Computable profinite groups and randomness

Department of Decision Sciences, Unisa, Pretoria, South Africa.

Willem L. Fouché,

joint work with Andre Nies

CCC 2020, 3 September 2020.

1 Context of project

- A case can be made that profinite groups are absolute Galois groups of fields (Waterhouse). Such groups have a natural (Krull) topology which can be expressed in the language of profinite topologies.
- This renders the groups topologically as compact Hausdorff spaces which are totally disconnected. These groups G have unique Haar measures μ with $\mu(G) = 1$.
- In this project, we consider μ-almost sure properties of elements of G and explore the algorithmically random complexity of almost sure properties relative to μ when the group G and μ have computable representations. At this stage we are particularly interested in Schnorr randomness in this context.
- In this talk, the cases when G is the absolute Galois group of a computable Hilbertian field with splitting algorithm, a finite field, or an effective pseudo-algebraically closed field will be discussed. (The notions will be explained during the talk).

2 Some terminology

- We fix an algebraic closure $\overline{\mathbb{Q}}$ of the field $\mathbb{Q}$.

  Then algebraically, the group $G = \mathrm{Aut}(\overline{\mathbb{Q}})$ is given by all the automorphisms of the field $\overline{\mathbb{Q}}$ that keeps $\mathbb{Q}$ fixed.
  It can be shown that

  $$G \simeq \varprojlim_N G/N,$$

  where N ranges over all the normal subgroups of finite index in G.

  The (Krull) topological structure of G is inherited by embedding $\varprojlim_N G/N$ into the product of all the G/N with N normal and of finite index in G.

  It follows that G is a compact Hausdorff group.

Being a projective limit of finitely many finite groups, one can embed G as a closed subgroup of the Baire space ω^ω.

Using ideas going back to Kronecker on effective Galois theory over the rationals we can embed G as a Π^0_1 subspace of ω^ω. The Haar measure on G is computable relative to this representation of G in Baire space.

- It is thus clear what it means to say that an element σ of G is Martin-Löf /Schnorr/ Kurtz random, for instance.

- Finally,
$$\hat{\mathbb{F}}_\omega \simeq \varprojlim_N \mathbb{F}_\omega/N,$$
where N ranges over the normal subgroups of finite index in the free group $\mathbb{F}_\omega$ on countably many generators.
- A field L is *pseudo-algebraically closed* (PAC) if every absolutely irreducible algebraic variety over L will have a point all coordinates of which belong to L. This notion is due to Ax in his work on the decidability of the first-order theory of finite fields.

3 A theorem

We shall discuss the following

Theorem 1 *(Fouché, Nies).* `Based on research as can be found in the book “Field arithmetic” by Fried and Jarden.`

- *Let G be the absolute Galois group of the field $\mathbb{Q}$ of rational numbers, topologised by the standard Krull topology.*
- *Write μ for the Haar probability measure on G.*

  Given a computable representation of G, μ and an element σ of G which is Martin-Löf-random relative to μ, write $[\sigma]_n$ for the topological normal closure of σ which is the smallest topological and normal subgroup of G that has σ as an element.

  Then $[\sigma]_n$ is isomorphic to $\hat{\mathbb{F}}_\omega$, the free profinite group on countably many generators.

  Moreover, the fixed field L_σ corresponding via Galois duality to the normal closed group $[\sigma]_n$, is pseudo-algebraically closed.

4 Profinite groups

- A topological group is said to be *profinite* if it is a projective limit over a directly ordered index set of finite groups.
- As such it is a compact Hausdorff totally disconnected group G. Therefore

$$G \simeq \varprojlim_{N} G/N,$$

  where N ranges over the open normal subgroups of G. Note that, the N ranges over normal subgroups of G of finite index in G. This is because each open subgroup of a compact group is of finite index in the group. So, each group G/N is finite.
- Any compact Hausdorff totally disconnected (Stone) group has such a representation.

5 Absolute Galois groups

Let k be a field and let $\overline{k}$ be an algebraic closure of k.

- The *absolute Galois group* $\mathrm{Gal}(k)$ is the group of field automorphisms of $\overline{k}$ which keep k fixed.
- It follows from Galois theory that

$$G := \mathrm{Gal}(k) \simeq \varprojlim_{N} G/N,$$

  where N ranges over the normal subgroups of G of finiite index.
- **Theorem 2** *(FNies) If k is a computable field with a splitting algorithm, then we can effectively embed $Gal(k)$ as a Π^0_1 (effectively closed) subspace of the Baire space ω^ω.*

6 Pseudo-Algebraically Closed (PAC) Fields

The notion of PAC arose from the study of the first order theory of finite fields and the question of its decidability. (Ax, early sixties).

1. A field F is *pseudofinite* if and only if it satisfies all first order properties of finite fields in the language of fields.
2. This is the case iff

   it is perfect and, for every n, it has a unique field extension of degree n

   AND it is PAC.
3. The absolute Galois group of a PAC field is a projective object in the category of profinite groups. The converse is also true (Lubotsky and van den Dries).
4. **Theorem 3** *(FNies) If K is a computable field with a splitting algorithm, the PAC property is given by a Π^0_2 predicate.*

7 Hilbertian fields

- A field k is Hilbertian if for every absolutely irreducible $f(T_1, \cdots, T_r, X_1, \ldots, X_s)$ with coefficients in k, there exists $(t_1, \ldots, t_r) \in k^r$ such that $f(t_1, \cdots, t_r, X_1, \ldots, X_s)$ is irreducible.
- The main theorem of this talk is also true for computable Hilbertian fields with splitting algorithm.
- The crucial observation here is that under these circumstances, we can, for every computable Hilbertian field with a splitting algorithm , for every natural number n, effectively construct a Galois extension L of k, having a Galois group isomorphic to the symmetry group S_n. This is an effective version of Hilbert's motivation for proving his irreducibilty theorem.

  This follows from the work of Kronecker and his, in modern language, constructive approach to Galois theory and this very deep insight of Hilbert.

8 Computable and constructive number theory and its links to diffusions: Perhaps an open problem and a side note

As it happens, while thinking about these issues during lockdown and the great talks at this conference on Fourier dimensions and fractal geometry, I was also thinking about a statement by Rumely to the effect:

Theorem 4 *(Rumely 1985)*

There is a primitive recursive algorithm to decide Hilbert's tenth problem over the ring of algebraic numbers.

His method, as he states unequivocally, does not give any information on how such solutions over the algebraic integers can be algorithmically found. His argument involves, among many things, tricky diffusions over adeles , but if we look at his arguments at infinite places, then we are back to fractal geometry and understanding Hausdorff and Fourier dimensions of fractal sets constructively or at least effectively in terms of Frostman measures that can be defined over these sets.

I feel Rumely's theorem is quite fundamental and deserves further exploration. I am somewhat bemused if not beguiled that his result is not better known.