Received: 7 December 2023 | Revised: 3 July 2024 | Accepted: 13 August 2024

DOI: 10.1112/jlms.70017

RESEARCH ARTICLE

Journal of the London Mathematical Society

Computability in infinite Galois theory and algorithmically random algebraic fields

Wesley Calvert[1] | Valentina Harizanov[2] | Alexandra Shlapentokh[3]

[1]School of Mathematical and Statistical Sciences, Southern Illinois University, Carbondale, Illinois, USA

[2]Department of Mathematics, The George Washington University, Washington, District of Columbia, USA

[3]Department of Mathematics, East Carolina University, Greenville, North Carolina, USA

Correspondence
Wesley Calvert, School of Mathematical and Statistical Sciences, Southern Illinois University, Mail Code 4408, 1245 Lincoln Drive, Carbondale, IL 62901, USA.
Email: wcalvert@siu.edu

Funding information
National Science Foundation, Grant/Award Number: DMS-1928930; Fulbright-Nehru Senior Research Fellowship; NSF FRG, Grant/Award Numbers: DMS-2152095, DMS-2152098

Abstract
We introduce a notion of algorithmic randomness for algebraic fields. We prove the existence of a continuum of algebraic extensions of $\mathbb{Q}$ that are random according to our definition. We show that there are noncomputable algebraic fields which are not random. We also partially characterize the index set, relative to an oracle, of the set of random algebraic fields computable relative to that oracle.

In order to carry out this investigation of randomness for fields, we develop computability in the context of the infinite Galois theory (where the relevant Galois groups are uncountable), including definitions of computable and computably enumerable Galois groups and computability of Haar measure on the Galois groups.

MSC 2020
03C57, 03D32, 03D45, 11U99 (primary)

1 | INTRODUCTION

We can often understand a class of structures better by understanding the "typical" elements of the class. In this paper, we propose a definition of a typical algebraic field. Intuitively, we would expect that a typical object is the most likely result of a selection at random from the class, perhaps with respect to some probability distribution. Thus, we refer to our typical fields as "random fields."

The study of random elements has been carried out for many classes of objects. Perhaps the most well-developed and fruitful example of such a study is the case of random graphs [6, 12, 13].

While the randomness discussed in that work was not algorithmic, it demonstrates the potential benefits of the investigation of random elements. In a benchmark example of the effectiveness of this technique, Pinsker used random graphs to answer a major question about the existence of a class of graphs (where the original problem made no mention of randomness) [25]. This leads us to hope that understanding random fields might lead to new insights about all fields.

There has also been work on random groups (including the work described in [11, 16, 20]), and random structures more generally [15, 19, 21–23]. These papers, collectively, give many definitions of typical elements of many classes of structures. It appears, however, that it is more difficult to make a meaningful definition of a typical element when discussing classes of structures that exhibit greater complexity.

It turns out that there is a combinatorial property (trivial definable closure) that determines whether a class of structures will have a single isomorphism type representing a typical element (in the sense of a suitably invariant probability measure on the class concentrating on that isomorphism type) [1–3]. Graphs have this property, but groups and—critically for this paper—fields do not.

In view of this, the problem of describing a typical, or random, field is more complicated than the analogous problem for graphs. In this paper, we will give a definition that we argue captures the notion of typicality on algebraic fields.

To achieve our results on random fields, we develop computability theory for absolute Galois groups, based on Krull topology. Galois groups of many infinite fields are uncountable and therefore the usual notions of computability are not applicable in this context. However, the graphs of absolute Galois groups of countable fields (defined in Section 4) are countable and therefore can be used to define a computable absolute Galois group. The fixed field of a Galois group which is computable in this sense turns out to be computable in the usual way confirming that our definition is a reasonable one. Things become more complicated when it is necessary to define c.e. absolute Galois groups that are not computable. The reader can find this discussion in Section 4.

To make use of our definition of a computable absolute Galois group, we had to make sure that the computability of a group and its fixed field extends to various properties of the field in an expected manner. The technical results pertaining to these matters can be found in Sections 2 and 3 and especially in Section 4.

For reasons above, this paper combines results from computability and computable structure theory, algorithmic randomness, and infinite Galois theory. As we point out below, we included some basic facts from these areas to make the paper readable by a wider audience.

In this paper, we state our results in the language of algebraic extensions of $\mathbb{Q}$ to simplify the presentation. Since $\mathbb{Q}$ has a splitting algorithm, we can construct a computable copy $\overline{\mathbb{Q}}$ of an algebraic closure in which the domain of $\mathbb{Q}$ is a computable subset. However, our work actually shows a good deal more. Everything in the present paper applies to any computable field with a splitting algorithm, for example, a countable function field.

1.1 | The structure of the paper

Because we hope to accommodate readers from diverse backgrounds, we have attempted to make the paper self-contained. In Section 2, we review standard background in computability. Section 2.3 introduces an important assumption used throughout the paper. Section 3 gives a similar background on Haar measure and absolute Galois groups, with Section 3.3 describing computability in this context.

Section 4 begins the technical heart of the paper, establishing important relationships between the computable structure theory of algebraic fields and that of their absolute Galois groups. This section establishes the vocabulary that allows us in Section 5 to finally define random fields, prove their existence, and make some preliminary investigations into their characterization and properties. Section 6 addresses the index set problem for random fields.

2 | BACKGROUND ON COMPUTABILITY

2.1 | Computable and c.e. sets, and computable functions

We follow the standard notations and definitions of computability theory. Good general references for this section are [4, 29, 30].

2.1.1 | Computable and computably enumerable sets

A set C of natural numbers (or of tuples of natural numbers) is *computable* if there is a decision procedure for identifying its elements. That is, there is a Turing machine that on an input x always halts and outputs 1 if $x \in C$ and outputs 0 if $x \notin C$. Computable sets encode decidable problems (i.e., problems that can be solved algorithmically). All finite sets are computable. Appealing to Church's Thesis, we say that a function is computable if and only if there is an algorithm to compute it.

A set E of natural numbers is *computably enumerable* (abbreviated by c.e.) if E is empty or there is a computable unary function f such that

$$E = \mathrm{ran}(f) = \{f(0), f(1), \ldots\}.$$

Hence, every computable set is c.e. For an infinite c.e. set an enumeration $f(0), f(1), \ldots$ can be modified by eliminating repetitions to be one-to-one. A classical result in computability shows there are c.e. sets that are not computable.

A partial function ψ is *partial computable* if there is a Turing machine that on every input in the domain of ψ halts and outputs its value, while on every input that is not in the domain of ψ it computes forever. It can be shown that a set E is c.e. if and only if it is the domain of a partial computable function ψ, that is, $E = \mathrm{dom}(\psi)$. Moreover, a set E is c.e. if and only there is a computable binary relation R such that for every x it is the case that

$$x \in E \Leftrightarrow (\exists y)R(x, y).$$

All c.e. sets can be simultaneously algorithmically enumerated by effectively enumerating all Turing machines. In other words, there is a computable enumeration of all unary partial computable functions and their domains partial. Clearly, the complement of a computable set is computable. On the other hand, there are c.e. sets—exactly the noncomputable c.e. sets—with complements that are not c.e. A well-studied example of a noncomputable c.e. set is the diagonal halting set K. The set K consists of all inputs e on which the Turing machine with index e (or the

eth computable function φ_e) halts. That is,

$$K = \{e : e \in W_e\} = \{e : \varphi_e(e) \text{ halts}\},$$

where W_e is the c.e. set that is the domain of the function φ_e computed by the Turing machine with index e.

2.1.2 | Arithmetical hierarchy

We have the following classification of subsets of natural numbers and, more generally, of relations on natural numbers. Π^0_n and Σ^0_n sets (relations) are levels in the *arithmetical hierarchy* obtained from computable relations by applying existential and universal quantifiers. More precisely, a set A is $\Sigma^0_0 = \Pi^0_0$ if it is computable. For $n > 0$, a set A is Σ^0_n if there is a computable $(n+1)$-ary relation R such that for every $a \in \mathbb{N}$,

$$a \in A \Leftrightarrow (\exists x_0)(\forall x_1) \cdots (Qx_{n-1})R(a, x_0, x_1, \dots, x_{n-1}),$$

where Q is $\exists$ if n is an odd number, and Q is $\forall$ if n is an even number.

Π^0_n sets are defined similarly starting with the universal quantifier. Clearly, the complement of a Σ^0_n set is a Π^0_n set and vice versa. We say that a set is Δ^0_n if it is both Σ^0_n and Π^0_n. It follows that Σ^0_1 sets are the c.e. sets, Π^0_1 sets are the co-c.e. sets, and $\Delta^0_0 = \Delta^0_1$ sets are the computable sets. A set is called *arithmetical* if it is Π^0_m for some m (or Σ^0_m for some m).

The superscript 0 in the notation Π^0_n and Σ^0_n indicates that all quantifiers will range only over natural numbers (and elements of structures that have been indexed by natural numbers). A superscript of 1 or more would indicate quantification over functions or higher-type objects, and will play no role in this paper.

Given a set complexity class $\mathfrak{C}$, such as Σ^0_n or Π^0_n, we say that a set X of natural numbers is *m-complete* $\mathfrak{C}$ if X is in $\mathfrak{C}$, and there is a computable reduction of every set Y in $\mathfrak{C}$ to X (i.e., X is $\mathfrak{C}$-hard). This reduction is a computable function $f : \mathbb{N} \to \mathbb{N}$ such that for every $n \in \mathbb{N}$, we have:

$$n \in Y \Leftrightarrow f(n) \in X.$$

Since the function f can be many–one function we call this completeness m-completeness. For example, the halting set is Σ^0_1 m-complete.

2.1.3 | Turing reducibility

For $Y \subseteq \mathbb{N}$, let

$$\varphi^Y_0, \varphi^Y_1, \varphi^Y_2, \dots$$

be a fixed effective enumeration of all unary partial Y-computable functions– - that is, functions which are computable using Y as an oracle. If an oracle Y is computable, then it is not needed, so we omit the superscript Y. For sets X and Y, we write $X \leqslant_T Y$ if X is Turing reducible to Y—that is, if the characteristic function of X is given by φ^Y_e for some e. The partial order relation $\leqslant_T$ gives rise to an equivalence relation $\equiv_T$, the equivalence classes of which are called Turing degrees. The Turing degree of $\varnothing$ or of any computable set is denoted $\mathbf{0}$.

For a set Y, the jump of Y is defined generalizing K as follows:

$$Y' = \{e : \varphi_e^Y(e) \text{ halts}\}.$$

Hence, $\varnothing' = K$. It can be shown that $Y <_T Y'$. The jump operator can be iterated: $Y^{(k+1)} = (Y^{(k)})'$, where $Y^0 = Y$.

For $n \geqslant 1$, let $\mathbf{y}^{(n)} = \deg(Y^{(n)})$. It can be shown that a set is Σ_n^0 if it is computably enumerable in (or relative to) $\mathbf{0}^{(n-1)}$. Hence, a set X is *arithmetical* if $X \leqslant_T \varnothing^{(k)}$ for some $k \geqslant 0$.

2.1.4 | Enumeration reducibility

A set X is *enumeration reducible* to a set Y, denoted by $X \leqslant_e Y$, if we can computably enumerate the elements of X from an enumeration of the elements of Y, where the enumeration of X does not depend on the order is which Y is enumerated. That is, $X = \Psi^Y$, where Ψ is some enumeration operator. If $X \leqslant_e Y$ then X is computably enumerable in Y. Moreover, Selman showed that $X \leqslant_e Y$ if and only if for every set C, if Y is computably enumerable in C, then X is computably enumerable in C. The partial order relation $\leqslant_e$ of sets gives rise to an equivalence relation, the equivalence classes of which are called enumeration degrees. There are also enumeration degrees of partial functions, called partial degrees.

2.1.5 | Computable formulas

We will only consider countable structures for computable languages. The universe A of an infinite countable structure $\mathscr{A}$ can be identified with the set of natural numbers. If L is the language of $\mathscr{A}$, then L_A is the language L expanded by adding a constant symbol for every $a \in A$, and $\mathscr{A}_A = (\mathscr{A}, a)_{a \in A}$ is the corresponding expansion of $\mathscr{A}$ to L_A. The *open diagram* of a structure $\mathscr{A}$, $D(\mathscr{A})$, is the set of all quantifier-free sentences of L_A true in $\mathscr{A}_A$. A structure is *computable* if its open diagram is computable. A structure for a finite language is computable if its domain is a computable set and its functions and relations are computable.

We will now define computable infinitary formulas. Computable Σ_0 and Pi_0 formulas are just the finitary quantifier-free formulas (i.e., the quantifier-free formulas involving only finitely many disjuctions, conjunctions and quantifiers). Let $n > 0$. A *computable* Σ_n *formula* is a c.e. disjunction of formulas

$$\exists \overline{u}\, \psi(\overline{x}, \overline{u}),$$

where ψ is a computable Π_m formula for some $m < n$.

A *computable* Π_n *formula* is a c.e. conjunction of formulas

$$\forall \overline{v}\, \theta(\overline{y}, \overline{v}),$$

where θ is a computable Σ_m formula for some $m < n$.

In a computable structure, a computable Σ_n formula defines a Σ^0_n set, and a computable Π_n formula defines a Π^0_n set. For more on computable structures and computable formulas, see [4, 14].

2.1.6 | Immune sets

In an attempt to construct a c.e. set of Turing degree strictly between the computable one and the degree of the halting set, Post introduced sets with "thin" complements with respect to c.e. sets.

Definition 2.1. A set of natural numbers is *immune* if it is infinite and does not contain any infinite c.e. subset.

The complements of immune sets may or may not be c.e. Those that are c.e. are called simple sets and were first constructed by Post. There is further proper strengthening of immune sets into hyperimmune, hyperhyperimmune, and cohesive sets. While there are countably many simple sets, it can be shown that there are continuum many cohesive sets.

Definition 2.2. A set $C \subseteq \mathbb{N}$ is *cohesive* if C is infinite and for every c.e. set W, either $W \cap C$ or $\overline{W} \cap C$ is finite.

(Here, $\overline{W}$ is the complement of W. Hence, a cohesive set C is indecomposable into two infinite parts by a c.e. set W.)

Definition 2.3. A set $C \subseteq \mathbb{N}$ is *r-cohesive* if C is infinite and for every computable set W, either $W \cap C$ is finite or $\overline{W} \cap C$ is finite.

Every cohesive set is r-cohesive, but the converse is not true. Every r-cohesive set is immune, but the converse is not true.

Lemma 2.4. *An r-cohesive set cannot have immune complement. Hence, a cohesive set cannot have immune complement.*

Proof. Assume that C is r-cohesive. Fix an infinite co-infinite computable set R. Then, either $R \cap C$ is finite or $\overline{R} \cap C$ is finite. If $R \cap C$ is finite, then $R - C$ is an infinite c.e. (in fact, computable) set such that $R - C \subseteq \overline{C}$. If $\overline{R} \cap C$ is finite, then $\overline{R} - C$ is an infinite c.e. (in fact, computable) set such that $\overline{R} - C \subseteq \overline{C}$. Hence, $\overline{C}$ is not immune. □

We now describe a property of sets of natural numbers that we will use in Section 5.

(*) $X \subseteq \mathbb{N}$ is an infinite co-infinite set such no co-infinite superset $S \supseteq X$ has an infinite c.e. subset (i.e., S is immune).

Lemma 2.5. *There is no set X with property (*).*

Proof. If X has property (*), then X must be immune. Otherwise, X has an infinite c.e. subset, so $S = X$ has an infinite c.e. subset, contradicting property (*).

If X has property (*), then $\overline{X}$ must be cohesive. Otherwise, there is a c.e. set W such that both $W \cap \overline{X}$ and $\overline{W} \cap \overline{X}$ are infinite. Let $S = X \cup W$. Then, S is co-infinite since $\overline{S} = \overline{W} \cap \overline{X}$ is infinite, and S contains an infinite c.e. subset W, contradicting property (*).

By Lemma 2.4, it is not possible to have a cohesive set with immune complement. □

2.2 | Computable structures

To study computability on a countable infinite structure, we construct a bijection from elements of the structure onto the natural numbers. The operations on the structure are then translated into the maps over natural numbers. It is tempting to say that a structure is computable (or c.e.) if and only if the image in the natural numbers is computable (resp. c.e.) and its operations are all computable.

Unfortunately, this definition does not really differentiate between computable and c.e. algebraic structures because, for example, we can always construct a computable isomorphic copy of a computably enumerable field. To understand the difference between computable and c.e. structures, one has to look at a problem of simultaneously representing two structures computably within a structure containing them both.

The issue of simultaneous computable enumeration is easy to see when it comes to fields. By a famous theorem of Rabin [26] we know that any computable (in the sense above) field has a computable algebraic closure (in the sense above). However, the theorem does not guarantee a simultaneous computable presentation of the algebraic closure and the original field within it.

The same result of Rabin also tells us that the simultaneous computable presentation of the field and its algebraic closure is possible if and only if the original field had a splitting algorithm (see Definition 2.9). In other words, given a computable field in the sense above without a splitting algorithm, we have a choice for a construction of the algebraic closure: either we make the original field computable in the sense above and we have a c.e. algebraic closure, or we have a c.e. presentation of the original field and a computable algebraic closure.

Definition 2.6 (Computable fields and c.e. fields). Let F be a computable field with a splitting algorithm, and $\overline{F}$ a computable algebraic closure of F such that F is a computable subset of $\overline{F}$. Then, a subfield of $\overline{F}$ is said to be *computable* if its set of elements is a computable subset of the set of natural numbers. A subfield of $\overline{F}$ is said to be *computably enumerable* if and only if its set of elements is computably enumerable.

Definition 2.7. We say that a sequence of fields $(F_i : i \in \mathbb{N})$ is *uniformly computable* if and only if there is a computable function ϕ such that $\phi(i)$ is the index for a Turing machine computing the characteristic function of F_i.

Remark 2.8. There exist sequences $(F_i : i \in \mathbb{N})$ of computable fields which are not uniformly computable. For instance, let $(p_i : i \in \mathbb{N})$ be an enumeration of the distinct rational primes. Then, the sequence of fields $\left(\mathbb{Q}(\sqrt{p_i}) : i \in \emptyset'\right)$ is not uniformly computable, since $\emptyset'$ is not computable. However, each individual field in the sequence is computable.

2.3 A fixed computable algebraic closure of $\mathbb{Q}$

For the rest of the paper, we fix a computable bijection $\sigma : \overline{\mathbb{Q}} \longrightarrow \mathbb{N}$ such that the images of the graphs of addition and multiplication are also computable. As noted above, $\sigma(\mathbb{Q})$ will be a computable set.

Note that even in this environment, many properties may remain ineffective. For instance, it is not clear that we could effectively determine, given the characteristic function of a field as a subset of $\overline{\mathbb{Q}}$, whether that field is a finite extension of $\mathbb{Q}$, or, if finite, what its degree would be.

Definition 2.9 (Splitting algorithm). Let K be a computable field. We say that K has a splitting algorithm if there is an effective procedure to determine whether a polynomial with coefficients in K is irreducible over K.

The following result is a part of Rabin's theorem we discussed above.

Proposition 2.10. *Every algebraic extension of $\mathbb{Q}$ within a fixed computable algebraic closure of $\mathbb{Q}$ is computable if and only if it has a splitting algorithm.*

Proof. Let $K \subset \overline{\mathbb{Q}}$ be a computable field. Given a polynomial over K we can find all of its roots in $\overline{\mathbb{Q}}$ and then determine which symmetric functions of the roots lie in K.

Conversely, suppose that a field K has a splitting algorithm. Given an element x of the algebraic closure we find some polynomial $p(T)$ over $\mathbb{Q}$ such that $p(x) = 0$ and determine the factorization of $p(T)$ over K. Then, $x \in K$ if and only if $p(T)$ has a factor $(T - x)$ over K. □

The following results are standard, first proved in [18]. We adjust them slightly for our context, somewhat more narrow than [18], where work inside a fixed algebraic closure was not assumed.

Lemma 2.11. *Let M/K be a finite extension of computable fields, given by computable characteristic functions of their domains and the degree of the extension. Then, there exists an effective procedure to find an element α such that $M = K(\alpha)$.*

Proof. Let $n = [M : K]$. Since K is computable, it has a splitting algorithm by Proposition 2.10. We test elements of M until we find an element $\alpha \in M$ satisfying an irreducible polynomial of degree n over K. □

Lemma 2.12. *There is an effective procedure which will, given a computable field K and an element $x \in \overline{\mathbb{Q}}$, determine the set of conjugates of x over K.*

Proof. Since K is computable, we proceed as follows. We find a polynomial $P(t)$ over $\mathbb{Q}$ satisfied by x. We then factor $P(t)$ over $\mathbb{Q}$ to determine an irreducible factor $Q(t)$ of $P(t)$ satisfied by x. We can then find all the other roots $x = x_1, \dots, x_m$ of $Q(t)$ in the computable algebraic closure, and by considering all possible symmetric functions of the conjugates determine the minimal polynomial $S(t)$ of x over K. □

Lemma 2.13. *Let $K \subset \overline{\mathbb{Q}}$ be a computable finite extension of $\mathbb{Q}$. Then, any finite extension of K is also computable, uniformly in the generators of the extension and in K. (Therefore, the splitting algorithm* *for the extension can also be constructed in a uniform fashion from the characteristic function of K and a generator of the extension.)*

Proof. Let K be a computable extension of $\mathbb{Q}$ generated by an element $\alpha \in \mathbb{Q}$. Since K has a splitting algorithm we can (by Lemma 2.12) determine all the distinct conjugates $\alpha_1 = \alpha, \dots, \alpha_n$ of α over K. Let $\beta \in \overline{\mathbb{Q}}$. Applying Lemma 2.12 again, let $\beta_1 = \beta, \dots, \beta_r$ be all the distinct conjugates of β over K. If $r > n$, then $\beta \notin K(\alpha)$.

Suppose now that $r \leqslant n$ and consider the following system in the unknowns $a_0, \dots, a_{n-1} \in \overline{\mathbb{Q}}$:

$$\sum_{i=0}^{n-1} a_i \alpha_k^i = \beta_{j_k}, k = 1, \dots, n,$$

where $\beta_{j_1} = \beta$ and $j_k \in \{1, \dots, r\}$. The determinant of the system is a Vandermonde determinant. Thus, for every choice for $j_2, \dots, j_n$ we can solve the system over $\overline{\mathbb{Q}}$ and see if the solutions are in K. If $\beta \in K(\alpha)$, the system has solutions in K for some choice of $j_2, \dots, j_n$. Conversely, if for some choice of $j_2, \dots, j_n$ the system has solutions $a_0, \dots, a_{n-1} \in K$, then $\beta = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \in K(\alpha)$. □

Corollary 2.14. *Let K be a computable field and let $\{\alpha_i : i \in \mathbb{N}\}$ be a computable sequence of elements of $\overline{K}$. Then, there is an effective procedure taking as its input the index of the element of the sequence and generating a characteristic function of $K(\alpha_1, \dots, \alpha_i)$ and the splitting algorithm for this field.*

2.4 | Computability on spaces of functions

So far we have discussed computability over countable structures containing objects describable by a finite input. However, to study randomness over algebraic extensions of $\mathbb{Q}$ one has to use some notion of computability for collections of objects that one cannot describe completely using a finite amount of information, for example, the elements of the absolute Galois group of $\mathbb{Q}$.

Definition 2.15 (Absolute Galois group). Let K be an algebraic extension of $\mathbb{Q}$. Then, the absolute Galois group of K, denoted by $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, is the group of all automorphisms of $\overline{\mathbb{Q}}$ which restrict to the identity function on K.

These elements, of course, are maps from a countable set to a countable set. In this section, we describe some of the standard tools for studying objects of this kind from the point of view of the computability theory.

Recall that we are working in a particular computable copy of $\overline{\mathbb{Q}}$, constructed via a fixed computable bijection $\sigma : \overline{\mathbb{Q}} \longrightarrow \mathbb{N}$. Thus, we could identify any map $f : \overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}$ with a countable sequence $\{a_i : i \in \mathbb{N}\}$ of natural numbers, where $f(\sigma^{-1}(i)) = \sigma^{-1}(a_i)$. Observe that this identification between the set of all maps from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}}$ and the set of all sequences of natural numbers is a bijection induced by σ.

In view of this identification of functions and sequences, to study computability on the set of all functions from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}}$, it is sufficient to study computability on the space of all infinite sequences of natural numbers.

The first question of such a study is to define a computable set of sequences. To make such a definition reasonable, one would want an algorithm that determines whether a particular sequence is in a given set. Unfortunately, an algorithm can take inputs of finite size only and therefore we can never specify the whole sequence as an input. This leaves us with only one option: we specify a finite part of a sequence.

The two obvious options are: we specify initial segments of a given sequence or any finite part of the graph of the corresponding function. Thus, we can possibly ask questions of the following sort about a collection S of sequences:

(1) Given a finite initial segment of a sequence: $a_1, \ldots, a_m$, is there a sequence in S with such an initial segment?
(2) Given two finite collections of integers $m_1, \ldots, m_r$ and $a_1, \ldots, a_r$, we can ask whether S contains a sequence $\{b_i : i \in \mathbb{N}\}$ such that $b_{m_j} = a_j, j = 1, \ldots, r$.

Are these two approaches equivalent? The answer to this question depends on the size of the potential set of values for a position in the sequence.

If the potential set of entries for any position in the sequence is infinite, then the graph input provides more information. Indeed, suppose we want to know whether S contains a sequence $\{b_i : i \in \mathbb{N}\}$ with $b_m = a$ for some fixed m and a. To answer this question using initial segments, we need potentially to ask a question about every possible initial segment of size m with the last element of the segment equal to a. If the number of such initial segments is infinite then this process might not converge.

Conversely, assuming we can answer questions about finite subsets of the graph of the function corresponding to a given sequence, we can effectively determine whether S contains a sequence with a prescribed initial segment.

At the same time if the number of possible entries for a position in a sequence is finite, then the information provided by finite subsets of the graph and finite initial segments is the same because for any m there will be only finitely many initial segments of size m.

Finally, we can ask whether it makes a difference whether we are allowed to specify only one element of the graph or finitely many when asking a question about sequences in S. The answer again depends on the number of possible values for a position in a sequence since asking about a finite part of the graph requires information about potentially infinitely many initial segments.

Indeed, suppose we want to know whether our set S of sequences contains a sequence with $b_i = a_1$ and $b_j = a_2$. Assuming $j > i$, to answer the question we need to know if there exists an initial segment of length j containing the above described entries in the positions i and j. As before, in the case of infinitely many values allowed for each position in the sequence, the information about pairs in the graphs of functions in S is not sufficient to answer this question.

At the same time if the number of potential values for each position is finite, then all three approaches are the same.

There are many implementations of the three approaches above. For example, the initial segment approach has been realized via a function

$$f_S(d,r) := \begin{cases} 1 & \text{if } B_r(d) \cap ({}^{\sigma}S) \neq \emptyset \\ 0 & \text{if } B_{2r}(d) \cap ({}^{\sigma}S) = \emptyset \\ 0 \text{ or } 1 & \text{otherwise} \end{cases}$$

where $d \in \omega^{<\omega}$, where r is a rational number, and where $B_r(d)$ is the ball of radius r about d in Baire space (see [31]). Indeed, this approach would give us an additional equivalent condition in Theorem 4.8.

In the case of an absolute Galois group of a countable field, the number of values assigned to each position is always finite because it is bounded by the number of roots of the minimal polynomial of the element in question over a primary field.

It must be remembered that in identifying functions $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ with ω^{ω}, this representation and everything around it—including the computability, depend on the specific bijection $\overline{\mathbb{Q}} \to \mathbb{N}$, a theme to which we will return in the next section.

3 | HAAR MEASURE

In this section, we will discuss Haar measure on the absolute Galois group of $\mathbb{Q}$. For the most part, we follow the presentation in Fried and Jarden (see [17]).

3.1 | Inverse limits and profinite topology

In this section, we review the notion of inverse limits and the topology arising from them.

Let I be a partially ordered set. An inverse system $(S_i, \pi_{i,j} : i, j \in I)$ consists of a family of sets $\{S_i : i \in I\}$ and for each $i \geqslant j \in I$, a function $\pi_{i,j} : S_i \to S_j$ so that $\pi_{i,i}$ is the identity function for each i, and $\pi_{i,k} = \pi_{j,k} \circ \pi_{i,j}$. In this paper, the S_i will generally be Galois groups of finite extensions.

Let $(S_i, \pi_{i,j})$ be an inverse system in which each S_i is a topological space, and let $S = \varprojlim S_i$. Further, let $\pi_i : S \to S_i$ be the restriction to S of the projection from $\prod_j S_j$ to S_i. To define a topology on S, we use the sets of the form $\pi_i^{-1}(U_i)$, where U_i is an open subset of S_i as a basis. When the S_i are finite sets with the discrete topology, as will often be the case in this paper, the induced topology is called the *profinite topology*. In our case, the S_i will be an inverse system of discrete finite subsets of Galois groups of finite extensions, and the resulting profinite topology is called the *Krull topology*.

Remark 3.1. From now on all references to open and closed sets will refer to Krull topology, unless some other topology is explicitly identified.

The proof of the following lemma can be found in Section 1.1, Chapter 1 of [17].

Lemma 3.2. *Let $\overline{H} \subset \overline{G} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ be such that $\overline{H}$ contains all elements of $\overline{G}$ restricting to the set of elements $H \subseteq Gal(K/\mathbb{Q})$ for some finite Galois extension K of $\mathbb{Q}$. In this case, $\overline{H}$ is a basic open subset of $\overline{G}$. Furthermore, this subset is also closed.*

We will need to use a smaller class of open sets which will still constitute a basis for Krull topology. To describe this class, we will use the following notation.

Definition 3.3. Let τ be an embedding from an algebraic number field to $\overline{\mathbb{Q}}$. Then, $E(\tau)$ is the set of all extensions of τ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Lemma 3.4. *Let $\{\alpha_i : i \in \mathbb{N}\} \subset \overline{\mathbb{Q}}$ be such that $\mathbb{Q}(\alpha_i) \subset \mathbb{Q}(\alpha_{i+1})$ and $\overline{\mathbb{Q}} = \bigcup_{i\in\mathbb{N}} \mathbb{Q}(\alpha_i)$. Let T_i be the set of all embeddings $\tau : \mathbb{Q}(\alpha_i) \longrightarrow \overline{\mathbb{Q}}$. Every open subset of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ is a union of sets of the form $E(\tau_i)$, where τ_i is an element of T_i.*

Proof. Let $K/\mathbb{Q}$ be a finite extension, let $\gamma : K \to \overline{\mathbb{Q}}$ be an embedding and let $E(\gamma)$ be the set of all extensions of γ in Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$. We want to show that $E(\gamma)$ is the union of a collection of sets of the form $E(\tau)$ for some $\tau \in T_i$ for some i. Let α_j be such that $K \subset \mathbb{Q}(\alpha_j)$. Let $\gamma_1, \dots, \gamma_r$ be all the distinct extensions of γ to $K(\alpha_j)$. Then $E(\gamma) = E(\gamma_1) \cup E(\gamma_2) \cup \cdots \cup E(\gamma_r)$. However, each $\gamma_m = \tau$ for some $\tau \in T_j$. Hence, the assertion of the lemma holds. □

Lemma 3.5. *A one element subset of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ is closed.*

Proof. By Lemma 1.1.3 of [17], the topology of the absolute Galois group is Hausdorff. In the Hausdorff topology, a set consisting of one point is closed. □

We will also make use of the following lemma.

Lemma 3.6. *Let $\sigma \in$ Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ and let K^σ be its fixed field. Then, the closure of the group generated by σ is Gal$(\overline{\mathbb{Q}}/K^\sigma)$.*

Proof. Let G_σ be the group generated by σ. Then, $G_\sigma \subset$ Gal$(\overline{\mathbb{Q}}/K^\sigma)$. By infinite Galois theory (Proposition 1.3.1 of [17]) we have that Gal$(\overline{\mathbb{Q}}/K^\sigma)$ is closed. Suppose that closure of G_σ is a proper subset of Gal$(\overline{\mathbb{Q}}/K^\sigma)$. In this case, we have two closed subgroups of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ corresponding to the same fixed field. This is impossible by the infinite Galois theory (again by Proposition 1.3.1 of [17]). □

3.2 | Computing Haar measure of absolute Galois groups

Let $G =$ Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$, and let $\mathscr{B}$ (the Borel field of G) be the smallest family of subsets of G containing all closed subsets and closed under taking complements in G and countable unions (hence also intersections).

Definition 3.7 (Haar measure). A Haar measure on G is a function $\mu : \mathscr{B} \to \mathbb{R}$ such that

- $0 \leqslant \mu(B) \leqslant 1$ for all $B \in \mathscr{B}$,
- $\mu(\emptyset) = 0, \mu(G) = 1$,
- If $\{B_i : i \in \mathbb{N}\}$ is a sequence of pairwise disjoint Borel sets, then $\mu(\bigcup_i B_i) = \sum_i \mu(B_i)$ (σ-additivity),
- If $B \in \mathscr{B}$ and $g \in G$, then $\mu(gB) = \mu(Bg) = \mu(B)$, and
- For each $B \in \mathscr{B}$ and each $\varepsilon > 0$ there exist an open set U and a closed set C such that $U \subseteq B \subseteq C$ and $\mu(C \setminus U) < \varepsilon$ (regularity).

By Propositions 18.1.3 and 18.2.1 of [17], Haar measure exists and it is unique.

Lemma 3.8 (A subgroup fixing a finite extension). *If K is a Galois number field, then Gal$(\overline{\mathbb{Q}}/K)$ is of Haar measure $\frac{1}{[K:\mathbb{Q}]}$.*

Proof. $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is the set of all extensions of the identity automorphism of K, and therefore is a basic open set, and hence a Borel set. (Of course, it is also closed, by the Fundamental Theorem of Infinite Galois Theory, as mentioned earlier.) Further, $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Thus, the index of the group must be the degree of K over $\mathbb{Q}$, and the measure must be $\frac{1}{[K:\mathbb{Q}]}$ by the invariance of Haar measure. □

Once we established the connection between the measure of the absolute Galois group of a Galois field with the degree of the field, we can now show that the same connection exists for all finite extensions of $\mathbb{Q}$.

Lemma 3.9. *Let K be any number field. Then, Gal*$(\overline{\mathbb{Q}}/K)$ *is of measure* $\frac{1}{[K:\mathbb{Q}]}$.

Proof. Let K^G be the Galois closure of K over $\mathbb{Q}$. Then, $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is the set of all extensions of automorphisms of K^G contained in the $\mathrm{Gal}(K^G/K)$. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ restricts to identity on K^G, then σ restricts to identity on K, and therefore $\mathrm{Gal}(\overline{\mathbb{Q}}/K^G) \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Further, if $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/K) - \mathrm{Gal}(\overline{\mathbb{Q}}/K^G)$, then τ restricts to a nontrivial automorphism of $\mathrm{Gal}(\overline{\mathbb{Q}}/K^G)$ restricting to identity on K. In other words, τ restricts to a non-trivial element of $\mathrm{Gal}(K^G/K)$. At the same time if $\tau, \gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ restrict to the same element of $\mathrm{Gal}(K^G/K)$, then $\gamma\tau^{-1} \in \mathrm{Gal}(\overline{\mathbb{Q}}/K^G)$. Hence, $[\mathrm{Gal}(\overline{\mathbb{Q}}/K) : \mathrm{Gal}(\overline{\mathbb{Q}}/K^G)] = [K^G : K]$. Therefore, by additivity of Haar measure we have that $\mu(\mathrm{Gal}(\overline{\mathbb{Q}}/K)) = [K^G : K]\mu(\mathrm{Gal}(\overline{\mathbb{Q}}/K^G))$. Therefore, by Lemma 3.8, we have that $\mu(\mathrm{Gal}(\overline{\mathbb{Q}}/K)) = [K^G : K]\frac{1}{[K^G:\mathbb{Q}]} = \frac{1}{[K:\mathbb{Q}]}$. □

Remark 3.10. Let $K/\mathbb{Q}$ be an infinite algebraic extension. Let $K = \bigcup_i K_i$, where $K_i \subset K_{i+1}$ and K_i is a number field. In this case, $\mathrm{Gal}(\overline{\mathbb{Q}}/K) = \bigcap_i \mathrm{Gal}(\overline{\mathbb{Q}}/K_i)$, where each $\mathrm{Gal}(\overline{\mathbb{Q}}/K_i)$ is a clopen set. Thus, the intersection is closed and hence measurable. Since $\mu\left(\mathrm{Gal}(\overline{\mathbb{Q}}/K)\right) \leqslant \mu(\mathrm{Gal}(\overline{\mathbb{Q}}/K_i))$ for every i, it follows that $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ has measure 0.

3.3 | Computable measures

In discussing a measure in the context of computability, it is reasonable to ask whether, or to what extent, the measure, considered as a function from measurable sets to real numbers, can be regarded as a computable function. Making sense of this general question is well beyond the scope of this paper. We can simplify this issue by considering computability of the measure on a distinguished class of sets.

Different choices of this distinguished class of sets can be justified on different grounds. For example, by Carathéodory's Extension Theorem (see, for instance, Theorem 12.8 of [28]), if we have a measure defined on an algebra $\mathscr{A}$ of sets (i.e., a collection of sets closed under complement, finite union, and finite intersection), then that measure admits a unique extension to the smallest σ-algebra containing $\mathscr{A}$. Thus, we might aim to have the restriction of the measure to some algebra of sets be, in some sense, computable. This is the approach taken by [5, 27].

Another approach is to choose the class of computable measurable sets. This is the approach taken by [24].

In this paper, we choose the first option. We plan, in future work, to explore the second. Our algebra of sets will be the algebra generated by the basic open sets of the Krull topology.

Lemma 3.11. *Let K be a Galois number field. Let $\tau \in Gal(K/\mathbb{Q})$. Let μ be the Haar measure. Then, $\mu(E(\tau)) = \mu(Gal(\overline{\mathbb{Q}}/K))$.*

Proof. If $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, then let $\tau^*, \tau^\# \in E(\tau)$. Then, $\tau^* \left(\tau^\#\right)^{-1} \upharpoonright_K = \mathrm{id}_K$. Therefore, $\tau^* \left(\tau^\#\right)^{-1} \in E(\mathrm{id}_K)$. Hence, $\tau^* \in E(\mathrm{id}_K) \left(\tau^\#\right)^{-1} = \mathrm{Gal}(\overline{\mathbb{Q}}/K) \left(\tau^\#\right)^{-1}$. So $E(\tau) = \mathrm{Gal}(\overline{\mathbb{Q}}/K)(\tau^\#)^{-1}$. Thus, $\mu(E(\tau)) = \mu(\mathrm{Gal}(\overline{\mathbb{Q}}/K)(\tau^\#)^{-1}) = \mu(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$. □

Corollary 3.12. *Let $\{K_1, \dots, K_n\}$ be a finite collection of number fields. Let $\tau_i \in Gal(K_i/\mathbb{Q})$. Then, there is an effective procedure to compute the Haar measure of $\bigcup_{i=1}^{n} E(\tau_i)$.*

Proof. By induction, it is enough to show how to compute the Haar measure of a union of two sets $E(\tau_1)$ and $E(\tau_2)$. Let K be any Galois number field containing K_1 and K_2. Let $\lambda_1, \dots, \lambda_r$ be all the extensions of τ_1 to $\mathrm{Gal}(K/\mathbb{Q})$. Similarly, let $\theta_1, \dots, \theta_m$ be all the extensions of τ_2 to $\mathrm{Gal}(K/\mathbb{Q})$. Then, $E(\tau_1) = \bigcup_{i=1}^{r} E(\lambda_i)$ and $E(\tau_2) = \bigcup_{j=1}^{m} E(\theta_j)$. Observe that $E(\lambda_i) \cap E(\lambda_j) = \emptyset$ for $i \neq j$. Similarly, $E(\theta_i) \cap E(\theta_j) = \emptyset$ for $i \neq j$. Let $\{\nu_1, \dots, \nu_l\} = \{\lambda_1, \dots, \lambda_r\} \cap \{\theta_1, \dots, \theta_m\}$. Finally, let $d = [K : \mathbb{Q}]$. Then, the measure

$$\mu(E(\tau_1) \cup E(\tau_2)) = \frac{r + m - l}{d}.$$

□

It is clear that a similar procedure will effectively compute the measure of a finite intersection of basic open sets and the complements. So, there is an effective way of computing the Haar measure of every set in the algebra.

4 | COMPUTABILITY THEORY OF ABSOLUTE GALOIS GROUPS

Because absolute Galois groups contain maps with countable domains, we will use the discussion in Section 2.4 to define computable and c.e. subsets of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. All methods for representing functions in Section 2.4 rely on a version of a graph of the set of functions under consideration. At this point, we take a closer look at different versions of such graphs. Below we list what seem to us the four most natural options for describing absolute Galois groups.

(1) The graph consists of pairs, (α, β) where β is one image of α under the action of the absolute Galois group, and $\alpha \in \overline{\mathbb{Q}}$.
(2) The graph consists of pairs, $\left(\vec{\alpha}, \vec{\beta}\right)$ where $\vec{\beta}$ is one image of $\vec{\alpha}$ under the action of the absolute Galois group, and $\vec{\alpha} \in \overline{\mathbb{Q}}^n$ for some positive integer n.
(3) The graph consists of sequences $(\alpha, \beta_1, \dots, \beta_n)$, where $\beta_1, \dots, \beta_n$ are *all possible images* of α under the action of the absolute Galois group, and $\alpha \in \overline{\mathbb{Q}}$.
(4) The graph consists of sequences $(\vec{\alpha}, \vec{\beta}_1, \dots, \vec{\beta}_n)$, where $\vec{\beta}_1, \dots, \vec{\beta}_n$ are *all possible images* of $\vec{\alpha}$ under the action of the absolute Galois group, and $\vec{\alpha} \in \overline{\mathbb{Q}}^n$ for some positive integer n.

Thus, we have four possible ways to represent absolute Galois groups. It would at first seem, for instance, that possibility 2 would contain more information than possibility 1, because it also includes information about consistency of images, and it would seem that possibility 4 would contain the most information. However, by working with a computable sequence generating $\overline{\mathbb{Q}}$ over $\mathbb{Q}$, and using complements of the graphs we will conclude that all versions of the graph are equivalent for some of our purposes (see Lemma 4.5).

In Lemma 4.6, we will show that all four sets are Turing equivalent. However, some differences arise at the level of enumeration reducibility, as we will see (Section 4.2).

4.1 | Computable absolute Galois groups

Here, we remind the reader that by a computable field we mean a field computable within a fixed computable algebraic closure of $\mathbb{Q}$.

Lemma 4.1. *Let $K \subset \overline{\mathbb{Q}}$ be a computable field. Then, there exists a computable sequence $\{\alpha_i : i \in \mathbb{N}\}$ such that $K = \mathbb{Q}(\{\alpha_i : i \in \mathbb{N}\})$.*

Proof. Given an element $\alpha \in \overline{\mathbb{Q}}$ we can determine whether $\alpha \in K$. Let $\alpha_1 \in K - \mathbb{Q}$ be such an element with the smallest code and let $K_1 = \mathbb{Q}(\alpha_1)$. (Note that this step is effective since K is computable.) By Lemma 2.13, we have that K_1 is also computable. Thus proceeding inductively we construct a computable sequence α_i such that $\bigcup_{i=1}^{\infty} \mathbb{Q}(\alpha_1, \dots, \alpha_i) = K$. □

Lemma 4.2. *If K is computable, then there exists a computable set of elements $\{\alpha_i : i \in \mathbb{N}\}$ of $\overline{\mathbb{Q}}$ such that $K(\{\alpha_i : i \in \mathbb{N}\}) = \overline{\mathbb{Q}}$. Further, the sequence can be selected so that for each $j \in \mathbb{N}$ we have that $K(\alpha_0, \dots, \alpha_j)$ is Galois over K.*

Proof. The sequence α_i can be constructed inductively in the following fashion. Find $\beta_0 \in \overline{\mathbb{Q}} - K$ with the smallest code. Next find all conjugates of β_0 over $\mathbb{Q}$. (This is an effective step since K is computable.) Let N_0 be the extension of K obtained by adjoining all conjugates of β_0 to K. Then N_0/K is Galois. Assume inductively that we have constructed N_i such that N_i/K is Galois. Now, we find $\beta_i \notin N_i$ with the smallest code and find all of its conjugates over K and adjoin them to N_i. The resulting field N_{i+1} is still Galois over $\mathbb{Q}$.

Since we always select an element not in N_i with the smallest code, every element of $\overline{\mathbb{Q}} - K$ will eventually be included at some step of the construction. Thus, $\overline{\mathbb{Q}} = \bigcup_{i=0}^{\infty} N_i$. □

Definition 4.3 (The graph and strong graph of a subset of an absolute Galois group). Let S be a subset of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(1) The *graph of S*, denoted by $\Gamma(S)$, is the set of pairs of the form (α, α_1), where every element of $\overline{\mathbb{Q}}$ appears as α, and α_1 is an image of α under the action of S. We denote by $S(\alpha)$ the set $\{\sigma(\alpha) : \sigma \in S\}$.

(2) Let S be a subset of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The *strong graph of S*, denoted $\Gamma_+(S)$, is the set of tuples of the form $(\vec{\alpha}, \vec{\alpha}_2, \dots, \vec{\alpha}_{k_\alpha})$, where every tuple of $\overline{\mathbb{Q}}$ appears as $\vec{\alpha}$ and $\vec{\alpha}_2, \dots, \vec{\alpha}_{k_\alpha}$ constitute a list (in order of increasing index) of *all* images of $\vec{\alpha}$ under the action of the subgroup.

Lemma 4.4. *Let S be a closed subset of $G(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $\tau \in G(\overline{\mathbb{Q}}/\mathbb{Q})$ be such that for every $\alpha \in \overline{\mathbb{Q}}$ we have that $\tau(\alpha) \in S(\alpha)$. Then, $\tau \in S$.*

Proof. Let $\{\alpha_i : i \in \mathbb{N}\} \subset \overline{\mathbb{Q}}$ be such that $\mathbb{Q}(\alpha_i) \subset \mathbb{Q}(\alpha_{i+1})$ and $\overline{\mathbb{Q}} = \bigcup_{i\in\mathbb{N}} \mathbb{Q}(\alpha_i)$. Let T_i be the collection of all embeddings of $\mathbb{Q}(\alpha_i)$ into $\overline{\mathbb{Q}}$. Suppose $\tau \notin S$. Then $\tau \in S^c$, where S^c, the complement of S in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, is open.

By Lemma 3.4, we know that the sets of the form $E(\nu)$—that is, extensions of a single embedding $\nu : \mathbb{Q}(\alpha_i) \to \overline{\mathbb{Q}}$ for some i, constitute a basis for the Krull topology. Therefore, for some collection $\Sigma = \{\tau_{i,j} : i, j \in \mathbb{N}\}$ where each $\tau_{i,j} \in T_i$ for some i, we have that $S^c = \bigcup E(\tau_{i,j})$. Hence, if $\tau \in S^c$, then for some i, j we have that $\tau_{i,j} \in \Sigma$ and $\tau_{|\mathbb{Q}(\alpha_i)} = \tau_{i,j}$ or equivalently $\tau(\alpha_i) = \tau_{i,j}(\alpha_i)$.

At the same time, for any $\mu \in S$ we have that μ cannot restrict to any $\tau_{i,j} \in \Sigma$ because $E(\tau_{i,j}) \subset S^c$. In other words, $\mu(\alpha_i) \neq \tau_{i,j}(\alpha_i)$. Therefore, if $\tau \in S^c$, we have that $\tau(\alpha_i) \notin S(\alpha_i)$ contradicting our assumptions on τ. □

We will frequently apply Lemma 4.4 in the case where S is the absolute Galois group of a field.

Lemma 4.5. *Let $S \subseteq Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $(\alpha_1, \dots, \alpha_k) \in \overline{\mathbb{Q}}^k$. Let A_S be the set of n-tuples $(\beta_1, \dots, \beta_n)$ such that there exists $\sigma \in S$ satisfying $\sigma(\alpha_i) = \beta_i$ for $i = 1, \dots, n$. Then $\Gamma(S) \geqslant_T A_S$.*

Proof. Using Lemma 2.11, we can effectively find an element $\gamma \in \overline{\mathbb{Q}}$ such that $\alpha_i \in \mathbb{Q}(\gamma)$ for all $i = 1, \dots, n$. Using $\Gamma(S)$, we determine all possible images of γ under the action of elements of S. Each potential image of γ will determine the image of the n-tuple $\alpha_1, \dots, \alpha_n$. □

Lemma 4.6. *Let $S \subseteq Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\Gamma(S) \equiv_T \Gamma_+(S)$.*

Proof. By letting $\vec{\alpha}$ range over singletons, it is clear that $\Gamma(S) \leqslant_T \Gamma_+(S)$. Since a Turing oracle for $\Gamma(S)$ gives information not only about elements of $\Gamma(S)$, but also about elements of its complement, the converse follows immediately from Lemma 4.5. □

Proposition 4.7. *If $G \subseteq Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\Gamma_+(G)$ is computably enumerable, then $\Gamma_+(G)$ is computable (and consequently $\Gamma(G)$ is also computable).*

Proof. Suppose we are given an enumeration of $\Gamma_+(G)$. For every $\alpha \in \overline{\mathbb{Q}}$, the listing of $\Gamma_+(G)$ contains exactly one tuple of the form $(\alpha, \beta_1, \dots, \beta_r)$, where $\beta_1, \dots, \beta_r$ are all the possible images of α under G. Therefore, the enumeration of $\Gamma_+(G)$ will eventually list the tuple corresponding to α. Since all elements of $\Gamma_+(G)$ are of the form above, we can effectively answer the question whether any tuple of the form $(\gamma, \delta_1, \dots, \delta_s) \in \Gamma_+(G)$. □

Of course, it is possible that two sets can be Turing equivalent, while one is c.e. and the other is not. For instance, let S be any set which is computably enumerable but not computable. Then $S \equiv_T S^c$, but S^c is not computably enumerable. However, we believe that the relationship between $\Gamma(G)$ and $\Gamma_+(G)$ is a natural example of this phenomenon.

As we show below, $\Gamma_+(G)^c \leqslant_e \Gamma(G)^c$. That is, given an enumeration of the complement of Γ, we can effectively produce an enumeration of the complement of Γ_+. Indeed, let $S \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and let $\bar{x} = (\alpha, \beta_1, \dots, \beta_r) \in \overline{\mathbb{Q}}^{r+1}$. Then, $\bar{x} \notin \Gamma_+(S)$ for one of two reasons. Either some β_i is not a conjugate of α over $\mathbb{Q}$ (and we can effectively determine that) or no element of S sends α to β_i. In the last case, the pair (α, β_i) will appear in the complement of $\Gamma(S)$. So, a listing of the complement of $\Gamma(S)$ will produce a listing of the complement of $\Gamma_+(S)$.

Since, for any S, the graph of S is contained in the set of all finite sequences of elements of $\overline{\mathbb{Q}}$, it follows that the graph of any subset of the absolute Galois group of $\mathbb{Q}$ is countable.

From the discussion in Section 2.4, it follows that the following theorem holds.

Theorem 4.8. *The following conditions on a subset S of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ are equivalent:*

(1) *For each $n \geqslant 1$ there is a computable function $I_n : \overline{\mathbb{Q}}^n \to \mathbb{N} \times \overline{\mathbb{Q}}^{<\omega}$ such that $I_n(\vec{\alpha}) = (m_{\vec{\alpha}}, T_S)$ if and only if T_S is a sequence of length $m_{\vec{\alpha}}$, and is exactly a sequence of images of $\vec{\alpha}$ under elements of S.*
(2) *$\Gamma_+(S)$ is computable.*
(3) *$\Gamma(S)$ is computable.*
(4) *There is a computable function (as described in Section 2.4)*

$$f_S(d,r) := \begin{cases} 1 & \text{if } B_r(d) \cap ({}^\sigma S) \neq \emptyset, \\ 0 & \text{if } B_{2r}(d) \cap ({}^\sigma S) = \emptyset, \\ 0 \text{ or } 1 & \text{otherwise} \end{cases}$$

where
(a) *$d \in \omega^{<\omega}$,*
(b) *r is a rational number, and*
(c) *$B_r(d)$ is the ball of radius r about d in Baire space.*

Remark 4.9. Theorem 4.8 also holds when "computable" is replaced by "computable relative to X" for any $X \subseteq \mathbb{N}$ since the proof relativizes.

We now define computability in the natural way.

Definition 4.10. We say that $S \subseteq \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is computable if and only if it satisfies the equivalent conditions of Theorem 4.8.

Definition 4.11 (Automorphism tree of the absolute Galois group of a field). Let K be a subfield of $\overline{\mathbb{Q}}$. Let $K \subset F_1 \subset \cdots$ be a tower of fields such that $\bigcup_{i=1}^{\infty} F_i = \overline{\mathbb{Q}}$ and F_{i+1}/F_i is finite for all $i \geqslant 1$, and such that the sequence $(F_i : i \in \mathbb{N})$ is uniformly computable in K (see Definition 2.7). Consider a tree of $\text{Gal}(\overline{\mathbb{Q}}/K)$ constructed in the following fashion. Let identity on K be the root of the tree. The level i of the tree will contain all extensions of the identity on K to embeddings of F_i into $\overline{\mathbb{Q}}$, and if τ on level $i+1$ is a child of μ on level i, then μ corresponds to an embedding of F_i into $\overline{\mathbb{Q}}$ and τ is an embedding of F_{i+1} restricting to μ on F_i.

Proposition 4.12. *Every path in the automorphism tree of a field K corresponds to an element of the absolute Galois group of K.*

Proof. Let $\tau_0 = \text{id}, \tau_1, \ldots$ be a path through the automorphism tree of the absolute Galois group of an algebraic field K. By construction τ_i is an embedding of F_i into $\overline{\mathbb{Q}}$ keeping K fixed and τ_i restricts to τ_{i-1} on F_{i-1}. We show that the path defines an automorphism τ of $\overline{\mathbb{Q}}$ fixing K. Let $\alpha \in \overline{\mathbb{Q}}$. Then by construction of $\{F_i : i \in \mathbb{N}\}$, we have that for some j the element $\alpha \in F_j$. Thus, $\tau_k(\alpha)$ for $k \geqslant j$ is defined and $\tau_k(\alpha) = \tau_r(\alpha)$ for any $r, k \geqslant j$. We set $\tau(\alpha) = \tau_j(\alpha)$.

Suppose $\beta \in \overline{\mathbb{Q}}$. Now β has finitely many conjugates over K, and they are all contained in some F_i, where τ_i must permute them. Thus, β is in the range of τ. The function τ is clearly an injective homomorphism and by the argument above it is surjective. Thus, it is an automorphism of $\overline{\mathbb{Q}}$ keeping K fixed. □

Proposition 4.13. *Let G_1, G_2 be two absolute Galois groups (of some fields, but these fields will play no explicit role in the statement or proof). Let $\{\alpha_i : i \in \mathbb{N}\}$ be such that $\mathbb{Q}(\alpha_i) \subset \mathbb{Q}(\alpha_{i+1})$ and $\bigcup_{i\in\omega} \mathbb{Q}(\alpha_i) = \overline{\mathbb{Q}}$. Then, $G_1 \cap G_2 \neq \{id\}$ if and only if there exists a sequence $\bar{\gamma} = \{\gamma_i : i \in \mathbb{N}\} \subset \overline{\mathbb{Q}}$ and a collection $\{T_{\bar{\gamma},i}\} \subset Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ such that*

1. *for all i we have that $\gamma_i \in G_1(\alpha_i) \cap G_2(\alpha_i) \subset \overline{\mathbb{Q}}$,*
2. *for all i, we have $T_{\bar{\gamma},i-1} = \{\tau \in G_1 \cap G_2 : \tau(\alpha_{i-1}) = \gamma_{i-1}\}$,*
3. *for all i we have $\gamma_i \in T_{\bar{\gamma},i-1}(\alpha_i)$, and*
4. *for all but finitely many i we have $\gamma_i \neq \alpha_i$.*

Proof. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\sigma \neq \mathrm{id}$, then there is a greatest i such that $\sigma(\alpha_i) = \alpha_i$. Otherwise, let $\{i_j : j \in \mathbb{N}\}$ be a sequence of indices such that $\sigma(\alpha_{i_j}) = \alpha_{i_j}$. Since $\bigcup\limits_{j\in\mathbb{N}} \mathbb{Q}(\alpha_{i_j}) = \overline{\mathbb{Q}}$, we have that σ does not move any element of $\overline{\mathbb{Q}}$ and therefore is equal to identity.

First, assume there exists $\sigma \in G_1 \cap G_2$ with $\sigma \neq \mathrm{id}$. Then, let $\gamma_i = \sigma(\alpha_i)$. This satisfies the first requirement. By the discussion above $\gamma_i \neq \alpha_i$ for all but finitely many i. So, the sequence $\bar{\gamma}$ satisfies the last requirement. Next, define $T_{\bar{\gamma},i}$ to satisfy the second requirement and observe that by construction of $\bar{\gamma}$ we have that $\sigma \in T_{\bar{\gamma},i-1}$. Therefore, $\gamma_i \in T_{\bar{\gamma},i-1}(\alpha_i)$ satisfying the third requirement.

Conversely, suppose there exists a sequence $\bar{\gamma} \subset \overline{\mathbb{Q}}$ and a collection $\{T_{\bar{\gamma},i}\} \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfying all the requirements above. It is enough to show that there exists an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(\alpha_i) = \gamma_i$, since by Lemma 4.4 such an automorphism $\sigma \in G_1 \cap G_2$. Further, the last requirement on the sequence $\{\gamma_i : i \in \mathbb{N}\}$ implies that $\sigma \neq \mathrm{id}$.

We define the automorphism σ inductively. Let $\sigma_0 = \mathrm{id}$. Assume we have defined $\sigma_{i-1} : \mathbb{Q}(\alpha_{i-1}) \longrightarrow \overline{\mathbb{Q}}$ by setting $\sigma_{i-1}(\alpha_{i-1}) = \gamma_{i-1}$ and let $\sigma_i(\alpha_i) = \gamma_i$. We claim that the sequence $\{\sigma_i : i \in \mathbb{N}\}$ is a path through an automorphism tree of $\mathbb{Q}$, where $F_i = \mathbb{Q}(\alpha_i)$. In other words, we claim that $\sigma_{i|F_{i-1}} = \sigma_{i-1}$.

By assumption there exists $\tau \in G_1 \cap G_2$ such that $\tau(\alpha_{i-1}) = \gamma_{i-1}$ and $\tau(\alpha_i) = \gamma_i$. Therefore, if we set $\sigma_i = \tau_{|\mathbb{Q}(\alpha_i)}$ we can conclude that $\sigma_i : \mathbb{Q}(\alpha_i) \longrightarrow \overline{\mathbb{Q}}$ is an embedding and $\sigma_i|_{\mathbb{Q}(\alpha_{i-1})} = \sigma_{i-1}$. Hence, by the definition of an automorphism tree, we have that $\{\sigma_i : i \in \mathbb{N}\}$ is a path. Thus, by Proposition 4.12 we have that there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(\alpha_i) = \gamma_i$. □

4.2 | Computably enumerable absolute Galois groups

Having defined computable absolute Galois groups, we now proceed to the more difficult situation of computably enumerable absolute Galois groups. In formulating these definitions, we would like to preserve some algorithmic parity between the graph and the strong graph. One difficulty is that while computability of the graph and the strong graph ultimately give the same information, the same is not true for computable enumerability. Indeed, Proposition 4.7, in combination with Lemma 4.6, shows that if the graph is computably enumerable but not computable, then the strong graph is not even computably enumerable and, as we discussed above, the enumeration relation connects the complements of the graph and the strong graph.

Since the connection of enumerability is between the complement of the graph and the complement of the strong graph, we adopt the following definition.

Definition 4.14 (c.e. Galois groups). Let G be an absolute Galois group. Then we say that G is c.e. if the complement of its graph is c.e.

The additional reason for using the complement of the graph, instead of the graph itself, is that to enumerate the field, we would need to know the complement of the graph. Since the focus of this paper is on random fields, and not on random groups, we believe that the correct location of the enumerability is in the fields. One alternative was to require *both* the graph of the group and the field to be computably enumerable, which would collapse enumerability to computability, but does not seem to change many of the results of this paper.

In general, we will refer to an absolute Galois group as having some algorithmic property (enumerability, computability relative to an oracle, etc.) if and only if the complement of its graph has this property.

Observe that if G is computable, then both its graph and its complement are c.e.

Proposition 4.15. *There is a Turing functional which, given the characteristic function of a subfield K of a fixed computable algebraic closure $\overline{\mathbb{Q}}$, will compute the characteristic function of the graph of Gal($\overline{\mathbb{Q}}/K$), and a Turing functional which will, given the characteristic function of the graph of a closed subgroup of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), compute the characteristic function of its fixed field.*

Proof. Using the characteristic function of $\Gamma(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$, we can determine the set of all $x \in \overline{\mathbb{Q}}$ which are fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, that is, the elements of K.

We now show that $\Gamma(\mathrm{Gal}(\overline{\mathbb{Q}}/K)) \leqslant_T K$. Using Lemma 2.12, we determine all the conjugates of x over K: $x = x_1, \dots, x_r$. Then, the pairs (x, x_i) are the only pairs from $\Gamma(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ that have x as its first component. □

Lemma 4.16. *There is a $\emptyset'$-enumeration of the computably enumerable absolute Galois groups.*

Proof. Recall that we identify a group with its graph, and a group is called computably enumerable just in case the complement of its graph is computably enumerable. The oracle $\emptyset'$ can enumerate (indeed, compute) not only the computably enumerable sets, but their complements, as well. There is, then, a $\emptyset'$-enumeration of the co-computably enumerable sets S of pairs (α_i, y) where $\{\alpha_i : i \in \mathbb{N}\}$ are as in Lemma 4.4. In other words, we enumerate the set of co-computably enumerable sets of the right type to be absolute Galois groups.

It remains to sieve the enumeration to list only genuine absolute Galois groups. To this end, using $\emptyset'$, we will check, for each i, whether the images for α_i given are consistent with the images given for α_j with $j < i$. We also check whether the set of partial automorphisms specified by restriction to $\mathbb{Q}(\alpha_i)$ constitutes a group under composition. For each i, there are only finitely many conditions to check. This procedure allows $\emptyset'$ to enumerate the computably enumerable absolute Galois groups, as required. □

5 | RANDOMNESS

5.1 | Defining random fields

In the definition that follows, the Martin–Löf tests are made against closed subgroups. In definitions of random reals, we do not consider any group structure and do not use closed sets. However, here the test should be limited to subgroups that correspond to subfields of $\overline{\mathbb{Q}}$, and these are the closed subgroups.

Definition 5.1. Let μ be the normalized Haar measure.

(1) A μ-test is a uniformly computably enumerable sequence $(S_i : i \in \mathbb{N})$ of closed subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\mu(S_i) < 2^{-i}$.
(2) We say that $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is *random* if for any μ-test $(S_i : i \in \mathbb{N})$ we have $\sigma \notin \bigcap_{i\in\mathbb{N}} S_i$.
(3) We say that an algebraic field is *random* if and only if it is an infinite extension of $\mathbb{Q}$ and its absolute Galois group contains a random element.

We recall that when we describe a uniformly computably enumerable sequence of subgroups, we mean that the sequence of complements of the graphs of those groups is uniformly computable.

Again, the choice of definition is not obvious. We might, from an algebraic perspective, be led to the following alternate definition.

Definition 5.2. Let μ be the normalized Haar measure.

(1) An element of $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is said to be *not Haar random* if it is contained in a computably enumerable subgroup of G of measure 0.
(2) An algebraic field is said to be *Haar random* if and only if it is an infinite extension of $\mathbb{Q}$ and its absolute Galois group contains a Haar random element.

We should note that this definition of Haar randomness is reminiscent of the standard definition of "weak 1-randomness," while the definition of random in the previous definition corresponds more closely with 1-randomness. Weak 1-randomness is a strictly weaker condition on real numbers than 1-randomness. However, this distinction collapses in our context.

Proposition 5.3. *An element $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is Haar random if and only if it is random. Consequently, an algebraic field is Haar random if and only if it is random.*

Proof. Suppose that H is a c.e. group of measure zero containing σ. Then, we may take $S_i = H$ for all $i \in \mathbb{N}$, showing that σ is not random. Suppose now that σ is not random but is Haar random. Then, there exists a sequence of c.e. absolute Galois groups such that $\mu(G_i) < 2^{-i}$ and $\sigma \in \bigcap_{i\in\mathbb{N}} G_i$. If $\mu(G_i) = 0$, for some i, then σ is not Haar random and we have a contradiction.

Assume now that the measures of all groups are positive. Let $H = \bigcap_{i\in\mathbb{N}} G_i$. Then, $\mu(H) = 0$, and the complement of $\Gamma(H)$ is the union of the complements of the $\Gamma(G_i)$. We want to show that H is c.e. (i.e., that the complement of the graph of H is c.e.) to obtain a contradiction. Note that, since the definition of a μ-test required a uniform sequence (i.e., a uniform enumeration of the complements of the $\Gamma(G_i)$), we know that the sequence $(\Gamma(G_i)^c : i \in \mathbb{N})$ is uniformly computably enumerable. It follows that the union of this sequence is computably enumerable, and H is computably enumerable. □

5.2 | Properties of random fields

The following property is related to the concept of an immune set.

Proposition 5.4. *Let K be an infinite extension of $\mathbb{Q}$. If K contains an c.e. subfield of infinite degree, then K is not random.*

Proof. Let K^- be an infinite degree c.e. field contained in K. Then, $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/K^-)$, while $\mathrm{Gal}(\overline{\mathbb{Q}}/K^-)$ is c.e. and of measure zero. □

It would be tempting to think that this means that random fields are immune. However, they do include the infinite c.e. set of rationals. We could, however, define another property related to immunity, that a field contain no c.e. subfield of infinite degree.

Lemma 5.5. *Let $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then, σ is random if and only if the fixed field of σ is of infinite degree and contains no c.e. subfields.*

Proof. If the fixed field of σ contains an infinite degree c.e. field K, then $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is of measure 0 and c.e. Further, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Thus, σ is not random. Conversely, suppose the fixed field of σ does not contain any c.e. subfields, but σ is not random. Then, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for some c.e. infinite degree field K and we have a contradiction. □

Corollary 5.6. *Let G be a closed subgroup of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$; that is, G is a Galois group of some field. Then G is not random if and only if the fixed field of every non-trivial element of G contains a c.e. field.*

Corollary 5.7. *For any Turing degree* **d** *there is a field of degree* **d** *which is not random.*

Proof. Let F_0 be generated over the rationals by the 2^qth roots of 2 (where q ranges over all natural numbers), and $X \in \mathbf{d}$. Note that F_0 is computably enumerable. Let $(p_i : i \in \mathbb{N})$ be the rational primes. We can then build an algebraic extension $F_{\mathbf{d}}$ of F_0 which includes $\sqrt[(p_{2i+1})]{p_{2i+1}}$ if and only if $i \in X$ and $\sqrt[(p_{2i+2})]{p_{2i+2}}$ if and only if $i \notin X$. Now $F_{\mathbf{d}}$ will have degree **d** and will contain a computably enumerable infinite extension F_0 of $\mathbb{Q}$. □

Corollary 5.8. *There is an algebraic field of infinite degree which is not random.*

Proof. By Corollary 5.6, any computably enumerable algebraic field of infinite degree will suffice. □

To prove the existence of random elements in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we need the following lemmas.

Lemma 5.9. *Let L be a subfield of $\overline{\mathbb{Q}}$ and $x \in \overline{\mathbb{Q}} \setminus L$. Let σ be an embedding of L into $\overline{\mathbb{Q}}$. Then, there is an extension of σ to $L(x)$ such that $\sigma(x) \neq x$.*

Proof. Let $P(T)$ be the monic irreducible polynomial of x over L. Then $\deg P(T) \geqslant 2$. If $\sigma(P) = P$, then we can set $\sigma(x)$ to be any root of $P(T)$ not equal to x. If $\sigma(P) \neq P$, then we can set $\sigma(x)$ to be any root of $\sigma(P)$. □

Lemma 5.10. *Let L be a finitely generated extension of $\mathbb{Q}$. Let σ be an embedding of L into $\overline{\mathbb{Q}}$. Then, there exists infinitely many $x \in \overline{\mathbb{Q}} \setminus L$ such that σ can be extended to $L(x)$ by setting $\sigma(x) = x$.*

Proof. Without loss of generality, assume that L is Galois over $\mathbb{Q}$ so that every irreducible polynomial over $\mathbb{Q}$ either remains prime over L or splits completely. Then, all polynomials irreducible over $\mathbb{Q}$ of degree prime to $[L : \mathbb{Q}]$ will remain prime over L. Let $x \in \overline{\mathbb{Q}}$ be such that its monic irreducible polynomial over $\mathbb{Q}$ remains prime over L. Then, $\mathbb{Q}(x)$ and L are linearly disjoint over $\mathbb{Q}$. If $\alpha \in \overline{\mathbb{Q}}$ is such that $L = \mathbb{Q}(\alpha)$ then the monic irreducible polynomials of α over $\mathbb{Q}$ and $\mathbb{Q}(x)$ are the same. Therefore, there exists an embedding τ of $L(x)$ into $\overline{\mathbb{Q}}$ such that τ is the identity on $\mathbb{Q}(x)$ and $\tau(\alpha) = \sigma(\alpha)$. □

Proposition 5.11 (Existence of random elements). *There exist a continuum of random elements $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.*

Proof. Let $\{K_i : i \in \mathbb{N}\}$ be an enumeration (perhaps not computable) of all infinite degree c.e. subfields of $\overline{\mathbb{Q}}$.

Stage 1: Pick an element $x_1 \in K_1 - \mathbb{Q}$. Define $\sigma(x_1) = y_1$, where $y_1 \neq x_1$ is a conjugate of x_1 over $\mathbb{Q}$. Set L_1 to be the Galois closure over $\mathbb{Q}$ of $\mathbb{Q}(x_1)$, and extend σ to L_1 in the natural way.

Stage 2: Pick an element $x_2 \notin L_1$ such that L_1 is linearly disjoint from $\mathbb{Q}(x_2)$ over $\mathbb{Q}$ and set $\sigma(x_2) = x_2$. (Such an x_2 exists by Lemma 5.10.) Set L_2 to be the Galois closure of $\mathbb{Q}(x_1, x_2)$ over $\mathbb{Q}$, and extend σ to L_2 in the natural way.

Stage $2n + 1$: Let K_m be an infinite degree c.e. field with the smallest index that has not appeared in the construction so far. Assume inductively that σ is defined for elements of $L_{2n} = \mathbb{Q}(x_1, \ldots, x_{2n})$. Find an element $x_{2n+1} \in K_m - L_{2n}$. This can always be done because K_m is not finitely generated. By Lemma 5.9 there is an extension of σ to $L_{2n}(x_{2n+1})$ such that $\sigma(x_{2n+1}) \neq x_{2n+1}$. Set L_{2n+1} to be the Galois closure of $L_{2n}(x_{2n+1})$ over $\mathbb{Q}$, extending σ to L_{2n+1} as before.

Stage $2n + 2$: Pick an element $x_{2n+2} \in \overline{\mathbb{Q}} - L_{2n+1}$ so that there is an extension of σ to $L_{2n+1}(x_{2n+2})$ such that $\sigma(x_{2n+2}) = x_{2n+2}$. (We can find such an element by Lemma 5.10.) Set L_{2n+2} to be the Galois closure of $L_{2n+1}(x_{n+2})$ over $\mathbb{Q}$, extending σ to L_{2n+2} as before.

Now, we have σ defined on $\bigcup_{n=1}^{\infty} L_n$. If $\bigcup_{n=1}^{\infty} L_n \neq \overline{\mathbb{Q}}$, then extend σ to $\overline{\mathbb{Q}}$.

In the even stages, we have arranged that σ fixes an infinite extension of $\mathbb{Q}$, while in the odd stages we have arranged that σ does not fix any infinite degree c.e. field, so σ is random. Moreover, at each stage s of the construction, we had infinitely many options for the choice of x_s—indeed, there are infinitely many options for x_s each of which leads to a different field L_s—so the total number of random automorphisms that can be constructed in this way is $2^{\aleph_0}$. □

Remark 5.12. Naturally, if σ is random, then σ^{-1} must be random as well since they both have the same fixed field. However, $\sigma \circ \sigma^{-1}$ is clearly not random, so the set of random automorphisms is not closed under composition.

Corollary 5.13. *There exists a random field.*

Proof. Let σ be a random element as constructed in the proof of Proposition 5.11. Observe that, by construction, the fixed field of σ is of infinite degree over $\mathbb{Q}$. Then let $G = \langle \sigma \rangle$ and F be the fixed field of G. Now the absolute Galois group of F will contain G, and so it will contain a random element. □

The following result is immediate from examining the technique of proof of Proposition 5.11.

Corollary 5.14. *There are $2^{\aleph_0}$ distinct random fields in $\overline{\mathbb{Q}}$.*

Corollary 5.15. *Let $F_1, \dots, F_k$ be random fields. Then*

(1) *If J is an infinite extension of $\mathbb{Q}$ and $J \subseteq F_1$, then J is random.*

(2) *If $F = \bigcap_{i=1}^{k} F_i$ is an infinite extension of $\mathbb{Q}$, then F is random.*

Proof. Item 1 is immediate from the definition of a random field, since the absolute Galois group of J contains that of F_1. Then, Item 2 follows from Item 1. □

5.2.1 | Does there exist a "super random" group?

One natural question one could ask is whether there exists a "super random" absolute Galois group, that is, the group where every non-trivial element is random. The fixed field of such a group would have no extension containing an infinite degree c.e. subfield. Existence of such a "super random" field corresponds to the existence of a subset $X \subset \mathbb{N}$ such that for any co-infinite superset $S \supseteq X$ we have that S contains no infinite c.e. subset. Unfortunately, as is shown by the argument in Lemma 2.5 such a set X does not exist. We summarize this finding in the following proposition.

Proposition 5.16. *Every random absolute Galois group contains a non-random non-trivial element. Equivalently, every random field is contained in a non-random field not equal to the algebraic closure.*

6 | THE SET OF INDICES FOR RANDOM FIELDS

The usual representation of a field in effective structure theory regards the field as having universe $\mathbb{N}$, and then identifies the field with its atomic diagram; that is, with the set of polynomial equations and inequations of elements true in that field. In particular, if the field is computable, or even computably enumerable, it may be identified by the index of a Turing machine the range of which is that atomic diagram.

A common way to calibrate the complexity of a class of structures is to determine the Turing degree of the set of indices of its members [7–10]. Suppose now that we fix an oracle of Turing degree $\mathbf{d}$. In this section, we attempt to calculate the Turing degree of the set of $\mathbf{d}$-indices for $\mathbf{d}$-computable random fields. Of course, if $\mathbf{d} = \mathbf{0}$, there are none. On the other hand, for other $\mathbf{d}$, the problem becomes nontrivial.

Proposition 6.1. *Let $X \subseteq \mathbb{N}$. The set of indices for X-computably enumerable subfields of $\overline{\mathbb{Q}}$ with infinite degree is m-complete $\Pi^0_2(X)$. Moreover, the same result holds when the language is expanded to include constant symbols for generators for the field over $\mathbb{Q}$.*

Proof. We give a uniform proof, but omit the notation of X. To show that the set of indices for infinite degree fields is Π^0_2, we will write a computable infinitary formula (see Section 2.1) which is true exactly in infinite degree fields. By a standard result of Ash (see [4]), this will show that the set of indices must be Π^0_2.

We first let I_n denote the (decidable [17]) set of irreducible polynomials over $\mathbb{Q}$ of degree strictly greater than n, and notice that the following collection of subfields $F \subset \overline{\mathbb{Q}}$ is exactly the set of infinite algebraic extensions of $\mathbb{Q}$.

$$\left\{ F \mid \bigwedge_{n\in\mathbb{N}} \left(\exists \alpha \in F \bigvee_{p \in I_n} p(\alpha) = 0 \right) \right\}.$$

Toward completeness, we note that the set of indices for infinite computably enumerable sets is m-complete Π^0_2 (see, for instance, Theorem 4.3.2 of [29]). To show that the set of indices for infinite extensions of $\mathbb{Q}$ is m-complete Π^0_2 it suffices to give a computable function f such that $f(e)$ is the index for an infinite extension of $\mathbb{Q}$ if and only if e is the index of an infinite c.e. set.

It suffices, then, to give a uniformly computable sequence of fields $(F_e : e \in \mathbb{N})$ such that F_e is an infinite extension of $\mathbb{Q}$ if and only if W_e is infinite. We let $(K_i : i \in \mathbb{N})$ be a uniformly computable sequence of fields (given by their atomic diagrams) with

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq \overline{\mathbb{Q}},$$

where $\overline{\mathbb{Q}} = \bigcup_{i\in\mathbb{N}} K_i$, and K_{i+1} is a finite extension of K_i. We note that for any i, the field K_i contains all K_j for $j < i$, so that any union, finite or infinite, of these fields will still be a field.

Now, to each computably enumerable set W_e we associate the subfield $F_e = \bigcup_{i \in W_e} K_i$. The result follows, since every infinite c.e. set W_e will give $F_e = \overline{\mathbb{Q}}$, and every finite c.e. set W_e will give a finite extension $F_e \supseteq \mathbb{Q}$. Effectively recovering the indices of Turing machines for the fields F_e, we have the desired function f on Turing machine indices. □

Corollary 6.2. *A set X'' can generate a listing of all X-computably enumerable absolute Galois groups of measure zero via their graphs.*

Proof. By Proposition 4.15, fields are uniformly Turing equivalent to the graphs of their absolute Galois groups. The corollary, then, is equivalent to enumerating the X-computably enumerable infinite extension fields of $\mathbb{Q}$. By the previous proposition, this set is $\Pi^0_2(X)$. Such a set is certainly enumerable from X''. □

Proposition 6.3. *Let G_c be a computably enumerable absolute Galois group. Let G be an arbitrary absolute Galois group. Then, $\Gamma(G)''$ can determine whether $G_c \cap G$ is trivial.*

Proof. By Corollary 4.13, it suffices to check whether, for each i there is some $j > i$ for which there exists a nontrivial element of $\Gamma(G_c)(\alpha_j) \cap \Gamma(G)(\alpha_j)$. This can be done in the second jump of $\Gamma(G)$, since G_c is computably enumerable. □

Corollary 6.4. *Let G be as above. Then, $\Gamma(G)'''$ can determine whether G is random.*

Proof. By Lemma 4.16, we can enumerate the computably enumerable subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ under $\emptyset'$. Then for each of these groups we will perform the computation of Proposition 6.3. The final judgment on the randomness of G is determined by whether, for every group enumerated, we have an empty intersection, each of which can be done by $\Gamma(G)''$, so that the full computation can be completed under $\Gamma(G)'''$, as required. □

ACKNOWLEDGMENTS

This material is partially based upon work supported by the National Science Foundation under grant DMS-1928930 while all three authors participated in a program hosted by the Mathematical Sciences Research Institute in Berkeley, California during Fall 2020 and Summer 2022. The first author was partially supported by a Fulbright-Nehru Senior Research Fellowship. The second author was partially supported by NSF FRG grant DMS-2152095. The third author was partially supported by NSF FRG grant DMS-2152098. The authors are grateful to Philip Dittmann for helpful comments, and to the anonymous referees for a very careful reading.

JOURNAL INFORMATION

The *Journal of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Wesley Calvert https://orcid.org/0000-0002-1355-2694

REFERENCES

1. N. Ackerman, C. Freer, A. Kwiatkowska, and R. Patel, *A classification of orbits admitting a unique invariant measure*, Ann. Pure Appl. Logic **168** (2017), 19–36.
2. N. Ackerman, C. Freer, and R. Patel, *Invariant measures concentrated on countable structures*, Forum Math. Sigma **4** (2016), e17.
3. N. Ackerman, C. Freer, and R. Patel, *The entropy function of an invariant measure*, Proceedings of the 14th and 15th Asian Logic Conferences, World Scientific Publishing, 2019, pp. 3–34.
4. C. J. Ash and J. Knight, *Computable structures and the hyperarithmetical Hierarchy*, North-Holland, 2000.
5. L. Bienvenu and W. Merkle, *Effective randomness for computable probability measures*, Electron. Notes Theor. Comput. Sci. **167** (2007), 117–130.
6. B. Bollobás, *Random graphs*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 73, Cambridge University Press, 2001.
7. W. Calvert, *The isomorphism problem for classes of computable fields*, Arch. Math. Logic **43** (2004), 327–336.
8. W. Calvert, *The isomorphism problem for computable Abelian p-groups of bounded length*, J. Symb. Log. **70** (2005), 331–345.
9. W. Calvert, E. Fokina, S. S. Goncharov, J. F. Knight, O. Kudinov, A. S. Morozov, and V. Puzarenko, *Index sets for classes of high rank structures*, J. Symb. Log. **72** (2007), 1418–1432.
10. W. Calvert, V. S. Harizanov, J. F. Knight, and S. Miller, *Index sets of computable structures*, Algebra Logic. **45** (2006), 306–325.
11. M. Cordes, M. Duchin, Y. Duong, M.-C. Ho, and A. P. Sánchez, *Random nilpotent groups I*, Int. Math. Res. Not. IMRN **7** (2018), 1921–1953.
12. P. Erdős and A. Rényi, *On random graphs I*, Publ. Math. Debrecen **6** (1959), 290–297.

13. P. Erdős and A. Rényi, *On the evolution of random graphs*, Magyar Tudományos Akadémi. Matematikai Kutató Intézetémek Közelményei **A** (1960), 17–60.
14. E. B. Fokina, V. Harizanov, and A. Melnikov, *Computable model theory*, Turing's Legacy: Developments from Turing's Ideas in Logic, Lecture Notes in Logic, vol. 42, Cambridge University Press/Association for Symbolic Logic, 2014, pp. 124–194.
15. W. L. Fouché, *Martin–Löf randomness, invariant measures and countable homogeneous structures*, Theory Comput. Syst. **52** (2013), 65–79.
16. J. N. Y. Franklin, M.-C. Ho, and J. F. Knight, *Free structures and limiting density*, 2022, in press.
17. M. D. Fried and M. Jarden, *Field arithmetic*, 2nd ed. Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 11, Springer, 2005.
18. A. Fröhlich and J. C. Shepherdson, *Effective procedures in field theory*, Philos. Trans. Roy. Soc. Lond. Ser. A **248** (1956), 407–432.
19. E. Glasner and B. Wiess, *Minimal actions of the group $\mathbb{S}(\mathbb{Z})$ of permutations of the integers*, Geom. Funct. Anal. **12** (2002), 964–988.
20. M. Gromov, *Random walk in random groups*, Geom. Funct. Anal. **13** (2003), 73–146.
21. M. Harrison-Trainor, B. Khoussainov, and D. Turetsky, *Effective aspects of algorithmically random structures*, Computability **8** (2019), 359–375.
22. B. Khoussainov, *A quest for algorithmically random infinite structures*, Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), ACM, 2014, 56.
23. B. Khoussainov, *A quest for algorithmically random infinite structures, II*, Logical Foundations of Computer Science, Lecture Notes in Computer Science, vol. 9537, Springer, 2016, pp. 159–173.
24. A. Pauly, D. Seon, and M. Ziegler, *Computing Haar measures*, 28th EACSL Annual Conference on Computer Science Logic, Schloss Dagstuhl—Leibniz Center for Informatics, 2020, pp. 34:1–34:17.
25. M. S. Pinsker, *On the complexity of a concentrator*, 7th International Teletraffic Conference, 1973, pp. 318/1–318/4.
26. M. O. Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.
27. J. Reimann, *Randomness —beyond Lebesgue measure*, Logic Colloquium 2006, Lecture Notes in Logic, Association for Symbolic Logic, 2009, pp. 247–279.
28. H. L. Royden, *Real analysis*, 2nd ed., Macmillan, 1968.
29. R. I. Soare, *Turing Computability*, Springer, 2016.
30. R. Weber, *Computability theory*, The Student Mathematical Library, American Mathematical Society, 2012.
31. K. Weihrauch, *Computable analysis*, Texts in Theoretical Computer Science, Springer, 2000.