Arithmetic statistics of Galois groups

David Kohel
Institut de Mathématiques de Marseille

ANTS 2018, Madison, 16 July 2018

Galois representations

The objective of this work is to characterize and understand the visible properties of finite representations of $\mathcal{G} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. As a profinite group, $\mathcal{G}$ is determined by its finite quotients, e.g.,

- The continuous representations on the Tate module $T_p(A)$ of an abelian variety A, a limit of its actions on $A[p^k]$, giving rise to representations in an associated Sato-Tate group (compact subgroup of $\mathrm{USp}(2g)$).
- The abelianization $\mathcal{G}^{ab}$ is obtained as a limit of the Galois groups $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The restriction to the tower $\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}$ gives the analogous representation on the p^k-torsion of the multiplicative group $\mathbb{G}_m$.

The representations are often inaccessible. By *visible properties* we refer to (values of) class functions on $\mathcal{G}$, in which the irreducible characters play the role of distinguished small elements.

Galois groups, Notation

In this work we focus on finite Galois representations, passing through a finite quotient. Specifically, let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree n, let $K = \mathbb{Q}[x]/(f(x))$ and let L be the normal closure of K. This determines

- a group $G = \mathrm{Gal}(L/\mathbb{Q})$, equipped with
- a permutation representation $G \hookrightarrow \mathcal{S}_n$.

We draw intuition from the orthogonal representations in $\mathrm{O}(n)$. In particular the *permutation representation* is the embedding in $\mathrm{O}(n)$ as permutation matrices, and the restriction to the orthogonal complement of $(1, \ldots, 1)$, gives the *standard representation* $\mathcal{S}_n \to \mathrm{O}(n-1)$.

Orthogonal groups, Notation

To a permutation with cycle type $(d_1, \ldots, d_t)$, the characteristic polynomial of its permutation representation is

$$P(x) = (x^{d_1} - 1) \cdots (x^{d_t} - 1) \in \mathbb{Z}[x],$$

and that of the standard representation is thus

$$S(x) = \frac{P(x)}{(x-1)} = x^{n-1} - s_1 x^{n-2} + \cdots + (-1)^{n-1} s_{n-1} \in \mathbb{Z}[x].$$

The integers $(s_1, \ldots, s_{n-1})$ associated to σ are *class invariants*.

Representation ring

Let G be a compact Lie group (e.g. $\mathrm{O}(n)$, $\mathrm{SO}(n)$ or a finite group), and denote the set of conjugacy classes of G by $\mathscr{C}\ell(G)$.

The *representation ring* of G is the free abelian group

$$\mathcal{R}(G) = \bigoplus_{\chi} \mathbb{Z}\chi,$$

on the set of irreducible characters $\chi : G \to \mathbb{C}$ of finite degree.

Since characters are in bijection with an isomorphism classes of representations, we can interpret $\mathcal{R}(G)$ as the Grothendieck group of representations of G of finite degree.

Addition on $\mathcal{R}(G)$ is identified with direct sum and multiplication with tensor product of representations. Elements of $\mathcal{R}(G)$ are *class functions* on G, i.e. are well-defined on $\mathscr{C}\ell(G)$.

The representation ring of $\mathrm{O}(n)$

Lemma (Takeuchi)

The virtual character ring $\mathcal{R}(O(n))$ is generated by s_k, $1 \leq k \leq n$, and

$$\mathcal{R}(\mathrm{O}(n)) \cong \frac{\mathbb{Z}[s_1, \ldots, s_n]}{(s_k s_n - s_{n-k}, s_n^2 - 1)}.$$

The restriction $\mathrm{Res} : \mathcal{R}(\mathrm{O}(n)) \to \mathcal{R}(\mathrm{SO}(n))$ surjects on

$$\mathcal{R}(\mathrm{SO}(n)) \cong \frac{\mathbb{Z}[s_1, \ldots, s_n]}{(s_k - s_{n-k}, s_n - 1)}$$

with kernel ideal $(s_n - 1)$.

N.B. The s_k are the characters of the representations on $\bigwedge^k(\mathbb{R}^n)$.

Representation ring parametrization

The standard representation in $\mathrm{O}(n-1)$ of a finite permutation group $G \subset \mathcal{S}_n$ gives a parametrization

$$\mathbb{Z}[s_1, \ldots, s_{n-1}] \longrightarrow \frac{\mathbb{Z}[s_1, \ldots, s_{n-1}]}{(s_k s_{n-1} - s_{n-k-1}, s_{n-1}^2 - 1)} \longrightarrow \mathcal{R}(G),$$

determined by the restriction map $\mathrm{Res} : \mathcal{R}(O(n-1)) \to \mathcal{R}(G)$.

We use this parametrization to obtain an polynomial forms, in $\mathbb{Q}[s_1, \ldots, s_{n-1}]$, for characters in $\mathcal{R}(G)$.

N.B. The tuple of values $(s_1, \ldots, s_{n-1})$ can be computed from the cycle type, and the cycle type of the Frobenius class at p is the list of degrees of irreducible factors of $f(x) \mod p$.

Inner product structure

Let $\{\mathcal{C}_1, \ldots, \mathcal{C}_h\}$ be the conjugacy classes and $\{\chi_1, \ldots, \chi_h\}$ the irreducible characters of a group G. The orthogonality relations for irreducible characters takes the form

$$\langle \chi_i, \chi_j \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \sum_{k=1}^{h} \frac{|\mathcal{C}_k|}{|G|} \chi_i(\mathcal{C}_k) \overline{\chi_j(\mathcal{C}_k)} = \delta_{ij}.$$

The terms $p(\mathcal{C}_k) = \dfrac{|\mathcal{C}_k|}{|G|}$ are the induced probabilities of $|\mathcal{C}_k|$.

In terms of a sample set S of initial primes, the inner products $\langle \chi_i, \chi_j \rangle$ of characters can be computed as the expectation of $\chi_i \overline{\chi}_j$:

$$\langle \chi_i, \chi_j \rangle := \mathbb{E}(\chi_i \overline{\chi}_j) \sim \mathbb{E}_S(\chi_i \overline{\chi}_j) = \frac{1}{|S|} \sum_{p \in S} \chi_i(p) \overline{\chi}_j(p).$$

where we interpret the value of a characters at p as its value on the Frobenius conjugacy class.

$\mathcal{A}_5$ example

The alternating group $\mathcal{A}_5$ has five irreducible characters $(1, \chi_1, \chi_2, \chi_3, \chi_4)$, of degrees $1, 4, 5, 3, 3$, of which χ_3 and χ_4 are conjugate over $\mathbb{Q}(\sqrt{5})$, hence $\chi_3 + \chi_4$ is a rational character of degree 6.
In terms of the permutation representations of degree 5, we find the parametrization (by $\mathbb{Q}[s_1, s_2] \cong \mathcal{R}(\mathrm{SO}(5)) \otimes \mathbb{Q}$),

$$(1, s_1, s_1^2 - s_2 - s_1 - 1, s_2) = (1, \chi_1, \chi_2, \chi_3 + \chi_4)$$

and in terms of the permutation representations of degree 6, we have parametrizations (by $\mathbb{Q}[s_1, s_2] \cong \mathcal{R}(\mathrm{SO}(6)) \otimes \mathbb{Q}$),

$$(1, s_1^2 - 2s_1 - s_2 - 1, s_1, s_2 - \chi_1) = (1, \chi_1, \chi_2, \chi_3 + \chi_4)$$

$\mathcal{A}_5$ example

By construction, the polynomials

$$f = x^5 - 5x^4 + 48x^3 + 28x^2 + 5x - 1,$$
$$g = x^6 + 4x^5 + 10x^4 - 10x^3 + 17x^2 + 10x + 1$$

have the same Galois closure. Jointly evaluating these characters (on factorization types of f and $g \bmod p$) over a small sample set (< 200 primes) yields the diagonal inner product matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

to the nearest integer.

Variance and convergence

The irreducible characters provide test functions with optimal convergence properties.

Naively, by the orthogonality relations for a system $\{\chi_1, \ldots, \chi_r\}$ of irreducible characters, it suffices to recognize the integer $\langle \chi_i, \chi_j \rangle$ in $\{0, 1\}$ to one bit of precision.

Moreover, we can interpret

$$\mathbb{E}_S(\chi_i \overline{\chi}_j) = \frac{1}{|S|} \sum_{p \in S} \chi_i(p) \overline{\chi}_j(p)$$

as a (sample) variance ($i = j$) or covariance ($i \neq j$) for S.
The irreducible characters provide minimal variance for any (integer-valued) test functions.

This theoretic argument holds up in experimental practice.

Asymptotics in the degree

The number of conjugacy classes for $\mathcal{S}_n$ is the partition number $p(n)$, whose asymptotic growth is known to be

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

For large n, this is prohibitively large, in particular,

$$p(120) = 1844349560 \text{ and } p(240) = 105882246722733.$$

Nevertheless the n characters $1, s_1, \ldots, s_{n-1}$ give a good system of (irreducible) test functions for $\mathcal{S}_n$, and for a proper subgroup G, if the cardinality of $\mathcal{C}\ell(G)$ is small, we may find a relatively small number of distinct test characters for G.

Asymptotics in the degree

As an example, we considered the example of a polynomial whose Galois group is the Weyl group $W(E_8)$, as constructed by Jouve, Kowalski and Zywina. A defining polynomial $f(x)$ has degree 240, the group order is 696729600, and there exist only 112 conjugacy classes.

Its quotient $W(E_8)/\{\pm 1\}$ admits a degree 120 permutation representation (namely $g(x)$ such that $f(x) = g(x^2)$) and has 67 conjugacy classes.

A subset of irreducible chracters, parametrized by $\mathbb{Q}[s_1, \ldots, s_{n-1}]$ was shown to stably converge to the identity matrix ($< 1/2$ in the ℓ_∞-norm with $< 2^{13}$ primes).

Perspectives

For a polynomial of low degree one can realize generators for the Galois group, and provable determine G. The arithmetic statistics give rapid, but heuristic, characterizations of G.

The approach through arithmetic statistics can be applied more generally to any (finite degree) Galois representations, e.g. from: global fields, exponential sums or weight one modular forms.

Moreover, we can compare disparate objects as long as each object provides the data of class functions on Frobenius elements.

As already seen in the case of number fields, this permits us to address whether the normal closures of two number fields admit a common subfield — reducing a question of linear independence of characters on $\mathcal{G}$ to an empirically computed inner product.