A first step towards automated conjecture-making in higher arithmetic geometry

Andreas Holmstrom

KodeBrain Labs, Ålesund, Norway
andreas@kodebrain.com
http://research.kodebrain.com/

Abstract. We present a framework for encoding information about objects from higher arithmetic geometry. This framework is built around a new kind of data type called a Tannakian symbol. The arithmetic objects we have in mind include modular forms (and more general automorphic representations), elliptic curves (and more general schemes, motives and algebraic stacks), finite graphs, group representations, and multiplicative functions (like the Euler totient function). The language of Tannakian symbols not only allows for representations of individual objects, but also representations of classes of objects, relations between objects, and various important unary and binary operations on objects. The development of this framework is the first small step in a long-term project aiming to apply machine-learning algorithms to some problems of current interest in modern arithmetic geometry.

Keywords: Tannakian categories, arithmetic geometry, zeta functions, motives, modular forms, lambda-rings, machine learning

1 Introduction

Arithmetic geometry is one of the most vibrant and abstract areas of modern pure mathematics. Out of the seven Millennium Problems, four come from pure mathematics, and of these four, one is solved and the remaining three belong to arithmetic geometry.

The prospect of artificially intelligent programs making new and deep discoveries in this area of mathematics is a tantalizing one. However, most of the concepts encountered in modern arithmetic geometry are not easily stored or manipulated by a computer. In the very long term, one may hope that advances in mathematical linguistics, as developed in Ganesalingam's thesis [9], may lead to new computer-generated discoveries and proofs in arithmetic geometry. In the short term however, it is natural to look for other, less ambitious routes to making partial progress on selected problems.

In this project paper, we present a framework for encoding data about objects from arithmetic geometry, with the aim of laying the foundation for future applications of machine-learning techniques in the field. This is a first brief survey of a project we have worked on for several years, and many of the details

will be expanded upon in future publications. Comments, especially suggestions for the design of computational experiments, are most welcome.

1.1 Arithmetic objects

Somewhat informally, we shall use the term "arithmetic object" to refer to any kind of object that is of central importance in arithmetic geometry. Some classes of such objects are: (1) Geometric objects (e.g. a scheme). The reader unfamiliar with the theory of schemes may think of a scheme simply as a system of polynomial equations. (2) Algebraic objects (a group, a ring, a Hopf algebra, etc.). (3) Homotopical objects (like an algebraic stack or a ring spectrum). (4) Combinatorial objects (for example a graph). (5) Analytic objects (e.g. a zeta function). (6) Objects in a Tannakian category. Examples of the latter include representations of finite groups, representations of Lie groups, Galois representations, automorphic representations, motives, Hodge structures, and F-isocrystals.

Technical definitions of all the above terms (schemes, Tannakian categories, etc) can be found in the online Encyclopedia of Mathematics [7]. Rather than giving all of these definitions here, we shall present explicit examples from most of these classes and explain how our proposed encoding framework applies to each example.

In addition to seeking encodings of single objects, a central goal of our work is to also encode information about *classes* of objects (for example the class of objects in some given Tannakian category), *operations* on objects (such as tensor product of group representations, or Tate twist of motives, or Dirichlet convolution of multiplicative functions), *relations* between objects (such as a representation being a direct summand of another), and *invariants* of objects (like the Euler characteristic of a scheme).

1.2 What would be required of a good encoding framework?

Let $\mathcal{C}$ be some class of arithmetic objects, for examples the class of all elliptic curves over the rational numbers, or the class of all finite undirected graphs, or the class of all complex representations of the Monster group.

We seek an encoding framework for objects in $\mathcal{C}$ satisfying the following properties:

1. To every object X in the class $\mathcal{C}$ we can assign a finite amount of structured data $\mathbf{E}(X)$. (We think of $\mathbf{E}(X)$ as an *elementary* or *electronic* "shadow" of the object X.)
2. Given a description of X, there should be an explicit algorithm computing $\mathbf{E}(X)$.
3. Many important invariants of X should be computable from $\mathbf{E}(X)$ only.
4. Many important operations on objects in $\mathcal{C}$ should correspond to explicit manipulations of the corresponding structured data.

5. Given two objects X and X' from different classes (say one graph and one elliptic curve), the two associated pieces of data $\mathbf{E}(X)$ and $\mathbf{E}(X')$ should "be of a similar form" (to facilitate the discovery of connections between different kinds of structures).
6. Many of the deepest theorems and conjectures about objects X in modern arithmetic geometry should have a formulation in terms of the associated data $\mathbf{E}(X)$ only.

Any encoding satisfying these requirements will have the property that a computer could in principle discover (or guess) interesting mathematical statements by searching for patterns in the structured data of many arithmetic objects.

We have found an approach that satisfies all of the above criteria for many classes of arithmetic objects. The framework is built around the notion of a *Tannakian symbol*. In many cases, the information contained in the Tannakian symbol is the same as the information contained in the "zeta function" of the arithmetic object, but Tannakian symbols are more flexible than zeta functions, and there are also cases where it makes sense to speak of Tannakian symbols even though there are no zeta functions around.

1.3 Previous work

We are not aware of any previous work with the explicit ambition of applying machine-learning algorithms to geometric, Tannakian and homotopical categories in higher arithmetic geometry. However, we have drawn inspiration from many places. Due to algorithmic breakthroughs over the past decade by Kedlaya [13], Harvey [11], [12], Costa and Tschinkel [5] and others, it is now possible to compute zeta functions of schemes in much higher dimensions and higher cohomological complexity than before, and these computations generate huge amounts of data, that can be interpreted in the language of Tannakian symbols. A project with the aim of collecting this kind of data has been launched under the name *the L-functions and Modular Forms Database* (LMFDB) [14]. From another direction, we have been inspired by the now classical work of Zeilberger on holonomic sequences [19], the PhD thesis and articles of Colton [2], [3], [4] on automated conjecture-making in number theory, and of course the Online Encyclopedia of Integer Sequences (OEIS) [16].

2 Summary of algebraic theory

The aim of this section is to define what Tannakian symbols are, and to summarize their most important algebraic properties. Proofs of these statements will be given elsewhere.

2.1 Algebraic structures

We begin by recalling some definitions from abstract algebra. A *monoid* is a set equipped with a binary operation that is associative and has an identity element.

A *group* is a monoid in which each element has an inverse. A monoid is called *commutative* if its binary operation is commutative. An *abelian* group is the same thing as a commutative group.

Example 1. The set of positive integers $\mathbb{N}$ is a monoid under addition, and it is also a monoid under multiplication. The set of all complex roots of unity is a monoid under multiplication.

A *commutative ring* is a set R with two binary operations, called addition $(+)$ and multiplication $(\,\cdot\,)$, with the requirements that R is an abelian group under addition, a commutative monoid under multiplication, and multiplication distributes over addition. The identity element for addition is denoted by 0, and the identity element for multiplication is denoted by 1.

Example 2. The set of integers $\mathbb{Z}$ is a commutative ring. The set $\mathbb{Z}/m$, identified with $\{0, 1, \ldots, m-1\}$ is a commutative ring for any integer $m \geq 2$, in which addition and multiplication are carried out modulo m. Whenever R is a commutative ring, the set $R[x]$ of polynomials in x with coefficients in R is also a commutative ring.

A *field* is a commutative ring in which the nonzero elements under multiplication form a group (and not just a monoid).

Example 3. The set $\mathbb{Q}$ of rational numbers is a field, and so is the set $\mathbb{R}$ of real numbers, and the set $\mathbb{C}$ of complex numbers.

A *monoid homomorphism* from one monoid to another monoid is a function which commutes with the binary operation and sends the identity element to the identity element. A *ring homomorphism* from a ring to another ring is a function which is a monoid homomorphism both with respect to addition and with respect to multiplication. An *isomorphism* (of rings or of monoids) is a homomorphism which admits a two-sided inverse.

Example 4. Let q be a positive integer. It is known that there exists a field with exactly q elements if an only if q is a power of a prime number (i.e. $q = p^e$ for some prime p and some positive integer e). Two such finite fields with the same number of elements are always isomorphic (i.e. there exists an ring isomorphism between them), and we write $\mathbb{F}_q$ for any finite field with exactly q elements.

It is possible to describe all finite fields in a very concrete way. First of all, when q is a prime number, the ring $\mathbb{Z}/q$ is a field with q elements. A more interesting example is the field with four elements $\mathbb{F}_4$, which can be described as the set $\{0, 1, \alpha, \alpha+1\}$ where addition is carried out modulo 2, and multiplication is carried out modulo 2 *and* modulo the relation $\alpha^2 = \alpha + 1$. Similar models of finite fields exist (but are not in general unique) for any prime power q.

A *lambda-ring* is, informally, a commutative ring R "equipped with all possible symmetric operations". The precise definition of "all possible symmetric operations" is expressed in the notion of a *lambda-structure* on a commutative

ring. The general definition of "lambda-structure" is given in terms of an infinite sequence λ^0, λ^1, λ^2, ... of functions (not ring homomorphisms!) from R to R, satisfying axioms that are a bit complicated. However, when the ring R is torsion-free (meaning that finite sums $x + x + \ldots + x$ are never zero unless x itself is zero), there is a simpler equivalent definition which we give here. All lambda-rings in this paper will be torsion-free, so this definition is enough for our purposes.

Definition 1. *Let R be a torsion-free commutative ring. A lambda-structure on R is an infinite sequence of ring homomorphisms ψ^1, ψ^2, ... from R to R satisfying the following axioms:*

1. $\psi^1(x) = x$ *for all* $x \in R$.
2. $\psi^m(\psi^n(x)) = \psi^{mn}(x)$ *for all* m, n *and all* $x \in R$.
3. $\psi^p(x) \equiv x^p \pmod{pR}$ *for all prime numbers* p *and all* $x \in R$.

The last condition means that the difference $\psi^p(x) - x^p$ can be written as a multiple of p, in the ring R. The homomorphisms ψ^m are called *Adams operations*.

2.2 Tannakian symbols

The kind of "structured data" we shall construct (denoted by $\mathbf{E}(X)$ in the introduction) will be called a *U-indexed M-valued Tannakian symbol*, and we now turn to the explanation of what this means.

Recall that a *multiset* is a unordered collection of elements, in which elements are allowed to be equal. For example, $\{2, 2, 2, 5\}$ is a multiset with four elements taken from the set of integers.

Definition 2. *Let M be a monoid. An* M-valued Tannakian symbol *is an ordered pair (A, B) of disjoint finite multisets with elements taken from M. We write $\mathbf{TS}(M)$ for the set of all M-valued Tannakian symbols.*

Conventions: We shall use the notation A/B or $\frac{A}{B}$ for the ordered pair (A, B), and will refer to A as the *upstairs* multiset and to B as the *downstairs* multiset. Also, if M happens to be a ring and we write $\mathbf{TS}(M)$, we always think of M as a *multiplicative* monoid (in other words, we forget the additive structure).

Example 5. The symbol $\{1, 1, i, -1, -i\}/\emptyset$ is an example of a $\mathbb{C}$-valued Tannakian symbol. Here i is a complex square root of -1 and $\emptyset$ is the empty multiset.

Definition 3. *Let U be a set. A U-indexed M-valued Tannakian symbol is a function from U to $\mathbf{TS}(M)$. The set of U-indexed M-valued Tannakian symbols will be denoted by $\mathbf{TS}_U(M)$.*

Example 6. Let $\mathbb{P}$ be the set of prime numbers, and let p denote a variable element of $\mathbb{P}$. Then $\{p^2, 1\}/\{p, p\}$ is a $\mathbb{P}$-indexed $\mathbb{N}$-valued Tannakian symbol.

Consider multisets $A = \{a_1, a_2, \ldots\}$, $B = \{b_1, b_2, \ldots\}$, $C = \{c_1, c_2, \ldots\}$ and $D = \{d_1, d_2, \ldots\}$ where all the elements are taken from the same monoid M. We define operations on Tannakian symbols by the following formulas:

$$\text{Addition:} \qquad \frac{A}{B} \oplus \frac{C}{D} = \frac{A \uplus C}{B \uplus D}$$

(Here $\uplus$ denotes disjoint union of multisets.)

$$\text{Multiplication:} \qquad \frac{A}{B} \otimes \frac{C}{D} = \frac{A \cdot C \uplus B \cdot D}{A \cdot D \uplus B \cdot C}$$

(Here $A \cdot C$ denotes the monoid product of A and C, i.e. the multiset of all possible products $a \cdot c$ with $a \in A$ and $c \in C$, listed with repetition.)

$$\text{Adams operations:} \qquad \psi^n\Big(\frac{A}{B}\Big) = \frac{\{a^n \mid a \in A\}}{\{b^n \mid b \in B\}}$$

(Here, if the element a is repeated several times in A, the element a^n is also repeated the same number of times on the right hand side.) In each of these operations, it is understood that if the operation results in a symbol in which the upstairs and the downstairs multisets are not disjoint, then we remove pairs of identical elements until the multisets are disjoint. A few examples will illustrate what this means.

Example 7. Computations in $\mathbf{TS}(\mathbb{Z})$:

$$\frac{\{5\}}{\{1,-1\}} \oplus \frac{\{1,1,1\}}{\{-1\}} = \frac{\{5,\cancel{1},1,1\}}{\{\cancel{1},-1,-1\}} = \frac{\{5,1,1\}}{\{-1,-1\}}$$

$$\frac{\{5\}}{\{1,-1\}} \otimes \frac{\{10\}}{\{3,7\}} = \frac{\{50,3,7,-3,-7\}}{\{15,35,10,-10\}}$$

$$\psi^2\Big(\frac{\{-1,-1,2,5\}}{\{1,-2,7\}}\Big) = \frac{\{\cancel{(-1)^2},(-1)^2,\cancel{2^2},5^2\}}{\{\cancel{1^2},\cancel{(-2)^2},7^2\}} = \frac{\{1,25\}}{\{49\}}$$

The main theorem about Tannakian symbols is the following:

Theorem 1. *For any monoid M, the set $\mathbf{TS}(M)$ is a lambda-ring under the operations $\oplus$, $\otimes$ and ψ^n. The same is true for $\mathbf{TS}_U(M)$ for any set U. Furthermore, $TS_U(M)$ is functorial in M as well as in U.*

One can go on and give explicit definitions of other structural features and invariants of Tannakian symbols, such as exterior powers, symmetric powers, virtual dimension, super-dimension, supertrace and superdeterminant. All this terminology comes from the setting of lambda-rings obtained by decategorifying Tannakian categories, but is retained also in situations where there is no Tannakian category involved. *The point of all this structure is that whenever elements of the monoid M can be stored and manipulated by a computer, the same is true for elements of $\mathbf{TS}_U(M)$, and the latter capture huge amounts of structure relevant for higher arithmetic geometry.*

2.3 Assignments and fibers

Now we can be a bit more precise about the picture we would like to paint of structured data assigned to arithmetic objects. Return to the situation where $\mathcal{C}$ is some class of arithmetic objects. Given such a class, we can in many cases choose a monoid M and a set U and construct a map

$$\mathbf{E} : \mathcal{C} \to \mathbf{TS}_U(M)$$

which satisfies most of the requirements in the introduction.

In such a setup, we are interested in the following general goals.

1. Understand how much information is lost when we pass from X to $\mathbf{E}(X)$. A way of making this more precise is to define the *fiber* of a Tannakian symbol S as the set of all arithmetic objects X in $\mathcal{C}$ with $\mathbf{E}(X) = S$. In many cases one can either prove that each fiber consists of at most one element, or give a bound on the size of the fiber.
2. Describe the image of $\mathbf{E}$.
3. Set up a correspondence between operations on arithmetic objects in $\mathcal{C}$ and operations on Tannakian symbols.

2.4 An elementary example: Linearly recursive sequences

Let $a_0, a_1, a_2, \ldots$ be a linearly recursive sequence in $\mathbb{C}$, with $a_0 = 1$. It is well-known that it is then possible to rewrite the power series $a_0 + a_1 t + a_2 t^2 + \ldots$ as a rational expression of the form $\prod_{j=1}^{n}(1-\beta_j t)/\prod_{i=1}^{m}(1-\alpha_i t)$, and we define the Tannakian symbol attached to the linearly recursive sequence to be A/B, with the multisets $A = \{\alpha_i\}$ and $B = \{\beta_j\}$. With this definition, taking the product of power series corresponds to adding Tannakian symbols.

3 Schemes

3.1 General theory

For the purposes of this article, we define an *affine scheme* to be a finite set of variables $x_1, x_2, \ldots, x_d$ together with a finite list of polynomial equations (with integer coefficients) in these variables. Given an affine scheme X and a field K, we write $X(K)$ for the set of solutions to the equations of X with values in the field K; elements of this set are called K-valued points of X.

We also define a *projective scheme* to be a finite set of variables $x_0, x_1, \ldots, x_d$ together with a finite list of *homogeneous* polynomial equations (with integer coefficients) in these variables. The equations are not required to be of the same degree. In this setting, we let $X(K)$ denote the set of *equivalence classes* of solutions with values in K, where two solutions are called equivalent if one is a scalar multiple of the other. For projective schemes, we never count the trivial solution in which all variables take the value zero.

As a special case we may take K to be the finite field $\mathbb{F}_q$, and the set $X(\mathbb{F}_q)$ is then automatically a finite set. We write $\#X(\mathbb{F}_q)$ for the cardinality of this set.

There is a general construction which associates a projective scheme to any affine scheme. If the affine scheme X is defined by equations

$$f_i(x_1, x_2, \ldots, x_d) = 0 \qquad i = 1, 2, \ldots m$$

then the associated projective scheme is defined by corresponding equations

$$F_i(x_0, x_1, x_2, \ldots, x_d) = 0 \qquad i = 1, 2, \ldots m$$

where F_i is obtained from f_i by multiplying each term by a suitable power of x_0 so that F_i becomes homogenous of degree $deg(f_i)$.

Example 8. The equation $x^2+1 = 0$ defines an affine scheme X (in one variable). It is easy to see that in this case, we have $X(\mathbb{Q}) = X(\mathbb{R}) = \emptyset$ (the empty set), but $X(\mathbb{C}) = \{i, -i\}$. Using modular arithmetic, we compute $X(\mathbb{F}_2) = X(\mathbb{F}_3) = \emptyset$ and $X(\mathbb{F}_5) = \{2, 3\}$. In general, for an odd prime p, the cardinality of $X(\mathbb{F}_p)$ is 2 or 0 depending on whether p is congruent to 1 or 3 modulo 4. This pattern is a special case of Gauss' famous quadratic reciprocity law, and quadratic reciprocity is an example of a pattern that can be expressed purely in terms of Tannakian symbols.

Theorem 2 (Dwork). *Let X be a scheme (affine or projective) and let p be a prime. There exists unique multisets $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $B = \{\beta_1, \ldots, \beta_n\}$ of complex numbers such that for all $k \geq 1$, we have*

$$\#X(\mathbb{F}_{p^k}) = \beta_1^k + \beta_2^k + \ldots + \beta_n^k - \alpha_1^k - \alpha_2^k - \ldots - \alpha_m^k$$

Definition 4. *Let X be a scheme and let p be a prime. We define the Tannakian symbol of X at p to be A/B, where A and B are the multisets in Dwork's theorem.*

For simple equations and small primes, the multisets appearing in Dwork's theorem can be computed by hand. Finding efficient algorithms for computing complicated examples is an active area of research in computational number theory.

Example 9. Since Wiles proved Fermat's Last Theorem using the Modularity theorem for elliptic curves, the class of elliptic curves has probably become the most famous class of schemes. As a simple example of an elliptic curve, take the scheme X defined by the equation $y^2 + y = x^3 - x^2$. At the prime $p = 2$, the symbol becomes:

$$\text{Affine case:} \quad \frac{\{-1+i, -1-i\}}{\{2\}} \qquad \text{Projective case:} \quad \frac{\{-1+i, -1-i\}}{\{1, 2\}}$$

The projective case is often the most interesting. In this example, deleting all numbers in the symbol except those with absolute value $\sqrt{2}$ corresponds to cutting out the "motive" $h^1(X)$ from X. One can also associate Tannakian symbols to modular forms, and the Modularity theorem can be formulated as saying that for every elliptic curve X, there exists a modular form which at all primes has the same Tannakian symbol as the motive $h^1(X)$.

Combining Tannakian symbols from all primes gives rise to a map from the class of elliptic curves to $\mathbf{TS}_{\mathbb{P}}(\mathbb{C})$. The fibers of this assignment are called *isogeny classes* of elliptic curves; it is known that these fibers are finite. Furthermore, elliptic curves come with a natural complexity measure N called the conductor (the above example has conductor 11), and by restricting attention to elliptic curves of, say, conductor less than 100000, we may restrict the set of indexing primes to a finite set without losing any information.

In general, the symbol attached to a projective scheme without singularities yields easy recipes for computing the Betti numbers and Euler characteristic of a scheme. In the above example the Betti numbers are 1, 2 and 1; these numbers are obtained by counting symbol elements with absolute value 1, $\sqrt{2}$, and 2, respectively. The Euler characteristic is computed by subtracting the number of elements upstairs from the number of elements downstairs; for this elliptic curve we get $2 - 2 = 0$. Plotting the numbers appearing in the symbol as points in the complex plane reveals symmetries related to Poincaré duality and patterns related to the Riemann hypothesis over finite fields (proved by Deligne, Fields medal 1978). All of this was originally formulated as the famous Weil conjectures in the 1950s.

After computing the Tannakian symbols for several primes (up to size $\sqrt{N}$ approximately) one can easily compute what's called values of L-functions - these are the values appearing in the two Millennium Problems called the (global) Riemann hypothesis and the Birch and Swinnerton-Dyer conjecture. These Tannakian symbols also allows for explicit formulations of many other deep questions of current interest to arithmetic geometers, such as the Sato-Tate conjecture, and various conjectures on Galois representations. The operations on Tannakian symbols correspond to operations in the so-called Grothendieck ring of motives, which is of interest not only in arithmetic geometry, but also in physics, where they are directly related to Feynman integral calculations in perturbative quantum field theory [15].

3.2 Case study: Arithmetic mirror symmetry

Let X_κ be the "quartic Dwork family", i.e. the projective scheme defined by the equation

$$x^4 + y^4 + z^4 + w^4 = 4\kappa xyzw$$

where κ is a integer-valued parameter (so that by varying κ we get a *family* of schemes). The scheme X_κ comes with a natural action of the group $\mathbb{Z}/4 \times \mathbb{Z}/4$. Taking the quotient scheme by this group action and resolving singularities yields a new scheme Y_κ, called the mirror of X_κ.

For concreteness, let's look at the prime $p = 41$. For $\kappa = 2$, we get[1] the following symbols:

$$\mathbf{E}(X_2) = \{1, 41, 41, 41, 41, -41, -41, \ldots, -41, \frac{25 - 8\sqrt{66}i}{2}, \frac{25 + 8\sqrt{66}i}{2}, 1681\}/\emptyset$$

[1] The examples here are adapted from the presentation of Ursula Whitcher [18], and were computed using computer code by Edgar Costa [5].

Here there are 4 copies of the number 41 and 16 copies of the number -41. For the mirror variety, which *a priori* might be expected to have a completely different symbol, we get

$$\mathbf{E}(Y_2) = \{1, 41, 41, \ldots, 41, -41, \frac{25 - 8\sqrt{66}i}{2}, \frac{25 + 8\sqrt{66}i}{2}, 1681\}/\emptyset$$

with 19 copies of the number 41, a single copy of the number -41, and an otherwise identical symbol!

Still working with $p = 41$, for the case $\kappa = 3$ we get:

$$\mathbf{E}(X_3) = \{1, 41, 41, \ldots, 41, -39 + 4\sqrt{10}i, -39 - 4\sqrt{10}i, 1681\}/\emptyset$$

with 20 copies of the number 41. And this time, the Tannakian symbol for the mirror variety Y_3 is

$$\mathbf{E}(Y_3) = \{1, 41, 41, \ldots, 41, -39 + 4\sqrt{10}i, -39 - 4\sqrt{10}i, 1681\}/\emptyset$$

with 20 copies of 41, which means... that the symbols are absolutely identical!!

Patterns of this kind is the subject of arithmetic mirror symmetry, a relatively recent field inspired by the physics of string theory. It is conceivable that a computer searching for patterns in Tannakian symbols could have identified the schemes X_κ and Y_κ as "similar", even if no human had ever thought of mirror symmetry.

4 More examples

4.1 Multiplicative functions

Much of elementary number theory (questions about primes, divisibility, etc.), can be formulated in terms of *multiplicative functions* from $\mathbb{N}$ to $\mathbb{C}$. In this context a function f is multiplicative if $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever m and n are coprime.

Let p be a prime. For all multiplicative functions appearing naturally in number theory, it turns out that the sequence of function values

$$f(1), f(p), f(p^2), f(p^3), \ldots$$

is linearly recursive, and hence we can associate a Tannakian symbol to the pair (f, p). Letting p vary over the set $\mathbb{P}$ of all prime numbers, we get a $\mathbb{P}$-indexed $\mathbb{C}$-valued Tannakian symbol attached to the multiplicative function f. For example, the Euler totient function has symbol $\{p\}/\{1\}$, the characteristic function of the square numbers has symbol $\{1, -1\}/\emptyset$, and the sum-of-divisors function has symbol $\{1, p\}/\emptyset$.

This assignment is injective on multiplicative functions, and for many classical classes of functions it stays injective even when U is reduced to a finite set of primes. Furthermore, Dirichlet convolution of functions correspond to addition of symbols, product of function corresponds to product of symbols (under a certain hypothesis), and norm operators on multiplicative functions correspond to certain Adams operations.

4.2 Graphs

There are at least three interesting ways of associating a Tannakian symbol to a (finite) graph. Firstly, given a graph X, we could define the Tannakian symbol of X to be $A/\emptyset$, where A is the spectrum of X, i.e. the multiset of eigenvalues of the adjacency matrix of X. With this definition, taking the disjoint union of graphs would correspond to addition of Tannakian symbols, and taking tensor product of graphs would correspond to multiplication of Tannakian symbols. Graphs with the same spectrum are called *isospectral*, so the fibers of this assignment would be classes of isospectral graphs.

Example 10. With this definition, the Tannakian symbol of the complete graph on 4 vertices would be $\{-1,-1,-1,3\}/\emptyset$

It is conjectured that almost all graphs are determined by their spectra. However, there are many cases of non-isomorphic graphs with identical spectrum. For example, the number of simple graphs on 9 vertices is 274668 (see OEIS: Sequence A000088), while the number of such graphs isospectral to at least one other graph is 51039 (OEIS: Sequence A099883).

A second approach would be to define the Tannakian symbol of a graph X to be $A/\emptyset$, where $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is the finite multiset of complex numbers appearing in the expression

$$\zeta_X(T) = \frac{1}{(1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_m T)}$$

where $\zeta_X(T)$ is the Ihara zeta function of the graph X.

Example 11. With this alternative definition, the Tannakian symbol of the complete graph on 4 vertices would be

$$\{-1,-1,1,1,1,2,\tfrac{-1+\sqrt{7}i}{2},\tfrac{-1+\sqrt{7}i}{2},\tfrac{-1+\sqrt{7}i}{2},\tfrac{-1-\sqrt{7}i}{2},\tfrac{-1-\sqrt{7}i}{2},\tfrac{-1-\sqrt{7}i}{2}\}/\emptyset$$

In a recent paper [6], Durfee and Martin conjecture that almost all graphs which are not determined by their spectrum are determined by their zeta function.

As a third possibility, one can associate a certain polynomial (the "graph polynomial") to any graph X. This polynomial defines a scheme, called the graph hypersurface of X, and we could associate Tannakian symbols to the graph X by counting points of its graph hypersurface, like we did in the previous section for an elliptic curve and the quartic Dwork family. We refer to Brown and Schnetz [1] for background, definitions, and extensive calculations motivated by applications to quantum field theory. One of their conclusions can be reformulated by saying that for many graphs, the Tannakian symbols constructed by this method seem to also come from modular forms.

4.3 Representations of finite groups

Let G be a finite group. Associated to G is its representation ring $R(G)$, a lambda-ring generated by irreducible complex representations under the operations of direct sum, tensor product, and exterior powers. Any element $g \in G$

gives rise to a lambda-ring homomorphism from $R(G)$ to $\mathbf{TS}(M)$, where M is the monoid of complex roots of unity. Combining several such maps, one obtains a lambda-ring homomorphism $\mathbf{E}$ from $R(G)$ into $\mathbf{TS}_U(M)$, where U is a subset of G. The most interesting choice of U, which we will use in the remainder of this section, is to pick one representative of each conjugacy class of G; this choice guarantees the injectivity of $\mathbf{E}$.

Many interesting patterns and unsolved problems about representations can be reformulated in terms of the map $\mathbf{E} : R(G) \to \mathbf{TS}_U(M)$. This is due to the fact that both the character table of G and the lambda-ring structure of $R(G)$ can be recovered from the values of $\mathbf{E}$.

Example 12. Taking G to be the Monster group, the character table is a 194 by 194 matrix, whose rank is 163. The number 163 also appears in the study of imaginary quadratic number fields; it is in fact the largest possible integer D such that the number field $\mathbb{Q}(\sqrt{-D})$ has class number 1 (meaning that its ring of integers is a unique factorization domain). The study of such number fields goes back to Gauss and is the simplest instance of Gauss' famous class number problem. As explained for example in the popular book of Mark Ronan [17], the appearance of the number 163 in both places might well be a coincidence, but it could also be a hint that there is some mysterious connection between the Monster group and algebraic number theory that is yet to be understood.

An even more spectacular pattern connected with the Monster group is the Monstrous Moonshine Conjecture, formulated by Conway and Norton and proved by Richard Borcherds (Fields medal 1998). The starting point of this wonderful story was the observation that a certain number obtained from the character table (the dimension of the smallest nontrivial irreducible representation) is (almost) equal to the coefficient of the linear term in the Fourier expansion of Klein's j-function.

Let's now turn to a much simpler group, for which everything can be worked out by hand.

Example 13. One of the simplest non-trivial examples of a finite group is the symmetric group S_3 of permutations on three objects. This group has 6 elements in total, partitioned into 3 conjugacy classes. Let e be the identity element, let t be any transposition (an element of order 2), and let r be one of the two "rotations" (an element of order 3). These three elements represent the three conjugacy classes of S_3. The number of irreducible representations of a finite group is the same as the number of conjugacy classes, and in our example, the irreducible representations are:

$\mathbb{C}_+$: The trivial representation, sending every permutation to 1.
$\mathbb{C}_-$: The sign representation, sending a permutation to its sign.
$\mathbb{C}^2$: A two-dimensional representation, visualized as a matrix action of S_3 on a triangle with vertices at the three cube roots of unity in the complex plane.

In this simple case, it is easy to compute the function $\mathbf{E}$ by hand. We get, for the three different choices of group element g:

$$\begin{array}{lll} \text{Case } g=e: & \mathbf{E}(\mathbb{C}_+)=\{1\}/\emptyset & \mathbf{E}(\mathbb{C}_-)=\{1\}/\emptyset \qquad \mathbf{E}(\mathbb{C}^2)=\{1,1\}/\emptyset \\ \text{Case } g=t: & \mathbf{E}(\mathbb{C}_+)=\{1\}/\emptyset & \mathbf{E}(\mathbb{C}_-)=\{-1\}/\emptyset \qquad \mathbf{E}(\mathbb{C}^2)=\{1,-1\}/\emptyset \\ \text{Case } g=r: & \mathbf{E}(\mathbb{C}_+)=\{1\}/\emptyset & \mathbf{E}(\mathbb{C}_-)=\{1\}/\emptyset \qquad \mathbf{E}(\mathbb{C}^2)=\{\omega,\omega^2\}/\emptyset \end{array}$$

Here ω is a primitive 3rd root of unity. Any element of $R(G)$ can be written as a formal difference $V-W$, where V and W are representations built as direct sums of irreducible ones, and we may compute in $R(G)$ by identifying such a formal difference with an ordered triple of symbols (using the injective map $\mathbf{E}$ and applying the rules for computing with Tannakian symbols). For example, we get (suppressing $\mathbf{E}$ from the notation): $\mathbb{C}^2 = \big(\ \{1,1\}/\emptyset\ ,\ \{1,-1\}/\emptyset\ ,\ \{\omega,\omega^2\}/\emptyset\ \big)$ and $\mathbb{C}_+ \oplus \mathbb{C}_- - \mathbb{C}^2 = \big(\ \emptyset/\emptyset\ ,\ \emptyset/\emptyset\ ,\ \{1,1\}/\{\omega,\omega^2\}\ \big)$. A similar computation shows that $\mathbb{C}^2 \otimes \mathbb{C}^2$ equals $\mathbb{C}_+ \oplus \mathbb{C}_- \oplus \mathbb{C}^2$, and in general any tensor product of representations can be expressed as a direct sum of irreducibles, using only Tannakian symbols.

4.4 Algebraic stacks

The arithmetic objects discussed so far in this paper were key players in many of the greatest arithmetic discoveries of the 20th century. However, in 21st century research, new classes of objects are becoming increasingly important, and these objects come from homotopy theory and higher category theory. The most beautiful application so far is probably the recent proof of the Tamagawa number conjecture by Gaitsgory and Lurie [8], in which homotopical objects called *stacks* play a prominent role. Stacks are a generalization of schemes, for which $X(\mathbb{F}_q)$ is no longer a set, but a *groupoid* or a *simplicial set*. There are several different ways of assigning Tannakian symbols to (certain classes of) stacks. The method used for schemes will work provided we accept infinite multisets. For example, the stack $B\mathbb{G}_m$ (the classifying stack of the multiplicative group) would then at the prime p have the Tannakian symbol $\{p^{-1}, p^{-2}, p^{-3}, \ldots\}/\emptyset$.

5 Final remarks on arithmetic pattern-detection

What constitutes an important discovery or a deep conjecture in arithmetic geometry? Looking at many examples in the literature, a few of which we have seen in the examples, it is reasonable to say that *deep arithmetic statements are often observations of patterns expressed in terms of Tannakian symbols.*

But is it conceivable that machine-learning algorithms really could have detected some of these patterns? And is it reasonable to expect machines to discover new patterns, maybe even of comparable interest to the Weil conjectures, Monstrous Moonshine, or arithmetic mirror symmetry? Although we do not claim to know the answer to these questions, we would like to end by suggesting two necessary features that such algorithms would have to incorporate in order to have any chance of making such discoveries.

5.1 Exotic metrics

In traditional data analysis, data points are given by vectors of real numbers (or rather floating point approximations), visualized as points in n-dimensional Euclidean space $\mathbb{R}^n$. Two data points are then considered to have similar features if they are close with respect to some metric on $\mathbb{R}^n$ derived from the standard metric $(x, y) \mapsto |x - y|$ on the set of real numbers.

Similarly, in a traditional neural network based on perceptrons or sigmoid neurons, the output of an individual neuron is a function of the size of an incoming real number, and "size" here refers to a measurement made using the standard metric on the real numbers.

In arithmetic geometry, many patterns and relations can be expressed in terms of a metric, *but* it is not enough to work with the standard metric on real numbers. Instead, the standard metric needs to be complemented by others, most importantly the p-adic metrics. For any prime number p, the p-adic metric on the set of rational numbers is defined as follows. For two distinct rational numbers x and y, there is a unique integer k such that $x - y$ can be written on the form $\pm p^k \cdot a/b$, where a and b are positive integers coprime to p. The p-adic distance $|x - y|_p$ between x and y is defined to be p^{-k}. This definition can be extended to irrational algebraic numbers, but unlike the standard metric, it is not defined for transcendental numbers.

Unravelling the definition, it is easy to see that as a special case, two integers x and y are congruent modulo p if and only if they are close in the sense that their p-adic distance is less than or equal to $1/2$. Combining different primes and using the Chinese remainder theorem, any arithmetic pattern involving congruences can be expressed (and hence potentially discovered) using p-adic metrics[2].

5.2 Symmetry detection

Another class of arithmetic patterns can be collected under the umbrella of symmetry. While the lambda-ring structure on Tannakian symbols in itself captures certain kinds of symmetry, there are also many other kinds, including Poincaré duality (seen in the symbol of a projective scheme without singularities), various symmetries in Hodge diamonds, symmetries of modular forms, and the fact that the number of rows in a character table equals the number of columns.

A mathematical treatment of symmetry invariably involves group theory, and in situations where the symmetry group is both finite and known, it is easy to implement algorithms for detecting symmetry. However, in cases where the symmetry group is infinite and/or unknown, the symmetry detection problem is more challenging. It would be interesting to explore the image recognition and computer vision literature on symmetry detection and think about whether known algorithms can be applied to arithmetic settings, for example to plots of complex numbers taken from a Tannakian symbol.

[2] It might also be interesting to build algorithms based on other kinds of metrics, like the I-adic metric on a polynomial ring (where I is an ideal of the ring), or the Granville-Soundararajan metric on multiplicative functions [10].

References

1. Brown, F., Schnetz, O.: Modular forms in quantum field theory. Communications in Number Theory and Physics 7(2), 293–325 (2013)
2. Colton, S.: Automated Theory Formation in Pure Mathematics. PhD. Thesis, Department of Artificial Intelligence, University of Edinburgh (2001)
3. Colton, S.: Automated Conjecture Making in Number Theory using HR, Otter and Maple. Journal of Symbolic Computation 39(5), 593–615 (2005)
4. Colton, S.: Refactorable Numbers - A Machine Invention. Journal of Integer Sequences 2, 99.1.2 (1999)
5. Costa, E., Tschinkel, Y.: Variation of Neron-Severi ranks of reductions of K3 surfaces. Experimental Mathematics 23, pp. 475–481 (2014)
6. Durfee, C., Martin, K.: Distinguishing graphs with zeta functions and generalized spectra. Linear Algebra Appl. 481, pp. 54–82 (2015)
7. Encyclopedia of Mathematics, `http://www.encyclopediaofmath.org/`
8. Gaitsgory, D., Lurie, J.: Weil's Conjecture for Function Fields. Preprint available at `http://www.math.harvard.edu/~lurie/papers/tamagawa.pdf`
9. Ganesalingam, M.: The Language of Mathematics - A Linguistic and Philosophical Investigation. Theoretical Computer Science and General Issues, Vol. 7805. Springer-Verlag Berlin Heidelberg (2013)
10. Granville, A., Soundararajan, K.: Pretentious multiplicative functions and an inequality for the zeta-function. In: De Koninck, J., Granville, A., Luca, F. (eds.): Anatomy of Integers, CRM Proceedings and Lecture Notes, Vol. 46 (2008)
11. Harvey, D.: Counting points on hyperelliptic curves in average polynomial time. Ann. of Math. (2) 179(2), 783–803 (2014)
12. Harvey, D.: Computing zeta functions of arithmetic schemes. Proc. Lond. Math. Soc. 111, no. 6, 1379–1401 (2015)
13. Kedlaya, K.S.: Computing Zeta Functions via p-adic Cohomology. In: Buell (ed.); Algorithmic Number Theory. LNCS, vol. 3076, pp. 1–17. Springer Berlin Heidelberg (2004)
14. The LMFDB Collaboration: The L-functions and Modular Forms Database. `http://www.lmfdb.org`
15. Marcolli, M.: Feynman motives. World Scientific, Hackensack, NJ (2010)
16. Online Encyclopedia of Integer Sequences, `http://oeis.org/`
17. Ronan, M.: Symmetry and the Monster: One of the greatest quests of mathematics. Oxford University Press, UK (2006)
18. Whitcher, U." Mirror symmetry and K3 surface zeta functions. Presentation given at ICERM, Oct 2015. Slides available at `https://icerm.brown.edu/sp-f15-w2/`
19. Zeilberger, D.: A holonomic systems approach to special functions identities. J. Comput. Appl. Math. 32(3), 321–368 (1990)