Counting mod $n$ in pseudofinite fields

Will Johnson

December 17, 2019

Abstract

We show that in an ultraproduct of finite fields, the mod-$n$ nonstandard size of definable sets varies definably in families. Moreover, if $K$ is any pseudofinite field, then one can assign “nonstandard sizes mod $n$” to definable sets in $K$. As $n$ varies, these nonstandard sizes assemble into a definable strong Euler characteristic on $K$, taking values in the profinite completion $\hat{\mathbb{Z}}$ of the integers. The strong Euler characteristic is not canonical, but depends on the choice of a nonstandard Frobenius. When $\text{Abs}(K)$ is finite, the Euler characteristic has some funny properties for two choices of the nonstandard Frobenius.

Additionally, we show that the theory of finite fields remains decidable when first-order logic is expanded with parity quantifiers. However, the proof depends on a computational algebraic geometry statement whose proof is deferred to a later paper.

1 Introduction

1.1 Euler characteristics

Let $M$ be a structure and $R$ be a ring. Let $\text{Def}(M)$ denote the collection of (parametrically) definable sets in $M$. Recall the following definitions from [17] and [18]. An $R$-valued Euler characteristic is a function $\chi : \text{Def}(M) \to R$ such that

- $\chi(\emptyset) = 0$
- $\chi(X) = 1$ if $X$ is a singleton
• \( \chi(X) = \chi(Y) \) if \( X \) and \( Y \) are in definable bijection.
• \( \chi(X \times Y) = \chi(X) \cdot \chi(Y) \)
• \( \chi(X \cup Y) = \chi(X) + \chi(Y) \) if \( X \) and \( Y \) are disjoint.

If the following additional property holds, then \( \chi \) is called a **strong** Euler characteristic:

• If \( f : X \to Y \) is a definable function and there is an \( r \in \mathbb{R} \) such that \( \chi(f^{-1}(y)) = r \) for all \( y \), then
  \[
  \chi(X) = r \cdot \chi(Y).
  \]

An Euler characteristic \( \chi \) is **definable** if the set \( \{ y \in Y : \chi(f^{-1}(y)) = r \} \) is definable for every definable function \( f : X \to Y \) and every \( r \in \mathbb{R} \).

1.2 Examples of Euler characteristics

The simplest example of an Euler characteristic is the counting function on a finite structure. If \( M \) is a finite structure, there is a \( \mathbb{Z} \)-valued Euler characteristic given by

\[
\chi(X) = |X|
\]

where \( |X| \) denotes the size of \( X \). This \( \chi \) is always strong and 0-definable.

Another well-known example is the Euler characteristic on dense o-minimal structures ([23], §4.2). If \( (M,<,...,) \) is a dense o-minimal structure, there is a \( \mathbb{Z} \)-valued Euler characteristic on \( M \), characterized by the fact that \( \chi(C) = -1^{\dim C} \) for any open cell \( C \). This Euler characteristic is strong and 0-definable. By work of Kamenkovich and Peterzil [15], it can be extended to \( M^{eq} \). On o-minimal expansions of the reals, \( \chi(X) \) agrees with the topological Euler characteristic for compact definable \( X \subseteq \mathbb{R}^n \).

Pseudofinite structures have strong Euler characteristics arising from counting mod \( n \). More precisely, if \( M \) is an ultraproduct of finite structures, there is a canonical strong Euler characteristic \( \chi_n : \text{Def}(M) \to \mathbb{Z}/n\mathbb{Z} \) defined in the following way. Let \( M \) be the ultraproduct \( \prod_{i \in I} M_i/\mathcal{U} \), and \( X = \phi(M; a) \) be a definable set. Choose a tuple \( \langle a_i \rangle_{i \in I} \in \prod_{i \in I} M_i \) representing \( a \). Then define \( \chi_n(X) \in \mathbb{Z}/n\mathbb{Z} \) to be the ultralimit along \( \mathcal{U} \) of the sequence

\[
\langle |\phi(M_i; a_i)| + n\mathbb{Z} \rangle_{i \in I}
\]

This ultralimit exists because \( \mathbb{Z}/n\mathbb{Z} \) is finite.

More intuitively, if we take \( \mathbb{Z}^* \) to be the ultrapower \( \mathbb{Z}^{\mathcal{U}} \simeq \mathbb{Z} \), then there is a nonstandard counting function \( \chi^* : \text{Def}(M) \to \mathbb{Z}^* \) assigning to each definable set \( X \subseteq M^n \) its nonstandard “size” in \( \mathbb{Z}^* \). Then \( \chi_n \) is the composition

\[
\text{Def}(M) \xrightarrow{\phi^*} \mathbb{Z}^* \to \mathbb{Z}^*/n\mathbb{Z}^* \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}
\]

The map \( \chi^* \) happens to be a strong Euler characteristic itself, but we will not consider it further.
The mod $n$ Euler characteristics on pseudofinite structures need not be defi nable. For example, consider an ultraproduct of the totally ordered sets \( \{0, 1, \ldots, m\} \) as $m \to \infty$. The resulting ultraproduct $(M, <)$ admits no defi nable $\mathbb{Z}/n\mathbb{Z}$-valued Euler characteristics (for $n > 1$). Indeed, if $\chi$ is an Euler characteristic on $M$, consider the function

$$f(a) = \chi([0, a]) \in \mathbb{Z}/n\mathbb{Z}$$

Then $f(b) = f(a) + 1$ when $b$ is the successor of $a$. The set $f^{-1}(0)$ must therefore contain every $n$th element of $M$, and hence cannot be defi nable, because $M$ is (non-dense) o-minimal.

We will see below (Theorem 1.1.1) that this does not happen with ultraproducts of finite fields: the $\chi_n$ are always defi nable on ultraproducts of finite fields.

On an ultraproduct $M$ of finite structures, these $\chi_n$ maps are compatible in the sense that the following diagram commutes when $n$ divides $m$:

\[
\begin{array}{ccc}
\text{Def}(M) & \xrightarrow{\chi_m} & \mathbb{Z}/m\mathbb{Z} \\
\downarrow{\chi_n} & & \downarrow \\
\mathbb{Z}/n\mathbb{Z} & & \\
\end{array}
\]

Consequently, they assemble into a map

$$\hat{\chi} : \text{Def}(M) \to \hat{\mathbb{Z}}$$

where $\hat{\mathbb{Z}}$ is the ring $\varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$.

More generally, if $M$ is any structure, we will say that a map $\chi : \text{Def}(M) \to \hat{\mathbb{Z}}$ is

1. an Euler characteristic if all the compositions $\text{Def}(M) \to \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ are Euler characteristics

2. a strong Euler characteristic if all the compositions $\text{Def}(M) \to \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ are strong Euler characteristics

3. a definable Euler characteristic if all the compositions $\text{Def}(M) \to \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ are definable Euler characteristics.

For 2 and 3, this is an abuse of terminology.

We can repeat the discussion above with the $p$-adics $\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$ instead of $\hat{\mathbb{Z}}$. Recall that

$$\hat{\mathbb{Z}} \cong \prod_{p} \mathbb{Z}_p$$

by the Chinese remainder theorem. Giving an Euler characteristic $\hat{\chi} : \text{Def}(M) \to \hat{\mathbb{Z}}$ is therefore equivalent to giving an Euler characteristic $\chi_p : \text{Def}(M) \to \mathbb{Z}_p$ for every $p$. Moreover, $\hat{\chi}$ is strong or definable if and only if every $\chi_p$ is strong or definable, respectively. It is sometimes more convenient to work with $\mathbb{Z}_p$ because it is an integral domain, unlike $\hat{\mathbb{Z}}$.  

3
1.3 Main results for pseudofinite fields

A structure is *pseudofinite* if it is infinite, yet elementarily equivalent to an ultraproduct of finite structures. By a theorem of Ax [2], a field $K$ is pseudofinite if and only if $K$ satisfies the following three conditions:

- $K$ is perfect
- $K$ is pseudo-algebraically closed: every geometrically integral variety over $K$ has a $K$-point.
- $\text{Gal}(K) \cong \hat{\mathbb{Z}}$, or equivalently, $K$ has a unique field extension of degree $n$ for each $n$.

Our first main result can be phrased purely in terms of pseudofinite fields.

**Theorem 1.1.**

1. Let $K = \prod_i K_i/\mathcal{U}$ be an ultraproduct of finite fields. Then the nonstandard counting functions $\chi_n$ are acl$^q(\emptyset)$-definable.

2. Every pseudofinite field admits an acl$^q(\emptyset)$-definable $\hat{\mathbb{Z}}$-valued strong Euler characteristic.

We make several remarks:

1. In Part 1, the acl$^q(\emptyset)$ is necessary: the nonstandard counting function is known to not be 0-definable, by Theorem 7.3 in [17].

2. In Part 2, the Euler characteristic is not canonical, but depends on a choice of a topological generator $\sigma \in \text{Gal}(K)$.

One approach to proving Theorem 1.1 would be to use etale cohomology. In fact, there should be a close connection between $\ell$-adic cohomology and the $\ell$-adic part of the Euler characteristic $\chi$—see Conjecture 6.3. This approach was originally suggested by Hrushovski, according to Krajíček’s comments at the end of [17].

We avoid this line of proof, because it is less elementary, and doesn’t handle the case where $\ell = \text{char}(K)$. Rather than using etale cohomology, we will use the more elementary theory of abelian varieties and jacobians, essentially falling back to Weil’s original proof of the Riemann hypothesis for curves.

Aside from Theorem 1.1, there is also a decidability theorem in terms of generalized parity quantifiers. For any $n \in \mathbb{N}$ and $k \in \mathbb{Z}/n\mathbb{Z}$, let $\mu^n_k x$ be a new quantifier. Interpret $\mu^n_k x : \phi(x)$ in finite structures as

The number of $x$ such that $\phi(x)$ holds is congruent to $k$ mod $n$.

In other words,

$$
\left( M \models \mu^n_k \vec{x} : \phi(\vec{x}, \vec{b}) \right) \iff \left( |\{\vec{a} : M \models \phi(\vec{a}, \vec{b})\}| \equiv k \pmod{n} \right).
$$

For example,
• $\mu_2^2 x$ means “there are an even number of $x$ such that…”
• $\mu_2^3 x$ means “there are an odd number of $x$ such that…”

We call $\mu_n^k$ a generalized parity quantifier.

Let $L_{\text{rings}}^\mu$ be the language of rings expanded with generalized parity quantifiers.

**Theorem 1.2.** Assuming Conjecture 5.2, the $L_{\text{rings}}^\mu$-theory of finite fields is decidable.

Unfortunately, this result is conditional on Conjecture 5.2, a technical statement about definability in algebraic geometry. While the conjecture is certainly true, it is hard to give a sane proof, for reasons discussed in §5. A complete proof will (hopefully) be given in future work [14].

### 1.4 Main results for periodic difference fields

The results of §1.3 can be stated more precisely in terms of difference fields. Recall that a difference field is a pair $(K, \sigma)$ where $K$ is a field and $\sigma$ is an automorphism of $K$.

**Definition 1.3.** A periodic difference field is a difference field $(K, \sigma)$ such that every element of $K$ has finite orbit under $\sigma$.

Periodic difference fields are not an elementary class in the language of difference fields. However, they constitute an elementary class when regarded as multi-sorted structures $(K_1, K_2, \ldots)$ where $K_i$ is the fixed field of $\sigma^i$, with the following structure:

• The difference-field structure on each $K_i$
• The inclusion map $K_n \to K_m$ for each pair $n, m$ with $n$ dividing $m$

These multi-sorted structures were considered by Hrushovski in [12], and we will give an overview of their basic properties in §3 below.

To highlight the fact that we are no longer working in the language of difference fields, we will call these structures periodic fields. If $(K_1, K_2, \ldots)$ is a periodic field, we let $K_\infty$ denote the associated periodic difference field

$$K_\infty = \lim_{\to n} K_n.$$  

We will abuse notation and write $(K_\infty, \sigma)$ when we really mean the associated periodic field $(K_1, K_2, \ldots)$.

For any $q$, let $\text{Fr}_q^q$ denote $(\mathbb{F}_q^{\text{alg}}, \phi_q)$, where $\phi_q$ is the $q$th power Frobenius. Thus $\text{Fr}_n^q = (\mathbb{F}_q^n, \phi_q)$. We will call the $\text{Fr}_q^q$’s Frobenius periodic fields. Frobenius periodic fields are essentially finite, in the sense that every definable set is finite. Consequently, ultraproducots of Frobenius periodic fields admit $\mathbb{Z}/n\mathbb{Z}$-valued strong Euler characteristics $\chi_n$.

There is a theory ACPF whose class of models can be described in several ways:
1. The existentially closed periodic fields.

2. The non-Frobenius periodic fields satisfying the theory of Frobenius periodic fields.

3. The periodic fields of the form \((K^{alg}, \sigma)\), where \(K\) is pseudofinite and \(\sigma\) is a topological generator of \(\text{Gal}(K)\).

(See Propositions 3.2, 3.13, and 3.3, respectively.) In particular, \(\text{ACPF}\) is the model companion of periodic fields, and non-principal ultraproducts of Frobenius periodic fields are models of \(\text{ACPF}\). The situation is analogous to, but much simpler than, the situation with \(\text{ACFA} \ [13]\).

Theorem 1.1 has the following analogue for periodic fields:

**Theorem 1.4.** Let \(\mathcal{C}\) be the class of Frobenius periodic fields and existentially closed periodic fields. There is a \(\hat{\mathbb{Z}}\)-valued strong Euler characteristic \(\chi\) on \((K, \sigma)\) in \(\mathcal{C}\) with the following properties:

- \(\chi\) is uniformly 0-definable across \(\mathcal{C}\).
- If \((K, \sigma)\) is a Frobenius periodic field, then \(\chi\) is the counting Euler characteristic:

\[\chi(X) = |X|\]

- If \((K, \sigma)\) is an ultraproduct of Frobenius periodic fields, then \(\chi\) is the nonstandard counting Euler characteristic.

If \(F\) is an abstract pseudofinite field, each topological generator \(\sigma \in \text{Gal}(F)\) turns \((F^{alg}, \sigma)\) into a periodic difference field satisfying \(\text{ACPF}\). There is no canonical choice of \(\sigma\), which is the reason for the non-canonicalness in Theorem 1.1.2.

There are also statements in terms of parity quantifiers. Let \(\mathcal{L}_{pf}\) be the first-order language of periodic fields, and let \(\mathcal{L}^\mu_{pf}\) be its expansion by generalized parity quantifiers.

**Theorem 1.5.**

1. Generalized parity quantifiers are uniformly eliminated on the class of Frobenius periodic fields.

2. Assuming Conjecture 5.2, the \(\mathcal{L}^\mu_{pf}\)-theory of Frobenius periodic fields is decidable.

This statement is stronger than what we can say about finite and pseudofinite fields. In fact, generalized parity quantifiers are not uniformly eliminated on finite fields (Lemma 6.8).
1.5 A special case

If $p$ is a prime, let $\mathbb{Z}_{\neg p}$ be the prime-to-$p$ completion of $\mathbb{Z}$:

$$\mathbb{Z}_{\neg p} = \lim_{\leftarrow (n,p)=1} \mathbb{Z}/n\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_\ell.$$  

If $K$ is a field, let $\text{Abs}(K)$ denote the subfield of absolute numbers, i.e., the relative algebraic closure of the prime field. Say that a field $K$ is mock-finite if $K$ is pseudofinite and $\text{Abs}(K)$ is finite. Say that $K$ is a mock-$\mathbb{F}_q$ if moreover $\text{Abs}(K) \cong \mathbb{F}_q$. For each prime power $q$, there is a unique mock-$\mathbb{F}_q$ up to elementary equivalence (Proposition 7.8.3).

The nonstandard Euler characteristics behave in a funny way on mock-finite fields:

**Theorem 1.6.** Let $K$ be a mock-$\mathbb{F}_q$, for some prime power $q = p^k$. There are two $\mathbb{Z}_{\neg p}$-valued 0-definable strong Euler characteristics $\chi$ and $\chi^\dagger$ on $K$, such that

1. If $V$ is a smooth projective variety over $\mathbb{F}_q$, then
   $$\chi(V(K)) = |V(\mathbb{F}_q)|$$
   $$\chi^\dagger(V(K)) = |V(\mathbb{F}_q)|/q^{\dim V}.$$  

2. If $X$ is any $\mathbb{F}_q$-definable set, then
   $$\chi(X) = |X \cap \text{dcl}(\mathbb{F}_q)|.$$  

   In particular, $\chi(X) \in \mathbb{Z}$.

3. If $X$ is any $\mathbb{F}_q$-definable set, then $\chi^\dagger(X) \in \mathbb{Q}$.

Using this, we construct a strange $\mathbb{Q}$-valued weak Euler characteristic on pseudofinite fields in §7.4.

1.6 Related work

Many people have considered non-standard sizes of definable sets in pseudofinite fields [1, 4, 7, 17, 18]. Non-standard sizes modulo $p$ were considered by Krajíček, who used them to prove the existence of non-trivial strong Euler characteristics on pseudofinite fields [17]. However, most research has focused on ordered Euler characteristics ([1] [18]) and the real standard part of non-standard sizes ([4, 7]). These topics can be seen as “non-standard sizes modulo the infinite prime.”

Dwork [6] and Kiefe [16] consider the behavior of $|\phi(\mathbb{F}_q)|$ as $q$ varies. Their work can be used to calculate the non-standard mod-$n$ sizes of 0-definable sets in pseudofinite fields of positive characteristic.

Almost everything in §7 is well-known to experts. The results specific to periodic fields probably appear in Hrushovski’s paper [12], which I have had trouble finding.
1.7 Notation

If \( K \) is a field, then \( K^{alg} \) (resp. \( K^{sep} \)) denotes the algebraic (resp. separable) closure, and \( \text{Gal}(K) \) denotes the absolute Galois group \( \text{Gal}(K^{sep}/K) = \text{Aut}(K^{sep}/K) \). We let

\[
\hat{\mathbb{Z}} = \lim_{\leftarrow n} \mathbb{Z}/n\mathbb{Z}
\]

denote the profinite completion of \( \mathbb{Z} \). The finite field with \( q \) elements is denoted \( \mathbb{F}_q \).

A variety over \( K \) is a finite-type separated reduced scheme over \( K \), not necessarily irreducible or quasi-projective. If \( V \) is a variety, then \( V(K) \) denotes the set of \( K \)-points of \( V \). A scheme \( X \) over \( K \) is geometrically integral or geometrically irreducible if \( X \times_K K^{alg} \) is integral or irreducible. A curve over \( K \) is a geometrically integral 1-dimensional smooth projective variety over \( K \).

Remark 1.7. If \( K \) is a perfect field and \( V \) is a variety, then geometrically irreducible is equivalent to geometrically integral.

2 Review of abelian varieties

Let \( A \) be an abelian variety over some field \( K \). For any \( n \in \mathbb{N} \), let \( A[n] \) denote the group of \( n \)-torsion in \( A(K^{alg}) \), viewed as an abelian group with \( \text{Gal}(K) \)-action. The \( \ell \)th Tate module

\[
T_{\ell}A = \lim_{\leftarrow n} A[\ell^n].
\]

See §18 of [20] for a precise definition. If \( g = \dim A \), then there are non-canonical isomorphisms

\[
T_{\ell}A \approx \mathbb{Z}_{\ell}^{2g}
\]

for all \( \ell \neq \text{char}(K) \). In particular, \( T_{\ell}A \) is a free \( \mathbb{Z}_\ell \)-module of rank \( 2g \). If \( p = \text{char}(K) \), then

\[
T_pA \approx \mathbb{Z}_p^r
\]

for some \( r \) known as the \( p \)-rank of \( A \). The \( p \)-rank is at most \( g \). Similar statements hold for the torsion subgroups:

\[
A[\ell^k] \approx (\mathbb{Z}/\ell^k)^{2g} \quad \ell \neq \text{char}(K)
\]
\[
A[p^k] \approx (\mathbb{Z}/p^k)^r \quad p = \text{char}(K).
\]

An isogeny on \( A \) is a surjective endomorphism \( f : A \to A \). An isogeny \( f \) is finite and flat ([19], Proposition I.7.1), hence has a well-defined degree \( \deg(f) \). Degree of finite flat maps is preserved in pullbacks, so \( \deg(f) \) can be described alternately as

- The length of the scheme-theoretic kernel of \( f \) (a finite group scheme over \( K \)).
- The degree of the fraction field extension.
If $f : A \to A$ is a non-surjective endomorphism, then $\deg(f)$ is defined to be 0.

Any endomorphism $f : A \to A$ induces an endomorphism $T_\ell(f)$ on the Tate modules. We can talk about the determinant and trace of this endomorphism.

**Fact 2.1** (cf. Theorem 19.4 in [20], or Proposition I.10.20 in [19]). If $f : A \to A$ is any endomorphism, and $\ell \neq \text{char}(K)$, then

$$\deg(f) = \det T_\ell(f).$$

**Corollary 2.2.** If $\alpha_1, \ldots, \alpha_{2g}$ denote the eigenvalues of $T_\ell(f)$, then for any polynomial $P(X) \in \mathbb{Z}[X],$

$$\deg(P(f)) = \prod_{i=1}^{2g} P(\alpha_i).$$

Because the left hand side is an integer independent of $\ell$, it follows that the $\alpha_i$ are algebraic numbers which do not depend on $\ell$.

The numbers $\alpha_1, \ldots, \alpha_{2g}$ are called the characteristic roots of the endomorphism $f$. The characteristic roots govern the counting of points on curves over finite fields:

**Fact 2.3** (= Theorem III.11.1 in [19]). Let $C$ be a curve over a finite field $\mathbb{F}_q$, and let $J$ be its Jacobian. Then

$$|C(\mathbb{F}_q)| = 1 - \left(\sum_{i=1}^{2g} \alpha_i\right) + q$$

where the $\alpha_i$ are the characteristic roots of the $q$th power Frobenius endomorphism $\phi_q : J \to J$.

**Corollary 2.4.** In the setting of Theorem 2.3, if $\ell$ is prime to $q$, then

$$|C(\mathbb{F}_q)| \equiv 1 - \text{Tr}(\phi_q|J[\ell^k]) + \text{Tr}(\phi_q|\mathbb{G}_m[\ell^k]) \quad (\mod \ell^k)$$

where $\mathbb{G}_m$ denotes the multiplicative group, $\mathbb{G}_m[\ell^k]$ denotes the group of $\ell^k$th roots of unity (in $\mathbb{F}_q^{alg}$), and $\text{Tr}(\sigma|M)$ denotes the trace of an endomorphism $\sigma$ of some free $\mathbb{Z}/\ell^k$-module $M$.

**Proof.** First of all note that there are non-canonical isomorphisms

$$J[\ell^k] \approx (\mathbb{Z}/\ell^k)^{2g}$$

$$\mathbb{G}_m[\ell^k] \approx \mathbb{Z}/\ell^k$$

and so the modules are indeed free $\mathbb{Z}/\ell^k$-modules, and the traces are meaningful. The trace $\text{Tr}(\phi_q|J[\ell^k])$ is simply the $\ell^k$-residue class of $\text{Tr}(\phi_q|T_\ell J)$. The action of $\phi_q$ on $\mathbb{G}_m$ is multiplication by $q$, so $\text{Tr}(\phi_q|\mathbb{G}_m[\ell^k])$ is exactly $q \pmod{\ell^k}$. \qed
2.1 Bad characteristic

We would like an analogue of Corollary 2.4 in the case of bad characteristic $\ell = p$.

**Lemma 2.5.** Let $Q(x)$ and $R(x)$ be two monic polynomials in $\mathbb{Q}_p[x]$. Let $\beta_1, \ldots, \beta_m \in \mathbb{Q}_p^{alg}$ be the roots of $Q(x)$, and $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}_p^{alg}$ be the roots of $R(x)$. Suppose that

$$v_p \left( \prod_{i=1}^{m} P(\beta_i) \right) \leq v_p \left( \prod_{i=1}^{n} P(\alpha_i) \right)$$

(1)

holds for every $P(x) \in \mathbb{Z}[x]$. Then $\{\beta_1, \ldots, \beta_m\}$ is a submultiset of $\{\alpha_1, \ldots, \alpha_m\}$, i.e., $Q(x)$ divides $R(x)$.

**Proof.** Let $\gamma_1$ be any element of $\mathbb{Q}_p^{alg}$. Let $q_1$ and $r_1$ be the multiplicities of $\gamma_1$ as a root of $Q(x)$ and $R(x)$, respectively. (Either can be zero.) We will show that $q_1 \leq r_1$.

The identity (1) extends by continuity to any $P(x) \in \mathbb{Z}_p[x]$. Let $\{\gamma_1, \ldots, \gamma_{\ell}\} \subseteq \mathbb{Q}_p^{alg}$ be the set of conjugates of $\gamma_1$ over $\mathbb{Q}_p$. For some non-zero $a \in \mathbb{Z}_p$, the polynomial

$$P(x) = a(x - \gamma_1) \cdots (x - \gamma_{\ell})$$

lies in $\mathbb{Z}_p[x]$. For any $\epsilon \in \mathbb{Z}_p$, we can apply (1) to $P(x + \epsilon)$, yielding

$$v_p \left( a^m \prod_{i=1}^{m} \prod_{j=1}^{\ell} (\beta_i + \epsilon - \gamma_j) \right) \leq v_p \left( a^n \prod_{i=1}^{n} \prod_{j=1}^{\ell} (\alpha_i + \epsilon - \gamma_j) \right),$$

or equivalently,

$$v_p \left( a^m \prod_{j=1}^{\ell} Q(\gamma_j - \epsilon) \right) \leq v_p \left( a^n \prod_{j=1}^{\ell} R(\gamma_j - \epsilon) \right).$$

(2)

Let $q_j$ and $r_j$ be the multiplicity of $\gamma_j$ as a root of $Q(x)$ and $R(x)$, respectively. If $v_p(\epsilon) \gg 0$, then (2) yields

$$O(1) + v_p(\epsilon) \cdot \sum_{j=1}^{\ell} q_j \leq O(1) + v_p(\epsilon) \cdot \sum_{j=1}^{\ell} r_j.$$

Thus $\sum_{j=1}^{\ell} q_j \leq \sum_{j=1}^{\ell} r_j$. But in fact $q_j = q_1$, because $Q(x)$ is over $\mathbb{Q}_p$. Similarly, $r_j = r_1$ independent of $j$. Thus $\ell \cdot q_1 \leq \ell \cdot r_1$. \hfill $\square$

Recall that the degree of an isogeny $f : A \to A$ is equal to the degree of the fraction field extension, and therefore factors into separable and inseparable parts:

$$\deg(f) = \deg_s(f) \cdot \deg_i(f).$$

Moreover, $\deg_s(f)$ is the size of the set-theoretic kernel of $f$ (20, §6, Application 3).

**Fact 2.6.** For any $\ell$ (possibly $\ell = p$),

$$v_\ell(\det T_\ell(\phi)) = v_\ell(|\ker \phi|) = v_\ell(\deg_s(\phi))$$

10
Fact 2.6 is implicit in the proof of Theorem 19.4 in [20] or Theorem I.10.20 in [19].

**Lemma 2.7.** Let $A$ be an abelian variety over $\mathbb{F}_q$ for $q = p^k$. Let $\beta_1, \ldots, \beta_r$ be the eigenvalues of $T_p(\phi_q)$, for $\phi_q$ the $q$th power Frobenius on $A$.

1. $\{\beta_1, \ldots, \beta_r\}$ is a submultiset of the characteristic roots $\{\alpha_1, \ldots, \alpha_r\}$ of $\phi_q$.

2. Each $\beta_i$ has valuation zero in $\mathbb{Q}_{p^\text{alg}}$.

**Proof.** By Corollary 2.2 and Fact 2.6, the following holds for any polynomial $P(x) \in \mathbb{Z}[x]$:

\[ v_p \left( \prod_{i=1}^{r} P(\beta_i) \right) = v_p(\det T_p(P(\phi_q))) = v_p(\deg_s(P(\phi_q))) \]

\[ \leq v_p(\deg(P(\phi_q))) = v_p \left( \prod_{i=1}^{2q} P(\alpha_i) \right). \]

Then (1) follows by Lemma 2.5. For (2), note that the $\beta_i$ are integral over $\mathbb{Z}_p$ because they are the eigenvalues of a linear map $\mathbb{Z}_p^r \to \mathbb{Z}_p^r$. Integrality implies that $v_p(\beta_i) \geq 0$. Moreover, the map $\mathbb{Z}_p^r \to \mathbb{Z}_q^r$ is invertible, because the $q$th power Frobenius is a bijection on points. Therefore, the $\beta_i^{-1}$ are also integral, of nonnegative valuation. \qed

**Lemma 2.8.** There is a computable function $h_1(d, d', p, s)$ with the following property. Let $(K, v)$ be an algebraically closed valued field of mixed characteristic $(0, p)$. Let $Q(x)$ be a monic polynomial of degree $d$, with roots $\alpha_1, \ldots, \alpha_d$. Suppose $d' \leq d$ and suppose that $v(Q(p^i)) \geq v(p^{id'})$ for $1 \leq i \leq h_1(d, d', p, s)$. Then at least $d'$ of the $\alpha_i$ satisfy $v(\alpha_i) \geq v(p^s)$.

**Proof.** We first claim that $h_1(d, d', p, s)$ exists for fixed $d, d', p, s$. Otherwise, by compactness there is $(K, v) \models \text{ACVF}_{0,p}$ and a monic polynomial $Q(x)$ of degree $d$ such that

\[ \forall i \in \mathbb{N} : v(Q(p^i)) \geq v(p^{id'}), \]

but fewer than $d'$ of the roots of $Q(x)$ have valuation greater than $v(p^s)$. Let $\alpha_1, \ldots, \alpha_d$ be the roots of $Q(x)$, sorted so that

\[ v(\alpha_1) \geq v(\alpha_2) \geq \cdots \geq v(\alpha_d). \]

Say that $\alpha_j$ is “infinitesimal” if $v(\alpha_j) \geq v(p^n)$ for every $n \in \mathbb{N}$. Then $\alpha_1, \ldots, \alpha_k$ are infinitesimal, and $\alpha_{k+1}, \ldots, \alpha_d$ are not, for some $k \leq d$. We claim $k \geq d'$. Otherwise, take $i \in \mathbb{N}$ so large that

\[ v(p^i) > v(\alpha_{k+1}) \]

\[ (d' - k) \cdot v(p^i) > \sum_{j=k+1}^{d} v(\alpha_j). \]

11
Note
\[ v(\alpha_k) > v(p^i) > v(\alpha_{k+1}). \]

Then
\[ v(Q(p^i)) = \sum_{j=1}^{k} v(p^i - \alpha_j) + \sum_{j=k+1}^{d} v(p^i - \alpha_j) \]
\[ = \sum_{j=1}^{k} v(p^i) + \sum_{j=k+1}^{d} v(\alpha_j) \]
\[ = k \cdot v(p^i) + \sum_{j=k+1}^{d} v(\alpha_j). \]

By assumption, \( v(Q(p^i)) \geq v(p^{i'}) = d' \cdot v(p^i) \), and so
\[ k \cdot v(p^i) + \sum_{j=k+1}^{d} v(\alpha_j) \geq d' \cdot v(p^i), \]
contradicting the choice of \( i \).

Therefore \( k \geq d' \). So at least \( d' \) of the roots of \( Q(x) \) are infinitesimal, hence have magnitude greater than or equal to \( p^s \), a contradiction. This shows that \( h_1(d, d', p, s) \) exists for each \( d, d', p, s \). Now if \( \tau_{d,d',p,s,h} \) is the first-order sentence expressing that \( h \) has the desired property with respect to \( d, d', p, s \), then
\[ \forall d, d', p, s \exists h : ACVF \vdash \tau_{d,d',p,s,h}. \]

Because \( \tau_{d,d',p,s,h} \) depends computably on \( d, d', p, s, h \), and the set of theorems in ACVF is computably enumerable, one can choose \( h \) to depend computably on \( d, d', p, s \).

**Lemma 2.9.** Let \( G \) be a finite connected commutative group scheme of length \( n \) over \( \mathbb{F}_q \). If \( n < q \) then the \( q \)-th power Frobenius morphism \( G \to G \) is the zero endomorphism.

**Proof.** We can write \( G \) as \( \text{Spec} \ A \) for some local Artinian \( n \)-dimensional \( \mathbb{F}_q \)-algebra \( A \). Let \( \mathfrak{m} \) be the maximal ideal of \( A \); by properties of local Artinian rings this is the sole prime ideal. We claim that the \( \mathbb{F}_q \)-algebra \( A/\mathfrak{m} \) is exactly \( \mathbb{F}_q \) (rather than a finite field extension), and that the quotient map
\[ A \to A/\mathfrak{m} \]
is dual to the inclusion of the identity element \( \text{Spec} \mathbb{F}_q \to G \). Indeed, the inclusion of the identity must correspond to some homomorphism \( f : A \to \mathbb{F}_q \). Since \( f \) is a homomorphism of \( \mathbb{F}_q \)-algebras, \( f \) is a left inverse to the structure map \( \mathbb{F}_q \to A \), and so \( f \) is surjective. The kernel is a prime ideal, necessarily \( \mathfrak{m} \).

Now by properties of Artinian local rings, the maximal ideal \( \mathfrak{m} \) is also the nilradical, so every \( x \in \mathfrak{m} \) is nilpotent. In fact, \( x^q = 0 \) for all \( x \in \mathfrak{m} \). Otherwise, the descending chain of ideals
\[ A \supseteq (x) \supseteq (x^2) \supseteq \cdots \supseteq (x^q) \supseteq (0) \]
would contradict length \( \leq q \).

So the \( q \)th power homomorphism on \( A \) annihilates \( m \), and must therefore be

\[
A \to A/m \tilde{\to} \mathbb{F}_q \hookrightarrow A
\]

Thus the \( q \)th power Frobenius on \( G \) must be \( G \to \text{Spec} \mathbb{F}_q \to G \), which is the zero endomorphism.

\[\square\]

**Fact 2.10.** Let \( G \) be a commutative finite group scheme over a field \( K \).

- Let \( G' \) be a finite subgroup scheme. Then the length of \( G' \) divides the length of \( G \).
- Let \( G^0 \) denote the connected component of \( G \). Then \( \ell(G^0) = \ell(G)/|G(K^{alg})| \).

The first point follows from Theorems 10.5-10.7 in [21]. The second point follows by the proof of Proposition 15.3 in [21].

**Lemma 2.11.** Suppose \( A \) is a \( g \)-dimensional abelian variety over \( \mathbb{F}_q \). Suppose \( q > p^{2g} \). Let \( r \) be the \( p \)-rank of \( A \). Let \( \phi_q \) denote the \( q \)th power Frobenius endomorphism of \( A \). Then \( \deg(\phi_q - p^r) \) is divisible by \( p^{i(2g-r)} \).

**Proof.** Take \( \ell \neq p \). By Fact 2.1, \( \deg(p^i) = p^{2g} \) because \( T_\ell A \) is a free \( \mathbb{Z}_\ell \)-module of rank \( 2g \). Let \( G \) denote the scheme-theoretic kernel of the multiplication-by-\( p^i \) endomorphism of \( A \). Then \( G \) is a finite group scheme of length \( \deg(p^i) = p^{2g} \). By definition of \( p \)-rank, \( G(\mathbb{F}_q^{alg}) \approx (\mathbb{Z}/p^i)^r \), so \( G(\mathbb{F}_q^{alg}) \) has size \( p^{ir} \). Therefore, the connected component \( G^0 \) of \( G \) has length \( p^{2g}/p^{ir} = p^{i(2g-r)} \), by Fact 2.10.

The endomorphism \( \phi_q : A \to A \) restricts to the \( q \)th-power Frobenius endomorphism on \( G \) and \( G^0 \). By assumption, \( q > p^{2g} \geq p^{i(2g-r)} \), and so \( \phi_q \) annihilates \( G^0 \) by Lemma 2.9.

Let \( G' \) denote the kernel of \( \phi_q - p^r \). Then \( G^0 \) is a closed subgroup scheme of \( G' \). By Fact 2.10

\[
\ell(G^0) = p^{i(2g-r)} \text{ divides } \ell(G) = \deg(\phi_q - p^r).
\]

\[\square\]

**Proposition 2.12.** There is a computable function \( h_2(p, s, g) \) with the following property. Let \( A \) be a \( g \)-dimensional abelian variety over \( \mathbb{F}_q \), with \( q = p^k > h_2(p, s, g) \). Let \( \phi_q \) denote the \( q \)th power Frobenius on \( A \). Let \( r \) be the \( p \)-rank of \( A \). Then we can write the characteristic roots of \( \phi_q \) as \( \alpha_1, \ldots, \alpha_{2g} \), where

- \( \alpha_1, \ldots, \alpha_r \) are the eigenvalues of \( T_p(\phi_q) : T_p A \to T_p A \).
- \( v_p(\alpha_i) > v_p(p^s) \) for \( i \in \{r + 1, r + 2, \ldots, 2g\} \).

**Proof.** Define

\[
h_2(p, s, g) = \max\{p^{2g-h_1(2g, d', p, s)} : 0 \leq d' \leq 2g\},
\]

where \( h_1 \) is as in Lemma 2.8. Suppose the assumptions hold. Then for any \( 1 \leq i \leq h_1(2g, 2g - r, p, s) \), we have

\[
q = p^k > h_2(p, s, g) \geq p^{2g-h_1(2g, 2g-r, p, s)} \geq p^{2g}.
\]

13
By Lemma 2.11
\[ v_p(\deg(\phi_q - p^i)) \geq v_p(p^{i(2g-r)}) \quad \text{for } i \leq h_1(2g, 2g - r, p, s). \]

Let \( Q(x) \) be the rational polynomial whose roots are the \( \alpha_i \). By Corollary 2.2
\[ \deg(\phi_q - p^i) = \prod_{i=1}^{2g} (\alpha_i - p^i) = Q(p^i). \]

Thus
\[ v_p(Q(p^i)) \geq v_p(p^{i(2g-r)}) \quad \text{for } i \leq h_1(2g, 2g - r, p, s). \]

By definition of \( h_1 \) (Lemma 2.8), it follows that at least \( 2g - r \) of the roots of \( Q(x) \) have \( p \)-adic valuation at least \( v_p(p^s) \). Meanwhile, Lemma 2.7 gives \( r \) roots \( \beta_1, \ldots, \beta_r \), coming from the eigenvalues of \( T_p(\phi_q) \). Each of these roots has valuation zero. There can be no overlap between the \( 2g - r \) roots of valuation at least \( v_p(p^s) \), and the \( r \) roots coming from \( T_p(\phi_q) \), so these together account for all \( 2g \) roots of \( Q(x) \).

Corollary 2.13. There is a computable function \( h(p, s, g) \) with the following property. Let \( C \) be a curve of genus \( g \) over a finite field \( \mathbb{F}_q \), and let \( J \) be its Jacobian. Suppose \( q \) is a power of \( p \), and \( q > h(p, s, g) \). Then
\[ |C(\mathbb{F}_q)| \equiv 1 - \Tr(\phi_q|J[p^s]) + \Tr(\phi_q|G_m[p^s]) \pmod{p^s}, \]
where the notation is as in Corollary 2.4.

Proof. Take \( h(p, s, g) \) to be the maximum of \( h_2(p, s, g) \) and \( p^s \). Suppose \( q > h(p, s, g) \). By Fact 2.3
\[ |C(\mathbb{F}_q)| = 1 + q - \sum_{i=1}^{2g} \alpha_i. \]

Working modulo \( p^s \), the term \( q \) vanishes, because \( q > h(p, s, g) \geq p^s \). Also, \( q > h_2(p, s, g) \), so by Proposition 2.12 we may assume that
- \( \alpha_1, \ldots, \alpha_r \) are the eigenvalues of \( T_p(\phi_q) \)
- \( \alpha_{r+1}, \ldots, \alpha_{2g} \) have valuation at least \( v_p(p^s) \).

Working modulo \( p^s \), we can therefore ignore \( \alpha_{r+1}, \ldots, \alpha_{2g} \). Thus
\[ |C(\mathbb{F}_q)| \equiv 1 - \sum_{i=1}^{r} \alpha_i \pmod{p^s}. \]

The right hand side is \( 1 - \Tr(\phi_q|J[p^s]) \). Finally, observe that \( \Tr(\phi_q|G_m[p^s]) \) vanishes, because \( T_p G_m \) is free of rank 0. (There is no \( p \)-torsion in the multiplicative group.)
3 Review of periodic difference fields

In this section, we review the basic facts about periodic fields. The original source for these results is apparently Hrushovski’s hard-to-find [12]. We will follow an approach that mimics the closely related case of ACFA ([3], [13]).

Recall that a periodic field \((K_\infty, \sigma)\) is secretly a multi-sorted structure \((K_1, K_2, \ldots)\) where \(K_n\) is the fixed field of \(\sigma^n\) on \(K_\infty\). The multi-sorted structure has the following functions and relations:

- The inclusion maps \(K_n \hookrightarrow K_m\) when \(n\) divides \(m\)
- The difference field structure on each \(K_n\)

3.1 Existentially closed periodic fields

If \((K_\infty, \sigma)\) is a periodic field, then \(K_n/K_1\) is a cyclic Galois extension of degree at most \(n\). Say that \((K_\infty, \sigma)\) is \textit{non-degenerate} if \(\text{Gal}(K_n/K_1) \cong \mathbb{Z}/n\mathbb{Z}\) for each \(n\). Equivalently, \(K_n \not\subseteq K_m\) for any \(m < n\).

**Lemma 3.1.** If \((K_\infty, \sigma)\) is a non-degenerate periodic field and \((L_\infty, \sigma)\) extends \((K_\infty, \sigma)\), then the natural map

\[\psi_n : L_1 \otimes_{K_1} K_n \to L_n\]

is an isomorphism of difference rings for all \(n \in \mathbb{N} \cup \{\infty\}\).

**Proof.** The \(n = \infty\) case follows by taking the limit, so we may assume \(n < \infty\). The image of \(\psi_n\) is the compositum \(K_nL_1\). This is an intermediate field in the Galois extension \(L_n/L_1\), so it must be \(L_m\) for some \(m\) dividing \(n\). By non-degeneracy, \(K_n \not\subseteq L_m\) for any \(m < n\). Thus \(K_nL_1 = L_n\) and the map is surjective. Non-degeneracy of \(K_\infty\) implies non-degeneracy of \(L_\infty\), and so

\[[K_n : K_1] = n = [L_n : L_1].\]

Counting dimensions, \(\psi_n\) must be injective. \(\square\)

Recall that a field extension \(L/K\) is \textit{regular} if \(L \otimes_K K^{alg}\) is a domain, or equivalently, a field. A field \(K\) is \textit{pseudo algebraically closed} (PAC) if \(K\) is relatively existentially closed in every regular extension. An equivalent condition is that \(V(K) \neq \emptyset\) for every geometrically integral variety \(V\) over \(K\). This property is first-order ([9], Proposition 10.9).

**Proposition 3.2.** A periodic field \((K_\infty, \sigma)\) is existentially closed if and only if

1. \(K_\infty \models \text{ACF},\)
2. \((K_\infty, \sigma)\) is non-degenerate, and
3. \(K_1\) is PAC.
Proof. Suppose (1) fails. Extend $\sigma$ to an automorphism $\sigma'$ of $K_{\infty}^{alg}$. Then $(K_{\infty}, \sigma)$ fails to be existentially closed in $(K_{\infty}^{alg}, \sigma')$.

Suppose (2) fails, so that $K_n = K_m$ for some $m < n$. Let $\sigma'$ be the automorphism of $K_\infty' := K_\infty(x_1, \ldots, x_n)$ extending $\sigma$ and mapping $x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n \mapsto x_1$.

Then $(K_{\infty}, \sigma)$ is not existentially closed in $(K_{\infty}', \sigma')$. Indeed, the equation $\sigma^n(x) = x \neq \sigma^m(x)$ has a solution in $K_{\infty}'$ but not $K_{\infty}$.

Suppose (3) fails, so $K_1$ is not existentially closed in some regular extension $L/K_1$. The difference ring $L_\infty := L \otimes_{K_1} K_\infty$ is a field by regularity of $L/K_1$. Then $L_{\infty}$ is a periodic field extending $K_{\infty}$, and $K_{\infty}$ is not existentially closed in $L_{\infty}$ because $K_1$ is not existentially closed in $L_1$.

Finally, suppose (1-3) all hold. Let $L_{\infty}$ be a periodic field extending $K_{\infty}$. Let $K_{\infty}^*$ be a big ultrapower of $K_{\infty}$ (in the language of periodic fields, not difference fields). It suffices to embed $L_{\infty}$ into $K_{\infty}^*$ over $K_{\infty}$. Note that

$$K_{\infty}^* = K_1^* \otimes_{K_1} K_{\infty} = K_1^* \otimes_{K_1} K_{1}^{alg}.$$ 

The first equality holds by Lemma 3.1 and (2); the second equality holds by (1) and the general fact that $K_{\infty}/K_1$ is algebraic. Similarly

$$L_{\infty} = L_1 \otimes_{K_1} K_{\infty} = L_1 \otimes_{K_1} K_1^{alg}.$$ 

Then $L_1/K_1$ is regular, so $K_1$ is existentially closed in $L_1$ by (3). It follows that $L_1$ embeds into $K_1^*$ over $K_1$. Tensoring with $K_{\infty}$, this gives the desired embedding of periodic fields:

$$L_{\infty} = L_1 \otimes_{K_1} K_{\infty} \hookrightarrow K_1^* \otimes_{K_1} K_{\infty} = K_{\infty}^*.$$ 

The conditions of Proposition 3.2 are first order, in spite of appearances to the contrary.

**Definition 3.3.** ACPF is the theory of existentially closed periodic fields. In other words, ACPF is the model companion of periodic fields.

The name “ACPF” is not standard, and is chosen by analogy with ACFA.

If $(K, \sigma)$ is a periodic field, let $\text{Abs}(K)$ denote the “absolute numbers,” the relative algebraic closure of the prime field in $K$. We can regard $\text{Abs}(K)$ as a substructure of $K$. The field $\text{Abs}(K)$ is algebraically closed whenever $K$ is.

**Lemma 3.4.** Two models $K_1, K_2 \models \text{ACPF}$ are elementarily equivalent if and only if $\text{Abs}(K_1) \cong \text{Abs}(K_2)$. More generally, if $F$ is a substructure of $K_1$ and $F = F^{alg}$, then any embedding of $F$ into $K_2$ is a partial elementary map from $K_1$ to $K_2$.

**Proof.** The proof is the same as for ACFA (3, Theorem 1.3). Let $L = \text{Frac}(K_1 \otimes_F K_2)$. Then $L$ is a periodic field amalgamating $K_1$ and $K_2$ over $F$. By companionability, $K_1$ and $K_2$ have the same type over $F$. 

16
Recall that a field is pseudofinite if it is perfect, PAC, and has absolute Galois group \( \hat{\mathbb{Z}} \). Models of ACPF are essentially pseudofinite fields with a choice of a generator of the Galois group:

**Proposition 3.5.** If \( K \) is pseudofinite and \( \sigma \) is a topological generator of \( \text{Gal}(K) \), then \((K^{\text{alg}}, \sigma) \models \text{ACPF}\). The periodic field \((K^{\text{alg}}, \sigma)\) and the pseudofinite field \( K \) are bi-interpretable after naming parameters. All models of ACPF arise in this way from pseudofinite fields.

**Proof.** Except for bi-interpretability, this follows from Proposition 3.2. Note that \( "(K^{\text{alg}}, \sigma)" \) is really the multisorted structure \((K_1, K_2, \ldots)\) where \( K_n \) is the degree \( n \) extension of \( K \). This can be interpreted in \( K \) by choosing a basis for each \( K_n \) and interpreting \( K_n \) as \( K_n \).

\[ \square \]

### 3.2 Definable sets

The following standard fact is an easy application of compactness:

**Fact 3.6.** Let \( \mathbb{M} \) be a monster model. Let \( A \subseteq \mathbb{M} \) be small. Let \( \mathcal{P} \) be a collection of \( A \)-definable subsets of \( \mathbb{M}^n \) closed under positive boolean combinations. Suppose the following holds:

For every \( a, b \in \mathbb{M}^n \), if

\[ \forall X \in \mathcal{P} : a \in X \implies b \in X, \]

then \( \text{tp}(a/A) = \text{tp}(b/A) \).

Then every \( A \)-definable subset of \( \mathbb{M}^n \) is in \( \mathcal{P} \).

We shall need the following geometric form of almost quantifier elimination. Recall that a morphism \( f : V_1 \to V_2 \) of \( K \)-varieties is quasi-finite if the fibers of the map \( V_1(K^{\text{alg}}) \to V_2(K^{\text{alg}}) \) are finite.

**Proposition 3.7.** Let \( (\mathbb{M}, \sigma) \) be a model of ACPF. Let \( (K_\infty, \sigma) \) be a non-degenerate substructure, with \( K_1 \) perfect. Let \( X \) be a \( K_\infty \)-definable subset of \( \mathbb{M}_1^n \). Then \( X \) is the image of \( V(\mathbb{M}_1) \to \mathbb{A}^n(\mathbb{M}_1) \) for some quasi-finite morphism \( V \to \mathbb{A}^n \) of \( K_1 \)-varieties.

**Proof.** Replacing \( \mathbb{M} \) with an elementary extension, we may assume \( \mathbb{M} \) is \( |K_\infty|^+ \)-saturated. Let \( \mathcal{P} \) be the class of definable subsets of \( \mathbb{M}_1^n \) of the specified form. We need to show that \( \mathcal{P} \) contains every \( K_\infty \)-definable subset of \( \mathbb{M}_1^n \).

Note that \( \mathcal{P} \) is closed under finite unions, because we can form coproducts \( V_1 \sqcup V_2 \) in the category of \( K_1 \)-varieties. Similarly, \( \mathcal{P} \) is closed under finite intersections, because of fiber products \( V_1 \times_{\mathbb{A}^n} V_2 \). Therefore, we can use Fact 3.6. Let \( a, b \) be two points in \( \mathbb{M}_1^n \). Suppose that for every \( X \in \mathcal{P} \),

\[ a \in X \implies b \in X. \]

We must show \( \text{tp}(a/K_\infty) = \text{tp}(b/K_\infty) \). Let \( (K_1(a)^{\text{alg}})_1 \) denote the fixed field of the periodic difference field \( K_1(a)^{\text{alg}} \subseteq \mathbb{M}_\infty \).
Claim 3.8. Let $c$ be an $m$-tuple from $(K_1(a)_{alg})_1$ and $\phi(x; y)$ be a quantifier-free $L_{rings}(K_1)$-formula such that $\phi(a; c)$ holds. Then there is an $m$-tuple $d$ from $\mathcal{M}_1$ such that $\phi(b; d)$ holds.

Proof. Strengthening $\phi(x; y)$, we may assume that

- $\phi(x; y)$ witnesses that $y \in K_1(x)^{alg}$.
- $\phi(\mathcal{M}_\infty)$ defines a locally closed subvariety $W$ of $\mathbb{A}^{n+m}$.

Then the projection $W \to \mathbb{A}^n$ is a quasi-finite morphism of varieties over $K_1$. Let $X \in \mathcal{P}$ be the image of $W(\mathcal{M}_1) \to \mathbb{A}^n(\mathcal{M}_1)$. Then

$$(a; c) \in W(\mathcal{M}_1) \implies a \in X \implies b \in X \implies (b; d) \in W(\mathcal{M}_1)$$

for some $m$-tuple $d \in \mathcal{M}_1$.

By saturation, the Claim holds even when $c$ is an infinite tuple and $\phi(x; y)$ is a type. Letting $c$ enumerate $(K_1(a)_{alg})_1$ and $\phi(x; y)$ be the complete type of $(a, c)$ over $K_1$, we obtain an embedding of fields

$$(K_1(a)_{alg})_1 \hookrightarrow \mathcal{M}_1$$

mapping $a$ to $b$ and $K_1$ to $K_1$ pointwise. By Lemma 3.1, we can apply the functor $- \otimes_{K_1} K_\infty$ and obtain an embedding of periodic fields

$$K_1(a)^{alg} \hookrightarrow \mathcal{M}_\infty$$

sending $a$ to $b$, and $K_\infty$ to $K_\infty$ pointwise. By Lemma 3.4, this is a partial elementary map, so $\text{tp}(a/K_\infty) = \text{tp}(b/K_\infty)$.

Claim

In Proposition 3.7, note that $\dim(V) \leq n$, because the geometric fibers of $V \to \mathbb{A}^n$ are finite.

Lemma 3.9. Let $K$ be a pseudofinite field, and $V$ be a 1-dimensional variety over $K$. In other words, $V(K^{alg})$ is 1-dimensional as a definable set in $K^{alg}$. Then there exist curves $^1 C_1, C_2, \ldots, C_n$ and a definable bijection between a cofinite subset of $V(K)$ and a cofinite subset of $\bigsqcup_{i=1}^n C_i(K)$.

Proof. Replacing $V$ with a closed subvariety, we may assume $V(K)$ is Zariski dense in $V(K^{alg})$. This ensures that the irreducible components of $V$ are geometrically irreducible. Let

$$V = D_1 \cup \cdots \cup D_n$$

be the decomposition of $V$ into irreducible components. Each $D_i$ is a 1-dimensional irreducible variety over $K$, hence has a unique smooth projective model $C_i$. Outside of finitely many exceptional points, there is a canonical bijection

$$D_1(K) \cup \cdots \cup D_n(K) \cong C_1(K) \sqcup \cdots \sqcup C_n(K).$$

^1Geometrically irreducible, smooth, and projective as always.
3.3 The theory of Frobenius periodic fields

Recall the Frobenius periodic fields $\text{Fr}_q^\infty = (\mathbb{F}_q^{\text{alg}}, \phi_q)$, where $\phi_q$ is the $q$th power Frobenius. There is an analogy

finite fields : pseudofinite fields :: Frobenius periodic fields : e.c. periodic fields.

Ax showed that a field $K$ is pseudofinite if and only if it is elementarily equivalent to a non-principal ultraproduct of finite fields. The analogous thing happens here.

**Definition 3.10.** $\widehat{\text{ACPF}}$ is the theory of periodic fields $K_\infty$ such that

1. $K_\infty \models \text{ACF}$
2. $K_\infty$ is non-degenerate
3. $K_1$ is a model of the theory $T_{\text{fin}}$ of finite fields.
4. If $K_1$ has size $q < \infty$, then $\sigma$ acts as the $q$th power Frobenius on $K_\infty$.

Ax showed that the models of $T_{\text{fin}}$ are exactly the finite and pseudofinite fields.

**Lemma 3.11.** The models of $\widehat{\text{ACPF}}$ are exactly

- Models of ACPF
- Frobenius periodic fields

**Proof.** If $(K_\infty, \sigma) \models \text{ACPF}$, then axioms (1) and (2) hold by definition, (3) holds because $K_1$ is pseudofinite by Proposition 3.5, and (4) is vacuous, as pseudofinite fields are infinite. If $(K, \sigma)$ is the $q$th Frobenius periodic field $\text{Fr}_q^q$, then all the axioms are trivial. Conversely, suppose $(K_\infty, \sigma) \models \widehat{\text{ACPF}}$. If $|K_1| = q < \infty$, then axiom (1) forces $K_\infty \cong \mathbb{F}_q^{\text{alg}}$ and axiom (4) forces $(K_\infty, \sigma) \cong \text{Fr}_q^q$. If $K_1$ is infinite, then (3) forces $K_1$ to be pseudofinite, hence PAC. Then (1) and (2) ensure $(K_\infty, \sigma) \models \text{ACPF}$. \qed

**Corollary 3.12.** If $(K_\infty, \sigma)$ is a non-principal ultraproduct of Frobenius periodic fields, then $(K_\infty, \sigma) \models \text{ACPF}$.

**Lemma 3.13.** If $(K_\infty, \sigma) \models \text{ACPF}$ and $K_\infty$ has characteristic 0, then $(K_\infty, \sigma)$ is elementarily equivalent to an ultraproduct of Frobenius periodic fields $\text{Fr}_p^p$ with $p$ prime.

**Proof.** For each prime $p$, let $\tilde{F}_p$ be the periodic field $(Q_{p,\text{un}}^\text{un}, \sigma)$, where $Q_{p,\text{un}}^\text{un}$ is the maximal unramified algebraic extension of $Q_p$, and $\sigma$ induces the $p$th power Frobenius on the residue field. By the Chebotarev density theorem, there is a non-principal ultraproduct $(\tilde{F}_p^*, \sigma)$ of $\tilde{F}_p$ such that

$$(\text{Abs}(\tilde{F}_p^*), \sigma) \cong (\text{Abs}(K), \sigma).$$
Now \( F^* \) has a \( \sigma \)-invariant valuation whose residue field is an ultraproduct \( F^* \) of Frobenius periodic fields \( \mathbb{F}_{p^q} \). Then \( F^* \) has characteristic 0, the valuation is equicharacteristic 0, and the residue map gives an isomorphism

\[
(\text{Abs}(F^*), \sigma) \cong (\text{Abs}(F^*), \sigma).
\]

By Lemma 3.14 and Corollary 3.12, \((K, \sigma) \equiv (F^*, \sigma)\).

**Lemma 3.14.** If \((K_\infty, \sigma) \models \text{ACPF} \) and \( K \) has characteristic \( p > 0 \), then \( K \) is elementarily equivalent to a non-principal ultraproduct of Frobenius periodic fields \( \mathbb{F}_{p^q} \), with \( q \) ranging over powers of \( p \).

**Proof.** Similar to Lemma 3.13 but easier (no valuations or Chebotarev). \(\square\)

**Proposition 3.15.**

1. A periodic field \((K, \sigma)\) is existentially closed if and only if it is elementarily equivalent to a non-principal ultraproduct of Frobenius periodic fields.

2. The elementary class generated by Frobenius periodic fields consists of the Frobenius periodic fields and existentially closed periodic fields.

3. \( \sim \text{ACPF} \) is the theory of Frobenius periodic fields.

Let \( T_{\text{prime}} \) be the theory of finite prime fields \( \mathbb{F}_p \). Ax showed that the models of \( T_{\text{prime}} \) are exactly the following:

- The finite prime fields \( \mathbb{F}_p \)
- The pseudofinite fields of characteristic 0.

Analogously, one can show:

**Proposition 3.16.**

1. A periodic field \((K, \sigma)\) is existentially closed of characteristic 0 if and only if it is elementarily equivalent to a non-principal ultraproduct of prime Frobenius periodic fields.

2. The elementary class generated by prime Frobenius periodic fields consists of:

   - Prime Frobenius periodic fields
   - Existentially closed periodic fields of characteristic 0

3. The theory of prime Frobenius periodic fields is axiomatized by \( \sim \text{ACPF} \) and the statement that \( K_1 \models T_{\text{prim}} \).

We leave the proof as an exercise to the reader.
4 Proof of the main theorem

4.1 The implicit definition

We will use the following forms of Beth implicit definability:

**Fact 4.1** (= Theorem 6.6.4 in [11]). Let $L^+ \supseteq L^-$ be languages. Let $T^-$ be an $L^-$ theory and $T^+$ be an $L^+$ theory extending $T^-$. Let $\phi(x)$ be an $L^+$ formula. Suppose that whenever $N \models T^-$, and $M^+_1$ and $M^+_2$ are two expansions of $N$ to a model of $T^+$, that $\phi(M^+_1) = \phi(M^+_2)$. Then there is an $L^-$-formula $\psi(x)$ such that $T^+ \vdash \phi \leftrightarrow \psi$.

**Corollary 4.2.** Let $L^+ \supseteq L^-$ be languages. Let $T^-$ be an $L^-$ theory and $T^+$ be an $L^+$ theory extending $T^-$. Suppose that

- $T^-$ is the theory of some (non-elementary) class $C$ of $L^-$-structures.
- Every model of $T^-$ has at most one expansion to a model of $T^+$.
- Every model in $C$ has at least one expansion to a model of $T^+$.

Then every model of $T^-$ has a unique expansion to a model of $T^+$, and $T^+$ is a definitional expansion of $T^-$. 

**Proof.** If $M \models T^-$, then $M$ is elementarily equivalent to an ultraproduct

$$M \equiv M' = \prod_{i \in I} M_i/U$$

of structures $M_i \in C$. Each $M_i$ can be expanded to a model of $T^+$, so the same holds for the ultraproduct $M'$. By Fact 4.1 and the assumptions, the $T^+$-structure on $M'$ is 0-definable from the $T^-$-structure. Therefore the $T^+$-structure transfers along the elementary equivalence $M' \equiv M$, giving a $T^+$-structure on $M$. So every model of $T^-$ expands to a model of $T^+$ in a unique way. By Fact 4.1, $T^+$ is a definitional expansion of $T^-$. □

We will apply both versions of implicit definability in the following context:

- The language $L^-$ is the language of periodic fields.
- The theory $T^-$ is $\widehat{\text{ACPF}}$, the theory of Frobenius periodic fields as in §3.3
- $C$ is the class of Frobenius periodic fields.
- The language $L^+$ is the expansion of $L^-$ by a new predicate $P_{\phi,n,k}(\bar{y})$ for every formula $\phi(\bar{x}; \bar{y}) \in L^-$, every $n \in \mathbb{N}$, and every $k \in \mathbb{Z}/n\mathbb{Z}$.

The theory $T^+$ is $T^-$ plus the following axioms:

1. For every $\phi$, $n$, and $b$, there is a unique $k \in \mathbb{Z}/n\mathbb{Z}$ such that $P_{\phi,n,k}(b)$ holds.
2. If \( \phi(K; b) = \phi'(K; b') \), then
\[
P_{\phi,n,k}(b) \iff P_{\phi',n,k}(b').
\]

3. If \( X \) is a definable set \( \phi(K; b) \), let \( \chi_n(X) \) denote the unique \( k \) such that \( P_{\phi,n,k}(b) \) holds.
(This is well-defined by (1) and (2).) Then \( \chi_n \) is a strong Euler characteristic for each \( n \).

4. The diagram
\[
\begin{array}{c}
\text{Def}(M) \\
\xrightarrow{\chi_n} \mathbb{Z}/n\mathbb{Z} \\
\downarrow \quad \downarrow \\
\mathbb{Z}/m\mathbb{Z} \\
\chi_m \\
\end{array}
\]

commutes when \( m \) divides \( n \).

5. Let \( C \) be a genus-\( g \) curve over \( K_1 \), and let \( J \) be its Jacobian. Let \( p^k \) be a prime power. Let \( h \) be the function from Corollary 2.13. If \( \text{char}(K) \neq p \) or if \( |K_1| > h(g, p, k) \), then \( \chi_{p^k}(C(K_1)) \) is given by the formula
\[
\chi_{p^k}(C(K_1)) = 1 - \text{Tr}(\sigma|J[p^k]) + \text{Tr}(\sigma|G_m[p^k]).
\]

Here, if \( G \) is a commutative group variety over \( K_1 \), then \( \text{Tr}(\sigma|G[n]) \) denotes the trace of the action of \( \sigma \) on the group of \( n \)-torsion in \( G(K_\infty) \).

Axioms 1-4 encode the statement that \( \chi \) is a \( \hat{\mathbb{Z}} \)-valued strong Euler characteristic, and Axiom 5 determines its value on curves. We discuss why Axiom 5 is first-order in \( \mathfrak{s}5 \).

### 4.2 Uniqueness

The “existence” part of Corollary 4.2 has already been verified:

**Proposition 4.3.** If \( \text{Fr}^q \) is a Frobenius periodic field, and \( \chi \) is the counting Euler characteristic, then \( \chi \) satisfies \( T^+ \). In particular, \( \text{Fr}^q \) admits an expansion to a model of \( T^+ \).

**Proof.** Examining the definition of \( T^+ \), axioms (1)-(4) merely say that \( \chi \) is a \( \hat{\mathbb{Z}} \)-valued strong Euler characteristic, which is trivial. Axiom (5) holds by Corollaries 2.4 and 2.13.

Therefore, it remains to prove the “uniqueness” part. Our goal is to show that on any \( (K, \sigma) \models \widehat{\text{ACP}} \), there is at most one \( \hat{\mathbb{Z}} \)-valued Euler characteristic satisfying the axioms of \( T^+ \). Until Proposition 4.7, we will restrict our attention to models of \( \text{ACP} \).

**Remark 4.4.** In Axiom 5 of \( T^+ \), the condition \( |K_1| > h(g, p, k) \) is automatic when \( K_1 \) is infinite, i.e., when \( (K_\infty, \sigma) \models \text{ACP} \). Therefore, for models of \( \text{ACP} \), Axiom 5 says the following: for any curve \( C \) over \( K_1 \) with Jacobian \( J \),
\[
\chi_{p^k}(C(K_1)) = 1 - \text{Tr}(\sigma|J[p^k]) + \text{Tr}(\sigma|G_m[p^k]).
\]

By the Chinese remainder theorem, this formula determines \( \chi_n(C) \) for any \( n \).
Lemma 4.5. Let $(K_\infty, \sigma)$ be a model of ACPF, admitting two expansions to a model of $T^+$. Let $\chi$ and $\chi'$ be the corresponding $\hat{\mathbb{Z}}$-valued strong Euler characteristics. Then $\chi(X) = \chi'(X)$ for every unary definable set $X \subseteq K_1$.

Proof. Say that a definable set is good if $\chi(X) = \chi'(X)$. Finite sets are good. If $X$ is in definable bijection with $Y$ and $X$ is good, then so is $Y$. A disjoint union of two good sets is good. If $S$ is a cofinite subset of $X$, then $S$ is good if and only if $X$ is good. Consequently, if a cofinite subset of $X$ is in definable bijection with a cofinite subset of $Y$, then $X$ is good if and only if $Y$ is good.

If $C$ is a curve over $K_1$, then $C(K_1)$ is good, by Remark 4.4. Any disjoint union of sets of this form is also good. By Lemmas 3.9, the set $V(K_1)$ is good for any 1-dimensional variety $X$ over $K_1$.

Now let $X$ be a definable subset of $(K_1)^1$. By Proposition 3.7, $X$ is the image of $V_1(K_1) \to \mathbb{A}^1(K_1)$ for some morphism $V_1 \to \mathbb{A}^1$ of $K_1$-varieties with geometrically finite fibers. Let $V_n$ denote the $n$-fold fiber product

$$V_1 \times_{\mathbb{A}^1} V_1 \times_{\mathbb{A}^1} \cdots \times_{\mathbb{A}^1} V_1,$$

$n$ times

Each of the morphisms $V_n \to \mathbb{A}^1$ has geometrically finite fibers, so each variety $V_n$ is 1-dimensional. Hence each set

$$Y_n := V_n(K_1)$$

is good. Note that $Y_n$ is the $n$-fold fiber product of $Y_1$ over $X$.

Let $m$ be a bound on the size of the fibers of $Y_1 \to X$. For $1 \leq k \leq m$, let $X_k$ denote the set of $a \in X$ such that $f^{-1}(a)$ has size $m$. Let $\alpha_k$ and $\beta_k$ denote $\chi(X_k)$ and $\chi'(X_k)$.

Because $\chi$ and $\chi'$ are strong Euler characteristics,

$$\chi(Y_n) = \sum_{k=1}^{m} \alpha_k k^n$$

$$\chi'(Y_n) = \sum_{k=1}^{m} \beta_k k^n$$

for all $n$. As the $Y_n$’s are good,

$$\sum_{k=1}^{m} \alpha_k k^n = \sum_{k=1}^{m} \beta_k k^n$$

for $n = 1, \ldots, m$. By invertibility of the Vandermonde matrix $\langle k^n \rangle_{1 \leq k \leq m, 1 \leq n \leq m}$, and the fact that $\hat{\mathbb{Z}}$ has no $\mathbb{Z}$-torsion, it follows that $\alpha_k = \beta_k$ for all $k$. Consequently,

$$\chi(X) = \sum_{k=1}^{m} \alpha_k = \sum_{k=1}^{m} \beta_k = \chi'(X).$$

Therefore $X$ is good. \qed
Lemma 4.6. For any $n$, the following statements are true:

$(S_n)$ Let $(K_\infty, \sigma)$ be a model of $ACPF$, admitting two expansions to a model of $T^+$. Let $\chi$ and $\chi'$ be the corresponding $\hat{\mathbb{Z}}$-valued strong Euler characteristics. Then $\chi(X) = \chi'(X)$ for every definable subset $X \subseteq (K_1)^n$.

$(T_n)$ If $(K_\infty, \sigma)$ is a model of $ACPF$, admitting an expansion to a model of $T^+$, and $\chi$ is the corresponding $\hat{\mathbb{Z}}$-valued strong Euler characteristic, then for every definable family $\{X_a\}_{a \in Y}$ of subsets of $(K_1)^n$, for every $m \in \mathbb{N}$ and for every $k \in \mathbb{Z}/m\mathbb{Z}$, the set

$$\{ a \in Y(K) : \chi(X_a) \equiv k \pmod{m} \}$$

is definable in the $L^-$-reduct $(K_\infty, \sigma)$.

Proof. Statement $S_1$ is Lemma 4.5. The implication $S_n \implies T_n$ follow by Beth implicit definability. It suffices to show

$$(S_1 \text{ and } S_n \text{ and } T_n) \implies S_{n+1}.$$ 

Assume the left hand side. Let $(K_\infty, \sigma), \chi, \chi'$ and $X \subseteq K_1 \times (K_1)^n$ be as in the statement of $S_{n+1}$. Fix $m \in \mathbb{N}$; we claim $\chi_m(X) = \chi'_m(X)$. For $t \in K_1$, let

$$X_t = \{ \bar{x} \in (K_1)^n : (t, \bar{x}) \in X \}$$

By statements $S_n$ and $T_n$, the sets

$$Y_k = \{ t \in K_1 : \chi(X_t) \equiv k \pmod{m} \}$$

$$Y'_k = \{ t \in K_1 : \chi'(X_t) \equiv k \pmod{m} \}$$

are equal and definable. Because $\chi$ and $\chi'$ are strong Euler characteristics,

$$\chi_m(X) = \sum_{k \in \mathbb{Z}/m\mathbb{Z}} k \cdot \chi_m(Y_k)$$

$$\chi'_m(X) = \sum_{k \in \mathbb{Z}/m\mathbb{Z}} k \cdot \chi'_m(Y'_k).$$

Then $\chi_m(Y_k) = \chi'_m(Y_k)$ by statement $S_1$, so putting things together, $\chi_m(X) = \chi'_m(X)$. As $m$ was arbitrary, $S_n$ holds.

Proposition 4.7. If $(K, \sigma)$ is a model of $\overline{ACPF}$, then there is at most one expansion of $(K, \sigma)$ to a model of $T^+$.

Proof. If $(K, \sigma)$ is a Frobenius periodic field, then $K_\infty$ is essentially finite and there is at most one $\hat{\mathbb{Z}}$-valued Euler characteristic. So assume $(K_\infty, \sigma) \models ACPF$. Let $\chi, \chi'$ be two $\hat{\mathbb{Z}}$-valued Euler characteristics satisfying $T^+$. Note that the sort $K_n$ is in definable bijection with $(K_1)^n$. If $X$ is any definable set in $K_\infty$, then $X$ is therefore in definable bijection with a definable subset $Y \subseteq (K_1)^m$ for some $m$. By statement $S_m$ of Lemma 4.6,

$$\chi(X) = \chi(Y) = \chi'(Y) = \chi'(X).$$
By Corollary 4.2 and Proposition 4.3, we conclude

**Proposition 4.8.** If \((K, \sigma)\) is a model of \(\widetilde{\text{ACPF}}\), then there is a unique expansion of \((K, \sigma)\) to a model of \(T^+\).

**Theorem** (Theorem 1.4). Let \(\mathcal{C}\) be the class of Frobenius periodic fields and existentially closed periodic fields. There is a \(\hat{\mathbb{Z}}\)-valued strong Euler characteristic \(\chi\) on \((K, \sigma)\) in \(\mathcal{C}\) with the following properties:

- \(\chi\) is uniformly 0-definable across \(\mathcal{C}\).
- If \((K, \sigma)\) is a Frobenius periodic field, then \(\chi\) is the counting Euler characteristic:
  \[
  \chi(X) = |X|.
  \]
- If \((K, \sigma)\) is an ultraproduct of Frobenius periodic fields, then \(\chi\) is the nonstandard counting Euler characteristic.

**Definition 4.9.** The canonical Euler characteristic on \((K, \sigma)\) is the \(\hat{\mathbb{Z}}\)-valued Euler characteristic of Theorem 1.4.

**Remark 4.10.** The canonical Euler characteristic \(\chi\) is the only \(\hat{\mathbb{Z}}\)-valued Euler characteristic that is uniformly 0-definable across all models of \(\widetilde{\text{ACPF}}\). Indeed, if \(\chi'\) is another uniformly definable Euler characteristic, and

\[
\chi(\phi(K; b)) \neq \chi'(\phi(K; b))
\]

for some model \(K\) and tuple \(b\), then \(K\) is elementarily equivalent to an ultraproduct of Frobenius periodic fields, so we can in fact take \(K\) to be a Frobenius periodic field. But Frobenius periodic fields are essentially finite, so \(\chi\) and \(\chi'\) must agree on \(K\), a contradiction.

**Remark 4.11.** There are other uniformly 0-definable \(\hat{\mathbb{Z}}\)-valued strong Euler characteristics on \(\text{ACPF}\). For example,

\[
(K_\infty, \sigma) \models \text{ACPF} \implies (K_\infty, \sigma^{-1}) \models \text{ACPF},
\]

and the canonical Euler characteristic on \((K_\infty, \sigma^{-1})\) induces a non-canonical Euler characteristic on \((K_\infty, \sigma)\). We shall have more to say about this in §7.3.

### 5 An interlude on definability and computability

This section discusses some of the technical issues related to Axiom 5 in the definition of \(T^+\). If one is willing to sweep these issues under the rug, this section can be skipped.

**Lemma 5.1.** In the definition of \(T^+\), Axiom 5 is expressible by first-order sentences.
Proof sketch. The assertion

\( J \) is the Jacobian of \( C \)

can be expressed as

\( J \) is a smooth projective group variety that is birationally equivalent (over \( K_1 \)) to \( \text{Sym}^g C \), the \( g \)th symmetric product of \( C \).

Indeed, the Jacobian is a smooth projective group variety because it is an abelian variety, and it is birationally equivalent to \( \text{Sym}^g C \) by the construction of the Jacobian in §V.1 of [22]. By Theorem I.3.8 in [19], any birational map between two projective group varieties extends to an isomorphism.

Even the following statement is rather non-trivial to express:

\( C \) is a (smooth projective) curve of genus \( g \)

Smoothness can be witnessed by covering projective space with Zariski open patches on which \( C \) is cut out by a system of equations whose matrix of partial derivatives has rank no higher than the codimension of \( C \). Geometric irreducibility can be witnessed as in the appendix of [8]. Genus can be determined by counting zeros and poles on a meromorphic section of the tangent bundle.

Hopefully, everything will be spelled out in greater detail in [14].

By being more careful, one can presumably show that the theory \( T^+ \) is not only first-order, but recursively axiomatized. We have gone too far out on a limb, so we state this as a conjecture:

**Conjecture 5.2.** In the language of \( T^+ \), there are sentences \( \tau_{g,p^k,n} \) depending recursively on the parameters, such that the following are equivalent for any \( g \geq 1 \), any prime power \( p^k \), and any structure \( (K_\infty, \sigma, \chi) \) satisfying \( \text{ACPF} \) and Axioms [4.7] of \( T^+ \):

1. \( (K_\infty, \sigma, \chi) \) satisfies \( \bigwedge_{n=1}^\infty \tau_{g,p^k,n} \).
2. For every genus \( g \) curve \( C \) over \( K_1 \) with Jacobian \( J \),

\[
\chi_{p^k}(C(K_1)) = 1 - \text{Tr}(\sigma|J[p^k]) + \text{Tr}(\sigma|\mathbb{G}_m[p^k]).
\]

**Lemma 5.3.** (Assuming Conjecture 5.2) The theory \( \widehat{\text{ACPF}} \) of §3.3 and the theory \( T^+ \) of §4.7 are recursively axiomatized.

**Proof.** For \( \widehat{\text{ACPF}} \), this is mostly clear. Axiom [3] saying that \( K_1 \) is a model of the theory of finite fields, is recursively axiomatized by Ax’s theorem on the decidability of the theory of finite fields.

The additional axioms of \( T^+ \) are plainly recursively enumerable, except for Axiom [3] which can be expressed by Conjecture 5.2. \( \square \)
Conjecture 5.2 is almost certainly true, by the method of Lemma 5.1. To “prove” Conjecture 5.2, we seemingly have three options:

1. A precise proof in terms of indexed families of formulas.
2. An informal “proof” in the style of Lemma 5.1.
3. A clever proof using subtle facts from algebraic geometry.

There is something deeply unsatisfying about each of these approaches. Approach 1 is extremely tedious; writing out the details would probably double the length of this paper. Moreover, the details would be an incomprehensible stew of indexed families of multi-variable formulas. For example, the statement that underlies Conjecture 5.2 is (almost) the following:

**Conjecture 5.4.** There are formulas $\phi_{n,g}(\bar{x}), \psi_{n,g}(\bar{x}, \bar{y}), \rho_{n,g}(\bar{x}, \bar{z})$ depending recursively on $n$ and $g$ such that for any perfect field $K$ and any $g$, if $X,Y$ are two definable sets, then the following are equivalent:

1. There is a genus-$g$ curve $C/K$ with Jacobian $J$, such that $X$ is in definable bijection with $C(K)$ and $Y$ is in definable bijection with $J(K)$.
2. There is some $n \in \mathbb{N}$ and some $\bar{a} \in \phi_{n,g}(K)$ such that $X$ is in definable bijection with $\psi_{n,g}(\bar{a}, K)$ and $Y$ is in definable bijection with $\rho_{n,g}(\bar{a}, K)$.

A proof written in this style would be nearly unreadable.

In contrast, Approach 2 is excessively informal. It is hard to convince oneself that Lemma 5.1 is really a proof of Conjecture 5.2, especially when one compares the relative lengths of the informal proof and the precise proof.

What seems to be missing is a language that would assign precise meaning to statements like the following:

- $\mathbb{P}^n$ depends nicely on $n$.
- The family of Zariski closed sets in $\mathbb{P}^n$ depends nicely on $n$.
- The family of smooth irreducible varieties of dimension $d$ depends nicely on $d$.
- If $C$ is a curve, the family of meromorphic functions $C \to \mathbb{P}^1$ depends nicely on $C$.
- If $C$ is a curve, if $f : C \to \mathbb{P}^1$ is meromorphic, and if $x \in C$, then the zero/pole-order of $f$ at $x$ depends nicely on $C,f,x$.
- The family of curves of genus $g$ depends nicely on $g$.
- If $C$ is a curve, then the Jacobian of $C$ depends nicely on $C$. 

27
Here, “nicely” is supposed to mean something like “recursively ind-definable, uniformly across all models.”

In future work ([14]), I hope to develop a toolbox that makes this notion precise, enabling a smoother proof of Conjecture 5.2. My hope is that this toolbox will be useful in other situations where one needs to verify the recursive axiomatizability of conditions from algebraic geometry.

Finally, we consider Approach 3—using clever tricks from algebraic geometry to simplify the problem. This approach probably works, but is conceptually unsatisfying. It should be possible to translate the informal proof into a precise proof that is not too long. It shouldn’t be necessary to resort to non-elementary facts from algebraic geometry to overcome a syntactic problem.

Remark 5.5. An analogous situation appears when one verifies that the theory of PAC fields is recursively axiomatized. The standard approach is to use Bertini’s theorem to reduce to the case of curves, and then project into the plane to reduce to the case of plane curves (see §10.2 in [9]). This is an instance of Approach 3.

6 Further results

6.1 Uniform definability of the counting Euler characteristic

Theorem [14] implies that the counting Euler characteristic is uniformly definable across all Frobenius periodic fields. This can be restated more explicitly as follows:

**Corollary 6.1.** For any formula $\phi(x; y)$ in the language of periodic fields, any $n \in \mathbb{N}$, and any $k \in \mathbb{Z}/n\mathbb{Z}$, there is a formula $\psi_{\phi,n,k}(y)$ such that for any Frobenius periodic field $\text{Fr}^q$ and any tuple $b$ from $\text{Fr}^q$,

$$\text{Fr}^q \models \psi_{\phi,n,k}(b) \iff |\phi(\text{Fr}^q; b)| \equiv k \pmod{n}$$

6.2 Evaluation on curves

**Proposition 6.2.** Let $(K_\infty, \sigma)$ be a model of ACPF. Let $C$ be a curve over $K_1$, and $J$ be the jacobian. For any prime $\ell$ (possibly the characteristic), the $\ell$-adic component of $\chi(C(K_1))$ is determined by the trace of the action of $\sigma$ on the $\ell$-adic Tate modules of $J$ and the multiplicative group $\mathbb{G}_m$:

$$1 - \text{Tr}(\sigma|T_\ell J) + \text{Tr}(\sigma|T_\ell \mathbb{G}_m).$$

**Proof.** This follows directly from Axiom 5 of $T^+$, and Remark 4.4. □

For $\ell \neq \text{char}(K)$, there should be a generalization using $\ell$-adic etale cohomology:
Conjecture 6.3. Let \((K_\infty, \sigma)\) be a model of ACPF, let \(V\) be a smooth projective variety over \(K_1\), and let \(\ell\) be a prime different from the characteristic. Then the \(\ell\)-adic component of \(\chi(V(K_1))\) is given by the formula
\[
2 \dim(V) \sum_{i=0}^{2 \dim(V)} (-1)^i \text{Tr}(\sigma^{-1}|H^i(V; \mathbb{Q}_\ell)),
\]
where \(H^i(V; \mathbb{Q}_\ell)\) denotes the \(\ell\)-adic cohomology:
\[
\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \lim_k H^i_{et}(V \times_{K_1} K_\infty; \mathbb{Z}/\ell^k).
\]

I suspect that Conjecture 6.3 is trivial with the right tools. If I understand correctly, the conjecture holds for Frobenius periodic fields, because of Grothendieck’s cohomological approach to the Weil conjectures (described in Hartshorne [10], Appendix C, §3-4). As long as Conjecture 6.3 can be stated as a conjunction of first-order sentences, it transfers to models of ACPF by Proposition 3.15. Thus, the only thing needing verification is that the groups \(H^i_{et}(V; \mathbb{Z}/\ell^k)\) depend definably on \(V\).

Remark 6.4. There should be a more general form of Conjecture 6.3 for arbitrary varieties, using cohomology with compact supports or intersection homology.

6.3 Pseudofinite fields

Lemma 6.5. Let \(K\) be a pseudofinite field and \(\sigma\) be a topological generator of \(\text{Gal}(K)\). The canonical \(\hat{\mathbb{Z}}\)-valued definable strong Euler characteristic on \((K^{\text{alg}}, \sigma)\) restricts to an \(\text{acl}^{\text{eq}}(0)\)-definable strong Euler characteristic on \(K\).

Proof. The structure \((K^{\text{alg}}, \sigma)\) and the field \(K\) have equivalent categories of (parametrically) definable sets, by the bi-interpretability of Proposition 3.5. Therefore, the definable strong Euler characteristic on \((K^{\text{alg}}, \sigma)\) determines a definable strong Euler characteristic \(\chi'\) on \(K\).

To prove \(\text{acl}^{\text{eq}}(0)\)-definability of \(\chi'\), we may pass to an elementary extension and assume \(K\) and \((K^{\text{alg}}, \sigma)\) are monster models. The Euler characteristic \(\chi'\) is not determined in an \(\text{Aut}(K)\)-invariant way, because of the choice of \(\sigma\). However, there are only boundedly many choices for \(\sigma\). Therefore \(\chi'\) has only boundedly many conjugates under \(\text{Aut}(K)\), so \(\chi'\) is \(\text{acl}^{\text{eq}}(0)\)-definable.

Theorem (Theorem 1.1).

1. Let \(K = \prod_i K_i / \mathcal{U}\) be an ultraproduct of finite fields. Then the nonstandard counting functions \(\chi_n\) are \(\text{acl}^{\text{eq}}(0)\)-definable.

2. Every pseudofinite field admits an \(\text{acl}^{\text{eq}}(0)\)-definable \(\hat{\mathbb{Z}}\)-valued strong Euler characteristic.
Proof. Part 2 is Lemma 6.5. For part 1, given an ultraproduct
\[ K = \prod_i \mathbb{F}_q / \mathcal{U}, \]
let \((L, \sigma) = \prod_i \text{Fr}_q / \mathcal{U}\) be the corresponding ultraproduct of Frobenius periodic fields. Then \(K \cong L_1\). The nonstandard counting functions on \(K\) are induced by the canonical Euler characteristic on \((L_\infty, \sigma)\). Therefore the nonstandard counting functions on \(K\) are \(\text{acl}^\text{eq}(0)\)-definable, by Lemma 6.5.

### 6.4 Elimination of parity quantifiers

For any \(n \in \mathbb{N}\) and \(k \in \mathbb{Z}/n\mathbb{Z}\), let \(\mu^n_k x\) be a new quantifier. Interpret \(\mu^n_k x : \phi(x)\) in finite structures as

The number of \(x\) such that \(\phi(x)\) holds is congruent to \(k \mod n\).

In other words,

\[
\left( M \models \mu^n_k \vec{x} : \phi(\vec{x}, \vec{b}) \right) \iff \left( |\{\vec{a} : M \models \phi(\vec{a}, \vec{b})\}| \equiv k \pmod{n} \right).
\]

For example,

- \(\mu^n_0 x\) means “there are an even number of \(x\) such that…”
- \(\mu^n_1 x\) means “there are an odd number of \(x\) such that…”

We call \(\mu^n_k\) generalized parity quantifiers.

Let \(\mathcal{L}^\mu_{\text{rings}}\) and \(\mathcal{L}^\mu_{\text{pf}}\) be the language of rings and the language of periodic fields, respectively, expanded with generalized parity quantifiers.

**Proposition 6.6** (= Theorem 1.5.1). Frobenius periodic fields uniformly eliminate generalized parity quantifiers. If \(\phi(\vec{x})\) is a formula in \(\mathcal{L}^\mu_{\text{pf}}\), then there is a formula \(\phi'(\vec{x}) \in \mathcal{L}_{\text{pf}}\) such that for any Frobenius periodic field \(\text{Fr}^q\) and any tuple \(\vec{a}\),

\[
\text{Fr}^q \models \phi(\vec{a}) \iff \text{Fr}^q \models \phi'(\vec{a}).
\]

**Proof.** Proceed by induction on the complexity of \(\phi(\vec{x})\). We may assume \(\phi(\vec{x})\) has the form

\[
\mu^n_k \vec{y} : \psi(\vec{x}, \vec{y}),
\]

for some formula \(\psi(\vec{x}, \vec{y}) \in \mathcal{L}_{\text{pf}}\). In this case, we can eliminate \(\mu^n_k\) by Corollary 6.1.

**Example 6.7.** The \(\mathcal{L}^\mu_{\text{pf}}\)-sentence

\[
\tau \overset{\text{def}}{=} \mu^5_2 x \in K_1 : x = x
\]

is equivalent in Frobenius periodic fields \(\text{Fr}^q\) to the \(\mathcal{L}_{\text{pf}}\)-sentence

\[
\tau' \overset{\text{def}}{=} 5 \neq 0 \land \forall x \in K_4 : (x^5 = 1 \rightarrow \sigma(x) = x^2).
\]

To see this, break into cases according to the congruence class of \(q\) modulo 5. Note that \(\text{Fr}^q \models \tau \iff q \equiv 2 \pmod{5}\).
• If \( q \equiv 0 \pmod{5} \), then \( \mathrm{Fr}^q \) has characteristic 5, so \( \tau' \) and \( \tau \) are both false.

• If \( q \equiv 2 \pmod{5} \), then \( \mathrm{Fr}^q \) does not have characteristic 5, and

\[
\forall x \in K_\infty : (x^5 = 1 \rightarrow x^q = x^2),
\]

so \( \tau \) and \( \tau' \) are both true.

• If \( q \equiv j \pmod{5} \) for \( j \neq 0, 2 \), then \( \mathrm{Fr}^q \) does not have characteristic 5. Let \( x \) be a primitive fifth root of unity. Then \( x \in K_4 \), because \( \text{Gal}(K_1(x)/K_1) \) is a subgroup of \((\mathbb{Z}/5\mathbb{Z})^\times\). Also,

\[
x^q = x^j \neq x^2,
\]

and so \( \tau' \) is false.

In contrast to Proposition 6.6, generalized parity quantifiers are not eliminated in finite fields:

**Lemma 6.8.** There is no \( \mathcal{L}_{\text{rings}} \)-sentence \( \rho \) equivalent to the following \( \mathcal{L}_{\text{rings}}^\mu \)-sentence in every finite field:

\[
\mu_5 5x : x = x.
\]

**Proof.** Suppose \( \rho \) exists. Then the following are equivalent for any model \((K_\infty, \sigma) \models \text{ACPF}:

• \( K_1 \) satisfies \( \rho \)

• \( K_\infty \) does not have characteristic 5, and the action of \( \sigma \) on the fifth roots of unity is given by

\[
\sigma(\omega) = \omega^2.
\]

Now take \((K_\infty, \sigma)\) satisfying ACPF and the two equivalent conditions. (For example, we can take \( K_\infty \) to be a non-principal ultraproducet of \( \mathrm{Fr}^p \) where \( p \) ranges over primes congruent to 2 mod 5. A non-principal ultrafilter exists by Dirichlet’s theorem.) Then \( K_1 \) satisfies \( \rho \), and \( \sigma \) acts on the fifth roots of unity by squaring. Consider a dual model

\[
(K_\infty^\dagger, \sigma) \cong (K_\infty, \sigma^{-1}).
\]

From the axioms of ACPF, it is clear that \((K_\infty^\dagger, \sigma) \models \text{ACPF} \). Since \( \sigma \) acts on fifth roots by squaring, \( \sigma^{-1} \) acts by cubing:

\[
\sigma^{-1}(\omega) = \omega^3,
\]

as 2 and 3 are multiplicative inverses modulo 5. So \((K_\infty^\dagger, \sigma)\) does not satisfy the two equivalent conditions, and in particular, \( K_1^\dagger \not\models \rho \). But this is absurd, since \( K_1^\dagger \) is isomorphic as a field to \( K_1 \).

**Remark 6.9.** The proof of Lemma 6.8 actually proves something stronger: parity quantifiers are not eliminated on the class of prime fields \( \mathbb{F}_p \). The non-elimination of parity quantifiers in finite fields was originally proven in [17], Theorem 7.3, using a slightly different method.
6.5 Decidability

Recall the theory $T^+$ of §4.1. For the rest of this section, we assume Conjecture 5.2.

Lemma 6.10. (Assuming Conjecture 5.2) There is a computable function which takes a formula $\phi(\bar{x})$ in the language of $T^+$ and outputs a formula $\phi'(\bar{x})$ in the language of periodic fields, such that $T^+ \vdash \phi \iff \phi'$.

Proof. By Lemma 5.3 the theory $\widetilde{ACP}$ of §3.3 and the theory $T^+$ of §4.1 are recursively axiomatized.

For each $\phi$, an equivalent formula $\phi'$ exists by Beth implicit definability (Fact 4.1) and the existence and uniqueness of the expansion to $T^+$ (Proposition 4.8). An algorithm can find $\phi'$ by searching all consequences of $T^+$ until it finds one of the form

$$\forall \bar{x} : \phi(\bar{x}) \leftrightarrow \phi'(\bar{x})$$

with $\phi'$ a formula in the pure language of periodic fields.

Corollary 6.11. (Assuming Conjecture 5.2)

1. In Corollary 6.1, the formula $\psi_{\phi,n,k}$ can be chosen to depend computably on $\phi$.

2. In Proposition 6.6, the elimination of generalized parity quantifiers can be carried out computably—the formula $\phi'$ can be chosen to depend computably on $\phi$.

Proof.

1. Corollary 6.1 is an instance of Lemma 6.10 so the conversion can be done computably.

2. As in the proof of Proposition 6.10 one converts a $L^\mu_{pf}$-formula into a pure $L_{pf}$-formula by recursion on the formula.

Theorem (Theorems 1.5.2 and 1.2). (Assuming Conjecture 5.2)

1. The $L^\mu_{pf}$-theory of Frobenius periodic fields is decidable.

2. The $L^\mu_{rings}$-theory of finite fields is decidable.

Proof. First note that the ($L_{pf}$-)theory of Frobenius periodic fields is decidable. By Proposition 3.15 the theory is completely axiomatized by $\widetilde{ACP}$. Therefore, the theory is computably enumerable. The theory is also co-computably enumerable. Indeed, a sentence $\tau$ is not part of the theory if and only if $F_{Fr}^q \models \neg \tau$ for some $q$. There is an algorithm taking $q$ and $\tau$ and outputting whether or not $F_{Fr}^q \models \tau$, because $F_{Fr}^q$ is essentially finite. So we can enumerate all the statements that fail in some Frobenius periodic field, which is the complement of the theory of Frobenius periodic fields. Thus the theory of Frobenius periodic fields is decidable, as claimed.

32
Now given a \( L^\mu_{\text{pf}} \)-sentence \( \tau \), we can computably convert it into an equivalent \( L^\mu_{\text{pf}} \)-sentence \( \tau' \), and use the previous paragraph to computably determine whether or not \( \tau' \) holds in every Frobenius periodic field. This proves the first point.

The second point follows, because there is a computable way to convert an \( L^\mu_{\text{rings}} \)-sentence \( \tau \) into a \( L^\mu_{\text{pf}} \)-sentence \( \tau' \) such that

\[
(K_\infty, \sigma) \models \tau' \iff K_1 \models \tau
\]

for any essentially finite periodic field \((K_\infty, \sigma)\). Taking \( K_\infty \) to be \( \text{Fr}_q \), we see that

\[
\text{Fr}_q \models \tau' \iff \mathbb{F}_q \models \tau.
\]

Therefore, \( \tau \) holds in every finite field if and only if \( \tau' \) holds in every Frobenius periodic field. Then we can apply the oracle for the first point to \( \tau' \).

\[\Box\]

7 Mock-finite fields

Recall that \( \text{Abs}(K) \) denotes the substructure of absolute numbers of \( K \)—the elements algebraic over the prime field.

**Definition 7.1.** A field \( K \) is mock-finite if \( K \) is pseudofinite and \( \text{Abs}(K) \) is finite.

We will see that mock-finite fields admit particularly nice Euler characteristics.

**Definition 7.2.** A field \( K \) is a mock-\( \mathbb{F}_q \) if \( K \) is pseudofinite and \( \text{Abs}(K) \cong \mathbb{F}_q \).

Note that \( K \) is mock-finite if and only if \( K \) is a mock-\( \mathbb{F}_q \) for some \( q \).

**Lemma 7.3.** Let \( K \) be a mock-\( \mathbb{F}_q \). Then the restriction homomorphism

\[
\text{Gal}(K) \to \text{Gal}(\mathbb{F}_q)
\]

is an isomorphism. Consequently, there is a unique topological generator \( \sigma \in \text{Gal}(K) \) extending the \( q \)th power Frobenius \( \phi_q \in \text{Gal}(\mathbb{F}_q) \).

**Proof.** The restriction homomorphism is surjective because \( \mathbb{F}_q \) is relatively algebraically closed in \( K \). Both Galois groups are isomorphic to \( \hat{\mathbb{Z}} \), and any continuous surjective homomorphism \( \hat{\mathbb{Z}} \to \hat{\mathbb{Z}} \) is an isomorphism. \[\Box\]

**Definition 7.4.** If \( K \) is a mock-\( \mathbb{F}_q \), the mock Frobenius automorphism is the unique \( \sigma \in \text{Gal}(K) \) extending the \( q \)th-power Frobenius \( \phi_q \in \text{Gal}(\mathbb{F}_q) \).

If \( p \) is a prime, let \( \mathbb{Z}_{-p} \) be the prime-to-\( p \) completion of \( \mathbb{Z} \):

\[
\mathbb{Z}_{-p} = \lim_{\substack{n \to \infty \atop (n,p)=1}} \mathbb{Z}/n\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_\ell.
\]
**Definition 7.5.** Let $K$ be a mock-finite field, and $\sigma$ be the mock Frobenius automorphism.

1. The *principal Euler characteristic* on $K$ is the $\mathbb{Z}_{-p}$-valued Euler characteristic induced by $\sigma$.

2. The *dual Euler characteristic* on $K$ is the $\mathbb{Z}_{-p}$-valued Euler characteristic induced by $\sigma^{-1}$.

The reason for the prime-to-$p$ restriction will become clear soon.

**Lemma 7.6.** *The principal and dual Euler characteristics are $0$-definable.*

*Proof.* They are definable by Lemma 6.5 and $\text{Aut}(K/\emptyset)$-invariant by construction.

---

7.1 Mock-frobenius periodic fields

**Definition 7.7.** A periodic field $(K, \sigma)$ is a *mock-Fr$_q$* if $(K, \sigma) \models \text{ACPF}$ and $\text{Abs}(K, \sigma) \cong \text{Fr}_q$.

**Proposition 7.8.** Let $q$ be a prime power.

1. The theory of mock-Fr$_q$ periodic fields is consistent and complete.

2. If $K$ is a mock-$\mathbb{F}_q$ and $\sigma$ is the mock Frobenius, then $(K^{\text{alg}}, \sigma)$ is a mock-Fr$_q$. Every mock-Fr$_q$ arises this way.

3. The theory of mock-$\mathbb{F}_q$ fields is consistent and complete.

*Proof.*

1. Mock-Fr$_q$ fields exist because we can embed Fr$_q$ into an existentially closed periodic field. Any two mock-Fr$_q$ fields are elementarily equivalent by Lemma 3.4.

2. Clear from Proposition 3.5 and the definitions.

3. Combine 1 and 2.

---

7.2 The principal Euler characteristic

Dwork proved the following part of the Weil conjectures, in [6].

**Fact 7.9.** *If $V$ is a variety over $\mathbb{F}_q$, then there are non-zero algebraic integers $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_\ell$ such that for every $n$,

$$|V(\mathbb{F}_{q^n})| = \alpha_1^n + \cdots + \alpha_m^n - \beta_1^n - \cdots - \beta_\ell^n.$$*

There is no assumption that $V$ is smooth, proper, or connected.

34
**Lemma 7.10.** Let $V, \alpha_i, \beta_j$ be as in Fact \(7.9\). Let $(K_\infty, \sigma)$ be a mock Fr$^q$, and let $\chi_\ell$ be the $\ell$-adic part of the canonical Euler characteristic on $K$. Then

$$\chi_\ell(V(K_1)) = \alpha'_1 + \cdots + \alpha'_m - \beta'_1 - \cdots - \beta'_\ell,$$

where

$$\alpha'_i = \begin{cases} \alpha_i & v_\ell(\alpha_i) = 0 \\ 0 & v_\ell(\alpha_i) > 0 \end{cases}$$

$$\beta'_i = \begin{cases} \beta_i & v_\ell(\beta_i) = 0 \\ 0 & v_\ell(\beta_i) > 0 \end{cases}$$

In other words, $\chi_\ell(V(K_1))$ is obtained from $|V(\mathbb{F}_q)|$ by dropping the terms of positive $\ell$-adic valuation.

**Proof.** Take a non-principal ultrafilter $U$ on $\mathbb{N}$, concentrating on the sets $1 + n\mathbb{Z}$ for every non-zero ideal $n\mathbb{Z}$.

**Claim 7.11.** The ultralimit of $|V(\mathbb{F}_{q^n})|$ in $\mathbb{Z}_\ell$ is given by the right-hand side of (7.10).

**Proof.** Take a finite extension $L/\mathbb{Q}_\ell$ such that $L$ contains all the $\alpha_i$ and $\beta_j$. Let $\mathcal{O}$ be the $\ell$-adic valuation ring on $L$. It suffices to show that for any non-zero ideal $I \triangleleft \mathcal{O}$, the following is true for “most” $n$:

$$\alpha_i^n \equiv \alpha'_i \pmod{I} \quad (4)$$

If $v_\ell(\alpha_i) > 0$, then $\lim_{n \to \infty} \alpha_i^n = 0$, and Equation (4) holds because $U$ is non-principal. If $v_\ell(\alpha_i) = 0$, then $\alpha_i$ is a unit in the finite ring $\mathcal{O}/I$. Let $m$ be the cardinality of the group of units $(\mathcal{O}/I)^\times$. Then

$$n \in m\mathbb{Z} \implies \alpha_i^n \equiv 1 \pmod{I}.$$  

Therefore

$$n \in 1 + m\mathbb{Z} \implies \alpha_i^n \equiv \alpha_i \pmod{I}.$$  

By choice of $U$, this holds for “most” $n$, verifying Equation (4). \(\square\) Claim

**Claim 7.12.** The ultralimit of $|V(\mathbb{F}_{q^n})|$ in $\mathbb{Z}_\ell$ is given by the left-hand side of (7.10).

**Proof.** Let $(K'_\infty, \sigma')$ be the ultraproduct of Frobenius periodic fields

$$(K'_\infty, \sigma') = \prod_{n \in \mathbb{N}} (\mathbb{F}_{q^n, \phi_q^n})/U.$$  

Then $(K'_\infty, \sigma') \Rightarrow ACPF$ by Corollary \(3.12\). For fixed $m$, note that

$$n \equiv 1 \pmod{m} \iff \phi_q^n|\mathbb{F}_{q^m} = \phi_q|\mathbb{F}_{q^m}.$$  

By choice of $U$, it follows that $\sigma'|\mathbb{F}_{q^m} = \phi_q|\mathbb{F}_{q^m}$. As this holds for all $m$,

$$\text{Abs}(K'_\infty, \sigma') \cong (\mathbb{F}_{q, \phi_q}).$$  

35
So \((K'_\infty, \sigma')\) is a mock-Fr\(^q\), and \((K'_\infty, \sigma') \equiv (K_\infty, \sigma)\). By uniform definability of \(\chi_\ell\),

\[ \chi_\ell(V(K'_1)) = \chi_\ell(V(K_1)). \]

The canonical Euler characteristic on \(K'_\infty\) is given by nonstandard counting, so \(\chi_\ell(V(K'_1))\) is the ultralimit of \(|V(Fr_q^n)| = |V(\mathbb{F}_q^n)|\).

\[\square_{\text{Claim}}\]

Now combine the two claims.

**Lemma 7.13.** Let \((K_\infty, \sigma)\) be a mock-Fr\(^q\).

1. If \(C\) is a curve over \(\mathbb{F}_q\), and \(\alpha_1, \ldots, \alpha_{2g}\) are the characteristic roots of the \(q\)-th-power Frobenius, then the prime-to-\(p\) part of \(\chi(C(K_1))\) equals \(|C(\mathbb{F}_q)|\).

2. If \(V\) is a 1-dimensional variety over \(\mathbb{F}_q\), then the prime-to-\(p\) part of \(\chi(V(K_1))\) equals \(|V(\mathbb{F}_q)|\).

3. If \(X\) is an Fr\(^q\)-definable subset of \(K_1\), then the prime-to-\(p\) part of \(\chi(X)\) equals \(|X \cap \mathbb{F}_q|\).

**Proof.**

1. By the Weil conjectures for curves ([10], Appendix C, §1), we know that

\[ C(\mathbb{F}_q^n) = 1 - \alpha_1^n - \cdots - \alpha_{2g}^n + q^n \]

for all \(n\). Moreover, the Poincare duality part of the Weil conjectures gives an equality of multi-sets:

\[ \{\alpha_1, \ldots, \alpha_{2g}\} = \{q/\alpha_1, \ldots, q/\alpha_{2g}\} \]

It follows that each \(\alpha_i\) is a unit in \(\mathbb{Q}_\ell^\times\), for \(\ell\) prime to \(p\). Therefore, by Lemma 7.10, the \(\ell\)-adic part of \(\chi(C(K))\) is given by

\[ \chi(C(K)) = 1 - \alpha_1 - \cdots - \alpha_{2g} + q = |C(\mathbb{F}_q)|. \]

2. Similar to Lemma 3.9, one can produce an \(\mathbb{F}_q\)-variety \(C\) and open subvarieties \(V' \subseteq V\) and \(C' \subseteq C\) such that

- \(V'\) is isomorphic to \(C'\) (over \(\mathbb{F}_q\))
- The complements \(V \setminus V'\) and \(C \setminus C'\) have finitely many \(K_1\)-points.
- When base changed to \(\mathbb{F}_q^{\text{alg}}\), \(C\) is a finite disjoint union of curves.

Every \(K^{\text{alg}}\)-point of \(V' \setminus V\) and \(C' \setminus C\) is in \(\mathbb{F}_q^{\text{alg}}\). Therefore

\[ \chi(V(K_1)) - |V(\mathbb{F}_q)| = \chi(V'(K_1)) - |V'(\mathbb{F}_q)| = \chi(C'(K_1)) - |C'(\mathbb{F}_q)| \]

\[ = \chi(C(K_1)) - |C(\mathbb{F}_q)| = 0, \]

where the final equality is Part [1].
3. By Proposition 3.7 there is a quasi-finite morphism $V \to \mathbb{A}_{\mathbb{F}_q}^1$ of $\mathbb{F}_q$-varieties such that $X$ is the image of $V(K_1) \to \mathbb{A}^1(K_1) = K_1$. For each $n$, let $V_n$ be the fiber product of $n$ copies of $V$ over $\mathbb{A}^1$. Then $V_n \to \mathbb{A}_{\mathbb{F}_q}^1$ is still quasi-finite, so $V_n$ has dimension at most 1. Let $Y_n$ be the definable set $V_n(K_1)$. By Part 2, $\chi(Y_n) = |Y_n(\mathbb{F}_q)|$.

Now use the argument of Lemma 4.5. Let $f : Y_1 \to X$ be the surjection induced by $V \to \mathbb{A}^1$. Let $X_k$ be the definable set of $a \in X$ such that the fiber $f^{-1}(a)$ has size $m$. Note that if $a \in X(\mathbb{F}_q)$, then every point in the fiber is field-theoretically algebraic over $a$, hence in $Y_1(\mathbb{F}_q)$.

The upshot is that the fibers of $Y_1(\mathbb{F}_q) \to X(\mathbb{F}_q)$ have size $k$ over $X_k(\mathbb{F}_q)$, and more generally the fibers of $Y_n(\mathbb{F}_q) \to X(\mathbb{F}_q)$ have size $k^n$ over $X_k(\mathbb{F}_q)$. Therefore,

$$|Y_n(\mathbb{F}_q)| = \sum_k k^n \cdot |X_k(\mathbb{F}_q)|$$

$$\chi(Y_n) = \sum_k k^n \cdot \chi(X_k),$$

where the second line is as in the proof of Lemma 4.5. By Part 2 the left hand sides agree. By the invertibility of Vandermonde matrices, it follows that $\chi(X_k) = |X_k(\mathbb{F}_q)|$. Summing over $k$, we see $\chi(X) = |X(\mathbb{F}_q)| = |X \cap \mathbb{F}_q|$. \hfill \Box

**Proposition 7.14.** Let $K$ be a mock-$\mathbb{F}_q$. Let $\chi$ be the principal Euler characteristic on $K$. For any definable set $X \subseteq K^n$, we have

$$\chi(X) = |X \cap \mathbb{F}_q^n|,$$

In particular, $\chi(X) \in \mathbb{Z}$.

Proof. Proceed by induction on $n$. For the base case $n = 1$, expand $K$ to a mock-$\mathbb{F}_q$ by Proposition 7.8.2 and then apply Lemma 7.13.3. Suppose $n > 1$. For $a \in K_1$, let $X_a$ denote the slice of $X$ over $a$:

$$X_a = \{ \bar{b} \in (K_1)^{n-1} : (a, \bar{b}) \in X \}.$$  

Fix $\ell^k$, and work with $\chi$ modulo $\ell^k$. For $i \in \mathbb{Z}/\ell^k$, let $S_i$ be the set of $a \in K_1$ such that $\chi(X_a) \equiv i \pmod{\ell^k}$. Each set $S_i$ is Fr$_q$-definable, so by induction $\chi(S_i) = |S_i \cap \mathbb{F}_q|$. Now for $a \in S_i \cap \mathbb{F}_q$, the set $X_a$ is Fr$_q$-definable, so by induction $\chi(X_a) = |X_a \cap \mathbb{F}_q^{n-1}|$. Then the following holds modulo $\ell^k$:

$$\chi(X) \equiv \sum_{i \in \mathbb{Z}/\ell^k} i \cdot \chi(S_i) \equiv \sum_{i \in \mathbb{Z}/\ell^k} i \cdot |S_i \cap \mathbb{F}_q|$$

$$\equiv \sum_{i \in \mathbb{Z}/\ell^k} \sum_{a \in S_i \cap \mathbb{F}_q} \sum_i \chi(X_a)$$

$$\equiv \sum_{a \in \mathbb{F}_q} \chi(X_a) \equiv \sum_{a \in \mathbb{F}_q} |X_a \cap \mathbb{F}_q^{n-1}|.$$

The final sum is $|X \cap \mathbb{F}_q^n|$. \hfill \Box
This lets us simplify Lemma 7.10.

**Corollary 7.15.** Let $V, \alpha_i, \beta_j$ be as in Fact 7.9. Let $F$ be a mock $\mathbb{F}_q$, and $\chi$ be its principal Euler characteristic. Then

$$\chi(V(F)) = \alpha_1 + \cdots + \alpha_m - \beta_1 - \cdots - \beta_\ell.$$ 

This implies something about the numbers appearing in Dwork’s theorem.

**Corollary 7.16.** If $V$ is a variety over $\mathbb{F}_q$, then the $\alpha_i$ and $\beta_j$ of Fact 7.9 have $\ell$-adic valuation zero for $\ell$ prime to $q$.

**Proof.** Let $\alpha'_i$ and $\beta'_i$ be as in Lemma 7.10. Let $F$ be a mock-$\mathbb{F}_q$, and $\chi_\ell$ be the $\ell$-adic part of the principal Euler characteristic. Comparing Lemma 8.10 and Corollary 7.15, we see

$$\alpha'_1 + \cdots + \alpha'_m - \beta'_1 - \cdots - \beta'_\ell = \alpha_1 + \cdots + \alpha_m - \beta_1 - \cdots - \beta_\ell.$$ 

Replacing $\mathbb{F}_q$ with $\mathbb{F}_q^n$ changes $\alpha_i$ to $\alpha_i^n$ and $\alpha'_i$ to $(\alpha'_i)^n$. Therefore, the following holds for any $n \geq 1$:

$$(\alpha'_1)^n + \cdots + (\alpha'_m)^n - (\beta'_1)^n - \cdots - (\beta'_\ell)^n = \alpha_1^n + \cdots + \alpha_m^n - \beta_1^n - \cdots - \beta_\ell^n.$$ 

Comparing Poincare series, one gets equality of multisets

$$\{\alpha'_1, \ldots, \alpha'_m\} = \{\alpha_1, \ldots, \alpha_m\}$$

$$\{\beta'_1, \ldots, \beta'_\ell\} = \{\beta_1, \ldots, \beta_\ell\}.$$ 

Therefore, none of the $\alpha'_i$ or $\beta'_i$ are zero, and every $\alpha_i$ and $\beta_i$ has $\ell$-adic valuation 0. \qed 

**Remark 7.17.** Corollary 7.16 can be proven using $\ell$-adic cohomology, but the proof given here is more elementary.

### 7.3 The Dual Euler Characteristic

Let $K$ be a mock-$\mathbb{F}_q$. Recall that the **dual Euler characteristic** on $K$ is the prime-to-$q$ part of the canonical Euler characteristic induced by $\sigma^{-1}$, where $\sigma$ is the mock Frobenius.

**Lemma 7.18.** Let $V$ be a variety over $\mathbb{F}_q$, and let $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_\ell$ be the algebraic integers from Fact 7.9. Let $K$ be a mock-$\mathbb{F}_q$ and let $\chi^\dagger$ be the dual Euler characteristic. Then

$$\chi^\dagger(V(K)) = \alpha_1^{-1} + \cdots + \alpha_m^{-1} - \beta_1^{-1} - \cdots - \beta_\ell^{-1}.$$ 

Moreover, this value is rational.

**Proof.** Similar to Lemma 7.10 but using an ultrafilter that concentrates on $-1 + n\mathbb{Z}$ for all $n$. Corollary 7.16 ensures that $v_\ell(\alpha_i) = 0$ for all $i$, so there is no need for any $\alpha'_i$’s or $\beta'_i$’s. Rationality is an easy exercise, using the fact that

$$\alpha_1^n + \cdots + \alpha_m^n - \beta_1^n - \cdots - \beta_\ell^n \in \mathbb{Z}$$

for all $n \in \mathbb{N}$. \qed
Proposition 7.19. If \( K \) is a mock-\( \mathbb{F}_q \) and \( \chi^\dagger \) is the dual Euler characteristic on \( K \), then \( \chi^\dagger(X) \in \mathbb{Q} \) for every \( \mathbb{F}_q \)-definable set \( X \).

Proof. If \( X \) is the set of \( K \)-points in some \( \mathbb{F}_q \)-definable variety, this follows from Lemma 7.18.

If \( X \) is a definable subset of \( K^n \), then Proposition 3.7 yields a quasi-finite morphism \( V \to \mathbb{A}^n \) of varieties over \( \mathbb{F}_q \), such that \( X \) is the image of \( V(K) \to \mathbb{A}^n(K_1) \). Let \( V_n \) be the \( n \)-fold fiber product of \( V \) over \( \mathbb{A}^1 \). By the argument of Lemma 4.5, \( \chi^\dagger(X) \) is given by some rational linear combination of the \( \chi^\dagger(V_n(K)) \).

Example 7.20. If \( V \) is a \( d \)-dimensional smooth projective variety over \( \mathbb{F}_q \), then the following identities of multisets hold by the Poincare duality part of the Weil conjectures:

\[
\{\alpha_1, \ldots, \alpha_m\} = \{q^d/\alpha_1, \ldots, q^d/\alpha_m\}
\]
\[
\{\beta_1, \ldots, \beta_{m'}\} = \{q^d/\beta_1, \ldots, q^d/\beta_{m'}\}.
\]

Therefore, for \( K \) a mock-\( \mathbb{F}_q \) with dual Euler characteristic \( \chi^\dagger \),

\[
\chi^\dagger(V(K)) = \alpha_1^{-1} + \cdots + \alpha_m^{-1} - \beta_1^{-1} - \cdots - \beta_{m'}^{-1}
\]
\[
= (\alpha_1 + \cdots + \alpha_m - \beta_1 - \cdots - \beta_{m'})/q^d = |V(\mathbb{F}_q)|/q^d.
\]

Putting everything together, we have proven:

Theorem (Theorem 1.6). Let \( K \) be a mock-\( \mathbb{F}_q \), for some prime power \( q = p^k \). There are two \( \mathbb{Z}_{\neq 0} \)-valued \( 0 \)-definable strong Euler characteristics \( \chi \) and \( \chi^\dagger \) on \( K \), such that

1. If \( V \) is a smooth projective variety over \( \mathbb{F}_q \), then

\[
\chi(V(K)) = |V(\mathbb{F}_q)|
\]
\[
\chi^\dagger(V(K)) = |V(\mathbb{F}_q)|/q^{\dim V}.
\]

2. If \( X \) is any \( \mathbb{F}_q \)-definable set, then

\[
\chi(X) = |X \cap \text{dcl}(\mathbb{F}_q)|.
\]

In particular, \( \chi(X) \in \mathbb{Z} \).

3. If \( X \) is any \( \mathbb{F}_q \)-definable set, then \( \chi^\dagger(X) \in \mathbb{Q} \).

7.4 The neutral Euler characteristic

Using the dual Euler characteristic on mock-finite fields, one can produce an exotic \( \mathbb{Q} \)-valued Euler characteristic \( \chi_0 \) on any pseudofinite field of characteristic 0. We outline the construction, omitting details because \( \chi_0 \) is less interesting than first expected (see Example 7.22).
1. Let $F$ be a pseudofinite field of characteristic zero, given explicitly as an ultraproduct of prime fields

$$F = \prod_i F_i/\mathcal{U}.$$ 

Suppose none of the $F_i$ have characteristic $\ell$.

2. For each $i$, let $K_i$ be a mock-$F_i$. Let $K$ be the ultraproduct

$$F = \prod_i K_i/\mathcal{U}.$$ 

One can show that $F \preceq K$.

3. Each $K_i$ has its dual Euler characteristic $\chi_i^\dagger$, taking values in the ring $\mathbb{Z}_\ell$. On $F_i$-definable sets, the Euler characteristic takes values in $\mathbb{Z}_\ell \cap \mathbb{Q}$.

4. Let $\mathbb{Z}_\ell^*$ and $\mathbb{Q}^*$ denote the ultrapowers $\mathbb{Z}_\ell^\mathcal{U}$ and $\mathbb{Q}^\mathcal{U}$. In the nonstandard limit, the $\chi_i^\dagger$ determine a $\mathbb{Z}_\ell^*$-valued Euler characteristic $\tilde{\chi}$ on $K$. When restricted to $F$-definable sets, $\tilde{\chi}$ takes values in $\mathbb{Q}^*$. Because $F \preceq K$, this gives a $\mathbb{Q}^*$-valued Euler characteristic $\tilde{\chi}$ on $F$.

5. Say that a weak Euler characteristic $\chi$ is *medial* if it satisfies the following partial version of strongness

If $f : X \to Y$ is a definable surjection between two definable sets, and every fiber has size $k < \infty$, then $\chi(X) = k \cdot \chi(Y)$.

One can verify that $\tilde{\chi}$ is a $\mathbb{Q}^*$-valued medial Euler characteristic on $F$.

6. If $V$ is a geometrically irreducible smooth projective variety over $F$, one can show using Example 7.20 and the Lang-Weil estimates that $\tilde{\chi}(V(F))$ is infinitesimally close to 1.

7. Using resolution of singularities and induction on dimension, one can show that for any variety $V/F$, the value $\tilde{\chi}(V(F))$ is infinitesimally close to an integer.

8. Using Proposition 3.7 and an argument similar to Lemma 4.5, one can show that if $X \subseteq F^n$ is definable, then $\tilde{\chi}(X)$ is infinitesimally close to a rational number.

9. Define $\chi_0(X)$ to be the standard part of $\tilde{\chi}(X)$. Then $\chi_0$ is a $\mathbb{Q}$-valued medial Euler characteristic on $F$. Also, $\chi_0(V(F)) = 1$ for any geometrically irreducible smooth projective variety $V/F$.

10. If $F'$ is *any* pseudofinite field of characteristic 0, then there is at most one $\mathbb{Q}$-valued medial Euler characteristic $\chi_0$ such that $\chi_0(V(F')) = 1$ for any geometrically irreducible smooth projective variety $V/F'$. This can be seen by resolution of singularities, induction on dimension, Proposition 3.7 and the proof of Lemma 4.3.
11. Therefore, every pseudofinite field of characteristic 0 admits a unique 0-definable \( \mathbb{Q} \)-valued medial Euler characteristic \( \chi_0 \) characterized by the fact that \( \chi_0(V(F)) = 1 \) for any smooth projective geometrically connected variety \( V \). This follows by a Beth implicit definability argument, similar to the proof of Proposition 4.8 and Theorem 1.4.

We call \( \chi_0 \) the neutral Euler characteristic.

**Remark 7.21.** Unlike the Euler characteristic of Lemma 6.5, \( \chi_0 \) is completely canonical, and is independent of the choice of a nonstandard Frobenius. If resolution of singularities holds in positive characteristic, then \( \chi_0 \) can be defined for all pseudofinite fields.

Unfortunately, the neutral Euler characteristic has bad properties:

**Example 7.22.** The neutral Euler characteristic is not strong. Consider the set

\[
S = \{(x, y, \lambda) : y^2 = x(x - 1)(x - \lambda) \text{ and } \lambda \neq 0, 1\}.
\]

One can view \( S \) as a family of elliptic curves \( E_\lambda \) parameterized by \( \lambda \). Each elliptic curve \( E_\lambda \) is missing one point at infinity, so

\[
\chi_0(E_\lambda) = \chi_0(\overline{E}_\lambda) - 1 = 1 - 1 = 0.
\]

Therefore, if \( \chi_0 \) were a strong Euler characteristic, one would have

\[
\chi_0(S) = 0 \cdot \chi_0(\mathbb{P}^1(F) \setminus \{0, 1, \infty\}) = 0 \cdot (1 - 3) = 0.
\]

On the other hand, one can directly count points in \( S \). For any finite field \( \mathbb{F}_q \) of characteristic \( \neq 2 \), the size of \( S(\mathbb{F}_q) \) turns out to be given by the formula

\[
|S(\mathbb{F}_q)| = \begin{cases} 
q^2 - q & \text{if } -1 \text{ is a square in } \mathbb{F}_q \\
q^2 - q - 2 & \text{if } -1 \text{ is not a square in } \mathbb{F}_q.
\end{cases}
\]

Essentially by Lemma 7.18, one sees that the dual Euler characteristic of \( S \) is given by

\[
\begin{cases} 
q^{-2} - q^{-1} & \text{if } -1 \text{ is a square in } \mathbb{F}_q \\
q^{-2} - q^{-1} - 2 & \text{if } -1 \text{ is not a square in } \mathbb{F}_q.
\end{cases}
\]

In the limit, \( q^{-1}, q^{-2} \to 0 \). Consequently, the neutral Euler characteristic of \( S(F) \) is given by

\[
\chi_0(S(F)) = \begin{cases} 
0 & \text{if } -1 \text{ is a square in } F \\
-2 & \text{if } -1 \text{ is not a square in } F.
\end{cases}
\]

In particular, \( \chi_0(S(F)) \) need not equal 0.

The neutral Euler characteristic seems to be governed by the weight 0 part of \( \ell \)-adic etale cohomology, in a manner analogous to Conjecture 6.3.
8 Directions for future research

There are several immediate directions for future research. The most important next step is verifying Conjecture 5.2, completing the proof that the $\mathcal{L}^\mu_{\text{rings}}$-theory of finite fields is decidable (Theorem 1.2). This will hopefully be carried out in [14]. Another key task is to relate the $\mathbb{Z}_\ell$-valued Euler characteristic to $\ell$-adic etale cohomology (Conjecture 6.3).

Another interesting direction is the following variant of Theorem 1.2:

Conjecture 8.1. The $\mathcal{L}^\mu_{\text{rings}}$-theory of the rings $\mathbb{Z}/n\mathbb{Z}$ is decidable.

The conjecture can be broken into several cases:

1. The rings $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. These are essentially handled by Theorem 1.2

2. The rings $\mathbb{Z}/p^k\mathbb{Z}$. For fixed $p$, the theory of these rings is closely related to $p$-adically closed fields. Indeed, any ultraproduct of $\mathbb{Z}/p^k\mathbb{Z}$ is interpretable in a $p$-adically closed field. If $p$ is allowed to vary, one also encounters henselian valued fields with pseudofinite residue field of characteristic 0. These theories are well-understood, and admit a form of cell decomposition. Mimicking the proofs of motivic integration, it should be possible to verify that elimination of parity quantifiers holds in the rings $\mathbb{Z}/p^k\mathbb{Z}$—modulo naming the nonstandard Frobenius.

3. The rings $\mathbb{Z}/n\mathbb{Z}$, where $n$ has multiple prime divisors. The theory of such rings can be analyzed using Feferman-Vaught theory, mimicking [5]. Elimination of parity quantifiers fails rather strongly, but can be recovered by expanding the boolean algebra sort with new predicates.

Lastly, it may be possible to generalize the definability of the canonical Euler characteristic from ACPF to its expansion ACFA. Although ACFA is not pseudofinite, its models are ultraproducts of Frobenius difference fields ([13]), and definable sets of finite rank are naturally pseudofinite.

8.1 Interactions with number theory?

We have relied heavily on algebraic geometry and number theory to prove a relatively simple model-theoretic fact. One could dream of reversing the process to obtain new results in number theory. Ultraproducts of finite fields are not the only source of pseudofinite fields. For example, if $\sigma$ is chosen randomly in $\text{Gal}(\mathbb{Q})$, then $(\mathbb{Q}^{\text{alg}}, \sigma) \models \text{ACPF}$ with probability 1, by [9], §16.6. Perhaps one can prove non-trivial facts by reasoning about nonstandard sizes of definable sets in these structures.

Unfortunately, we have probably done nothing interesting from a number-theoretic point of view. The nonstandard “sizes” on pseudofinite fields should be a simple artifact of etale cohomology, by Conjecture 6.3. Etale cohomology is already well-understood. Combinatorial facts about sizes correspond to well-known facts about cohomology. The fact that $\chi(X \times Y) = \chi(X) \cdot \chi(Y)$ corresponds to the Künneth formula. When $f : E \to B$ is a morphism, the
strong Euler characteristic property allows us to calculate the “size” of $E$ by “integrating” the “sizes” of the fibers over $B$. This property corresponds to the Leray spectral sequence.

One tool which might be new on the model-theoretic side is elimination of imaginaries, which holds in ACPF by work of Hrushovski [12]. When $X$ is interpretable, or definable with quantifiers, we know that $\chi(X)$ is “integral,” lying in $\hat{\mathbb{Z}}$ rather than $\hat{\mathbb{Z}} \otimes \mathbb{Q}$. There may be some number-theoretic content to this.

It feels as if there could be some connection between the canonical Euler characteristic and $p$-adic L-functions. The classical L-functions associated to number fields and elliptic curves are defined in terms of point counting. In some cases, these L-functions can be converted to $p$-adic analytic functions by extrapolating the values at negative integers. Insofar as we are counting points on varieties mod $p^k$, there is a spiritual connection to the $p$-adic part of the canonical Euler characteristic.

Moreover, $p$-adic integration appears in both contexts. If $\chi$ is a strong $\mathbb{Z}_p$-valued Euler characteristic, and $f : E \to B$ is a definable function, then $\chi$ induces a $p$-adic measure $\mu$ on $B$, and one can calculate $\chi(E)$ by $p$-adic integration

$$\chi(E) = \int_{x \in B} \chi(f^{-1}(x)) \, d\mu(x).$$

This was essentially how $\chi(X)$ was calculated in Lemma 4.6. Meanwhile, $p$-adic integration plays a key role in the theory of $p$-adic L-functions. For example, the Riemann zeta function is given on negative integers by a $p$-adic Mellin transform: there is some $c \in \mathbb{Z}_p^\times$ and $p$-adic measure $\mu$ on $\mathbb{Z}_p$ such that for positive integers $k$,

$$\zeta(-k) = \frac{1}{1 - c^{k+1}} \int_{\mathbb{Z}_p} x^k \, d\mu(x).$$

This Mellin transform is the underlying reason why the Kubota-Leopoldt $p$-adic zeta function exists. In some cases, the measure $\mu$ can be given a pseudofinite interpretation. For example, if $p$ is odd and $\alpha$ is a nonstandard integer whose $p$-adic standard part is $-1/2$, then $\zeta(-k)$ is given\(^2\) by $p$-adic standard part of the sum

$$\frac{1}{2 - 2^{-k}} \sum_{n=1}^\alpha n^k.$$  

\(^2\)Let $B_k(x)$ denote the $k$th Bernoulli polynomials

$$\sum_{k=0}^\infty \frac{B_k(x) t^k}{k!} = \frac{t e^{xt}}{e^t - 1},$$

and let $B_k$ denote the Bernoulli numbers $B_k(0)$. The identity

$$\frac{B_{k+1}(1/2) - B_{k+1}(0)}{k+1} = (2^{-k} - 2) \frac{B_{k+1}}{k+1}$$

can be proven by an easy exercise in generating functions. Let $\approx$ denote equality of standard parts. Then
In other words, (5) holds with $c = 1/2$ and $\mu$ equal to (half) the nonstandard counting measure on the pseudofinite set $\{1, 2, \ldots, \alpha\}$. Thus there are several vague connections between the canonical Euler characteristic on pseudofinite fields, and $p$-adic L-functions. I lack the expertise to pursue this connection further.

References

[1] Omaima Mostafa Alshanqiti. *Pseudo-finite rings and their generalizations*. PhD thesis, University of Manchester, 2015.

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

[3] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, April 1999.

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

[5] Jamshid Derakhshan and Angus Macintyre. Model theory of adeles I. arXiv:1603.09698 [math.LO], 2016.

[6] B. M. Dwork. On the rationality of the zeta function of an algebraic variety. *American J. Math.*, 82:631–648, 1960.

[7] Richard Elwes and Dugald Macpherson. A survey of asymptotic classes and measurable structures. In Zoé Chatzidakis, Dugald Macpherson, Anand Pillay, and Alex Wilkie, editors, *Model Theory with Applications to Algebra and Analysis*, pages 125–160. Cambridge University Press, 2008.

[8] James Freitag, Wei Li, and Thomas Scanlon. Differential Chow varieties exist. *J. London Math. Soc.*, 95(1):128–156, February 2016.

[9] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer, 2008.

The following holds for positive integers $k$,

\[
\zeta(-k) = \frac{-B_{k+1}}{k+1} = \frac{1}{2 - 2^{-k}} \left( \frac{B_{k+1}(1/2) - B_{k+1}(0)}{k+1} \right) \\
\approx \frac{1}{2 - 2^{-k}} \left( \frac{B_{k+1}(\alpha + 1) - B_{k+1}(0)}{k+1} \right) = \frac{1}{2 - 2^{-k}} \sum_{n=1}^{\alpha} n^k,
\]

by well-known relations between the Bernoulli numbers, the zeta function, and sums of $k$th powers.
[10] Robin Hartshorne. *Algebraic Geometry*. Number 52 in Graduate Texts in Mathematics. Springer, 1977.

[11] Wilfrid Hodges. *Model Theory*. Encyclopedia of mathematics and its applications. Cambridge University Press, 1993.

[12] Ehud Hrushovski. Pseudo-finite fields and related structures. In Luc Bélair, editor, *Model theory and Applications*, volume 11 of *Quaderni di matematica*. Aracne, 2002.

[13] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms. arXiv:math/0406514v1, 2004.

[14] Will Johnson et al. Computable ind-definability. In progress, 2020?

[15] Sofya Kamenkovich and Ya’acov Peterzil. Euler characteristic of imaginaries in o-minimal structures. Preprint, available at [http://math.haifa.ac.il/kobi/paper.3.pdf](http://math.haifa.ac.il/kobi/paper.3.pdf), September 2014.

[16] Catarina Kiefe. Sets definable over finite fields: their zeta-functions. *Trans. Amer. Math. Soc.*, 223:45–59, 1976.

[17] Jan Krajíček. Uniform families of polynomial equations over a finite field and structures admitting an euler characteristic of definable sets. *Proc. London Math. Soc.*, 3(81):257–284, 2000.

[18] Jan Krajíček and Thomas Scanlon. Combinatorics with definable sets: Euler characteristics and Grothendieck rings. *The Bulletin of Symbolic Logic*, 6(3):311–330, September 2000.

[19] James S. Milne. Abelian varieties (v2.00), 2008. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).

[20] David Mumford. *Abelian Varieties*. Number 5 in Studies in Mathematics. Tata Institute of Fundamental Research, 1970.

[21] Richard Pink et al. Finite group schemes and p-divisible groups, 2005. Course notes available at [http://www.math.ethz.ch/~pink/FiniteGroupSchemes.html](http://www.math.ethz.ch/~pink/FiniteGroupSchemes.html).

[22] Jean-Pierre Serre. *Algebraic Groups and Class Fields*. Graduate Texts in Mathematics. Springer, 1988.

[23] Lou van den Dries. *Tame Topology and O-minimal Structures*. Number 248 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1998.