UNDECIDABILITY OF SOME ELEMENTARY THEORIES OVER PAC FIELDS

Gregory CHERLIN*
Department of Mathematics, Rutgers University, New Brunswick, NJ 08903, USA

Moshe JARDEN**
School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel

Communicated by A. Prestel
Received 30 July 1984

Introduction

We consider in this work the absolute Galois group, $G(\mathbb{Q})$, of $\mathbb{Q}$ equipped with the normalized Haar measure μ. For a positive integer e and an e-tuple $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in G(K)^e$ we denote by $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ the fixed field in $\tilde{\mathbb{Q}}$ of $\sigma_1, \ldots, \sigma_e$. The following two properties of $\tilde{\mathbb{Q}}(\sigma)$ are known to be true ([11] and [12]) for almost all $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$ (here $\tilde{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$):

(1a) every absolutely irreducible variety defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ has a $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$-rational point; and

(1b) $G(\mathbb{Q}(\boldsymbol{\sigma}))$ is isomorphic to the free profinite group on e generators.

They have been used in [14] to prove that the theory $T_1(\mathbb{Q}, e)$ of sentences in the language of fields that are true in almost all fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is decidable. In (6) it has been even proved that this theory is primitive recursive.

Shelah suggested that it would be natural to consider the theory $T(\mathbb{Q}, e)$ of all sentences in the language of fields extended by e unary operation symbols $\Sigma_1, \ldots, \Sigma_e$ (we denote the extended language by $\mathcal{L}(\text{ring } \mathbb{Q}, e)$) which hold in the structures $\langle \tilde{\mathbb{Q}}, \sigma_1, \ldots, \sigma_e \rangle$ for almost all $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$. Every sentence ϑ of the language of fields naturally corresponds to a sentence ϑ^* of $\mathcal{L}(\text{ring}, \mathbb{Q}, e)$ such that ϑ holds in $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ if and only if ϑ^* holds in $(\tilde{\mathbb{Q}}, \boldsymbol{\sigma})$. So, we may consider $T_1(\mathbb{Q}, e)$ as a subtheory of $T(\mathbb{Q}, e)$. More generally, for each positive integer n, we may consider sentences of $\mathcal{L}(\text{ring}, \mathbb{Q}, \text{e})$ where we restrict the variables to range only on elements of degree at most n over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Then, [9], the theory of these *n-bounded sentences* is primitive recursive.

In this work we put a limit on decidability results of this type; we prove that for

* Research supported by NSF Grant MCS-8301806.
** Work partially done while the author was a member of The Institute for Advanced Study at Princeton and partially while he visited UCI. Research supported by the fund for Basic Research administered by the Israel Academy of Sciences and Humanities.

$e \geq 2$, $T(\mathbb{Q}, e)$ is an undecidable theory (Theorem 3.1). Moreover we show that arithmetic is interpretable in $T(\mathbb{Q}, e)$.

We also consider the *probability,* prob(ϑ) *that a sentence is true in the structure* $\langle \tilde{\mathbb{Q}}, \boldsymbol{\sigma} \rangle$. This is the measure of the set

$$\text{Truth}(\vartheta) = \{\boldsymbol{\sigma} \in G(\mathbb{Q})^e \mid \vartheta \text{ is true in } \langle \tilde{\mathbb{Q}}, \boldsymbol{\sigma} \rangle\}.$$

If ϑ is a bounded statement, then prob(ϑ) is a rational number which can be effectively computed from ϑ (an immediate consequence of [9, Corollary 1.9]). Here we prove that for an arbitrary ϑ, prob(ϑ) is an arithmetically defined real number. (Theorem 5.4). Conversely, for each arithmetically defined real number r between 0 and 1 there exists a sentence ϑ with prob(ϑ) $= r$ (Theorem 6.5). In particular prob(ϑ) obtains transcendental values. Here r is said to be *arithmetically definable* if there exists a formula $\varphi(X, Y)$ of arithmetic such that for each $a, b \in \mathbb{N}$, $\varphi(a, b)$ is true if and only if $r < a/b$.

The main idea behind the proof of these results is to encode enough finite sets in the fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Applying Kummer theory we show (Section 1) how to use the operation of the σ's on the elements of $\tilde{\mathbb{Q}}$ to encode the group of roots of unity in $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Similarly we encode the $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$-division points of each elliptic curve E defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. For $e \geq 2$ and for almost all $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$, all these sets are finite ([13] and [8]). Once this is done we use an idea of Duret [4] to encode all subsets of these sets. Thus we get weak monadic theories encoded in $T(\mathbb{Q}, e)$. Then, using the roots of unity we interpret the theory of finite graphs in $T(\mathbb{Q}, e)$ (Proposition 2.3). A use of elliptic curves leads to the interpretation of arithmetic in $T(\mathbb{Q}, e)$ (Proposition 2.4).

The proof that each prob(ϑ) is an arithmetically definable number is based on the identity $\text{Truth}((\exists X)\varphi(X)) = \bigcup_{x \in \tilde{\mathbb{Q}}} \text{Truth}(\varphi(x))$, and on the observation, that if $\psi(X_1, \ldots, X_n)$ is a quantifier free formula in the extended language and $x_1, \ldots, x_n \in \tilde{\mathbb{Q}}$, then prob($\psi(\mathbf{x})$) is a rational number which can be effectively computed from $\psi(\mathbf{x})$.

To prove the converse we first find for the given arithmetically definable real r an arithmetically definable subset B_0 of $\mathbb{N}$ such that r is essentially equal to the probability that the number of roots of unity $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ belongs to B_0. Then we use the interpretation of arithmetic in $T(\mathbb{Q}, e)$ to obtain a sentence ϑ of $\mathcal{L}(\text{ring}, \mathbb{Q}, \in)$ such that prob(ϑ) $= r$.

Finally we note that our methods fail in the case $e = 1$, since for almost all $\sigma G(\mathbb{Q})$ the field $\tilde{\mathbb{Q}}(\sigma)$ contains infinitely many roots of unity [5], and also infinitely many division points of every elliptic curve defined over it [6]. On the other hand all our results for the case $e \geq 2$ are actually proved for an arbitrary infinite base field K finitely generated over its prime field.

1. Division points over $\tilde{K}(\boldsymbol{\sigma})$

Throughout this paper we shall be working over a fixed infinite base field K, finitely generated over its prime field. It is well known that such a field is

Hilbertian [15, p. 155]. We denote by $G(K)$ the absolute Galois group of K and for each e equip $G(K)^e$ with its unique normalized Haar measure μ. For each $\mathfrak{o} = (\sigma_1, \ldots, \sigma_e) \in G(K)^e$ let $K_s(\mathfrak{o})$ be the fixed field of $\sigma_1, \ldots, \sigma_e$ in the separable closure K_s of K, and let $\tilde{K}(\mathfrak{o})$ be the maximal purely inseparable extension of $K_s(\mathfrak{o})$.

Recall that a field L is said to be *PAC* (*pseudo algebraically closed*) if every absolutely irreducible nonempty variety V defined over L has an L-rational point. The algebraic and model theory of these fields will be treated quite thoroughly in the forthcoming monograph [7].

We summarize some well known properties of almost all fields $K_s(\mathfrak{o})$ for $e \geq 2$ that eventually lead to the undecidability of the theory of almost all structures $\langle \tilde{K}, \mathfrak{o} \rangle$. For any field F we denote by $U(F)$ the group of roots of unity in F. We also denote by ζ_n a primitive nth root of 1.

Proposition 1.1. *For every integer $e \geq 2$ and almost all $\mathfrak{o} \in G(K)^e$*

(a) *$\tilde{K}(\mathfrak{o})$ is PAC;*

(b) *$G(\tilde{K}(\mathfrak{o}))$ is isomorphic to the free profinite group $\hat{F}_e$, on e generators;*

(c) *$U(\tilde{K}(\mathfrak{o}))$ is a finite group; and*

(d) $U(\tilde{K}(\mathfrak{o})) = \{z \in \tilde{K} \mid \bigwedge_{i=1}^{e} \sigma_i z = z \wedge (\exists \alpha \in \tilde{K})[\alpha \neq 0 \wedge \sigma_1 \alpha = z\alpha]\}$.

Also, for every positive integer n the measure of the set of all $\mathfrak{o} \in G(K)^e$ such that $|U(\tilde{K}(\mathfrak{o}))| \geq n$ is positive.

Proof. See [11, p. 76] for (a), [12, p. 286] for (b) and [13, p. 124] for (c).

In order to prove (d) let $\mathfrak{o} \in G(K)^e$ and let $L = \tilde{K}(\mathfrak{o})$, and consider first an element z of the right hand side of (d). Let α be as above and denote by n the degree of the Galois hull of $L(\alpha)$ over L. Then $\alpha = \sigma_1^n \alpha = z^n \alpha$, hence $z^n = 1$.

For the converse we may assume that (b), (c) hold. Let $z \in L$ be a primitive nth root of unity. Since $G(L)$ is free the map $\sigma_1 \mapsto 1 + \mathbb{Z}$ extends to an epimorphism of $G(L)$ onto $\mathbb{Z}/n\mathbb{Z}$. The fixed field, N, of the kernel of this epimorphism is a cyclic extension of L of degree n and the restriction of σ_1 to N generates $\mathcal{G}(N/L)$. By Kummer theory, N is generated over L by a nonzero element α such that $\alpha^n \in L$. Then $\sigma_1 \alpha = \zeta_n \alpha$, for some primitive nth root of unity $\zeta_n \in L$. Since $z = \zeta_n^i$ for some $1 \leq i \leq n-1$, we have $\sigma_i \alpha^i = z\alpha^i$. Thus z belongs to the right hand side of (d).

The last part of the proposition follows from the fact that $G(K(\zeta_n))^e$ has positive measure. □

The roots of unity form the torsion subgroup of the multiplicative group of the field. To derive a stronger undecidability for the theory of almost all $\langle \tilde{K}, \mathfrak{o} \rangle$ we need information about the torsion of infinitely many elliptic curves over $\tilde{K}(\mathfrak{o})$.

Let L be a field of characteristic $\neq 2.3$. Recall that the *Weierstrass normal form* of an elliptic curve E over L is $Y^2 = 4X^3 - g_2 X - g_3$ where $\Delta = g_2^3 - 27g_3^2 \neq 0$. This form is completely determined by the j-invariant $j = 12^3 g_2^3 \Delta^{-1}$ and the Hasse

invariant $\gamma = -\frac{1}{2}g_2 g_3^{-1} \bmod (K^*)^2$. If $\mathrm{char}(L) = 2$ or $\mathrm{char}(L) = 3$, E has different Weierstrass normal forms; both of them are nevertheless cubic functions in X and Y [23, Appendix]. In each case $E(L)$, the set of L-rational points of L, is an abelian group, with the point at infinity as the zero, and with addition given by rational functions over L (e.g. [3, p. 214]). Let $E_n = \{P \in E \mid nP = 0\}$ be the set of n-division points of E, $E_n(L) = \{P \in E(L) \mid nP = 0\}$, and $E_{\mathrm{tor}}(L)$ the set of points of $E(L)$ of finite order.

Proposition 1.2 [8, p. 259]. *For each $e \geqslant 2$, for almost all $\sigma \in G(K)^e$ and for every elliptic curve E defined over $\tilde{K}(\sigma)$, the group $E_{\mathrm{tor}}(\tilde{K}(\sigma))$ is finite.*

It is well known that for each elliptic curve E defined over K, the group E_n is finite, and even isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, if n is relatively prime to $\mathrm{char}(K)$ [3, p. 219]. The field $K(E_n)$ is then a finite Galois extension of K which contains ζ_n [8, *p.* 218] and $\mathcal{G}(K(E_n)/K)$ operates faithfully on E_n. Thus the transformation group $(\mathcal{G}(K(E_n)/K), E_n)$ is isomorphic to a subgroup of $(\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}), \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$. This means that there are two maps (denoted by the same letter), an embedding $\Phi: \mathcal{G}(K(E_n)/K) \to \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ and an isomorphism $\Phi: E_n \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ such that $\Phi(\sigma P) = \Phi(\sigma) \cdot \Phi(P)$ for each $\sigma \in \mathcal{G}(K(E_n)/K)$ and $P \in E_n$.

Lemma 1.3. *For every positive integer n relatively prime to* $\mathrm{char}(K)$ *there is a sequence $E_1, E_2, E_3, \ldots$ of elliptic curves defined over K such that for each $i \geqslant 1$ there is an embedding*

$$\Phi_i: (\mathcal{G}(K(E_{i,n})/K), E_{i,n}) \to (\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$$

of transformation groups such that

$$\sigma(\zeta_n) = \zeta_n^{\det(\Phi_i(\sigma))} \quad \text{for every } \sigma \in \mathcal{G}(K(E_{i,n})/K)$$

and which maps $\mathcal{G}(K(E_{i,n})/K(\zeta_n))$ isomorphically onto $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$. *Moreover, we may take the sequence of fields $K(E_{1,n})$, $K(E_{2,n})$, $K(E_{3,n}), \ldots$ to be linearly disjoint over $K(\zeta_n)$.*

Proof. Let E be an elliptic curve with a transcendental j-invariant. Then it is well known (Igusa [10, p. 469]) that there exists an embedding

$$\Phi: (\mathcal{G}(K(j, E_n)/K(j)), E_n) \to (\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}), \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$$

of transformation groups such that

$$\sigma(\zeta_n) = \zeta_n^{\det(\Phi(\sigma))} \quad \text{for every } \sigma \in \mathcal{G}(K(j, E_n)/K(j))$$

and which maps $\mathcal{G}(L(j, E_{i,n})/L(j))$ isomorphically onto $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ for every algebraic extension L of $K(\zeta_n)$.

Suppose by induction that we have already found elliptic curves $E_1, \ldots, E_m$ that satisfy the above requirements. Then $L = K(E_{1,n}, \ldots, E_{m,n})$ is a finite Galois extension of K that contains ζ_n. For each $j' \in K^\times$ consider the elliptic curve E'

defined over K with j' as its j-invariant. The specialization $j \to j'$ defines a good reduction of E to E' which maps the group E_n isomorphically onto E'_n (Cassels [3, p. 254]). Since K is Hilbertian we may choose j' such that this reduction induces isomorphisms

$$(\mathcal{G}(K(j, E_n)/K(j)), E_n) \cong (\mathcal{G}(K(E'_n)/K), E'_n)$$

and

$$\mathcal{G}(L(j, E_n)/L(j)) \cong \mathcal{G}(L(E'_n)/L) \cong \mathcal{G}(K(\zeta_n, E'_n)/K(\zeta_n)).$$

We may therefore choose E_{m+1} as E'. □

Proposition 1.4. *For each positive integer e, for almost all $\sigma \in G(K)^e$ and for every $n \in \mathbb{N}$ there exists an elliptic curve E, defined over K, and which has a $\tilde{K}(\sigma)$-rational point P of order n.*

Proof. It suffices to fix e and n, and to prove that for almost all $\sigma \in G(K)^e$ there exists an elliptic curve E, defined over K, which has a $\tilde{K}(\sigma)$-rational point of order n.

We may use the sequence $E_1, E_2, E_3, \ldots$ of elliptic curves, introduced in Lemma 1.3. The action of $\mathcal{G}(K(\zeta_n)/K)$ on ζ_n induces an isomorphism onto a subgroup A of $\mathbb{Z}/n\mathbb{Z}$. For each $a \in A$ there is σ in $\mathcal{G}(K(E_{i,n})/K)$ such that $\det(\Phi_i(\sigma)) = a$. Since Φ_i maps $\mathcal{G}(K(E_{i,n})/K(\zeta_n))$ onto $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ each $g \in \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ with $\det(g) = a$ is the image under Φ_i of some element of $\mathcal{G}(K(E_{i,n})/K)$. Let $a_1, \ldots, a_e \in A$ and for each $i \geqslant 1$ denote by $a_{i1}, \ldots, a_{ie}$ the elements of $\mathcal{G}(K(E_{i,n})/K)$ which are mapped under Φ_i (Lemma 1.3), respectively, onto the matrices

$$\begin{pmatrix} 1 & 0 \\ 1-a_1 & a_1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ 1-a_e & a_e \end{pmatrix}.$$

For each j we have

$$\begin{pmatrix} 1 & 0 \\ 1-a_j & a_j \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{and} \quad \det\begin{pmatrix} 1 & 0 \\ 1-a_j & a_j \end{pmatrix} = a_j.$$

Since the order of $\binom{1}{1}$ is n so is the order of $P_i = \Phi_i^{-1}\binom{1}{1}$, $\alpha_{ij}(P_i) = P_i$ and $\sigma_{ij}(\zeta_n) = \zeta_n^{a_j}$. Hence, for each σ in the set

$$S(i, \mathbf{a}) = \{\sigma \in G(K)^e \mid \mathrm{Res}_{K(E_{i,n})}\, \sigma = \sigma_i\}$$

there exists a point in $E_i(\tilde{K}(\sigma))$ of order n. Thus, in order to conclude the proof, it suffices to prove that the measure of the union S of all $S(i, \mathbf{a})$'s is 1.

Indeed, choose a $\tau \in G(K)^e$ (depending on $\mathbf{a}$) such that $\tau_j(\zeta_n) = \zeta_n^{a_j}$, for $j = 1, \ldots, e$. Then $\tau^{-1} \cdot S(i, \mathbf{a}) \subseteq G(K(\zeta_n))^e$. Since the fields $K(E_{1,n}), K(E_{2,n}), \ldots$ are linearly disjoint over $K(\zeta_n)$, the sequence $\tau^{-1} \cdot S(1, \mathbf{a}), \tau^{-1} \cdot S(2, \mathbf{a}), \ldots$ is independent in the probability space $G(K(\zeta_n))^e$ [12, p. 285]. Also, the measure of $S(i, \mathbf{a})$ is nonzero and independent of i. Hence the measure of $S(\mathbf{a}) =$

$\bigcup_{i=1}^{\infty} S(i, \mathbf{a})$, in $G(K(\xi_n))^e$ is 1. Thus, in the space $G(K)^e$ we have

$$\mu(S(\mathbf{a})) = \mu\left(\bigcup_{i=1}^{\infty} \tau^{-1} \cdot S(i, \mathbf{a})\right) = |A|^{-e}.$$

For two distinct e-tuples $\mathbf{a}, \mathbf{a}' \in A^e$, the sets $S(\mathbf{a})$ and $S(\mathbf{a}')$ are disjoint. Since there are $|A|^e$ such sets, their union, S, is of measure 1. □

The recognition of $E_{\mathrm{tor}}(\tilde{K}(\sigma))$ in $E(\tilde{K})$, in terms of σ, depends on the following combination of [14, Theorem 2.2] and [14, Lemma 1.1].

Proposition 1.5. *For every positive integer e, for almost all $\sigma \in G(K)^e$, for every absolutely irreducible variety V defined over $L = \tilde{K}(\sigma)$ and for every birational transformation η of V of finite order, defined over L, there exists a point $a \in V(\tilde{K})$ such that $\sigma_i(a) = \eta(a)$, for $i = 1, \ldots, e$.*

Corollary 1.6. *For each $e \geq 1$, for almost all $\sigma \in G(K)^e$ and for every elliptic curve E defined over $L = \tilde{K}(\sigma)$*

$$E_{\mathrm{tor}}(L) = \left\{ Z \in E(\tilde{K}) \;\middle|\; \bigwedge_{i=1}^{e} \sigma_i z = z \wedge (\exists a \in E(\tilde{K}))\sigma_1 a = a + z \right\}; \tag{1}$$

the sum, $a + z$, is taken by the law of addition in E.

Proof. Suppose first that a point $z \in E(\tilde{K})$ belongs to the right hand side of (1). Then $z \in E(L)$ and there exists a point a as above. Let n be the degree of the Galois hull of $L(a)$ over L. Then $a = \sigma_i^n a = a + nz$, hence $nz = 0$, i.e. $z \in E_{\mathrm{tor}}(L)$.

To prove the converse we may assume that σ satisfies Proposition 1.5. Then each $z \in E_{\mathrm{tor}}(L)$ induces a birational transformation of E, $x \mapsto x + z$, of finite order and defined over L. Then there exists a point $a \in E(\tilde{K})$ such that $\sigma_i a = a + z$, for $i = 1, \ldots, e$. Thus z belongs to the right hand side of (1). □

The following result holds for arbitrary fields but it is in particular useful for PAC fields.

Proposition 1.7 (Duret [9, 4.3 and 5.2]). *Let $a_1, \ldots, a_k, b_1, \ldots, b_l$ be distinct elements of a field L*

(a) *If n is relatively prime to* $\mathrm{char}(L)$ *and c is a nonzero element of L, then the variety V defined over L by the system of equations*

$$X + a_i = Y_i^n, \quad \text{for } i = 1, \ldots, k; \qquad X + b_j = cZ_j^n, \quad \text{for } j = 1, \ldots, l$$

is nonempty and absolutely irreducible.

(b) *If* $\mathrm{char}(L) = p$, *$a_1, \ldots, a_k, b_1, \ldots, b_l$ are linearly independent over $\mathbb{F}_p$ and $c \in L$, then the variety defined by the system of equations*

$$a_i Y = Y_i^p - Y_i, \quad \text{for } i = 1, \ldots, k;$$
$$b_j X + c = Y_j^p - Y_i, \quad \text{for } j = 1, \ldots, l$$

is nonempty and absolutely irreducible.

Proof. (a) Let x be a transcendental element over L and let y_i, z_j be algebraic elements over $L(x)$ such that $x + a_i = y_i^n$, for $i = 1, \ldots, k$ and $x + b_j = cz_j^n$, for $j = 1, \ldots, l$.

Since $x + a_1, \ldots, x + a_k, x + b_1, \ldots, x + b_l$ are distinct prime elements of $\tilde{L}[x]$, they are also multiplicatively linearly independent modulo $(\tilde{L}(x)^\times)^n$. Thus, by Kummer theory $\mathcal{G}(\tilde{L}(x, \mathbf{y}, \mathbf{z})/\tilde{L}(x)) \cong (\mathbb{Z}/n\mathbb{Z})^{k+l}$ [18, p. 219]; in particular $\tilde{L}(x, y_1), \ldots, \tilde{L}(x, y_k), \tilde{L}(x, z_1), \ldots, \tilde{L}(x, z_l)$ are linearly disjoint over $\tilde{L}(x)$. This means that $Y_i^n - (x + a_i)$ is an irreducible polynomial over $L(x, y_1, \ldots, y_{i-1})$, for $i = 1, \ldots, k$ and $cZ_j^n - (x + b_j)$ is an irreducible polynomial over $L(x, \mathbf{y}, z_1, \ldots z_{j-1})$, for $j = 1, \ldots, l$. Therefore, if $(\xi, \boldsymbol{\eta}, \zeta)$ is a $\tilde{K}$-rational point of V, then the $\tilde{L}$-specialization $x \to \xi$ can be successively extended to an $\tilde{L}$-specialization $(x, \mathbf{y}, \mathbf{z}) \to (\xi, \boldsymbol{\eta}, \zeta)$ [17, p. 10]. We conclude that V is an absolutely irreducible variety with $(x, \mathbf{y}, \mathbf{z})$ as a generic point. Finally note that, since $n^{k+1} = [\tilde{L}(x, \mathbf{y}, \mathbf{z}) : \tilde{K}(x)] \leq [L(x, \mathbf{y}, \mathbf{z}) : L(x)] \leq n^{k+l}$, the fields $L(x, \mathbf{y}, \mathbf{z})$ and $\tilde{L}(x)$ are linearly disjoint over $L(x)$. Hence $L(x, \mathbf{y}, \mathbf{z})$ is a regular extension of L, therefore V is defined over L.

(b) Replace Kummer theory by Artin–Schreier theory [24, p. 221] and proceed as before. Note that the assumption about the linear independence over $\mathbb{F}_p$ of $a_1, \ldots, a_k, b_1, \ldots, b_l$ implies that the additive group $\mathcal{P}(L(x)) = \{u^p - u \mid u \in L(x)\}$ has index p^{k+l} in the group generated by $a_1 x, \ldots, a_k x, b_1 x - c, \ldots, b_l x - c$ and by $\mathcal{P}(L(x))$. □

2. Coding in PAC fields with monadic quantifiers

Every first order language $\mathcal{L}$ naturally extends to a language $\mathcal{L}_n$, the *language of n-adic quantifiers*. It is the simplest extension of $\mathcal{L}$ which allows for each $m \leq n$ quantification over certain m-ary relations on the underlying sets of structures of $\mathcal{L}$. To obtain $\mathcal{L}_n$ from $\mathcal{L}$ adjoin for each $m \leq n$ a sequence of *m-ary variable symbols* $X_{m,1}, X_{m,2}, X_{m,3}, \ldots$. The variable symbols of $\mathcal{L}$ are taken here as $x_1, x_2, x_3, \ldots$. An *atomic formula* of $\mathcal{L}_n$ is either an atomic formula of $\mathcal{L}$ or a formula $(x_{i(1)}, \ldots, x_{i(m)}) \in X_{mj}$, where $m \leq n$ and $i(1), \ldots, i(m), j$ are positive integers. As usual we close the set of formulas of $\mathcal{L}_n$ under negation, disjunction, conjunction and quantification on variables. A *structure* for $\mathcal{L}_n$ (or an *n-adic structure for* $\mathcal{L}$) is a system $\langle A, \mathcal{Q}_1, \ldots, \mathcal{Q}_n \rangle$, where A is a structure for $\mathcal{L}$ and, for each $m \leq n$, $\mathcal{Q}_m$ is a nonempty collection of m-ary relations on the underlying set of A (which we also denote by A). The structure is *weak* if for each m, all relations in $\mathcal{Q}_m$ are finite. We interpret the variables x_i as elements of A and the variables X_{mj} as elements of $\mathcal{Q}_j$. Thus "$(x_1, \ldots, x_m) \in X_{mj}$" means "$(x_1, \ldots, x_m)$ belongs to X_{mj}", "$\exists x_i$" means "there exists an element x_i in A" and "$\exists X_{mj}$" means "there exists an element X_{mj} in $\mathcal{Q}_m$".

Theories of $\mathcal{L}_n$, *n-adic theories*, are often undecidable. Thus whenever we "interpret" such a theory in another theory (e.g., a theory of PAC fields), the latter also turns out to be undecidable.

To be more precise let T and T^* be theories of languages $\mathscr{L}$ and $\mathscr{L}^*$, respectively. An *interpretation* of T in T^* is a recursive map $\vartheta \mapsto \vartheta^*$ of sentences of $\mathscr{L}$ onto sentences of $\mathscr{L}^*$ such that $T \vDash \vartheta$ if and only if $T^* \vDash \vartheta^*$. Obviously, if T is undecidable, then so is T^*.

We are mainly interested in the case where $\mathscr{L} = \mathscr{L}(\text{ring}, K)$ is the language of rings enriched by constant symbols for each element of K. For integers $q \geqslant 2$ and p, and for a field F, we say that *hypothesis* $H(p, q)$ *holds in* F if

$$\text{char}(F) = p, \quad p \nmid q, \quad \zeta_q \in F \quad \text{and} \quad (F^\times)^q \neq F^\times;$$

or

$$\text{char}(F) = p, \quad p \mid q \quad \text{and} \quad \mathscr{P}(F) = \{u^p - u \mid u \in F\} \neq F.$$

Similarly we say that a class, $\mathscr{F}$, of n-adic structures over fields satisfies *hypothesis* $H(p, q)$ if for each structure $\langle F, \mathscr{Q}_1, \ldots, \mathscr{Q}_n \rangle$ in $\mathscr{F}$, F is a field that satisfies hypotheses $H(p, q)$.

For the next lemma consider a class $\mathscr{F}$ of weak monadic structures over PAC fields that satisfy condition $H(p, q)$, for some p and q. To each $\langle F, \mathscr{Q} \rangle$ in $\mathscr{F}$ we associate another monadic structure $\langle F, \mathscr{Q}' \rangle$ and denote the class of all $\langle F, \mathscr{Q}' \rangle$'s by $\mathscr{F}'$. The definition of $\langle F, \mathscr{Q}' \rangle$ is divided into two cases:

Case A, $p \nmid q$: $\mathscr{Q}'$ is the collection of all sets

$$D(A, u) = \{a \in A \mid (\exists y \in F)[y \neq 0 \,\&\, a + u = y^q\}, \quad \text{where } A \in \mathscr{Q} \text{ and } u \in F.$$

Case B, $p \mid q$: $\mathscr{Q}'$ is the collection of all sets

$$E(A, u, v) = \left\{a \in A \mid (\exists y \in F)\left[\frac{v}{u + a} = y^p - y\right]\right\}, \quad \text{where } A \in \mathscr{Q} \text{ and } u, v \in F.$$

In both cases each $X \in \mathscr{Q}'$ is contained in some $A \in \mathscr{Q}$.

Lemma 2.1. (a) *For each structure* $\langle F, \mathscr{Q} \rangle$ *in* $\mathscr{F}$ *the collection* $\mathscr{Q}'$ *consists of all subsets of the sets* $A \in \mathscr{Q}$.

(b) *The monadic theory* $\text{Th}(\mathscr{F}')$ *is interpretable in* $\text{Th}(\mathscr{F})$.

(c) *To each formula* $\varphi(X)$ *in* $\mathscr{L}_1$ *we recursively associate another formula* $\varphi'(X)$ *of* $\mathscr{L}_1$ *such that for every* $\langle F, \mathscr{Q} \rangle \in \mathscr{F}$ *and* $A \in \mathscr{Q}$ *we have*: $\langle F, \mathscr{Q}' \rangle \vDash \varphi(A)$ *if and only if* $\langle F, \mathscr{Q} \rangle \vDash \varphi'(A)$.

Proof. We treat each of the above cases separately.

Case A: Choose an element $c \in F - F^q$. Let $A \in \mathscr{Q}$ and let X be a subset of A. By Proposition 1.7(a), and since A is finite and F is PAC, there exist $u \in F$ and $y_a \in F^\times$ for each $a \in A$ such that $a + u = y_a^q$ for all $a \in X$ and $a + u = cy_a^q$ for all $a \in A - X$. Then $X = D(A, u)$, since $(F^\times)^q \cap c(F^\times)^q = \emptyset$. This proves (a).

Now define a map $\varphi \to \varphi^*$ from formulas of $\mathscr{L}_1$ onto formulas of $\mathscr{L}_1$ by induction on the structure of φ. If φ is an atomic formula of $\mathscr{L}$, let $\varphi^* = \varphi$. If φ is the formula $a \in X$, define φ^* to be the formula

$$a \in A_X \wedge (\exists y_X)[y_X \neq 0 \wedge a + u_X = y_X^q]$$

where u_X, y_X are variables symbols on elements and A_X is a variable symbol on sets attached to the variable X. Next let the star operation commute with negation, disjunction, conjunction and quantification on elements. Finally, if ψ^* has been defined for a formula ψ and φ is the formula $(\exists X)\psi$, then define φ^* to be $(\exists A_X)(\exists u_X)\psi^*$.

One verifies now by induction on the structure of a formula $\varphi(\mathbf{z}, X_1, \ldots, X_n)$ with the free variables among $\{\mathbf{z}, X_1, \ldots, X_n\}$ that for each monadic structure $\langle F, \mathcal{Q}\rangle$ in $\mathcal{F}$, for $A_1, \ldots, A_n \in \mathcal{Q}$ and $u_1, \ldots, u_n \in F$ we have

$$\begin{aligned} &\langle F, \mathcal{Q}\rangle \models \varphi^*(\mathbf{z}, A_1, u_1, \ldots, A_n, u_n) \quad \Leftrightarrow \\ &\langle F, \mathcal{Q}'\rangle \models \varphi(\mathbf{z}, D(A_1, u_1), \ldots, D(A_n, u_n)). \end{aligned} \tag{1}$$

In particular, if ϑ is a sentence of $\mathcal{L}_1$, then ϑ is true in $\langle F, \mathcal{Q}'\rangle$ if and only if ϑ^* is true in $\langle F, \mathcal{Q}\rangle$. Thus the map $\vartheta \mapsto \vartheta^*$ is an interpretation of the $\mathrm{Th}(\mathcal{F}')$ in $\mathrm{Th}(\mathcal{F})$.

For a formula $\varphi(X)$ of $\mathcal{L}_1$ let $\varphi'(X)$ be the formula

$$(\exists v_X)[\varphi^*(X, v_X) \wedge (\forall a_X)[a_X \in X \to (\exists z_X)[z_X \neq 0 \wedge a_X + v_X = z_X^q]]].$$

For each $A \in \mathcal{Q}$ there exists $v \in F$ such that $A = D(A, v)$. It follows from (1) that $\langle F, \mathcal{Q}'\rangle \models \varphi(A)$ if and only if $\langle F, \mathcal{Q}\rangle \models \varphi'(A)$. This proves (c).

Case B: Choose an element $c \in F - \mathcal{P}(F)$, let $A \in \mathcal{Q}$ and let X be a subset of A. Since F is an infinite field, there exists an element $u \in F$ such that $\sum_{a \in A} \alpha(a)(u + a)^{-1} \neq 0$ for every function $\alpha : A \to \mathbb{F}_p$ which is not identically zero. Now apply Proposition 1.7(b) to find $v \in F$ and for each $a \in A$ an element $y_a \in F$ such that $(u + a)^{-1}v = y_a^p - y_a$ for each $a \in X$ and $(u + a)^{-1}v = y_a^p - y_a + c$ for each $a \in A - X$. It follows that $E(A, u, v) = X$. This proves (a). The proofs of (b) and (c) are done as in Case A. □

Our next construction allows us to replace monadic structures by certain n-adic structures. As before we start from a class $\mathcal{F}$ of weak monadic structures over PAC fields that satisfies hypotheses $H(p, q)$. For each structure $\{F, \mathcal{Q}\rangle \in \mathcal{F}$ and for every $m \leqslant n$ let $\mathcal{Q}_m$ be the collection of all subsets of $A_1 \times \cdots \times A_m$, where $A_1, \ldots, A_m \in \mathcal{Q}$. Denote by $\mathcal{F}_n$ the class of n-adic structures $\langle F, \mathcal{Q}_1, \ldots, \mathcal{Q}_n\rangle$ obtained in this way.

Lemma 2.2. $\mathrm{Th}(\mathcal{F}_n)$ *is interpretable in* $\mathrm{Th}(\mathcal{F})$. *Moreover, to each formula* $\varphi(X)$ *in* $\mathcal{L}_1$ *we can recursively associate a formula* $\varphi'(X)$ *in* $\mathcal{L}_1$ *such that for every* $\langle F, \mathcal{Q}\rangle \in \mathcal{F}$ *and* $A \in \mathcal{Q}$ *we have*

$$\langle F, \mathcal{Q}_1, \ldots, \mathcal{Q}_n\rangle \models \varphi(A) \quad \Leftrightarrow \quad \langle F, \mathcal{Q}\rangle \models \varphi'(A).$$

Proof. The interpretation of $\mathrm{Th}(\mathcal{F}_n)$ in $\mathrm{Th}(\mathcal{F})$ goes through the theories of two auxiliary classes of weak monadic structures.

For each $\langle F, \mathcal{Q}\rangle$ in $\mathcal{F}$ and each $m \leqslant n$ consider the bilinear map

$\pi : F^m \times F^m \to F$ defined by $\pi(\mathbf{c}, \mathbf{x}) = \sum_{i=1}^m c_i x_i$. Extend $\mathscr{Q}$ to

$$\mathscr{Q}' = \bigcup_{m=1}^{n} \{\pi(\mathbf{c}, A_1 \times \cdots \times A_m) \mid \mathbf{c} \in F^m \text{ and } A_1, \ldots, A_m \in \mathscr{Q}\}$$

and let $\mathscr{F}'$ be the class of all monadic structures $\langle F, \mathscr{Q}' \rangle$. Then the relation $B = \pi(\mathbf{c}, A_1, \ldots, A_m)$ between the sets in $\mathscr{Q}$ and the sets in $\mathscr{Q}'$ gives an obvious interpretation of $\mathrm{Th}(\mathscr{F}')$ in $\mathrm{Th}(\mathscr{F})$. We can then use this interpretation and the identity $A = \pi(1, A)$ to recursively associate to each formula $\varphi(X)$ of $\mathscr{L}_1$ a formula $\varphi'(X)$ of $\mathscr{L}_1$ such that $\langle F, \mathscr{Q}' \rangle \models \varphi(A)$ if and only if $\langle F, \mathscr{Q} \rangle \models \varphi'(A)$, for every $\langle F, \mathscr{Q} \rangle \in \mathscr{F}$ and $A \in \mathscr{Q}$.

Next replace each $\langle F, \mathscr{Q}' \rangle \in \mathscr{F}'$ by the weak monadic structure $\langle F, \mathscr{Q}'' \rangle$, where $\mathscr{Q}''$ consists of all subsets of sets in $\mathscr{Q}'$. Lemma 2.1 asserts that the theory of $\mathscr{F}''$, of $\mathscr{F}''$, the class of all $\langle F, \mathscr{Q}'' \rangle$, is interpretable in $\mathrm{Th}(\mathscr{F}')$. Moreover, by Lemma 2.1, we can recursively associate to each formula $\varphi(X)$ of $\mathscr{L}_1$ a formula $\varphi''(X)$ of $\mathscr{L}_1$ such that $\langle F, \mathscr{Q}'' \rangle \models \varphi(A)$ if and only if $\langle F, \mathscr{Q}' \rangle \models \varphi''(A)$, for every $\langle F, \mathscr{Q} \rangle \in \mathscr{F}$ and $A \in \mathscr{Q}$.

Finally, for each $\langle F, \mathscr{Q} \rangle \in \mathscr{F}$, $m \leqslant n$, $\mathbf{c} \in F^m$, $A_1, \ldots, A_m \in \mathscr{Q}$ and $B \subseteq \pi(\mathbf{c}, A_1 \times \cdots \times A_m)$, the set

$$S(\mathbf{c}, A_1, \ldots, A_m, B) = \{(x_1, \ldots, x_m) \in A_1 \times \cdots \times A_m \mid \pi(\mathbf{c}, \mathbf{x}) \in B\}$$

belongs to $\mathscr{Q}_n$. Conversely, let $A_1, \ldots, A_m \in \mathscr{Q}$. Since F is infinite there exists $\mathbf{c} \in F^m$ such that $\sum_{i=1}^m (x_i - x_i')c_i \neq 0$ for every distinct $\mathbf{x}, \mathbf{x}' \in A_1 \times \cdots \times A_m$. Then the map $\mathbf{x} \mapsto \pi(\mathbf{c}, \mathbf{x})$ from $A_1 \times \cdots \times A_m$ into F is injective. Hence, if we start from $R \subseteq A_1 \times \cdots \times A_m$ and define $B = \{\pi(\mathbf{c}, \mathbf{x}) \mid \mathbf{x} \in R\}$, then $R = S(\mathbf{c}, A_1, \ldots, A_m, B)$. This representation of $\mathscr{Q}_m$ gives an obvious interpretation of $\mathrm{Th}(\mathscr{F}_n)$ in $\mathrm{Th}(\mathscr{F}'')$. Moreover, the identity $A = S(1, A, A)$, can be used to recursively associate to each formula $\varphi(X)$ of $\mathscr{L}_1$ a formula $\varphi'(X)$ of $\mathscr{L}_1$ such that $\langle F, \mathscr{Q}_1, \ldots, \mathscr{Q}_n \rangle \models \varphi(A)$ if and only if $\langle F, \mathscr{Q}'' \rangle \models \varphi'(X)$ for every $\langle F, \mathscr{Q} \rangle \in \mathscr{F}$ and $A \in \mathscr{Q}$.

A combination of the above three interpretations gives the desired one. □

Proposition 2.3. *Let $\mathscr{F}$ be a class of weak monadic structures over PAC fields that satisfies hypotheses $H(p, q)$. Assume that*

(2) *For every $n \geqslant 1$ there exists $\langle F, \mathscr{Q} \rangle \in \mathscr{F}$ and there exists $A \in \mathscr{Q}$ of cardinality at least n.*

Then $\mathrm{Th}(\mathscr{F})$ *is undecidable.*

Proof. Apply Lemma 2.2, for $n = 2$, to $\mathscr{F}$. Then recursively associate to each sentence ϑ in the language $\mathscr{L}(\mathrm{graph})$ of symmetric graphs the sentence ϑ^* of $\mathscr{L}_2$

$$(\forall A \in \mathscr{Q}_1)(\forall R \in \mathscr{Q}_2)[R \subseteq A \times A \text{ and } R \text{ symmetric} \Rightarrow (A, R) \models \vartheta].$$

Let T be the set of sentences ϑ of $\mathscr{L}(\text{graph})$ such that $\text{Th}(\mathscr{F}_2) \models \vartheta^*$. By (2) and by Lemma 2.2, $T = \text{Th}(\text{finite symmetric graphs})$, hence [5, p. 79] T is nonrecursive. It follows that $\text{Th}(\mathscr{F}_2)$, hence also $\text{Th}(\mathscr{F})$ is undecidable. □

Remark. Proposition 2.3 remains true if we remove the restriction on the structures to be weak and demand instead in (2) that A is finite. Similar changes should be made in Lemmas 2.1 and 2.2.

In our next proposition we replace (2) by a stronger condition and then interpret arithmetic in $\text{Th}(\mathscr{F})$. This is a stronger result than the interpretation of the theory of finite graphs in $\text{Th}(\mathscr{F})$, since it is known that arithmetic is much more complicated than the theory of finite graphs. By 'Arithmetic' we mean the complete theory of the structure $\mathscr{N} = \langle \mathbb{N}, +, \cdot, 1 \rangle$.

Proposition 2.4. *Let $\mathscr{F}$ be a class of weak monadic structures over PAC fields that satisfies hypotheses $H(p, q)$. Assume that for all $\langle F, \mathscr{D} \rangle \in \mathscr{F}$ the cardinality of the sets $A \in \mathscr{D}$ is unbounded. Then* $\text{Th}(\mathscr{N})$ *is interpretable in* $\text{Th}(\mathscr{F})$. *Moreover there is a recursive map $\varphi(x) \mapsto \varphi^*(X)$ from formulas of arithmetic to formulas of $\mathscr{L}_1$ such that for all $\langle F, \mathscr{D} \rangle \in \mathscr{F}$ and $A \in \mathscr{D}$ we have $\langle F, \mathscr{D} \rangle \models \varphi^*(A)$ if and only if $\mathscr{N} \models \varphi(|A|)$.*

Proof. We apply Lemma 2.2, for $n = 3$, to $\mathscr{F}$ and interpret $\text{Th}(\mathscr{N})$ in $\text{Th}(\mathscr{F}_3)$. Recall that for each $\langle F, \mathscr{D} \rangle \in \mathscr{F}$, the collection $\mathscr{D}_1$ contains with each set A all subsets of A. Therefore the map $A \mapsto |A|$ maps $\mathscr{D}_1$ onto $\mathbb{N}$.

We give explicit first-order definitions of the preimages in $\mathscr{D}_1$ of $=$, $+$ and $\cdot$:

Equality: $|A_1| = |A_2| \Leftrightarrow (\exists R \in \mathscr{D}_2)[R \subseteq A_1 \times A_2$ is a bijection between A_1 and $A_2]$.

Addition: $|A_1| + |A_2| = |A| \Leftrightarrow$ there exist B_1, B_2 in $\mathscr{D}_1$ partitioning A with $|A_1| = |B_1|$ and $|A_2| = |B_2|$.

Multiplication: $|A_1| \cdot |A_2| = |A|$ if and only if there exists R in $\mathscr{D}_3$ such that $R \subseteq A_1 \times A_2 \times A$ is a bijection between $A_1 \times A_2$ and A.

This interpretation gives a recursive map, $\varphi(x) \mapsto \varphi'(X)$, from formulas of $\mathscr{L}(\text{arith})$ with the variable x onto formulas $\varphi'(X)$ with the variable X such that for all $\langle F, \mathscr{D} \rangle \in \mathscr{F}$ and for each $A \in \mathscr{D}_1$

$$\langle F, \mathscr{D}_1, \mathscr{D}_2, \mathscr{D}_3 \rangle \models \varphi'(A) \Leftrightarrow \mathscr{N} \models \varphi(|A|).$$

In particular, if ϑ is a sentence of $\mathscr{L}(\text{arith})$, then $\mathscr{N} \models \vartheta$ if and only if $\text{Th}(\mathscr{F}_3) \models \vartheta'$. □

Remark. It can be shown that the interpretability of $\text{Th}(\mathscr{N})$ in $\text{Th}(\mathscr{F})$ follows already from the existence of a structure $\langle F, \mathscr{D} \rangle \in \mathscr{F}$ such that the cardinality of the sets $A \in \mathscr{D}$ is unbounded.

3. The theory of almost all $\langle \tilde{K}, \sigma_1, \ldots, \sigma_e \rangle$'s

We combine the methods developed in Section 2 with the algebraic background of Section 1 to obtain undecidability results for theories over PAC fields

Recall that we are working over a fixed infinite base field K, finitely generated over its prime field. For each $e \geq 1$ extend the language $\mathcal{L}(\text{ring}, K)$ (Section 2) to a language $\mathcal{L} = \mathcal{L}(\text{ring}, K, e)$ by adding e unary function symbols $\Sigma_1, \ldots, \Sigma_e$ and also extend $\mathcal{L}$ to a language $\mathcal{L}(\text{ring}, \tilde{K}, e)$ by adding constant symbols for each element of $\tilde{K}$. Every e-tuple $(\sigma_1, \ldots, \sigma_e)$ of automorphism of K_s over K extends uniquely to an e-tuple of automorphisms of $\tilde{K}$, also denoted by $\sigma_1, \ldots, \sigma_e$. So $\langle \tilde{K}, \boldsymbol{\sigma} \rangle$ is a structure for $\mathcal{L}(\text{ring}, \tilde{K}, e)$. We denote by $T(K, e)$ the set of all sentences ϑ of $\mathcal{L}(\text{ring}, K, e)$ true in $\langle \tilde{K}, \boldsymbol{\sigma} \rangle$, for almost all $\boldsymbol{\sigma} \in G(K)^e$. In general we define the *truth set of* a sentence ϑ of $\mathcal{L}(\text{ring}, \tilde{K}, e)$ as

$$\text{Truth}(\vartheta) = \{\boldsymbol{\sigma} \in G(K)^e \mid \langle \tilde{K}, \boldsymbol{\sigma} \rangle \models \vartheta\}.$$

It is a measurable set. Indeed, if $\varphi(x_1, \ldots, x_n)$ is a quantifier free formula and $x_1, \ldots, x_n \in \tilde{K}$, then $\text{Truth}(\varphi(x_1, \ldots, x_n))$ is an open-closed set. For an arbitrary formula $\varphi(\mathbf{x}, y)$ we have

$$\text{Truth}((\exists y)\varphi(\mathbf{x}, y)) = \bigcup_y \text{Truth}(\varphi(\mathbf{x}, y)),$$

where y ranges over $\tilde{K}$. Conclude by induction on structure that $\text{Truth}(\vartheta)$ is even a Borel subset of $G(K)^e$.

The measure of $\text{Truth}(\vartheta)$ may be considered as the probability of ϑ to be true among the $\langle \tilde{K}, \boldsymbol{\sigma} \rangle$'s and we write $\text{Prob}(\vartheta) = \mu(\text{Truth}(\vartheta))$.

Theorem 3.1. *For $e \geq 2$, $T(K, e)$ is an undecidable theory. Moreover* $\text{Th}(\mathcal{N})$ *is interpretable in $T(K, e)$. Also, there is a recursive map $\varphi(x) \mapsto \varphi^*$ from formulas in arithmetic onto sentences in* $\mathcal{L}(\text{ring}, K, e)$ *such that for almost all $\boldsymbol{\sigma} \in G(K)^e$*

$$\mathcal{N} \models \varphi(|U(\tilde{K}(\boldsymbol{\sigma}))|) \Leftrightarrow \langle \tilde{K}, \boldsymbol{\sigma} \rangle \models \varphi^*.$$

Proof. Let S be the intersection of the countably many sets $\text{Truth}(\vartheta)$ where $\vartheta \in T(K, e)$ and the set $\{\boldsymbol{\sigma} \in G(K)^e \mid \tilde{U}(K(\boldsymbol{\sigma}))$ is finite$\}$ (Proposition 1.1). Then $\mu(S) = 1$. For each $\boldsymbol{\sigma} \in S$ the field $\tilde{K}(\boldsymbol{\sigma})$ is a PAC field that satisfies hypotheses $H(\text{char}(K), 2)$ and $U(\tilde{K}(\boldsymbol{\sigma}))$, the group of roots of unity in $K(\boldsymbol{\sigma})$, is finite. We associate with $\boldsymbol{\sigma}$ the monadic structure over $\tilde{K}(\boldsymbol{\sigma})$, consisting of one set, namely $U(\tilde{K}(\boldsymbol{\sigma}))$ and let $\mathcal{F}$ be the class of all these structures. Since $U(\tilde{K}(\boldsymbol{\sigma}))$ is unbounded as $\boldsymbol{\sigma}$ ranges over S (Proposition 1.1), Proposition 2.3 implies that $\text{Th}(\mathcal{F})$ is undecidable.

Proposition 1.1(d) suggests an interpretation of $\text{Th}(\mathcal{F})$ in $\text{Th}(K, e)$: replace $z \in A$ by

$$(\exists a)\Big(\bigwedge_{i=1}^{e} \sigma_i z = z \wedge \sigma_1 z = za\Big).$$

If φ^* is the interpretation of a formula φ of $\mathscr{L}_1$, then φ^* is also the interpretation of $(\exists A)\varphi$. We conclude that $T(K, e)$ is undecidable.

To interpret $\mathrm{Th}(\mathscr{N})$ in $T(K, e)$ we first consider an elliptic curve E defined over an algebraic extension L of K as the set of solutions in $\tilde{K}^2$ of a certain cubic, $f(X, Y)$, in Weierstrass normal form. Denote by $E'_{\mathrm{tor}}(L)$ the set of first coordinates of points in $E_{\mathrm{tor}}(L)$. Note that for each $x \in E'_{\mathrm{tor}}(L)$ there exists at most three points of $E(L)$ having x as their first coordinate. Now associate with each $\sigma \in S$ the collection

$$\mathscr{Q}'(\sigma) = \{U(\tilde{K}(\sigma))\} \cap \{E'_{\mathrm{tor}}(\tilde{K}(\sigma)) \mid E \text{ is an elliptic curve defined over } \tilde{K}(\sigma)\}.$$

By Proposition 1.2 we may assume that every set in $\mathscr{Q}'(\sigma)$ is finite. By Proposition 1.4, the cardinality of the sets in $\mathscr{Q}'(\sigma)$ is unbounded. Thus, the class $\mathscr{F}' = \{\langle \tilde{K}(\sigma), \mathscr{Q}'(\sigma)\rangle \mid \sigma \in S\}$ of monadic structures satisfies the conditions of Proposition 2.4. Conclude that $\mathrm{Th}(\mathscr{N})$ is interpretable in $\mathrm{Th}(\mathscr{F}')$. Moreover, there is a recursive map $\varphi(x) \mapsto \varphi'(X)$, from formulas of arithmetic onto formulas of $\mathscr{L}_1$ such that for every $\sigma \in S$ and every $A \in \mathscr{Q}'(\sigma)$, $\mathrm{Th}(\mathscr{N}) \models \varphi(|A|)$ if and only if $\langle \tilde{K}(\sigma), \mathscr{Q}'(\sigma)\rangle \models \varphi'(A)$.

Now use Corollary 1.6, to interpret $\mathrm{Th}(\mathscr{F}')$ in $T(K, e)$. Observe that here $\exists A$ should be replaced by saying "there exist coefficients in $\tilde{K}(\sigma)$ of the cubic $f(X, Y)$ such that the corresponding discriminant is not zero" (here it is necessary to distinguish between $\mathrm{char}(K) = 2$, $\mathrm{char}(K) = 3$ and $\mathrm{char}(K) \neq 2, 3$), while "$x \in A$" should be interpreted as "x is a root of unity or x is the first coordinate of an elliptic curve E defined over $\tilde{K}(\sigma)$". Conclude that $\mathrm{Th}(\mathscr{N})$ is interpretable in $T(K, e)$.

Finally we reserve a monadic variable, say X_1, to be interpreted only as $U(\tilde{K}(\sigma))$, while all other monadic variables are interpreted as before, either as $U(\tilde{K}(\sigma))$ or as $E'_{\mathrm{tor}}(\tilde{K}(\sigma))$. This gives a recursive map $\varphi'(X_1) \mapsto \varphi^*$ from formulas of $\mathscr{L}_1$ onto sentences of $\mathscr{L}(\mathrm{ring}, K, e)$ such that for every $\sigma \in S$, $\langle \tilde{K}(\sigma), \mathscr{Q}'(\sigma)\rangle \models \varphi'(U(\tilde{K}(\sigma)))$ if and only if $\langle \tilde{K}, \sigma\rangle \models \varphi^*$. Combine this with the above to obtain the final statement of the theorem. □

Problem 3.2. Is $T(K, 1)$ a decidable theory?

4. Arithmetically defined functions

Recall that an n-ary relation R on $\mathbb{N}$ is *arithmetically definable* (we will usually omit the word 'arithmetically') if there exists a formula $\varphi(x_1, \ldots, x_n)$ of $\mathscr{N}$ such that for each $\mathbf{x} \in \mathbb{N}^n$, we have $\mathbf{x} \in R$ if and only if $\mathscr{N} \models \varphi(\mathbf{x})$. Similarly define *definable functions* $f : \mathbb{N}^n \to \mathbb{N}$.

A real number r is said to be *definable* if there exists a formula $\varphi(x, y)$ of $\mathscr{N}$ such that $r > a/b$ if and only if $\mathscr{N} \models \varphi(a, b)$. In particular every rational number is definable. More generally, a sequence $\{q_n\}_{n=1}^{\infty}$ of real numbers is said to be

definable, if there exists a formula $\psi(x, y, z)$ of $\mathcal{N}$ such that $q_n > a/b$ if and only if $\mathcal{N} \models \psi(n, a, b)$. Similarly one defines a *definable sequence* $\{q_n(k)\}_{n=1}^{\infty}$ *of real-valued functions* and observes that if $q(k) = \lim_{n\to\infty} q_n(k)$, for every $k \in \mathbb{N}$, then $q(k)$ is a definable real-valued function.

It is well known that recursive functions are definable. Moreover, a function (resp. relation) which is defined from definable functions by the recursive operations (composition of functions, induction and minimalizations) is itself definable [22, p. 313].

Lemma 4.1. *Let $\{q_n\}_{n=1}^{\infty}$ be a definable sequence of nonnegative real numbers with $a = \sum_{n=1}^{\infty} q_n$ finite. Suppose that for all n we have*

$$q_n \leqslant \sum_{i>n} q_i. \tag{1}$$

Then for each definable real r with $0 < r \leqslant a$ there is a definable increasing sequence $\{n(i)\}_{i=1}^{\infty}$ such that $\sum_{i=1}^{\infty} q_n(i) = r$.

Proof. Define the sequence $\{n(i)\}_{i=1}^{\infty}$ by induction so that for each k

$$0 < r - q_{n(1)} - \cdots - q_{n(k)} \leqslant \sum_{i>n(k)} q_i. \tag{2}$$

Indeed, if $q_{n(1)}, \ldots, q_{n(k)}$ have already been defined, then, since $q_i \to 0$, and by (2) there exists an $i > n(k)$ such that $q_i < r - q_{n(1)} - \cdots - q_{n(k)}$. Let $n(k+1)$ be the first integer larger than $n(k)$ such that

$$q_{n(k+1)} < r - q_{n(1)} - \cdots - q_{n(k)}. \tag{3}$$

If $n(k+1) = n(k) + 1$, then, by (2),

$$r - q_{n(1)} - \cdots - q_{n(k)} - q_{n(k+1)} \leqslant \sum_{i>n(k)} q_i - q_{n(k)+1} = \sum_{i>n(k+1)} q_i.$$

If $n(k+1) > n(k) + 1$, then, by (1)

$$r - q_{n(1)} - \cdots - q_{n(k)} \leqslant q_{n(k+1)-1} \leqslant \sum_{i>n(k+1)-1} q_i.$$

Thus in both cases (2) holds for $k+1$. Note that to define $n(1)$ (2) degenerates to the assumption $0 < r \leqslant \sum_{i>0} q_i$.

The right hand side of (2) is the tail of a convergent series. Conclude that $r = \sum_{i=1}^{\infty} q_{n(i)}$. Also, the definition of $\{n(i)\}_{i=1}^{\infty}$ involves only recursive operations on the definable number r and the definable sequence $\{q_n\}_{n=1}^{\infty}$. Hence $\{n(i)\}_{i=1}^{\infty}$ is a definable sequence. □

Lemma 4.2. *Let B be a definable set of positive integers and let T be a finite set, disjoint from B. Suppose that $q : T \cup B \to \mathbb{R}$ is a definable function such that*

(4a) *$q_n \geqslant 0$ for each $n \in T \cup B$ and $s = \sum_{n\in T\cup B} q_n$ is finite;*

(4b) *$q_t \leqslant \max_{b\in B} q_n$ for each $t \in T$; and*

(4c) *for every $b \in B$ there exists $b' \in B$ such that $\frac{1}{2} q_b < q_{b'} < q_b$.*

Then for all definable r with $0 < r \leq s$, there exists a subset T_0 of T and a definable subset B_0 of B such that $\sum_{t \in T_0} q_t + \sum_{b \in B_0} q_b = r$,

Proof. By Lemma 4.1 it suffices to define a bijective map $\pi : \mathbb{N} \to T \cup B$ such that the sequence $\{q_{\pi(n)}\}_{n=1}^{\infty}$ satisfies condition (1).

Indeed define first π from $\{1, \ldots, |T|\}$ onto T in an arbitrary way. Then proceed by induction. Assume that $n > |T|$ and that $\pi(n)$ has already been defined such that if $i \in B - \{\pi(|T|+1), \ldots, \pi(n)\} = C$, then $q_i \leq q_{\pi(n)}$. Define $\pi(n+1)$ as the first element of C such that $q_{\pi(n+1)} = \max_{i \in C} q_i$. Then $\pi : \mathbb{N} - \{1, \ldots, |T|\} \to B$ is injective. Since for every $\varepsilon > 0$ there are only finitely many $b \in B$ such that $q_b \geq \varepsilon$, the map π is also surjective.

If $n \leq |T|$, then (4b) implies that $q_{\pi(n)} \leq \sum_{i>n} q_{\pi(i)}$. For $n > |T|$, (4c) gives a subset $\{b(0), b(1), b(2), \ldots\}$ of B such that $\pi(n) = b(0)$ and $\frac{1}{2} q_{b(j)} < q_{b(j+1)} < q_{b(j)}$ for $j = 0, 1, 2, \ldots$. For each $j \geq 1$ let $n(j) > |T|$ such that $\pi(n(j)) = b(j)$. Then $n < n(j)$ and $q_{\pi(n(j))} > 2^{-j} q_{\pi(n)}$. Hence

$$\sum_{n<i} q_{\pi(i)} \geq \sum_{j=1}^{\infty} q_{\pi(n(j))} \geq \sum_{j=1}^{\infty} 2^{-j} q_{\pi(n)} = q_{\pi(n)},$$

as required. □

5. Definability of Prob(ϑ)

In this section we assume that $e \geq 1$. We saw in Section 3 that for each sentence ϑ of $\mathcal{L}(\text{ring}, \tilde{K}, e)$, Truth($\vartheta$) is measurable.

To describe the nature of Prob(ϑ) we assume that K is an explicitly given finitely generated extension of a prime field. Then one can effectively give an encoding $i : \tilde{K} \to \mathbb{N}$ such that $i(K)$ is a recursive subset of $i(\tilde{K})$ [6, Theorem 2.6]. This can be used to explicitly encode the formulas of $\mathcal{L}(\text{ring}, \tilde{K}, e)$ in $\mathbb{N}$ such that 1 is not a code of a formula.

Let A_n (resp. E_n) denote the set of sentences $\vartheta \in \mathcal{L}(\text{ring}, \tilde{K}, e)$ in *prenex form* (i.e., consisting of a string of quantifier variables followed by a quantifier-free formula) whose intial quantifier string is of the form $(\forall x)(\exists y) \cdots$ (resp. $(\exists \mathbf{x})(\forall \mathbf{y}) \cdots$) and is of length n (that is, there are n distinct blocks of quantifiers). Denote by Truth(A_n) (resp. Truth(E_n)) the collection of all sets Truth(ϑ) with $\vartheta \in A_n$ (resp. $\vartheta \in E_n$). Then the equalities

$$\text{Truth}((Q\mathbf{x})\varphi(\mathbf{x})) \cup \text{Truth}((Q\mathbf{y})\psi(\mathbf{y})) = \text{Truth}((Q\mathbf{x}, \mathbf{y})\varphi(\mathbf{x}) \vee \psi(\mathbf{y})),$$

$$\text{Truth}((Q\mathbf{x})\varphi(\mathbf{x})) \cap \text{Truth}((Q\mathbf{y})\psi(\mathbf{y})) = \text{Truth}((Q\mathbf{x}, \mathbf{y})\varphi(\mathbf{x}) \wedge \psi(\mathbf{y}))$$

(where Q is either $\exists$ of $\forall$ $\varphi(\mathbf{x})$ (resp. $\psi(\mathbf{y})$) is a formula in $\mathcal{L}(\text{Ring}, \tilde{K}, e)$ whose free variables are among the x_i's (resp, y_i's); the x_i's do not occur in $\psi(\mathbf{y})$ and the y_j's do not occur in $\varphi(\mathbf{x})$), imply that Truth(A_n) and Truth(E_n) are closed under finite unions and intersections.

Definition. For $n \geq 0$, the collection $\mathrm{Truth}(A_n)$ (resp. $\mathrm{Truth}(E_n)$) is *encoded* by a function f from $\mathbb{N}$ onto $\mathrm{Truth}(A_n)$ (resp. $\mathrm{Truth}(E_n)$) and functions $g_1, g_2 : \mathbb{N}^2 \to \mathbb{N}$ if

(1a) $f(\mathrm{code}(\vartheta)) = \mathrm{Truth}(\vartheta)$, for every $\vartheta \in A_n$ (resp. $\vartheta \in E_n$);

(1b) $f(g_1(k, m)) = f(k) \cup f(m)$ and $f(g_2(k, m)) = f(k) \cap f(m)$, for all $k, m \in \mathbb{N}$; and

(1c) g_1, g_2 and the ternary relation on $\mathbb{N}$ defined by $\mu(f(k)) > a/b$ are definable.

Lemma 5.1. $\mathrm{Truth}(E_0)$ *is an encoded collections of subsets of* $G(K)^e$.

Proof. In each sentence $\vartheta \in E_0$ there are only finitely many elements $x_1, \ldots, x_n$ involved. Let L be a finite normal extension of K that contains $x_1, \ldots, x_n$ and denote by L_0 the maximal separable extension of K in L. The number c of e-tuples $\boldsymbol{\tau} \in \mathcal{G}(L_0/K)^e$ such that $\langle L, \boldsymbol{\tau} \rangle \models \vartheta$ can be effectively computed [6, Lemma 2.5] and $\mathrm{Prob}(\vartheta) = c/[L_0 : K]^e$. In particular the function $\mathrm{code}(\vartheta) \mapsto \mathrm{Prob}(\vartheta)$ is recursive. Write $\mathrm{Prob}(\vartheta)$ as $a(\vartheta)/b(\vartheta)$, where $a(\vartheta) = 0$ and $b(\vartheta) = 1$, or $a(\vartheta)$ and $b(\vartheta)$ are relatively prime positive integers.

Define now $f(\mathrm{code}(\vartheta)) = \mathrm{Truth}(\vartheta)$ for $\vartheta \in E_0$ and $f(m) = 0$ for $m \in \mathbb{N} - \mathrm{Truth}(E_0)$. Let also $g_1(\mathrm{code}(\eta), \mathrm{code}(\vartheta)) = \mathrm{code}(\eta \vee \vartheta)$, $g_1(k, \mathrm{code}(\vartheta)) = \mathrm{code}(\vartheta)$, $g_1(\mathrm{code}(\eta), m) = \mathrm{code}(\eta)$ and $g_1(k, m) = 1$, for $\eta, \vartheta \in E_0$ and $k, m \in \mathbb{N}$-$\mathrm{Truth}(E_0)$. Finally let $g_2(\mathrm{code}(\eta), \mathrm{code}(\vartheta)) = \mathrm{code}(\eta \wedge \vartheta)$, for $\eta, \vartheta \in E_0$ and $g_2(k, m) = 1$ if k or m belong to $\mathbb{N} - \mathrm{Truth}(E_0)$. Then (1b) is satisfied. Also, g_1, g_2 and the ternary relation "$\mu(f(k)) > \alpha/b$" are recursive, hence definable. Thus f, g_1 and g_2 encode $\mathrm{Truth}(E_0)$. □

Lemma 5.2. *Suppose that the functions* f, g_1 *and* g_2 *encode* $\mathrm{Truth}(A_n)$. *Then we can define functions* f', g_1' *and* g_2' *that encode* $\mathrm{Truth}(E_{n+1})$.

Proof. Denote by $\tilde{K}^{<\omega}$ the set of all finite sequences of elements of $\tilde{K}$ and define a map $h_0 : E_{n+1} \times \tilde{K}^{<\omega} \to A_n$ by

$$h_0(\text{“}(\exists \mathbf{x})\varphi(\mathbf{x})\text{”}, \mathbf{a}) = \begin{cases} \varphi(\mathbf{a}) & \text{if } \mathbf{x} \text{ and } \mathbf{a} \text{ are of equal length,} \\ \text{“false”} & \text{otherwise,} \end{cases}$$

where "false" is some fixed false sentence in A_n. Use $i : \tilde{K} \to \mathbb{N}$ to encode $\tilde{K}^{<\omega}$ in $\mathbb{N}$ by a function $i_* : \tilde{K}^{<\omega} \to \mathbb{N}$; e.g., $i_*(x_1, \ldots, x_n) = p_1^{i(x_1)} \cdots p_n^{i(x_n)}$, where $p_1, \ldots, p_n$ are the first n primes. Define an 'inverse' function $i_*^{-1} : \mathbb{N} \to \tilde{K}^{<\omega}$ by $i_*^{-1}(m) = \mathbf{a}$ if $i(\mathbf{a}) = m$ and $i_*^{-1}(m) = 1$ if $m \notin i(\tilde{K}^{<\omega})$ and let $h : \mathbb{N} \times \mathbb{N} \to A_n$ be the function defined by

$$h(k, m) = \begin{cases} f(\mathrm{code}(h_0(\text{“}(\exists \mathbf{x})\varphi(\mathbf{x})\text{”}, i_*^{-1}(m)))) \\ \qquad \text{if } k = \mathrm{code}(\text{“}(\exists \mathbf{x})\varphi(\mathbf{x})\text{”}) \text{ and } \text{“}\varphi(\mathbf{x})\text{”} \in A_n, \\ \emptyset \quad \text{if } k \notin \mathrm{code}(E_{n+1}). \end{cases}$$

Then define f' on $\mathbb{N}$ by

$$f'(k) = \bigcup_{m=1}^{\infty} h(k, m). \tag{2}$$

if $k \notin \text{code}(E_{n+1})$, then $f'(k) = \emptyset$. On the other hand, if $k = \text{code}(\vartheta)$, $\vartheta = $ "$(\exists \mathbf{x})\varphi(\mathbf{x})$", "$\varphi(\mathbf{x})$" $\in A_n$ and $\mathbf{x} = (x_1, \ldots, x_r)$, then

$$\begin{aligned} f'(k) &= \bigcup_{m=1}^{\infty} f(\text{code}(h_0(\vartheta, i_*^{-1}(m)))) \\ &= f(\text{code}(h_0(\vartheta, 1))) \cup f(\text{code}(\text{"false"})) \cup \bigcup_{\mathbf{a} \in \tilde{K}^r} f(\text{code}(\varphi(\mathbf{a}))) \\ &= \bigcup_{\mathbf{a} \in \tilde{K}^r} \text{Truth}(\varphi(\mathbf{a})) = \text{Truth}(\text{"}(\exists \mathbf{x})\varphi(\mathbf{x})\text{"}). \end{aligned}$$

Thus f' maps $\mathbb{N}$ onto $\text{Truth}(E_{n+1})$ and satisfies $f'(\text{code}(\vartheta)) = \text{Truth}(\vartheta)$ for each $\vartheta \in E_{n+1}$.

Next it is possible to define in $\mathcal{N}$ a function $g_1 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that if $\zeta = $ "$(\exists \mathbf{x})\varphi(\mathbf{x})$" and $\eta = $ "$(\exists \mathbf{y})\psi(\mathbf{y})$" are two sentences in E_{n+1}, then $g_1(\text{code}(\zeta), \text{code}(\eta)) = \text{code}(\vartheta)$, where $\vartheta = $ "$(\exists \mathbf{x}', \mathbf{y}')\varphi(\mathbf{x}') \vee \psi(\mathbf{y}')$" and $\mathbf{x}'$, $\mathbf{y}'$ are strings of variables (belonging to $\{x_1, x_2, x_3, \ldots\}$) that do not occur in $\zeta \vee \eta$, of the same length as $\mathbf{x}$, $\mathbf{y}$ respectively. Then

$$\begin{aligned} f'(g_1(\text{code}(\zeta), \text{code}(\eta))) &= f'(\text{code}(\vartheta)) = \text{Truth}(\vartheta) \\ &= \text{Thruth}(\zeta) \cup \text{Truth}(\eta) = f'(\text{code}(\zeta)) \cup f'(\text{code}(\eta)). \end{aligned}$$

If $m \notin \text{code}(E_{n+1})$ define $g_1(\text{code}(\zeta), m) = \text{code}(\zeta)$; if $k \notin \text{code}(E_{n+1})$ define $g_1(k, \text{code}(\eta)) = \text{code}(\eta)$ and if $k, m \notin \text{code}(E_{n+1})$ define $g_1(k, m) = 1$. In all cases $f'(g_1(k, m)) = f'(k) \cup f'(m)$.

Dualize now this definition to obtain a definable function $g_2 : N \times \mathbb{N} \to \mathbb{N}$ such that $f'(g_2(k, m)) = f'(k) \cap f'(m)$.

It remains to prove that the ternary relation on $\mathbb{N}$ given by "$\mu(f'(k)) > a/b$" is definable. Indeed, there is a function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ which is inductively defined from g_1, and hence is arithmetically definable such that $f(g(k, m)) = \bigcup_{j=1}^{m} h(k, j)$. Then, the relation $R(k, m, a, b)$ which expresses

$$\mu(f(g(k, m))) > a/b$$

is arithmetically definable.

If now $k = \text{code}(\vartheta)$ and $\vartheta = $ "$(\exists \mathbf{x})\varphi(\mathbf{x})$" $\in E_{n+1}$, then, by (2),

$$\mu(f'(k)) = \mu\left(\bigcup_{m=1}^{\infty} h(k, m)\right) = \lim_{m \to \infty} \mu(f(g(k, m))).$$

Therefore the relation "$\mu(f'(k)) > a/b$" is arithmetically definable. □

Theorem 5.3. *For each sentence ϑ of $\mathcal{L}(\text{ring}, \tilde{K}, e)$, $\text{Prob}(\vartheta)$ is a definable real number.*

Proof. Every sentence ϑ of $\mathscr{L}(\text{ring}, \tilde{K}, e)$ is equivalent to a sentence in prenex form, and hence can be considered as belonging to A_n or E_n, for some $n \geqslant 0$. Use induction on n to prove that Truth(A_n) and Truth(E_n) are encoded collections of subsets of $G(K)^e$. Note since $A_0 = E_0$, the case $n = 0$ is covered by Lemma 5.1. The transition from A_n to E_{n+1} is covered by Lemma 5.2 and the transition from E_n to A_{n+1}, is similar but dual.

It follows from conditions (1a) and (1c) in the definition of 'encoded' that for each sentence ϑ, the binary relation on $\mathbb{N}$ given by "Prob$(\vartheta) > a/b$" is definable. Hence Prob(ϑ) is definable. □

6. Presentation of definable reals as Prob(ϑ); char(K) = 0

We assume in this section that $e \geqslant 2$ and that K is a finitely generated extension of $\mathbb{Q}$.

Definition. A positive even integer m is said to be a *cyclotomic number* for K if $K \cap \mathbb{Q}_{ab} \subseteq \mathbb{Q}(\zeta_m)$. Here Q_{ab} is the maximal abelian extension of $\mathbb{Q}$ and ζ_m denotes a primitive mth root of 1.

If K is explicitly given, then $K \cap \tilde{\mathbb{Q}}$ and therefore also $K \cap \mathbb{Q}_{ab}$ can be explicitly computed [6, Lemma 2.7]. By the Kronecker–Weber theorem [19, p. 210] there exists an even m such that $K \cap \mathbb{Q}_{ab} \subseteq \mathbb{Q}(\zeta_m)$. So m can be recursively computed by checking the last inclusion successively for $m = 2, 4, 6, 8, \ldots$.

The degree of cyclotomic extensions of finitely generated extensions of $\mathbb{Q}$ can be expressed with *Euler's totient function*, $\varphi(n)$. This is the number of positive integers less than n which are relatively prime to n. It is well known that

$$\varphi(n) = n \prod_{l \mid n} \left(1 - \frac{1}{l}\right) \tag{1}$$

(here and throughout the rest of this section we reserve the letter l to range over the primes). In particular φ is multiplicative, i.e. $\varphi(mn) = \varphi(m)\varphi(n)$ for m and n relative primes; $\varphi(l) = l - 1$; and $\varphi(nl) = \varphi(n)l$ if $l \mid n$. For arbitrary $m, n \in \mathbb{N}$, we write $\mathbf{d} = \gcd(m, n)$ and $\mathbf{k} = \text{lcm}(m, n)$, use $mn = dk$ and (1) and find that $\varphi(m)\varphi(n) = \varphi(d)\varphi(k)$. Now, it is well known that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ [19, p. 47]. Thus, using $\mathbb{Q}(\zeta_k) = \mathbb{Q}(\zeta_m, \zeta_n)$, we have

$$[\mathbb{Q}(\zeta_k) : \mathbb{Q}(\zeta_d)] = \frac{\varphi(k)}{\varphi(d)} = \frac{\varphi(m)}{\varphi(d)} \cdot \frac{\varphi(n)}{\varphi(d)} = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_d)][\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_d)].$$

It follows that $\mathbb{Q}(\zeta_m)$ is linearly disjoint from $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}(\zeta_d)$. This will be useful below.

Lemma 6.1. *If m is a cyclotomic number for K, then*

(a) $|U(K(\zeta_m))| = m$;

(b) $[K(\zeta_k):K(\zeta_m)] = \varphi(k)/\varphi(m)$, *for every multiple k of m*;

(c) *if $\gcd(m, n) = d$ and $\zeta_d \in K$, then $K(\zeta_m)$ is linearly disjoint from $K(\zeta_n)$ over K; and*

(d) *if F is an extension of K and $n = |U(F)|$ is finite, then*

$$|U(K(\zeta_m) \cap F)| = \gcd(m, n).$$

Proof. The field $K(\xi_m)$ is linearly disjoint from $\mathbb{Q}_{ab}$ over $\mathbb{Q}(\zeta_m)$. Hence $U(K(\zeta_m)) = U(\mathbb{Q}(\zeta_m))$. Since m is even, the last group has order m. This proves (a).

For (b), the above mentioned linear disjointness gives

$$[K(\zeta_k):K(\zeta_m)] = [\mathbb{Q}(\zeta_k):\mathbb{Q}(\zeta_m)] = \varphi(k)/\varphi(m).$$

Now we prove (c). Let $K_0 = \mathbb{Q}_{ab} \cap K$. Since $\mathbb{Q}(\zeta_m)$ is linearly disjoint from $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_d)$ and $\mathbb{Q}(\zeta_d) \subseteq K_0 \subseteq \mathbb{Q}(\zeta_m)$, the fields $k_0(\zeta_m)$ and $K_0(\zeta_n)$ are linearly disjoint over K_0. Also, K is linearly disjoint from $K_0(\zeta_r)$ for every positive integer r. Let $k = \operatorname{lcm}(m, n)$. Then $K(\zeta_k) = K(\zeta_m)K(\zeta_n)$ and $K_0(\zeta_k) = K_0(\zeta_m)K_0(\zeta_n)$. Hence

$$[K(\zeta_k):K] = [K_0(\zeta_k):K_0] = [K_0(\zeta_m):K_0][K_0(\zeta_n):K_0] = [K(\zeta_m)K][K(\zeta_n):K].$$

It follows that $K(\zeta_m)$ is linearly disjoint from $K(\zeta_n)$ over K.

Finally we prove (d). Since $U(K(\zeta_m) \cap F)$ is a subgroup of both $U(K(\zeta_m))$ and $U(F)$, its order, d, divides m (by (a)) and n. On the other hand, since $\zeta_n \in U(F)$, we have $\zeta_{\gcd(m,n)} \in K(\zeta_m) \cap F$. Hence $\gcd(m, n) \mid d$. It follows that $\gcd(m, n) = d$. □

Fix a cyclotomic number m for K and let $M = K(\zeta_m)$. For each divisor d of m let

$$\Gamma(d) = \{\tau \in \mathcal{G}(M/K)^e \mid |U(M(\tau))| = d\}$$

($M(\tau)$ is the fixed field of τ in M). For each positive integer n let

$$P(n) = \{\sigma \in G(K)^e \mid |U(\tilde{K}(\sigma))| = n\}.$$

Lemma 6.2. *For $d = \gcd(m, n)$ and $k = \operatorname{lcm}(m, n)$ we have*

$$\mu(P(n)) = \frac{|\Gamma(d)|}{[M:K]^e} \frac{\varphi(m)^e}{\varphi(k)^e} \prod_{\substack{l \nmid m/d \\ l \mid n}} \left(1 - \frac{1}{l^e}\right) \prod_{\substack{l \nmid m/d \\ l \nmid n}} \left(1 - \frac{1}{(l-1)^e}\right), \tag{2}$$

Proof. For each $\tau \in \Gamma(d)$ let $p(n, \tau) = \{\sigma \in P(n) \mid \operatorname{res}_M \sigma = \tau\}$. By Lemma 6.1(d); $P(n)$ is the disjoint union of all $p(n, \tau)$ with $\tau \in \Gamma(d)$. Hence, it suffices to prove

for each $\tau \in \Gamma(d)$ that

$$\mu(P(n,\tau)) = \frac{1}{[M:K]^e}\frac{\varphi(m)^e}{\varphi(k)^e}\prod_{\substack{l \nmid m/d \\ l \mid n}}\left(1-\frac{1}{l^e}\right)\prod_{\substack{l \nmid m/d \\ l \nmid n}}\left(1-\frac{1}{(l-1)^e}\right), \tag{3}$$

Indeed let $E = M(\tau)$, $N = E(\zeta_n)$ and

$$Q(n, N, l) = \{\sigma \in G(N)^e \mid N(\zeta_{nl}) \notin \tilde{K}(\sigma)\}.$$

Notice that since m is also a cyclotonic number for E, Lemma 6.1(c) implies that $M \cap N = E$. We divide the rest of the proof into parts.

Part A: *A representation of* $P(n, \tau)$. We claim that

$$P(n,\tau) = \{\sigma \in G(N)^e \mid \mathrm{res}_M \sigma = \tau\} \cap \bigcap_{l \nmid m/d} Q(n, N, l) \tag{4}$$

Indeed, if $\sigma \in P(n, \tau)$, then $U(\tilde{K}(\sigma))$ is a cyclic group of order n and therefore contains ζ_n but no ζ_{nl}. It follows that σ belongs to $Q(n, N, l)$ for every prime l. Conversely, suppose that σ belongs to the right hand side of (4). Then n divides $|U(\tilde{K}(\sigma))|$. If $|U(\tilde{K}(\sigma))| > n$, then there exists a prime l which divides m/d such that $N(\zeta_{nl}) \subseteq \tilde{K}(\sigma)$. But, since $dl = \gcd(m, nl)$, we have $E \cap E(\zeta_{dl}) \subseteq M \cap \tilde{K}(\sigma)$, a contradiction. Thus σ also belongs to $P(n, \tau)$.

Part B: *Independence of the intersectands at* (4). If l does not divide m/d, then $\gcd(m, nl) = d$. Hence, by Lemma 6.1(c), $M \cap N(\zeta_{nl}) = M \cap E(\zeta_{nl}) = E$. It follows that $N(\zeta_{nl})$ is linearly disjoint from $K(\zeta_k)$ over N, and $kl = \mathrm{lcm}(m, nl)$. Continue by induction and prove in this way for distinct primes $l_1, \ldots, l_T$ which do not divide m/d, that $N(\zeta_{nl_1 \cdots l_r})$ is linearly disjoint from M over E. Therefore the collection of fields $N(\zeta_{nl})$ for $l \nmid m/d$ and the field $K(\zeta_k)$ are linearly disjoint over N. This implies that the intersectands on the right hand side of (4) are independent in the probability space $G(N)^e$ [12, Lemma 4.1].

Part C: *Computation of measures.* Denote by μ_N the normalized Haar measure of $G(N)^e$. If $l \nmid m/d$ and $l \mid n$, then, by Part B, and by Lemma 6.1(b)

$$[N(\zeta_{nl}):N] = [K(\zeta_{kl}):K(\zeta_k)] = \varphi(kl)/\varphi(k) = l.$$

Hence,

$$\mu_N(Q(n, N, l)) = 1 - [N(\zeta_{nl}):N]^{-e} = 1 - l^{-e}.$$

If $l \nmid m/d$ and $l \nmid n$, then $l \nmid k$. Hence, as above, $[N(\zeta_{nl}):N] = \varphi(kl)/\varphi(k) = l - 1$. Therefore $\mu_N(Q(n, N, l)) = 1 - (l-1)^{-e}$. It follows from (4) and from Part B that

$$\mu_N(P(n,\tau)) = \frac{1}{[M:E]^e}\prod_{\substack{l \nmid m/d \\ l \mid n}}\left(1-\frac{1}{l^e}\right)\prod_{\substack{l \nmid m/d \\ l \nmid n}}\left(1-\frac{1}{(l-1)^e}\right). \tag{5}$$

On the other hand Lemma 6.1(b) gives

$$\mu(P(n,\tau)) = \frac{1}{[N:K]^e}\mu_N(P(n,\tau)) = \frac{1}{[E:K]^e}\frac{\varphi(m)^e}{\varphi(k)^e}\mu_N(P(n,\tau)) \tag{6}$$

The combination of (5) and (6) gives (3). □

Remark 6.3. If $p > mn$ is a prime, then, in the notation of Lemma 6.2, $K(\zeta_p)$ is linearly disjoint from MN. For each $\lambda \in \mathcal{G}(K(\zeta_p)/K)$ let

$$S(\lambda) = \{\sigma \in G(K)^e \mid \mathrm{res}_{K(\zeta_p)}\sigma = \lambda\}.$$

If $\lambda = 1$, then, by (4), $P(n) \cap S(\lambda)$ is empty, hence $\mu(P(n) \cap S(\lambda)) = 0$. If $\lambda \neq 1$, then, to compute $\mu(P(n) \cap S(\lambda))$, replace the pth factor on the right hand side of (3) by $(p-1)^{-e}$. Thus, in this case

$$\mu(p(n) \cap S(\lambda)) = \mu(P(n))(p-1)^{-e}\left(1 - \frac{1}{(p-1)^e}\right)^{-1} < (p-1)^{-e}. \tag{7}$$

In both cases $\mu(P(n) \cap S(\lambda))$ is computable.

Since $e \geq 2$, the infinite product $\prod_l (1-(l-1)^{-e})(1-l^{-e})^{-1}$ converges. Hence there exists a positive integer c_0 such that if $c_0! \mid m$ and $p > c_0$, then for every positive integer n

$$0.9 < \frac{1-p^{-e}}{1-(p-1)^{-e}} \prod_{\substack{l \nmid m \\ l \mid n}} \frac{1-(p-1)^{-e}}{1-l^{-e}} < 1.1. \tag{8}$$

Every multiple of a cyclotomic number for K is also a cyclotomic number for K. So we may choose m such that (8) holds.

Lemma 6.4. *There exists $c > 0$ such that for every divisor d of m and for every positive integer n with $\gcd(m, n) = d$ and $\varphi(\mathrm{lcm}(m, n)) > c\varphi(m)$ there exists a positive integer n' such that $\gcd(m, n') = d$, $\varphi(\mathrm{lcm}(m, n')) > c\varphi(m)$ and $\frac{1}{2}\mu(P(n)) < \mu(P(n')) < \mu(P(n))$.*

Proof. By the prime number theorem there exists $c_1 > 0$ such that for every $x > c_1$ there exists a prime p such that

$$\sqrt[e]{1.1}x < p - 1 < \sqrt[e]{1.8}x \tag{9}$$

Take $c = \max(m, c_0, c_1)$ and let n be a positive integer such that $\varphi(k) > c\varphi(m)$, where $k = \mathrm{lcm}(m, n)$. By (9) there exists a prime p such that

$$\sqrt[e]{1.1}\frac{\varphi(k)}{\varphi(m)} < p - 1 < \sqrt[e]{1.8}\frac{\varphi(k)}{\varphi(m)}. \tag{10}$$

In particular $p > c_0, m$. Take $n' = dp$. Then $\gcd(m, n') = d$ and $k' = \mathrm{lcm}(m, n') = mp$. Hence $\varphi(k') = \varphi(m)(p-1) > \varphi(k) > c\varphi(m)$. Now combine (8) with (10):

$$\frac{1}{2} < \frac{\varphi(k)^e}{\varphi(m)^e(p-1)^e}\frac{1-p^{-e}}{1-(p-1)^{-e}} \prod_{\substack{l \nmid m \\ l \mid n}} \frac{1-(l-1)^{-e}}{1-l^{-e}} < 1. \tag{11}$$

Compute from (2) that $(P(n'))/\mu(P(n))$ is equal to the middle term of (11), to conclude the proof. □

Theorem 6.5. *Let K be a finitely generated extension of $\mathbb{Q}$ and let $e \geqslant 2$. Then for every definable real number r between 0 and 1 there exists a sentence ϑ of $\mathcal{L}(\text{ring}, K, e)$ such that* $\text{Prob}(\vartheta) = r$.

Proof. In the notation of the preceding Lemma 6.2 let $A = \{n \in \mathbb{N} \mid \Gamma(\gcd(m, n)) \neq \emptyset\}$. Since the membership of n in A depends only on $\gcd(m, n)$, the set A is recursive. By Lemma 6.2, $\mu(P(n)) \neq 0$ if and only if $n \in A$. Since for almost all $\boldsymbol{\sigma} \in G(K)^e$, $U(\tilde{K}(\boldsymbol{\sigma}))$ is finite (Proposition 1.1), this implies that $\sum_{n \in A} \mu(P(n)) = 1$. We divide the rest of the proof into two parts.

Part A: *A presentation of r as a sum of measures.* In the notation of Lemma 6.4 let $B = \{n \in A \mid \varphi(\text{lcm}(m, n)) > c\varphi(m)\}$. Since $\lim_{k \to \infty} \varphi(k) = \infty$ [21, p. 114], B is a recursive cofinite subset of A. Choose a prime p greater than m and every $n \in A - B$ such that $(p-1)^{-e} < \max_{n \in B} \mu(P(n))$. For $(n, \boldsymbol{\lambda}) \in (A - B) \times \mathcal{G}(K(\zeta_p)/K)^e = T$ define $q_{n,\lambda} = \mu(P(n) \cap S(\boldsymbol{\lambda}))$, and for $n \in B$ define $q_n = \mu(P(n))$. By Lemma 6.2 and Remark 6.3, $q : T \cup B \to \mathbb{R}$ is a definable function and $\sum_{x \in T \cup B} q_x = 1$. Inequality (7) implies (4b) of Section 4, and Lemma 6.4 implies (4c) of Section 4. Conclude from Lemma 4.2 that for each definable real $0 < r \leqslant 1$ there exist distinct $(n_1, \boldsymbol{\lambda}_1), \ldots, (n_k, \boldsymbol{\lambda}_k) \in T$ and there exists a definable subset B_0 of B such that

$$\sum_{i=1}^{k} \mu(P(n_i) \cap S(\boldsymbol{\lambda}_i)) + \sum_{n \in B_0} \mu(P(n)) = r. \tag{12}$$

Part B: *Representation of the left hand side of* (12) *as* $\text{Prob}(\vartheta)$. For $i = 1, \ldots, k+1$ let $\psi_i(x)$ be the formula $x = n_i$, and let $\psi_{k+1}(x)$ be a formula of arithmetic such that $\mathcal{N} \models \psi_{k+1}(x)$ if and only if $n \in B_0$. For $i = 1, \ldots, k+1$ there exists a sentence ϑ_i of $\mathcal{L}(\text{ring}, K, e)$ such that for almost all $\boldsymbol{\sigma} \in G(K)^e$, the truth of ϑ_i in $\langle \tilde{K}, \boldsymbol{\sigma} \rangle$ is equivalent to the truth of $\psi_i(|U(\tilde{K}(\boldsymbol{\sigma}))|)$ in $\langle \tilde{K}, \boldsymbol{\sigma} \rangle$ (Theorem 3.1).

For each $\boldsymbol{\lambda} \in \mathcal{G}(K(\zeta_p)/K)^e$ let $\boldsymbol{\lambda}(\zeta_p) = (\zeta_p^{c(\lambda_1)}, \ldots, \zeta_p^{c(\lambda_e)})$, with integers $c(\lambda_1), \ldots, c(\lambda_e)$ between 1 and $p-1$. Let $\vartheta_{\boldsymbol{\lambda}}$ be the following sentence of $\mathcal{L}(\text{ring}, K, e)$

$$(\exists z)\left[z^p = 1 \wedge z \neq 1 \wedge \bigwedge_{i=1}^{e} \sigma_i z = z^{c(\lambda_i)}\right].$$

Then $\langle \tilde{K}, \boldsymbol{\sigma} \rangle \models \vartheta_{\boldsymbol{\lambda}}$ if and only if $\text{res}_{K(\zeta_p)} \boldsymbol{\sigma} = \boldsymbol{\lambda}$. The desired sentence ϑ of $\mathcal{L}(\text{ring}, K, e)$ can now be taken as

$$\bigvee_{i=1}^{k} (\vartheta_i \wedge \vartheta_{\lambda_i}) \vee \vartheta_{k+1}.$$

The measure of ϑ is equal to the left hand side of (12), hence to r. □

Corollary 6.6. *Let K be a finitely generated extension of $\mathbb{Q}$ and let $e \geqslant 2$. Then there exists sentences ϑ of $\mathcal{L}(\text{ring}, K, e)$ such that* $\text{Prob}(\vartheta)$ *are transcendental numbers.*

Proof. The number π^{-1} is a definable transcendental number between 0 and 1.

Example 6.7. For $K = \mathbb{Q}$, take ϑ to be the sentence

$$(\forall z)\left[\left[\bigwedge_{i=1}^{e} \Sigma_i z = z \wedge (\exists a)[a \neq 0 \wedge \Sigma_1 z = za]\right] \rightarrow z = 1 \vee z = -1\right].$$

By Proposition 1.1(d), ϑ is an interpretation of the statement "$|U(\tilde{\mathbb{Q}}(\sigma))| = 2$". Compute from (2) that

$$\mathrm{Prob}(\vartheta) = \prod \left(1 - \frac{1}{(l-1)^e}\right) \tag{13}$$

However, it seems to be unknown if the right hand side of (13) is transcendental.

Problem 6.8. Fina a concrete example of a sentence ϑ in $L(\mathrm{ring}, \mathbb{Q}, 2)$ such that $\mathrm{Prob}(\vartheta)$ is transcendental.

7. Presentation of definable reals as Prob(ϑ); char(K) = p

Throughout this section K denotes an infinite finitely generated extension of $\mathbb{F}_p$, and $e \geqslant 2$. Then $\tilde{\mathbb{F}}_p \cap K = \mathbb{F}_q$, where q is a power of p. For each positive integer n denote by $K_n = \mathbb{F}_{q^n}K$ the unique cyclic constant field extension of degree n. As for the characteristic 0 case we first compute the measure of the sets

$$P(m) = \{\sigma \in G(K)^e \mid |U(\tilde{K}(\sigma))| = m\}.$$

Lemma 7.1. *For each positive integer n, $\mu(P(q^n - 1)) = n^{-e}\zeta(e)^{-1}$, where ζ is the Riemann zeta function. If $m + 1$ is not a power of q, then $\mu(P(m)) = 0$.*

Proof. For each field E containing K, $U(E) = (\tilde{\mathbb{F}}_p \cap E)^\times$, a cyclic group of order $q^n - 1$, for some $n \geqslant 1$, or an infinite group. Thus, if m is not of the form $q^n - 1$, then $\mu(P(m)) = 0$.

For the first assertion note that

$$P(q^n - 1) = \{\sigma \in G(K_n) \mid K_{nl} \not\subseteq \tilde{K}(\sigma) \text{ for every prime } l\} \tag{1}$$

Since the fields K_{nl}, as l ranges over the primes, are linearly disjoint over K_n,

$$\mu(P(q^n - 1)) = n^{-e} \prod_l \left(1 - \frac{1}{l^e}\right) = n^{-e}\zeta(e)^{-1}. \quad \square \tag{2}$$

Theorem 7.2. *For every definable real number r between 0 and 1 there exists a sentence ϑ of $\mathcal{L}(\mathrm{ring}, K, e)$ such that* $\mathrm{Prob}(\vartheta) = r$.

Proof. By Proposition 1.1 and by Lemma 7.1, $\sum_{n=1}^{\infty} \mu(P(q^n - 1)) = 1$. Let

$B = \{n \in \mathbb{N} \mid n > (\sqrt[e]{2}-1)^{-1}\}$ and compute from (2) that for each $n \in B$ we have

$$\tfrac{1}{2}\mu(P(q^n-1)) < \mu(P(q^{n+1}-1)) < \mu(P(q^n-1)).$$

Choose a prime $l_0 > (1+(\sqrt[e]{2}-1)^{-1})\zeta(e)^{1/e}$ and note that if $n \leqslant (\sqrt[e]{2}-1)^{-1}$, then $n < l_0$, hence K_n is linearly disjoint from $L = K_{l_0}$ over K. For each $\lambda \in \mathcal{G}(L/K)^e$ let $S(\lambda) = \{\sigma \in G(K)^e \mid \mathrm{res}_L\, \sigma = \lambda\}$. If $\lambda = 1$, and $n \leqslant (\sqrt[e]{2}-1)^{-1}$, then $P(q^n-1) \cap S(\lambda)$ is empty (by (1)). If $\lambda \neq 1$, *then*,

$$\mu(P(q^n-1) \cap S(\lambda)) = \mu(P(q^n-1))\mu(S(\lambda)) < l_0^{-e}. \tag{3}$$

Note that (2) implies that $\mu(P(q^n-1))$ is a monotonically decreasing function of n. Hence $\max_{b\in B} \mu(P(q^b-1))$ is achieved for the smallest $b \in B$. This b is less than $1+(\sqrt[e]{2}-1)^{-1}$. It follows from (2) and (3) that

$$\mu(P(q^n-1) \cap S(\lambda)) < \max_{b\in B} \mu(P(q^b-1)).$$

For $(n, \lambda) \in (\mathbb{N}-B) \times \mathcal{G}(L/K)^e = T$ define $q_{n,\lambda} = \mu(P(q^n-1) \cap S(\lambda))$ and for $n \in B$ define $q_n = \mu(p(q^{n-1}))$. By (2) and (3), $q : T \cup B \to \mathbb{R}$ is a definable function and $\sum_{x\in T\cup B} q_x = 1$. By Lemma 4.2 there exist distinct elements $(n_1, \lambda_1), \ldots, (n_k, \sigma_k) \in T$ and there exists a definable subset B_0 of B such that

$$\sum_{i=1}^{k} \mu(P(q^{n_i}-1) \cap S(\lambda_i)) + \sum_{n\in B_0} \mu(P(q^n-1)) = r. \tag{4}$$

For $i = 1, \ldots, k$ let $\psi_i(x)$ be the formula $x = q^{n_i}-1$. For $i = k+1$, let $\psi_{k+1}(x)$ be a formula of arithmetic such that $\mathcal{N} \models \psi_{k+1}(x)$ if and only if $x = q^n - 1$ and $n \in B_0$ (note that since q^n is a recursive function of n, such a formula exists). The rest of the proof follows now as in Part B of the proof of Theorem 6.5 (replace p by l_0, ζ_p by ζ_r with $r = q^{l_0}-1$ and $K(\zeta_p)$ by L). □

Example 7.3. For $K = \mathbb{F}_p(t)$, where t is transcendental over $\mathbb{F}_p$, take ϑ as the interpretation in $\mathcal{L}(\mathrm{ring}, K, e)$ of the statement "$|(U(\tilde{K}(\sigma)))| = p-1$". Then $\mu(S(\vartheta)) = \prod(1-l^{-e}) = \zeta(e)^{-1}$. In particular for $e = 2d$, even numbers,

$$\zeta(e) = (-1)^{d-1}\frac{(2\pi)^e}{2(e!)}B_e,$$

[2, p. 387], where B_e is the e-th Bernoulli number. Since B_e is rational [2, p. 382], $\zeta(e)$ is transcendental.

8. More undecidability results

In this section we sketch more undecidability results over PAC fields over finite fields that can be proved by the methods developed so far or by a slight modification of them.

Proposition 8.1. *Let $\mathcal{F}$ be a class consisting of one weak monadic structure*

$\langle F, \mathcal{Q}\rangle$, where F ia a PAC *field of characteristic p which is not separably closed. Suppose that*

(1) *For every $n \geq 1$ there exists $A \in \mathcal{Q}$ with $|A| \geq n$.*

Then Th($\mathcal{N}$) *is interpretable in* Th($\mathcal{F}$).

Proof. Let $\hat{F}$ be a nontrivial Galois extension of F of minimal degree. By Sylow's theorem $\hat{F}$ contains an extension of F' of F such that $\hat{F}/F'$ is a cyclic extension of a prime degree l. If $l \neq p$, then $F(\zeta_l)/F$ is a Galois extension of degree $\leq l-1 < [\hat{F}:F]$. By the minimality of $\hat{F}$, $\zeta_l \in F$. Use Kummer theory to find a primitive element c for $\hat{F}/F'$ such that $c^l \in F'$. So, hypotheses $H(p, l)$ (Section 2) holds in F'. If $p = l$, then, by the Artin–Schreier theory, hypotheses $H(p, l)$ holds in F'. By a lemma of Ax [1, p. 268], F' is PAC. Therefore, by Proposition 2.4, Th($\mathcal{N}$) is interpretable in Th($\mathcal{F}'$). It is now routine to interpret Th($\mathcal{F}'$) in Th($\mathcal{F}$). So Th($\mathcal{N}$) is interpretable in Th($\mathcal{F}$). □

Example 8.2. Let F be an infinite algebraic extension of a finite field and let $\mathcal{Q}$ be the collection of all finite subfields of F. By the Lang–Weil theorem [20], F is PAC. Hence arithmetic can be interpreted in Th($\langle F, \mathcal{Q}\rangle$).

Remark. It can be shown that if $\mathcal{Q}$ contains infinite sets but the A's in (1) are finite, then Th($\mathcal{F}$) is undecidable.

For the next result suppose that K is a finite field but otherwise retain the convention of Section 3.

Theorem 8.3. *For a finite field K and for $e \geq 2$ the theory $T(K, e)$ is undecidable.*

Proof. Here we need to replace Proposition 1.1 by the following result [13, Lemmas 7.1 and 7.2]: For almost all $(\sigma_1, \ldots, \sigma_e) \in G(K)^e$

(1a) $\tilde{K}(\sigma_1)$ is an infinite field, hence a PAC field (Example 8.2);

(1b) for every positive integer n, $\tilde{K}(\sigma_1)$ has a cyclic extension of degree n; and

(1c) $\tilde{K}(\boldsymbol{\sigma})$ is a finite field.

We also need the simple observation:

(2) For every positive integer n, the measure of the set of $\boldsymbol{\sigma} \in G(K)^e$ such that $|\tilde{K}(\boldsymbol{\sigma})| \geq n$ is positive.

As in the proof of theorem 3.1 let S the intersection of the sets Truth(ϑ), where ϑ ranges over $T(K, e)$ and the set of $\boldsymbol{\sigma} \in G(K)^e$ satisfying (1). To each $\boldsymbol{\sigma} \in S$ associate the monadic structure $\langle \tilde{K}(\sigma_1), \{\tilde{K}(\boldsymbol{\sigma})\}\rangle$ and let $\mathcal{F}$ be the class of all these structures. By Proposition 2.3, Th($\mathcal{F}$) is undecidable. Now interpret Th($\mathcal{F}$) in $T(K, e)$ in the obvious way and conclude that $T(K, e)$ is an undecidable theory. □

The following result settles a point raised by Macintyre.

Theorem 8.4. *For a prime p, let $\mathcal{Q}$ be the collection of all finite subfields of $\tilde{\mathbb{F}}_p$. Then* Th($\mathcal{N}$) *is interpretable in the theory of the monadic structure* $\langle \tilde{\mathbb{F}}_p, \mathcal{Q} \rangle$.

Proof. Note that although $\tilde{\mathbb{F}}_p$ is a PAC field it does not satisfy hypotheses $H(p, q)$. So, we can not apply Proposition 2.3 directly. On the other hand each of the finite fields satisfies hypotheses $H(p, 2)$, but it is not PAC. Nevertheless, it is always possible to solve a given system of equations in a larger finite field. Thus we are able to modify the proof of Proposition 2.4.

We make this idea explicit for the first step, the analogue of Lemma 2.1. First let $q = 2$ if $p \neq 2$ and $q = 3$ if $p = 2$. Then each $E \in \mathcal{Q}$ satisfies hypotheses $H(p, q)$, except in the case $p = 2$, where we have to assume that $\zeta_3 \in E$. For $E, F \in \mathcal{Q}$ such that $E \subseteq F$ and for $u \in F$ let

$$D(E, F, u) = \{a \in E \mid (\exists y \in F)[y \neq 0 \text{ and } a + u = y^q]\},$$

and let $\mathcal{Q}'$ be the collection of all $D(E, F, u)$'s. We prove that $\mathcal{Q}'$ consists of all finite subsets of $\tilde{\mathbb{F}}_p$.

Indeed, for a finite subset X of $\tilde{\mathbb{F}}_p$ let E be a finite field that contains X (and ζ_3 if $p = 2$). Choose an element $c \in E^\times - (E^\times)^q$. The system of equations $a + u = y_a^q$ for $a \in X$ and $a + u = cy_a^q$ for $a \in A - X$ is absolutely irreducible (Proposition 1.7). By the Lang–Weil theorem these equations have a solution with $y_a \neq 0$ for all $a \in A$ in each finite field F which is sufficiently large. If an addition F is an odd extension of E (resp. of degree prime to 3, if $p = 2$), then $c \in F^\times - (F^\times)^q$. It follows that $X = D(E, F, u)$.

To interpret Th($\langle \tilde{\mathbb{F}}_p, \mathcal{Q} \rangle$) in Th($\langle \tilde{\mathbb{F}}_p, \mathcal{Q} \rangle$) replace $a \in X$ by

$$u_X \in F_X \wedge E_X \subseteq F_X \wedge (\exists y_X)[y_X \neq 0 \wedge y_X \in F_X \wedge a + u_X = y_X^q],$$

and $\exists X$ by $(\exists E_X)(\exists F_X)(\exists u_X)$.

Finally, to interpret Th($\mathcal{N}$) in Th($\langle \tilde{\mathbb{F}}_p, \mathcal{Q}' \rangle$) repeat the proof of Lemma 2.2. Again, if $A_1, \ldots, A_m$ are subsets of a finite subfield E of $\tilde{\mathbb{F}}_p$, solve the system of inequalities $\sum_{i=1}^m (x_i - x_i')c_i = 0$, where $\mathbf{x} \neq \mathbf{x}'$ range over $A_1 \times \cdots \times A_m$, in an appropriate finite extension F of E. Then proceed as in Proposition 2.4. □

Remark 8.5 (Macintrye)**.** The same method shows the theory of pairs $\langle F, E \rangle$ of finite field $E \subseteq F$ (resp. $E \subseteq F \subset \tilde{\mathbb{F}}_p$) is undecidable (Follow the proof of Proposition 2.3). This stands in contrast to the decidability of the theory of all finite fields (resp. finite subfields of $\tilde{\mathbb{F}}_p$) (Ax[1, p. 264]).

References

[1] J. Ax, The elementary theory of finite fields, Ann. of Math. 88 (1968) 239–271.
[2] Z.I. Borevich and I.R. Shafarevich, Number Theory (Academic Press, New York, 1966).
[3] J.W.S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc. 41 (1969) 193–291.

[4] J.-L. Duret, Les corps faiblement algébraiquement clos non separablement clos ont la propriété d'indépendence, in: Pacholski et. al. eds., Model Theory of Algebra and Arithmetic, Lecture Notes in Math. 834 (Springer, Berlin, 1980) 136–157.
[5] Ju.L. Ershov, I.A. Lavrov, A.D. Taimanov and M.A. Taitslin, Elementary theories, Russian Math. Survey 20 (4) (1965) 35–105.
[6] M. Fried, D. Haran and M. Jarden, Galois stratification over Frobenius fields, Adv. Math. 51 (1984) 1–35.
[7] M. Fried and M. Jarden, Field Arithmetic.
[8] W.-D. Geyer and M. Jarden, Torsion points of elliptic curves over large algebraic extensions of finitely generated fields, Israel J. Math. 31 (1978) 257–297.
[9] D. Haran and M. Jarden, Bounded statements in the theory of algebraically closed fields with distinguished automorphisms, J. reine angew. Math. 337 (1982) 1–17.
[10] J.I. Igusa, Fibre Systems of Jacobian varieties (III, Fibre systems of elliptic curves), Amer. J. Math. 81 (1959) 454–475.
[11] M. Jarden, Elementary statements over large algebraic fields, Tran. AMS 164 (1972), 67–91.
[12] M. Jarden, Algebraic extensions of finite corank of Hilbertian fields, Israel J. Math. 18 (1974) 279–307.
[13] M. Jarden, Roots of unity over large algebraic fields, Math. Ann. 213 (1975) 109–127.
[14] M. Jarden, An analogue of Čebotarev density theorem for fields of finite corank, J. Math. Kyoto Univ. 20 (1980) 141–147.
[15] M. Jarden and U. Kiehne, The elementary theory of algebraic fields of finite corank, Invent. Math. 30 (1975) 275–294.
[16] S. Lang, Diophantine Geometry (Interscience, New York, 1962).
[17] S. Lang, Introduction to Algebraic Geometry (Interscience, New York, 1964).
[18] S. Lang, Algebra (Addison-Welsey, Reading, 17A, 1967).
[19] S. Lang, Algebraic Number Theory (Addison-Wesley, Reading, MA, 1970).
[20] S. Lang and A. Weil, Number of points of varieties in finite fields, Amer. J. Math. 76 (1954) 819–827.
[21] W.J. LeVeque, Topics in Number Theory I (Addison-Welsey, Reading, MA, 1958).
[22] H. Rogers, The Theory of Recursive Functions and Effective Computability (McGraw-Hill, New York, 1967).
[23] P. Roquette, Analytic Theory of Elliptic Functions over Local Fields (Vandenhoeck & Ruprecht, Göttingen, 1970).