COMBINATORICS WITH DEFINABLE SETS: EULER CHARACTERISTICS AND GROTHENDIECK RINGS

JAN KRAJÍČEK AND THOMAS SCANLON

ABSTRACT. We recall the notions of weak and strong Euler characteristics on a first order structure and make explicit the notion of a Grothendieck ring of a structure. We define partially ordered Euler characteristic and Grothendieck ring and give a characterization of structures that have non-trivial partially ordered Grothendieck ring. We give a generalization of counting functions to locally finite structures, and use the construction to show that the Grothendieck ring of the complex numbers contains as a subring the ring of integer polynomials in continuum many variables. We prove the existence of universal strong Euler characteristic on a structure. We investigate the dependence of the Grothendieck ring on the theory of the structure and give a few counterexamples. Finally, we relate some open problems and independence results in bounded arithmetic to properties of particular Grothendieck rings.

1. INTRODUCTION

What of elementary combinatorics holds true in a class of first order structures if sets, relations, and maps must be definable? For example, no finite set is in one-to-one correspondence with itself minus one point, and the same is true also for even infinite sets of reals if they, as well as the correspondences, are semi-algebraic, i.e. are definable in the real closed field $\mathbb{R}$. Similarly for constructible sets and maps in $\mathbb{C}$. On the other hand, the infinite Ramsey statement $\infty \to (\infty)^2_2$ fails in $\mathbb{C}$; the infinite unordered graph $\{(x,y) \mid x^2 = y \vee y^2 = x\}$ on $\mathbb{C}$ has no definable infinite clique or independent set. For a bit more involved examples consider: given two sets A, B, finite or infinite, there is an embedding of one into the other one. This is true also in the definable sense in $\mathbb{R}$ but not in $\mathbb{C}$. No finite set can be partitioned into m-element classes ($m \geq 2$) with the set minus one point also partitioned into m-element classes (this is the counting modulo m principle). This is true also for definable sets in $\mathbb{R}$ and $\mathbb{C}$ but for an algebraically closed field of non-zero characteristic the validity of the principle depends on m.

Particularly interesting situations arise when a principle of finite combinatorics holds not just for finite sets but also for definable sets, whether finite or infinite, and vice versa, when a principle of infinitary combinatorics fails for infinite definable sets.

The question was originally motivated by [9] where some combinatorics behind the representation theory of symmetric groups is lifted from finite sets to Euler

1991 *Mathematics Subject Classification.* Primary 03C07; Secondary 03F20, 68Q15.

Key words and phrases. First order structure, Euler characteristic, Grothendieck ring.

Partially supported by cooperative research grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech Republic) and the grant # A 101 99 01 of the Academy of Sciences of the Czech Republic.

Partially supported by an NSF MSPRF.

structures, in order to obtain a criterion for lower bounds on the degree of Nullstellensatz proof system. However, the connection to proof systems is not the topic of this paper. We consider this type of questions interesting in their own right and we study them from a purely model-theoretic point of view. Although this paper contains new material, its main purpose is to isolate a few notions, examples and problems that seem to us to be important.

The paper is organized as follows. In section 3 we recall the notions of weak and strong Euler characteristics on a first order structure and make explicit the notion of the Grothendieck ring of a structure, and recall a few facts from [9]. In section 4 we define and study partially ordered Euler characteristic and Grothendieck rings and give a characterization of structures that have non-trivial partially ordered Grothendieck ring. We give, in section 5, a generalization of counting functions to locally finite structures, and use the construction to show that the Grothendieck ring of complex numbers contains as a subring the ring of integer polynomials in continuum many variables. In section 6 we prove the existence of universal strong Euler characteristic on a structure. Section 7 is devoted to several open problems and to examples and partial results related to them. In particular, we investigate the dependence of the Grothendieck ring on the theory of the structure. In section 8 we relate some open problems and independence results in bounded arithmetic to properties of particular Grothendieck rings. Finally, the paper is concluded by a short section on abstract dimension function on a structure in the spirit of Schanuel [19].

We thank B. Poonen for the proofs of Lemmas 5.3 and 5.4, and P. Pudlák and J. Sgall for discussions about Problem 8.5.

2. Preliminaries

In this section we recall some definitions.

A structure is a first-order structure in a many-sorted language. If M is a one-sorted first-order structure, then we regard M as a many-sorted structure by taking the finite Cartesian powers of M as the basic sorts with the usual co-ordinate functions connecting these sorts. By M^{eq} we mean the many-sorted structure constructed from M having as its basic sorts the factor sets S/E where S is a basic sort of M and E is a definable equivalence relation. Definability always means with parameters.

If M is a structure, S is a basic sort of M, and $\varphi(x)$ is formula with free variable x ranging over S, then $\varphi(M) := \{x \in S^M : M \models \varphi(x)\}$. We may identify definable sets with the formulas defining them. So, if X is an M-definable set, then we might write $X(M)$ for X.

If M is a structure and S is a basic sort, then $\mathrm{Def}^S(M)$ is the set of all definable subsets of S. The set $\mathrm{Def}(M)$ is the union over all basic sorts S of $\mathrm{Def}^S(M)$. Two definable sets $A, B \in \mathrm{Def}(M)$ are definably isomorphic if there is a definable bijection $f : A \to B$. The set of definable sets in M up to definable isomorphism is denoted by $\widetilde{\mathrm{Def}}(M)$. Denote the quotient map by $[\,] : \mathrm{Def}(M) \to \widetilde{\mathrm{Def}}(M)$.

The onto-pigeonhole principle $ontoPHP$ is the statement that there are no set A, $a \in A$, and an injective map f from A onto $A \setminus \{a\}$. The (ordinary) pigeonhole principle PHP asserts that f cannot be onto any proper subset of A, i.e. any injective $f : A \to A$ is onto.

The modular counting principle $Count_m$ for $m \geq 2$, asserts that there is no set A, a subset $B \subseteq A$ of size $1 \leq |B| < m$, an m-partition R of A (i.e., a partition into blocks of size m), and an m-partition S of $A \setminus B$.

We say that a structure M satisfies one of the principles iff the principle holds when all sets, relations, functions are definable. We shall denote this fact $M \models PHP$ and similarly.

Note that if M is finite this is just finite combinatorics as all finite sets are definable. Similarly, if all subsets of (an infinite) M are definable, it is just infinitary combinatorics.

3. Euler characteristics and Grothendieck rings

Schanuel introduced Euler characteristics in slightly more generality than we consider in [19]. In this section we recall some constructions and some of their basic properties.

Given a structure M we give $\widetilde{\mathrm{Def}}(M)$ an $\mathcal{L}(+,\cdot,0,1)$ structure by defining

- $0 := [\varnothing]$;
- $1 := [\{*\}]$ where $* \in M$ is any element;
- $[A] + [B] := [A' \cup B']$ where $[A] = [A']$, $[B] = [B']$ and $A' \cap B' = \varnothing$; and
- $[A] \cdot [B] := [A \times B]$

$\widetilde{\mathrm{Def}}(M)$ is not a ring as $(\widetilde{\mathrm{Def}}(M), +, 0)$ is not a group.

Definition 3.1 ([9, Def 2.1])**.** Let M be a structure. A (weak) Euler characteristic on M with values in the commutative ring with unity R is a map $\chi : \mathrm{Def}(M) \to R$ of the form

$$\chi = \chi' \circ [\,]$$

such that χ' is an $\mathcal{L}(+,\cdot,0,1)$-homomorphism $\chi' : \widetilde{\mathrm{Def}}(M) \to R$. The fact that the values of χ are in R is sometimes denoted by symbol χ/R.

A strong Euler characteristic on M is a weak Euler characteristic $\chi : \mathrm{Def}(M) \to R$ satisfying the fiber condition:

If $f : A \to B$ is a definable function between definable sets, $c \in R$, and $\chi(f^{-1}\{b\}) = c$ for all $b \in B$, then $\chi(A) = c \cdot \chi(B)$.

The next theorem is from [9]; we recall it with its proof as the underlying construction is used in Definition 3.3 and Theorem 7.3.

Theorem 3.2 ([9, Thm.3.1])**.** *Let M be a structure. The following two properties are equivalent:*

(1) $M \models ontoPHP$.
(2) *There is a non-trivial ring R such that M admits weak χ/R.*

Proof: ([9])

The second property implies the first one as otherwise obviously $0 = 1$ in R. Assume now that the first property holds.

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

q.e.d

Definition 3.3. The Grothendieck ring of a structure M, denoted $K_0(M)$, is the ring $\tilde{R}$ constructed in the proof of Theorem 3.2. The particular weak Euler characteristic $\chi_0/K_0(M)$ constructed there is called the universal weak Euler characteristic.

Theorem 3.2 can thus be reformulated as

Corollary 3.4. *For M a structure, $K_0(M)$ is non-trivial iff $M \models ontoPHP$. If $\chi : \mathrm{Def}(M) \to R$ is a weak Euler characteristic then χ factors through χ_0.*

Example 3.5. Let M be finite. Then: $K_0(M) = \mathbb{Z}$.

Example 3.6. Let $\mathbb{R}$ be the real closed field. Then: $K_0(\mathbb{R}) = \mathbb{Z}$.

To see this let us denote χ_g the geometric Euler characteristic constructed on $\mathrm{Def}(\mathbb{R})$ via triangulation, and dim the dimension (see [5]). The existence of χ_g implies that $K_0(\mathbb{R})$ has $\mathbb{Z}$ as a quotient. On the other hand, for any two $A, B \in Def(\mathbb{R})$ having the same Euler characteristic $\chi_g(A) = \chi_g(B)$ and dimension $\dim(A) = \dim(B)$ there is a definable bijection $f : A \to B$ (see [5]). Assume that we have two definable sets U, V with $\chi_g(U) = \chi_g(V)$ but of possibly different dimensions. We may assume that $U, V \in \mathrm{Def}^{\mathbb{R}^k}(\mathbb{R})$, with $\dim(U), \dim(V) < k$. Pick $X \in \mathrm{Def}^{\mathbb{R}^k}(\mathbb{R})$ disjoint from both. Then $U \cup X$ and $V \cup X$ have the same χ_g as well as the dimension, and so are equivalent via a definable bijection. This means, that their classes in $K_0(\mathbb{R})$ are the same, by the definition of $K_0(\mathbb{R})$. Hence χ_g is the weak Euler characteristic from Theorem 3.2 and so $K_0(\mathbb{R}) = \mathbb{Z}$.

Example 3.7. Let $\mathbb{C}$ be the complex numbers. Then $K_0(\mathbb{C}) \supset \mathbb{Z}$. In fact, $K_0(\mathbb{C})$ admits $\mathbb{Z}[u, v]$ as a quotient.

The second statement is due to Denef and Loeser [4] and rests to a large extent upon the Hodge theory. We prove a stronger version of the first assertion in section 5.

Example 3.8. Given a prime p there is a pseudo-finite field F for which there are at least two distinct quotients of $K_0(M)$ isomorphic to $\mathbb{F}_p$.

This example is taken from [9, Thm.7.3].

We conclude the section by recalling from [9] a sufficient condition on M ensuring that $K_0(M)$ admits a particular finite field as a quotient.

Theorem 3.9 ([9])**.** *Let p be a prime and suppose that M satisfies the modular counting principle* Count_p*. Then $K_0(M)$ admits $\mathbb{F}_p$ as a quotient.*

If a linear ordering of M is definable in M and $K_0(M)$ admits $\mathbb{F}_p$ as a quotient then, on the other hand, M satisfies Count_p*.*

This is [9, L.3.6 and Thm.3.7].

4. Partially ordered Grothendieck rings

Definition 4.1. A partially ordered ring is a pair (R, P), where R is a ring (commutative with 1) and $P \subseteq R$ such that

(1) $0 \in P \ \& \ 1 \in P$
(2) $P + P \subseteq P$
(3) $P \cdot P \subseteq P$
(4) $x \neq 0 \ \& \ x \in P \Rightarrow -x \notin P$

We call P the set of non-negative elements.

Equivalently, a partially ordered ring is a commutative ring R with unity given together with a partial ordering $<$ for which $0 < 1$, $x < y \Rightarrow x + z < y + z$, and $(z > 0 \& x < y) \rightarrow xz < yz$. The equivalence is given by $P := \{x : x \geq 0\}$ and $x \leq y \Leftrightarrow y - x \in P$.

Definition 4.2. A weak Euler characteristic $\chi : \mathrm{Def}(M) \rightarrow R$ on the structure M is partially ordered if (R, P) is a partially ordered ring and $\chi(\mathrm{Def}(M)) \subseteq P$.

Equivalently, if $A \subseteq B$ are definable sets, then $\chi(A) \leq \chi(B)$.

Theorem 4.3. *Let M be a structure. The universal weak Euler characteristic $\chi_0 : \mathrm{Def}(M) \rightarrow K_0(M)$ is partially ordered iff M satisfies the pigeonhole principle PHP.*

Proof:

Equip already $\widetilde{\mathrm{Def}}(M)$ with the partial ordering defined as: $A \leq B$ iff there are disjoint sets $A', B', X \in \mathrm{Def}(M)$ such that $A = [A']$, $B = [B']$, and such that there is a definable injective mapping of $A' \cup X$ into $B' \cup X$. The fact, that the equivalence relation $A \leq B \wedge B \leq A$ induced by the partial ordering is not coarser than equality is exactly the principle PHP. **q.e.d**

Example 4.4. The universal weak Euler characteristic $\chi_0 : \mathrm{Def}(\mathbb{C}) \rightarrow K_0(\mathbb{C})$ on $\mathbb{C}$ is partially ordered. However, no strong χ/R on $\mathbb{C}$ is partially ordered.

The first part is, by Theorem 4.3, essentially a theorem of Ax [1] that $\mathbb{C} \models PHP$ and we expand on this observation in section 5. For the second part consider the two-to-one map $x \mapsto x^2$ on $\mathbb{C}^\times$. This certifies, using the fiber property of χ, that $\chi(\mathbb{C}^\times) = 2 \cdot \chi(\mathbb{C}^\times)$. Hence $\chi(\mathbb{C}^\times) = 0$ and $\chi(\mathbb{C}) = 1$. But $\{0, 1\} \subseteq \mathbb{C}$ is definable and has the Euler characteristic 2, contradicting the definition of partially ordered χ. A generalization of Ax's theorem to proalgebraic spaces is studied in [6]. The pigeonhole principle goes under the robotic name of "surjunctive" there.

Moreover, there is no nontrivial ordered Euler characteristic on $\mathbb{R}$ as the function $x \mapsto x + 1$ on the definable set $\{x \in \mathbb{R} : x > 0\}$ witnesses the failure of PHP.

Theorem 4.5. *If M is an infinite structure satisfying the pigeon hole principle, then the polynomial ring in one variable over $\mathbb{Z}$ is a subring of $K_0(M)$.*

Proof: By Theorem 4.3, the universal weak Euler characteristic $\chi_0 : \mathrm{Def}(M) \rightarrow K_0(M)$ is a partially ordered weak Euler characteristic. Let $X := \chi_0([M])$. If $(R, <)$ is a partially ordered ring and $a, b \in R$, then we define $a \ll b$ if there exists a positive integer k such that for any $n \in \omega$ we have $na < kb$.

Claim: *Let n be a natural number. If $P(x) \in \mathbb{Z}[x]$ is a polynomial of degree less than n, then $P(X) \ll X^n$ in $K_0(M)$.*

Proof of Claim: We prove this claim by induction on n. If $n = 0$, then $P = 0$, $X^0 = 1$, and $0 < 1$ by the definition of a partially ordered ring.

For $n = 1$, P is a constant polynomial a. Let $m \in \omega$. If $a \leq 0$, then $X > 0 \geq ma$. Otherwise, observe that for any m there is some subset of M of size ma (as M is infinite) so that $a \ll X$.

Consider now the case of $n + 1$. Write $P(X) = a + X \cdot Q(X)$ where $a \in \mathbb{Z}$. Let $k \in \omega$ so that for any $m \in \omega$ we have $mQ(X) < kX^n$. Then $mP(X) = ma + mX \cdot Q(X) < X + XkX^n \leq X^{n+1} + kX^{n+1} = (1 + k)X^{n+1}$. $\dashv$

Let now $P(x) \in \mathbb{Z}[x]$ be a nonzero polynomial. Write $P(x) = ax^d + Q(x)$ where Q is a polynomial of degree less than d and $a \neq 0$. Note that $P(X) = 0 \Leftrightarrow -P(X) = 0$, so we may and do assume that $a > 0$. By the claim we have $Q(X) \ll X^d \leq aX^d$. In particular, $Q(X) \neq -aX^d$ so $P(X) \neq 0$. Therefore, the map $\mathbb{Z}[x] \to K_0(M)$ given by $P(x) \mapsto P(\chi_0([M]))$ is an injection. **q.e.d**

We say that a structure satisfies the first *comparing of cardinalities* property CC_1 if for any two definable sets A, B, there is either a definable injective mapping of A into B or of B into A. The property CC_1 implies, in the presence of PHP, that the Grothendieck ring $K_0(M)$ is non-trivial and linearly ordered.

The intuitive property of comparing cardinalities can be formulated also in another way. We say that a structure satisfies the property CC_2 if for any two non-empty definable sets A, B, there is either a definable injective mapping of A into B or a definable surjective mapping of A onto B.

Both properties hold true for $\mathbb{R}$. To see CC_1 let A, B be two definable sets, w.l.o.g. from the same $Def^{\mathbb{R}^k}(\mathbb{R})$. If $dim(A) = dim(B)$, then we delete from either A or B few points to arrange also $\chi_g(A) = \chi_g(B)$. Then, similarly as in Example 3.6, we have a definable bijection between the modified pair, and hence an embedding of one of A or B into the other. If $\dim(A) < \dim(B)$, first replace B by its subset of dimension $\dim(A)$ and then proceed as before. The second comparing cardinalities property is treated analogously.

5. Counting functions

As noted earlier, the universal Euler characteristic for a finite structure is nothing other than the function which assigns to a definable set its cardinality. For infinite structures, such a counting function respects addition and multiplication, but it is not a ring homomorphism as cardinal addition and multiplication do not satisfy cancellation. However, infinite structures which are well-approximated by finite structures inherit counting functions from the finite approximations. In this section we note that counting functions on locally finite structures amalgamate to give a ring homomorphism from the Grothendieck ring to a ring of integer valued functions. Our construction works for any directed limit.

If $(I, <)$ is a directed set and $\{R_i\}_{i \in I}$ is a family of structures indexed by I, then we define the eventual product of this family to be the reduced product $\prod_{i \in I} R_i/\mathcal{C}$ where $\mathcal{C}$ is the filter generated by the cones on I. More concretely, $(x_i)_{i \in I} \sim (y_i)_{i \in I} \Leftrightarrow (\exists j \in I)(\forall k \geq j) x_k = y_k$.

We say that structure M is a *strong direct limit* of the directed system of structures $\{M_i\}_{i \in I}$ if $f : M^n \to M$ is a definable n-ary function, defined over M_i, then for any $j \geq i$ f maps (the image in M of) M_j^n back into M_j.

Theorem 5.1. *If $M = \varinjlim_{i \in I} M_i$ is a strong direct limit of structures and M eliminates quantifiers, then there is a natural homomorphism of rings from the Grothendieck ring of M to the eventual product of the Grothendieck rings of the directed system,*

$$\psi : K_0(M) \to \prod_{i \in I} K_0(M_i)/\mathcal{C} \ .$$

Proof: We define ψ on $\mathrm{Def}(M)$ as follows. Let X be a definable set. As M is the directed limit of the M_i's, there is some index i for which X is M_i definable by a

quantifier-free formula. Let $(x_j)_{j\in I} \in \prod_{j\in I} K_0(M_j)$ be the I-sequence with $x_j = 0$ for $j \not\geq i$ and $x_j = \chi_0(X_j) \in K_0(M_j)$ for $j \geq i$. Let $\psi(X)$ be the image of $(x_j)_{j\in I}$ in the eventual product. It is a routine matter to check that ψ is a well-defined homomorphism, but we include the details below.

The value of $\psi(X)$ does not depend on the choice of i: Suppose we were to choose $i' \in I$ so that X is defined over $M_{i'}$ and let $(x'_j)_{j\in I}$ be the element of $\prod_{j\in I} K_0(M_j)$ constructed from this choice of i'. As I is directed, there is some $i'' \in I$ with $i'' \geq i, i'$. Thus, $\{j : x_j = x'_j\} \supseteq \{j : j \geq i''\} \in \mathcal{C}$ which means by definition that the images of these elements in the reduced product are equal.

We check now that ψ induces a well-defined map on $\widetilde{\mathrm{Def}}(M)$. Suppose X and Y are definable with $[X] = [Y] \in \widetilde{\mathrm{Def}}(M)$. Take $i \in I$ so that X and Y are both defined over M_i and the isomorphism between X and Y is also defined over M_i. As M is a strong direct limit, $\chi_0(X) = \chi_0(Y) \in K_0(M_j)$ for all $j \geq i$. Thus, $\psi(X) = \psi(Y)$.

The fact that ψ respects the ring structure should be clear. **q.e.d**

Remark 5.2. The construction of the eventual limit is functorial. That is, if $\{\rho_i : R_i \to S_i\}_{i\in I}$ is a set of homomorphisms indexed by the directed set $(I, <)$, then the map given by co-ordinatewise application of the ρ_i's induces a map $\rho : \prod_{i\in I} R_i/\mathcal{C} \to \prod_{i\in I} S_i/\mathcal{C}$.

We apply the above construction to algebraically closed fields. For p a rational prime, $\mathbb{F}_p^{alg}$, the algebraic closure of the field $\mathbb{F}_p$ of p elements may be realized as a strong limit $\mathbb{F}_p^{alg} = \varinjlim \mathbb{F}_{p^n}$ where the directed index set is $\mathbb{Z}_+$ ordered by divisibility. The fact that this is a strong limit follows from quantifier elimination (which shows that every definable function $(\mathbb{F}_p^{alg})^n \to \mathbb{F}_p^{alg}$ is piecewise a polynomial composed with some integral power of the Frobenius) and the fact each finite field is perfect.

Each finite field $\mathbb{F}_q$ is finite, so its Grothendieck ring is $\mathbb{Z}$ with the function from $\widetilde{\mathrm{Def}}(\mathbb{F}) \to \mathbb{Z}$ given by counting. The above proposition yields a homomorphism $\psi_p : K_0(\mathbb{F}_p^{alg}) \to \prod_{n\in\omega} \mathbb{Z}/\mathcal{C}$. We use this homomorphism to exhibit a large algebraically independent subset of $K_0(\mathbb{F}_p^{alg})$. The following lemmata will show that if $\{E_i\}_{i\in I}$ is a set of pairwise non-isogenous ordinary elliptic curves over $\mathbb{F}_p^{alg}$, then $\{\psi_p(\chi_0(E_i))\}_{i\in I}$ is algebraically independent in $\prod_{n\in\omega} \mathbb{Z}/\mathcal{C}$. We then show that this property persists to $\mathbb{C}$ so that $K_0(\mathbb{C})$ contains an algebraically independent set of size continuum.

We recall Weil's formula for the number of points on an elliptic curve over a finite field (a reference for this and some facts used later is [13]). Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. The q-power Frobenius induces an algebraic endomorphism $F : E \to E$. The minimal polynomial of F over $\mathbb{Z}$ (considered as a subring of the endomorphism ring of E) is of the form $X^2 - aX + q$ with $a^2 < 4q$. Let α and $\bar{\alpha} \in \mathbb{C}$ be the conjugate roots of $X^2 - aX + q$. Then, for any n, the number of points in E rational over $\mathbb{F}_{q^n}$ is $1 - \alpha^n - \bar{\alpha}^n + q^n$. We refer to α as the *eigenvalue of Frobenius of* E. Of course, one cannot see the difference between α and $\bar{\alpha}$, but this choice should cause no confusion.

Weil's formula implies algebraic independence of non-isogenous ordinary elliptic curves once one knows that the eigenvalues of a family of non-isogenous elliptic curves are multiplicatively independent. This fact ought to be well-known, but we

could not find this statement in the literature. The proof given below is due to B. Poonen.

Lemma 5.3 (Poonen). *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}^\times$ be n complex numbers. We assume that $|\alpha_i| = 1$ and that $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] \leq 2$. If there is a non-trivial multiplicative relation among $\alpha_1, \ldots, \alpha_n$, then $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\alpha_j)$ for some $i \neq j$ or α_i is a root of unity for some i.*

Proof: We work by induction on n. The case of $n = 1$ is trivial. Consider the case of $n+1$. Suppose that $\prod_{i=1}^{n+1} \alpha_i^{m_i} = 1$ is a multiplicative relation. By induction, we may assume that all m_i's are nonzero, that no α_i is a root of unity, and that no two distinct α_i's generate the same quadratic extensions. As $\mathbb{Q}(\alpha_n) \neq \mathbb{Q}(\alpha_{n+1})$, there is some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1})/\mathbb{Q})$ with $\sigma(\alpha_n) = \alpha_n$ and $\sigma(\alpha_{n+1}) \neq \alpha_{n+1}$.

Note that

$$1 = \sigma(\prod_{i=1}^{n+1} \alpha_i^{m_i}) \prod_{i=1}^{n+1} \alpha_i^{m_i} = \prod_{\{i:\sigma(\alpha_i)\neq\alpha_i\}} |\alpha_i|^{m_i} \prod_{\{i:\sigma(\alpha_i)=\alpha_i\}} \alpha_i^{2m_i} = \prod_{\{i:\sigma(\alpha_i)=\alpha_i\}} \alpha_i^{2m_i}$$

This gives a nontrivial multiplicative among $\alpha_1, \ldots, \alpha_n$ contradicting the inductive hypothesis. **q.e.d**

Lemma 5.4 (Poonen). *If $E_1, \ldots, E_n$ are n pairwise (absolutely) non-isogenous elliptic curves over the finite field $\mathbb{F}_q$, then their eigenvalues of Frobenius $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent.*

Proof: Replacing q by q^2 and therefore each α_i by α_i^2 we may assume that q is a square. Set $e_i := \frac{\alpha_i}{|\alpha_i|} = \frac{\alpha_i}{\sqrt{q}}$. If there is a non-trivial multiplicative dependence amongst $\{\alpha_1, \ldots, \alpha_n\}$, then there must be such a dependence amongst $\{e_1, \ldots, e_n\}$. By Lemma 5.3, either some e_i is a root of unity or for some $i \neq j$ we have $\mathbb{Q}(e_i) = \mathbb{Q}(e_j)$.

An elliptic curve has eigenvalue of Frobenius a root of unity times the square-root of q if and only if it is supersingular and any two supersingular elliptic curves are absolutely isogenous. So, only one of the e_i's, say e_1, can be a root of unity. If the multiplicative relation involved any other e_i, then by raising the expression to the twelfth power, we would obtain a non-trivial multiplicative relation among $e_2, \ldots, e_m$. In this case we must have $\mathbb{Q}(\alpha_i) = \mathbb{Q}(e_i) = \mathbb{Q}(e_j) = \mathbb{Q}(\alpha_j)$ for some $i \neq j$, but the theory of complex multiplication shows that the Frobenii of two ordinary elliptic curves generate the same quadratic field if and only if the curves are absolutely isogenous. Thus, the only possible multiplicative relation among the e_i's is $e_i^m = 1$ (if E_i is supersingular), but $|\alpha_i^m| = q^{\frac{m}{2}} \neq 1$ unless $m = 0$. Therefore, there can be no multiplicative dependence amongst $\{\alpha_1, \ldots, \alpha_n\}$. **q.e.d**

Corollary 5.5. *If $E_1, \ldots, E_n$ are absolutely non-isogenous ordinary elliptic curves over a finite field $\mathbb{F}_q$ with eigenvalues of Frobenius $\alpha_1, \ldots, \alpha_n$, then $q, \alpha_1, \ldots, \alpha_n$ is a multiplicatively independent set.*

Proof: Without loss of generality, we may replace q with q^2. Let E_0 be a supersingular elliptic curve over $\mathbb{F}_q$. By the above lemma, the eigenvalues of Frobenius of $E_0, \ldots, E_n$ are multiplicatively independent. The eigenvalue of Frobenius of E_0 is a square root of q. Thus, $\sqrt{q}, \alpha_1, \ldots, \alpha_n$ are multiplicatively independent; and therefore $q, \alpha_1, \ldots, \alpha_n$ are multiplicatively independent. **q.e.d**

The next lemma translates multiplicative independence of the base of exponentials into algebraic independence.

Lemma 5.6. *Let $\alpha_1, \ldots, \alpha_n$ be sequence of algebraic numbers. Let $A_i : \mathbb{Z}_+ \to \mathbb{C}$ be the function $m \mapsto \alpha_i^m$. If $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent, then $A_1, \ldots, A_n$ are algebraically independent.*

Proof: Let $\mathfrak{p}$ be a nonzero prime of $\mathbb{Z}[\alpha_1, \alpha_1^{-1}, \ldots, \alpha_n, \alpha_n^{-1}]$. Let K be the $\mathfrak{p}$-adic completion of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. We will actually show that $A_1, \ldots, A_n$ are algebraically independent over K.

We work by induction on n. Suppose that $P(x_1, \ldots, x_n) \in \mathcal{O}_K[x_1, \ldots, x_n]$ is a nonzero integral polynomial for which $f(z) := P(A_1(z), \ldots, A_n(z)) \equiv 0$ as a function on $\mathbb{Z}_+$. We may assume that the hypersurface $V(P)$ defined by $P = 0$ has minimal degree among all possible witnesses of algebraic dependencies.

Replacing each α_i with the same power corresponds to restricting f to a smaller set. So, we may and do assume that each α_i is $\mathfrak{p}$-adically close enough to 1 so that the $\mathfrak{p}$-adic logarithm is defined at α_i. Let $B_i := \log_{\mathfrak{p}}(\alpha_i)$.

We note that f extends uniquely to a $\mathfrak{p}$-adic analytic function which has infinitely many zeroes and is therefore identically zero. Thus, the Taylor expansion of f is identically zero.

If we write

$$P(x_1, \ldots, x_n) = \sum_I p_I x^I$$

then we find that

$$0 = \frac{d}{dz} f(z) = \sum_I \sum_{i=1}^n p_I I_i B_i A(z)^I =: Q(A_1(z), \ldots, A_n(z)) \ .$$

If $V(Q) \not\supseteq V(P)$, then $(A_1(z), \ldots, A_n(z)) \in V(P, Q)$ which is a variety of dimension strictly less than $n-1$ (which would be ruled out by induction) or it is a hypersurface of degree strictly less than that of $V(P)$ (violating the minimality condition on P). Thus, there is some $\lambda \in K$ for which $Q = \lambda P$. That is, $\lambda p_I = (\sum_{i=1}^n I_i B_i) p_I$ for all multi-indices I. Taking $I \neq J$ with $p_I \neq 0$ and $p_J \neq 0$, we find that $\sum_{i=1}^n (J_i - I_i) B_i = 0$. As $I \neq J$, this equation gives a non-trivial $\mathbb{Z}$-linear relation among the B_i's. Applying the exponential function, this gives a non-trivial multiplicative relation among the α_i's. **q.e.d**

Theorem 5.7. *If $E_1, \ldots, E_n$ are non-isogenous ordinary elliptic curves over the algebraically closed field $\mathbb{F}_p^{alg}$, then $\chi_0(E_1), \ldots, \chi_0(E_n)$ are algebraically independent in $K_0(\mathbb{F}_p^{alg})$.*

Proof: Take q so that $E_1, \ldots, E_n$ are all defined over $\mathbb{F}_q$. Let $\alpha_1, \ldots, \alpha_n$ be the eigenvalues of Frobenius on $E_1, \ldots, E_n$. If

$$\psi_p(\chi_0(E_1)), \ldots, \psi_p(\chi_0(E_n))$$

were algebraically dependent, then there would be an algebraic dependence among $q^z, \alpha_1^z, \ldots, \alpha_n^z$ considered as functions on $\mathbb{Z}_+$. We know this to be impossible. **q.e.d**

Corollary 5.8. *There is an injective homomorphism $\mathbb{Z}[\{x_j : j \in \mathfrak{c}\}] \to K_0(\mathbb{C})$, where $\mathfrak{c}$ is the cardinality of continuum.*

Proof: Realize $\mathbb{C}$ as an ultraproduct $\prod_p \mathbb{F}_p^{alg}/\mathcal{U}$. We have a natural homomorphism $\varphi : K_0(\prod_p \mathbb{F}_p^{alg}/\mathcal{U}) \to \prod_p K_0(\mathbb{F}_p^{alg})/\mathcal{U}$. By Loś's Theorem, if $\{(j_p^\delta)\}_{\delta \in I}$ is a set of sequences of

j-invariants so that for any finite set $\delta_1, \ldots, \delta_n$ the set of p with $E_{j_p^{\delta_1}}, \ldots, E_{j_p^{\delta_n}}$ ordinary and pair-wise non-isogenous is in $\mathcal{U}$, then $\{\varphi(E_{[j^\delta]_\mathcal{U}})\}$ is an algebraically independent set. As there are infinitely many isogeny classes of ordinary elliptic curves over $\mathbb{F}_p^{alg}$, we may choose I to have the cardinality of the continuum. **q.e.d**

One could prove Corollary 5.8 by a direct algebraic argument, but the argument presented here shows that the algebraic independence holds even at the level of the Euler characteristics constructed from counting in finite fields.

6. Universal strong Euler characteristic

We would like a theorem analogous to Theorem 3.2 but for strong Euler characteristic, i.e. respecting also the fiber condition imposed on χ. Hence, one should factor $K_0(M)$ also by "relations" (one for each definable $f : A \to B$ and all $c \in R$):

$$\textbf{IF } \forall b \in B; \chi(f^{(-1)}(b)) = c \quad \textbf{THEN } \chi(A) = c \cdot \chi(B)$$

However, this is only a clause while we want equations. Imposing one of these relations may very well force one to impose another such not previously apparent. We note here that every structure admits a universal strong Euler characteristic.

Theorem 6.1. *For any structure M there is a universal strong Euler characteristic $\chi : \mathrm{Def}(M) \to K^s(M)$.*

Proof: We begin with some notation. If $f : A \to B$ is a definable family and $b \in B$, then we denote by $A(b)$ the fiber $f^{-1}\{b\}$.

We build χ by transfinite recursion. Start with $\chi_0 : \mathrm{Def}(M) \to K_0(M)$ the universal weak Euler characteristic. We build an inductive system of rings $\{\psi_{\alpha,\beta} : K_\alpha(M) \to K_\beta(M)\}_{\alpha<\beta}$ setting $\chi_\alpha := \psi_{0,\alpha} \circ \chi_0$. At successor stages $\alpha + 1$, let

$$K_{\alpha+1}(M) := K_\alpha(M)/(\{\chi_\alpha(B)\chi_\alpha(A(b_0)) - \chi_\alpha(A) : f : A \to B \text{ a definable family}$$
$$\text{with } b_0 \in B \text{ and } \chi_\alpha(A(b)) = \chi_\alpha(A(b_0)) \text{ for all } b \in B\})$$

and take for $\varphi_{\alpha,\alpha+1}$ the quotient map. At limit ordinals λ, we set $K_\lambda(M) := \varinjlim_{\alpha\to\lambda} K_\alpha(M)$ and let $\varphi_{\alpha,\lambda} : K_\alpha(M) \to K_\lambda(M)$ be the universal map to the direct limit. The universal strong Euler characteristic is $\chi_\alpha : \mathrm{Def}(M) \to K_\alpha(M)$ for $\alpha \gg 0$. We could take $\alpha = |\mathcal{L}_M|^+$.

The verification that this construction works is routine, but for completeness we include it.

Claim 1: *If $\varphi_{\alpha,\alpha+1} = \mathrm{id}_{K_\alpha(M)}$, then $\varphi_{\alpha,\beta} = \mathrm{id}_{K_\alpha(M)}$ for all $\beta > \alpha$.*

Proof of Claim: We prove this by transfinite induction on $\beta > \alpha$ with the result being assumed for $\beta = \alpha + 1$. For $\beta = \gamma + 1$ assuming the result for γ, if we have a definable family $f : A \to B$ and $b_0 \in B$ so that $\chi_\gamma(A(b)) = \chi_\gamma(A(b_0))$ holds for all $b \in B$, then by hypothesis we have $\chi_\alpha(A(b)) = \chi_\alpha(A(b))$ for all $b \in B$ already. Hence, by the definition of $K_{\alpha+1}(M)$, the equation $\chi_{\alpha+1}(A) - \chi_{\alpha+1}(A(b_0)) \cdot \chi_{\alpha+1}(B) = 0$ already holds in $K_{\alpha+1}(M)$ so that composing with $\varphi_{\alpha+1,\gamma}$ we see that $\chi_\gamma(A) = \chi_\gamma(A(b_0)) \cdot \chi_\gamma(B)$. As this is true for any such family, the quotient map $K_\gamma(M) \to K_{\gamma+1}(M)$ is the identity. At limits, this follows from the general fact that a limit of identity maps is the identity map. ⊣

Claim 2: *There is some* $\alpha < |\mathcal{L}_M|^+$ *such that* $\varphi_{\alpha,\alpha+1} = \mathrm{id}_{K_\alpha(M)}$.

Proof of Claim: Define $E_\alpha := \ker \varphi_{0,\alpha+1} \setminus \ker \varphi_{0,\alpha}$. Assuming that no such α exists, then $|\widetilde{\mathrm{Def}}(M)| \geq |K_0(M)| \geq \bigcup_{\alpha < |\mathcal{L}_M|^+} |E_\alpha| \geq |\mathcal{L}_M|^+ > |\widetilde{\mathrm{Def}}(M)|$ which is impossible. ⊣

First, we check that $\chi : \mathrm{Def}(M) \to K^s(M)$ is a strong Euler characteristic. Since $\chi = \varphi_{0,\alpha} \circ \chi_0$ is the composition of a ring homomorphism with the universal weak Euler characteristic, χ is at least a weak Euler characteristic. We check the fibre condition. Let $f : A \to B$ be a definable family and $b_0 \in B$ so that $\chi(A(b)) = \chi(A(b_0))$ for all $b \in B$. Take $\beta < \alpha$ large enough so that the inductive system has stabilized. Then $\chi_\beta(A(b)) = \chi_\beta(A(b_0))$ holds for all $b \in B$. The defining relations on $K_{\beta+1}(M)$ ensure that $\chi_{\beta+1}(A) = \chi_{\beta+1}(A(b_0)) \cdot \chi_{\beta+1}(B)$, so that applying $\varphi_{\beta+1,\alpha}$ we see that $\chi(A) = \chi(A(b_0)) \cdot \chi(B)$.

Next, we check that χ is universal. Let $\xi : \mathrm{Def}(M) \to R$ be any strong Euler characteristic. We show by transfinite induction that for every β there is a unique map $\tilde{\xi}_\beta : K_\beta(M) \to R$ so that $\xi = \tilde{\xi}_\beta \circ \chi_\beta$. For $\beta = 0$ this is simply the statement that χ_0 is the universal weak Euler characteristic. At a successor stage, we observe that if $f : A \to B$ is a definable family and $b_0 \in B$ with $\chi_\beta(A(b)) = \chi_\beta(A(b_0))$ for all $b \in B$, then $\xi(A(b)) = \tilde{\xi}_\beta(\chi_\beta(A(b))) = \tilde{\xi}_\beta(\chi_\beta(A(b_0))) = \xi(A(b_0))$ for all $b \in B$. Thus, $\xi(A) = \xi(A(b_0)) \cdot \xi(B)$ so that $\tilde{\xi}_\beta(\chi_\beta(A) - \chi_\beta(A(b_0)) \cdot \chi_\beta(B)) = 0$. That is, $\tilde{\xi}_\beta$ vanishes on the kernel of $\varphi_{\beta,\beta+1}$ so it induces a unique map on $K_{\beta+1}(M)$ as claimed. Finally, at limit stages, the existence and uniqueness of $\tilde{\xi}_\beta$ manifests the universality of the direct limit. **q.e.d**

7. Problems on Grothendieck rings and Euler structures

Problem 7.1. Is there a combinatorially transparent analogue of Theorem 3.2 for the universal strong Euler characteristic?

Problem 7.2. What is the relation between Grothendieck rings of elementarily equivalent structures?

Some properties of $K_0(M)$ are obviously properties of the theory of M. For example, whether $K_0(M)$ is non-trivial, by Theorem 3.2, or whether any particular finite ring is a quotient of $K_0(M)$, by [9, Thm.3.4]. Furthermore, if M is an elementary substructure of N then $K_0(M)$ is naturally embedded into $K_0(N)$. This is obvious from the construction (see also [9, L.3.2]). In fact, more is true.

Theorem 7.3. *Let M and N be two elementary equivalent structures. Then $\widetilde{\mathrm{Def}}(M) \equiv_{\exists_1} \widetilde{\mathrm{Def}}(N)$ in the language of rings. Thus, as the Grothendieck ring is existentially interpretable in $\widetilde{\mathrm{Def}}(M)$, we have $K_0(M) \equiv_{\exists_1} K_0(N)$.*

Proof: We begin by observing that if $\mathcal{U}$ is an ultrafilter on some index set I, then $\widetilde{\mathrm{Def}}(M^{\mathcal{U}})$ is a substructure of $\widetilde{\mathrm{Def}}(M)^{\mathcal{U}}$. As a general rule, if $A \subseteq B \subseteq C$ are $\mathcal{L}$-structures for some first-order language $\mathcal{L}$ and $A \preceq C$ is an elementary extension, then the extension $A \subseteq B$ preserves existential formulas (with parameters from A). Applying this general fact to $\widetilde{\mathrm{Def}}(M) \subseteq \widetilde{\mathrm{Def}}(M^{\mathcal{U}}) \subseteq \widetilde{\mathrm{Def}}(M)^{\mathcal{U}}$, we see that the inclusion $\widetilde{\mathrm{Def}}(M) \subseteq \widetilde{\mathrm{Def}}(M^{\mathcal{U}})$ preserves existential formulas.

By a theorem of Shelah [20], if $M \equiv N$, then there is an ultrafilter $\mathcal{U}$ so that $M^{\mathcal{U}} \cong N^{\mathcal{U}}$. Combining this fact with the previous paragraph we have $\widetilde{\mathrm{Def}}(M) \equiv_{\exists_1} \widetilde{\mathrm{Def}}(M^{\mathcal{U}}) \cong \widetilde{\mathrm{Def}}(N^{\mathcal{U}}) \equiv_{\exists_1} \widetilde{\mathrm{Def}}(N)$, as claimed. **q.e.d**

Example 7.4. One cannot replace $\exists_1$-equivalence by even $\forall\exists$-equivalence in general as the following example demonstrates.

Let $\mathcal{L} := \mathcal{L}(E)$ be the language having a single binary relation. Let M be the $\mathcal{L}$-structure in which E is interpreted as an equivalence relation for which every E-class is finite and for each positive integer n there is exactly one E-class of size n. By quantifier elimination in $\mathcal{L}_M$, $K_0(M)$ is generated by the image of $\mathrm{Def}^{M^1}(M)$. As M is a locally finite structure, we see that $K_0(M)$ is a partially ordered ring. Thus, $K_0(M)$ is isomorphic to $\mathbb{Z}[T]$ with $T = \chi_0([M])$. Let $N \succ M$ be the countable elementary extension in which there is exactly one infinite E-class, C. Realizing N as a submodel of an ultrapower of M, one sees that $\mathbb{Z} \ll \chi_0([C]) \ll \chi_0([N])$ so that $K_0(N)$ is isomorphic to $\mathbb{Z}[T,S]$ with $T = \chi_0([N])$ and $S = \chi_0([C])$. The inclusion $\mathbb{Z}[T] \hookrightarrow \mathbb{Z}[T,S]$ is not even an $\forall\exists$-extension as $\mathbb{Z}[T]$ has Krull dimension two while $\mathbb{Z}[T,S]$ has Krull dimension three. The condition that a Noetherian commutative ring have Krull dimension less than three may be expressed by:

$$(\forall x,y,z)(\exists a,b,c)[ax+by+cz = 1 \vee ax+by = z \vee by+cz = x \vee ax+cz = y]$$

Remark 7.5. If M is $\aleph_0$-saturated, then for any elementary extension $N \succeq M$ we have $K_0(M) \preceq K_0(N)$.

Remark 7.6. The above proof actually takes place at the level of $\widetilde{\mathrm{Def}}(M)$ and passes to $K_0(M)$ via the interpretability of $K_0(M)$ in $\widetilde{\mathrm{Def}}(M)$ in the language of rings. The same proof fails for strong Euler characteristics as the fiber condition is not definable in the ring language. In fact, there are structures which admit no non-trivial strong Euler characteristic but which have elementary extensions possessing non-trivial strong Euler characteristics. If $A \subseteq M$ is a subset, then we denote by $\mathrm{Def}(M)_{/A}$ the class of A-definable sets in M and by $\widetilde{\mathrm{Def}}(M)_{/A}$ the class of A-definable sets in M up to M-isomorphism. If $M \preceq N$ is an elementary extension, then the identification of $\widetilde{\mathrm{Def}}(M)$ with $\widetilde{\mathrm{Def}}(N)_{/M}$ induces a map from the image of $\widetilde{\mathrm{Def}}(N)_{/M}$ in $K^s(N)$, denoted $K^s(N)_{/M}$, onto $K^s(M)$. This map may have a nontrivial kernel.

Problem 7.7. Which fields admit nontrivial strong Euler characteristic?

Algebraically closed fields of characteristic zero, real closed fields, finite and pseudo-finite fields do admit strong Euler characteristic (see [9] for examples).

Algebraically closed fields of positive characteristic do not admit strong Euler characteristics (cf. also [9, Sec.5]). We give the calculation in characteristic greater than two. Let K be an algebraically closed field of characteristic $p > 2$. The function $K^\times \to K^\times$ given by $x \mapsto x^2$ has fibers of size two over every point so that by the fiber condition, $\chi([K^\times]) = 0$. The function $K \setminus \{0,1\} \to K^\times$ given by $x \mapsto x^{p+1} - x^p$ has fibers of size $p+1$ over every point so that $-1 = \chi([K \setminus \{0,1\}]) = (p+1)\chi([K^\times]) = 0$. For characteristic two use the Artin-Schreier map $x \mapsto x^2 + x$ to calculate $\chi([K]) = 0$ and then use $x \mapsto x^3 + x^2$ as above.

D. Haskell [7] has shown that p-adic fields do not even admit non-trivial weak Euler characteristics.

Do any other fields admit strong χ/R?

Problem 7.8. Which fields admit nontrivial strong partially ordered Euler characteristic?

We note that such a field is necessarily perfect and quasi-finite. That is, its absolute Galois group is isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of the integers.

Finite and pseudo-finite do, while real closed and algebraically closed do not. Obviously, even weak ordered χ implies perfection.

However, weak ordered χ is not enough to guarantee pseudo-finiteness. To see this we borrow an example from [1]. Consider the field that is a union of finite fields with p^{q^k} elements, $k = 1, 2, \ldots$, and p, q fixed different primes. It is perfect, PAC (pseudo-algebraically closed) but not pseudo-finite. In the field the algebraic and the model-theoretic closure coincide and so a definable function is piece-wise rational. Hence such a field satisfies PHP (otherwise some of the finite subfields would contain a counter-example to PHP), and that yields, by Theorem 4.3, an ordered weak χ.

A class of fields of interest with respect to this problem is the class of non-standard finite fields in models of arithmetic, defined as residue fields modulo a non-standard prime. If the models satisfy PA the fields are just - up to elementary equivalence - pseudo-finite fields of characteristic zero, cf. [11]. In these models the fields admit an ordered strong Euler characteristic based on counting.

Now assume the models satisfy only some bounded arithmetic theory (cf. Section 8). If counting were definable in the theory, the fields admit again an ordered strong Euler characteristic. Hence a proof that only finite or pseudo-finite fields admit strong partially ordered χ either gives an independence of counting from the bounded arithmetic theory or improves upon [11] considerably (for a partial result in this direction see [3]).

Problem 7.9. To what extent is the Grothendieck ring of a structure definable (perhaps in terms of some imaginary parameters associated to the structure)?

Especially interesting cases: $\mathbb{C}$ and models of $I\Delta_0^{top}$ (see next section).

We remark that the universal weak Euler characteristic in $\mathbb{R}$ is definable in $\mathbb{R}$, cf. [5] while the universal strong Euler characteristic on $\mathbb{C}$ is definable in $\mathbb{C}$. In particular, given a definable $f : A \to B$ between definable A, B, and given $n \in \mathbb{Z}$, the set $\{b \in B \mid \chi_0(f^{(-1)}(b)) = n\}$ is also definable.

A particularly interesting special case of the previous problem is

Problem 7.10. Describe all $\chi/\mathbb{F}_q$ on pseudo-finite fields, or at least on ultraproducts of finite fields.

This problem is related to [9, Thm.7.3] (see remarks there).

8. Examples from bounded arithmetic

Bounded arithmetic $I\Delta_0$, defined by Parikh [14], is a subtheory of Peano arithmetic with induction for bounded formulas only (the language is $\{0, 1, +, \times, =, \leq\}$) (see also [8] for a general reference on bounded arithmetic). One of the oldest and most interesting open problems about bounded arithmetic was posed by A. Macintyre some twenty years ago: Does $I\Delta_0$ prove that no function defined by a Δ_0-formula maps injectively an interval $[0, n]$ into $[0, n)$? This statement is called the Δ_0 pigeonhole principle $\Delta_0 - PHP$; similarly for the onto-version. We shall see that the problem simply asks whether a certain Grothendieck ring is trivial or not.

First let us observe that $\Delta_0 - PHP$ is equivalent to the version of PHP formulated for all Δ_0 maps and Δ_0 sets that are not cofinal. Assume $f : X \to X$ maps injectively a non-cofinal set $X \subseteq [0, n]$ into its proper subset. By possibly adding n to X and changing one or two values of f we may assume that $n \in X \setminus Rng(f)$. Then the map extending f by identity $id_{[0,n]\setminus X}$ contradicts the original formulation of $\Delta_0 - PHP$.

Let $I\Delta_0^{top}$ be the theory like $I\Delta_0$ but only on bounded intervals $[0, e]$ (it was considered already by Paris and Wilkie). Namely, the language L_B of the theory is as of $I\Delta_0$ augmented by a new constant e, except that the operations $+$ and $\times$ are replaced by ternary relations $\oplus$, $\otimes$ (standing for their graphs). The constant e is interpreted as the largest element with respect to the linear ordering $\leq$, and the axiomatization states basic properties of 0, 1, $\oplus$, $\otimes$, $\leq$ on the interval $[0, e]$, and asserts the induction for all formulas (all quantifiers are implicitly bounded by e).

Having a model M of $I\Delta_0$ and $n \in M$, $[0, n]$ is a model of $I\Delta_0^{top}$ under the natural interpretation of the language. On the other hand, a model $[0, e]$ of $I\Delta_0^{top}$ defines uniquely (via e-adic notation for numbers) a model M of $I\Delta_0$, in which $[0, e]$ is an initial interval and in which the (standard) powers of e are cofinal. Definable subsets of $[0, e]^k$, $k = 0, 1, \ldots$, are in one-to-one correspondence with subsets of M that are definable by Δ_0-formulas and that are not cofinal in M. Thus M satisfies PHP for Δ_0 sets and maps iff $[0, e]$ satisfies PHP for all definable sets and maps. Hence we have

Theorem 8.1. *The Δ_0-PHP (resp. the Δ_0-ontoPHP) is independent from $I\Delta_0$ iff there is a model $M \models I\Delta_0^{top}$ for which $K_0(M) = 0$ or χ_0 is not a partially ordered Euler characteristic (resp. $K_0(M) = 0$).*

Various independence results are known for a modification of these theories. Namely, one augments the language by a unary predicate symbol α. The symbol α may appear in $\Delta_0(\alpha)$-formulas in induction axioms but the theory, denoted $I\Delta_0(\alpha)$, has no special axioms about α. (One may think about α as about unknown oracles in complexity theory.) The theory $I\Delta_0(\alpha)^{top}$ is defined analogously as before. Assuming that the predicate α is not cofinal in M, the relation between models of $I\Delta_0(\alpha)$ and $I\Delta_0(\alpha)^{top}$ is as described above, taking n such that some power n^k bounds α.

Example 8.2. Let p, q be two different primes. There is a structure M whose Grothendieck ring $K_0(M)$ admits $\mathbb{F}_q$ as a quotient but not $\mathbb{F}_p$. In particular, $K_0(M)$ does not admit $\mathbb{Z}$ as a quotient.

By [2] there is a model N of $I\Delta_0(\alpha)$ that satisfies $\Delta_0(\alpha)$-$Count_q$ but not the $\Delta_0(\alpha)$-Count$_p$ (the counting principles are also restricted to non-cofinal sets). The

structure M is a suitable model of $I\Delta_0(\alpha)^{top}$, obtained from N as above. By Theorem 3.9 the validity of $Count_q$ guarantees the existence of weak $\chi/\mathbb{F}_q$ while the failure of Count_p shows that no weak $\chi/\mathbb{F}_p$ exists on M.

The weak pigeonhole principle WPHP asserts that no two disjoint copies $A \dot\cup A$ of a set A can be injectively mapped into A. This principle is prominent in bounded arithmetic and complexity theory.

Example 8.3. There is a structure M whose Grothendieck ring $K_0(M)$ is trivial but which satisfies the weak pigeonhole principle $WPHP$.

By [16, 10, 18] there is a model N of $I\Delta_0(\alpha)$ that satisfies $\Delta_0(\alpha)$-$WPHP$ but not the $\Delta_0(\alpha)$-$ontoPHP$. The structure M is again a suitable model of $I\Delta_0(\alpha)^{top}$, obtained from N as above. For another example, consider $(\mathbb{N}, S)$ where S is the successor operation.

Example 8.4. There are structures M_1 and its elementary extension M_2 such that the Grothendieck ring $K_0(M_1)$ is properly included in $K_0(M_2)$.

Let N be a non standard model of true arithmetic. Consider models N_e of $I\Delta_0^{top}$ with universe $[0, e]$ for $e \in N$. We claim that there are non-standard $e_1, e_2 \in N$ such that N_{e_1} is an elementary substructure of N_{e_2} and $2^{e_1} < e_2$. The former condition means that e_1, e_2 satisfy in N the same bounded formulas with any parameters smaller than e_1. The existence of suitable e_1, e_2 follows, in particular, from an argument that the Paris-Harrington principle implies the consistency of PA, as given in [15].

Take $M_i := N_{e_i}$, $i = 0, 1$. It remains to show that for some $B \in Def(M_2)$, the universal weak Euler characteristic $\chi_{M_2}(B) \in K_0(M_2) \setminus K_0(M_1)$. Put $B := [0, e_2)$. Assume $\chi_{M_2}(B) \in K_0(M_1)$, so there is a definable (in M_2) bijection between disjoint unions $A \cup X$ and $B \cup X$, where $A \in Def(M_1)$ and $X \in Def(M_2)$. The bijection is also definable in N and hence preserves cardinalities of finite sets. So $|A| = |B|$. But that is impossible as $|A| \leq e_1^k < 2^{e_1} < e_2 = |B|$, for some standard k.

We conclude the section by a problem motivated by considerations about Macintyre's problem mentioned earlier. We shall not explain the connection here, but the problem seems to be sufficiently interesting in its own right.

In general form the problem asks whether the principles of comparing cardinalities CC_1 or CC_2 formulated at the end of section 4 hold effectively. Specifically (for CC_1) this can be formulated as follows: Is there a constant k such that whenever A and B are subsets of $\{0,1\}^n$ that are computable by circuits of size S, then there is an injective mapping f of either A into B or vice versa such that the graph of f is computable by a circuit of size $\leq S^k$?

This general problem is clearly related to counting of polynomial time sets and using Toda's theorems [21] one can answer the problem in the negative, assuming that the polynomial time hierarchy does not collapse.

It would be very interesting however, to solve the problem unconditionally at least in the case of AC^0 circuits.

To make this self-contained let us give a model-theoretic definition of what it means that a sequence of sets X_n of subsets of $\{1, \ldots, n\}^k$, $n = 1, 2, \ldots$, is AC^0 definable. Let $R(x_1, \ldots, x_k)$ be a k-ary relation symbol. Then $\{X_n\}_{n<\omega}$ is AC^0 definable iff there are a first order language L not containing R, L-structures A_n with universe $\{1, \ldots, n\}$, $n = 1, 2, \ldots$, and a sentence Φ in language $L \cup \{R\}$ such that for any n and any $Y \subseteq \{1, \ldots, n\}^k$, $Y \in X_n$ iff the expanded structure (A_n, Y) satisfies Φ.

We propose the following combinatorial example. Sets A and $B(k)$, for $k > 0$ a fixed number, will be sets of graphs on n vertices without loops. The set A consists of directed graphs that are vertex-disjoint unions of directed cycles. The set $B(k)$ consists of undirected graphs that are vertex-disjoint unions of cycles, each cycle having one of k colors. In particular, in graphs from $B(1)$ all cycles have the same color.

Clearly all sets A, $B(k)$ are AC^0 definable.

Problem 8.5. (1) Is there an embedding of $B(1)$ into A with AC^0 definable graph?
(2) Is there a bijection between $B(2)$ and A with AC^0 definable graph?
(3) Is there an embedding of A into $B(k)$, any $k > 2$, with AC^0 definable graph?

(M. Ajtai told us that he proposed exactly problem 2. some ten years ago.) We would expect the answer in the negative for all three questions.

9. Abstract dimension

In classical geometric examples a notion closely associated to Euler characteristic is that of dimension. In this section we recall a few facts specialized to the category of definable sets. We do not have any original material to add but we think that the topic should be further investigated and we wish to bring it to an attention.

We recall first a construction of Schanuel [19]. Schanuel uses the notion of a "rig", a "ring without negatives". (Other authors use the term "semiring.") Examples: natural numbers $\mathbb{N}$, polynomials from $\mathbb{N}[x]$, the collection $\widetilde{\mathrm{Def}}(M)$ of definable sets modulo definable bijections we defined earlier. Other examples come from distributive categories: rigs of isomorphism classes of objects added by coproduct and multiplied by product.

Formally, a rig is a structure with two commutative monoid structures $(R, 0, +)$ and $(R, 1, \cdot)$ related by: $a \cdot 0 = 0$ and by distributivity.

An abstract dimension function on M is a rig homomorphism $d : \widetilde{\mathrm{Def}}(M) \to R$ on $\widetilde{\mathrm{Def}}(M)$ with values in a rig R satisfying $1 + 1 = 1$. One may regard such a structure as an upper semi-lattice $(R, e, \leq, \vee, 0, \oplus)$ in which $+$ on $\widetilde{\mathrm{Def}}(M)$ becomes $\vee$, $\cdot$ becomes $\oplus$, 0 maps to e, and 1 maps to 0.

There is a *universal (abstract) dimension* dim on M, an arbitrary structure. It is the map $[\,] : \mathrm{Def}(M) \to \widetilde{\mathrm{Def}}(M)$ composed with a universal map $\dim : \widetilde{\mathrm{Def}}(M) \to \mathcal{D}(M)$ from the rig $\widetilde{\mathrm{Def}}(M)$ to the quotient of $\widetilde{\mathrm{Def}}(M)$ by the congruence defined by $1 + 1 = 1$. The explicit construction is as follows. Define on $\widetilde{\mathrm{Def}}(M)$

$$a \leq b \text{ iff } \exists n \in \mathbb{N} \exists x \in \widetilde{\mathrm{Def}}(M); a + x = \overbrace{b + \cdots + b}^{n \text{ times}}$$

and then define a congruence by:

$$a \sim b \text{ iff } a \leq b \wedge b \leq a \ .$$

This always yields a nontrivial rig as obviously $[\{a\}] \not\leq [\emptyset]$. However, the qualification non-trivial may mean just having cardinality 2.

Let us mention a few examples. The real closed field $\mathbb{R}$ admits a dimension function constructed via triangulation of definable sets, *cf* [5]. It is the geometric dimension with values in $\mathbb{N} \cup \{-\infty\}$. In stability theory the global ranks on definable

sets, for example Morley rank, factor through dim. Definable sets in the ring of integers $\mathbb{Z}$ have only three possible dimensions, corresponding to the empty set, finite sets and infinite sets (all non-empty finite set have the same dimension and all infinite sets have even the same $[\,]$-value in $\widetilde{\mathrm{Def}}(\mathbb{Z})$).

It would be very interesting if under some general conditions the values of χ_0 and dim classify definable sets up to definable bijections. This is, for example, the case of $\mathbb{R}$, cf. [5].

References

[1] J. Ax, The elementary theory of finite fields, *Annals of Mathematics*, **88(2)**, (1968), pp.239-271.

[2] 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.

[3] P. D'Aquino and A. Macintyre, Non standard finite fields over $I\Delta_0 + \Omega_1$, (1999), preprint.

[4] J. Denef and F. Loeser, Germs of arcs on singular algebraic varieties and motivic integration, *Inventiones Mathematicae*, **135**, (1999), pp.201-232.

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

[6] M. Gromov, Endomorphisms of symbolic algebraic varieties, *J. of the European Mathematical Society*, **1(2)**, (April 1999), pp.109-236.

[7] D. Haskell, $K_0(\mathbb{Q}_p) = 0$, unpublished notes, (1999).

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

[9] J. Krajíček, Uniform families of polynomial equations over a finite field and structures admitting an Euler characteristic of definable sets, *Proc. London Mathematical Society*, to appear. (preprint 1997).

[10] J. Krajíček, P. Pudlák, and A. Woods, Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, *Random Structures and Algorithms*, **7(1)**, (1995), pp.15-39.

[11] A. Macintyre, Residue fields of models of P, in: *Logic, Method. and Phil. of Sci.*, eds. L.E.Cohen et. al., (1982), pp.193-206.

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

[13] C. Moreno, *Algebraic Curves Over Finite Fields*, Cambridge University Press, (1993).

[14] R. Parikh, Existence and feasibility in arithmetic, *Journal of Symbolic Logic*, **36**, (1971), pp.494-508.

[15] J. B. Paris and L. Harrington, A mathematical incompleteness in Peano Arithmetic, in: *Handbook of Mathematical Logic*, Ed. J. Barwise, (1978), pp.1133-1142. North-Holland.

[16] J. B. Paris, A. J. Wilkie, and A. R. Woods, Provability of the pigeonhole principle and the existence of infinitely many primes, *Journal of Symbolic Logic*, **53**, (1988), pp.1235–1244.

[17] 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.

[18] T. Pitassi, P. Beame, and R. Impagliazzo, Exponential lower bounds for the pigeonhole principle, *Computational complexity*, **3**, (1993), pp.97-308.

[19] 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.

[20] S. Shelah, Every two elementarily equivalent models have isomorphic ultrapowers, *Israel J. Math* **10** (1971), 224 233.

[21] Toda, S. (1989) On the computational power of PP and $\oplus P$, in:*Proc. 30th IEEE Symp. on the Found. of Computer Science*, pp. 514-519.

Mathematical Institute, Academy of Sciences, Žitná 25, Prague, 115 67, The Czech Republic

E-mail address: krajicek@math.cas.cz

University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley, CA 94720-3840, USA

E-mail address: scanlon@math.berkeley.edu