Random Subgroups of Rationals

Ziyuan Gao
Department of Mathematics, National University of Singapore, Singapore
matgaoz@nus.edu.sg

Sanjay Jain
School of Computing, National University of Singapore, Singapore
sanjay@comp.nus.edu.sg

Bakhadyr Khoussainov
Department of Computer Science, University of Auckland, New Zealand
bmk@cs.auckland.ac.nz

Wei Li
Department of Mathematics, National University of Singapore, Singapore
matliw@nus.edu.sg

Alexander Melnikov
Institute of Natural and Mathematical Sciences, Massey University, New Zealand
A.Melnikov@massey.ac.nz

Karen Seidel
Hasso Plattner Institute, University of Potsdam, Germany
karen.seidel@hpi.uni-potsdam.de

Frank Stephan
Department of Mathematics, National University of Singapore, Singapore
fstephan@comp.nus.edu.sg

Abstract

This paper introduces and studies a notion of *algorithmic randomness* for subgroups of rationals. Given a randomly generated additive subgroup $(G, +)$ of rationals, two main questions are addressed: first, what are the model-theoretic and recursion-theoretic properties of $(G, +)$; second, what learnability properties can one extract from G and its subclass of finitely generated subgroups? For the first question, it is shown that the theory of $(G, +)$ coincides with that of the additive group of integers and is therefore decidable; furthermore, while the word problem for G with respect to any generating sequence for G is not even semi-decidable, one can build a generating sequence β such that the word problem for G with respect to β is co-recursively enumerable (assuming that the set of generators of G is limit-recursive). In regard to the second question, it is proven that there is a generating sequence β for G such that every non-trivial finitely generated subgroup of G is recursively enumerable and the class of all such subgroups of G is behaviourally correctly learnable, that is, every non-trivial finitely generated subgroup can be semantically identified in the limit (again assuming that the set of generators of G is limit-recursive). On the other hand, the class of non-trivial finitely generated subgroups of G cannot be syntactically identified in the limit with respect to any generating sequence for G. The present work thus contributes to a recent line of research studying algorithmically random infinite structures and uncovers an interesting connection between the arithmetical complexity of the set of generators of a randomly generated subgroup of rationals and the learnability of its finitely generated subgroups.

2012 ACM Subject Classification Theory of computation → Pseudorandomness and derandomization; Theory of computation → Inductive inference

Keywords and phrases Martin-Löf randomness, subgroups of rationals, finitely generated subgroups of rationals, learning in the limit, behaviourally correct learning

Digital Object Identifier 10.4230/LIPIcs.MFCS.2019.25

44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019).
Editors: Peter Rossmanith, Pinar Heggernes, and Joost-Pieter Katoen; Article No. 25; pp. 25:1–25:14
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Related Version A full version of the paper is available at `https://hal.archives-ouvertes.fr/hal-01970683v2/document`

Funding Sanjay Jain was supported in part by NUS grant C252-000-087-001. Furthermore, Ziyuan Gao, Sanjay Jain and Frank Stephan have been supported in part by the Singapore Ministry of Education Academic Research Fund Tier 2 grant MOE2016-T2-1-019 / R146-000-234-112. Bakhadyr Khoussainov was supported by the Marsden fund of Royal Society of New Zealand. Karen Seidel was supported by the German Research Foundation (DFG) under Grant KO 4635/1-1 (SCL) and by the Marsden fund of Royal Society of New Zealand.

Acknowledgements The authors would like to thank Philipp Schlicht and Tin Lok Wong for helpful discussions, as well as thank Timo Kötzing for pointers to the literature.

1 Introduction

The concept of *algorithmic randomness*, particularly for strings and infinite sequences, has been extensively studied in recursion theory and theoretical computer science [6, 15, 19]. It has also been applied in a wide variety of disciplines, including formal language and automata theory [14], machine learning [29], and recently even quantum theory [20]. An interesting and long open question is whether the well-established notions of randomness for infinite sequences have analogues for infinite structures such as graphs and groups. Intuitively, it might be reasonable to expect that a collection of random infinite structures possesses the following characteristics: (1) randomness should be an isomorphism invariant property; in particular, random structures should not be computable; (2) the collection of random structures (of any type of algebraic structure) should have cardinality equal to that of the continuum. The standard random infinite graph thus does not qualify as an algorithmically random structure; in particular, it is isomorphic to a computable graph and has a countable categorical theory. Very recently, Khoussainov [12, 13] defined algorithmic randomness for infinite structures that are akin to graphs, trees and finitely generated structures.

This paper addresses the following three open questions in algorithmic randomness: (A) is there a reasonable way to define algorithmically random structures for standard algebraic structures such as groups; (B) can one define algorithmic randomness for groups that are not necessarily finitely generated; (C) what are the model-theoretic properties of algorithmically random structures? The main contribution of the present paper is to answer the first two questions positively for a fundamental and familiar algebraic structure, the *additive group of rationals*, denoted $(\mathbb{Q}, +)$, and to answer the third question with respect to this structure. Prior to this work, question (A) was answered for structures such as *finitely generated* universal algebras, connected graphs, trees of bounded degree and monoids [12]. Concerning question (C), it is still unknown whether the first order theory of algorithmically random graphs (or trees) is decidable. In fact, it is not even known whether any two algorithmically random graphs (of the same bounded degree) are elementarily equivalent [12].

As mentioned earlier, one goal of this work is to formulate a notion of randomness for subgroups of $(\mathbb{Q}, +)$. This is a fairly natural class of groups to consider, given that the isomorphism types of its subgroups have been completely classified, as opposed to the current limited state of knowledge about the isomorphism types of even rank 2 groups. As has been known since the work of Baer [1], the subgroups of $(\mathbb{Q}, +)$ coincide, up to isomorphism, with the torsion-free Abelian groups of rank 1. Moreover, the group $(\mathbb{Q}, +)$ is robust enough that it has uncountably many algorithmically random subgroups (according to our definition of algorithmically random subgroups of $(\mathbb{Q}, +)$), which contrasts with the fact that there is a unique standard random graph up to isomorphism. At the same time, the algorithmically random subgroups of $(\mathbb{Q},+)$ are not too different from one other in the sense that they are all elementarily equivalent (a fact that will be proven later), which is similar to the case of standard random graphs being elementarily equivalent.

The properties of the subgroups of $(\mathbb{Q},+)$ were first systematically studied by Baer [1] and then later by Beaumont and Zuckerman [3]. Later, the group $(\mathbb{Q},+)$ was studied in the context of automatic structures [28]. An early definition of a random group is due to Gromov [10]. According to this definition, random groups are those obtained by first fixing a set of generators, and then randomly choosing (according to some probability distribution) the relators specifying the quotient group. An alternative definition of a general random infinite structure was proposed by Khoussainov [12, 13]; this definition is based on the notion of a *branching class*, which is in turn used to define Martin-Löf tests for infinite structures entirely in analogy to the definition of a Martin-Löf test for sequences. An infinite structure is then said to be Martin-Löf random if it passes every Martin-Löf test in the preceding sense.

Like Gromov's definition of a random group, the one adopted in the present work is syntactic, in contrast to the semantic and algebraic definition due to Khoussainov. However, rather than selecting the relators at random according to a prescribed probability distribution for a fixed set of generators, our approach is to directly encode a Martin-Löf random binary sequence into the generators of the subgroup. More specifically, we fix any binary sequence R, and define the group G_R as that generated by all rationals of the shape $p_i^{-n_i}$, where p_i denotes the $(i+1)$-st prime and n_i is the number of ones occurring between the i-th and $(i+1)$-st occurrences of zero in R; n_0 is the number of starting ones, and if there is no $(i+1)$-st zero then n_j is defined to be zero for all j greater than i and G_R is generated by all $p_{i'}^{-n_{i'}}$ with i' less than i and all $p_i^{-n'}$ such that n' is any positive integer. G_R is then said to be *randomly generated* if and only if R is Martin-Löf random. In order to derive certain computability properties, it will always be assumed in the present paper that any Martin-Löf random sequence associated to a randomly generated subgroup of $(\mathbb{Q},+)$ is also limit-recursive. It may be observed that no finitely generated subgroup of $(\mathbb{Q},+)$ is randomly generated in the sense adopted here; this corresponds to the intuition that in any "random" infinite binary sequence R, the fraction of zeroes in the first n bits should tend to a number strictly smaller than one as n grows to infinity.

The first main part of this work is devoted to the study of the model-theoretic and recursion-theoretic properties of randomly generated subgroups of $(\mathbb{Q},+)$. It is shown that the theory of any randomly generated subgroup coincides with that of the integers with addition (denoted $(\mathbb{Z},+)$), and is therefore decidable[1]. Next, we define the notion of a *generating sequence* for a randomly generated group G_R; this is an infinite sequence β such that G_R is generated by the terms of β. We then consider the word problem for G_R with respect to β: this is the problem of determining, given any two finite integer sequence representations σ and τ of elements of G_R with respect to β, whether or not σ and τ represent the same element of G_R. We show that the word problem for G_R with respect to *any* generating sequence β is never recursively enumerable (r.e.); on the other hand, one can construct a generating sequence β' for G_R such that the corresponding word problem for G_R is co-r.e. Moreover, one can build a generating sequence β'' for G_R such that the word problem for the quotient group of G_R by $\mathbb{Z}$ with respect to β'' is r.e.

The second main part of this paper investigates the learnability of non-trivial finitely generated subgroups of randomly generated subgroups of $(\mathbb{Q},+)$ from positive examples, also

[1] For a proof of the decidability of the theory of $(\mathbb{Z},+)$, often known as *Presburger Arithmetic*, see [16, pages 81–84].

known as learning from text. Stephan and Ventsov [25] examined the learnability of classes of substructures of algebraic structures; the study of more general classes of structures was undertaken in the work of Martin and Osherson [17, Chapter III]. The general objective is to understand how semantic knowledge of a class of concepts can be exploited to learn the class; in the context of the present problem, semantic knowledge refers to the properties of every finitely generated subgroup of any randomly generated subgroup of rationals, such as being generated by a single rational [1]. It may be noted that the present work considers learning of the actual representations of finitely generated subgroups, as opposed to learning their structures up to isomorphism, as is considered in the learning framework of Martin and Osherson [17]. Various positive learnability results are obtained: it will be proven, for example, that for any randomly generated subgroup G_R of $(\mathbb{Q},+)$, there is a generating sequence β for G_R such that the set of representations of every non-trivial finitely generated subgroup of G_R with respect to β is r.e.; furthermore, the class of all such representations can be identified in the limit up to semantic equivalence. On the other hand, it will be seen that the class of all such representations can never be learnable in the limit. Similar results hold for the class of non-trivial finitely generated subgroups of the quotient group of G_R by $\mathbb{Z}$. Thus this facet of our work implies a connection between the limit-recursiveness of the set of generators of a randomly generated subgroup of $(\mathbb{Q},+)$ and the learnability of its non-trivial finitely generated subgroups.

2 Preliminaries

Any unexplained recursion-theoretic notation may be found in [22, 24, 21]. For background on algorithmic randomness, we refer the reader to [6, 19]. We use $\mathbb{N} = \{0, 1, 2, \ldots\}$ to denote the set of all natural numbers and $\mathbb{Z}$ to denote the set of all integers. The $(i+1)$-st prime will be denoted by p_i. $\mathbb{Z}^{<\omega}$ denotes the set of all finite sequences of integers. Throughout this paper, $\varphi_0, \varphi_1, \varphi_2, \ldots$ is a fixed acceptable programming system of all partial recursive functions and $W_0, W_1, W_2, \ldots$ is a fixed *acceptable numbering of all recursively enumerable* (abbr. r.e.) *sets* of natural numbers. We will occasionally work with objects belonging to some countable class X different from $\mathbb{N}$; in such a case, by abuse of notation, we will use the same symbol W_e to denote the set of objects obtained from W_e by replacing each member x with $F(x)$ for some fixed bijection F between $\mathbb{N}$ and X.

Given any set S, S^* denotes the set of all finite sequences of elements from S. By $D_0, D_1, D_2, \ldots$ we denote any fixed *canonical indexing of all finite sets* of natural numbers. Cantor's pairing function $\langle \cdot, \cdot \rangle \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is given by $\langle x, y \rangle = \frac{1}{2}(x+y)(x+y+1) + y$ for all $x, y \in \mathbb{N}$. The symbol K denotes the *diagonal halting problem*, i.e., $K = \{e \mid e \in \mathbb{N},\ \varphi_e(e) \text{ converges}\}$. The *jump* of K, that is, the relativised halting problem $\{e \mid e \in \mathbb{N}; \varphi_e^K(e)\downarrow\}$, will be denoted by K'.

For $\sigma \in (\mathbb{N} \cup \{\#\})^*$ and $n \in \mathbb{N}$ we write $\sigma(n)$ to denote the element in the n-th position of σ. Further, $\sigma[n]$ denotes the sequence $\sigma(0), \sigma(1), \ldots, \sigma(n-1)$. Given a number $a \in \mathbb{N}$ and some fixed $n \in \mathbb{N}$, $n \geq 1$, we denote by a^n the finite sequence $a, \ldots, a$, where a occurs exactly n times. Moreover, we identify a^0 with the empty string ε. For any finite sequence σ we use $|\sigma|$ to denote the length of σ. The concatenation of two sequences σ and τ is denoted by $\sigma \circ \tau$; for convenience, and whenever there is no possibility of confusion, this is occasionally denoted by $\sigma\tau$. For any sequence β (infinite or otherwise) and $s < |\beta|$, $\beta\restriction_s$ denotes the initial segment of β of length $s+1$. For any $m \geq 1$ and $p \in \mathbb{Z}$, $I_m(p)$ denotes the vector of length m whose first $m-1$ coordinates are 0 and whose last coordinate is p. Furthermore, given two vectors $\alpha = (a_i)_{0 \leq i \leq m}$ and $\beta = (b_i)_{0 \leq i \leq m}$ of equal length, $\alpha \cdot \beta$ denotes the scalar product of α and β, that is, $\alpha \cdot \beta := \sum_{i=0}^{m} a_i b_i$. For any $c \in \mathbb{Z}$ and $\sigma := (b_i)_{0 \leq i \leq m} \in \mathbb{Z}^{<\omega}$, $c\sigma$ denotes the vector obtained from σ by coordinatewise multiplication with c, that is, $c\sigma := (cb_0, cb_1, \ldots, cb_m)$. For any non-empty $S \subseteq \mathbb{Q}$, $\langle S \rangle$ denotes $\{\sum_{i=0}^{k} c_i s_i \mid k \in \mathbb{N} \wedge c_i \in \mathbb{Z} \wedge s_i \in S\}$.

Cantor space, the set of all infinite binary sequences, will be denoted by 2^ω. The set of finite binary strings will be denoted by $2^{<\omega}$. For any binary string σ, $[\sigma]$ denotes the cylinder generated by σ, that is, the set of infinite binary sequences with prefix σ. For any $U \subseteq 2^{<\omega}$, the open set generated by U is $[U] := \bigcup_{\sigma \in U}[\sigma]$. The Lebesgue measure on 2^ω will be denoted by λ; that is, for any binary string σ, $\lambda([\sigma]) = 2^{-|\sigma|}$. By the Carathéodory Theorem, this uniquely determines the Lebesgue measure on the Cantor space.

3 Randomly Generated Subgroups of Rationals

We first review some basic definitions and facts in algorithmic randomness which in our setting is always understood w.r.t the Lebesgue measure. An *r.e. open set* R is an open set generated by an r.e. set of binary strings. Regarding W_e as a subset of $2^{<\omega}$, one has an enumeration $[W_0], [W_1], [W_2], \ldots$ of all r.e. open sets. A *uniformly r.e. sequence* $(G_m)_{m<\omega}$ *of open sets* is given by a recursive function f such that $G_m = [W_{f(m)}]$ for each m. As infinite binary sequences may be viewed as characteristic functions of subsets of $\mathbb{N}$, we will often use the term "set" interchangeably with "infinite binary sequence"; in particular, the subsequent definitions apply equally to subsets of $\mathbb{N}$ and infinite binary sequences.

Martin-Löf [18] defined randomness based on tests. A *Martin-Löf test* is a uniformly r.e. sequence $(G_m)_{m<\omega}$ of open sets such that $(\forall m < \omega)[\lambda(G_m) \leq 2^{-m}]$. A set $Z \subseteq \mathbb{N}$ *fails* the test if $Z \in \bigcap_{m<\omega} G_m$; otherwise Z *passes* the test. Z is *Martin-Löf random* if Z passes each Martin-Löf test. Schnorr [23] showed that Martin-Löf random sets can be described via martingales. A *martingale* is a function $\mathrm{mg} : 2^{<\omega} \to \mathbb{R}^+ \cup \{0\}$ that satisfies for every $\sigma \in 2^{<\omega}$ the equality $\mathrm{mg}(\sigma \circ 0) + \mathrm{mg}(\sigma \circ 1) = 2\mathrm{mg}(\sigma)$. For a martingale mg and a set Z, the martingale mg *succeeds* on Z if $\sup_n \mathrm{mg}(Z(0)\ldots Z(n)) = \infty$.

▶ **Theorem 1.** *[23] For any set Z, Z is Martin-Löf random iff no r.e. martingale succeeds on Z.*

The following characterisation of all subgroups of $(\mathbb{Q}, +)$ forms the basis of our definition of a random subgroup.

▶ **Theorem 2.** *[3] Let G be any subgroup of $(\mathbb{Q}, +)$. Then there is an integer z, as well as a sequence $(n_i)_{i<\omega}$ with $n_i \in \mathbb{N} \cup \{\infty\}$ such that $G = \left\{ \frac{a \cdot z}{\Pi_{i=0}^{k} p_i^{m_i}} \mid a \in \mathbb{Z} \wedge k \in \mathbb{N} \wedge (\forall i \leq k)[m_i \in \mathbb{N} \wedge m_i < n_i]\right\}$.*

▶ **Definition 3.** *Let $R \in 2^\omega$ be a real in the Cantor space, i.e. an infinite sequence of 0's and 1's. Then the group G_R is the subgroup of the rational numbers $(\mathbb{Q}, +)$ generated by $a_0, a_1, \ldots$ with $a_i = \frac{1}{p_i^{n_i}}$ for all $i \in \mathbb{N}$, where for each $i \in \mathbb{N}$, by p_i we denote the $(i+1)$-st prime and by n_i the number of consecutive 1's in R between the i-th and $(i+1)$-st zero in R, with which we let n_0 count the number of starting 1's. If there is no $(i+1)$-st zero, we let $n_i := \infty$, meaning that for all n the fraction $\frac{1}{p_i^n}$ is in G_R.*

Clearly, $(\mathbb{Z}, +)$ is always a subgroup of G_R and $\frac{1}{p_i} \notin G_R$ if and only if the i-th and $(i+1)$-st zero in R are consecutive. Thus, if R ends with infinitely many zeros, then G_R is isomorphic to $(\mathbb{Z}, +)$. Moreover, there is a prime p_i such that $\frac{1}{p_j} \notin G_R$ for all $j > i$ and $\frac{1}{p_i^n} \in G_R$ for all $n \in \mathbb{N}$, for short p_i infinitely divides G_R, if and only if R ends with an infinite sequence of 1's.

▶ **Lemma 4.** *If $R \in 2^\omega$ is Martin-Löf random, then n_i is finite for every $i \in \mathbb{N}$, where n_i is defined as in Definition 3. In other words, the group G_R is not infinitely divisible by any prime.*

Proof. This is an easy observation, as in no Martin-Löf random w.r.t the Lebesgue measure only finitely many 0's occur. ◀

A similar argument shows that for Martin-Löf random R there are infinitely many primes occurring as basis of a denominator of a generator.

▶ **Definition 5.** *Fix a probability distribution μ on the natural numbers and let $X = (X_i)_{i \in \mathbb{N}}$ be a sequence of iid random variables taking values in $\mathbb{N}$ with distribution $X_i \sim \mu$ for all $i \in \mathbb{N}$. Denote by H_X the subgroup of $(\mathbb{Q}, +)$ generated by $\{p_i^{-X_i} \mid i \in \mathbb{N}\}$, where p_i denotes the $(i+1)$-st prime.*

The so obtained random group might follow a more uniform process.

▶ **Lemma 6.** *If μ is the distribution on $\mathbb{N}$ assigning 0 probability $\frac{1}{2}$, 1 probability $\frac{1}{4}$, 2 probability $\frac{1}{8}$ and n probability 2^{-n-1}, then with probability 1 holds $H_X = G_R$ for some Martin-Löf random R.*

Proof. This follows immediately, as the set of ML-randoms has measure 1 with respect to the Lebesgue measure. From $X_0 = n_0$, $X_1 = n_1$, …, $X_i = n_i$, … we obtain an infinite binary sequence $R \in 2^\omega$ by recursively appending $1^{n_i}0$ in step i to the already established initial segment of R, starting with the empty string. By definition the Lebesgue measure assigns probability $\frac{1}{2^{n+1}}$ to having the (intermediate) subsequence $1^n 0$ in R. This is exactly the probability of the event $X_i = n$. ◀

A *generating sequence for G_R* is an infinite sequence $(b_i)_{i<\omega}$ such that $\langle b_i \mid i < \omega \rangle = G_R$. We will often deal with generating sequences rather than minimal generating sets for G_R, mainly due to the fact that if the terms of a sequence β are carefully chosen based on a limiting recursive programme for R (so that β itself is limiting recursive), then, as will be seen later, the set of representations of elements of G_R with respect to β can have certain desirable computability properties, such as equality being co-r.e.

▶ **Proposition 7.** *Suppose $R \leq_T K$ is Martin-Löf random. Then there does not exist any strictly increasing recursive enumeration $i_0, i_1, i_2, \ldots$ such that for each j, there is some $n_{i_j} \geq 1$ with $p_{i_j}^{-n_{i_j}} \in G_R$.*

▶ **Theorem 8.** *If $R \leq_T K$ is Martin-Löf random, then $(G_R, +)$ is co-r.e., meaning that $+$ is recursive and there is a generating sequence with respect to which equality is co-r.e.*

Proof. For a fixed generating sequence $(q_i)_{i<\omega}$ of G_R there is an epimorphism from the set of finite sequences of integers $\mathbb{Z}^{<\omega}$ to G_R by identifying $\sigma = (\sigma(0), \ldots, \sigma(|\sigma|-1))$ with $x = \sum_{i=0}^{|\sigma|-1} \sigma(i) q_i$. We call σ a representation of x w.r.t. $(q_i)_{i<\omega}$ or $(q_i)_{i<n+1}$.

Obviously, for any generating sequence of G_R addition is recursive as only the components of the representations have to be added as integers.

In order to prove that equality is co-r.e., we construct a specific generating sequence $(b_i)_{i<\omega}$. Based on the result R^s of the computation of R after s steps, we are going to define finite sequences β_s of rational numbers recursively, such that $|\beta_s| = s+1$ and inequality on $\{-s-1, \ldots, s+1\}^{s+1} \subseteq \mathbb{Z}^{s+1}$, interpreted as representations w.r.t. β_s, is decided and extends the inequalities on $\{-s, \ldots, s\}^s$, even though they originate from an interpretation as representations according to β_{s-1}. With this in the limit we obtain a generating sequence of G_R, meaning that for every i there is some $s_i > i$ such that for all $s \geq s_i$ the i-th element of β_s is the same as the i-th element of β_{s_i}, which we denote by b_i. Further, $(b_i)_{i\in\mathbb{N}}$ generates G_R and for this generating sequence equality will be co-r.e.

In the following we write $n_{i,s}$ for n_i according to R^s, i.e. the number of 1's between the i-th and $(i+1)$-st zero in R^s, as introduced in Definition 3. As R^s does not end with infinitely many 1's, $n_{i,s}$ can be computed in finitely many steps for every i and s.

$s = 0$. Let $\beta_0 = (1)$.

$s \rightsquigarrow s+1$. Check for every $i \leq s$ whether $n_{i,s} = n_{i,s+1}$. If $n_{i,s} = n_{i,s+1}$ let $\beta_{s+1}(i) = \beta_s(i)$. Replace all $\frac{1}{p_i^{n_{i,s}}}$ occurring in β_s with $n_{i,s} \neq n_{i,s+1}$ by some respective integer, for which existence we argue below, such that

$$\Delta_{(q_i)_{i<s+1}} = \{\, (\sigma_0, \sigma_1) \in (\, \{-s-1, \dots, s+1\}^{s+1}\,)^2 \mid \\ \sigma_0, \sigma_1 \text{ represent different elements w.r.t. } (q_i)_{i<s+1} \,\}$$

stays the same or enlarges if $(q_i)_{i<s+1}$ equals the first $s+1$ entries of β_{s+1} instead of β_s. Further, let

$$\beta_{s+1}(s+1) = \frac{1}{p_j^{n_{j,s+1}}},$$

where $j \leq s+1$ is minimal such that $\frac{1}{p_j^{n_{j,s+1}}}$ is an element of $G_{R^{s+1}}$ and does not yet occur in $\beta_{s+1}\restriction(s+1)$. If there is no such j, let $\beta_{s+1}(s+1) = 1$.

For example, if the tape after stage $s = 2$ started with $1111010\ldots$, after 3 steps contained $1101010\ldots$ and $\beta_2 = (1, \frac{1}{2^4}, \frac{1}{3})$, then in β_3 we would have to replace $\frac{1}{2^4}$ by an integer w such that for arbitrary integers $u_0, u_1, u_2, v_0, v_1, v_2$ between -3 and 3 we have

$$u_0 + u_1\frac{1}{2^4} + u_2\frac{1}{3} \neq v_0 + v_1\frac{1}{2^4} + v_2\frac{1}{3} \quad\Rightarrow\quad u_0 + u_1 w + u_2\frac{1}{3} \neq v_0 + v_1 w + v_2\frac{1}{3}$$

and $\beta_3(3)$ would be $\frac{1}{2^2}$.

We proceed by showing that there is always such an integer w.

▷ Claim 9. For every $s \in \mathbb{N}$ in step $s+1$ it is possible to alter finitely many entries of β_s to obtain $\beta_{s+1}\restriction(s+1)$ such that $\Delta_{\beta_s} \subseteq \Delta_{\beta_{s+1}\restriction(s+1)}$.

Proof of the Claim. Let $s \in \mathbb{N}$. It suffices to show that one entry can be replaced in this desired way. As the argument does not depend on the position, we further assume that it is the last entry. For all $(\sigma_0, \sigma_1) \in \Delta_{\beta_s}$ we want to prevent

$$\sum_{i=0}^{s-1} \sigma_0(i)\beta_s(i) + \sigma_0(s)w = \sum_{i=0}^{s-1} \sigma_1(i)\beta_s(i) + \sigma_1(s)w.$$

This is a linear equation having zero or one solution in $\mathbb{Q}$. As there are only finitely many choices for the pair (σ_0, σ_1), an integer not fulfilling any of these equations can be found in a computable way. ◁

We continue by proving that the entries of the β_s stabilize, such that in the limit we obtain a sequence $(b_i)_{i<\omega}$ of elements of G_R.

▷ Claim 10. For every $i \in \mathbb{N}$ there is some $s_i \geq i$ such that for all $s \geq s_i$ we have $\beta_s(i) = b_i$, with $b_i = \beta_{s_i}(i)$.

Proof of the Claim. Let $i \in \mathbb{N}$. If there is $s_i > i$ such that the entry $\beta_{s_i-1}(i)$ had to be changed, then $\beta_{s_i}(i)$ is an integer and thus, it will never be changed lateron. In case this does not happen, we obtain $\beta_s(i) = \beta_i(i)$ for all $s \geq i$ and therefore $s_i = i$. ◁

By the next claim the just constructed sequence generates the random group.

▷ Claim 11. The sequence $(b_i)_{i<\omega}$ generates G_R.

Proof of the Claim. Let $i \in \mathbb{N}$ and a_i as in Definition 3. We argue that there is some j with $a_i = b_j$. Let m_i be the position of the $(i+1)$-st zero in the Martin-Löf random R. Then there is s' such that after s' computation steps $R{\upharpoonright}(m_i+1)$ is not changed any more. Thus, after at most i additional steps all generators of G_R having one of the first i primes as denominator are in the range of $\beta_{s'+i}$. ◁

Finally, we observe that w.r.t. the generating sequence $(b_i)_{i<\omega}$ all pairs of unequal elements of G_R can be recursively enumerated.

▷ Claim 12. Equality in $(G_R, +)$ is co-r.e.

Proof of the Claim. We run the algorithm generating $(b_i)_{i<\omega}$ and in step s return all elements of the finite set Δ_{β_s}. As inequalities w.r.t β_s yield inequalities w.r.t. $(b_i)_{i<\omega}$, we only enumerate correct information. Further, for every two elements x, y of G_R fix representations w.r.t. $(b_i)_{i<\omega}$ and s' large enough such that not more than the first s' of the b_i occur in these representations, all of these have stabilized up to stage s' and all coefficients in the representations take values between $-s'-1$ and $s'+1$. Then $x \neq y$ if and only if the tuple of their representations is in $\Delta_{\beta_{s'}}$. ◁

This finishes the proof of the theorem. ◀

As there are K-recursive Martin-Löf random reals, we obtain the following corollary.

▶ **Corollary 13.** *There exists a co-r.e. random subgroup of the rational numbers.*

▶ Remark 14. Proposition 7 implies, in particular, that if $R \leq_T K$ is Martin-Löf random, then there cannot exist any generating sequence for G_R with respect to which equality of members of G_R is r.e. Indeed, suppose that such a generating sequence β did exist, so that $E := \{(\sigma, \tau) \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta{\upharpoonright}_{|\sigma|-1} = \tau \cdot \beta{\upharpoonright}_{|\tau|-1}\}$ is r.e. Fix any $\sigma_0 \in \mathbb{Z}^{<\omega}$ such that $\sigma_0 \cdot \beta_{|\sigma_0|-1} = 1$ (since $1 \in G_R$, such a σ_0 must exist). Then there is a strictly increasing recursive enumeration $i_0, i_1, i_2, \ldots$ such that for all j, i_j is the first ℓ found for which the following hold: (i) $\ell > i_{j'}$ whenever $j' < j$; (ii) there are $n_\ell \geq 1$ and relatively prime positive integers q, r with $p_\ell \nmid q$ and $p_\ell \nmid r$ such that for some m, $(q\sigma_0, I_m(rp_\ell^{n_\ell})) \in E$. Note that

$$\begin{aligned}(q\sigma_0, I_m(rp_\ell^{n_\ell})) \in E &\Leftrightarrow q = (q\sigma_0) \cdot \beta_{|\sigma_0|-1} = I_m(rp_\ell^{n_\ell}) \cdot \beta_{m-1} = rp_\ell^{n_\ell} b_{m-1} \\ &\Leftrightarrow b_{m-1} = qp_\ell^{-n_\ell} r^{-1}.\end{aligned}$$

The Martin-Löf randomness of R implies that β contains infinitely many terms of the form $\frac{q'}{r' p_{\ell'}^{n'_{\ell'}}}$ with $n'_{\ell'} \geq 1$, q' and r' relatively prime and positive, $p_{\ell'} \nmid q'$ and $p_{\ell'} \nmid r'$. Thus i_j is defined for all j, and by Proposition 7 this contradicts the Martin-Löf randomness of R.

Further, a variation of the algorithm yields that equality of the proper rational part is r.e. on random groups.

▶ **Theorem 15.** *If $R \leq_T K$ is Martin-Löf random, then equality modulo 1 on $(G_R, +)$ is r.e. with respect to some generating sequence.*

The next main result is concerned with the model-theoretic properties of random subgroups of rationals. We recall that two structures (in the model-theoretic sense) M and N with the same set σ of non-logical symbols are *elementarily equivalent* (denoted $M \equiv N$) iff they satisfy the same first-order sentences over σ; the *theory* of a structure M (denoted $\mathrm{Th}(M)$) is the set of all first-order sentences (over the set of non-logical symbols of M) that are satisfied by M. The reader is referred to [16] for more background on model theory. We will prove a result that may appear a bit surprising: even though Martin-Löf random subgroups of $(\mathbb{Q}, +)$ (viewed as classes of integer sequence representations) are not computable, any such subgroup is elementarily equivalent to $(\mathbb{Z}, +)$ - the additive group of integers - and thus has a decidable theory. In other words, the incomputability of a random subgroup of rationals, at least according to the notion of "randomness" adopted in the present work, has little or no bearing on the decidability of its first-order properties. We begin by showing that the theory of any subgroup G of rationals reduces to that of the subgroup of $(\mathbb{Q}, +)$ generated by the set of all rationals either equal to 1 or of the shape p^{-n}, where p is a prime infinitely dividing G and $n \in \mathbb{N}$. Our proof of this fact rests on a sufficient criterion due to Szmielew [27] for the elementary equivalence of two groups; this result will be stated as it appears in [11].

▶ **Theorem 16.** *([27], as cited in [11]) Let p be a prime number and G be a group. For all $n \geq 1$, $k \geq 1$ and elements $g_1, \ldots, g_k \in G$, define $G[p^n] := \{x \in G \mid p^n x = 0\}$ and the following predicate $C(p; g_1, \ldots, g_k)$:*

$C(p; g_1, \ldots, g_k) \Leftrightarrow$ the images $g'_1, \ldots, g'_k$ of $g_1, \ldots, g_k$ in the factor group $\overline{G} := G/G[p^n]$are such that $g'_1 + p\overline{G}, \ldots, g'_k + p\overline{G}$ are linearly independent in $\overline{G}/p\overline{G}$.

Define the parameters $\alpha_{p,n}(G), \beta_p(G)$ and $\gamma_p(G)$ as follows.

$$\begin{aligned}
\alpha_{p,n}(G) &:= \sup\{k \in \mathbb{N} \mid G \text{ contains } \mathbb{Z}^k_{p^n} \text{ as a pure subgroup}\},\\
\beta_p(G) &:= \inf\{\sup\{k \in \mathbb{N} \mid \mathbb{Z}^k_{p^n} \text{ is a subgroup of } G\} \mid n \in \mathbb{N}\},\\
\gamma_p(G) &:= \inf\{\sup\{k \in \mathbb{N} \mid (\exists x_1, \ldots, x_k) C(p; x_1, \ldots, x_k)\} \mid n \in \mathbb{N}\}.
\end{aligned}$$

(Here $pG := \{pg \mid g \in G\}$ and $\mathbb{Z}^k_{p^n}$ is the k-th power of the primary cyclic group on p^n elements, that is, it consists of all elements $(a_0, \ldots, a_{k-1})$ such that $a_0, \ldots, a_{k-1} \in \mathbb{Z}_{p^n}$.) Then any two groups H and L are elementarily equivalent iff $\alpha_{q,m}(H) = \alpha_{q,m}(L)$, $\beta_q(H) = \beta_q(L)$ and $\gamma_q(H) = \gamma_q(L)$ for all primes q and all $m \geq 1$.

The definition of a *pure* subgroup will not be used in the proof of the subsequent theorem; it will be observed that if G is a subgroup of the rationals, then for $k \geq 1$ and $n \geq 1$, it cannot contain $\mathbb{Z}^k_{p^n}$ as a subgroup in any case, so that $\alpha_{p,n}(G) = \beta_p(G) = 0$.

▶ **Theorem 17.** *Let G be a subgroup of $(\mathbb{Q}, +)$. Then $G \equiv [\mathbb{Z}]_{P(G)}$, where $P(G) := \{i \in \mathbb{N} \mid (\forall x \in G)(\forall n \in \mathbb{N})[\frac{x}{p_i^n} \in G]\}$ denotes the set of all primes infinitely dividing G and for a set of primes P we write $[\mathbb{Z}]_P$ for the subgroup of $(\mathbb{Q}, +)$ generated by $\{1\} \cup \{\frac{1}{p^k} \mid p \in P, k \in \mathbb{N}\}$.*

Note that $\mathrm{Th}([\mathbb{Z}]_K, +)$ is undecidable; in contrast, for R Martin-Löf random we have $P(G_R) = \varnothing$, so the promised corollary follows.

▶ **Corollary 18.** *Let $R \in 2^\omega$ be Martin-Löf random. Then $(G_R, +)$ and $(\mathbb{Z}, +)$ have the same theories.*

One may ask whether this still holds for richer structures. This is not the case, as for example the theory of $(G, +, <)$ is different from $\mathrm{Th}(\mathbb{Z}, +, <)$, as in the latter $x = 1$ is a satisfying assignment for the formula $x + x > x \wedge \forall y < x\, \neg y + y > y$. There does not exist an $x \in G_R$ with this property for a ML-random R.

4 Learning Finitely Generated Subgroups of a Random Subgroup of Rationals

In this section, we investigate the learnability of non-trivial finitely generated subgroups of any group G_R generated by a Martin-Löf random sequence R such that $R \leq_T K$. First, we introduce some additional notation.

▶ **Notation 19.** *Let $R \leq_T K$ be Martin-Löf random and let $\beta := (b_i)_{i<\omega}$ be any generating sequence of G_R. For any subgroup F of G_R, F_β denotes the set of all representations of elements of F with respect to β, that is, $F_\beta := \{\sigma \in \mathbb{Z}^{<\omega} \mid \sum_{i=0}^{|\sigma|-1} \sigma(i) b_i \in F\}$. Furthermore, define $\mathcal{F}_\beta := \{F_\beta \mid F$ is a non-trivial finitely generated subgroup of $G_R\}$.*

We will consider learning from *texts*, where a text is an infinite sequence that contains all elements of F_β for the F to be learnt and may contain the symbol #, which indicates a pause in the data presentation and thus no new information. For any text T and $n \in \mathbb{N}$, $T(n)$ denotes the $(n+1)$-st term of T and $T[n]$ denotes the finite sequence $T(0), \ldots, T(n-1)$, i.e., the *initial segment* of length n of T; $\mathrm{content}(T[n])$ denotes the set of non-pause elements occurring in $T[n]$. A *learner* M is a recursive function mapping $(\mathbb{Z}^{<\omega} \cup \{\#\})^*$ into $\mathbb{N} \cup \{?\}$; the ? symbol permits M to abstain from conjecturing at any stage. A learner is fed successively with growing initial segments of the text and it produces a sequence of conjectures $e_0, e_1, e_2, \ldots$, which are interpreted with respect to a fixed *hypothesis space*. In the present paper, we stick to the standard hypothesis space, a fixed Gödel numbering $W_0, W_1, W_2, \ldots$ of all r.e. subsets of $\mathbb{Z}^{<\omega}$. In our setting from the generator $\frac{q}{m}$ of F we can immediately derive an index e for F_β and therefore in the proofs we argue for learning q and m. The learner is said to *behaviourally correctly* (denoted **Bc**) learn the representation F_β of a finitely generated subgroup F with respect to a fixed generating sequence β for G_R iff on every text for F_β, the sequence of conjectures output by the learner converges to a correct hypothesis; in other words, the learner almost always outputs an r.e. index for F_β [7, 5, 2]. If almost all of the learner's hypotheses on the given text are equal in addition to being correct, then the learner is said to *explanatorily* (denoted **Ex**) learn F_β (or it learns F_β *in the limit*) [9].

A useful notion that captures the idea of the learner converging on a given text is that of a *locking sequence*, or more generally that of a *stabilising sequence*. A sequence $\sigma \in (\mathbb{N} \cup \{\#\})^*$ is called a *stabilising sequence* [8] for a learner M on some set L if $\mathrm{content}(\sigma) \subseteq L$ and for all $\tau \in (L \cup \{\#\})^*$, $M(\sigma) = M(\sigma \circ \tau)$. A sequence $\sigma \in (\mathbb{N} \cup \{\#\})^*$ is called a *locking sequence* [4] for a learner M on some set L if σ is a stabilising sequence for M on L and $W_{M(\sigma)} = L$.

The following proposition due to Blum and Blum [4] will be occasionally useful.

▶ **Proposition 20.** *[4] If a learner M explanatorily learns some set L, then there exists a locking sequence for M on L. Furthermore, all stabilising sequences for M on L are also locking sequences for M on L.*

Clearly, also a **Bc**-version of Proposition 20 holds.

It is not clear in the first place whether or not every finitely generated subgroup of a randomly generated subgroup of $(\mathbb{Q}, +)$ can even be represented as an r.e. set. This will be clarified in the next series of results. We recall that a *finitely generated subgroup* F of G_R is any subgroup of G_R that has some *finite generating set* S, which means that every element of F can be written as a linear combination of finitely many elements of S and the inverses of elements of S. F is *trivial* if it is equal to $\{0\}$; otherwise it *non-trivial.* Furthermore, if G_R is a subgroup of $(\mathbb{Q}, +)$, then any finitely generated subgroup F of G_R is *cyclic*, that is, $F = \left\langle \frac{q}{m} \right\rangle$ for some $q \in \mathbb{N}$ and $m \in \mathbb{N}$ with $\gcd(q, m) = 1$ (see, for example, [26, Theorem 8.1]). The latter fact will be used freely throughout this paper. For any generating sequence β for G_R and any finitely generated subgroup F of G_R, the set of representations of elements of F with respect to β will be denoted by F_β.

▶ **Theorem 21.** *Let $R \leq_T K$ be Martin-Löf random. Then there is a generating sequence $(b_i)_{i<\omega}$ of G_R such that for every non-trivial finitely generated subgroup F of G_R the set F_β is r.e.*

▶ Remark 22. The statement of Theorem 21 excludes the trivial subgroup because for any generating sequence $\beta := (b_i)_{i<\omega}$ for G_R, $\langle 0 \rangle_\beta$ cannot be r.e. To see this, suppose, by way of contradiction, that $\langle 0 \rangle_\beta$ were r.e. Given any $\sigma, \sigma' \in \mathbb{Z}^{<\omega}$, set $\ell = \max(\{|\sigma| - 1, |\sigma'| - 1\})$, and for all $i \in \{0, \ldots, \ell\}$, $w_i = \sigma(i)$ if $i \leq |\sigma| - 1$ and 0 otherwise, and $v_i = \sigma'(i)$ if $i \leq |\sigma'| - 1$ and 0 otherwise. Then $\sigma \cdot \beta \upharpoonright_{|\sigma|-1} = \sigma' \cdot \beta \upharpoonright_{|\sigma'|-1} \Leftrightarrow \sigma \cdot \beta \upharpoonright_{|\sigma|-1} - \sigma' \cdot \beta \upharpoonright_{|\sigma'|-1} = 0 \Leftrightarrow \sum_{i=0}^{\ell} (w_i - v_i) b_i = 0 \Leftrightarrow (w_0 - v_0, w_1 - v_1, \ldots, w_\ell - v_\ell) \in \langle 0 \rangle_\beta$. Thus if $\langle 0 \rangle_\beta$ were r.e., then equality with respect to β would also be r.e., which, as was shown earlier, is impossible.

We note that there cannot be any generating sequence β for G_R such that there are finitely generated subgroups F, F' of G_R with F_β r.e. and F'_β co-r.e.

▶ **Theorem 23.** *Let $R \leq_T K$ be Martin-Löf random. Let β be any generating sequence for G_R. Then for any finitely generated subgroups F and F' of G_R, one of the following holds: (i) both F_β and F'_β are r.e., (ii) both F_β and F'_β are co-r.e., or (iii) at least one of F_β and F'_β is neither r.e. nor co-r.e.*

▶ **Theorem 24.** *Let $R \leq_T K$ be Martin-Löf random. Then there is a generating sequence β of G_R such that F_β is r.e. for every non-trivial finitely generated subgroup F of G_R and $\mathcal{F}_\beta$ is* **Bc***-learnable.*

The next result shows, in contrast to Theorem 24, that if $R \leq_T K$ is Martin-Löf random, then, given *any* generating sequence β for G_R such that F_β is r.e. for every non-trivial finitely generated subgroup F of G_R, the class $\mathcal{F}_\beta$ is not explanatorily learnable.

▶ **Theorem 25.** *Let $R \leq_T K$ be Martin-Löf random. Suppose $\beta := (b_i)_{i<\omega}$ is a generating sequence for G_R such that for any non-trivial finitely generated subgroup F of G_R, F_β is r.e. Then $\mathcal{F}_\beta$ is not* **Ex***-learnable.*

The next theorem considers the learnability of the set of representations of any finitely generated subgroup F of the quotient group $G_R/\mathbb{Z}$ with respect to the generating sequence for $G_R/\mathbb{Z}$ constructed in the proof of Theorem 15. Slightly abusing the notation defined in Notation 19, for any generating sequence β for $G_R/\mathbb{Z}$, F_β will denote the set of representations of any subgroup F of $G_R/\mathbb{Z}$ with respect to β, and $\mathcal{F}_\beta$ will denote $\{F_\beta \mid F \text{ is a finitely generated subgroup of } G_R/\mathbb{Z}\}$.

▶ **Theorem 26.** *Suppose $R \leq_T K$ is Martin-Löf random. Let $G_R/\mathbb{Z}$ be the quotient group of G_R by $\mathbb{Z}$. Then there is a generating sequence β for $G_R/\mathbb{Z}$ such that F_β is r.e. for all finitely generated subgroups of $G_R/\mathbb{Z}$ and $\mathcal{F}_\beta$ is* **Bc***-learnable.*

As in the case of the collection of non-trivial finitely generated subgroups of G_R, the class $\mathcal{F}_\beta$ is not explanatorily learnable with respect to any generating sequence β for $G_R/\mathbb{Z}$. The proof is entirely analogous to that of Theorem 25.

▶ **Theorem 27.** *Let $R \leq_T K$ be Martin-Löf random. Suppose $\beta := (b_i)_{i<\omega}$ is a generating sequence for $G_R/\mathbb{Z}$ such that for any finitely generated subgroup F of $G_R/\mathbb{Z}$, F_β is r.e. Then $\mathcal{F}_\beta$ is not* **Ex***-learnable.*

A natural question is whether the learnability or non-learnability of a class of representations for a collection of subgroups of G_R is independent of the choice of the generating sequence for G_R. We have seen in Theorem 25, for example, that the non explanatory learnability of the class of non-trivial finitely generated subgroups of G_R holds for *any* generating sequence for G_R such that F_β is r.e. whenever F is a finitely generated subgroup. The next theorem gives a positive learnability result that is to some extent independent of the choice of the generating sequence: for any generating sequence β for G_R such that equality with respect to β is K-recursive and F_β is r.e. whenever F is a finitely generated subgroup of G_R, the class $\mathcal{F}_\beta$ is explanatorily learnable relative to oracle K.

▶ **Theorem 28.** *Let $R \leq_T K$ be Martin-Löf random. Then for any generating sequence β for G_R such that equality with respect to β is K-recursive (in other words, the set $E_\beta := \{(\sigma,\sigma') \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta_{|\sigma|-1} = \sigma' \cdot \beta_{|\sigma'|-1}\}$ is K-recursive) and F_β is r.e. for all finitely generated subgroups of G_R, $\mathcal{F}_\beta$ is* $\mathbf{Ex}[K]$*-learnable.*

We recall from Theorem 15 that there is a generating sequence $\beta := (b_i)_{i<\omega}$ for G_R such that equality modulo 1 with respect to β is r.e.; in other words, the set $\{(\sigma,\sigma') \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta_{|\sigma|-1} \equiv \sigma' \cdot \beta_{|\sigma|'-1}\ (mod\ 1)\}$ is r.e. The next result considers the learnability of a class that is in some sense "orthogonal" to the class $\mathbb{Z}_\beta$: the class of all sets of representations of $\mathbb{Z}$ with respect to *any* generating sequence β' for G_R such that $\mathbb{Z}_{\beta'}$ is r.e. In the statement and proof of the next theorem, for any generating sequence β for G_R, let E_β denote the set $\{(\sigma,\sigma') \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta_{|\sigma|-1} = \sigma' \cdot \beta_{|\sigma'|-1}\ (mod\ 1)\}$.

▶ **Theorem 29.** *Let $R \leq_T K$ be Martin-Löf random. Let $\mathcal{G}_0$ be the collection of all generating sequences β for G_R such that E_β is r.e., and define $\mathcal{E}_0 := \{E_\beta \mid \beta \in \mathcal{G}_0\}$. Then $\mathcal{E}_0$ is not* **Bc***-learnable.*

In contrast to Theorem 29, we present a positive learnability result for the collection of all E_β such that E_β is co-r.e. The learnability is with respect to a hypothesis space which uses co-r.e. indices. That is to say, given any text T, the learner will on T always output an r.e. index for sets of the form $(\mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega}) \setminus E_{\beta'}$, where $E_{\beta'}$ is some co-r.e. set. In the statement and proof of the next theorem, given any generating sequence β for G_R such that equality with respect to β is co-r.e., E_β will denote the set $\{(\sigma,\sigma') \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta_{|\sigma|-1} = \sigma' \cdot \beta_{|\sigma'|-1}\}$.

▶ **Theorem 30.** *Let $R \leq_T K$ be Martin-Löf random. Let $\mathcal{G}_1$ be the collection of all generating sequences β for G_R such that E_β is co-r.e., and define $\mathcal{E}_1 := \{E_\beta \mid \beta \in \mathcal{G}_1\}$. Then $\mathcal{E}_1$ is explanatorily learnable relative to oracle K using co-r.e. indices. That is to say, there is a K-recursive learner M such that for any $E_\beta \in \mathcal{E}_1$ and any text T for E_β, M on T will output an r.e. index for $(\mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega}) \setminus E_\beta$ in the limit.*

5 Conclusion and Possible Future Research

This paper introduced a method of constructing random subgroups of rationals, whereby Martin-Löf random binary sequences are directly encoded into the generators of the group.

It was shown that if the Martin-Löf random sequence associated to a randomly generated subgroup G is limit-recursive, then one can build a generating sequence β for G such that the word problem for G is co-r.e. with respect to β, as well as another generating sequence β' such that the word problem for $G/\mathbb{Z}$ with respect to β' is r.e. We also showed that every non-trivial finitely generated subgroup of G has an r.e. representation with respect to a suitably chosen generating sequence for G; moreover, the class of all such r.e. representations is behaviourally correctly learnable but never explanatorily learnable. We did not, however, extend the definition of algorithmic randomness to *all* Abelian groups; we suspect that such a general definition might be out of reach of current methods due to the fact that the isomorphism types of even rank 2 groups (subgroups of $(\mathbb{Q}^2, +)$) are still unknown.

References

1 Reinhold Baer. Abelian groups without elements of finite order. *Duke Mathematical Journal*, 3(1):68–122, March 1937.

2 Janis Bārzdiņš. Two theorems on the limiting synthesis of functions. *Latv. Gos. Univ. Uch. Zapiski*, 210:82–88, 1974. (In Russian).

3 Ross A. Beaumont and Herbert S. Zuckerman. A characterization of the subgroups of the additive rationals. *Pacific Journal of Mathematics*, 1(2):169–177, 1951.

4 Lenore Blum and Manuel Blum. Toward a Mathematical Theory of Inductive Inference. *Information and Control*, 28:125–155, 1975.

5 John Case and Carl Smith. Comparison of identification criteria for machine inductive inference. *Theoretical Computer Science*, 25:193–220, 1983.

6 Rod Downey and Denis Hirschfeldt. *Algorithmic Randomness and Complexity.* Springer-Verlag, Berlin, Heidelberg, 2010.

7 Jerome A. Feldman. Some decidability results on grammatical inference and complexity. *Information and Control*, 20(3):244–262, 1972.

8 Mark A. Fulk. *A Study of Inductive Inference Machines.* PhD thesis, State University of New York at Buffalo, Buffalo, NY, USA, 1986.

9 E. M. Gold. Language Identification in the Limit. *Information and Control*, 10:447–474, 1967.

10 Mikhail Gromov. Random walk in random groups. *Geometric and Functional Analysis*, 13:73–146, 2003.

11 Nazif G. Khisamiev. Chapter 17:Constructive abelian groups. In Yu. L. Ershov, S. S. Goncharov, A. Nerode, J. B. Remmel, and V. W. Marek, editors, *Handbook of Recursive Mathematics*, volume 139 of *Studies in Logic and the Foundations of Mathematics*, pages 1177–1231. Elsevier, 1998.

12 Bakhadyr Khoussainov. A Quest for Algorithmically Random Infinite Structures. In *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)*, CSL-LICS '14, pages 56:1–56:9, 2014.

13 Bakhadyr Khoussainov. A Quest for Algorithmically Random Infinite Structures, II. In *Logical Foundations of Computer Science - International Symposium, LFCS 2016*, pages 159–173, 2016.

14 Ming Li and Paul Vitány. A New Approach to Formal Language Theory by Kolmogorov Complexity. *SIAM Journal on Computing*, 24(2):398–410, 1995.

15 Ming Li and Paul Vitány. *An Introduction to Kolmogorov Complexity and Its Applications.* Springer-Verlag, New York, NY, USA, 3rd edition, 2008.

16 David Marker. *Model theory: an introduction*, volume 217 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, NY, USA, 2002.

17 Eric Martin and Daniel N. Osherson. *Elements of scientific inquiry.* MIT Press, Cambridge, Massachusetts, 1998.

18 Per Martin-Löf. The definition of random sequences. *Information and Control*, 9(6):602–619, 1966.

19 André Nies. *Computability and Randomness.* Oxford University Press, Inc., New York, NY, USA, 2009.

20 André Nies and Volkher Scholz. Martin-Löf random quantum states. *arXiv preprint arXiv:1709.08422*, 2017.

21 Piergiorgio Odifredd. *Classical Recursion Theory.* North-Holland, Amsterdam, 1989.

22 Hartley Rogers, Jr. *Theory of Recursive Functions and Effective Computability.* MIT Press, Cambridge, MA, USA, 1987.

23 Claus-Peter Schnorr. A Unified Approach to the Definition of a Random Sequence. *Mathematical Systems Theory*, 5(3):246–258, 1971.

24 Robert I. Soare. *Recursively Enumerable Sets and Degrees: A Study of Computable Functions and Computably Generated Sets.* Perspectives in Mathematical Logic. Springer Berlin Heidelberg, 1999.

25 Frank Stephan and Yuri Ventsov. Learning algebraic structures from text. *Theoretical Computer Science*, 268(2):221–273, 2001.

26 Sándor Szabó and Arthur D. Sands. *Factoring groups into subsets.* Lecture Notes in Pure and Applied Mathematics. Chapman and Hall/CRC Press, 6000 Broken Sound Parkway NW, Suite 300, 2009.

27 Wanda Szmielew. Elementary properties of Abelian groups. *Fundamenta Mathematicae*, 41(2):203–271, 1955.

28 Todor Tsankov. The additive group of the rationals does not have an automatic presentation. *Journal of Symbolic Logic*, 76(4):1341–1351, 2011.

29 Volodya Vovk, Alexander Gammerman, and Craig Saunders. Machine-Learning Applications of Algorithmic Randomness. In *Proceedings of the Sixteenth International Conference on Machine Learning (ICML 1999)*, pages 444–453, 1999.