ZETA FUNCTIONS OF EQUIVALENCE RELATIONS OVER FINITE FIELDS

TIBOR BEKE

ABSTRACT. We prove the rationality of the generating function associated to the number of equivalence classes of $\mathbb{F}_{q^k}$-points of a constructible equivalence relation defined over the finite field $\mathbb{F}_q$. This is a consequence of the rationality of Weil zeta functions and of first-order formulas, together with the existence of a suitable parameter space for constructible families of constructible sets.

1. INTRODUCTION

The motivating problem in enumerative terms. Fix a prime power q, and let $\mathbb{F}_{q^k}$ denote the finite field with q^k elements. Let $\mathbf{x} = x_1, x_2, \ldots, x_n$ and $\mathbf{y} = y_1, y_2, \ldots, y_n$ be tuples of variables, and let $S\langle \mathbf{x} \rangle = \bigvee_i \bigwedge_j p_{ij}(\mathbf{x}) \stackrel{?}{=} 0$ and $R\langle \mathbf{x}; \mathbf{y} \rangle = \bigvee_i \bigwedge_j f_{ij}(\mathbf{x}, \mathbf{y}) \stackrel{?}{=} 0$ be finite boolean combinations of polynomial conditions defined over $\mathbb{F}_q$. (That is, $p_{ij}(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}]$ and $f_{ij}(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ are polynomials and '$\stackrel{?}{=}$' is meant to indicate that equalities and not-equalities are both allowed.) R induces a relation on n-tuples from $\mathbb{F}_{q^k}$:

$$\langle a_1, a_2, \ldots, a_n \rangle \sim_R \langle b_1, b_2, \ldots, b_n \rangle \text{ iff } R\langle a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n \rangle \text{ holds.}$$

Assume that when restricted to tuples satisfying the condition $S\langle \mathbf{x} \rangle$, R is an equivalence relation for each k. Write N_k for the cardinality of the set of R-equivalence classes of $\mathbb{F}_{q^k}$-points and consider the generating function

$$z(S/R; t) = \sum_{k=1}^{\infty} N_k \, t^{k-1}.$$

The symbol S/R is (for the time being) just a placeholder, while the letter 'z' is a reminder of the formal analogy with the logarithmic derivative of the Weil zeta function of a variety. Their relationship is summarized in

Theorem 1. There exist a polynomial $p(t)$ with integer coefficients, together with finitely many varieties $\mathcal{W}_i$ over $\mathbb{F}_q$ and coefficients $c_i \in \mathbb{Q}$ such that

$$z(S/R; t) = p(t) + \sum_{i=1}^{N} c_i \frac{d}{dt} \log Z(\mathcal{W}_i, t) \tag{1.1}$$

where $Z(\mathcal{W}_i, t)$ is the Weil zeta function of $\mathcal{W}_i$.

Date: March 11, 2010.

It follows that $z(S/R;t)$ is rational, with partial fraction expansion of the form

$$z(S/R;t) = p(t) \,+\, \sum_i r_i \, \frac{\alpha_i}{1-\alpha_i t}$$

where $r_i \in \mathbb{Q}$ and the α_i are Weil q-numbers of various weights. (Indeed, as a consequence of Deligne's proof of the Weil conjectures, for any $\mathcal{W}/\mathbb{F}_q$ one has

$$\frac{d}{dt} \log Z(\mathcal{W}, t) = \sum_{k=1}^{\infty} \operatorname{card}\left\{\mathcal{W}(\mathbb{F}_{q^k})\right\} t^{k-1} = \sum_j n_j \, \frac{\beta_j}{1-\beta_j t}$$

for certain Weil q-numbers β_j and integers n_j.)

There are examples showing that neither the polynomial 'correction' $p(t)$ nor the assumption that the c_i are non-integral can be omitted from (1.1) in general.

The proof of (1.1) depends on two facts: being able to form the quotient S/R as a geometric object, and being able to count rational points in it. Both of these have been known in the logic community under the names of *elimination of imaginaries for algebraically closed fields* (cf. Poizat [Poi83]) and *rationality of the zeta function of a first-order formula in the language of rings* (cf. Kiefe [Kie76]). Let us state what elimination of imaginaries means in this case, in a direct geometric language.

For a field k, let Constr_k be the category whose objects are affine constructible sets defined over k and whose morphisms are (set-theoretical) functions whose graph is constructible. (See the next section for precise definitions.) Recall that for an equivalence relation $R \rightrightarrows S$ in a category, the quotient $S \xrightarrow{q} Q$ is defined as the coequalizer of the two arrows. This quotient is said to be *effective* if the canonical map $R \to S \times_Q S$ is an isomorphism.

Theorem 2. In Constr_k, equivalence relations have quotients and are effective.

Applying this to the motivating situation (with $k = \mathbb{F}_q$), the problem of counting R-equivalence classes of $\mathbb{F}_{q^k}$-points of S becomes the problem of counting $\mathbb{F}_{q^k}$-points of the quotient $Q = S/R$ *such that* the point corresponds to a non-empty equivalence class of $\mathbb{F}_{q^k}$-points. This becomes subsumed under the following problem: given a constructible subset C of affine space $\mathbb{A}^{n+m}$ over $\mathbb{F}_q$, let

$$N_k = \operatorname{card}\{x \in \mathbb{A}^n(\mathbb{F}_{q^k}) \mid p^{-1}(x) \cap C \text{ has an } \mathbb{F}_{q^k}\text{-point}\}$$

where $\mathbb{A}^{n+m} \xrightarrow{p} \mathbb{A}^n$ is the projection. The corresponding generating function $\sum_{k=1}^{\infty} N_k \, t^{k-1}$ is known to be of the same type as the right-hand side of (1.1). In fact, that counting problem is a very special case of the one for first-order formulas in the language of rings, i.e. ones whose explicit affine form is

$$N_k = \operatorname{card}\{\langle x_1, x_2, \ldots, x_n\rangle \in (\mathbb{F}_{q^k})^n \mid (\mathsf{Q}_1 y_1 \in \mathbb{F}_{q^k})\,(\mathsf{Q}_2 y_2 \in \mathbb{F}_{q^k}) \cdots (\mathsf{Q}_m y_m \in \mathbb{F}_{q^k})\, B\langle \mathbf{x}, \mathbf{y}\rangle\}$$

where each quantifier Q_i is either the universal $\forall$ or the existential $\exists$ one, and B is a boolean combination of polynomial conditions in the tuples of variables $\mathbf{x}$ and $\mathbf{y}$. The rationality of the associated generating function was first established by Kiefe [Kie76]; see Fried–Jarden [FJ05] for a correction and complete proof.

It is easy to extend these considerations to non-affine constructible sets; that is the subject of Prop. 2.4.

Theorem 2 follows from

Theorem 3. Let $\mathcal{X}$, $\mathcal{Y}$ be varieties over a field k, with $\mathcal{X}$ projective. Let C be a constructible subset of $\mathcal{X} \times_k \mathcal{Y}$. There exist a variety $\mathcal{Z}$ and a constructible morphism $\mathcal{Y} \xrightarrow{f} \mathcal{Z}$ over k such that for closed points y_1, y_2 of $\mathcal{Y}$, the fibers C_{y_1} and C_{y_2} (i.e. their projections to $\mathcal{X}$) are the same if and only if $f(y_1) = f(y_2)$.

Applying Theorem 3 when $\mathcal{X} = \mathcal{Y}$ and C is the graph of a constructible equivalence relation (on a constructible subset S of $\mathcal{X}$), the constructible subset $f(S)$ of $\mathcal{Z}$ furnishes a parametrization of C-equivalence classes, which is readily seen to be an effective quotient in the category Constr_k. Theorem 3 is thus also a proof of elimination of imaginaries, different from the ones by Poizat [Poi83] and Holly [Hol93]. It is a stronger statement than just elimination of imaginaries in that it shows the existence of a moduli space for constructible families of constructible sets. Indeed, when C is a family of closed subvarieties of $\mathcal{X}$ indexed by $\mathcal{Y}$ then Theorem 3 is part of the statement that the Hilbert scheme of $\mathcal{X}$ exists. Theorem 3 is proved by reducing the situation to Hilbert schemes with the help of flat stratifications and by expressing C as a suitably canonical and 'fiberwise smoothly varying' boolean combination of closed sets in $\mathcal{X}$.

Since morphisms in the category Constr_k are not necessarily continuous, quotients are much easier to construct than in the delicate world of varieties or schemes. Quotients in Constr_k being *effective* can be thought of as expressing their being "geometric"; this suffices as far as the counting of rational points is concerned. Sections 2 and 3 contain examples and further discussion. The rest of this introduction is devoted to what is *not* contained in this article, esp. work on stacks and the model theory of fields.

Related work and related questions. Let $\mathcal{Y} \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}$ be a groupoid object in the category of schemes of finite type over $\mathbb{F}_q$. (There are thus also structure maps $\mathcal{X} \xrightarrow{i} \mathcal{Y}$ and $\mathcal{Y} \times_{\mathcal{X}} \mathcal{Y} \xrightarrow{m} \mathcal{Y}$ and diagrammatic conditions expressing that m is an associative multiplication with identity i etc.) Two common ways for such groupoid-schemes to arise are as equivalence relations $\mathcal{R} \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}$ in the category of schemes, and as 'action groupoids' $\mathcal{G} \times \mathcal{X} \underset{\mathrm{pr}_2}{\overset{a}{\rightrightarrows}} \mathcal{X}$ corresponding to an action a of the group-scheme $\mathcal{G}$ on $\mathcal{X}$. Let R be the image of $\mathcal{Y}$ in $\mathcal{X} \times_{\mathbb{F}_q} \mathcal{X}$ along s, t. Then R is a constructible equivalence relation on $\mathcal{X}$. (Indeed, this is the most common way for constructible equivalence relations to arise, but see the next section for more examples.)

For two $\mathbb{F}_{q^k}$-points of $\mathcal{X}$ to be R-related means that some point of $\mathcal{Y}$ (defined over, possibly, a finite extension of $\mathbb{F}_{q^k}$) maps to them via s, t. Said slightly differently, let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. Then $\mathcal{Y}(\mathbb{F}) \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}(\mathbb{F})$ is a groupoid (of sets), and the coefficient N_k of $z(\mathcal{X}/R; t)$ is the number of connected components of $\mathcal{Y}(\mathbb{F}) \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}(\mathbb{F})$ that contain an F_{q^k}-point.

Two other — and in many ways, more natural — counting problems associated with a groupoid-scheme$\mathcal{Y} \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}$ as above concern the following sequence of numbers and their generating series (or formal zeta functions):

$$\mu_k := \mu\big\{\, \mathcal{Y}(\mathbb{F}_{q^k}) \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}(\mathbb{F}_{q^k}) \,\big\} \tag{1.2}$$

$$\iota_k := \pi_0\big\{\mathcal{Y}(\mathbb{F}_{q^k}) \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}(\mathbb{F}_{q^k})\big\} \tag{1.3}$$

Note that $\mathcal{Y}(\mathbb{F}_{q^k}) \underset{t}{\overset{s}{\rightrightarrows}} \mathcal{X}(\mathbb{F}_{q^k})$ is a finite groupoid (of sets). The 'measure' μ (much better thought of as an Euler characteristic!) associates to a finite groupoid G the rational number

$$\mu\{G\} = \sum_{\xi \in \pi_0(G)} \frac{1}{\operatorname{card}\{\operatorname{Aut}(\xi)\}}$$

the sum of the reciprocals of the sizes of automorphism groups of objects representing the isomorphism classes of G. $\pi_0\{G\}$ is the number of connected components (number of isomorphism types of objects) of the groupoid G.

With suitable assumptions on $\mathcal{X}$, $\mathcal{Y}$ and the structure maps, the groupoid represents — or is an 'atlas' of — a suitable generalized space (algebraic space, Deligne–Mumford stack, Artin stack, in increasing generality). A beautiful result of Behrend [Beh93] asserts that

$$\mu_k = q^{\dim \mathcal{S}} \sum_{p \geqslant 0} (-1)^p \operatorname{tr} \Phi_q | H^p(\overline{\mathcal{S}}_{\mathrm{sm}}, \mathbb{Q}_l) \tag{1.4}$$

whenever $\mathcal{S} = \{\mathcal{Y} \rightrightarrows \mathcal{X}\}$ is a smooth stack over $\mathbb{F}_q$, $\overline{\mathcal{S}}$ its base extension to an algebraic closure of $\mathbb{F}_q$, Φ_q the *algebraic* Frobenius (note that this is responsible for the appearance of the normalizing factor $q^{\dim \mathcal{S}}$) and $H^*(\overline{\mathcal{S}}_{\mathrm{sm}}, \mathbb{Q}_l)$ denotes l-adic cohomology associated to the smooth site of $\overline{\mathcal{S}}$. He proves that the associated zeta function is rational when $\mathcal{S}$ is a Deligne–Mumford stack.

Behrend's proof of (1.4) proceeds by computing both sides separately, and observing that they are equal. (This is done for quotient stacks in [Beh93], to which the general case is reduced in [Beh03].) It is not clear what form a general Grothendieck–Lefschetz formula would take for algebraic stacks. See, however, Kim [Kim95] for the topological case.

As regards (1.3), one could be more ambitious and consider the sequence

$$(\phi/\psi)_k = \operatorname{card}\big\{\phi(\mathbb{F}_{q^k}) \bmod \psi(\mathbb{F}_{q^k})\big\}$$

where ϕ is a first-order formula in the language of rings over $\mathbb{F}_q$ and ψ is a first-order definable equivalence relation on ϕ. It is a safe guess that the corresponding generating function permits an expression of 'Weil type', cf. (1.1). See Chatzidakis–van den Dries–Macintyre [CvdDM92] for Lang–Weil type estimates on the quantities $(\phi/\psi)_k$. Chatzidakis and Hrushovski [CH99] prove elimination of imaginaries over pseudofinite fields (subject to certain delicate conditions) and their results should settle the rationality of the associated generating function as well.

Kiefe's proof of the rationality of the zeta function of a formula proceeds by establishing (for large enough extensions of the base field $\mathbb{F}_q$) a combinatorial bijection between a suitable integer multiple of the number of tuples satisfying a formula and rational points of an associated variety. Over pseudo-finite fields, the issue of 'large enough' disappears — equivalently, there is no correction term $p(t)$ in (1.1) — and the work of Denef and Loeser provides a motivic interpretation of the summands $Z(\mathcal{W}_i, t)$. (See Denef–Loeser [DL02] and also Hales [Hal05] for a wonderfully illuminating discussion.) The problem of interpreting these counting problems directly in terms of cohomological fixed-point formulas seems to be open.

That R be an *equivalence* relation is essential in all these considerations. One may surmise that for a 'generic' constructible relation R on variety over $\mathbb{F}_q$ (so that no finite iteration of it is an equivalence relation) the generating function associated to the number of R_{eq}-equivalence classes of $\mathbb{F}_{q^k}$-points will not be rational. (Here R_{eq} is the smallest set-theoretic equivalence relation containing R.) The easiest example to experiment with is probably $x \sim_R x^n$ (for some fixed n), but this will be done elsewhere.

Acknowledgements. I am indebted to Endre Szabó, Brian Conrad and Thomas Scanlon for providing essential clues and references. This article would not exist without their help.

2. Quotients, constructible sets, zetas

Recollections on categorical quotients. Let $\mathcal{C}$ be a category. A *relation* on an object X is a jointly monic pair of arrows $R \underset{r_2}{\overset{r_1}{\rightrightarrows}} X$. It is a *categorical equivalence relation* if for all objects Z of $\mathcal{C}$, the pair r_1, r_2 induces an equivalence relation on $\hom_{\mathcal{C}}(Z, X)$. If $\mathcal{C}$ has finite limits (i.e. pullbacks and a terminal objects) then a relation on X amounts to a subobject $R \rightarrowtail X \times X$ and being an equivalence relation can be phrased by diagrammatic analogues of the usual notions of reflexivity, symmetry and transitivity. (See e.g. Borceux [Bor94] vol.II. 2.5 for extensive discussion.) A *categorical quotient* $X \xrightarrow{q} Q$ of an equivalence relation is a coequalizer of $R \underset{r_2}{\overset{r_1}{\rightrightarrows}} X$, i.e. a morphism out of X that is initial among those with equal compositions with r_1 and r_2. This quotient is said to be *effective* if the square

$$\begin{tikzcd} R \arrow[r, "r_1"] \arrow[d, "r_2"'] & X \arrow[d, "q"] \\ X \arrow[r, "q"] & Q \end{tikzcd}$$

is a pullback.

When objects X of the category are equipped with 'underlying sets' whose elements biject with morphisms from the terminal object into X, then the effectiveness condition implies that two elements of X are identified in the quotient if and only if they are R-related; in general, it says the same about Z-valued points.

In the context of algebraic geometry, the data $R \overset{r_1}{\underset{r_2}{\rightrightarrows}} X$ (say, two maps between two varieties) may have different categorical quotients (possibly none), depending on the category one works in; see Knutson [Knu71] and Kollár [Kol09] for many examples. Even if a categorical quotient exists, it may be 'pathological', which is often exhibited by the fact that it is not effective. (Consider, for example, collapsing the complement of the origin in affine space to a point.) So it is quite a pleasant surprise that the category Constr_k of affine constructible sets and morphisms (see below) has effective equivalence relations. Ultimately, this is due to the fact that given an equivalence relation $R \overset{r_1}{\underset{r_2}{\rightrightarrows}} X$ in Constr_k, the object X can be Zariski-locally 'taken apart' and stratified into pieces over which multi-valued choice functions (i.e. sections) of R exist. The existence of effective quotients in Constr_k seems to have few implications for the (much harder) problem of GIT quotients or quotients of étale equivalence relations, but it suffices for counting points.

Definition 2.1. For a field k, let Constr_k be the category whose objects are affine constructible sets $C \subseteq \mathbb{A}^n_k$ (any $n > 0$) and where a morphism $\langle C, \mathbb{A}^n_k\rangle \xrightarrow{f} \langle D, \mathbb{A}^m_k\rangle$ is a (set-theoretic) function $C \xrightarrow{f} D$ whose graph is a constructible subset of $\mathbb{A}^{n+m}_k$.

Remark on algebraic geometric vs. logic conventions. Readers of the model-theoretic literature may find the following definition more natural. Choose an algebraic closure $\overline{k}$ of k. Let Constr^g_k be the category whose objects are pairs $\langle S, n\rangle$ where S is a subset of $\overline{k}^n$ that is the set of tuples satisfying a (finite) boolean combination of (quantifier-free) polynomial conditions, where the polynomials have coefficients from k. Morphisms are set-theoretic functions whose graphs belong to Constr^g_k.

The categories Constr_k and Constr^g_k are equivalent, though of course their objects are not literally the same. (The functor of taking geometric, i.e. $\mathrm{spec}(\overline{k})$-points of the former furnishes the equivalence.) Since having effective quotients of equivalence relations is an 'abstract' categorical property of Constr_k, the proof of Theorem 2 (and much of this paper, in fact) could be cast in either of these equivalent languages, and in this context there is scant reason for preferring one over the other. We keep the language of algebraic geometry as 'default' for the last part of this paper, since it is the natural environment for Hilbert schemes and notions such as flatness.

Under categorical product and coproduct, Constr_k forms a distributive category. The isomorphism classes of its objects form a semiring, the Grothendieck ring of which is isomorphic to the Grothendieck ring of varieties. But as the category Constr_k itself is seldom used, we list some of its properties. Any morphism $\langle C, \mathbb{A}^n_k\rangle \xrightarrow{f} \langle D, \mathbb{A}^m_k\rangle$ can be represented by data $C_i \xrightarrow{f_i} D$ where C_i, $i = 1, 2, \ldots, n$, is a decomposition of C into constructible subsets and f_i is a regular morphism with domain some neighborhood of C_i in $\mathbb{A}^n$. Given objects $C_i \subseteq \mathbb{A}^{n_i}_k$, $i = 1, 2, \ldots, n$, choose n closed points p_i of $\mathbb{A}_k$ and let $C_i \mapsto C_i \times p_i$ be embeddings $C_i \to \mathbb{A}^{n_i}_k \times \mathbb{A}_k$ with disjoint image. Their union serves as a coproduct of the C_i. Any k-point of an affine space is a terminal object. To compute the pullback of $\langle C_i, \mathbb{A}^{n_i}_k\rangle \xrightarrow{f} \langle D, \mathbb{A}^m_k\rangle$ $(i = 1, 2)$, decompose the C_i into a disjoint union of locally closed subvarieties, compute their pullback as varieties, and take their disjoint union.

Thus finite limits exist in Constr_k. If $C \xrightarrow{f} D$ is a morphism, note that fibers of f over closed points of D can be computed set-theoretically.

For a constructible set S, let $\{S\}$ denote its underlying set of points and $|S|$ its underlying set of closed points. A relation $R \rightrightarrows S$ in Constr_k induces a relation on $\{S\}$ and on $|S|$ via the natural map

$$\{R\} \hookrightarrow \{S \times_k S\} \twoheadrightarrow \{S\} \times \{S\}.$$

The following proposition will not be used in this paper; it is included for completeness.

Proposition 2.2. *Let $R \rightrightarrows S$ be a relation in Constr_k. The following are equivalent:*

(i) *R is a categorical equivalence relation on S.*
(ii) *R induces an equivalence relation on $\{S\}$.*
(iii) *R induces an equivalence relation on $|S|$.*

Proof. (i)⇒(ii)⇒(iii) are immediate. To show (iii)⇒(i), note that saying that R is a categorical equivalence relation on S amounts to saying that $\Delta \subseteq R$, $\sigma(R) \subseteq R$ and $\mathrm{pr}_{13}(R) \subseteq R$ where $\Delta \subset S \times_k S$ is the diagonal, $S \times_k S \xrightarrow{\sigma} S \times_k S$ swaps the factors, and $S \times_k S \times_k S \xrightarrow{\mathrm{pr}_{13}} S \times_k S$ is the projection. But (as computed in the category Constr_k) these amount to inclusions of point-sets. Now if C_1, C_2 are constructible subsets of $\mathbb{A}^n_k$ and for all closed points p of $\mathbb{A}^n_k$, $p \in C_1$ iff $p \in C_2$, then $C_1 = C_2$. (This is a consequence of the Nullstellensatz.) Therefore, whether a morphism in Constr_k is a monomorphism (resp. isomorphism) can be detected on closed points. □

Given the rationality of generating functions associated to existential formulas, Theorem 2 implies Theorem 1 in a straightforward way. Below, the ground field will be $k = \mathbb{F}_q$.

Proposition 2.3. *Let $R \rightrightarrows S$ be an equivalence relation in Constr_k with effective quotient $S \xrightarrow{r} Q$. Then there is a bijection*

$$\left\{S(\mathbb{F}_{q^k})/R\right\} \xrightarrow{u} \left\{x \in Q(\mathbb{F}_{q^k}) \mid r^{-1}(x) \text{ contains an } \mathbb{F}_{q^k}\text{-point.}\right\}$$

Proof. u sends an $\mathbb{F}_{q^k}$-point x of S to $r(x)$. Since r is defined over $\mathbb{F}_q$ and respects R, this results in a well-defined map from $\left\{S(\mathbb{F}_{q^k})/R\right\}$ to $Q(\mathbb{F}_{q^k})$. Since $R \to S \times_Q S$ is an isomorphism, two points of S get identified if and only if they are R-related. Hence u is injective. The image of u is (tautologously) the displayed set. □

At this point, as mentioned in the introduction, one can appeal to the theorem of Kiefe–Fried–Jarden (see [FJ05] Theorem 31.3.7, and also the Notes at the end of Ch. 31).

One can introduce a 'global' version of Constr_k whose objects are pairs $\langle C, \mathcal{X}\rangle$ with C a constructible subject of the variety $\mathcal{X}$ over k, and where a morphism $\langle C, \mathcal{X}\rangle \to \langle D, \mathcal{Y}\rangle$ is a set-theoretic map whose graph is a constructible subset of $\mathcal{X} \times_k \mathcal{Y}$, and construct effective quotients. As far as point-counting is concerned, however, the affine case already implies

Proposition 2.4. *Let R be a constructible equivalence relation on the variety $\mathcal{X}$. Then the generating function $z(\mathcal{X}/R; t)$ has the form of (1.1).*

Proof. Choose a cover of $\mathcal{X}$ by open affines $\mathcal{U}_i \hookrightarrow \mathcal{X}$, $i = 1, 2, \ldots, N$. That amounts to a constructible equivalence relation $Q \rightrightarrows \mathcal{U}$ on $\mathcal{U} = \sqcup_{i=1}^N \mathcal{U}_i$ such that (on underlying points) $\mathcal{X} = \mathcal{U}/Q$. The given R restricts to a constructible equivalence relation on each $\mathcal{U}_i$; the disjoint union of these is a constructible equivalence relation on $\mathcal{U}$ that we will denote T. Let $Q * T$ be the smallest (set-theoretical) equivalence relation on $\mathcal{U}$ containing both Q and T. Thus, for underlying points $x, y \in \mathcal{U}$, $x \sim_{Q*T} y$ if and only if there exist $x_i \in \mathcal{U}$, $i = 0, 1, \ldots, n$ such that $x = x_0$, $y = x_n$ and for all $0 \leqslant i < n$, Qx_ix_{i+1} or Tx_ix_{i+1}.

Thinking of these x_i as points of $\mathcal{X}$, note that they are all R-related. Suppose there existed i, j such that x_i and x_j both belong to $\mathcal{U}_p$ for some $1 \leqslant p \leqslant N$. Since x_i and x_j are R-related (as points of $\mathcal{X}$), they will then be T-related as points of $\mathcal{U}$. Thence, in the chain $x_0, x_1, \ldots, x_n$, at most two points from each piece $\mathcal{U}_p$ of the cover need to be used. By the pigeonhole principle, it is enough to consider chains of length at most $2N$. This permits the description of $Q * T$ as the union of finitely many relations, each of which is a finite composite of constructible relations. $Q * T$ is therefore constructible.

As point-sets,

$$\mathcal{X}/R = \big(\mathcal{U}/Q\big)/T = \mathcal{U}/Q * T$$

Working over a finite field $\mathbb{F}_q$, since all Q-identifications were gluing along open sets,

$$\mathcal{X}(\mathbb{F}_{q^k})/R = \mathcal{U}(\mathbb{F}_{q^k})/Q * T$$

But $Q * T$ is a constructible equivalence relation on the affine $\mathcal{U}$. If the relation R is only given on a constructible subset S of $\mathcal{X}$, extend it to a constructible equivalence relation on all of $\mathcal{X}$ by the identity relation outside S. This finishes the reduction of the non-affine case to the affine one. $\square$

We give some examples of equivalence relations whose zeta functions can be worked out 'by hand'.

Example 2.5. Let $\mathcal{X}/\mathbb{F}_q$ be a variety and let $\sim_{\mathcal{X}}$ be the full relation $\mathcal{X} \times_k \mathcal{X}$. Then

$$z(\mathcal{X}/\sim_{\mathcal{X}}; t) = \sum_{k=1}^{\infty} E_k \cdot t^{k-1}$$

where

$$E_k = \begin{cases} 1 & \text{if } \mathcal{X}(\mathbb{F}_{q^k}) \text{ is non-empty} \\ 0 & \text{if } \mathcal{X}(\mathbb{F}_{q^k}) \text{ is empty.} \end{cases}$$

Decomposing $\mathcal{X}$ into absolutely irreducible subvarieties and using Lang-Weil, it follows that there exist positive integers n_i such that for large enough k, the set $\mathcal{X}(\mathbb{F}_{q^k})$ is non-empty iff k is a multiple of one of the n_i. Thence $z(\mathcal{X}/\sim_{\mathcal{X}}; t)$ is a sum of rational functions of the form $\dfrac{t^{m_i}}{1 - t^N}$ where N is the least common multiple of the n_i, minus a sum of monomials. (See also Example 2.8.)

Example 2.6. Fix some positive integer n and consider the equivalence relation on $\mathbb{A}^1_{\mathbb{F}_q}$ defined (in polynomial terms) by $x^n = y^n$. Setting e.g. $n = 3$ and with $q \equiv -1 \pmod 3$,

$$N_k = \begin{cases} 1 + \frac{q^k - 1}{3} & \text{if } k \text{ is even} \\ q^k & \text{if } k \text{ is odd} \end{cases}$$

$$z(\mathbb{A}^1/x^3 \sim y^3; t) = \frac{1}{3} \cdot \frac{1}{1-t} - \frac{1}{3} \cdot \frac{1}{1+t} + \frac{2}{3} \cdot \frac{q}{1-qt} + \frac{1}{3} \cdot \frac{q}{1+qt}$$

Thus the coefficients c_i in Theorem 1 will not be integral in general.

Example 2.7. Let $\mathcal{X} = \mathbb{A}^n \times \mathbb{A}^m$ with a distinguished constructible subset $C \subseteq \mathcal{X}$, and let $\mathrm{pr} : \mathbb{A}^n \times \mathbb{A}^m \to \mathbb{A}^n$ be the projection. Let us revert to logical notation (boldface symbols stand for vectors of variables, and set-membership is shorthand for the evaluation of a boolean combination of polynomial conditions) and consider the following equivalence relation $R\langle \mathbf{z}_1, \mathbf{z}_2 \rangle$ on $\mathcal{X}$

$$\big(\mathbf{z}_1 = \mathbf{z}_2\big) \text{ or } \big(\mathbf{z}_1 \in C \text{ and } \mathbf{z}_2 \in C \text{ and } \mathrm{pr}(\mathbf{z}_1) = \mathrm{pr}(\mathbf{z}_2)\big)$$

Then $\mathrm{card}\{\mathcal{X}(\mathbb{F}_{q^k})/R\} =$

$$= \mathrm{card}\,\big\{(\mathcal{X} \setminus C)(\mathbb{F}_{q^k})\big\} + \mathrm{card}\,\big\{\mathbf{x} \in \mathbb{A}^n(\mathbb{F}_{q^k}) \mid \exists \mathbf{y} \in \mathbb{A}^m(\mathbb{F}_{q^k}) \text{ such that } (\mathbf{x}, \mathbf{y}) \in C\big\}$$

$$= \mathrm{card}\,\big\{(\mathcal{X} \setminus C)(\mathbb{F}_{q^k})\big\} + \mathrm{card}\,\big\{\mathbb{A}^n(\mathbb{F}_{q^k})\big\} - \mathrm{card}\,\big\{\mathbf{x} \in \mathbb{A}^n(\mathbb{F}_{q^k}) \mid \forall \mathbf{y} \in \mathbb{A}^m(\mathbb{F}_{q^k})\,,\ (\mathbf{x}, \mathbf{y}) \notin C\big\}$$

where $(\mathcal{X} \setminus C)$ is the complement of C in $\mathcal{X}$. So the rationality of generating functions for $\mathcal{X}/R$ imply those of counting problems involving one block of quantifiers over a finite field.

More generally, zeta functions of first-order formulas with n quantifier alternations and of first-order equivalence relations defined by $n-1$ quantifier alternations are mutually expressible. For us, however, the case of a single block of existential quantifiers (and ultimately, the rationality of Weil zeta functions) will serve as 'black boxes'.

Example 2.8. Specialize Example 2.7 by taking $m = 1$ and $C \subset \mathbb{A}^n \times \mathbb{A}^1$ to be the *complement* of the set defined by

$$\big\{(\mathbf{x}, y) \in \mathbb{A}^n \times \mathbb{A}^1 \mid \mathbf{x} \in A \text{ and } y^{q^N} = y\big\}$$

where A is a constructible subset of $\mathbb{A}^n$ and N some unspecified positive integer. Then

$$\mathrm{card}\{\mathcal{X}(\mathbb{F}_{q^k})/R\} = \mathrm{card}\,\big\{(\mathcal{X} \setminus C)(\mathbb{F}_{q^k})\big\} + \mathrm{card}\,\big\{\mathbb{A}^n(\mathbb{F}_{q^k})\big\} - a_k$$

where

$$a_k = \begin{cases} \mathrm{card}\,\big\{A(\mathbb{F}_{q^k})\big\} & \text{if } k|N \\ 0 & \text{otherwise.} \end{cases}$$

Thus $z(\mathcal{X}/R; t)$ differs from $\frac{d}{dt} \log Z(\mathcal{X} \setminus C, t) + \frac{d}{dt} \log Z(\mathbb{A}^n, t)$ by the polynomial $p(t) = \sum_{k=1}^{N} a_k\, t^k$. (In fact, any polynomial with non-negative integer coefficients can appear as the 'error term' in the zeta function of an equivalence relation.)

3. Parametrizing and quotienting constructible sets

For a field k and varieties $\mathcal{X}$, $\mathcal{Y}$, a *constructible family of constructible subsets of $\mathcal{X}$ parametrized by $\mathcal{Y}$* will simply mean a constructible subset C of $\mathcal{X} \times_k \mathcal{Y}$. Suppose one could find a variety $\mathcal{Z}$ and morphism $\mathcal{Y} \xrightarrow{f} \mathcal{Z}$ over k such that for closed points y_1, y_2 of $\mathcal{Y}$, the fibers S_{y_1} and S_{y_2} (i.e. their projections to $\mathcal{X}$) are the same if and only if $f(y_1) = f(y_2)$. This specializes to the formation of quotients in the category Constr_k: taking $\mathcal{X} = \mathcal{Y}$ and C to be the graph of a constructible equivalence relation on a constructible subset S of $\mathcal{X}$, the map $S \xrightarrow{f} f(S)$ will serve as S/C.

When C is a family of closed subvarieties of $\mathcal{X}$ parametrized by $\mathcal{Y}$, the object $\mathcal{Z}$ can be taken to be the Hilbert scheme of $\mathcal{X}$, equipped with a universal family such that any (proper, flat) family of closed subschemes of $\mathcal{X}$ arises from it uniquely via pullback. Point-set theoretically, by definition, any constructible set can be written as a boolean combination of Zariski-closed sets. A modicum of care is needed to find an expression that varies suitably 'continuously' in flat families. This is done in Prop. 3.4 and Lemma 3.5 below. Using flat stratifications, it is then easy to combine the data into an object that is universal the way the Hilbert scheme is, but in the category Constr_k.

The appearance of the Hilbert scheme would render this method of constructing quotients all but hopeless for computations. Holly [Hol93] has given a beautifully direct proof of elimination of imaginaries over algebraically closed fields that amounts to a stand-alone and constructive proof of Theorem 2. For completeness and comparison, let us outline her argument here in a geometric form, valid over any field k. It begins with the observation that though epimorphisms do not split in Constr_k, finitely multi-valued sections exists. More precisely, let S be a constructible subset of $\mathbb{A}_k^n \times \mathbb{A}_k^m$. Then there exist a constructible subset s of $\mathbb{A}_k^n \times \mathbb{A}_k^m$ and an integer N such that

(i) $s \subseteq S$
(ii) for all $x \in \mathbb{A}_k^n$, s_x is non-empty if S_x is
(iii) for all $x \in \mathbb{A}_k^n$, $\mathrm{card}\{s_x\} \leqslant N$
(iv) if $x_1, x_2 \in \mathbb{A}_k^n$ are such that $S_{x_1} = S_{x_2}$ then $s_{x_1} = s_{x_2}$.

(Here s_x is shorthand for $\{y \in \mathbb{A}_k^m \mid \langle x, y\rangle \in s\}$ as usual.)

One can find an injective morphism t from the space of unordered tuples from $\mathbb{A}_k^m$ of cardinality at most N, into $\mathbb{A}_k^M$ for some suitable M. Composing s with t, one obtains a morphism $\mathbb{A}_k^n \xrightarrow{f} \mathbb{A}_k^M$ with the property that if x_1, x_2 are such that $S_{x_1} = S_{x_2}$ then $f(x_1) = f(x_2)$. Note that the converse is not claimed (and does not necessarily hold!), i.e. in general the 'code' f does not separate the fibers of S.

Suppose, however, that S is the graph of a constructible equivalence relation (on a constructible subset of $\mathbb{A}_k^n = \mathbb{A}_k^m$.) Then S_{x_1} and S_{x_2} are either the same or disjoint, so, by property (i) and the injectivity of t, $f(x_1) = f(x_2)$ will hold if and only if $S_{x_1} = S_{x_2}$. So being able to satisfy (i) through (iv) suffices for the construction of quotients by equivalence relations.

Proposition 3.1. *Let S be a constructible subset of $\mathbb{A}_k^n \times \mathbb{A}_k^m$. Then there exist a constructible set s and an integer N with the properties (i) through (iv).*

First, an easy

Lemma 3.2. *Let $X \xrightarrow{f} Y$ be a map in Constr_k. The locus $\{y \in Y \mid f^{-1}(y) \text{ is infinite}\}$ is a constructible subset of Y.*

Proof. Let X_n be the n-fold deleted fiber product of X over Y; that is to say, X_n is $X \times_Y X \times_Y \cdots \times_Y X$ from which one removes the 'fat diagonal', the locus of tuples some of whose coordinates are equal. The image of X_n in Y, which is a constructible subset of Y, is the locus of points above which the fiber of f has at least cardinality n. By constructibility, there is a finite upper bound on the cardinalities of the finite fibers of f, implying the claim. □

The proof of Prop. 3.1 is then by induction on m. For $m = 1$, let $C_{\mathsf{fin}} \sqcup C_{\mathsf{inf}}$ be the decomposition of $\mathbb{A}^n_k$ into the loci of x such that S_x is finite resp. infinite. Over C_{fin}, let s be the full relation (all of S). Over C_{inf}, by constructibility, the fibers are cofinite subsets of $\mathbb{A}_k$; moreover, there is an upper bound K on the cardinality of $\mathbb{A}_k - S_x$ for $x \in C_{\mathsf{inf}}$. Now let W be a finite constructible subset of $\mathbb{A}_k$ of cardinality greater than K and let $s = \{\langle x, y\rangle \mid y \in S_x \cap W\}$ for $x \in C_{\mathsf{inf}}$. The existence of the uniform bound N again follows by constructibility of s.

Suppose now that the requisite s can be found whenever $m < M$ and let $S \subseteq \mathbb{A}^n_k \times \mathbb{A}^M_k$ be given. Write $M = i + j$ with $0 < i, j < M$ and write pr_n resp. pr_{n+i} for the projection from $\mathbb{A}^n_k \times \mathbb{A}^M_k$ to $\mathbb{A}^n_k$ resp. $\mathbb{A}^{n+i}_k$ (remembering the first n resp. $n+i$ coordinates). Considering $\mathrm{pr}_{n+i}(S)$ as subset of $\mathbb{A}^n_k \times \mathbb{A}^i_k$, one has a multi-valued section s_0 by the induction hypothesis. Considering S as subset of $\mathbb{A}^{n+i}_k \times \mathbb{A}^j_k$, again there is a multi-valued section s_1 by the induction hypothesis. The relation s on $\mathbb{A}^n_k \times \mathbb{A}^{i+j}_k$ defined by '$\langle x, y, z\rangle$ such that $s_0(x, y)$ and $s_1(\langle x, y\rangle, z)$' then does what is required. (Here x, y, z belong to $\mathbb{A}^n_k$, $\mathbb{A}^i_k$, $\mathbb{A}^j_k$ respectively.) □

The tuple-coding function t exists by elementary invariant theory, starting from the fact that the algebra of invariants under the action of Σ_N on the polynomial ring

$$\mathbb{Z}[x_{11}, x_{12}, \ldots, x_{1m}, \ldots, \ldots, x_{N1}, x_{N2}, \ldots, x_{Nm}]$$

is finitely generated. (See Holly [Hol93] for a direct description.)

We now turn to the proof of Theorem 3 and constructible quotients via Hilbert schemes.

Good stratifications of constructible families. Let $\mathcal{X}$ be a variety over the field k and $C \subseteq \mathcal{X}$ constructible with closure $Z_0 = \overline{C}$. Let C_1 be the set-theoretic difference $Z_0 - C$. Then C_1 is constructible and as long as $C \neq \varnothing$, one has $\dim C_1 < \dim C$. (The dimension of a constructible set is defined to be that of its closure; the dimension of a Zariski-closed set will mean its combinatorial dimension, i.e. the supremum of the lengths of its properly decreasing chains of closed irreducible subsets.) Iterating, it follows that any constructible C possesses boolean presentations of the form

$$\begin{aligned} C &= Z_0 - C_1 \\ &= Z_0 - (Z_1 - C_2) \\ &= Z_0 - (Z_1 - (Z_2 - C_3)) \\ &\cdots \\ &= Z_0 - \Big(Z_1 - \big(Z_2 - (\cdots - (Z_{i-1} - C_i)..)\big)\Big) = \ldots \end{aligned}$$

where $Z_i = \overline{C_i}$, and the sequence of sets C_i is defined inductively by $C_0 = C$, $C_{i+1} = \overline{C_i} - C_i = Z_i - C_i$. The C_i form a sequence of constructible subsets of $\mathcal{X}$ of decreasing dimension, hence terminating at the empty set. If $C_n \neq \varnothing$ but $C_{n+1} = \varnothing$, we will refer to the boolean expression

$$Z_0 - \Big(Z_1 - \big(Z_2 - (\cdots - (Z_{n-1} - Z_n)..)\Big)$$

thus obtained as the *canonical presentation of* C. It is uniquely determined by $C \subseteq \mathcal{X}$.

Let C be a constructible subset of $\mathcal{X} \times_k \mathcal{Y}$ with canonical presentation $C = Z_0 - \Big(Z_1 - \big(Z_2 - (\cdots - (Z_{n-1} - Z_n)..)\Big)$. Over a closed point y of $\mathcal{Y}$, the fiber C_y of C is understood set-theoretically; it is a constructible subset of X_y.

Definition 3.3. We will say that $C \subseteq \mathcal{X} \times_k \mathcal{Y}$ is *good* if for every closed point y of $\mathcal{Y}$, the canonical presentation of C_y in X_y equals

$$Z_{0,\,y} - \Big(Z_{1,\,y} - \big(Z_{2,\,y} - (\cdots - (Z_{n-1,\,y} - Z_{n,\,y}) \dots \big)\Big)$$

where $Z_{i,\,y}$ is the fiber of Z_i over y.

Proposition 3.4. *Given a constructible $C \subseteq \mathcal{X} \times_k \mathcal{Y}$, there exists a stratification of $\mathcal{Y}$ into finitely many locally closed subvarieties $\mathcal{Y}_i$ such that for each i, the restriction of C to the i^{th} stratum — that is, $C_i = C \cap (\mathcal{X} \times_k \mathcal{Y}_i)$ considered as constructible subset of $\mathcal{X} \times_k \mathcal{Y}_i$ — is good.*

The proof follows by iterating

Lemma 3.5. *Let $\mathcal{W} \xrightarrow{f} \mathcal{Y}$ be a morphism of varieties over k and C a constructible subset of $\mathcal{W}$. For closed $y \in Y$, write $\mathrm{cl}(C_y)$ for the closure of $C \cap f^{-1}(y)$ in $f^{-1}(y)$ and $\mathrm{cl}(C)$ for the closure of C in $\mathcal{W}$. There exists a non-empty open subset U of $\mathcal{Y}$ such that for $y \in U$, one has $\mathrm{cl}(C_y) = \mathrm{cl}(C)_y$.*

Indeed, the lemma implies (by noetherian induction) that $\mathcal{Y}$ can be stratified into finitely many locally closed subvarieties over each of which, closure of the fiber of C equals the fiber of its closure. But this is the first stage of the construction of the canonical presentation of C; at the second stage, one takes the difference of $\mathrm{cl}(C)$ and C and can apply the lemma again. (Note that it does not follow that the canonical presentation has the same length over each member of the stratification; only that over each stratum, taking the canonical presentation commutes with taking the fiber.)

Proof of the lemma. Note that if the claim holds for constructible C_1, C_2 in $\mathcal{W}$ then it also holds for their union. Decomposing C into a disjoint union of locally closed subvarieties, it thus suffices to consider the case when $\mathcal{W}$ is a variety and C equals $\mathcal{W}$ minus a Zariski-closed set S. If S has the same dimension as $\mathcal{W}$ then (since $\mathcal{W}$ is assumed irreducible) the statement is vacuously true; so assume $\dim(S) < \dim(\mathcal{W})$. Also without loss of generality, f is dominant and $\mathcal{Y}$ irreducible. By generic flatness, there exists a non-empty open subset V_1 of $\mathcal{Y}$ such that for $y \in V_1$, $f^{-1}(y)$ is non-empty and each of its irreducible components has dimension $d = \dim(\mathcal{W}) - \dim(\mathcal{Y})$. On a non-empty open subset V_2 of $\mathcal{Y}$, the dimension of the fiber S_y of S is less than d. One can now set $U = V_1 \cap V_2$. Indeed, for $y \in U$, $C_y = f^{-1}(y) - S_y$ is an algebraic set each of whose irreducible components has dimension d, minus a set of dimension less than d. Thus $\mathrm{cl}(C_y) = f^{-1}(y) = \mathrm{cl}(C)_y$ as required. $\square$

Suppose now that one has a good stratification for a family $C \subseteq \mathcal{X} \times_k \mathcal{Y}$. Consider the canonical presentation of C restricted to the i^{th} stratum:

$$C_i = Z_{0,\,i} - \Big(Z_{1,\,i} - \big(Z_{2,\,i} - (\cdots - (Z_{n_i - 1,\,i} - Z_{n_i,\,i}) \ldots) \big) \Big)$$

For each of $j = 1, 2, \ldots, n_i$, there exists a flattening stratification of $\mathrm{pr}_2(Z_{j,\,i}) \subseteq \mathcal{Y}$, over the strata of which $Z_{j,\,i}$ restricts to a flat family. These flattening stratifications have a common refinement; so the following definition is non-vacuous:

Definition 3.6. A *good and flat stratification* for the constructible $C \subseteq \mathcal{X} \times_k \mathcal{Y}$ consists of a stratification of $\mathcal{Y}$ into finitely many locally closed subvarieties $\mathcal{Y}_i$ such that for each i, the restriction C_i of C to $\mathcal{X} \times_k \mathcal{Y}_i$ has canonical presentation

$$C_i = Z_{0,\,i} - \Big(Z_{1,\,i} - \big(Z_{2,\,i} - (\cdots - (Z_{n_i - 1,\,i} - Z_{n_i,\,i}) \ldots) \big) \Big)$$

that is good *and* where each boolean summand $Z_{j,\,i}$ is flat over $\mathcal{Y}_i$.

Assume now $\mathcal{X}$ projective, so the Hilbert scheme $\mathrm{Hilb}(\mathcal{X})$ exists. Since the individual $Z_{j,\,i}$ form flat families over the respective bases $\mathcal{Y}_i$, they are classified by morphisms $\mathcal{Y}_i \xrightarrow{p_{ij}} \mathrm{Hilb}(\mathcal{X})$. The morphisms f_i with these as components

$$f_i : \quad \mathcal{Y}_i \xrightarrow{\langle p_{i1}, p_{i2}, \ldots, p_{in_i} \rangle} \mathrm{Hilb}(\mathcal{X})^{n_i}$$

together comprise a constructible map $\mathcal{Y} \xrightarrow{f} \mathcal{Z}$ into a finite disjoint union of products of components of $\mathrm{Hilb}(\mathcal{X})$. (Since $\mathcal{Y}_i$ is quasi-compact, f_i meets only finitely many components of $\mathrm{Hilb}(\mathcal{X})^{n_i}$, corresponding to certain tuples of Hilbert polynomials, suppressed from notation.)

Consider two closed points x, y of $\mathcal{Y}$ with, say, $x \in \mathcal{Y}_i$ and $y \in \mathcal{Y}_j$. The fibers C_x and C_y (thought of as constructible subsets of $\mathcal{X}$) are the same if and only if they have the same canonical presentation within $\mathcal{X}$. Since the $\mathcal{Y}_i$, $\mathcal{Y}_j$ were part of a good stratification, that happens if and only if the fibers over x (resp. over y) of the canonical presentation of C restricted to $\mathcal{Y}_i$ (resp. $\mathcal{Y}_j$) coincide, if and only if they are classified by the same tuple of points in $\mathrm{Hilb}(X)$, if and only if $f(x) = f(y)$ in $\mathcal{Z}$. So $f(\mathcal{Y}) \subseteq \mathcal{Z}$ — arising with the help of any good and flat stratification for $C \subseteq \mathcal{X} \times_k \mathcal{Y}$ — is a constructible set parametrizing the isomorphism types of fibers of the constructible family C.

One could now go further and exhibit a tautologous constructible family $U \subseteq \bigsqcup_i \, \mathcal{X} \times \mathrm{Hilb}(\mathcal{X})^{n_i}$ fitting into a diagram

$$\begin{tikzcd}
C \arrow[r, dotted] \arrow[d, tail] & U \arrow[d, tail] \\
\mathcal{X} \times \mathcal{Y} \arrow[r, dotted] \arrow[d, two heads] & \bigsqcup_i \mathcal{X} \times \mathrm{Hilb}(\mathcal{X})^{n_i} \arrow[d, two heads] \\
\mathcal{Y} \arrow[r, dotted] & \bigsqcup_i \mathrm{Hilb}(\mathcal{X})^{n_i}
\end{tikzcd}$$

where the first vertical arrow is an inclusion and the second one a projection. U is given, over the image of each stratum $\mathcal{Y}_i$, by the canonical boolean expression whose summands are parametrized by n_i-tuples of points in $\mathrm{Hilb}(\mathcal{X})$. The horizontal dotted arrows are constructible morphisms, i.e. graphs of morphisms from a stratification of the domain to the target.

Note that choices have been made along the way. Though some of those could be eliminated (for example, by making use of the — unique — coarsest flat stratification), the resulting diagram becomes a pullback only in the category Constr_k, taking the reduced structure on $\mathrm{Hilb}(\mathcal{X})$.

REFERENCES

[Beh93] Kai A. Behrend, *The Lefschetz trace formula for algebraic stacks*, Inventiones Mathematicae **112** (1993), no. 1, 127–149.

[Beh03] ______, *Derived l-adic categories for algebraic stacks*, vol. 163, Mem. Amer. Math. Soc., no. 774, American Mathematical Society, 2003.

[Bor94] Francis Borceux, *Handbook of categorical algebra, vol.I-III.*, Cambridge University Press, 1994.

[CH99] Zoé Chatzidakis and Ehud Hrushovski, *Model theory of difference fields*, Transactions of the American Mathematical Society **351** (1999), no. 8, 2997–3071.

[CvdDM92] Zoé Chatzidakis, Lou van den Dries, and Angus Macintyre, *Definable sets over finite fields*, J. Reine Angew. Math. **427** (1992), 107–135.

[DL02] J. Denef and F. Loeser, *Motivic integration and the Grothendieck group of pseudo-finite fields*, Proceedings of the International Congress of Mathematicians (ICM 2002), vol. 2, Higher Education Press, Beijing, 2002, pp. 13–23.

[FJ05] Michael Fried and Moshe Jarden, *Field arithmetic. Second edition*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), no. 11, Springer-Verlag, 2005.

[Hal05] Thomas Hales, *What is motivic measure?*, Bulletin of the American Mathematical Society (N.S.) **42** (2005), no. 2, 119–135.

[Hol93] Jan Holly, *Definable operations on sets and elimination of imaginaries*, Proceedings of the American Mathematical Society **117** (1993), no. 4, 1149–1157.

[Kie76] Catarina Kiefe, *Sets definable over finite fields: their zeta-functions*, Transactions of the American Mathematical Society **223** (1976), 45–59.

[Kim95] Minhyong Kim, *A Lefschetz trace formula for equivariant cohomology*, Ann. Sci. cole Norm. Sup. (4) **28** (1995), no. 6, 669–688.

[Knu71] Donald Knutson, *Algebraic spaces*, Lecture Notes in Mathematics, no. 203, Springer-Verlag, 1971.

[Kol09] János Kollár, *Quotients by finite equivalence relations*, arXiv:0812.3608v2 [math.AG], 2009.

[Poi83] Bruno Poizat, *Une théorie de galois imaginaire*, Journal of Symbolic Logic **48** (1983), no. 4, 1151–1170.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MASSACHUSETTS, LOWELL, ONE UNIVERSITY AVENUE, LOWELL, MA 01854

E-mail address: tibor_beke@uml.edu