Zeta types and Tannakian symbols

Andreas Holmstrom & Torstein Vik

Uppsala University / Fagerlia Upper Secondary School

2nd Conference on Artificial Intelligence and Theorem Proving
Obergurgl, March 26-30, 2017

My background:

- 2010: PhD, University of Cambridge (Number theory/homotopy theory)
- 2011: Postdoc positions in France
- 2012-current: High-school teacher in Ålesund, Norway
- Still passionate about mathematics
- Current research projects tied to various computational student projects.

Torstein Vik and Ane Espeseth with the
Norwegian Minister of Education and Research

Introduction

Starting point: Objects of interest in modern number theory.

- Arithmetical functions, e.g. the Euler φ function
- L-functions and zeta functions
- Motives, Galois representations, automorphic representations (Langlands program)
- Varieties, schemes, stacks (Geometry)
- Groups and their representations (Tannakian categories)

Introduction

Currently, there are very few connections between modern research on these objects and modern formalization, automated conjecturing, and automated reasoning (as far as we are aware).

Main goal:

- Make a computer produce mathematics of interest to a human number theorist!

  We are willing to use any tools available, from very simple search and matching techniques to advanced machine learning.

Introduction

Challenges:

- Find good computer representations of objects
- Automatically generate interesting conjectures
- Automatic reasoning / proofs of conjectures??

Computer representations

From a practical point of view, the task of finding a computer representation of a mathematical object is presented to us in different situations.

1. The object is finite in nature. Example: A finite graph, or a rational number.
2. The object is countably infinite. Example: A integer sequence $a_1, a_2, \ldots$, or a single real number.
3. The object is very big (in some sense). Example: The category of all commutative rings, or the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$, or the functor which sends a commutative ring R to the set of its invertible elements.

Computer representations

We want to emphasize a few points here:

- We are interested in representations that are useful in practice, in actual applications of automated conjecturing and automated reasoning.
- These notions of usefulness is vague, but we would argue that they exclude most forms of human-readable mathematical prose, such as the phrase "the category of all commutative rings".
- We are interested specifically in the number-theoretic objects listed above, not in a general abstract theory of useful computer representations of mathematical objects.

Computer representations

Objects of interest:

- Arithmetical functions, e.g. the Euler φ function
- L-functions and zeta functions
- Motives, Galois representations, automorphic representations (Langlands program)
- Varieties, schemes, stacks (Geometry)
- Groups and their representations (Tannakian categories)

Computer representations

In case 1 (finite objects), there will be various ways of representing the object without any loss of information.

In the graph example, we may choose the adjacency matrix, the incidence matrix, or the adjacency list, and so on.

Even in this simple situation, the choice of representation can be important with regards to usefulness for a specific application.

Computer representations

In case 2 (countably infinite objects), several things may happen:

- 2A We can be clever and construct a finite representation (e.g. a closed formula for a_n)
- 2B We can define a meaningful metric on objects, and find a finite representation guaranteed to be accurate up to some small error. Example: The real number π can be represented as 3.1416, and this representation is much more useful than the representation 98214 (this is decimals no. 100 to 104.)
- 2C We're unable to find a useful computer representation.

Computer representations

In case 3 (very big objects), we may try to find a crude "approximation" (in some sense) to the object.

Example: The category of all representations of a given finite group G can be approximated by its Grothendieck ring, which if finitely generated, and hence can be given a finite representation (using Tannakian symbols). Generalization: Tannakian categories.

Example: The functor taking a commutative ring to its set of invertible elements is an example can be approximated by a certain zeta type. Generalization: Schemes.

Zeta types and Tannakian symbols

We want to propose a framework for computer representations of number-theoretic objects that is "good enough" for interesting applications.

Terminology: Zeta types and Tannakian symbols

For this talk, we focus on the simplest use case, namely classical multiplicative functions.

Zeta types and Tannakian symbols

We define a zeta type to be a two-dimensional array of "numbers", indexed in one direction by a prime number p, and in the other direction by a positive integer e.

Example:

	$e=1$	$e=2$	$e=3$	$e=4$	$e=5$
$p=2$	3	6	12	24	48
$p=3$	4	12	36	108	324
$p=5$	6	30	150	750	3750
$p=7$	8	56	392	2744	19208
$p=11$	12	132	1452	15972	175692

Zeta types and Tannakian symbols

Note: Multiplicative functions are absolutely everywhere in number theory.

Definition

A function $f : \mathbb{N} \to \mathbb{C}$ is multiplicative if

- $f(1) = 1$
- $f(m \cdot n) = f(m) \cdot f(n)$ whenever m and n are coprime.

These axioms imply that the function values $f(p^e)$ at prime power arguments completely determine the function.

Zeta types and Tannakian symbols

The Online Encyclopedia of Integer Sequences (OEIS) contains many multiplicative functions.

Example: The Euler φ function. Definition $\varphi(n)$ is the number of invertible elements in the ring $\mathbb{Z}/n$.

Computer representation in the OEIS: 1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8, 12, 10, 22, 8, 20, 12, 18, 12, 28, 8, 30, 16, 20, 16, 24, 12, 36, 18, 24, 16, 40, 12, 42, 20, 24, 22, 46, 16, 42, 20, 32, 24, 52, 18, 40, 24, 36, 28, 58, 16, 60, 30, 36, 32, 48, 20, 66, 32, 44

Difficult to see any clear pattern, or find interesting relations to other functions.

Zeta types and Tannakian symbols

The idea of using a zeta type is that we display only the function values $\varphi(p^e)$.

This removes lots of redundant information, and reorganises the remaining data in a nicer way.

Zeta types and Tannakian symbols

The zeta type of the Euler φ function:

	$e=1$	$e=2$	$e=3$	$e=4$	$e=5$
$p=2$	1	2	4	8	16
$p=3$	2	6	18	54	162
$p=5$	4	20	100	500	2500
$p=7$	6	42	294	2058	14406
$p=11$	10	110	1210	13310	146410

Zeta types and Tannakian symbols

Example: The Möbius μ function.

OEIS: 1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0, -1, 1, 1, 0, -1, 0, -1, 0, 1, 1, -1, 0, 0, 1, 0, 0, -1, -1, -1, 0, 1, 1, 1, 0, -1, 1, 1, 0, -1, -1, -1, 0, 0, 1, -1, 0, 0, 0, 1, 0, -1, 0, 1, 0, 1, 1, -1, 0, -1, 1, 0, 0, 1, -1, -1, 0, 1, -1, -1, 0, -1, 1, 0, 0, 1, -1

Zeta types and Tannakian symbols

Example: The Möbius μ function.

	$e=1$	$e=2$	$e=3$	$e=4$	$e=5$
$p=2$	-1	0	0	0	0
$p=3$	-1	0	0	0	0
$p=5$	-1	0	0	0	0
$p=7$	-1	0	0	0	0
$p=11$	-1	0	0	0	0

Zeta types and Tannakian symbols

Each row in the zeta types we have seen satisfy a linear recursion.

Let's consider the generating series of a row.

Example:

$$1 - 1t + 0t^2 + 0t^3 + \ldots = 1 - t = \frac{1-t}{1}$$

Zeta types and Tannakian symbols

For the rows of the Euler φ function: At $p = 2$:

$$1 + 1t + 2t^2 + 4t^3 + 8t^4 + \ldots = \frac{1-t}{1-2t}$$

At $p = 3$:

$$1 + 2t + 6t^2 + 18t^3 + 54t^4 + \ldots = \frac{1-t}{1-3t}$$

At $p = 5$:

$$1 + 4t + 20t^2 + 100t^3 + 500t^4 + \ldots = \frac{1-t}{1-5t}$$

Zeta types and Tannakian symbols

General computation:

$$1 + (p-1)t + (p^2-p)t^2 + (p^3-p^2)t^3 + \ldots =$$
$$= (1 + pt + p^2t^2 + p^3t^3 + \ldots) - (t + pt^2 + p^2t^3 + \ldots) =$$
$$= \frac{1}{1-pt} - \frac{t}{1-pt} = \frac{1-t}{1-pt}$$

Tannakian symbol of the Euler φ function: $\frac{\{p\}}{\{1\}}$

Zeta types and Tannakian symbols

We can compute Tannakian symbols for all classical multiplicative functions in the literature:

$\frac{\{\widetilde{1,1}\}}{\varnothing}$	Number of divisors
$\frac{\{1,p\}}{\varnothing}$	Sum of divisors
$\frac{\{1,p^k\}}{\varnothing}$	k'th divisor function
$\frac{\{p\}}{\{1\}}$	Euler totient function
$\frac{\{-1\}}{\varnothing}$	Liouville function
$\frac{\{1\}}{\{2\}}$	The γ-function

Zeta types and Tannakian symbols

The Tannakian symbol is a *finite* representation of a multiplicative function (if the function is nice enough).

For functions which are less nice, but motivic, there is a *metric* such that the first rows determine the zeta type up to some small error.

Analogy: The rows of a zeta type are like the decimals of a real number (!)

An automated identity finder

Among the simplest nontrivial theorems about multiplicative functions we find so-called identities between different functions.

Example: Values of the Euler φ function:

n	1	2	3	4	5	6	7	8	9	10	11	12	...	20
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	...	8

n	**1**	**2**	**3**	4	5	**6**	7	8	9	10	11	12	...	20
$\varphi(n)$	①	①	②	2	4	②	6	4	6	4	10	4	...	8

n	**1**	**2**	3	**4**	**5**	6	7	8	9	**10**	11	12	...	**20**
$\varphi(n)$	①	①	2	②	④	2	6	4	6	④	10	4	...	⑧

An automated identity finder

The general rule here can be formulated by the formula

$$\sum_{d|n} \varphi(d) = n \tag{1}$$

An automated identity finder

Example: Values of the τ function:

n	1	2	3	4	5	6	7	8	9	10	11	12	..	16	..	25
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6	..	5	..	3

$$\sum_{d|n^2}(-1)^{\Omega(d)}\tau(d)\tau(\frac{n^2}{d}) = \tau(n) \qquad (2)$$

An automated identity finder

In [73]:
```
funcs = [phi, id, id_2, tau, sigma, liouville, mu]

sums = [l + r for l, r in itertools.combinations_with_replacement(funcs, 2)]

for lhs in sums:
    for rhs in funcs:
        if lhs == rhs:
            print html(lhs & rhs)
```

$$\sum_{d_0|n} \varphi(d_0) \cdot \tau\left(\frac{n}{d_0}\right) = \sigma(n)$$

$$\sum_{d_0|n} d_0 \cdot \mu\left(\frac{n}{d_0}\right) = \varphi(n)$$

$$\sum_{d_0|n} \sigma(d_0) \cdot \mu\left(\frac{n}{d_0}\right) = n$$

An automated identity finder

It seems like our automated identity finder produces all known identities between classical multiplicative functions, with proofs.

Some of these are certainly publishable results.

Future applications

Automatic conjecturing?

One possible approach to automatic conjecturing is to use the recent Sage framework of Larson and van Cleemput. This takes as input any collection of mathematical objects and a set of real invariants of these objects, and produces conjectures in the form of inequalities between combinations of these invariants.

Reference: Larson, C. E., Van Cleemput, N.: Automated Conjecturing I: Fajtlowicz's Dalmatian Heuristic Revisited. Artificial Intelligence 231, 17–38 (2016)

Future applications

Recall the objects we are really interested in.

Let us look at a few examples.

Future applications

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.

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.

(Computations borrowed from a presentation by Ursula Whitcher, using code by Edgar Costa.)

Future applications

Look at $p = 41$. For $\kappa = 2$, the scheme X_κ has symbol:

$$\{1, 41, 41, 41, 41, -41,$$

$$-41, \ldots, -41, \frac{25 - 8\sqrt{66}i}{2}, \frac{25 + 8\sqrt{66}i}{2}, 1681\}/\emptyset$$

Here there are 4 copies of the number 41 and 16 copies of the number -41.

For the mirror variety Y_2, we get

$$\{1, 41, 41, \ldots, 41, -41, \frac{25 - 8\sqrt{66}i}{2}, \frac{25 + 8\sqrt{66}i}{2}, 1681\}/\emptyset$$

with 19 copies of the number 41, a single copy of the number -41.

Future applications

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

$$\{1, 41, 41, \ldots, 41, -39 + 4\sqrt{10}i, -39 - 4\sqrt{10}i, 1681\}/\emptyset$$

with 20 copies of 41.

Completely identical symbols!

Future applications

Question: Is there an explicit algebraic operator on $K_0(Mot)$ that sends the class of a variety to the class of its mirror?

There are literally hundreds of questions like this about explicit constructions in Grothendieck rings, which we can investigate using Tannakian symbols.

Future applications

One final example: For any element of $K_0(Mot)$, and any integer n, there should be a "special value formula".

The simplest case is Euler's Basel problem. Take the scheme $x = 0$ and the integer $n = 2$. We get

$$\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}$$

For elliptic curves: Birch-Swinnerton-Dyer conjecture.

Future applications

The L-function of an elliptic curve may look like this:

	$e = 1$	$e = 2$	$e = 3$	$e = 4$	$e = 5$
$p = 2$	1	-1	-3	-1	5
$p = 3$	0	-3	0	9	0
$p = 5$	-3	4	3	-29	72
$p = 7$	-1	-6	13	29	-120
$p = 11$	-1	1	-1	1	-1

Future applications

The Hasse-Weil zeta function of the elliptic curve $y^2 + y = x^3 - x^2$ gives:

	$e = 1$	$e = 2$	$e = 3$	$e = 4$	$e = 5$
$p = 2$	5	5	5	25	25
$p = 3$	5	15	20	75	275
$p = 5$	5	35	140	595	3025
$p = 7$	10	60	310	2400	

One of the numbers appearing in the Birch-Swinnerton-Dyer conjecture for this curve is 5.

We are not claiming any of this will lead to new results on BSD, but there are interesting connections, and we may hope to better understand some simpler problems.

Representation rings

Example: Consider a finite group G, and the category $Rep_{\mathbb{C}}(G)$.

Can take the *Grothendieck ring* $K_0(Rep_{\mathbb{C}}(G))$.

It is a commutative ring, generated by the irreducible representations.

Addition $\leftrightarrow$ direct sum of representations

Multiplication $\leftrightarrow$ tensor product of representations.

Exterior powers give extra algebraic structure, giving us a *lambda-ring*, with lambda-operations, Adams operations, and more.

Representation rings

Representation rings are sometimes described only as commutative rings.

Example: The Grothendieck ring of $Rep_{\mathbb{C}}(S_3)$ is isomorphic to $\mathbb{Z}[X, Y]/(XY - Y, X^2 - 1, Y^2 - X - Y - 1)$

(Here 1 is the trivial rep, X is the sign rep (dim 1), and Y is the 2-dimensional irrep.)

But this is bad - the lambda-ring structure is important!

Representation rings

Example: Consider (complex) representations of a compact connected complex Lie group.

The Grothendieck ring is generated *as a ring* by elements in one-to-one correspondence with the nodes of the associated Dynkin diagram.

The Grothendieck ring is generated *as a lambda-ring* by elements in one-to-one correspondence with the *arms* of the Dynkin diagram.

There are also structure theorems characterizing which lambda-rings can occur as representation rings of these Lie groups, as well as a theorem saying that the Lie group itself is determined by the Grothendieck ring together with one extra piece of data.

Representation ring

General categorical framework for categories like $Rep_{\mathbb{C}}(G)$: *Tannakian categories*.

For any such category $\mathcal{T}$, the Grothendieck ring $K_0(\mathcal{T})$ is a lambda-ring.

Main question: Can we give explicit descriptions of these lambda-rings in a way that clearly captures also the lambda-ring structure?

Lambda-rings

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 $x \in R$.

Tannakian symbols

Let M be a commutative monoid (set with a binary operation that is associative, commutative, and has an identity element).

Example: $M = \mathbb{C}^*$ (under multiplication).

A *finite multiset* is a finite unordered list of elements (repeated elements allowed).

A *Tannakian symbol* (with values in M) is an ordered pair of finite multisets with elements taken from M. We require the multisets to be disjoint.

Notation: $\frac{A}{B}$

Example: $\frac{\{2,2,5,5\}}{\{1,1,1\}}$

Tannakian symbols

Operations on Tannakian symbols (examples):

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

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

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

Tannakian symbols

We write $TS(M)$ for the set of Tannakian symbols with values in M.

Theorem: $TS(M)$, with the above operations, is a lambda-ring.

As a commutative ring, it is isomorphic to the monoid algebra of M.

TS is a functor from commutative monoids to lambda-rings.

Let U be a set. We write $TS(M)^U$ for the set of functions from U to $TS(M)$ (think of this as vectors of symbols, indexed by U).

Tannakian symbols

Main conjecture:

Let $\mathcal{T}$ be a Tannakian category, with Grothendieck ring $K_0(\mathcal{T})$.
Let L be any sub-lambda-ring or quotient lambda-ring of $K_0(\mathcal{T})$.

- There exists a monoid M, a set U, and an *injective lambda-ring homomorphism*

$$L \hookrightarrow TS(M)^U$$

.

- If L is finitely generated, then U may be taken to be finite.
- There exists a practical algorithm associated to L that takes an element of $TS(M)^U$ as input and determines whether it comes from L.

Thank you!