EXPONENTIAL SUMS IN PSEUDOFINITE FIELDS AND APPLICATIONS

IVAN TOMAŠIĆ

Abstract. We show how character integrals in pseudofinite fields can be applied to the study of 'random' reducts of pseudofinite fields.

1. Introduction

This paper falls naturally into two parts. In the first part we lift the classical estimates for exponential sums in finite fields to the context of exponential integrals in pseudofinite fields (yielding equidistribution-style results), where the integration is with respect to the measure from [3].

The subject of exponential sums in finite fields has a long and rich history, culminating with Deligne's celebrated proof of Weil conjectures in [5]. We choose to concentrate only on additive and multiplicative character sums over a variety for the moment.

A great motivating force in Model Theory in the past few decades has been a conjecture by Zil'ber that a model of an uncountably categorical theory must essentially be either a trivial (degenerate) structure, or a vector space, or an algebraically closed field. The conjecture was refuted in full generality in [9], and then proved for Zariski structures in [10]. An important open question, addressed in [13], is whether the above trichotomy holds for structures interpretable in algebraically closed fields. By analogy, one can also ask whether it is possible to classify rank one structures interpretable in pseudofinite fields. In that case, we expect that:

(1) model-theoretically trivial structures should be those governed exclusively by randomness and probabilistic phenomena, e. g., various random graphs;
(2) one-based nontrivial structures should be identifiable with vector spaces (see [17]), again equipped with additional random structure, e. g., a non-degenerate bilinear form;
(3) non-one-based structures should interpret a finite extension of the ground field.

2000 *Mathematics Subject Classification.* Primary 03C60, 11G25, 11T23, 14G10, 14G15. Secondary 03C35, 05C80.

The research was done as a part of an EPSRC-funded project at the University of Leeds.

In the second part of this paper we are making the first step toward the case (1) above. More precisely, let X be a variety over a pseudofinite field F, let f be a regular (or rational when X is irreducible) function on $X \times X$ and let $k > 1$ a natural number. We consider graphs of the form $\langle X(F), R\rangle$, where $R(x, y) \equiv \exists Z f(x, y) = Z^k$. In Section 5 we exhibit a family of relatively complex examples which are ω-categorical. On the other hand, as a somewhat surprising development, in Section 6 we find graphs arising in a similar fashion which are not ω-categorical.

It seems well-known to combinatorists that exponential sums can be quite useful for constructing random graphs (they would probably consider the class of finite *Paley graphs* first), as mentioned in the citation before 3.13. This corresponds (more or less) to our Example 4.4, where $X = \mathbb{A}^1$, $f(x, y) = x + y$ and $k = 2$. We were also informed by Daniel Lascar that his student A. Delobelle had done some research on the reducts of pseudofinite fields, but without the aid of exponential sums. However, we could not find any evidence in the literature that the problem was ever treated at the present level of generality.

The role of exponential sums (integrals) is to provide much stronger amalgamation results (cf. 3.13, 5.7) than the Independence Theorem normally used by model theorists for similar tasks. The Independence Theorem allows amalgamating types over independent parameters extending a given Lascar strong type, whereas we obtain explicit necessary and sufficient (definable) conditions on parameters a_i for which the (Kummer-type) formulae $R(x, a_i)$ can be amalgamated.

While the theory of multiplicative character integrals suffices for the study of graphs as above, in a forthcoming paper we develop the theory suitable for treating graphs of the form $R(x, y) \equiv \exists Z f(x, y, Z) = 0$. We use the machinery of Galois stratification and Čebotarev's theorem ([7]) for estimating the character sums appearing in the definition of Artin L-functions ([8]). We can even lift certain aspects of Deligne's equidistribution theorem to the context of pseudofinite fields.

The additive and multiplicative character sums considered in Section 3 are just instances of this more general framework corresponding to Artin-Schreier and Kummer coverings. In that more general case, however, we shall not have such detailed understanding of the reducts as in Section 5, for example.

Notation is mostly standard throughout the text. The algebraic closure of a field $\mathfrak{k}$ is denoted by $\bar{\mathfrak{k}}$. For a scheme S, a *variety over* S is a separated and reduced scheme of finite type over S. In most of our applications S will just be the spectrum of a field $\mathfrak{k}$ and in that case we will just speak of a *variety over* $\mathfrak{k}$. Given a variety X over $\mathfrak{k}$, by $\overline{X}$ we shall denote the variety $X \times_{\mathrm{Spec}(\mathfrak{k})} \mathrm{Spec}(\bar{\mathfrak{k}})$ (X considered over $\bar{\mathfrak{k}}$). We say that X is *absolutely* (or *geometrically*) *irreducible* if the corresponding $\overline{X}$ is irreducible. For a scheme

X and a field $\mathfrak{k}$, the set of $\mathfrak{k}$-rational points, $X(\mathfrak{k})$, is the set of all morphisms $\mathrm{Spec}(\mathfrak{k}) \to X$.

The author would like to thank Dugald Macpherson for suggesting the study of 'random' reducts of pseudofinite fields, Kevin Buzzard, William Crawley-Boevey and Nicholas Katz for useful discussions, and Lou van den Dries for the idea of proof of Theorem 7.1. The author is grateful to the referee, whose suggestions significantly improved the exposition of the paper.

2. Measure and integration in pseudofinite fields

A field F is called *pseudofinite* if it is perfect, its absolute Galois group is $\hat{\mathbb{Z}}$ and every absolutely irreducible variety over F has an F-rational point. Principal examples of pseudofinite fields arise as ultraproducts of finite fields. For more information on pseudofinite fields we refer the reader to [1] and [7].

Let us quote the Main Theorem and several other results of [3].

Theorem 2.1. *Let $\phi(X, Y)$ be a formula in the language of rings, with $X = (X_1, \ldots, X_m)$ as parametric variables and $Y = (Y_1, \ldots, Y_n)$. Then there is a positive constant C and a finite set D of pairs (d, μ) with $d \in \{0, \ldots, n\}$ and μ a positive rational number, such that for each finite field $\mathfrak{k} = \mathbb{F}_q$ and each $x \in \mathfrak{k}^m$, if the set $\phi(x, \mathfrak{k}^n) := \{y \in \mathfrak{k}^n : \mathfrak{k} \models \phi(x, y)\}$ is nonempty, then $|\operatorname{card}(\phi(x, \mathfrak{k}^n)) - \mu q^d| \leq C q^{d-(1/2)}$ for some $(d, \mu) \in D$.*

Moreover, for each $(d, \mu) \in D$ there is a formula $\phi_{d,\mu}(X)$ that defines in each finite field $\mathfrak{k}$ the set of $x \in \mathfrak{k}^m$ such that $|\operatorname{card}(\phi(x, \mathfrak{k}^n)) - \mu q^d| \leq C q^{d-(1/2)}$.

Working over a pseudofinite field, the authors also give the interpretation to the numbers d and μ as *dimension* and *measure* in the following way.

Let $\phi(X, Y)$ be a formula, and let C, D be as in the theorem above. Then, for all sufficiently large finite fields $\mathfrak{k}$, and for every tuple $x \in \mathfrak{k}^n$, there exists a unique pair $(d, \mu) \in D$ with $|\operatorname{card}(\phi(x, \mathfrak{k}^n)) - \mu q^d| \leq C q^{d-(1/2)}$. Hence, there exists a unique pair $(d, \mu) \in D$ such that $\mathfrak{k} \models \phi_{d,\mu}(x)$. Therefore the same will be true in pseudofinite fields as well.

Definition 2.2. If S is a set definable in a pseudofinite field F by the formula $\phi(x, Y)$ for $x \in F^n$, then we define the pair $(\dim(S), \mu(S))$ to be the unique pair $(d, \mu) \in D$ such that $F \models \phi_{d,\mu}(x)$.

Proposition 2.3. *Let F be a pseudofinite field.*

(1) *If S is a definable set then $\dim(S)$ is equal to the algebraic dimension of the Zariski closure of S (in $\overline{F}$).*
(2) *For an absolutely irreducible variety X over F, $\mu(X) = 1$.*
(3) *If S and T are disjoint definable sets, then*

$$\mu(S \cup T) = \begin{cases} \mu(S) + \mu(T) & \text{if } \dim(S) = \dim(T), \\ \mu(S) & \text{if } \dim(S) > \dim(T), \\ \mu(T) & \text{if } \dim(S) < \dim(T). \end{cases}$$

(4) *Let $f : S \to T$ be a definable function. If for all $a \in T$, $\dim(f^{-1}(a)) = d$ then $\dim(S) = \dim(T)+d$. If additionally for all $a \in T$, $\mu(f^{-1}(a)) = m$, then $\mu(S) = m\mu(T)$.*

For readers proficient in stability and simplicity theory, let us just remark that the above dimension coincides with the U and S_1 ranks.

Remark 2.4. Let F be an pseudofinite field, which is $\aleph_1$-compact, i. e., a countable intersection of definable sets is empty if and only if a finite subintersection is. Let $S \subseteq F^n$ be a definable set. By $\mathrm{Def}(S)$ we denote the set of all definable subsets of S. The μ from above induces a finitely additive measure μ_S on $\mathrm{Def}(S)$ by:

$$\mu_S(T) := \begin{cases} \mu(T)/\mu(S) & \text{if } \dim(T) = \dim(S), \\ 0 & \text{if } \dim(T) < \dim(S). \end{cases}$$

Let $\mathfrak{M}_S$ be the σ-algebra generated by $\mathrm{Def}(S)$. We can extend μ_S to $\mathfrak{M}_S$ in a natural way to get a real measure also denoted by μ_S. This is made possible by the following consequence of $\aleph_1$-compactness. If T_i, $i < \omega$ are sets in $\mathrm{Def}(S)$ with $\dim(T_i) < \dim(S)$ for all i, there are no definable sets $T \subseteq \bigcup_{i<\omega} T_i$ such that $\dim(T) = \dim(S)$.

For any function $f : S \to \mathbb{C}$ which is measurable in the measure space $(S, \mathfrak{M}_S, \mu_S)$, we can speak of the integral $\int_S f\, d\mu_S$, as in [14], for example.

However, we will not need the theory of integration in this generality. In the present paper we shall only integrate simple functions with definable level sets, sometimes referred to as *definable*. If $s : S \to \mathbb{C}$ is such,

$$s = \sum_{i=1}^{n} \alpha_i \chi_{A_i},$$

with $\alpha_i \in \mathbb{C}$ and $A_i \in \mathrm{Def}(S)$, we have

$$\int_S s\, d\mu_S = \sum_{i=1}^{n} \alpha_i \mu_S(A_i).$$

This makes sense *without* the assumption of $\aleph_1$-compactness, or any other 'largeness' assumption on F.

Example 2.5. Although the measure on definable sets was $\mathbb{Q}$-valued, some measurable sets will have irrational measures, as the following amusing example shows. For a prime number p, let A_p be the definable set $\{(x, y) : x, y \text{ are } p\text{-th powers}\}$. By common sense or Remark 3.12, all A_p are independent events and $\mu(\bigcap_p A_p^c) = \prod_p(1 - p^{-2}) = 1/\zeta(2) = 6/\pi^2$, where ζ is the Riemann zeta function.

3. Character sums

Let $(G, \cdot)$ be an abelian group. For the purposes of this paper, a *character* χ of G will be a homomorphism of G into the multiplicative group of complex numbers. If G is finite, $\chi^{|G|}(g) = \chi(g^{|G|}) = \chi(1) = 1$ for every $g \in G$, so the values of χ are $|G|$-th roots of unity. The *order* of a character χ of G is the order of χ in the group of all characters of G.

Fact 3.1. *The number of characters of a finite abelian group G is $|G|$.*

Let $\mathbb{F}_q$ be a finite field. An *additive* (resp. *multiplicative*) *character* of $\mathbb{F}_q$ is a character of the additive (resp. multiplicative) group of $\mathbb{F}_q$.

Fact 3.2.
(1) *If $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ denotes the absolute trace function (an additive surjective map with kernel $\{x^p - x : x \in \mathbb{F}_q\}$), then the function χ_1 defined by*

$$\chi_1(c) = e^{2\pi i\, \mathrm{Tr}(c)/p}, \ \textit{for } c \in \mathbb{F}_q,$$

is an additive character and all additive characters of $\mathbb{F}_q$ are obtained as $\chi_b(c) := \chi_1(bc)$ for $b \in \mathbb{F}_q$. Note that, upon identifying $\mathbb{F}_p$ with $\mathbb{Z}/p\mathbb{Z}$, the value of the exponential expression is well-defined.
(2) *Let g be a fixed primitive element of $\mathbb{F}_q$. The function ψ_1 with*

$$\psi_1(g^j) = e^{2\pi i j/(q-1)}, \ \textit{for } j = 0, 1, \ldots, q-2,$$

is a multiplicative character, and the group of multiplicative characters is generated by ψ_1.

In this section we shall investigate definable (i.e. with definable level-sets) additive and multiplicative characters of pseudofinite fields of finite order. There are interesting multiplicative characters of infinite order, as shown in Example 3.7, but we defer the study of those, as well as more general characters arising in algebraic geometry, to a later paper.

Definition 3.3. We shall say that a field F *contains the n-th roots of unity*, if the group of n-th roots of unity in F has order n. Note that if $\mathrm{char}(F) = p > 0$ and F contains the n-th roots of unity for some $n > 1$, then clearly p does not divide n.

Lemma 3.4. *Let F be a pseudofinite field.*
(1) *If F is of characteristic $p > 0$, let $B_p(x)$ be the formula $\exists y\ x = y^p - y$. Thus $B_p(F) = \{y^p - y : y \in F\}$. Then*

$$F^+/B_p(F) \simeq \mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}.$$

An element $a \in F$ such that $F = \bigcup_{c \in \mathbb{F}_p} ca + B_p(F)$ is called additively primitive for F.

(2) *Let $n > 1$ be a natural number and let $P_n(x)$ be the formula $\exists y\, x = y^n$. Thus $P_n(F)$ is the multiplicative subgroup of n-th powers in $F^\times$. Suppose that F contains the n-th roots of unity. Then*

$$F^\times/P_n(F) \simeq \mathbb{Z}/n\mathbb{Z},$$

*the cyclic group of order n. An element $g \in F$ such that $F^\times = \dot{\bigcup}_{j<n} g^j P_n(F)$ (disjoint union) is called n-*primitive *for F.*

Proof. (1) The sentence $\exists y \forall x \bigvee_{c\in\mathbb{F}_p} B_p(x - cy)$ is true in all finite fields of characteristic p and thus also holds in F.

(2) The sentence $\exists y \forall x \neq 0\ \dot{\bigvee}_{j<n} P_n(x/y^j)$ (exclusive disjunction) is true in all sufficiently large finite fields containing the n-th roots of unity and therefore holds in pseudofinite fields with n-th roots of unity as well. □

Proposition 3.5. *Let F be a pseudofinite field.*

(1) *Suppose F is of characteristic $p > 0$. Let a be an additively primitive element for F. The map*

$$\tau_a(x) := c, \text{ for } x \in ca + B_p(F),$$

is a definable additive surjection $F \to \mathbb{F}_p$, and if we fix one primitive element a, all the definable additive maps $F \to \mathbb{F}_p$ are obtained as $\tau_{a,b}(x) := \tau_a(bx)$ for $b \in F$. Furthermore, all the definable additive characters are obtained as

$$\chi_{a,b}(x) = e^{2\pi i \tau_{a,b}(x)/p}, \text{ for } b \in F.$$

(2) *If F is of characteristic zero, there are no nontrivial definable additive characters of F.*

(3) *Let $n > 1$ be a natural number and let $P_n(F)$ be the multiplicative subgroup of n-th powers in $F^\times$. If g is n-primitive for F, let $\psi_g(c) = e^{2\pi i j/n}$, for $c \in g^j P_n(F)$. All the multiplicative characters of order n on a pseudofinite field with n-th roots of unity arise in this way and there is $\varphi(n)$ of them, where $\varphi(n) = |\{m < n : (m,n) = 1\}|$ is the Euler function.*

Proof. (1) Let $\tau : F \to \mathbb{F}_p$ be an arbitrary definable additive map, defined as $\tau(x) = y$ if $F \models \varphi(x, y, c)$ for some fixed $b \in F$. Then

$$F \models \exists Z \text{“}\varphi(X, Y, Z) \text{ is additive onto } \mathbb{F}_p\text{”},$$

and the same will hold in sufficiently large finite fields $\mathbb{F}_q$ of characteristic p. However, for each $\mathbb{F}_q$ of characteristic p,

$$\begin{aligned}&\mathbb{F}_q \models \forall Z \text{“}\varphi(X, Y, Z) \text{ is additive onto } \mathbb{F}_p\text{”} \to \\ &\qquad \exists T \exists W \text{“}T \text{ additively primitive”} \wedge \forall X \forall Y\, \varphi(X, Y, Z) \leftrightarrow \tau_{T,W}(X, Y),\end{aligned}$$

and our τ must arise as some $\tau_{a',b'}$ on F. If a was the fixed primitive element and $a' \in ca + B_p(F)$ for some $c \in \mathbb{F}_p$, then $\tau_{a',b'} = \tau_{a,cb'}$. The claims about additive characters reduce to the above by composing the characters with an isomorphism of the group of p-th roots of unity and $\mathbb{F}_p$.

(2) F^+ has no definable subgroups of finite index.

(3) If $\psi : F^\times \to U$ is an arbitrary multiplicative character of order n, $\ker(\psi) = P_n(F)$ and it must arise from a n-primitive element. Furthermore, if g is a n-primitive element, some h can be n-primitive if and only if $h \in g^m P_n(F)$ with $(m, n) = 1$. □

Remark 3.6. It is clear from item (3) above that F has a multiplicative character of order $n > 1$ if and only if F contains the n-th roots of unity in the sense of 3.3.

Example 3.7. Let F be an $\aleph_1$-compact pseudofinite field of characteristic p, fix a prime $l \neq p$ (we allow characteristic zero), and suppose F contains the l^n-th roots of unity, for all $n > 0$. By $\aleph_1$-compactness, $P_{l^\infty}(F) := \bigcap_n P_{l^n}(F)$ is a nontrivial multiplicative subgroup of infinite index. The quotients $F^\times/P_{l^n} \simeq \mathbb{Z}/l^n\mathbb{Z}$, together with natural quotient maps, form an inverse system and clearly we have a map

$$F^\times/P_{l^\infty}(F) \simeq \varprojlim_n F^\times/P_{l^n}(F) \simeq \mathbb{Z}_l^+.$$

Composing with the exponential of a non-canonical embedding of $\mathbb{Z}_l$ into $\mathbb{C}$, we obtain a multiplicative character $F^\times \to \mathbb{C}$ of infinite order.

In the remainder of this paper we conventionally extend multiplicative characters by $\psi(0) = 0$ and $\psi(\infty) = 0$. The following is our main theorem on exponential sums in pseudofinite fields.

Theorem 3.8. *Let X be a geometrically irreducible variety over a pseudofinite field F and let f be a rational function on X. Suppose either:*

1. *χ is a multiplicative character of F of order $n > 1$ and f is not an n-th power of a rational function on $\overline{X}$, or*
2. *χ is an additive character $\chi_{a,1}$ (in the notation of 3.5) of F and f is not of the form $g^p - g$ for some $g \in \overline{F}(\overline{X})$.*

Then

$$\int_X \chi \circ f \, d\mu_X = 0.$$

Although this is an easy consequence of the following uniform estimates on exponential sums in finite fields, we do not pursue this approach, but rather give a completely self-contained measure-theoretic proof below.

Fact 3.9 ([2], [4], [5], [11])**.** *Fix an integer $n > 1$. Let S be a variety over $\mathbb{Z}$ and let $f : X \to \mathbb{A}^1_S$ be a variety over an affine line over S. Suppose that for every finite field $\mathfrak{k}$ and for every $s \in S(\mathfrak{k})$, $X_s := X \times_S \mathfrak{k}$ is geometrically irreducible of dimension d and either:*

(1) *for every finite field* $\mathfrak{k}$ *containing* n*-th roots of unity and* $s \in S(\mathfrak{k})$*, we are given a multiplicative character* χ_s *of* $\mathfrak{k}$ *of order* n *and* $f_s : X_s \to \mathfrak{k}$ *is not an* n*-th power of a rational function on* $\overline{X}_s$*, or*

(2) S *is of characteristic* p*, for every finite field* $\mathfrak{k}$ *and* $s \in S(\mathfrak{k})$*, we are given the additive character* χ_s *which is the* χ_1 *character of* $\mathfrak{k}$ *(in the notation of 3.2), and* f_s *is not of form* $g^p - g$ *for some rational* g *on* $\overline{X}_s$*, or*

(3) S *is of characteristic* 0*, for every finite field* $\mathfrak{k}$ *and* $s \in S(\mathfrak{k})$*,* χ_s *is a nontrivial additive character of* $\mathfrak{k}$ *and the induced morphism* $\overline{X}_s \to \bar{\mathfrak{k}}$ *is not constant.*

Then there exists a constant $C > 0$ *such that for all finite fields* $\mathfrak{k}$ *(containing* n*-th roots of unity in case (1)) and all* $s \in S(\mathfrak{k})$ *we have the estimate*

$$\left| \sum_{x \in X_s(\mathfrak{k})} \chi_s(f_s(x)) \right| \leq C |\mathfrak{k}|^{d-1/2}.$$

Remark 3.10. Let X be a geometrically irreducible variety over a field $\mathfrak{k}$, let f be a rational function on X and let $n > 1$ be a natural number.

(1) If $\mathfrak{k}$ contains the n-th roots of unity, the following conditions are equivalent:
   (a) $f = g^n$ for some rational function g on $\overline{X}$;
   (b) $f = cg^n$ for some rational function g on X and constant $c \in \mathfrak{k}$.

(2) If $\mathfrak{k}$ is of characteristic p, then the following conditions are equivalent:
   (a) $f = g^p - g$, for some g rational on $\overline{X}$;
   (b) $f = g^p - g + c$, for some g rational on X and constant $c \in \mathfrak{k}$.

Thus, the nontriviality conditions of 3.8 and 3.9 are in fact necessary.

Proof. Let K_0 be the function field of X and let L_0 be a finite Galois extension of K_0. Let L/K be the corresponding Galois extension obtained by extending scalars to the separable closure $\mathfrak{k}^s$ of $\mathfrak{k}$. Furthermore, denote by $\mathfrak{l}$ the relative separable closure of $\mathfrak{k}$ in L_0. It is an easy exercise to check the exactness of the sequence:

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_0/K_0) \to \mathrm{Gal}(\mathfrak{l}/\mathfrak{k}) \to 1.$$

To check (1) above, let L_0 be obtained by adjoining $\sqrt[n]{f}$ to K_0 and assume $f = g^n$ in K. By Kummer theory, the above sequence reduces to $1 \to 1 \to \mathbb{Z}/d\mathbb{Z} \to \mathrm{Gal}(\mathfrak{l}/\mathfrak{k}) \to 1$ for some d dividing n, and thus $\mathrm{Gal}(\mathfrak{l}/\mathfrak{k})$ must be $\mathbb{Z}/d\mathbb{Z}$. Again by Kummer, $\mathfrak{l} = \mathfrak{k}(\alpha)$ with $\alpha^d = c \in \mathfrak{k}$ and it follows by exactness that $f/c^{n/d}$ is an n-th power in K_0. For (2), we do the same with the Artin-Schreier extension. $\square$

Proof of Theorem 3.8. Let us prove the multiplicative case, the additive one being analogous.

First, we reduce to the case when f is not a d-th power of a rational function on $\overline{X}$ for all $d > 1$ dividing n. Indeed, suppose the theorem is true in all such cases, and let f be a d-th power, but not an n-th power, for some d dividing n. By 3.10, f can be written as $f = cg^d$, for $c \in F$ and g rational on X. If d is maximal such, then χ^d is a character of order n/d and g is not a k-th power over $\overline{X}$ for any $k > 1$ dividing n/d. Thus,

$$0 = \chi(c) \int_X \chi^d \circ g \; d\mu_X = \int_X \chi \circ (cg^d) \; d\mu_X = \int_X \chi \circ f \; d\mu_X.$$

Assume now f is not a d-th power over $\overline{X}$, for all $d > 1$ dividing n. Suppose α is n-primitive in F and $\chi = \chi_\alpha$. We may assume that the variety X is normal geometrically irreducible and that f is regular.

For each $i < n$, we consider the variety

$$Y_i := \{(x, y) : x \in X, y^n = \alpha^{-i} f(x)\}.$$

Formally speaking, Y_i is the normalisation of X in the field L_0 obtained by adjoining the n-th root of $\alpha^{-i} f$ to the function field K_0 of X. Let L/K be the Galois extension obtained by extending scalars from F to $\overline{F}$, and let F' be the relative algebraic closure of F in L. Using Kummer theory and the assumptions on f, the exact sequence (as in the proof of 3.10)

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_0/K_0) \to \mathrm{Gal}(F'/F) \to 1$$

reduces to $1 \to \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(F'/F) \to 1$, and we can conclude that $F' = F$, i. e., F is relatively algebraically closed in L and Y_i is absolutely irreducible. Hence, by 2.3(2), $\mu(Y_i) = 1$.

On the other hand, let

$$X_i := \{x \in X(F) : P_n(\alpha^{-i} f(x))\}.$$

The natural projection map $Y_i \to X$ induces a surjection $Y_i(F) \to X_i$ with all fibres of size n. Thus, by 2.3(4), $\mu_X(X_i) = \mu(X_i) = 1/n$. Finally,

$$\int_X \chi \circ f \; d\mu_X = \sum_{i=0}^{n-1} \chi(\alpha^i) \mu_X(X_i) = \frac{1}{n} \sum_{i=0}^{n-1} \chi(\alpha^i) = 0.$$

□

Corollary 3.11. *With notation of the above theorem, let $\chi : F \to \mathbb{C}$ be a multiplicative character of order n, and suppose f is not a d-th power for all $d|n$, $d > 1$. Let $G = \chi(F^\times)$ denote the group of n-th roots of unity in $\mathbb{C}$ and let $c : G \to \mathbb{C}$ be any function. Then*

$$\int_X c \circ \chi \circ f \, d\mu_X = \int_G c \, d\mu_G,$$

where μ_G is the normalised counting measure on G.

Proof. Since G is abelian, any $\mathbb{C}$-valued function on G is central and therefore a linear combination of irreducible characters, which are just homomorphisms of G into $\mathbb{C}^\times$. It is clear that if α is a trivial character, $\int_X \alpha \circ \chi \circ f \, d\mu_X = 1 = \int_G \alpha \, d\mu_G$. If α is nontrivial, then $\alpha \circ \chi$ is a multiplicative character of F of order $|\alpha|$ dividing n and therefore $\int_X \alpha \circ \chi \circ f \, d\mu_X = 0 = \int_G \alpha \, d\mu_G$ by 3.8. The statement follows by linearity. □

Remark 3.12. Considering characteristic functions of singletons from G in the above corollary, we easily recover the following fact, already present in the proof of 3.8. Let $\chi_n : F \to \mathbb{C}$ be a multiplicative character of order n, and suppose f is not a d-th power for all $d|n$, $d > 1$. Then, for every $j < n$, $\mu_X(\{x : \chi_n(f(x)) = e^{2\pi i j/n}\}) = 1/n$.

We found an idea for the following result in [16], where it was formulated only for quadratic characters over finite fields for the case $X = \mathbb{A}^1$. It provides (many) solutions to consistent systems of 'character equations'. Model theorists should view it as a strengthening of the Independence (amalgamation) Theorem. It also provides explicit conditions for certain definable sets to be independent when viewed as events in the underlying probability space.

Theorem 3.13. *Let X be a geometrically irreducible variety over a pseudo-finite field F and let χ be a multiplicative character of order $n > 1$. Suppose $f_0, \dots, f_{m-1}$ are rational functions on X such that no partial product $f_0^{r_0} \cdots f_{m-1}^{r_{m-1}}$, $r_0, \dots, r_{m-1} \in \{0, \dots, n-1\}$ (not all zero) can be written as a n-th power of a rational function on $\overline{X}$. Then*

$$\mu_X(\{x \in X(F) : \chi(f_0(x)) = e^{2\pi i j_0/n}, \dots, \chi(f_{m-1}(x)) = e^{2\pi i j_{m-1}/n}\}) = \frac{1}{n^m},$$

for any choice of $j_0, \dots, j_{m-1} \in \{0, \dots, n-1\}$.

Proof. Although an elegant proof in style of 3.11 may be found, we keep a proof closer to the original from [16] for clarity.

Let $\zeta_0, \dots, \zeta_{n-1}$ be the n-th roots of unity and let

$$L_i(T) := \frac{\prod_{j \neq i}(T - \zeta_j)}{\prod_{j \neq i}(\zeta_i - \zeta_j)} = \frac{\prod_{j \neq i}(-\zeta_j)}{\prod_{j \neq i}(\zeta_i - \zeta_j)} + L_i'(T) = \frac{1}{n} + L_i'(T),$$

where $L_i'(T)$ is a polynomial of degree $n-1$ with no constant coefficient. Now clearly

$$\mu_X(\{x : \chi(f_l(x)) = \zeta_{j_l}, l < m\}) = \int_X \prod_{l<m} L_{j_l}(\chi(f_l(x))) = \frac{1}{n^m},$$

since $\int_X \chi(\prod_{l<m} f_l^{r_l}) = 0$ for $r_l < n$ (not all zero) by assumption of nontriviality and 3.8. □

Remark 3.14. Since composing with a non-canonical embedding of $\mathbb{Q}_l$ into $\mathbb{C}$ radically changes the topology, integrating the character from 3.7 with respect to the completed measure from 2.4 is beyond the extent of this paper.

4. An application: reducts of pseudofinite fields

We refine somewhat the setup from the introduction: let X be a variety over a pseudofinite field F, let f be a regular function on $X \times X$ and let $\chi : F \to \mathbb{C}$ be a multiplicative character of order $n > 1$ as in Section 3. Given $x, y \in X(F)$, we let $R_j(x, y)$ if $\chi(f(x, y)) = e^{2\pi ij/n}$ and consider $\langle X(F), R_0, \dots, R_{n-1}\rangle$ as a coloured graph. Of course, we may also consider rational functions f when X is irreducible. We will mostly be interested in the case when f is symmetric and thus defines an undirected graph, although the definitions and results given below make sense in general.

Definition 4.1. Let X be an absolutely irreducible variety over F and let f be a regular function on $X \times X$ which is not a n-th power of a rational function on $\overline{X \times X}$. For $c \in X(F)$, we shall denote the regular function $f(x, c)$ on X by f_c.

(1) If $X = \mathbb{A}^1$, we write $a \sim_1 b$ if f_a and f_b share a root in $\overline{F}$; let $\sim$ be the transitive closure of $\sim_1$.
(2) Write $c \in cl(A)$, if there exist a finite subset $\{a_1, \dots, a_m\}$ of A and a sequence $j, j_1, \dots, j_m \in \{0, \dots, n-1\}$, $j \neq 0$ such that $f_c^j f_{a_1}^{j_1} \cdots f_{a_m}^{j_m}$ is an n-th power of a rational function on $\overline{X}$.
(3) We shall say that a polynomial $f \in F[x, y]$ satisfies the condition:
(F1), if the resultant $\operatorname{res}(f_a, f_b)$ is a nontrivial polynomial in a and b;
(F2), if the discriminant $\Delta(f_a)$ is a nonconstant polynomial in a.

Lemma 4.2. (1) *$a \sim_1 b$ if and only if the resultant $\operatorname{res}(f_a, f_b) = 0$; in particular, $\sim_1$ is a closed condition and, provided f satisfies the non-triviality condition (F1), $a \sim_1 b$ implies that $b \in acl(a)$;*
(2) *if $n > 1$ is prime, $(X(F), cl)$ is a pregeometry (matroid); in case when $X = \mathbb{A}^1$ and f satisfies (F1) and (F2), it is locally finite, i.e. the closure of a finite set is finite;*
(3) *when $X = \mathbb{A}^1$ and $n > 1$ is prime, under the assumption (F2), there is a finite set F_0, such that on $F \setminus F_0$, if $b \in cl(a_1, \dots, a_m)$, then $b \sim_1 a_i$ for some i.*

Proof. The statement (1) is self-explanatory. In (2), the fact that $cl(cl(A)) = cl(A)$ follows from the assumption that n is prime. The exchange property is immediate. The local finiteness follows e.g. directly from Corollary 7.3, although it can be obtained more elementarily along the lines of (1) and (3).

For (3), let F_0 be the finite set of roots of $\Delta(f_a)$. Thus, each f_a with $a \in F \setminus F_0$ only has simple roots in the algebraic closure of F. If $f_c^j f_{a_1}^{j_1} \cdots f_{a_m}^{j_m} = g^n$, a root of f_c appears on the right hand side with multiplicity divisible by n, and since $j < n$, it must appear in one of f_{a_i}'s as well. $\square$

From now on, we assume $n > 1$ is prime so that cl is indeed a pregeometry. The definition of cl was chosen so that, in conjunction with 3.13 and 3.10, we get the following:

Corollary 4.3. *If $\{a_1, \ldots, a_m\}$ is cl-independent, then for every choice of colours $i_1, \ldots, i_m$ we can find some t with $R_{i_j}(t, a_j)$. Furthermore, for any $b \in cl(a_1, \ldots, a_m)$, the colour of the edge between t and b is determined by $i_1, \ldots, i_m$.*

Therefore, as long as the pregeometry cl is not too complicated, the whole graph is not too far from just a random coloured graph.

Example 4.4. Let $X = \mathbb{A}^1$, $f(x, y) = x+y$ and let χ be the quadratic character. Then $R_0(x, y)$ if $x + y$ is a square and $R_1(x, y)$ otherwise. It is obvious that $cl(B) = B$ for every set B and that every tuple of distinct elements $a_1, \ldots, a_m, b_1, \ldots, b_r$ is cl-independent. Thus, for every such tuple we can find an x such that $R_0(x, a_i)$ and $R_1(x, b_j)$. We conclude that $\langle F, R_0 \rangle$ is just the random graph well known to combinatorists and model-theorists.

The graph in the example above is known to be ω-categorical, i.e. its theory has a unique countable model up to isomorphism. It is natural to ask whether all graphs of that kind are ω-categorical. Although it is possible to find quite intricate examples which still are ω-categorical (as in Section 5), the answer is shown to be negative in Section 6.

5. The conic case

Let the base variety be $X = \mathbb{A}^1$ and suppose $f(x, y) \in F[x, y]$ is an absolutely irreducible polynomial. Consider the variety Y defined by $f(x, y)$. Then f_a and f_b share a root if there exists $\alpha \in \overline{F}$ with $f(\alpha, a) = 0$ and $f(\alpha, b) = 0$, i.e. if the vertical line $x = \alpha$ intersects $\overline{Y}$ at levels a and b. Thus the product of several instances of f being a n-th power corresponds to the existence of a certain rectangular configuration on $\overline{Y}$.

Let us define closed sets $H, V \subseteq \overline{Y} \times \overline{Y}$ by $((x, y), (x', y')) \in H$ if $(x, y) \in \overline{Y}$, $(x', y') \in \overline{Y}$ and $y = y'$ and $((x, y), (x', y')) \in V$ if $(x, y) \in \overline{Y}$, $(x', y') \in \overline{Y}$ and $x = x'$. Let h and v be the *correspondences* (not algebraic maps; in fact they are multi-valued) defined by the Zariski closures of $H \setminus \Delta$ and $V \setminus \Delta$, where $\Delta \subseteq \overline{Y} \times \overline{Y}$ is the diagonal. If we projectivize the whole situation (to have Bezout's theorem), then h (resp. v) are exactly graphs of the multimaps assigning to a point P the remaining $deg(f) - 1$ many points on the same horizontal (resp. vertical) line. Let ϕ be the composite of v and h as correspondences. Consider only quadratic characters for simplicity. It is clear that $f_{a_1} \cdots f_{a_n}$ is a square implies that $a_1 \in \phi^n(a_1)$. One way of investigating fixed points of a correspondence is the Lefschetz fixed point formula for étale cohomology, but we abandon these general considerations and observe the following special case.

Let $f(x,y)$ be a symmetric polynomial over F defining an absolutely irreducible conic Y and let χ be the quadratic character. We sometimes denote R_0 by just R, and R_1 by $\neg R$. By an affine change of coordinates, we can forget about linear terms in f. Also, without loss of generality, we may divide by the coefficient of x^2 and y^2 (whether it is a square or not), so we assume that $f(x,y) = x^2 + \beta xy + y^2 - \gamma$.

The correspondence ϕ mentioned above turns out to be a function (because the degree of f is 2), and it maps $(x_0, y_0) \in \overline{Y}$ to $((\beta^2-1)x_0 + \beta y_0, -\beta x_0 - y_0)$. So ϕ is a linear map with matrix:

$$\begin{pmatrix} \beta^2 - 1 & \beta \\ -\beta & -1 \end{pmatrix}.$$

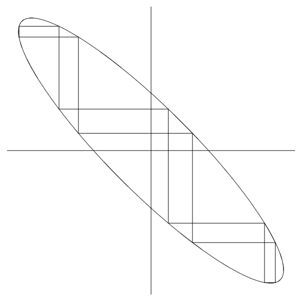
It is clear now that ϕ^n can have fixed points only if some eigenvalues of ϕ are n-th roots of unity. It turns out that if one eigenvalue is an n-th root of unity, so is the other one. To summarise, if ζ is an n-th primitive root of unity and we choose β such that $\beta^2 = \zeta + 2 + 1/\zeta = (\sqrt{\zeta} + 1/\sqrt{\zeta})^2$, then $\phi^n = I$. For all other values of β, no power of ϕ has fixed points and there are no nontrivial ways to make a product of instances of f a square.

From now on, fix an $n > 1$, choose the corresponding β as above, and assume β is in our pseudofinite field F. In this case we have the following cyclic behaviour of $\sim_1$. if $a_0 \in F \setminus (cl(\emptyset)/\sim)$, either $\tilde{a}_0 = \{a_0\}$, or $\tilde{a}_0 = \{a_0, \dots, a_{n-1}\}$, for some $a_1, \dots, a_{n-1}$ with $a_0 \sim_1 a_1 \sim_1 \cdots \sim_1 a_{n-1} \sim_1 a_0$.

It is also clear that cl is n-disintegrated. Moreover,

$$cl(B) = \bigcup_{B_0 \subseteq B, |B_0| = n} cl(B_0) \subseteq \bigcup_{b \in B} \tilde{b}.$$

The case for $n = 7$ is shown in the diagram below.



We see that many points have $n-1$ rather special points associated with them. Thus, intuitively, if we are to prove that our graph is ω-categorical by a variant of the back-and-forth argument, we will need to add the whole class of a point in each step of our construction, and not just the point itself. Therefore we will be required to work over a variety which describes what the relevant classes look like.

Since $\operatorname{res}(f_a, f_b) = (a-b)^2(a^2 + (2-\beta^2)ab + b^2 - \beta^2\gamma)$, clearly $a \sim_1 b$ for $a \neq b$ if and only if $r(a,b) = 0$, where by r we denote the second factor from the resultant above. Let $d(x) = (2-\beta^2)^2x^2 - 4(x^2 - \beta^2\gamma)$ be the discriminant of the equation $r(x,y) = 0$ (in y).

Let I be the ideal in $F[x_0, \dots, x_{n-1}]$ generated by:

$$\begin{array}{cc}
r(x_0, x_1) & \\
 & x_0 + x_2 + (2-\beta^2)x_1 \\
r(x_1, x_2) & \\
 & x_1 + x_3 + (2-\beta^2)x_2 \\
\vdots & \vdots \\
r(x_{n-2}, x_{n-1}) & \\
 & x_0 + x_{n-2} + (2-\beta^2)x_{n-1} \\
r(x_{n-1}, x_0) & \\
 & x_1 + x_{n-1} + (2-\beta^2)x_0
\end{array}$$

Notice that the linear polynomials in the right column make sure that e.g. x_0 is not repeated as x_2 and they make all the conditions in the left column superfluous, except the first one. Let $X = \operatorname{Spec}(F[x_0, \dots, x_{n-1}]/I)$ be the variety defined by I, easily seen to be smooth and (absolutely) irreducible of dimension 1, i.e., a smooth curve. It is clear that if $(x_0, \dots, x_{n-1}) \in X(F)$, then $\tilde{x}_0 = \{x_0, \dots, x_{n-1}\}$. Also, if $d(x_0)$ is not a square in F, then $\tilde{x}_0 = \{x_0\}$.

In order to determine all 'allowed' R-configurations between classes, we define more closure operators.

We work with pairs (α, β), where α is a variable x_i for $i < n$ and β is either a variable x_j for $j < n$ or an element of F. Then $f(\alpha, \beta)$ makes sense as a polynomial. After composing with appropriate coordinate projections, $f(\alpha, \beta)$ can also be viewed as a regular function on X. For some β, and a tuple $t_0, \dots, t_{n-1}$, we shall write $\beta(t) = t_j$ if $\beta = x_j$ and $\beta(t) = b$ if $\beta = b \in F$.

Definition 5.1. We write:

1. $(\alpha_1, \beta_1) \sim_1 (\alpha_2, \beta_2)$ if the regular functions $f(\alpha_1, \beta_1)$ and $f(\alpha_2, \beta_2)$ vanish at the same point of $X(\overline{F})$; also, let $\sim$ be the transitive closure of $\sim_1$;
2. $(\alpha, \beta) \in cl_X(A)$ if there are $\{(\alpha_1, \beta_1), \dots, (\alpha_k, \beta_k)\} \subseteq A$ and $j_1, \dots, j_k \in \{0, 1\}$ such that
$$f(\alpha, \beta) f(\alpha_1, \beta_1)^{j_1} \cdots f(\alpha_k, \beta_k)^{j_k}$$
is a square of a rational function on $\overline{X}$;
3. $b \in cl'_X(A)$ if there are $\{a_1, \dots, a_k\} \subseteq A$, as well as m, i_j such that
$$(x_m, b) \in cl_X\left(\{(x_{i_1}, a_1), \dots, (x_{i_k}, a_k)\} \cup \{(x_j, x_l) : j \neq l < n\}\right);$$

(4) $b \in cl_1(A)$ if there are $\{a_1, \ldots, a_k\} \subseteq A$ and $j_0, \ldots, j_k \in \{0, 1\}$ such that

$$f_b d^{j_0} f_{a_1}^{j_1} \cdots f_{a_k}^{j_k}$$

is a square of polynomial.

Lemma 5.2. *Let the finite set F_0 be the union of $\sim$-classes of:*

- $cl(\emptyset) \cup cl_1(\emptyset) \cup cl'_X(\emptyset)$;
- *parameters b such that*

$$(x_m, b) \in cl_X(\{(x_{m_i}, b_i) : i < r\} \cup \{(x_{i_j}, x_{l_j}) : j < s\}),$$

for some choice of indices, (x_m, b) is not contained in cl_X of any proper subset of the above, and $b \not\sim b_i$ for all $i < r$ (this in fact forces $(x_m, b) \sim_1 (x_{i_j}, x_{l_j})$ for some j by claim (1) below).

(1) *If $(x_i, b) \sim_1 (x_j, c)$, then $b \sim c$.*
(2) *cl_X, cl_1 are locally finite pregeometries.*
(3) *cl'_X and cl_1 are $\sim$-disintegrated on $F \setminus F_0$, i.e. $cl'_X(B) \subseteq \bigcup_{b \in B} \tilde{b}$ (and similarly for cl_1).*

Proof. Chasing definitions yields (1). Items (2) and (3) follow in the same style as Lemma 4.2. For the latter we use the fact that X is smooth so its local rings are unique factorisation domains and we can count the multiplicities of zeroes. $\square$

Applying Theorem 3.13 over X and the previous lemma, we obtain:

Corollary 5.3.

(1) *If the set $\{(\alpha_1, \beta_1), \ldots, (\alpha_k, \beta_k)\}$ is cl_X-independent, for every choice of $i_1, \ldots, i_k$ in $\{0, 1\}$ we can find $(t_0, \ldots, t_{n-1}) \in X(F)$ such that $R_{i_j}(\alpha_j(t), \beta_j(t))$.*

Moreover, if $(\alpha, \beta) \in cl_X((\alpha_1, \beta_1), \ldots, (\alpha_k, \beta_k))$, the colour of the edge between $\alpha(t)$ and $\beta(t)$ is determined by $i_1, \ldots, i_k$.

(2) *If $a_1, \ldots, a_k$ are cl_1-independent, for each choice of $i_1, \ldots, i_k \in \{0, 1\}$ we can find t such that $d(t)$ is not a square and $R_{i_j}(t, a_j)$.*

Moreover, if $b \in cl_1(a_1, \ldots, a_k)$, the colour of the edge between t and b is determined by $i_1, \ldots, i_k$.

Thus, cl_X-independence allows us to find a class of size n, whereas cl_1-independence allows us to find a class of size 1 satisfying certain graph conditions (on $F \setminus F_0$, these are the only possibilities).

Definition 5.4. If an ordering on a class $\tilde{x}$ is given, we shall write $\bar{x}$ for the corresponding tuple. Let A be a (finite) set of parameters. Then:

(1) let $t(\bar{x}/A)$ denote the quantifier-free type of $\bar{x}$ over A in the graph language;

(2) let $t(\bar{x}, \bar{y})$ (resp. $t^*(\bar{x}, \bar{y})$) denote the quantifier-free type of $\bar{x} \cup \bar{y}$ in the graph language (resp. the quantifier-free type of $\bar{x} \cup \bar{y}$ with edges between the elements of $\bar{y}$ omitted);
(3) let $S_1 = \{t(\bar{x}) : \bar{x}$ is some ordering of $\tilde{x}, x \in F \setminus F_0\}$;
(4) given $t \in S_1$ and $\bar{y}$, let $S_2(t; \bar{y}) = \{t(\bar{x}, \bar{y}) : \tilde{x} \neq \tilde{y}, t(\bar{x}) = t\}$ and $S_2^*(t; \bar{y}) = \{t^*(\bar{x}, \bar{y}) : \tilde{x} \neq \tilde{y}, t(\bar{x}) = t\}$.

Lemma 5.5. *There is a finite $F_1 \subseteq F$ such that:*

(1) $S_1 = \{t(\bar{x}) : \bar{x} \in F \setminus F_1\}$;
(2) *for all $\bar{b}, \bar{c} \in F \setminus F_1$ of the same cardinality, and for any $t \in S_1$, $S_2^*(t; \bar{b}) = S_2^*(t; \bar{c})$; in particular, if $t(\bar{b}) = t(\bar{c})$, then $S_2(t, \bar{b}) = S_2(t, \bar{c})$.*

Proof. Statement (1) is trivial on its own. For (2), every cl_X dependency condition on X is closed by Corollary 7.3, and since X is an irreducible curve, it is either the whole of X or finite. The same argument applies to cl_1. □

By the previous lemma, it makes sense to talk about $S_2(t, t')$ for $t, t' \in S_1$ (outside $F_1/\sim$).

Definition 5.6. Let E be the finite set of 'exceptional points' $F_0 \cup F_1/\sim$ and let $S_1(E) := \{t(\bar{x}/E) : x \notin E\}$. Notice that we have a restriction map $t \mapsto t \restriction \emptyset$ from $S_1(E)$ to S_1.

Finally we can formulate an amalgamation result strengthening the Independence Theorem well-suited for a back-and-forth argument.

Corollary 5.7. *For every distinct tuple of $\sim$-classes $\tilde{a}_0, \ldots, \tilde{a}_{k-1} \in F \setminus E$, for every $t \in S_1(E)$, for every choice of 'allowed configurations' $c_i \in S_2(t \restriction \emptyset; t(\bar{a}_i))$, there exists an $\bar{x}$ with $t(\bar{x}/E) = t$ and $t(\bar{x}, \bar{a}_i) = c_i$ for every $i < k$.*

Proof. Combine Lemma 5.2, Corollary 5.3 and Lemma 5.5. □

Theorem 5.8. *The graph $\langle F, R \rangle$ is ω-categorical and trivial in the model-theoretic sense.*

Proof. Let us name constants for elements of E to start with. Notice that the predicates for $x \in cl(y_1, \ldots, y_m)$ are definable using just R: x will be in the closure of $y_1, \ldots, y_m$ when for every t, the colour of the edge between t and x is determined by colours of edges between t and y_i. Using cl, we see that $\sim$ is also a definable equivalence relation: $x \sim y$ is equivalent to $\exists z_1, \ldots, z_{n-1}$ $(x \in cl(y, z_1, \ldots, z_{n-1}) \wedge x \notin cl(z_1, \ldots z_{n-1}))$. The predicates for cl_X are definable in a similar way: cl_X detects when we cannot freely add a $\sim$-class. As for cl_1, the points x with $d(x)$ not a square are distinguished by the fact that their $\sim$-class is of size 1. This is all we need to translate the statement of Corollary 5.7 into the graph language.

Now it is clear how to do a variant of the back-and-forth construction, adding a $\sim$-class in each step, to show that any two countable graphs axiomatised by the above axiom scheme are isomorphic. It will be analogous to proving that the following vertex- and edge-coloured random graph is ω-categorical:

(1) the finite set of vertex colours is C;
(2) given two vertex colours t, t', the finite set of allowed edge-colours is $C(t, t')$;
(3) for every k, and every set of distinct vertices $\{a_i : i < k\}$ where a_i is coloured by some $t_i \in C$, for each choice of a vertex colour $t \in C$ and edge colours $c_i \in C(t, t_i)$, we can find an x coloured by t such that the edge between x and a_i is c_i.

Since we have shown above that $\langle F, R, E\rangle$ is ω-categorical, the same holds for $\langle F, R\rangle$, since ω-categoricity is preserved by naming and especially forgetting finitely many constants.

For each point $x \in F$, $acl_{\langle R,E\rangle}(x) = \tilde{x} \cup E$, and thus $acl_{\langle R,E\rangle}(A) = \bigcup_{a\in A} acl_{\langle R,E\rangle}(a)$ so the structure $\langle F, R, E\rangle$ is trivial. On the other hand, we have been careful to choose $E \subseteq acl_R(\emptyset)$ in the first place, so $\langle F, R\rangle$ is trivial too. $\square$

6. Non-ω-categorical case

The main idea of this section is to exploit the fact that we can find algebraic groups with torsion points of arbitrarily high order to find 'random' reducts of pseudofinite fields which are not ω-categorical.

Let us give a template for the construction. Suppose $(G, \cdot)$ is an algebraic group defined over a pseudofinite field F with the property that $G(F)$ contains all the torsion points of G and G has torsion points of any order. For a smoother exposition, we assume F is large enough so that $G(F)$ contains generic points.

In case we desire an example of a non-ω-categorical directed graph, suppose we can find a 'generic' regular or rational function g on G such that for no n and no distinct torsion points $p_1, \dots, p_n$, the function $g(x \cdot p_1) \cdots g(x \cdot p_n)$ is a square of a rational function on $\overline{G}$. Define f on $G \times G$ by $f(x, y) := g(x \cdot y)g(x \cdot y^2)$ and let $R_0(x, y)$ if $f(x, y)$ is a square in F and $R_1(x, y)$ otherwise.

For an example of a non-ω-categorical undirected graph, we need a 'generic' function g such that for no n and no distinct torsion points $p_1, \dots, p_n$, no subproduct of $g(x \cdot p_1) \cdots g(x \cdot p_n)g(x^2 \cdot p_1) \cdots g(x^2 \cdot p_n)$ is a square of a rational function on $\overline{G}$. Then we let $f(x, y) := g(x \cdot y)g(x \cdot y^2)g(x^2 \cdot y)g(x^2 \cdot y^2)$ and take R_0 and R_1 as above.

Now, in either of the cases, for every n, if p is a torsion point of order $2^n - 1$, we will have that $f(x, p)f(x, p^2) \cdots f(x, p^{2^{n-1}})$ is a square of a rational function and no subproduct of it is a square of a rational function. Thus, cl associated with this f is not n-disintegrated for any n. In particular, in view of 4.3, for each $n > 1$ we have a formula $\phi_n(x)$ saying:

"there exist $x_1, \dots x_{n-1}$ such that for each choice $i_1, \dots, i_{n-1} \in \{0,1\}$, there is a t such that $\bigwedge_{1\leq j\leq n-1} R_{i_j}(t, x_j)$, but for each t the edge between t and x is determined by $i_1, \dots, i_{n-1}$".

For $m \neq n$, ϕ_m and ϕ_n are not equivalent, because if p is a torsion point of order $2^n - 1$, p satisfies ϕ_n but not ϕ_m. Therefore, by the Ryll-Nardzewski Theorem, $\langle G(F), R_0, R_1\rangle$ is not ω-categorical because we have infinitely many 1-formulae.

It is straightforward to adopt this in the case G is just the multiplicative group of the field; the function $g(Z) := Z - \alpha$, for α a transcendental element in F, is as required. We shall show the details in the case of elliptic curves below. Both of these examples, however, provide infinitely many algebraic types, because they only have finitely many torsion points of each order. If the reader requires an example with infinitely many non-algebraic types, the author suggests studying the case of $G = SL_2$ (the author has not worked out the details).

For the theory of elliptic curves and (mostly standard) notation, we refer the reader to [15].

Let (E, O) be an elliptic curve over $\mathbb{Q}$, and let us assume O is the point at infinity. In order to carry out our idea, we want to pick a pseudofinite field K so that the elliptic curve has torsion points of every order over K.

For every $m \geq 1$ we have 'division polynomials' $\phi_m, \theta_m, \omega_m \in \mathbb{Q}[x, y]$ such that for $P = (x, y) \in E(\overline{\mathbb{Q}})$ with $[m]P \neq O$,

$$[m]P = \left(\frac{\theta_m(x,y)}{\psi_m(x,y)^2}, \frac{\omega_m(x,y)}{\psi_m(x,y)^3}\right).$$

Fact 6.1. *Let $P \in E(\overline{\mathbb{Q}}) \setminus \{O\}$, $m \geq 1$. Then $P \in E[m]$ if and only if $\psi_m(P) = 0$. Furthermore,*

$$\bar{f}_m := \begin{cases} \psi_m, & m \text{ odd,} \\ \psi_m/\psi_2, & m \text{ even,} \end{cases}$$

is a polynomial that depends only on x. If $P = (x, y) \in E(\overline{\mathbb{Q}})$ is such that $[2]P \neq O$, and $m > 2$, then $P \in E[m]$ if and only if $\bar{f}_m(x) = 0$.

Now, pick a pseudofinite field K of characteristic 0 where all $\bar{f}_m$, $m > 2$ split and such that E has a point above each root of $\bar{f}_m$ in K. This can be achieved as follows: for each m, let $\mathfrak{k}_m$ be a finite field where all f_j, $j \leq m$ split and E has points above all roots of f_j, $j \leq m$ in $\mathfrak{k}_m$. Then take K to be a nonprincipal ultraproduct of $\mathfrak{k}_m$'s. We shall observe E over K. In particular, by the construction:

Lemma 6.2. *With E and K as above, $E[m](K) \neq 0$ for all $m \geq 2$.*

Let us choose a 'generic' rational function g on E/K by the following lemma.

Lemma 6.3. *There exists $g \in K(E)$ such that, if $Q_1, \dots, Q_m \in E(\overline{K})$ are the zeros of g and $P_1, \dots, P_n \in E(\overline{K})$ are the poles of g (and all zeros are of multiplicity 1), no point among $P_i \ominus P_j$ $(i \neq j)$, $Q_i \ominus Q_j$ $(i \neq j)$, $P_i \ominus Q_j$, is a torsion point.*

Proof. The proof is easiest in the framework of groups definable in simple theories, but we give an explanation in the field-theoretic language as well. Pick two independent generic points Q_1 and Q_2 in $E(K)$ (Q_1 and Q_2 are algebraically independent points of transcendence degree 1). Then, $Q_3 := \ominus(Q_1 \oplus Q_2)$ is independent of Q_1 and of Q_2 and clearly no $Q_i \ominus Q_j$ is a torsion point (torsion points cannot have transcendence degree 1). Let g be a rational function induced by the 'line' through Q_1, Q_2, Q_3. It will have simple zeroes at Q_1, Q_2, Q_3 and a pole at O of order 3. □

Proposition 6.4. *With E and g as above, let $f(X, Y) := g(X \oplus Y)g(X \oplus [2]Y)$. Given $n > 1$, pick a torsion point P of order $2^n - 1$. Then*

$$f(X, P)f(X, 2P) \cdots f(X, 2^{n-1}P)$$

is a square of a rational function. Furthermore, no subproduct of the above is a square of a rational function.

Proof. The product is a square just by the choice of P. If a proper subproduct was a square, we would have that $g(X \oplus m_1P)$ and $g(X \oplus m_2P)$ must share a zero over $\overline{K}$ for some m_1, m_2 with $m_1P \neq m_2P$. This would mean that there is an X so that $X \oplus m_1P = Q_i$ and $X \oplus m_2P = Q_j$, which implies that $(m_1 - m_2)P = Q_i \ominus Q_j$, but by the choice of g, this can only happen if $i = j$ and thus $m_1P = m_2P$. □

7. Bounds in polynomial ideals

The goal of this section is to prove constructibility of the condition that a regular function on an absolutely irreducible variety be generically geometrically of form g^n (or $g^p - g$ when the characteristic of the ground field is $p > 0$).

We must remark that this is obvious from the standard constructibility and base change theorems from étale cohomology; in that language, the conditions are equivalent to the vanishing of the constructible sheaf of higher direct images with compact support of the Kummer (resp. Artin-Schreier) sheaf. The referee has remarked that one can very elegantly deduce the same results from 3.8, using the definability of the measure.

We give a slightly more general result below, expanding upon the results of [6] and using the nonstandard methods explored there.

Let $\mathfrak{k}$ be an internal field, I a prime ideal in $\mathfrak{k}[Y]$ where $Y = (Y_1, \dots, Y_n)$, and $R := \mathfrak{k}[Y]/I$. Let $R^* := \mathfrak{k}[Y]_{int}/I\mathfrak{k}[Y]_{int}$. By faithful flatness of [6], $I\mathfrak{k}[Y]_{int} \cap \mathfrak{k}[Y] = I$ and we may assume R is a subring of R^*. Let K be the fraction field of R and K^* be the fraction field of R^*.

Theorem 7.1. *With the above notation, K^* is a regular extension of K.*

Proof. By Noether normalisation, we may assume (by an absolute change of variables) that there is an $r \leq n$ such that $I \cap \mathfrak{k}[Y_1, \dots, Y_r] = 0$ and R is integral over the subring $\mathfrak{k}[Y_1, \dots, Y_r]$. In other words, $R = \mathfrak{k}[Y_1, \dots, Y_r][a]$, where $a_i = Y_{r+i}/I$ for $1 \leq i \leq n - r$ and each a_i is integral over $\mathfrak{k}[Y_1, \dots, Y_r]$.

It is readily verified that $R^* = \mathfrak{k}[Y_1, \dots, Y_r]_{int}[a]$. Also, $I \cap \mathfrak{k}[Y_1, \dots, Y_r] = 0$ implies that $I\mathfrak{k}[Y]_{int} \cap \mathfrak{k}[Y_1, \dots, Y_r]_{int} = 0$, just as in Lemma 3.6 of [6].

Let us denote by K_0 the fraction field of $\mathfrak{k}[Y_1, \dots, Y_r]$ and by K_0^* the fraction field of $\mathfrak{k}[Y_1, \dots, Y_r]_{int}$. By Lemma 2.2 in [6], K_0^* is a regular extension of K_0. Since $K = K_0(a)$ and $K^* = K_0^*(a)$ with a algebraic over K_0, general facts about regular extensions (e.g. [12], Theorem 4.13) yield that K^* is a regular extension of K. $\square$

We are in fact interested in the following 'standard' corollary of the above.

Theorem 7.2. *Fix integers $d, m, n, r > 0$ and polynomials $f, g, f_1, \dots, f_r \in \mathbb{Z}[X, Y]$ of (total) degree less than d, where $X = (X_1, \dots, X_m)$ are parametric variables and $Y = (Y_1, \dots, Y_n)$. Let $F \in \mathbb{Z}[T]$ be also of degree less than d. Given a field $\mathfrak{k}$ and a tuple $x \in \mathfrak{k}^m$ we have the following data: the ideal $I_x = \langle f_1(x, Y), \dots, f_r(x, Y)\rangle$ in $\mathfrak{k}[Y]$, the ring $R_x = \mathfrak{k}[Y]/I_x$, the affine scheme $V_x = \mathrm{Spec}(R_x)$ and regular functions $f_x, g_x \in R_x$ induced by polynomials $f(x, Y), g(x, Y) \in \mathfrak{k}[Y]$. The set*

$$\{x \in \mathfrak{k}^m : V_x \textit{ abs. irreducible, } g_x \neq 0,\ f_x/g_x = F(h) \textit{ for some } h \in \bar{\mathfrak{k}}(V_x)\}$$

is constructible, i. e. definable by a quantifier-free formula depending only on d, m, n, r but not on the field $\mathfrak{k}$.

Proof. Notice that we want to define a set of parameters in the field $\mathfrak{k}$ so that a certain condition holds over the algebraic closure $\bar{\mathfrak{k}}$. There is a standard trick to achieve this. Suppose a formula ϕ_F defines the parameters x of rational functions over $\mathfrak{k}$ which are of form $F(h)$ for some $h \in \mathfrak{k}(V_x)$, uniformly over all $\mathfrak{k}$.

By quantifier elimination for algebraically closed fields, there is a quantifier-free formula ϕ_F^0 equivalent to ϕ_F modulo the theory of algebraically closed fields. But then, for any field $\mathfrak{k}$, its algebraic closure $\bar{\mathfrak{k}}$, and $x \in \mathfrak{k}^m$,

$$\mathfrak{k} \models \phi_F^0(x) \text{ if and only if } \bar{\mathfrak{k}} \models \phi_F(x),$$

and thus ϕ_F^0 is our sought-after formula.

In order to find ϕ_F, it is enough to show that there are bounds for the degrees of numerator and denominator of h such that $f_x/g_x = F(h)$, uniform in $\mathfrak{k}$ and x. Suppose not; for every integer N there is a field $\mathfrak{k}_N$ and $x_N \in \mathfrak{k}_N$ such that $f_{x_N}/g_{x_N} = F(u_N/v_N)$ in $\mathfrak{k}_m(V_{x_N})$, with $\deg(u_N), \deg(v_N) \geq N$ and we cannot find a degree lower than N that works.

If we take a structure containing all fields $\mathfrak{k}_N$, polynomial rings $\mathfrak{k}_N[X,Y]$, $\mathbb{N}$, and take an enlargement (in the sense of nonstandard methods of [6]) of this structure, we will contradict Theorem 7.1. $\square$

Before stating the next result, let us recall that regular functions on a variety induced by polynomials of bounded degree form a finite dimensional vector space and it is customary to consider the corresponding projective space. This does not affect our considerations since the properties we are interested in are invariant under scaling functions.

Corollary 7.3. *Let $V = \mathrm{Spec}(R)$ be an absolutely irreducible affine variety over a field $\mathfrak{k}$ with the ring of regular functions $R = \mathfrak{k}[Y_1,\dots,Y_m]/I$. Let n and d be integers. Let P_n be the subset of the projective space of regular functions $\overline{f} \in R$ induced by polynomials $f \in \mathfrak{k}[Y_1,\dots,Y_m]$ of degree at most d which are n-th powers of rational functions in $\overline{\mathfrak{k}}(V)$. The set P_n is closed.*

Proof. We may assume that V is normal, because if $\tilde{V}$ is the normalisation of V, f induces an n-th power on V if and only if it does on $\tilde{V}$. The 'complexity' of polynomials defining the normalised variety does not get out of hand by [6]. Also, in view of the first paragraph in the proof of 7.2, we may assume $\mathfrak{k}$ is algebraically closed.

Let P_n^l denote the subset of P_n consisting of (classes of) regular functions $\overline{f}$ induced by polynomials f of degree at most d such that there exists a regular function $\overline{g}$ induced by a polynomial g of degree at most l with $\overline{f} = \overline{g}^n$. By classical elimination theory, each P_n^l is closed in the projective space of regular functions induced by polynomials of degree at most d (as an image of a projective variety). By Theorem 7.2, P_n is definable. On the other hand,

$$P_n \leftrightarrow \bigvee_l P_n^l,$$

and $P_n^l \subseteq P_n^{l'}$ for $l \leq l'$, so there must be an l such that $P_n \leftrightarrow P_n^l$. $\square$

References

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

[2] E. Bombieri, *On exponential sums in finite fields. II*, Inventiones Mathematicae **47** (1978), no. 1, 29–39.

[3] Zoé Chatzidakis, Lou van den Dries, and Angus Macintyre, *Definable sets over finite fields*, Journal für die reine und angewandte Mathematik **427** (1992), 107–135.

[4] P. Deligne, *Applications de la formule des traces aux sommes trigonométriques*, Cohomologie étale, Springer-Verlag, Berlin, 1977, Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier, Lecture Notes in Mathematics, Vol. 569, pp. 168–232.

[5] Pierre Deligne, *La conjecture de Weil. II*, Institut des Hautes Études Scientifiques. Publications Mathématiques **52** (1980), 137–252.

[6] L. van den Dries and K. Schmidt, *Bounds in the theory of polynomial rings over fields. A nonstandard approach*, Inventiones Mathematicae **76** (1984), no. 1, 77–91.

[7] Michael D. Fried and Moshe Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 11, Springer-Verlag, Berlin, 1986.
[8] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, vol. 9, Exp. No. 279, Soc. Math. France, Paris, 1995, 41–55.
[9] Ehud Hrushovski, *A new strongly minimal set*, Annals of Pure and Applied Logic **62** (1993), no. 2, 147–166, Stability in model theory, III (Trento, 1991).
[10] Ehud Hrushovski and Boris Zilber, *Zariski geometries*, Journal of the American Mathematical Society **9** (1996), no. 1, 1–56.
[11] Nicholas M. Katz, *Sommes exponentielles*, Astérisque, vol. 79, Société Mathématique de France, Paris, 1980. Course taught at the University of Paris, Orsay, Fall 1979. With a preface by Luc Illusie, notes written by Gérard Laumon, with an English summary.
[12] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
[13] E. D. Rabinovich, *Definability of a field in sufficiently rich incidence systems*, QMW Maths Notes, vol. 14, Queen Mary and Westfield College School of Mathematical Sciences, London, 1993, With an introduction by Wilfrid Hodges.
[14] Walter Rudin, *Real and complex analysis*, third ed., McGraw-Hill, New York, 1987.
[15] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.
[16] T. Szőnyi, *Some applications of algebraic curves in finite geometry and combinatorics*, Surveys in combinatorics, 1997 (London), London Math. Soc. Lecture Note Ser., vol. 241, Cambridge Univ. Press, Cambridge, 1997, pp. 197–236.
[17] Ivan Tomašić and Frank Wagner, *Applications of the group configuration theorem in simple theories*, Journal of Mathematical Logic, **3** (2003), no. 2, 239–255.

Ivan Tomašić, Institut Girard Desargues, Université Lyon 1, 21 avenue Claude Bernard, 69622 Villeurbanne Cedex, France

E-mail address: `tomasic@igd.univ-lyon1.fr`