}^{p-1} X_i \times Y_{a-i}$ onto Z_a (the term $a - i$ is modulo p). Hence $\chi(Z_a) = \sum_{i=0}^{p-1} \chi(X_i) \chi(Y_{a-i})$ and the equality follows.

The second part is analogous.

q.e.d.

3 More on Euler structures

The reason for the non-existence of weak χ/R in Example 2.6 is, in fact, the only one.

Theorem 3.1 *Let M be a structure. The following two properties are equivalent:*

1. *For no $X \in Def^{\infty}(M)$ is there a definable bijection between X and X without one element.*

2. *There is a non-trivial ring R such that M admits weak χ/R.*

Proof :

The second property implies the first one by conditions 1., 2. and 4. of Definition 2.1. Assume now that the first property holds.

Define an equivalence relation on $Def^{\infty}(M)$ by: $X \sim Y$ iff there is a definable (in M) bijection between X and Y. Denote R_0 the factor set $Def^{\infty}(M)/\sim$. We equip R_0 with an interpretation of the ring language as follows:

1. $0 := \emptyset/\sim$.

2. $1 := \{a\}/\sim$, for any $a \in M$.

3. $(X/\sim) + (Y/\sim) = (Z/\sim)$, if for some disjoint $X' \in (X/\sim)$ and $Y' \in (Y/\sim)$ it holds that $X \cup Y \sim Z$.

4. $(X/\sim) \cdot (Y/\sim) = (Z/\sim)$, if $X \times Y \sim Z$.

The structure $(R_0, 0, 1, +, \cdot)$ is not a ring (as $(R_0, 0, +)$ is not a group) but it is a (Burnside) rig in the sense of Schanuel [37] (a "ring without negatives").

Define an equivalence relation $\sim_1$ on R_0 by: $a \sim_1 b$ iff $a + c = b + c$ for some $c \in R_0$, and let R_1 be the factor rig $R_0/\sim_1$. $(R_1, 0, +)$ is still not a group but it is a cancellative monoid. Let R be the unique minimal ring that embeds R_1. R is non-trivial iff R_1 is, i.e. iff 0 and 1 are not $\sim_1$-equivalent in R_0. The later condition is equivalent to the hypothesis of the theorem.

q.e.d.

Note that algebraically closed fields of all characteristics satisfy the first condition of Theorem 3.1, cf. Example 5.5.

Lemma 3.2 *Let M_1, M_2 be two structures of the same signature, and assume that M_1 is an elementary substructure of M_2. Assume that M_2 admits weak χ/R.*

Then M_1 admits weak χ/R too.

Proof :

Let χ_2 be an Euler characteristic on M_2 over R. Let $X_1 \subseteq M_1^k$ be defined in M_1 by $\phi(\overline{a}, \overline{x})$, for some parameters $\overline{a} \in M_1^\ell$.

Take $X_2 \subseteq M_2^k$ defined in M_2 by the same formula and put:

$$\chi_1(X_1) := \chi_2(X_2) \ .$$

It is easy to see that χ_1 does not depend on the particular definition $\phi(\overline{a}, \overline{x})$ and that it satisfies the first four conditions of Definition 2.1.

q.e.d.

I do not know if the lemma can be extended to non - weak χ/R; the same proof does not apply as one does not have a control over the Euler characteristic of fibers $f^{(-1)}(b)$ for b outside of M_1, even if f is definable in M_1 and satisfies there the hypothesis of the fiber condition 5 of definition 2.1. However, if χ is definable (see Section 7), then f satisfying the hypothesis of the fiber condition in M_1 satisfies it also in M_2 and the same proof goes through.

Lemma 3.3 *Let M_i, $i \in I$, be structures of the same signature, and assume that M is an ultraproduct of M_i. Assume that all M_i admit (weak) χ/R, where R is finite.*

Then M admits (weak) χ/R too.

Proof :

The ultraproduct naturally carries χ (the ultraproduct of the Euler characteristics of M_i) with values in the ultrapower of R. However, as R is finite this ultrapower is isomorphic to R.

q.e.d.

The use of ultraproduct is certainly not necessary as Euler expansions of M over a finite R are just expansions of M satisfying a certain infinite first-order theory (see the proof of Theorem 7.2) and hence compactness would suffice. However, we shall find the ultraproduct formulation handy later on.

The next theorem shows that the property whether M admits weak χ/R, for finite R, is really a property of its theory.

Theorem 3.4 *Let M_1, M_2 be two structures of the same signature, and assume that M_1 is elementarily equivalent to M_2. Assume that M_1 admits weak χ/R, where R is finite.*

Then M_2 admits weak χ/R too.

Proof :

By a theorem of Shelah [39], there are ultrapowers M_i^* of M_i, $i = 1, 2$, that are isomorphic.

If M_1 admits weak χ/R so does M_1^* (by Lemma 3.3) and thus M_2^* too. As M_2 is an elementary substructure of M_2^*, it admits weak χ/R also, by Lemma 3.2.

q.e.d.

It is clear that structures admitting $\chi/(\mathbf{Z}/m)$ are axiomatizable by a first-order scheme in the original language (use compactness). However, a natural axiomatisation is possible using the so called counting principles, see [1].

Definition 3.5 *Let $m \geq 2$ and let M be a first-order structure. We say that M satisfies* counting principle modulo m, *written $M \models Count_m$, if there are no definable set $X \subseteq M^k$ and two definable equivalence relations R, S on X such that*

1. *Every class of R has size m.*
2. *Every class of S except one* exceptional class *has size m and the exceptional class has size between* 1 *and* $m-1$.

In [1] it is proved that if M can be definably linearly ordered and p is a prime, then M admits weak $\chi/\mathbf{F}_p$ iff $M \models Count_p$ ([1] has no fiber condition 5. of Definition 2.1). One direction (the next lemma) is simple and holds for any $m \geq 2$. The proof of the other direction can be modified so that the assumption about the existence of a linear ordering is not needed (Theorem 3.7).

Lemma 3.6 ([1]) *Assume that M admits weak $\chi/(\mathbf{Z}/m)$, and that a linear ordering of M is definable in M.*

Then $M \models Count_m$.

Proof :

Assume that X, R, S witness the failure of $Count_m$ in M. Using R and the definable linear ordering of M (and consequently of M^k) define $X_i \subseteq X$, $i = 1, \ldots, m$, the sets of the i-th elements of classes of R. There are definable bijections between X_1 and all X_i (pair two elements in the same classes) so in $\mathbf{Z}/m$:

$$\chi(X) = \sum_i \chi(X_i) = m \cdot \chi(X_1) = 0 \ .$$

Similarly we may partition $X \setminus Y$ using S into X'_i, where Y is the exceptional class of S, so that in $\mathbf{Z}/m$:

$$\chi(X) = \chi(Y) + \chi(X \setminus Y) = \chi(Y) + \sum_i \chi(X'_i) = \chi(Y) + m \cdot \chi(X'_1) = \chi(Y) \ .$$

However, $1 \leq \chi(Y) \leq m-1$ and hence $\chi(Y)$ is non-zero in $\mathbf{Z}/m$. That is a contradiction.

q.e.d.

Theorem 3.7 *Let p be a prime and assume that $M \models Count_p$.*

Then M admits weak $\chi/\mathbf{F}_p$.

Proof :

If $M \models Count_p$ then, in particular, M satisfies the hypothesis of Theorem 3.1. This is because if $f : X \to X \setminus \{a\}$ is a bijection then $X \times \{c_1, \ldots, c_p\}$ (c_i distinct) admits two equivalence relations: S_1 with classes $\{(x, c_1), \ldots, (x, c_p)\}$, $x \in X$, and S_2 with classes $\{(x, c_1), \ldots, (x, c_{p-1}), (f(x), c_p)\}$, $x \in X$, with one missing point (a, c_p).

Let R be the (non-trivial) ring constructed in the proof of Theorem 3.1 (we use also the notation from that proof).

Define an ideal I in R as follows. It is sufficient to specify I on R_1. Let $a \in R_1$. Then $a \in I$ iff a has the form $a = (X/\sim)/\sim_1$ for some $X \in Def^\infty(M)$ such that there exists a definable equivalence relation S on X whose all classes have p elements. It is clear that I is indeed an ideal in R, and is proper by $Count_p$.

We claim that $R' := R/I$ is a ring of characteristic p that satisfies the identity $x^p = x$. The former is obvious. For the later let $a \in R_1$ has the form $a = (Z/\sim)/\sim_1$ for some $Z \in Def^\infty(M)$, and let Δ_Z be the diagonal in Z^p (i.e., in $Z \times \ldots \times Z$, p-times) and $Y := Z^p \setminus \Delta_Z$. Hence $\Delta_Z \sim Z$. Define an equivalence relation S on Y by: $(y_1, \ldots, y_p) S (y'_1, \ldots, y'_p)$ iff $(y'_1, \ldots, y'_p)$ can be obtained from $(y_1, \ldots, y_p)$ by a cyclic permutation. This proves that $a^p - a \in I$.

Finally, take a maximal ideal J in R' and the factor R'/J. Necessarily $R'/J \simeq \mathbf{F}_p$, as it is a field of characteristic p satisfying the identity $x^p = x$.

q.e.d.

We remark that Ajtai's proof [1] of a similar statement in the presence of a definable linear ordering in M uses the ordering in a non-trivial way in the proofs of properties F5 (the last paragraph) and F6 there.

The theorem cannot be reversed in general: an algebraically closed field of characteristic p is an example of a structure admitting weak $\chi/\mathbf{F}_p$ (even weak $\chi/\mathbf{Z}$ by Example 5.5) but not satisfying $Count_p$ (by Theorem 5.1).

Lemma 3.8 *If $M \models Count_m$ then $M \models Count_n$, for all $n|m$.*

Proof :

If X, R, S witness the failure of $Count_n$ in M, we may replace every point in X by its $\frac{m}{n}$ copies. Such inflated X, R, S form a counterexample to $Count_m$.

q.e.d.

For finite M a form of converse holds too, cf.[5, Sec.2]. Identical argument as there proves the same converse for infinite structures with a definable linear order.

4 Solvability criterion

The aim of this section is to prove the following theorem generalising a theorem of Ajtai [2] from finite structures to Euler structures. A prime p is fixed throughout the section.

Theorem 4.1 *Let F be a uniform family of linear polynomials over $\mathbf{F}_p$, with variables indexed by k-indices and polynomials indexed by ℓ-indices.*

Then there is $\nu \geq 1$, depending only on k and ℓ, and $Q \subseteq \{0, \ldots, p^\nu - 1\}$ such that the following holds for any sufficiently large Euler structure $(M, \chi/(\mathbf{Z}/p^\nu))$ (finite or infinite):

$$F^M \text{ is solvable in } (M, \chi/(\mathbf{Z}/p^\nu)) \quad \text{iff} \quad \chi(M) \in Q \ .$$

The rest of the section consists of the proof of the theorem. For degree lower bounds in Section 6 we need only the statement of the theorem but nothing used for its proof; hence a reader interested only in the lower bounds but not keen on details can skip the rest of the section.

The proof follows the construction from [28] that extends and modifies a construction from [2]. Ajtai [2] constructs generators for group algebra submodules of the tabloid modules that are definable in particular expansions of the underlying structure (that is always finite in [2, 28]). The expansions used allow to linearly order the universe (in order to define a standard tableaux) and to simulate a counting modulo a fixed power of p (in order to sum various definable functions over sets of ℓ-tuples). This extra structure is already discarded in [28] at the expense of replacing a bounded size set of generators of the submodule by a uniform family generating the submodule as a vector space. The counting in the expanded structures in [2] is reduced in [28] to the knowledge of $M \pmod{p^\nu}$, and will be replaced here by counting using the Euler characteristic. In particular, polynomials are evaluated by the Euler characteristic in the sense of Definition 2.7.

Let us give now an example illustrating why we need χ over some $\mathbf{Z}/p^\nu$ rather than just over $\mathbf{F}_p$. Consider a set X of 2-indices formed by unordered pairs of different elements of M. If $|M| = n$ is finite then $|X| \pmod 2$ does not depend only on $n \pmod 2$ but on $n \pmod 4$. A calculation showing that $2\chi(X) = \chi(M)(\chi(M) - 1)$ is valid also for infinite M. Namely, let $R \subseteq M \times X$ be the element-hood relation. Then R-degree of any element of M is $\chi(M) - 1$ while the R-degree of any element of X is 2. Thus $\chi(M)(\chi(M)-1) = 2\chi(X)$, by Lemma 2.2. Hence to be able to count modulo 2 sets of 2-indices it is necessary to count modulo 4 subsets of M. A general statement we need is the following.

Given M and $r \geq 1$, denote by $(M, Index(M, r))$ the two-sorted structure expanding M by the element-hood relation between elements of M and $\leq r$-element subsets of M occurring in $Index(M, r)$.

The next lemma is analogous to [28, L. 1.7] but the construction is a bit different as we must use only definable maps and relations and not a priory counting.

Lemma 4.2 *Let M be a set without a structure, possibly with a distinguished set C of constants. Given $r \geq 1$ there is $\nu \geq 1$ such that any Euler structure*

$$(M, \chi/(\mathbf{Z}/p^{\nu}))$$

uniquely determines an Euler structure

$$((M, Index(M,r)), \chi'/\mathbf{F}_p)$$

on an $L^*(C)$-expansion of M with the property that

$$\chi(X) \equiv \chi'(X) \ (mod\ p)$$

for all $X \in Def^{\infty}(M)$.

Moreover, if $f : Index(M,r) \to \mathbf{F}_p$ is a definable function then

$$\sum_{j \in Index(M,r)} f(j) \ (mod\ p)$$

as defined by χ', depends only on $\chi(M)$ and $\chi(C)$, provided $p^{\nu} > (r!)^r$.

Proof :

A natural approach to extending χ to χ' is to represent r-indices, say $j = (j_1, \ldots, j_r)$, by ordered r-tuples of ordered elements of $supp(j_i)$, and instead of counting the χ'-cardinality of a set of j's count the χ-cardinality of the set of corresponding tuples. However, every j is represented by many such tuples and we need to verify that the usual arithmetic of ordered and unordered tuples can be carried from axioms of Euler characteristic only. As an illustration that it is so we compute the χ-cardinalities of the sets of realizations of all possible types of j's.

We wish to compute $\chi(J)$, where J is the set of realizations of a type $\mathbf{tp}_C(j/A)$ of $j \in Index(M,r)$, and show

Claim 1: *$\chi(J)$ (mod p) depends on $\chi(M)$, $\chi(A)$ and $\chi(C)$ only, if ν is large enough.*

(The value of ν will be specified later.)

We proceed by induction on r. For simplicity we first disregard C and A. Let $j = j_1, \ldots, j_r$ and $j^- = j_1, \ldots, j_{r-1}$. If $r = 1$ then J is the set of j_1-element subsets of M and this is handle as the case $j_1 = 2$ before the lemma. For $r > 1$, let J^- be the set of realizations of $\mathbf{tp}_C(j^-)$. Then an element $j \in J$ is in a one-to-one correspondence with the triple j^-, $\mathbf{tp}_C(j^*/supp(j^-))$ where $j^* := j_1, \ldots, j_{r-1}, j_r \cap supp(j^-)$, and $\mathbf{tp}_C(j_r \setminus supp(j^-)/supp(j^-))$. Elements j^- comprise J^-. The set of realizations of $\mathbf{tp}_C(j^*/supp(j^-))$ has only boundedly many realizations (depending on r), and the set of realizations of $\mathbf{tp}_C(j_r \setminus$

$supp(j^-)/supp(j^-))$ is in one-to-one correspondence with the set of t-element subsets of $M \backslash supp(j^-)$, for $t := |j_r \backslash supp(j^-)|$. As $t \leq r$, the Euler characteristic of the last set modulo p depends, as before, only on Euler characteristic module a fixed power of p (depending on r), see the claim below.

Hence
$$\chi(J) = \chi(J^-) \cdot c \cdot \chi([X]^s)$$
where c is bounded, X is a definable set and $s \leq r$. By induction assumption the claim holds for $\chi(J^-)$, so it holds for $\chi(J)$ as well, provided we have the following

Claim 2: *For any $s \geq 1$ and any $X \in Def^{\infty}(M)$ with at least s elements the set $[X]^s$ of s-element subsets of X (a particular s-indices) satisfies:*
$$\chi([X]^s) \cdot s! = \chi(X) \cdot (\chi(X) - 1) \cdot \ldots \cdot (\chi(X) - s + 1) \ .$$

The claim is verified by induction on s. The case $s = 1$ is obvious. For $s > 1$ we have
$$\chi([X]^s) \cdot s = \chi([X \setminus \{a\}]^{s-1}) \cdot \chi(X)$$
where $a \in X$ is any element. This is seen as the case $s = 2$ before the lemma, taking the element-hood relation $R \subseteq [X]^s \times X$ and applying Lemma 2.2. By induction hypothesis then
$$\chi([X \setminus \{a\}]^{s-1}) \cdot (s-1)! = (\chi(X) - 1) \cdot \ldots \cdot (\chi(X) - s + 1)$$
which together imply the equality.

Returning back to our original aim, we notice that the number of ordered tuples representing an index j as described at the beginning of the proof is at most $(r!)^r$. Hence the above computation shows that as long as $p^{\nu} > (r!)^r$, χ uniquely determines χ'.

q.e.d.

For the rest of the section fix the polynomial system F and the Euler structure $(M, \chi/(\mathbf{Z}/p^{\nu}))$; ν is fixed but unspecified at this point. We shall assume familiarity with some notions and some constructions from [28]. However, we give in detail all definitions and their modifications needed to our case.

Definition 4.3 1. *An* r-partition *of M is a tuple $\mu = \mu_1, \ldots, \mu_k$ of natural numbers such that*
$$|M| - \sum_{i=1}^{k} \mu_i \geq \sum_{i=1}^{k} \mu_i$$
and $r \geq \mu_1$ and $r - 1 \geq k$. (Note that the first inequality always holds if M is infinite.)

The partition is proper if moreover

$$|M| - \sum_{i=1}^{k} \mu_i \geq \mu_1 \geq \mu_2 \geq \ldots \geq \mu_k$$

2. *Let* $\mu = \mu_1, \ldots, \mu_k$ *be an* r*-partition. A* μ-tabloid *is a* $(k+1)$*-tuple of subsets* $X_0, X_1, \ldots, X_k$ *of* M *such that*

   (a) X_i*'s form a partition of* M.

   (b) $|X_i| = \mu_i$, *for* $i \geq 1$.

3. *A* μ-tableaux t *is a* μ*-tabloid* $X_0, \ldots, X_k$ *together with*

   (c) *Linear orderings of* $X_1, \ldots, X_k$.

   (d) *A linearly ordered subset* $X_0' \subseteq X_0$ *of size* μ_1.

   If t *is a tableaux,* $\{t\}$ *denotes the underlying tabloid (forgetting the data in (c), (d).*

We picture tableaux t as arranged into rows $X_0, \ldots, X_k$ and columns, the ith column ($i \leq \mu_1$) consisting of the ith elements of the rows (if they exist). We do not order into columns the remaining elements $X_0 \setminus X_0'$ of the first row.

Definition 4.4 *Let* $\mu = \mu_1, \ldots, \mu_k$ *be a proper* r*-partition and* t *a* μ*-tableaux.* $C_t \subseteq \mathbf{Sym}_C(M)$ *is the* column stabiliser *subgroup of the symmetric group of* M *containing those* $\pi \in \mathbf{Sym}_C(M)$ *such that*

1. $\pi \equiv id$ *on* $X_0 \setminus\ (X_0' \cup X_1 \cup \ldots \cup X_k)$.
2. π *fixes set-wise all* μ_1 *columns of* $X_0', X_1, \ldots, X_k$.

Note that $|C_t| \leq ((k+1)!)^r \leq (r!)^r$, and that if μ is an r-partition then μ-tabloids correspond to particular r-indices (forgetting X_0).

Definition 4.5 *Let* μ *be an* r*-partition. The tabloid module* M^μ *is the set of all* $L^*(C)$*-definable (with parameters) maps from the sets of* μ*-tabloids to* $\mathbf{F}_p$*. Such an element shall be denoted as* $\sum f(\{t\})\{t\}$ *or as* $\sum_j u_j j$ *with* j *ranging over* μ*-tabloids.*

Note that this definition yields the usual definition of [25] if M is finite. However, if M is infinite then it is not the case that M^μ is a vector space with the basis formed by the μ-tabloids.

In what follows we extend the arguments from [28] from finite structures to Euler structures (possibly infinite). We show that definitions as well as proofs carry directly to this more general context; we consider in detail the important Submodule theorem of James [25] (generalised to Theorem 4.9 here).

We remark that Gray [19, 20] extended a part of James's characteristic - free representation theory of the symmetric group from finite to infinite. In particular, he studied $\mathbf{F}_p\mathbf{Sym}(M)$ - submodules of a permutation module generated by unordered k - tuples of elements over infinite M (note that this is itself a proper submodule of M^μ as defined here, for $\mu = \mu_1$ being unordered k - tuples).

Following [28] we say that V *generates* a $\mathbf{F}_p[\mathbf{Sym}_C(M)]$-submodule U iff it generates U as an $\mathbf{F}_p[\mathbf{Sym}_C(M)]$-module, and that it *generates* U *as a vector space* iff U is the $\mathbf{F}_p$-linear span of V.

Definition 4.6 *1. Let μ be a proper r-partition and t a μ-tableaux. The* signed column sum *of t is*

$$\kappa_t := \sum_{\pi \in C_t} (sgn\ \pi)\pi$$

and the polytabloid *of t is*

$$e_t := \{t\}\kappa_t$$

2. The Specht module S^μ is the $\mathbf{F}_p[\mathbf{Sym}_C(M)]$-submodule of M^μ spanned by all polytabloids e_t.

Note that S^μ is defined identically as in [25], and that it is a cyclic submodule generated by any polytabloid e_t ([25, 4.5]).

Lemma 4.7 *1. Let t, t^* be two μ-tableaux. Then $\{t^*\}\kappa_t$ is either 0 or e_t or $-e_t$.*

2. Let $u \in M^\mu$ be arbitrary and let t be an arbitrary μ-tableau. Then there is $c \in \mathbf{F}_p$ such that $u\kappa_t = c \cdot e_t$.

Proof :

Assume $\{t^*\}\kappa_t \neq 0$. By the construction then for some $\pi \in C_t$ we have $\{t^*\} = \{t\}\pi$ (as in [25, 4.6]). So

$$\{t^*\}\kappa_t = \{t\}\pi\kappa_t = (\text{sgn}\ \pi)e_t\ .$$

This proves the first part.

For the second part write $u = \sum_{\{t^*\}} u_{\{t^*\}}\{t^*\}$, $u_{\{t^*\}} \in \mathbf{F}_p$, with $\{t^*\}$ ranging over some ($L^*(C)$-definable sets of) μ-tabloids. By the first part of the lemma, $\{t^*\}\kappa_t = c_{\{t^*\}}e_t$, where $c_{\{t^*\}}$ is 0, 1 or -1, and $c_{\{t^*\}}$ is $L^*(C)$-definable from $\{t^*\}$ (as C_t has a bounded size so is explicitly definable using elements of t as parameters). So the sum $\sum_{\{t^*\}} u_{\{t^*\}}c_{\{t^*\}}$ is definable and hence can be evaluated by χ (cf. Definition 2.7). So $u\kappa_t = c \cdot e_t$ where $c := \sum_{\{t^*\}} u_{\{t^*\}}c_{\{t^*\}}$ (use Lemma 2.8).

q.e.d.

Definition 4.8 *Let $u = \sum_j u_j j$, $v = \sum_j v_j j$ be two elements of M^μ, where j ranges over μ-tabloids. Define the bilinear form $\langle u, v\rangle$ as follows:*

$$\langle u, v\rangle \ := \ \sum_j u_j v_j$$

The map sending j to $u_j v_j \in \mathbf{F}_p$ is $L^*(C)$-definable, hence the sum can be evaluated by the Euler characteristic.

The bilinear form determines a notion of orthogonality. The following statement is a version of James's submodule theorem [25, Thm.4.9] in our situation.

Theorem 4.9 *Let $U \subseteq M^\mu$ be an arbitrary $\mathbf{F}_p[\mathbf{Sym}_C(M)]$-submodule. Then either $S^\mu \subseteq U$ or $U \subseteq (S^\mu)^\perp$.*

Proof :

Consider two cases: the first occurs when $u\kappa_t \neq 0$ for some $u \in U$ and some μ-tableaux t, the second otherwise. In the first case, by Lemma 4.7, $u\kappa_t = ce_t$ for some non-zero $c \in \mathbf{F}_p$. So $c^{-1}(u\kappa_t) = e_t \in U$ too and hence $S^\mu \subseteq U$.

To calculate the second case note that $\langle u\pi, v\rangle = \langle u, v\pi^{(-1)}\rangle$ for a permutation $\pi \in \mathbf{Sym}_C(M)$ and as $sgn(\pi) = sgn(\pi^{(-1)}$ also $\langle u\kappa_t, v\rangle = \langle u, v\kappa_t\rangle$. Then, in the second case, necessarily for all $u \in U$ and all t:

$$0 = \langle u\kappa_t, \{t\}\rangle = \langle u, e_t\rangle \ .$$

So $U \subseteq (S^\mu)^\perp$.

q.e.d.

Second ingredient from [25, 24] used in [28] is a characterisation of the Specht module and its orthogonal complement as the kernel and the range of certain linear maps, respectively. We give the definitions of these maps and state the characterisations; the translation of their proofs from [25, 24] to the present context is equally straightforward as in the case of the Submodule theorem, and is left to the reader.

Definition 4.10 *Let $\mu = (\mu_1, \ldots, \mu_k)$ be a proper r- partition.*

1. *For $0 \leq i < k$ and $0 \leq v < \mu_{i+1}$ a map $\psi_{i,v}$ is defined as follows:*

   The map $\psi_{i,v}$ maps M^μ to $M^{\lambda^{i,v}}$

   $$\lambda^{i,v} = (\mu_1, \mu_2, \ldots, \mu_{i-1}, \mu_i + \mu_{i+1} - v, v, \mu_{i+2}, \ldots, \mu_k)$$

   by sending a μ - tabloid T to the sum $\sum\{T' \mid T' \in X_T\}$, where X_T is the set of all $\lambda^{i,v}$ - tabloids T' that agree with T on all rows except on the ith and the $(i+1)$st ones, and the $(i+1)$st row of T' is a subset of the $(i+1)$st row of T of size v.

2. *The maps* $\varphi_{i,v} : M^{\lambda^{i,v}} \to M^{\mu}$ *are defined as follows:* $\varphi_{i,v}$ *maps a* $\lambda^{i,v}$ *- tabloid* T *to the sum* $\sum_{T' \in X_T} T'$*, where* X_T *is the set of all* μ *- tabloids agreeing with* T *in all except the* i*th and the* $(i+1)$*st rows, with the* $(i+1)$*st row of* T' *being the* $(i+1)$*st row of* T *together with some* $\mu_i - v$ *elements of the* i*th row of* T*.*

The sums in both parts are evaluated by the Euler characteristic.

Maps $\varphi_{i,v}$ are in [24] denoted $\psi_{i,-v}$; we use the notation of [28] as it is somewhat less confusing. The following theorem extends [25, Cor.17.18] (first part) and [24, Cor.3] (second part) to the context of Euler structures.

Theorem 4.11 *Let* $\mu = (\mu_1, \ldots, \mu_k)$ *be a proper partition.*

1. $S^{\mu} = \bigcap_{i=0}^{k-1} \bigcap_{v=0}^{\mu_{i+1}-1} Ker(\psi_{i,v})$.
2. $(S^{\mu})^{\perp} = \sum_{i=0}^{k-1} \sum_{v=0}^{\mu_{i+1}-1} Rng(\varphi_{i,v})$.

We may extend now [28, Thms.3.3 and 3.5] to our context. For F a uniform linear system with variables indexed by $Mon(M, k', 1)$, $k' \geq k$, let $V(F^M)$ denote the vector space of solutions of the homogeneous system $F^M \overline{x} = 0$, and $V_k(F^M)$ its projection onto $M^{(k)}$.

Theorem 4.12 *For any* $k \geq 1$ *there are* $\nu \geq 1$*,* $c \geq 1$*,* $k' \geq k$ *and at most* c *uniform linear systems* K^s*,* $s \leq c$*, with variables indexed by* $Mon(M, k', 1)$ *such that the following holds true for any sufficiently large Euler structure* $(M, \chi/(\mathbf{Z}/p^{\nu}))$*: Any* $U \subseteq Poly(M, k, 1)$*, an* $\mathbf{F}_p[\mathbf{Sym}_C(M)]$*-submodule, is one of the vector spaces* $V_k((H^s)^M)$*.*

Furthermore, for any two linear systems H_1, H_2 *with variables indexed by* $Mon(M, k', 1)$ *the validity of the inclusion* $V_k(H_1^M) \subseteq V_k(H_2^M)$ *depends only on* M *(mod* p^{ν}*).*

Proof :

The proof can follow literally the construction and arguments in [28]. This is because earlier definitions and statements we gave in this section (most notably Theorems 4.9 and Theorem 4.11) extend the notions smoothly from [25, 24] to the case of an infinite Euler structure M.

In particular, monomials from $Mon(M, k, 1)$ are encoded by $Index(M, k)$ and thus $Poly(M, k, 1)$ is itself an $\mathbf{F}_p[\mathbf{Sym}_C(M)]$-submodule of the tabloid module M^{μ}, μ-tabloids encoding k-indices where μ is an r-partition for suitable r (for example, $r \leq 2^k$ in the encoding used in [28]). Theorems 4.9 and 4.11 are repeatedly used to construct a vector space basis in an inductive process. The length of this induction (defined in [28]) depends on r but not on M.

The constant $\nu \geq 1$ is the constant provided by Lemma 4.2 for $r \leq 2^k$ as above.

q.e.d.

Proof of Theorem 4.1:

We follow the proof of [2, Thm.2 and Cor.6] from [2, Thm.7'], replacing it by Theorem 4.12 (see also [28, Thm.3.6]).

If F consists only of homogeneous linear equations there is nothing to prove as there is always the trivial solution. Otherwise we may assume that F contains exactly one non-homogeneous equation, say $F_{\overline{\emptyset}}$. This can be achieved by replacing every non-homogeneous F_i by $F_i - c_i F_{i_0}$, for some fixed F_{i_0} and suitable $c_i \in \mathbf{F}_p$, and by renaming F_{i_0} to $F_{\overline{\emptyset}}$. It is easy to see that this transformation preserves the uniformity of F.

Define F^1 by dropping from F the equation $F_{\overline{\emptyset}} = 0$, and F^2 by changing the non-zero absolute coefficient of $F_{\overline{\emptyset}}$ to zero.

Let U^1 and U^2 be the subspaces of $Poly(M, k, 1)$ of solutions in the sense of Definition 2.7 of F^1 and F^2 respectively. As F^1, F^2 are uniform, U^1 and U^2 are by Lemma 1.7 $\mathbf{F}_p[\mathbf{Sym}_C(M)]$-submodules of $Poly(M, k, 1)$. $U^2 \subseteq U^1$ and clearly F^M has a solution iff $U^2 \not\subseteq U^1$.

By Theorem 4.12, whether or not $U^1 \setminus U^2 \neq \emptyset$ depends only on $M \pmod{p^\nu}$.

This completes the proof of Theorem 4.1.

q.e.d.

To conclude the section let us note that Theorem 4.1 cannot be extended to non-linear systems F.

Example 4.13 *The uniform system $\neg PHP$ from the introduction is a degree 2 system solvable in $\mathbf{R}$ (take, for example, $f : \mathbf{R} \to \mathbf{R}$ sending any $x > 0$ to $x + 1$ and fixing all $x \leq 0$) but unsolvable for any finite N.*

5 Examples from field theory

We start with algebraically closed fields.

Theorem 5.1 (L. van den Dries, D. Marker, G. Martin [15]) *Let K be an algebraically closed field and $m \geq 2$. Let $S \in Def^2(K)$ be an equivalence relation on K all of whose classes except one exceptional class have m elements, and let the exceptional class has B elements for some $1 \leq B \leq m$. Then:*

1. *If $char(K) = 0$ or $char(K) > m$ then $B = 1$.*
2. *If $char(K) = 2 = m$ then $B = 2$.*
3. *If $char(K) = p > 2$ and $p < m \leq \frac{3}{2}p$ then $B \equiv p + 1 \pmod m$.*

Moreover, these are the only restrictions on B.

The theorem is derived from Lüroth's theorem (alternatively it can be derived from Hurwitz's theorem). A generalisation to smooth projective curves over K was proved by Albert (see [30, p.22]). He showed that the number B of exceptional points in any equivalence relations S on a smooth projective curve C must satisfy $B \equiv \chi(C) \pmod{m}$, where $\chi(C)$ is the Euler characteristic derived from the cohomology of projective space (cf.[21, III.5]).

Note that for $char(K) = 0$ the result follows immediately from Example 2.3 and Lemma 3.6, as $\mathbf{C}$ is definable in $\mathbf{R}^2$. For $m = 2$ the theorem determines B uniquely for all characteristics. In fact, a bit more holds. Namely $Count_2$ is satisfied in all dimensions.

Theorem 5.2 *Let K be an algebraically closed field. Then $K \models Count_2$ and K admits weak $\chi/\mathbf{F}_2$.*

Proof :

Consider first the case $char(K) = p > 0$. Let X, S, R, e be a counter-example to $Count_2$ with R a 2-partition of a definable $X \subseteq K^k$, and S a 2-partition of $X \setminus \{e\}$, where $e \in X$. Define $f_R : X \to X$ by the condition $\{a, f_R(a)\} \in R$, for all $a \in X$. So $f_R^{(2)} = f_R$.

Similarly define $f_S : X \setminus \{e\} \to X \setminus \{e\}$. By quantifier elimination and compactness (see e.g. [32] or [30]) it holds:

1. X is quantifier-free definable.

2. f_R and f_S are piece-wise, i.e. on (quantifier-free) definable subsets, of the form
$$Frob^{(-j)}(r(\overline{x}))$$
where $Frob$ is the Frobenius map on K: $x \mapsto x^p$, and r is a rational function.

Let $A \subseteq K$ be a finite set containing e and all the parameters from the definitions 1. and 2..

By elementary equivalence of all algebraically closed fields of the same characteristic we may assume without a loss of generality that $K = \tilde{\mathbf{F}}_p$. Let $\mathbf{F}_{p^\ell} \subseteq \tilde{\mathbf{F}}_p$ be a subfield of $\tilde{\mathbf{F}}_p$ large enough to contain A. Then X, R, S, e constitute a counter-example to $Count_2$ in $\mathbf{F}_{p^\ell}$ which is impossible as $Count_2$ holds in all finite structures..

The case of $char(K) = 0$ follows either from Example 2.4, or by compactness from the non-zero characteristic.

This proves $K \models Count_2$. The second part of the theorem follows from Theorem 3.7.

q.e.d.

Next lemma extends Lemma 3.6 (with the qualification *weak* omitted) to algebraically closed fields..

Lemma 5.3 *Assume K is an algebraically closed field and $K \models \neg Count_m$ for some $m \geq 2$.*

Then K does not admit $\chi/(\mathbf{Z}/m)$.

Proof :

Let $X \in Def^\infty(K)$, R and S be a counterexample to $Count_m$ in K with $1 \leq B \leq m-1$ exceptional points. By elimination of imaginaries (cf.[30, 32]) m-element subsets of K^k are coded by elements of some K^ℓ, ℓ depending on k, m (for example, by symmetric polynomials, i.e. by their coefficients).

Let Y_R and Y_S be subsets of K^ℓ of the codes of classes of R and S respectively. Consider a relation $R^* \subseteq X \times Y_R$ consisting of pairs (x, y) such that x is in the R-class coded by y. Similarly define $S^* \subseteq X \times Y_S$.

The R^*-degree of any $x \in X$ is 1 and of any $y \in Y$ is m. So by Lemma 2.2:

$$\chi(X) = m \cdot \chi(Y_R) \ .$$

The S^*-degree of any $x \in X$ is also 1 except of the exceptional B elements of S having S^*-degree 0. The S^*-degree of any $y \in Y$ is m. So again by Lemma 2.2:

$$\chi(X) - B = m \cdot \chi(Y_S)$$

hence

$$B = m \cdot (\chi(Y_R) - \chi(Y_S)) = 0 \ .$$

That is a contradiction.

q.e.d.

The lemma has, together with Theorem 5.1, the following corollary.

Corollary 5.4 *Let K be an algebraically closed field of $char(K) = p > 0$.*

Then K admits neither $\chi/\mathbf{F}_p$ if $p > 2$ nor $\chi/(\mathbf{Z}/m)$ if $m > \frac{3}{2}p$.

I do not know if K satisfies $Count_m$ whenever it satisfies it in dimension 1 (i.e., no counterexample can be $X \in Def^1(K)$). If so, then Theorems 3.7 and 5.1 alone imply that any algebraically closed field K admits weak $\chi/\mathbf{F}_q$ for primes $q < char(K)$. This, and more, is indeed true but for much deeper reasons, as the next example points out.

Example 5.5 *Let K be an algebraically closed field of $char(K) = p > 0$, and let ℓ be a prime different from p.*

Then Euler - Poincaré characteristic $\chi_c(X, \mathbf{Q}_\ell)$ given by the étale cohomology with ℓ - adic coefficients (cf. [17, 31]) determines a weak $\chi/\mathbf{Z}$.

Let us turn to pseudo-finite fields. These are infinite fields satisfying the theory of all finite fields, see e.g. [8] or the introduction to [22].

Theorem 5.6 *Pseudo-finite fields admit weak* χ/R*, for any finite* R*.*

Proof :
Any pseudo-finite field is elementarily equivalent to an ultraproduct of finite fields. As all finite fields trivially admit all $\chi/(\mathbf{Z}/m)$ and so also χ/R for all finite R, so do their ultraproducts (by Lemma 3.3). Hence all pseudo-finite fields admit weak χ/R (by Theorem 3.4).

q.e.d.

Now we turn to p-adics.

Lemma 5.7 *Let* $(\mathbf{Q}_p, \chi)$ *be an Euler structure. Then:*

$$(\chi(\mathbf{Q}_p) - 1) \cdot (\chi(\mathbf{Z}_p) - 1) = (\chi(\mathbf{Z}_p) - 1)^2$$

Proof :
Consider the bijection $({\mathbf{Z}_p}^*)^2 \to {\mathbf{Q}_p}^* \times {\mathbf{Z}_p}^*$ given by $(a, b) \to (a/b, \mathrm{hcf}(a, b))$, with the highest common factor chosen in a definable way. In particular, the first bracket in the equation corresponds to non-zero elements in $\mathbf{Q}_p$ expressed as ratios of coprime (p-adic) integers, the second bracket corresponds to non-zero integer scalars, and the right-hand side to non-zero elements in $\mathbf{Q}_p$, expressed as ratios of two not necessarily distinct coprime integers. Clearly the bijections between these definable sets are definable.

q.e.d.

Lemma 5.8 *Let* $q \geq 2$ *be a prime and let* $(\mathbf{Q}_p/(\chi/\mathbf{F}_q))$ *be an Euler structure. Then either* $q = 2 = p$*, or* $q | p - 1$ *and* $\chi(\mathbf{Z}_p) = 1$*.*

Proof :
Recall first that $\mathbf{Z}_p$ is definable in $\mathbf{Q}_p$, and observe that necessarily

1. $\chi(\mathbf{Q}_p) = 2 \cdot \chi(\mathbf{Z}_p) - 1$, as $\mathbf{Q}_p$ is in definable bijection (mimicking the construction of a quotient field) with a disjoint union of $\mathbf{Z}_p$ and inverses to non-zero elements in $\mathbf{Z}_p$.
2. $(p - 1)\chi(\mathbf{Z}_p) = 0$, as $\mathbf{Z}_p$ is equal to a disjoint union of $p\mathbf{Z}_p$, $1 + p\mathbf{Z}_p$, $2 + p\mathbf{Z}_p, \ldots, (p - 1) + p\mathbf{Z}_p$.

Define

$$P_n := \{x \in \mathbf{Q}_p \mid \exists y \neq 0, y^n = x\}$$

Then $\mathbf{Q}_p^*$ is a disjoint union of cosets of P_n; let $k(n)$ be the number of the cosets. So

$$\chi(\mathbf{Q}_p^*) = k(n)\chi(P_n)$$

Also $n|k(n)$ as $k(n) = [\mathbf{Q}_p^* : P_n]$. Hence taking $n := q$ yields $\chi(\mathbf{Q}_p^*) = 0$.

Using 1. above it follows:

$$\chi(\mathbf{Q}_p^*) = 2(\chi(\mathbf{Z}_p) - 1)$$

which gives that either $q = 2$ or $\chi(\mathbf{Z}_p) = 1$.

Using 2., the later option implies that $q|p-1$. This yields the statement.

q.e.d.

Note that in the previous two lemmas having a weak χ suffices.

Theorem 5.9 *For $p > 2$, $\mathbf{Q}_p$ does not admit weak $\chi/\mathbf{F}_q$, for any q not dividing $p-1$. $\mathbf{Q}_2$ does not admit weak $\chi/\mathbf{F}_q$, for any q.*

Proof : [2]

Lemma 5.8 implies the first part and rules out $q > p = 2$. the remaining case to rule out is $p = q = 2$. By the proof of Lemma 5.8 then $\chi(\mathbf{Q}_p) = 1$ (always) and $\chi(\mathbf{Z}_p) = 0$ (if $q = 2$). That contradicts Lemma 5.7, however.

q.e.d.

The theorem rules out the existence of some $\chi/\mathbf{F}_q$ but does not offer any positive examples. In this connection, as pointed out by L. van den Dries, there is an interesting remark in Serre [38]. Namely he considers two compact d-dimensional p-adic manifolds M, N and shows that these are analytically isomorphic iff $a_M \equiv a_N \pmod{p^d - 1}$, where M (resp. N) is a_M copies of $(\mathbf{Z}_p)^d$ (resp. a_N copies). This is akin to a property of $\chi/\mathbf{R}$, cf.[13, 14].

6 Degree lower bounds

We prove several degree lower bounds for NS and PC using the following sufficient condition derived from Theorem 4.1. We formulate the theorem to give non - constant lower bounds (as this is the most interesting threshold) but remark that the method of [28] gives in the same way actually $\Omega(\log(N))$ degree lower bounds for NS and $\Omega(\log\log(N))$ for PC.

Note that in the theorem we require Euler structure on M^* rather than just on M. This is because Lemma 4.2 allows to lift χ for M to M^* only for pure $L^*(C)$-structures but not necessarily for richer ones. In the applications we use structures that eliminate imaginaries and hence χ automatically lifts from M to M^*.

[2] D. Haskell proved recently that the p-adics admit no non-trivial χ/R, any R.

Theorem 6.1 *Let F be a uniform polynomial system of degree at most d polynomials (with variables indexed by k-indices and equations indexed by ℓ-indices), and let g be a uniform polynomial (i.e., a family consisting of one polynomial) with the same variables. Let $t \geq 1$. Then there is $\nu \geq 1$ depending only on k, ℓ, d and t such that the following holds.*

Assume that there is an Euler structure $(M^*, \chi/(\mathbf{Z}/p^\nu))$ in which a solution to $F^M = 0$ is definable (not necessarily $L^*(C)$-definable) not satisfying $g^M = 0$.

Then for no finite sufficiently large N, $N \equiv \chi(M) \pmod{p^\nu}$, does g^N have a degree t NS- or PC-proof from F^N.

Proof :

Let $t \geq 1$ be fixed. The idea of the proof is that we shall show in the Euler structure that both NS and PC (with their intrinsic definitions) are sound. The statement for NS follows from the statement for PC as any degree t NS-proof yields trivially a degree t PC-proof: derive first all multiples of F_i occurring in the NS-proof and the sum them all up (in fact, NS-proofs can be characterised as particular PC-proofs, see [6, Thm.4.1]). On the other hand, by [28, Thm.5.5] uniform families admitting constant degree PC-proofs admit also constant degree NS-proofs. Thus it is enough to treat the case of NS only.

Let $NS(t, F, g)$ be a uniform system constructed as $NS(d, \neg Count_q)$ in Example 1.2. This system will be solvable for finite N iff there is a degree at most t NS-proof of g^N from F^N. In particular, let $u_{i,j}$ be variables, i ranging over ℓ-indices and j ranging over monomials of degree at most t (i.e., particular tk-indices). Variable $u_{i,j}$ is intended to represent the coefficient (from $\mathbf{F}_p$) of the monomial j in G_i, if $\sum_i G_i F_i = g$ is the alleged NS-proof. Then such G_i of degree at most t exists iff

$$\sum_i \sum_{j_1, j_2 : j_1 \cup j_2 = j} u_{i,j_1} F_{i,j_2} = g_j$$

for all j (we put $g_j := 0$ for monomials j not occurring in g).

Let $a = (a_j)_j$ be the value of monomial j under a fixed assignment to variables of F satisfying all $F_i = 0$ but not $g = 0$. We shall show that this is a contradictory situation by computing the sum (via Euler characteristic):

$$\sum_i (\sum_{j_1} u_{i,j_1} a_{j_1})(\sum_{j_2} F_{i,j_2} a_{j_2})$$

to two different values. The sum is equal to

$$\sum_j \sum_i (\sum_{j_1, j_2 : j_1 \cup j_2 = j} u_{i,j_1} a_{j_1} F_{i,j_2} a_{j_2})$$

and assuming that $(u_{i,j})_{i,j}$ satisfy $NS(t, F, g)$ then it is also equal to

$$\sum_j g_j a_j$$

which does not equal 0 by the assumption.

On the other hand, by the hypothesis about a again all

$$\sum_{j_2} F_{i,j_2} a_{j_2} = 0$$

so the original sum is equal to 0 as well. That is a contradiction. It is straightforward to see that properties of evaluations of sums we used are among those provided for Euler structures by Lemma 2.8.

By Theorem 4.1 now (with F there being $NS(t, F, g)$ here), the system $NS(t, F, g)$ cannot be solved in any finite sufficiently large N of cardinality equal to $\chi(M)$ modulo p^ν either. As for finite N the unsolvability of $NS(t, F, g)^N$ means that g^N has no degree t NS-proof from F^N, we are done.

q.e.d.

The argument rests on two properties of the linear system $NS(t, F, g)$. First, its solvability for finite N is equivalent to the existence of degree t proof. Secondly, it is not some ad hoc system satisfying the first condition but it formalises the intrinsic definition of NS-provability as we need to prove the "soundness" of NS using the definition by the linear system. A proof for PC following similar lines is possible. The construction of the linear systems used as the intrinsic definition of PC in M (replacing $NS(t, F, g)$ above) and the proof of its soundness are more involved. The first part, the linear systems characterising PC, is provided by [28].

Example 6.2 ([34]) *There is no $t \geq 1$ such that for all finite N there are degree at most t PC-proofs of 1 (the so called refutations) from the system $\neg PHP^N$, over any $\mathbf{F}_p$.*

This follows from Theorem 6.1 and Example 4.13. $\chi(\mathbf{R}) = -1$ in Example 4.13 (cf. [13, 14]); to get other values modulo p^ν, consider the same function but defined on $\mathbf{R}$ without $i = 1, \ldots, p^\nu - 2$ negative numbers.

Next we derive two new degree lower bounds (proved in the same way). These examples are motivated by [35] and [27, Cor.11.3.3].

Example 6.3 *The system Dense with variables $x_{i,j}$ for $i \neq j$ and polynomials*

1. $x_{i,j}^2 - x_{i,j}$, *all* $i \neq j$.
2. $x_{i,j} + x_{j,i} - 1$, *all* $i \neq j$.
3. $x_{i,j} x_{j,k}(1 - x_{i,k})$, *all* i, j, k *different.*
4. $x_{i,j}(1 - \sum_{k \neq i,j} x_{i,k} x_{k,j})$, *all* $i \neq j$.

has no bounded degree PC-refutations (i.e., proof of 1) over any $\mathbf{F}_p$.

The system *Dense* is not solvable for any finite N as its solution defines a dense linear order $\{(i,j) \mid x_{i,j} = 1\}$ on the universe. However, it is trivially solvable in $(\mathbf{R}, \chi/\mathbf{Z})$. Hence Theorem 6.1 applies.

Example 6.4 *The system Max with variables $x_{i,j}$ for $i \neq j$ and y_i, and polynomials*

1. $x_{i,j}^2 - x_{i,j}$, *all* $i \neq j$.
2. $y_i^2 - y_i$.
3. $x_{i,j} + x_{j,i} - 1$, *all* $i \neq j$.
4. $x_{i,j}x_{j,k}(1 - x_{i,k})$, *all* i, j, k *different.*
5. $1 - y_0$.
6. $y_i(1 - \sum_{j \neq i} x_{i,j}y_j)$.

has no bounded degree PC-refutations (i.e., proof of 1*) over any* $\mathbf{F}_p$.

The system Max is not solvable for any finite N as its solution defines a linear order on the universe with a non-empty subset $0 \in \{i \mid y_i = 1\}$ not having a maximal element in the ordering. Again, it is trivially solvable in $(\mathbf{R}, \chi/\mathbf{Z})$ and Theorem 6.1 applies.

7 Definability of Euler characteristic

In this section we concern ourselves with the definable dependence of Euler characteristic on parameters.

Definition 7.1 *Let $(M, \chi/R)$ be an Euler structure. We say that χ is definable in M iff for all formulas $\phi(x_1, \ldots, x_k, y_1, \ldots, y_\ell)$ and all $a \in R$, the set*

$$\{\overline{x} \in M^k \mid \chi(\{\overline{y} \in M^\ell \mid M \models \phi(\overline{x}, \overline{y})\}) = a\}$$

is definable in M.

We say that χ is definable in a theory T iff such definitions common to all models of T exists.

Note that $\chi/\mathbf{Z}$ is definable in real closed fields, cf.[13]. By Theorems 3.7 and 5.2 all algebraically closed fields admit weak $\chi/\mathbf{F}_2$ but I do not know if it is definable, or even if the weak $\chi/\mathbf{Z}$ provided in Example 5.5 is definable.

Theorem 7.2 *Let T be a theory and R be finite. Assume that all models M of T admit exactly one (weak) χ/R.*

Then such an χ/R is unique and is definable in T.

Proof :

We shall use Beth's definability theorem. For every formula $\phi(\overline{x}, \overline{y})$ in the language of M and every $a \in R$ take a new relation symbols $R^a_\phi(\overline{x})$ with intended meaning

$$R^a_\phi(\overline{x}) \text{ is true} \quad \text{iff} \quad \chi(\{\overline{y} \mid \phi(\overline{x}, \overline{y})\}) = a$$

and write down the axioms of an Euler characteristic (of weak Euler characteristic, respectively).

By the hypothesis of the theorem, predicates R^a_ϕ are implicitly definable in T, and hence also explicitly.

q.e.d.

As $\chi/\mathbf{Z}$ is unique in algebraic closed fields of characteristic 0 (cf. [14]), $\chi/(\mathbf{Z}/m)$, any $m \geq 2$, is definable in their theory. I do not know if the weak $\chi/\mathbf{Z}$ provided for algebraically closed fields of non - zero characteristic by étale cohomology (see Example 5.5) is unique.

I have also one negative result.

Theorem 7.3 *Let $q \geq 2$ be a prime. Then the unique $\chi/\mathbf{F}_q$ in finite fields is not definable in the theory of finite fields.*

In fact, if the order of a prime p in ${\mathbf{F}_q}^*$ is at least 3 then the unique $\chi/\mathbf{F}_q$ is not definable in the theory of fields $\mathbf{F}_{p^\ell}$, $\ell \geq 1$, and, in particular, the cardinality of $\mathbf{F}_{p^\ell}$ modulo q is not definable in $\mathbf{F}_{p^\ell}$'s.

Proof :

If $\chi/\mathbf{F}_q$ were definable then there are, in particular, sentences $\Phi_{q,i}$, $i = 0, \ldots, q-1$, such that $\mathbf{F}_{p^\ell} \models \Phi_{q,i}$ iff $p^\ell \equiv i \pmod{q}$. We shall show that for $q \geq 5$ such a sentence does not exists for at least one i. Note that for $q = 2, 3$ such sentences do exist; we treat the cases $q = 2, 3$ separately.

Pick a prime p such that the minimal $t \geq 1$ for which $p^t \equiv 1 \pmod{q}$ is at least 3. Pick $1 < i < t$ coprime to t. Then:

1. $p^{tk+1} \equiv p \pmod{q}$, any $k \geq 1$.
2. $p^{tk+i} \equiv p^i \pmod{q}$, any $k \geq 1$.
3. For all $1 < j < t$: $p^j \not\equiv p \pmod{q}$, by the choice of t.

Now take the sentence

$$\Psi := \Phi_{q,(p \bmod q)} \wedge 0 = 1 + \ldots + 1 \quad (p\text{-times})$$

Then, by 3. above, $\mathbf{F}_{p^\ell} \models \Psi$ iff $\ell \equiv 1 \pmod{t}$.

The main theorem of Ax [3, p.240] implies, in particular, that there is $\omega \geq 1$ such that for all sufficiently large ℓ from the set

$$W := \{s \cdot \omega \mid s \geq 1 \wedge (s, \omega) = 1\}$$

$\mathbf{F}_{p^\ell}$ satisfies Ψ. Hence also $\ell \equiv 1 \pmod t$. But, as $(t,i)=1$, there are infinitely many primes $r \equiv i \pmod t$, by Dirichlet's theorem. Then for infinitely many $\ell' := s \cdot r \cdot \omega \in W$ (s as in the definition of W), $\ell' \equiv s \cdot i \cdot \omega \equiv i \pmod t$. This means that $\mathbf{F}_{p^{\ell'}}$ satisfies Ψ for such ℓ' too. However, that is a contradiction as by 2. and 3. above $p^{\ell'} \not\equiv p \pmod q$.

It remains to prove cases $q = 2$ and $q = 3$. We start with the later one. Define $X_{p^\ell} \subseteq \mathbf{F}_{p^\ell}$ as $X_{p^\ell} := \{y \in \mathbf{F}_{p^\ell} \setminus \{0\} \mid \exists x; x^3 = y\}$. Then, for $p > 3$ for which $x^3 = 1$ has three distinct roots, $|\mathbf{F}_{p^\ell}| = p^\ell = 3 \cdot |X_{p^\ell}| + 1$, so

$$p^\ell \equiv 4 \pmod 9 \ \text{ iff } \ \chi_3(X_{p^\ell}) = 1 \ .$$

Take e.g. $p := 7$. Then $7^\ell \equiv 4 \pmod 9$ iff $\ell \equiv 2 \pmod 3$, but the set $\{\ell \geq 1 \mid \ell \equiv 2 \pmod 3\}$ contains no set W of the form as above. Hence Ax's theorem implies that $\chi_3(X_{p^\ell})$ is not definable in $\mathbf{F}_{p^\ell}$'s.

The case $q = 2$ is treated analogously. Take $X_{p^\ell} := \{y \in \mathbf{F}_{p^\ell} \setminus \{0\} \mid \exists x; x^2 = y\}$ and $p := 3$. Then

$$p^\ell \equiv 3 \pmod 4 \ \text{ iff } \ \chi_2(X_{p^\ell}) = 1 \ .$$

We have $3^\ell \equiv 3 \pmod 4$ iff ℓ is odd, but odd numbers do not contain any set as W. So $\chi_2(X_{p^\ell})$ is undefinable in $\mathbf{F}_{p^\ell}$'s.

q.e.d.

Note that Theorems 7.2 and 7.3 imply that the class of pseudo-finite fields admits at least two non-equivalent $\chi/\mathbf{F}_q$, any $q \geq 2$. It is interesting to find extra parameters (structure) needed to define Euler characteristic on pseudo - finite fields (here [26] could help, see also [18, Sec.26.3]).

E. Hrushovski pointed out to me that perhaps (i) in any particular ultraproduct of finite fields the particular $\chi/\mathbf{F}_q$ is definable from suitable imaginary parameters related to étale cohomology (see also Example 5.5), and (ii) that in any pseudo-finite field every $\chi/\mathbf{F}_q$ might be definable from parameters related to non - standard Frobenius automorphisms, cf. [10, 29].

Whether (i) admits a more model - theoretic treatment and whether or not (ii) holds are interesting open problems, among others stemming from this paper.

Acknowledgements:

I outlined Theorem 6.1 during a DIMACS meeting in April 1996. I thank L. van den Dries (Urbana), I. Kříž (Ann Arbor), A. Macintyre (Edinburgh), J. Nekovář (Cambridge) and A. Wilkie (Oxford) for discussions on various related topics, D. Evans (Norwich) for references [19, 20], M. Aschenbrenner (Urbana) and E. Hrushovski (Jerusalem) for comments on sections 3 and 7 respectively, and O. Gabber (IHES) for confirming some facts behind Example 5.5.

References

[1] M.Ajtai, On the existence of modulo p cardinality functions, in: Feasible Mathematics II, eds. P. Clote and J. Remmel, Birkhauser. (1994), pp.1-14.

[2] M.Ajtai, Symmetric systems of linear equations modulo p, a preprint, (1994). Available as a report number TR94-015 of the *Electronic Colloquium on Computational Complexity*, http://www.eccc.uni-trier.de/eccc

[3] J. Ax, The elementary theory of finite fields, *Annals of Mathematics*, **88**, (1968), pp.239-271.

[4] P. Beame, S. A. Cook, J. Edmonds, R. Impagliazzo, and T. Pitassi, The relative complexity of NP search problems, in: Proceedings of the 27th ACM STOC, (1995), pp.303-314.

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

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

[7] S. R. Buss, and J. Krajíček, An application of boolean complexity to separation problems in bounded arithmetic, *Proceedings of the London Mathematical Society*, **69(3)**, (1994), pp.1-21.

[8] Z. Chatzidakis, Model theory of finite fields and pseudo-finite fields, *Annals of Pure and Applied Logic*, Vol. **88(2-3)**, (1997), pp.95-108.

[9] Z. Chatzidakis, L. van den Dries, and A. Macintyre, A., Definable sets over finite fields, *J. für die reine und angewandte Math.*, **427**, (1992), pp.107-135.

[10] Z. Chatzidakis, and E. Hrushovski, Model theory of difference fields, preprint, (1997).

[11] M. Clegg, J. Edmonds, and R. Impagliazzo, Using the Groebner basis algorithm to find proofs of unsatisfiability, in: *Proceedings of the 28th ACM Symposium on Theory of Computing*, ACM Press. (1996), pp.174-183.

[12] J. Denef, L. van den Dries, p-adic and subanalytic sets, *Annals of Math.*, **128**, (1988), pp.79-138.

[13] L. van den Dries, O-minimal structures, in: *Logic: from Foundations to Applications*, Eds.W.Hodges, M.Hyland, C.Steinhorn, J.Truss. European ASL meeting, Keele'93, Oxford Science Publ., Clarendon Press, Oxford. (1996), pp.137-186.

[14] L. van den Dries, *Tame topology and o-minimal structures*, London Math. Soc. Lecture Note Series, Vol. **248**, (1998), Cambridge University Press.

[15] L. van den Dries, D. Marker, and G. Martin, Definable equivalence relations on algebraically closed fields, *J. Symbolic Logic*, **54(3)**, (1989), pp.928-935.

[16] L. van den Dries, and C. Miller, On the real exponential filed with restricted analytic functions, *Israel J. of Math.*, **85**, (1994), pp.19-56.

[17] E. Freitag, and R. Kiehl, *Etale cohomology and the Weil conjecture*, Springer-Verlag, (1988).

[18] M. D. Fried, and M. Jarden, *Field arithmetic*, Springer-Verlag, (1986).

[19] D. G. D. Gray, The submodule structure of some permutation modules, *PhD. Thesis*, University of East Anglia, (1997).

[20] D. G. D. Gray, The structure of some permutation modules for the symmetric group of infinite degree, *J. of Algebra*, **193**, (1997), pp.122-143.

[21] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math., **52**, Springer Verlag, (1977).

[22] E. Hrushovski, and A. Pillay, Groups definable in local fields and pseudo-finite fields, *Israel J. of Math.*, **85**, (1994), pp.203-262.

[23] R. Impagliazzo, P. Pudlák, and J. Sgall, Lower Bounds for the Polynomial Calculus and the Groebner Basis Algorithm, preprint, (1997). Available as a report number TR97-042 of the *Electronic Colloquium on Computational Complexity*, http://www.eccc.uni-trier.de/eccc

[24] G. D. James, The module orthogonal to the Specht module, *J. of Algebra*, **46**, (1977), pp.451-456.

[25] G. D. James, *The representation theory of the symmetric groups*, LN in Mathematics, **Vol. 682**, Springer-Verlag, (1978).

[26] C. Kiefe, Sets definable over finite fields: Their Zeta functions, *Transactions of the A.M.S.*, **223**, (1976), pp.45-56.

[27] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[28] J. Krajíček, On the degree of ideal membership proofs from uniform families of polynomials over a finite field, *Illinois J. of Mathematics*, to appear (preprint 1997).

[29] A. Macintyre, Generic automorphisms of fields, *Annals of Pure and Applied Logic*, Vol. **88(2-3)**, (1997), pp.165-180.

[30] D. Marker, M. Messmer, and A. Pillay, *Model theory of fields*, Lecture Notes in Logic, Vol. **5**, Springer, (1996).

[31] J. S. Milne, *Étale cohomology*, Princeton University press, (1980).

[32] A. Pillay, Model theory of algebraically closed fields, in proceedings: *Stability theory and algebraic geometry, an introduction*, eds. E.Bouscaren and D.Lascar, to appear.

[33] A. Pillay, and C. Steinhorn, Definable sets in ordered structures I., *Transactions of the A.M.S.*, **295**, (1986), pp.565-592.

[34] A. A. Razborov, Lower bounds for the polynomial calculus, *Computational Complexity*, to appear (preprint 1997).

[35] S. Riis, Making infinite structures finite in models of second order bounded arithmetic, in: *Arithmetic,Proof Theory and Computational Complexity*, eds. P. Clote and J. Krajíček, Oxford University Press. (1993), pp.289-319.

[36] J. Robinson, Definability and decision problems in arithmetic, *J. of Symbolic Logic*, **14(2)**, (1949), pp.98-114.

[37] S. H. Schanuel, Negative sets have Euler characteristic and dimension, in: *Category Theory* Como'90, eds. A.Carboni, M.Pedicchio, G.Rosolini. LN in Mathematics, **1488**, Springer. (1991), pp.379-385.

[38] J. P. Serre, *Lie algebras and Lie groups*, Springer Verlag, (1992).

[39] S. Shelah, Every two elementary equivalent models have isomorphic ultrapowers, *Israel J. Math.*, **10**, (1971), pp.224-233.

[40] E. Sontag, Remarks on piecewise-linear algebra, *Pacific J. of Mathematics*, **98(1)**, (1982), pp.183-201.

[41] A. W. Strzebonski, Euler characteristic in semialgebraic and O-minimal groups, *J. of Pure and Applied Algebra*, **96**, (1994), pp.173-201.

[42] A. J. Wilkie, Some model completeness results for expansions of the ordered fields of reals by Pfaffian functions and exponentiation, *J. of the A.M.S.*, **9(4)**, (1996), pp.1051-1094.

[43] A. J. Wilkie, A general theorem on the complement and some new o-minimal structures, preprint, (1996).