Pseudofinite counting functions mod n

Will Johnson

August 28, 2013

1 Introduction

Let M be a structure and R be a finite ring (commutative and unital). Unless stated otherwise, "definable" means "definable with parameters." Let $\mathrm{Def}(M)$ denote the collection of definable sets in M. Recall the following definitions. A *weak R-valued Euler characteristic* is a function $\chi : \mathrm{Def}(M) \to R$ 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.

Equivalently, χ is a homomorphism from the Grothendieck ring $K(\mathrm{Def}(M))$ to R. If the following additional property holds, then χ is called a *strong* Euler characteristic:

> If $f : X \to Y$ is a definable function and $r \in R$ is such that for every $y \in Y$, $\chi(f^{-1}(y)) = r$, then
> $$\chi(X) = r \cdot \chi(Y).$$

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

If $R = \mathbb{Z}/n\mathbb{Z}$ and M is a finite structure, there is a (unique) Euler characteristic $\chi : \mathrm{Def}(M) \to \mathbb{Z}/n\mathbb{Z}$ assigning every set its size mod n. This χ is always strong and $\emptyset$-definable. If M is an ultraproduct of finite structures, then there is a canonical strong Euler characteristic $\chi : \mathrm{Def}(M) \to \mathbb{Z}/n\mathbb{Z}$ coming from the ultraproduct. Specifically, if M is an ultraproduct $\prod_{i \in I} M_i/\mathcal{U}$, and X is a definable set in M of the form $\phi(M; a)$, and a is the class of some tuple $\langle a_i \rangle_{i \in I} \in \prod_{i \in I} M_i$, then take $\chi(X)$ to be the ultralimit of $|\phi(M_i; a_i)|$ mod n. This limit Euler characteristic will always be strong, but need not be definable.

In the case where M is an ultraproduct of finite fields it is known that this canonical $\mathbb{Z}/n\mathbb{Z}$-valued Euler characteristic is not $\emptyset$-definable. Here, we show that it is definable with parameters, and that it is in a certain sense definable in terms of the non-standard Frobenius. Moreover, this definition scheme yields a recipe which takes an arbitrary pseudofinite field K and a choice of a topological generator of $\mathrm{Gal}(K)$, and yields a strong definable $\mathbb{Z}/n\mathbb{Z}$-valued Euler characteristic on K.

In more detail, define a *garden*[1] to be a difference field (K, σ) such that every element of K has a finite orbit under σ. Interpreted in the language of difference fields, this is not a first-order condition. However, the class of gardens can be viewed as a first-order elementary class by working in a multi-sorted language with a sort K_n for the fixed field of σ^n, for every $n \geq 1$. One includes the difference field structure on each K_n, and the inclusion maps $K_d \to K_n$ for $d|n$. For notational simplicity, however, we will denote a garden as (K, σ), rather than $(K_1, K_2, \ldots)$. The following facts are known, or easy to show:

1. If K is a pseudo-finite field and σ is a topological generator of $\mathrm{Gal}(K) \cong \hat{\mathbb{Z}}$, then (K^{alg}, σ) is an existentially closed garden, and all EC gardens are of this form.

2. In particular, the class of gardens has a model companion, whose models are the gardens (K, σ) such that $K = K^{alg}$ and the fixed field K_1 of σ is pseudo-finite.

3. If (K, σ) is an EC garden, then every definable subset of K_1 (the fixed field of σ) is already definable (with parameters) in K_1 as a pure pseudo-finite field. This is easy.

4. If $q = p^r$ is a prime power, define the *qth Frobenius garden* F_q to be $\mathbb{F}_q^{alg} = \mathbb{F}_p^{alg}$ with σ equal to the qth power Frobenius map $x \mapsto x^q$. Any non-principal ultraproduct of Frobenius gardens is an EC garden, and up to elementary equivalence, every EC garden arises this way.

5. If K is a garden, let $\mathrm{Abs}(K)$ denote the sub-garden consisting of the absolute numbers, i.e., the numbers algebraic over the prime field. Then two EC gardens K_1 and K_2 are elementarily equivalent if and only if $\mathrm{Abs}(K_1)$ is isomorphic to $\mathrm{Abs}(K_2)$.

6. EC gardens have elimination of imaginaries (proven by Hrushovski). We probably won't use this fact.

7. EC gardens are supersimple of finite SU-rank, and have a well-defined dimension theory.

Although the Frobenius gardens F_q are infinite, they have the property that every definable set is finite, so we have a unique $\mathbb{Z}/n\mathbb{Z}$-valued Euler characteristic coming from the counting function. Any ultraproduct (K, σ) of Frobenius gardens therefore gets a non-standard mod-n counting function, which will be a strong Euler characteristic $\chi : \mathrm{Def}(K) \to \mathbb{Z}/n\mathbb{Z}$.

[1] Hrushovski considers this kind of structure, but apparently doesn't give a name to it. Hence this silly name that I just made up.

We will show that *this* function is $\emptyset$-definable. Restricting to the fixed field, we get strong Euler characteristics on pseudo-finite fields, which are definable (but not $\emptyset$-definable).

Equivalently, the unique mod-n Euler characteristics on the Frobenius gardens are uniformly definable across q. In other words,

Theorem 1.1. *For every formula $\phi(x; y)$ in the language of gardens, and every n, k, there is a formula $\psi(y)$ such that for F a Frobenius garden and b a tuple from F,*

$$|\phi(F; b)| \equiv k \mod n \iff F \models \psi(b).$$

As an example, suppose x is a variable from the sort K_1, things fixed by σ, and suppose $\phi(x;)$ says that $x \neq 0$. So $\phi(F_q)$ is $\mathbb{F}_q^\times$. Then $|\mathbb{F}_q^\times| = q - 1$, which is congruent to 2 mod 5 if and only if q is congruent to 3 mod 5. We can detect this occurrence by looking at the action of σ on the 5th roots of unity, which will always live in $\mathbb{F}_{q^4}$. In particular, we can take ψ to be the sentence

$$\exists y : y^5 = 1 \wedge \sigma(y) = y^3,$$

where y is a variable from the sort fixed by σ^4.

Let $\hat{\mathbb{Z}}$ denote the Prufer ring, the inverse limit of $\mathbb{Z}/n\mathbb{Z}$ as n ranges over positive integers. Specifying a (weak) Euler characteristic $\chi : \mathrm{Def}(M) \to \hat{\mathbb{Z}}$ on a structure M is equivalent to specifying a collection of $\mathbb{Z}/n\mathbb{Z}$-valued (weak) Euler characteristics $\chi_n : \mathrm{Def}(M) \to \mathbb{Z}/n\mathbb{Z}$ satisfying some obvious compatibilities ($\chi_n(X)$ is the mod n reduction of $\chi_m(X)$ if n divides m). By abuse of terminology, we say that $\chi : \mathrm{Def}(M) \to \hat{\mathbb{Z}}$ is strong or definable if every χ_n is strong or definable, respectively. Note that if M is finite (or if every sort of M is finite), then there is a unique $\hat{\mathbb{Z}}$-valued Euler characteristic, and it is strong and definable. If M is an ultraproduct of finite structures, then M again has a canonical $\hat{\mathbb{Z}}$-valued Euler characteristic, which is strong but not necessarily definable. Then a restatement of Theorem 1.1 is the following:

Theorem 1.2. *If (K, σ) is an EC garden, then there is a $\emptyset$-definable $\hat{\mathbb{Z}}$-valued Euler characteristic $\chi : \mathrm{Def}(K) \to \hat{\mathbb{Z}}$ which is uniformly defined across all EC gardens, and which agrees with the non-standard counting functions when (K, σ) is an ultraproduct of Frobenius gardens.*

If K_0 is a pseudofinite field, then we get a map from topological generators of $\mathrm{Gal}(K_0)$ to $\hat{\mathbb{Z}}$-valued strong definable Euler characteristics of K_0. So pseudo-finite fields have many $\hat{\mathbb{Z}}$-valued strong definable Euler characteristics.

Remark 1.3. *Not all $\hat{\mathbb{Z}}$-valued strong definable Euler characteristics arise this way, for stupid reasons. If K_0 is pseudo-finite and σ, τ are two topological generators of $\mathrm{Gal}(K_0)$, then the above recipe yields two $\hat{\mathbb{Z}}$-valued Euler characteristics χ_σ and χ_τ. From the chinese remainder theorem, one knows that $\hat{\mathbb{Z}}$ is a product $\prod_p \mathbb{Z}_p$. Concoct a new $\hat{\mathbb{Z}}$-value Euler characteristic χ that agrees with χ_σ on the 2-adic part of $\hat{\mathbb{Z}}$, and agrees with χ_τ on the p-adic part, for odd p. I doubt that χ is of the form χ_ρ for any $\rho \in \mathrm{Gal}(K_0)$.*

Remark 1.4. *One can similarly define what it means to be $\mathbb{Z}_p$-valued strong definable Euler characteristic. It might well be the case that the above construction produces all $\mathbb{Z}_p$-valued strong definable Euler characteristics. My attempts to prove this haven't worked out, however.*

Remark 1.5. *If (K, σ) is an EC garden, then (K, σ) has strong definable $\hat{\mathbb{Z}}$-valued Euler characteristics other than the canonical one. Indeed, (K, σ^{-1}) is also an EC garden, and its canonical $\hat{\mathbb{Z}}$-valued Euler characteristic disagrees with that of (K, σ), but is still a strong definable Euler characteristic, because (K, σ) and (K, σ^{-1}) have the same definable sets.*

2 Reduction to the case of curves

Theorem 1.2 follows directly from Theorem 1.1. By the Chinese remainder theorem, in Theorem 1.1 we may reduce to the case where n is a prime power ℓ^k. The above discussion works with $\hat{\mathbb{Z}}$ replaced with $\mathbb{Z}_\ell$, and so in what follows we will work with $\mathbb{Z}_\ell$-valued Euler characteristics. The prime ℓ will remain fixed through what follows. When there are prime powers q being discussed, we will *not* assume that q is prime to ℓ.

If M is a structure, we can encode a $\mathbb{Z}_\ell$-valued Euler characteristic on M in terms of the predicates which pick out the definable sets X such that $\chi(X) \equiv n \bmod \ell^k$, for every $n \in \mathbb{Z}/\ell^k\mathbb{Z}$. Specifically, for each predicate $\phi(x; y)$ in the original language of M, each k and each $n \in \mathbb{Z}/\ell^k\mathbb{Z}$, we add a predicate $\phi_{n,k}(y)$ such that $\phi_{n,k}(b)$ holds if and only if $\chi(\phi(M; b))$ is congruent to n mod ℓ^k. This allows us to treat $\mathbb{Z}_\ell$-valued Euler characteristics as first order structure.

Let T_0 denote the set of first-order statements true of the Frobenius gardens. A model of T_0 is either a Frobenius garden or an EC garden. Now for each q, let F'_q denote the qth Frobenius garden F_q with the additional data of the unique $\mathbb{Z}_\ell$-valued Euler characteristic χ. Let T denote the set of statements true in all the F'_q. For example, the fact that χ is a strong $\mathbb{Z}_\ell$-valued Euler characteristic is included in T.

It suffices to show that every model of T_0 has a unique expansion to a model of T, since Theorem 1.1 then follows by By Beth's implicit definability theorem. In fact, since T is a conservative extension of T_0, it suffices to show that every model of T_0 has at most one expansion to a model of T.

If $(K, \sigma) \models T_0$, let's say that a $\mathbb{Z}_\ell$-valued Euler characteristic $\mathrm{Def}(K) \to \mathbb{Z}_\ell$ is *nice* if $(K, \sigma, \chi) \models T$. We need to show that any two nice Euler characteristics on a model of T_0 agree.

If (K, σ) is a Frobenius garden, this is automatic, since there is only one $\mathbb{Z}_\ell$-valued Euler characteristic, owing to the finiteness of every definable set. It remains to consider the case where (K, σ) is an EC garden. If (K, σ) is an EC garden and X is a definable subset of (K, σ), say that X is *determined* if any two nice Euler characteristics on (K, σ) assign the same value to X. (If (K, σ) admits no nice Euler characteristics, then every set is vacuously determined.) It suffices to show that every definable subset of every EC garden is determined.

Several observations should be made about this notion:

1. If two sets are in definable bijection, and one is determined, then so is the other.

2. Finite sets are determined.

3. If X and Y are determined, so are their cartesian product $X \times Y$ and their disjoint union $X \coprod Y$.

4. If X, Y and $X \cap Y$ are determined, then so is $X \cup Y$, by inclusion-exclusion. More generally, if $X_1, \ldots, X_n$ is a family of overlapping sets, and any intersection of the X_i's is determined, then $\bigcup_{i=1}^n X_i$ is also determined. Again, this follows by inclusion exclusion.

5. If X and Y are two sets, and the symmetric difference of X and Y is finite, then X is determined if and only if Y is determined.

For now, we will make the following assumption, which encapsulates most of the algebraic geometry of the argument:

Assumption 2.1. *Let (K, σ) be an EC garden. Let C be an absolutely irreducible smooth curve defined over K_1 (the fixed-field of σ). Then the definable set $C(K_1)$ is determined.*

We will verify this assumption in the next section. For now, we will prove Theorem 1.1 assuming Assumption 2.1.

Recall that in EC gardens, we have a well-defined rank $R(a/B)$, which can be defined as the transcendence degree of the difference field generated by a and B over the difference field generated by B. Also, if X is a definable set, its rank $R(X)$ is defined to be the maximum of $R(a/B)$ as a ranges over $X(\mathfrak{M})$, where B is a set of parameters over which X is defined, and $\mathfrak{M}$ is a saturated elementary extension of our original EC garden. This does not depend on the choice of B. The rank R satisfies the Lascar inequalities, is definable in families, is finite, and has the property that $R(X) > 0$ if and only if X is infinite. Moreover, sets in definable bijection have the same rank. (Presumably this rank is the same thing as SU-rank, though this fails in the more general case of ACFA so I'm leery about asserting this.)

Lemma 2.2. *Let (K, σ) be an EC garden and $X \subset (K_1)^n$ be a quantifier-free definable set of rank 1. Then there are absolutely irreducible smooth affine curves $C_1, \ldots, C_m \subset \mathbb{A}^n$, defined over K_1, such that X differs from $\bigcup_{i=1}^m C_i(K_1)$ by a finite set.*

Proof. We may assume (K, σ) is saturated. Recall that the sorts of (K, σ) are $K_1, K_2, \ldots$, where K_n is the fixed-field of σ^n. Each K_n is a degree-n Galois extension of K_1, so after naming parameters we may identify K_n with $(K_1)^n$. In particular, after choosing a basis for each K_n and naming the structure coefficients (in K_1), there is a very nice way of interpreting K_n in K_1. In particular, we can identify elements of K_n with n-tuples in K_1, and all the function symbols on K_n and between the K_n's are given by terms. Consequently, any quantifier-free definable subset of $(K_1)^n$ can be expressed entirely using terms from the K_1 sort. Since σ acts trivially on K_1, it follows that the definition can be expressed entirely in the language of rings. In other words, X must be $\phi(K_1)$ for some formula $\phi(-)$ in the language of rings over K_1. Let L be a small subfield of K_1 containing the parameters needed to define $\phi(-)$. We may assume that L is relatively algebraically closed in K_1.

If a and B are from K_1, then the rank $R(a/B)$ is merely the transcendence degree of a over B. Consequently, the fact that $R(a/L) \leq 1$ for every a from X implies that every $a \in X$ belongs to an L-definable curve or L-definable finite set. By compactness, X is in the union of finitely many L-definable curves. Let $C_1, \ldots, C_m$ be those affine curves C over L such that there is at least one point in X which is generic on C, i.e., one point $a \in X$ such that $\mathrm{qftp}(a/L)$ is the generic type of C. (If there were infinitely many such curves, then X would not be contained in a finite union of curves over L.) Then X differs from $\bigcup_{i=1}^m C_i(K_1)$ at only finitely many points. Indeed, if $a \in (K_1)^n$ is a point that belongs to exactly one of X and $\bigcup_{i=1}^m C_i$, then $R(a/L) = 0$. First of all, if $a \in X$, then $R(a/L) \leq R(X) = 1$, so the only way this could fail is if $R(a/L) = 1$. But then $\mathrm{qftp}(a/L)$ is the generic type of some curve C, and by choice of the C_i's, C is one of them. Thus $x \in \bigcup_{i=1}^m C_i$. Conversely, if $a \in \bigcup_{i=1}^m C_i$, then certainly $R(a/L) = tr.deg(a/L)$ is at most 1. So unless $R(a/L) = 0$, we have $R(a/L) = 1$. But then a is the generic point on some C_i. By choice of the C_i, there is some $b \in X$ such that b is also a generic point on C_i, over L. This implies that $\mathrm{qftp}(a/L) = \mathrm{qftp}(b/L)$. As X is quantifier-free definable over L, $a \in X$.

So the symmetric difference of X and $\bigcup_{i=1}^m C_i(K_1)$ contains only points of rank 0. As it is a definable set, it must have rank 0, hence be finite. Finally, we observe that the C_i are definable over L. To see this, embed K_1 into a monster model of ACF. Each C_i is the curve corresponding to $\mathrm{tp}(a/L)$ for some $a \in K_1$. The canonical base of $\mathrm{stp}(a/L)$ is in both $\mathrm{acl}(L)$ and $\mathrm{dcl}(aL) \subset K_1$. As L is relatively algebraically closed in K_1, this canonical base must be in L, so $\mathrm{tp}(a/L)$ is stationary and C_i is defined over L. □

Lemma 2.3. *Let (K, σ) be an EC garden and X be a quantifier-free definable set of rank 1. Then X is determined.*

Proof. The set X might live in some sorts other than K_1, but because of the facts mentioned at the start of the previous proof, X is in definable bijection with a quantifier-free definable set $Y \subset (K_1)^n$. Since X is determined if and only if Y is determined, we may replace X with Y and then assume that $X \subset (K_1)^n$. Then the previous lemma applies, so X differs at only finitely many points from a set of the form $\bigcup_{i=1}^n C_i(K_1)$, where each C_i is an absolutely irreducible affine curve defined over K_1. We may assume that the C_i are distinct, so $C_i \cap C_j$ is finite for $i \neq j$. By remarks above, it suffices to show that $\bigcup_{i=1}^n C_i(K_1)$ is determined. By inclusion-exclusion, it suffices to show that any intersection of $C_i(K_1)$'s is determined. An intersection of more than one is finite, hence determined, so it remains to see that $C_i(K_1)$ is determined for each i. Let C_i' be a smooth projective model of C_i. Then $C_i'(K_1)$ and $C_i(K_1)$ differ at only finitely many points, and $C_i'(K_1)$ is determined by Assumption 2.1, so by remarks above, $C_i(K_1)$ is determined. □

We will use the following fact, which is an easy consequence of model completeness of the theory of EC gardens and the ability to amalgamate gardens over algebraically closed bases:

Fact 2.4. *Let $\phi(x)$ be a formula in the language of gardens, with x a tuple. Then $\phi(x)$ is equivalent in EC gardens to a statement of the form*

$$\exists y : \psi(y; x)$$

where y is a tuple from various sorts, where $\psi(y;x)$ is quantifier-free, and where $(K,\sigma) \models \psi(a;b)$ implies $R(a/b) = 0$ for any EC garden (K,σ) and tuples a, b.

Lemma 2.5. *Let (K,σ) be an EC garden. Let X be a definable set of rank 1. Then there is a quantifier-free definable set Y and a definable surjection function $f : Y \to X$ such that the fiber products Y, $Y \times_X Y$, $Y \times_X Y \times_X Y$, ... are also quantifier-free definable sets of rank 1. Furthermore, we may assume that Y is defined over the same parameters that X is defined over, and that the fibers of f are finite and uniformly bounded in size.*

Proof. We may assume that (K,σ) is sufficiently saturated. The set X is of the form $\phi(K;b)$ for some parameter b. By Fact 2.4, $\phi(x;y)$ is of the form $\exists z : \psi(x;y;z)$, where $\psi(a;b;c)$ implies that $R(c/ab) = 0$ in any EC garden. Let Y be the set of $(x;z)$ such that $\psi(x;b;z)$ holds. Then Y is defined over b. Let $f : Y \to X$ be the coordinate projection. By definition of X, this is surjective. The nth fiber product is clearly just the set of $(x; z_1, \ldots, z_n)$ such that $\bigwedge_{i=1}^n \psi(x;b;z_i)$ holds. This is a quantifier-free definable set. It has rank 1: suppose $(a;c_1,\ldots,c_n)$ is a tuple satisfying $\bigwedge_{i=1}^n \psi(a;b;c_i)$. Then because $\psi(a;b;c_i)$ holds, $R(c_i/ab) = 0$ for each i. And $a \in X$, so $R(a/b) \le 1$. Consequently,

$$R(ac_1 \cdots c_n/b) \le R(c_1/ab) + \cdots + R(c_n/ab) + R(a/b) \le 0 + \ldots + 0 + 1 \le 1.$$

So the nth fiber product has rank at most 1. Since it surjects onto X, it has rank 1.

The fibers of f are finite and uniformly bounded in size: by saturation, it suffices to show they are finite. But for each $a \in X$, the fiber $f^{-1}(a)$ is exactly $\psi(a;b;K)$. Since every element of this set has rank 0 over a, b, this set must be finite. □

Lemma 2.6. *Let (K,σ) be an EC garden. Let $Y \to X$ be a definable surjection, and suppose all fibers have size at most m. Suppose that the first m fiber products Y, $Y \times_X Y$, $Y \times_X Y \times_X Y$, ... are determined. Then X is determined.*

Proof. Let χ and χ' be two nice Euler characteristics. For $1 \le k \le m$, let X_k denote the set of $a \in X$ such that $f^{-1}(a)$ has size m. Let α_k and β_k denote $\chi(X_k)$ and $\chi'(X_k)$. Let Y_j denote the j-fold fiber product of Y over X. So $Y_1 = Y$ and $Y_0 = X$. There is a natural projection map $f_j : Y_j \to X$, and the fiber over a point in X_k has size k^j. Because χ and χ' are strong Euler characteristics, it must be the case that

$$\chi(Y_j) = \sum_{k=1}^m \alpha_k k^j$$

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

Now since Y_j is determined for $j = 1, \ldots, m$, we know that

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

for $j = 1, \ldots, m$. By invertibility of the Vandermonde matrix $\langle k^j \rangle_{1 \le k \le m,\ 1 \le j \le m}$, we have $\alpha_i = \beta_i$ for $1 \le i \le m$. Consequently,

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

As χ and χ' were arbitrary, X is determined. □

Lemma 2.7. *Let D be a definable set in an EC garden (K, σ). Suppose D has positive rank. Then there is a definable map f from D to a definable set of rank 1, such that every fiber of f has lower rank than D itself.*

Proof. We may assume that D lives in a power of K_1, since K_n is in definable bijection with K_1^n. We prove the lemma for $D \subset K_1^m$, by induction on m.

For the base case where $m = 1$, D can have rank at most 1. Take f to be the identity map. Clearly this works. For the inductive step, suppose $m > 1$. Let π be a coordinate projection $K_1^m \to K_1$ such that $\pi(D)$ is infinite. (If no such coordinate projection existed, then D would be finite.) Let

$$E = \{x \in K_1 : R(\pi^{-1}(x) \cap D) = R(D)\}.$$

This is definable. By Lascar inequalities, E must have SU-rank 0, so E is a finite set $\{e_1, \ldots, e_k\}$. By the inductive hypothesis, for each i there is a definable map f_i from $\pi^{-1}(e_i) \cap D$ to a set of rank 1, with every fiber of lower dimension than $SU(\pi^{-1}(e_i) \cap D) = SU(D)$. Let R be the set of points of D not projecting onto E. Let g be the restriction of π to R. Then g is a map from R to a set of rank 1, and the fibers of g have lower rank than $SU(D)$. Conclude by taking f to be the map from D to the disjoint union of $g(R)$ and the ranges of the f_i's. □

Finally we prove Theorem 1.1, assuming Assumption 2.1.

Proof (of Theorem 1.1). We prove by induction on n that every definable set of rank n in every EC garden is determined. As explained above, this suffices to prove Theorem 1.1. The case where $n = 0$ is obvious. Combining Lemmas 2.3, 2.5 and 2.6, we get the base case where $n = 1$. For the inductive step, suppose we know that all definable sets of rank at most $n \ge 1$ are determined. It then follows by Beth's implicit definability theorem that the restriction of nice Euler characteristics to definable sets of rank at most n are definable. In other words, if χ and χ' are two nice Euler characteristics on an EC garden, then not only do χ and χ' agree on sets of rank at most n, but in any definable family $\{E_b\}_{b \in B}$ of sets of rank at most n, for any k and m, the set of b such that $\chi(E_b) \equiv m \bmod \ell^k$ is a definable subset of B.

Now fix some EC garden (K, σ) and some definable set X of rank $n+1$. Let χ and χ' be two nice Euler characteristics on (K, σ). By Lemma 2.7, there is a definable map $f : X \to Y$ where Y is a set of lower rank, and where the fibers of f have rank at most n. For each $y \in Y$, let X_y denote $f^{-1}(Y)$. Then $\{X_y\}_{y \in Y}$ is a definable family of sets of rank at most n. Therefore, for each y we have $\chi(X_y) = \chi'(X_y)$. Moreover, for any k and m, the set of $y \in Y$

such that $\chi(X_y) \equiv m \bmod \ell^k$ is a definable subset of Y. Denote this set $Y_{k,m}$; it is also the set of $y \in Y$ such that $\chi'(X_y) \equiv m \bmod \ell^k$.

Because χ and χ' are strong Euler characteristics, it follows that for each k,

$$\chi(X) \equiv \sum_{m \in \mathbb{Z}/\ell^k\mathbb{Z}} m\chi(Y_{k,m}) \qquad \bmod \ell^k$$

$$\chi'(X) \equiv \sum_{m \in \mathbb{Z}/\ell^k\mathbb{Z}} m\chi'(Y_{k,m}) \qquad \bmod \ell^k$$

Now $Y_{k,m}$ is a definable subset of Y, and Y has rank at most n, so by induction $\chi(Y_{k,m}) = \chi'(Y_{k,m})$. Hence the right hand sides agree, and we conclude that $\chi(X) \equiv \chi'(X) \bmod \ell^k$ for every k. It follows that $\chi(X) = \chi'(X)$. As χ and χ' were arbitrary, X is determined. This completes the inductive proof. □

It remains to verify Assumption 2.1.

3 The case of smooth curves

From algebraic geometry and the Weil conjectures, one knows a great many facts about smooth curves over finite fields. Let C be a smooth absolutely irreducible curve over $\mathbb{F}_q$. Let J be the Jacobian of C. Let g be the genus of C. One knows that there exist algebraic integers $\alpha_1, \ldots, \alpha_{2g}$, each with absolute value $\sqrt{q}$, such that for any n,

$$|C(\mathbb{F}_{q^n})| = 1 - \alpha_1^n - \cdots - \alpha_{2g}^n + q^n$$

$$|J(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g}(1 - \alpha_i^n)$$

Let $\phi : J \to J$ be an isogeny. It is known that there exist algebraic integers $\beta_1, \ldots, \beta_{2g}$ such that for any polynomial $P(X) \in \mathbb{Z}[X]$,

$$\deg(P(\phi)) = \prod_{i=1}^{2g} P(\beta_i),$$

where $\deg(P(\phi))$ is 0 if $P(\phi) : J \to J$ is not an isogeny, and is the degree of $P(\phi)$ as an isogeny, otherwise, i.e., the length of the finite group scheme $\ker P(\phi)$. If $\phi : J \to J$ is the qth-power geometric Frobenius, then for $P(X) = X^n - 1$, the endomorphism $P(\phi)$ has as its kernel exactly the points of $J(\mathbb{F}_{q^n})$. Since this is finite, $P(\phi)$ is an isogeny, and in fact it is a separable isogeny, by looking at the tangent space. Thus $\deg P(\phi)$ is just the set-theoretic size of the kernel. So

$$\prod_{i=1}^{2g}(1 - \beta_i^n) = \deg P(\phi) = |J(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g}(1 - \alpha_i^n).$$

This holds for all n. Using the fact that $|\alpha_i| = \sqrt{q}$, one can prove that the β_i are the same as the α_i, up to permutation.

In summary,

Fact 3.1. *If C is a smooth curve over a finite field $\mathbb{F}_q$, J is the Jacobian of C, and $\phi : J \to J$ is the qth-power geometric Frobenius, then there exist algebraic integers $\alpha_1, \ldots, \alpha_{2g}$ such that for every n,*

$$|C(\mathbb{F}_{q^n})| = 1 - \alpha_1^n - \cdots - \alpha_{2g}^n + q^n$$

and for every $P(X) \in \mathbb{Z}[X]$,

$$\deg P(\phi) = \prod_{i=1}^{n} P(\alpha_i).$$

Now if we know the values of $\deg(\phi - n) = \prod_{i=1}^{2g}(\alpha_i - n)$ for all n, then we can interpolate to find the coefficients of the characteristic polynomial of ϕ, i.e., the symmetric polynomials in the α_i's. In particular, we can determine $\sum_{i=1}^{2g} \alpha_i$, which almost determines $|C(\mathbb{F}_q)|$. This is roughly how we'll prove that $C(K_1)$ is determined, for (K, σ) an EC garden.

Often, $\phi - n$ will not be a separable isogeny. To get a handle on its degree, we need to use some basic facts about finite group schemes over algebraically closed fields.

Fact 3.2. *Let K be an algebraically closed field. The category of commutative finite group schemes over K is abelian. Every object has a canonical decomposition as a sum of a constant group scheme (coming from a commutative finite group) and a local group scheme, i.e., a group scheme G with $G^{red} = 0$, or equivalently, with exactly one K-point. If K has characteristic zero, every finite group scheme is constant. Consequently the simple group schemes are of the form $\mathbb{Z}/\ell\mathbb{Z}$ for ℓ a prime. If K has characteristic p, then one additionally has the local group schemes $\mu_p = \operatorname{Spec} K[X]/(X^p - 1)$ and $\alpha_p = \operatorname{Spec} K[X]/(X^p - X)$ (with their usual multiplicative and additive group laws). If $0 \to G \to G' \to G'' \to 0$ is an exact sequence, then $l(G') = l(G'') + l(G)$, where $l(G)$ denotes the length or order of the group scheme G, i.e., the dimension of the coordinate ring of G as a K-vector space. A finite group scheme G is always annihilated by multiplication by $l(G)$. If G is a local group scheme, then $l(G)$ is a power of p.*

From the equation $l(G') = l(G'') + l(G)$ and the fact that these orders are finite, one sees that every commutative finite group scheme admits a composition series with simple quotients. If G is reduced/constant then the quotients will all be reduced/constant (because one can take the set-theoretic composition series in this case), and if G is local then the quotients will all be local (because a local group scheme cannot map surjectively onto a non-local group scheme, and cannot contain a non-local group scheme as a subgroup). If G and G' are simple commutative finite group schemes, and one of G or G' is reduced/constant while the other is local, then there are no homomorphisms between G and G', because G and G' are not isomorphic. If G and G' are arbitrary commutative finite group schemes, and one is reduced/constant while the other is local, then there are still no homomorphisms $G \to G'$, by an inductive argument using the compositions series of G and G'.

Consequently, if we write an arbitrary commutative finite group scheme G as a direct sum $G_0 \oplus G_{red}$, with G_0 local and G_{red} reduced, then

$$\mathrm{End}(G) \cong \mathrm{End}(G_0) \oplus \mathrm{End}(G_{red})$$

Lemma 3.3. *Let G be a finite commutative group scheme. Suppose ℓ is a prime (possibly the characteristic) and ℓ^k divides the order of G. Then ℓ^k divides the order of the ℓ^k-torsion in G.*

Proof. We may assume $k > 0$. First of all we show that there is a subgroup scheme $H \leq G$ of order ℓ^k. If G is reduced, then G comes from a finite group and H exists by the Sylow theorems or the classification of finite abelian groups. If G is local, then $l(G)$ is a power of p, the characteristic, so $\ell = p$. Using the composition series of G in terms of μ_p and α_p, it follows that some subgroup of G has order p^k. Finally, if G is neither local nor reduced, then we can write G as a direct sum $G_{red} \oplus G_0$, with G_{red} the reduced part of G and G_0 the local part. Then $l(G) = l(G_{red}) \cdot l(G_0)$. Therefore we can partition k as $k = k_{red} + k_0$, so that $\ell^{k_{red}}$ divides $l(G_{red})$ and ℓ^{k_0} divides $l(G_0)$. Then we can find $H_{red} \leq G_{red}$ and $H_0 \leq G_0$ having orders $\ell^{k_{red}}$ and ℓ^{k_0}, respectively. Taking $H = H_{red} + H_0 \subset G$, we then conclude that $l(H) = \ell^k$.

Now that we have H, note that H is annihilated by its order ℓ^k, so H is a subgroups cheme of the ℓ^k-torsion of G. Therefore, the order of the ℓ^k-torsion of G is divisible by the order of H, which is ℓ^k. □

Lemma 3.4. *If K is a field of characteristic p and X is a finite K-scheme of length less than or equal to p^n, then the n-fold iterate of the absolute Frobenius factors through $X^{red} \subseteq X$, where X^{red} is the maximal reduced closed subscheme of X.*

Proof. Write $X = \operatorname{Spec} A$, where A is K-algebra of dimension at most p^n. Let I be the nilradical of A, so $X^{red} = \operatorname{Spec} A/I$. For $\alpha \in I$, we have $\alpha^{p^n} = 0$. In fact, if $P(X) \in K[X]$ generates the kernel of of the homomorphism $K[X] \to K[\alpha]$ sending X to α, then $K[\alpha] \cong K[X]/(P(X))$. Nilpotence of α implies that some power of X is divisible by $P(X)$, forcing $P(X) = X^m$ for some m. Then $K[X]/(P(X)) = K[X]/(X^m)$ has dimension m over K, so $m \leq p^n$. As $P(\alpha) = 0$, α^m vanishes and hence α^{p^n} does as well.

So every element of the nilradical I has vanishing p^nth power, or equivalently is killed by the nth iterate of the absolute Frobenius. This means that the nth iterate of the absolute Frobenius map factors through $A \to A/I$, a map which is equivalent to $X^{red} \to X$ on the level of schemes. □

Lemma 3.5. *Let G be a finite commutative group scheme over $\mathbb{F}_q^{alg}$; suppose that G is defined over $\mathbb{F}_q$, i.e., $G = G' \times_{\operatorname{Spec} \mathbb{F}_q} \operatorname{Spec} \mathbb{F}_q^{alg}$ for some group scheme G' over $\mathbb{F}_q$. Thus there is a qth power geometric Frobenius map $\phi : G \to G$, which is automatically a homomorphism of group schemes over $\mathbb{F}_q^{alg}$. If the order of G is q or less, then $\phi : G \to G$ factors through the reduced part G_{red} of G.*

Proof. Let Abs_q denote the qth-power absolute Frobenius. The qth-power geometric Frobenius $\phi : G \to G$ is obtained by pulling back $Abs_q : G' \to G'$ along $\operatorname{Spec} \mathbb{F}_q^{alg} \to \operatorname{Spec} \mathbb{F}_q$. If $\tau : G \to G$ is the coefficient-twisting isomorphism obtained by pulling back Abs_q : $\operatorname{Spec} \mathbb{F}_q^{alg} \to \mathbb{F}_q^{alg}$ along $G \to \operatorname{Spec} \mathbb{F}_q^{alg}$, then it so happens that $\tau \circ \phi = Abs_q$. Thus $\phi = \tau^{-1} \circ Abs_q$. Now by Lemma 3.4, $Abs_q : G \to G$ factors through $G^{red} \to G$. The composition $G^{red} \hookrightarrow G \overset{\tau^{-1}}{\to} G$ factors through $G^{red} \hookrightarrow G$, because G^{red} is a reduced scheme. Consequently, $\tau^{-1} \circ Abs_q$ must also factor through $G^{red} \to G$. □

Fix ℓ. For each prime power q, consider F_q with the following additional structure:

1. For each genus g curve C defined over $\mathbb{F}_q$, the values of the symmetric polynomials of the $\alpha_1(C), \ldots, \alpha_{2g}(C)$ as elements of $\mathbb{Z}_\ell$. Specifically, for each k, n, m, g, and each formula $\phi(x; y)$ in the language of rings, we include predicates which pick out the values of b such that $\phi(\mathbb{F}_q^{alg}; y)$ is a smooth curve of genus g, and the nth symmetric polynomial of the $\alpha_1(C), \ldots, \alpha_{2g}(C)$ is congruent mod ℓ^k to m.

2. For each genus g curve C over $\mathbb{F}_q$ and each $P(X) \in \mathbb{Z}[X]$ the numbers $N_{P(X),k}$, $N_{P(X),k,red}$ and $N_{P(X),k,0}$ defined as follows: let J be the Jacobian of C. Let $\phi : J \to J$ be the qth power geometric Frobenius on J. Let $G_{P(X),k}(C)$ denote the part of J annihilated by both $P(\phi)$ and ℓ^k, i.e., the ℓ^k-torsion in $\ker P(\phi)$, or the kernel of the action of $P(\phi)$ on the ℓ^k-torsion. Let $N_{P(X),k}(C)$, $N_{P(X),k,0}(C)$ and $N_{P(X),k,red}(C)$ denote the order of the group schemes $G_{P(X),k}(C)$, its local part, and its reduced part. We can make these into first-order structure by using the fact that all are bounded by the order of the ℓ^k-torsion in J, which is ℓ^{2kg}.

Call F_q with this extra structure F_q', and let T' be the set of all first-order statements true in the F_q'. Recall that T_0 is the theory of the F_q's as pure gardens.

Lemma 3.6. *Each model of T_0 can be extended to a model of T' in at most one way. Thus, by Beth's implicit definability theorem, the extra structure on the F_q's is uniformly definable in the language of gardens.*

Proof. The following first-order statements are true of the above data, in every F_q:

(a) $N_{P(X),k}(C) = N_{P(X),k,red}(C) \cdot N_{P(X),k,0}(C)$.

(b) $N_{P(X),k,red}(C)$ actually equals the number of points in $J(\mathbb{F}_q^{alg})$ which are ℓ^k-torsion and annihilated by $P(\phi)$, because the reduced part of $G_{P(X),k}(C)$ is the constant group scheme coming from this set-theoretic abelian group. Note that $\phi : J(\mathbb{F}_q^{alg}) \to J(\mathbb{F}_q^{alg})$ is the same map as σ, so we can also say that $N_{P(X),k,red}(C)$ equals the number of points in $J(\mathbb{F}_q^{alg})$ which are ℓ^k-torsion and annihilated by $P(\sigma)$.

(c) The numbers $N_{P(X),k,red}(C)$ and $N_{P(X),k,0}(C)$ are always at least one, hence never zero.

(d) ℓ^k divides $N_{P(X),k}$ if and only if ℓ^k divides $\prod_{i=1}^{2g} P(\alpha_i(C))$. This follows by Lemma 3.3 and the fact that $\prod_{i=1}^{2g} P(\alpha_i(C))$ is exactly the degree of $P(\phi)$, hence the order of the finite group scheme $\ker P(\phi)$ (unless $P(\phi)$ isn't an isogeny, in which case $\ker P(\phi)$ contains an abelian variety, so ℓ^k certainly divides the order of the ℓ^k-torsion in $\ker P(\phi)$, and ℓ^k also divides $0 = \deg P(\phi)$).

(e) If the first sort (the fixed field of σ) has more than ℓ^{2kg} elements, then $N_{X,k,0}(C) = N_{0,k,0}(C)$. To see this, note that the ℓ^k-torsion is a commutative group scheme of order ℓ^{2kg}, defined over $\mathbb{F}_q$, with geometric qth-power Frobenius induced by ϕ. Let H be the ℓ^k-torsion, and write H as the sum of the reduced part H_{red} and the local part H_0. Since $q > \ell^{2kg}$, Lemma 3.5 implies that ϕ must map H into H_{red}. By the comments before Lemma 3.3, the action of ϕ on H must send H_{red} into H_{red} and H_0 into H_0. In particular, ϕ must annihilate H_0. Therefore, the entirety of H_0 is in the kernel of ϕ. Now $G_{0,k}(C)$ is H and $G_{X,k}(C)$ is the kernel of the action of ϕ on H. So the local part of $G_{0,k}(C)$ lies entirely in $G_{X,k}(C)$, and therefore the two groups have the same local part, so $N_{0,k,0}(C) = N_{X,k,0}(C)$.

(f) If $N_{X,k,0}(C) = N_{0,k,0}(C)$, then $N_{P(X),k,0}(C) = N_{P(0),k,0}(C)$ for every $P(X) \in \mathbb{Z}[X]$. The first statement asserts that ϕ acts trivially on the local part of the ℓ^k-torsion, and if this holds, then $P(\phi)$ acts just like $P(0)$.

(g) For $n \in \mathbb{Z}$, $N_{n,k}(C)$ equals $\gcd(n, \ell^k)^{2g}$, where $\gcd(x, y)$ denotes the greatest common divisor of x and y. Indeed, $G_{n,k}(C)$ is exactly the maximal subgroup scheme of J annihilated by both multiplication by n and by multiplication by ℓ^k. Equivalently, $G_{n,k}(C)$ is the part of J annihilated by the ideal $(n, \ell^k) \subset \mathbb{Z}$, which is the principal ideal generated by $\gcd(n, \ell^k)$. So $G_{n,k}(C)$ is just the $\gcd(n, \ell^k)$-torsion in J. By well-known facts about Abelian varieties, this group scheme has order $\gcd(n, \ell^k)^{2g}$.

It follows that these first-order statements hold in every model of T'. Now let M be a model of T_0. If (K, σ) is a Frobenius garden F_q, then this is witnessed by some first-order statement (specifically the statement saying that K_1 has exactly q elements). It is part of the axioms of T' that if the underlying garden is isomorphic to F_q, then the extra structure must be whatever it is for F'_q. In particular, the extra structure is uniquely determined. (Maybe it's worth pointing out that every automorphism of F_q as a garden extends to an automorphismi of F'_q.)

So suppose that (K, σ) is an EC garden instead of a Frobenius garden. Suppose we have two ways of expanding K to a model of T'. Denote one with the symbols above, and the other with primed symbols. By (e), one knows that $N_{X,k,0}(C) = N_{0,k,0}(C)$ and $N'_{X,k,0}(C) = N'_{0,k,0}(C)$ for every C. Consequently, by (f)

$$N_{P(X),k,0}(C) = N_{P(0),k,0}(C) \text{ and } N'_{P(X),k,0}(C) = N'_{P(0),k,0}(C) \tag{1}$$

for every $P(X)$ and k and C. By (b), we know that

$$N_{P(X),k,red}(C) = N'_{P(X),k,red}(C) \tag{2}$$

for every $P(X)$ and k and C, because both sides must actually equal the number ℓ^k-torsion points in $J(K)$ annihilated by $P(\sigma)$. (Note that the ℓ^k-torsion must live in some sort K_m where m depends only on ℓ^k, so the number of ℓ^k-torsion points is truly something that can be expressed by first-order conditions in our multi-sorted structure.) Similarly, by (g)

$$N_{n,k}(C) = \gcd(n, \ell^k)^{2g} = N'_{n,k}(C) \tag{3}$$

for every k and every $n \in \mathbb{Z}$. Combining (a), (c), (2) and (3),

$$N_{n,k,0}(C) = \frac{N_{n,k}(C)}{N_{n,k,red}(C)} = \frac{N'_{n,k}(C)}{N'_{n,k,red}(C)} = N'_{n,k,0}(C) \tag{4}$$

for every k and every $n \in \mathbb{Z}$. By (1), it follows that

$$N_{P(X),k,0}(C) = N_{P(0),k,0}(C) = N'_{P(0),k,0}(C) = N'_{P(X),k,0}(C) \tag{5}$$

for arbitrary $P(X)$, k, and C. Finally, combining (a), (2) and (5), we see that

$$N_{P(X),k}(C) = N_{P(X),k,0}(C) \cdot N_{P(X),k,red}(C) = N'_{P(X),k,0}(C) \cdot N'_{P(X),k,red}(C) = N'_{P(X),k}(C) \tag{6}$$

for arbitrary $P(X)$, k, and C.

Combining (6) with (d), we see moreover that for any k and $P(X)$ and C,

$$\ell^k | \prod_{i=1}^{2g} P(\alpha_i(C)) \iff \ell^k | \prod_{i=1}^{2g} P(\alpha'_i(C)).$$

In other words,

$$\left| \prod_{i=1}^{2g} P(\alpha_i(C)) \right|_\ell = \left| \prod_{i=1}^{2g} P(\alpha'_i(C)) \right|_\ell \tag{7}$$

for arbitrary $P(X)$ and C. By Lemma 3.7 below, it follows that the $\alpha_i(C)$ are a permutation of the $\alpha'_i(C)$. Consequently, the elementary symmetric polynomials take the same values. Combined with (6), (2) and (5), we see that our two expansions of (K, σ) are the same. □

Lemma 3.7. *Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be two n-element multisets of elements of $\mathbb{Q}_\ell^{alg}$. In fact, suppose that the α_i are the roots of some degree n polynomial over $\mathbb{Q}_\ell$, and assume the same for the β_i. Suppose that for every polynomial $P(X) \in \mathbb{Z}[X]$, the following holds:*

$$\left| \prod_{i=1}^{n} P(\alpha_i) \right|_\ell = \left| \prod_{i=1}^{n} P(\beta_i) \right|_\ell . \tag{8}$$

Then the α_i are a permutation of the β_i.

Proof. By continuity, (8) continues to hold for $P(X)$ in $\mathbb{Z}_\ell[X]$. By clearing denominators, it clearly even extends to $P(X) \in \mathbb{Q}_\ell[X]$. Let γ be an arbitrary element of $\mathbb{Q}_\ell^{alg}$. We will show that γ occurs with the same multiplicity in the α_i's as in the β_i's. Let $P(X)$ be the minimal polynomial of γ over $\mathbb{Q}_\ell$. Let $\gamma_1 = \gamma, \gamma_2, \ldots, \gamma_m$ be the roots of $P(X)$. There are no multiplicities. Let d be the multiplicity of γ among the α_i's, possibly zero. By Galois symmetry γ_j also occurs with multiplicity d among the α_i's, for each j. Now if ϵ is small, then

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \gamma_j + \epsilon) = \prod_{i=1}^{n} P(\alpha_i + \epsilon)$$

is proportional to ϵ^{dm} (i.e., $O(\epsilon^{dm})$ and $\Omega(\epsilon^{dm})$). Indeed, each term $(\alpha_i - \gamma_j + \epsilon)$ approaches a nonzero constant if $\alpha_i \neq \gamma_j$, and is proportional to ϵ if $\alpha_i = \gamma_j$. The total number of pairs (i, j) such that $\alpha_i = \gamma_j$ is exactly dm (d for each value of j).

It follows that

$$\lim_{\epsilon \to 0} \frac{\left|\prod_{i=1}^{n} P(\alpha_i + \epsilon)\right|_\ell}{\left|\epsilon^{dm}\right|_\ell}$$

exists and is nonzero. Similarly, if e denotes the multiplicity of γ among the β_i's, then

$$\lim_{\epsilon \to 0} \frac{\left|\prod_{i=1}^{n} P(\beta_i + \epsilon)\right|_\ell}{\left|\epsilon^{em}\right|_\ell}$$

exists and is nonzero. The numerators of the fractions in these two limits are the same, by assumption. The only way both limits can exist and be non-zero is therefore if $em = dm$, implying $e = d$. So γ occurs the same number of times among the α_i's as among the β_i's. As γ was arbitrary, we are done. □

Finally, we prove Assumption 2.1.

Proof (of Assumption 2.1). We need to show that size mod ℓ^k of $C(\mathbb{F}_q)$ is $\emptyset$-definable in the Frobenius garden F_q in terms of the coefficients of C, uniformly across q. By Lemma 3.6, the function which takes (the coefficients of) a smooth projective curve $C/\mathbb{F}_q$ and returns $\alpha_1(C) + \cdots + \alpha_{2g}(C)$ mod ℓ^k is uniformly $\emptyset$-definable across q. It turns out that the value mod ℓ^k of q is also uniformly $\emptyset$-definable across F_q, i.e., for every k and m there is a sentence $\phi_{k,m}$ in the language of gardens such that $F_q \models \phi_{k,m}$ if and only if $q \equiv m$ mod ℓ^k. Specifically, we can take $\phi_{k,m}$ to be

$$\exists y : y^{\ell^k} = 1 \wedge \sigma(y) = y^m,$$

where y is a variable from the appropriate sort that will contain all the ℓ^k-roots of unity.

Now the function which takes (the coefficients of) a smooth projective curve $C/\mathbb{F}_q$ and returns $1 - \alpha_1(C) - \cdots - \alpha_{2g}(C) + q$ mod ℓ^k, or equivalently, returns $|C(\mathbb{F}_q)|$ mod ℓ^k, is uniformly $\emptyset$-definable across the Frobenius gardens.

Consequently, in the terminology of §2, $C(K_1)$ is determined for every smooth projective curve C. Every smooth curve C' differs from some smooth projective curve C by finitely many points, so $C'(K_1)$ is determined as well, proving Assumption 2.1. □