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 → Inductive inference, Theory of computation → Pseudorandomness and derandomization

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..2019.

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, 16, 19]. It has also been applied in a wide variety of disciplines, including formal language and automata theory [15], machine learning [31], 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 [13, 14] 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 algorithmically 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 these three questions positively for a fundamental and familiar algebraic structure, the *additive group of rationals*, denoted $(\mathbb{Q}, +)$. Prior to this work, question (A) was answered for structures such as *finitely generated* universal algebras, connected graphs, trees of bounded degree and monoids [13]. 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 [13].

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 [2], 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 [2] and then later by Beaumont and Zuckerman [3]. Later, the group $(\mathbb{Q}, +)$ was studied in the context of automatic structures [30]. 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 [13, 14]; 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. The existence of a branching class of groups, and thus of continuunm many Martin-Löf random groups, was only recently established [11].

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. For a similar reason, no randomly generated subgroup G_R is infinitely divisible by a prime, that is, there is no prime p such that p^{-n} belongs to G_R for all n.

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: in detail, 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 known as learning from text. Stephan and Ventsov [27] 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 [18, 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 [2]. It may be noted that the present work considers learning

[1] For a proof of the decidability of the theory of $(\mathbb{Z},+)$, often known as *Presburger Arithmetic*, see [17, pages 81–84].

of the actual representations of finitely generated subgroups, which are all isomorphic to each other, as opposed to learning their structures up to isomorphism, as is considered in the learning framework of Martin and Osherson [18]. 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 is *behaviourally correctly* learnable, that is, all these 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 *explanatorily* learnable, or 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 [23, 25, 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 $s < |\beta|$, $\beta \upharpoonright_s$ 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 $[W_0], [W_1], [W_2], \dots$ 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 [22] defined randomness based on tests. A *Martin-Löf test* is a uniformly r.e. sequence $(G_m)_{m<\omega}$ of open sets such that $(\forall m<\omega)[\lambda(G_m) \le 2^{-m}]$. 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 [24] 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 $\sup_n \mathrm{mg}(Z(0)\dots Z(n)) = \infty$.

▶ **Theorem 1.** *[24] 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* $G = \left\{ \frac{a\cdot z}{\Pi_{i=0}^k p_i^{m_i}} \mid a\in\mathbb{Z} \wedge k \in \mathbb{N} \wedge (\forall i \le k)[m_i \in \mathbb{N} \wedge m_i < n_i]\right\}$.

▶ **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 $a_0, a_1, \dots$ 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^n0 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 $p_{i_j}^{-n_{i_j}} \in G_R$.*

Proof. Suppose that such an enumeration did exist. We show that this contradicts the Martin-Löf randomness of R. By Theorem 1, it suffices to show that there is a recursive martingale mg succeeding on R. Define mg as follows. For any $\sigma \in \{0,1\}^*$, if there is some j such that σ contains at least i_j occurrences of 0 and the i_j-th occurrence of 0 is immediately succeeded by 0, then set $\mathrm{mg}(\sigma) = 0$. Else, let j be the largest j' for which either $j' = 0$ or σ contains at least $i_{j'}$ occurrences of 0, and set

$$\mathrm{mg}(\sigma) = \begin{cases} 2^{j+1} & \text{if } \sigma \text{ contains at least } i_j \text{ 0's and the } i_j\text{-th occurrence of 0 in } \sigma \text{ is not} \\ & \text{the last bit of } \sigma; \\ 2^j & \text{otherwise.} \end{cases}$$

It may be directly verified that mg satisfies the martingale equality $\mathrm{mg}(\sigma) = \frac{1}{2}(\mathrm{mg}(\sigma 0) + \mathrm{mg}(\sigma 1))$ for all $\sigma \in \{0,1\}^*$. Furthermore, $\mathrm{mg}(R(0)R(1)\ldots R(n))$ grows to infinity with n and so mg succeeds on R, contradicting the fact that R is Martin-Löf random. ◀

▶ **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

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

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.** *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.** *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.** *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 $R \restriction (m_i + 1)$ 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.** *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 9.** *There exists a co-r.e. random subgroup of the rational numbers.*

▶ Remark. 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 $E := \{(\sigma, \tau) \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta \restriction_{|\sigma|-1} = \tau \cdot \beta \restriction_{|\tau|-1}\}$ 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 10.** *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.*

Proof. The construction of the generating sequence follows the construction of $(b_i)_{i<\omega}$ in the proof of Theorem 8 with the main difference that in step $s+1$ instead of making sure that in case of replacements no already enumerated inequalities are destroyed, we have to make sure that all equalities modulo 1 that have been established in the first s steps are preserved. Formally, this reads as $E_{\beta_s} \subseteq E_{\beta_{s+1}}$ with

$$E_{(q_i)_{i<s+1}} = \{ (\sigma_0, \sigma_1) \in (\{-s-1, \ldots, s+1\}^{s+1})^2 \mid \\ \sigma_0, \sigma_1 \text{ modulo 1 represent the same element w.r.t. } (q_i)_{i<s+1} \}.$$

As we have to preserve equality modulo 1 and each prime occurs at most once as basis of a denominator, we may use 0 to replace the prime power fraction(s) if necessary. The rest of the proof works the same way. ◀

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 [17] 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 [29] for the elementary equivalence of two groups; this result will be stated as it appears in [12].

▶ **Theorem 11.** *([29], as cited in [12]) 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.

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

(Here $pG := \{pg \mid g \in G\}$ and $\mathbb{Z}_{p^n}^k$ 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 $\mathbb{Z}_{p^n}^k$ as a subgroup in any case, so that $\alpha_{p,n}(G) = \beta_p(G) = 0$.

▶ **Theorem 12.** *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 $\{1\} \cup \{\frac{1}{p^k} \mid p \in P, k \in \mathbb{N}\}$.*

Proof. Define the predicate $C(p; x_1, \ldots, x_k)$ and the parameters $\alpha_{p,n}, \beta_p$ and γ_p as in Theorem 11. Let p be a prime number and suppose $n \geq 1$. By Theorem 11, it suffices to show that the three parameters $\alpha_{p,n}, \beta_p$ and γ_p coincide on G and $[\mathbb{Z}]_{P(G)}$. First, $\mathbb{Z}_{p^n}^k$ cannot be a subgroup of G or $[\mathbb{Z}]_{P(G)}$ when $k \geq 1$ and $n \geq 1$ since by Theorem 2, no non-trivial subgroup of any subgroup of rationals can be torsion[2]; thus $\alpha_{p,n}$ and β_p are both equal to 0 for G as well as $[\mathbb{Z}]_{P(G)}$. For a similar reason, $G[p^n] := \{x \in G \mid p^n x = 0\} = \{0\}$ for every p and $n \in \mathbb{N}$, and therefore $\overline{G} := G/G[p^n] = G/\{0\} = G$ and $\overline{G}/p\overline{G} = G/pG$. Furthermore, G/pG may be regarded as a vector space over the field $\mathbb{Z}_p$, and $(\exists x_1, \ldots, x_k)C(p; x_1, \ldots, x_k)$ holds iff the dimension of the $\mathbb{Z}_p$-vector space G/pG (denoted $\dim_{\mathbb{Z}_p}(G/pG)$) is at least k. It follows that

$$
\begin{aligned}
\gamma_p(G) &= \inf\{\sup\{k \in \mathbb{N} \mid (\exists x_1, \ldots, x_k)C(p; x_1, \ldots, x_k)\} \mid n \in \mathbb{N}\} \\
&= \inf\{\sup\{k \in \mathbb{N} \mid \dim_{\mathbb{Z}_p}(G/pG) \geq k\} \mid n \in \mathbb{N}\} \\
&= \dim_{\mathbb{Z}_p}(G/pG).
\end{aligned}
$$

Similarly, $[\mathbb{Z}]_{P(G)}/p[\mathbb{Z}]_{P(G)}$ is a $\mathbb{Z}_p$-vector space and $\gamma_p([\mathbb{Z}]_{P(G)}) = \dim_{\mathbb{Z}_p}\left([\mathbb{Z}]_{P(G)}/p[\mathbb{Z}]_{P(G)}\right)$. Thus it suffices to show that $\dim_{\mathbb{Z}_p}(G/pG) = \dim_{\mathbb{Z}_p}\left([\mathbb{Z}]_{P(G)}/p[\mathbb{Z}]_{P(G)}\right)$.

Case 1: $p \in P(G)$. Then $pG = G$. It follows that $G/pG = G/G = \{0\}$; the same argument shows that $[\mathbb{Z}]_{P(G)}/p[\mathbb{Z}]_{P(G)} = \{0\}$.

Case 2: $p \notin P(G)$. Then there is some non-zero $x \in G$ such that $p^{-1} \cdot x \notin G$. It may be assumed without loss of generality that $x = 1$ because if $x = u \cdot v^{-1}$ for some non-zero integers u and v, then, taking $G' = vG$, G' is a subgroup of $(\mathbb{Q}, +)$ that is isomorphic to G such that $P(G) = P(G')$. Assuming $p^{-1} \notin G$, there is a fixed integer z such that G is generated (as a subgroup of $(\mathbb{Q}, +)$) by rationals of the shape zq^{-n}, where q ($\neq p$) is prime and $n \geq 1$. As before, it may be assumed without loss of generality that $z = 1$. It will be shown that each such generator is congruent to an integer modulo pG. Fix a generator of the shape q^{-n}. Let m and l be integers such that $mq^n + lp = 1$. Then $q^{-n} = m + p \cdot (l \cdot q^{-n})$. It follows that G/pG is isomorphic to $\mathbb{Z}_p$ and so $\dim_{\mathbb{Z}_p}(G/pG) = \dim(\mathbb{Z}_p) = 1$. Using the case assumption that $p^{-1} \notin P(G)$, one also has that $p^{-1} \notin [\mathbb{Z}]_{P(G)}$, and so the same argument as before yields $\dim_{\mathbb{Z}_p}\left([\mathbb{Z}]_{P(G)}/p[\mathbb{Z}]_{P(G)}\right) = 1$. ◀

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.

[2] We recall that a group G is *torsion* iff for every $x \in G$, there is some n such that x^n is equal to the identity element of G.

▶ **Corollary 13.** *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 $R \leq_T K$. More specifically, we will examine for any given G_R the set F_β of representations of elements of any non-trivial finitely generated subgroup F of G_R with respect to a fixed generating sequence β for G_R such that all F_β are r.e., and consider the learnability of the class of all such sets of representations.

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 $T(0), \dots, T(n-1)$, i.e., the *initial segment* of length n of T; 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 $e_0, e_1, e_2, \dots$, 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 $W_0, W_1, W_2, \dots$ 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, 1]. 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 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 14.** *[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 14 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, $F = \left\langle \dfrac{q}{m} \right\rangle$ for some $q \in \mathbb{N}$ and $m \in \mathbb{N}$ with $\gcd(q, m) = 1$ (see, for example, [28, 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 15.** *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.*

Proof. We denote the set of all non-trivial finitely generated subgroups of G_R by $\mathcal{F}$ and modify the construction of the generating sequence $(b_i)_{i<\omega}$ in the proof of Theorem 8. In contrast we show that for every $F \in \mathcal{F}$ there is some s_F such that for every $s \geq s_F$ in step $s+1$ we can assure that replacements do not violate the property to represent an element of F, i.e. it is possible to change entries of β_s to obtain $\beta_{s+1}\restriction(s+1)$, such that we have $F_{\beta_s} \subseteq F_{\beta_{s+1}\restriction(s+1)}$, where

$$F_{(q_i)_{i<s+1}} = \{\, \sigma \in \{-s-1, \ldots, s+1\}^{s+1} \mid \\ \sigma \text{ represents an element of } F \text{ w.r.t. } (q_i)_{i<s+1} \,\}.$$

Let $F \in \mathcal{F}$, then there are q and m coprime, such that F is generated by $\frac{q}{m}$. Let $h \in \mathbb{N}$ be such that all prime factors of q or m are less or equal to p_h. We let $s_F \in \mathbb{N}$ be such that all b_i having powers of a prime below p_h as denominator have stabilized up to stage s_F and the exponents occurring in the prime factorizations of q and m are $\leq s_F$.

We may assume that only the j-th component $\beta_s(j) = \frac{1}{p_\ell^{n_{\ell,s}}}$ for some $\ell > h$ has to be replaced by some integer w. Thus, for all $\sigma \in F_{\beta_s}$ we want to make sure

$$\sum_{\substack{i=0,\\ i\neq j}}^{s} \sigma(i)\beta_s(i) + \sigma(j)w \in F.$$

For this, it suffices to show that $\sigma(j)(w-\beta_s(j)) \in F$. By the Chinese Remainder Theorem there exists some integer w such that for all $i < \ell$ we have $1 \equiv p_\ell^{n_{\ell,s}} w \mod p_i^s$. With this there is some integer z such that

$$\sigma(j)\left(w - \beta_s(j)\right) = \frac{\sigma(j)}{p_\ell^{n_{\ell,s}}}\left(p_\ell^{n_{\ell,s}} w - 1\right) = z\, \frac{\sigma(j)}{p_\ell^{n_{\ell,s}}} \prod_{i<\ell} p_i^s.$$

Because $\ell > h$ we obtain that $\sigma(j)$ divided by $p_\ell^{n_{\ell,s}}$ is an integer and moreover q is a factor of $\prod_{i<\ell} p_i^s$. All integer-multiples of q are members of F. In a nutshell, enumerating $\{\sigma \in \mathbb{Z}^{<s_F} \mid \sigma \circ 0^{s_F - |\sigma|} \in F_{\beta_{s_F}}\}$ and all elements of F_{β_s} for $s \geq s_F$ yields the set of all representations of elements of F w.r.t. $(b_i)_{i<\omega}$. ◀

▶ Remark. The statement of Theorem 15 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 $\sigma \cdot \beta\restriction_{|\sigma|-1} = \sigma' \cdot \beta\restriction_{|\sigma'|-1} \Leftrightarrow \sigma \cdot \beta\restriction_{|\sigma|-1} - \sigma' \cdot \beta\restriction_{|\sigma'|-1} = 0 \Leftrightarrow$

$\sum_{i=0}^{\ell}(w_i - v_i)b_i = 0 \Leftrightarrow (w_0 - v_0, w_1 - v_1, \ldots, w_\ell - v_\ell) \in \langle 0 \rangle_\beta$. 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 16.** *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.*

Proof. Fix any generating sequence $\beta := (b_i)_{i<\omega}$ for G_R. Assume, by way of contradiction, that for some $F = \left\langle \dfrac{m'}{m} \right\rangle$ and $F' = \left\langle \dfrac{m''}{m'''} \right\rangle$, where $m, m', m'', m''' \in \mathbb{Z}$ and $m, m''' > 0$, F_β is r.e. and F'_β is co-r.e; without loss of generality, assume that $m''' = m$. It will be shown that this implies the existence of a strictly increasing recursive enumeration $i_0, i_1, i_2, \ldots$ such that $p_{i_j}^{-1} \in G_R$ for all j. For all j, let i_j be the first ℓ found such that $i_j > i_{j'}$ for all $j' < j$ and there is some $\sigma \in \mathbb{Z}^{<\omega}$ such that the following conditions are satisfied.

1. $(m' p_\ell \sigma) \cdot \beta\restriction_{|\sigma|-1} \in F_\beta$.
2. For all $i \in \{1, \ldots, p_\ell - 1\}$, $(m'' i \sigma) \cdot \beta\restriction_{|\sigma|-1} \notin F'_\beta$.

The Martin-Löf randomness of R implies that there are arbitrarily large primes p with $p^{-1} \in G_R$. For each $p^{-1} \in G_R$ such that $p > m$, there is some $\sigma_0 \in \mathbb{Z}^{<\omega}$ with $\sigma_0 \cdot \beta\restriction_{|\sigma_0|-1} = p^{-1}$, and so $m' p \sigma_0 \cdot \beta\restriction_{|\sigma_0|-1} = m' \in \langle F \rangle$. Moreover, for all $i \in \{1, \ldots, p-1\}$, since $p \nmid i$ and $p \nmid m$, one has $m'' i \sigma_0 \cdot \beta\restriction_{|\sigma_0|-1} = m'' i p^{-1} \notin \langle F' \rangle$. Hence i_j is defined for all j. Furthermore, suppose some prime p_ℓ and $\sigma_1 \in \mathbb{Z}^{<\omega}$ satisfy Conditions 1 and 2. Condition 1 implies that $m' p_\ell \sigma_1 \cdot \beta\restriction_{|\sigma_1|-1} \in \left\langle \dfrac{m'}{m} \right\rangle$, and so

$$p_\ell \sigma_1 \cdot \beta\restriction_{|\sigma_1|-1} \in \langle m^{-1} \rangle. \tag{1}$$

Condition 2 implies that $m'' \sigma_1 \cdot \beta\restriction_{|\sigma_1|-1} \notin \left\langle \dfrac{m''}{m} \right\rangle$, and so

$$\sigma_1 \cdot \beta\restriction_{|\sigma_1|-1} \notin \langle m^{-1} \rangle. \tag{2}$$

It follows from (1) and (2) that if $\sigma_1 \cdot \beta\restriction_{|\sigma_1|-1} = \dfrac{q}{r}$ for some relatively prime integers q and r with $r > 0$, then $q \neq 0$, $r \nmid m$ and $p_\ell \mid r$. Consequently, $p_\ell^{-1} \in G_R$, as required. But the existence of a strictly increasing recursive enumeration $i_0, i_1, i_2, \ldots$ such that $p_{i_j}^{-1} \in G_R$ for all j contradicts Proposition 7. ◀

▶ **Notation 17.** *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 $G_R\}$.*

▶ **Theorem 18.** *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.*

Proof. We will reuse the generating sequence $\beta := (b_i)_{i<\omega}$ for G_R constructed in the proof of Theorem 15. For all $i, t \in \mathbb{N}$, let $b_{i,t}$ denote the t-th approximation to the $(i+1)$-st element of β. Define a learner M on any text T as follows. Let s be the length of the text segment seen so far. First, let $a_0, \ldots, a_\ell$ be all the positive integers such that for every $i \in \{0, \ldots, \ell\}$, there is some $\sigma \in \mathrm{content}(T[s])$ for which $\sigma = (a_i)$. If no such a_i exists, then M just outputs a default index, say an r.e. index for the set of representations for $\langle 1 \rangle$. Otherwise, M uses $q' := \gcd(a_0, \ldots, a_\ell)$ as its current guess for the numerator of the target subgroup's generating element. Next, define an approximation $m_{s,t}$ to the denominator of the target subgroup for every $t \geq s$ as follows. Consider every element of $\mathrm{content}(T[s])$ of the shape $(0, \ldots, 0, q'p_i^{h_i}, 0, \ldots, 0)$, where (1) $\gcd(q', p_i) = 1$, (2) $q'p_i^{h_i}$ is the only non-zero coordinate of the element and it occurs in the $(j+1)$-st position, (3) $b_{j,t} = p_i^{-h'_i}$ for some $h'_i \geq h_i$, and (4) h_j is the smallest number h'' such that $\left(0, \ldots, 0, q'p_i^{h''}, 0, \ldots, 0\right) \in \mathrm{content}(T[s])$ (as before, $q'p_i^{h''}$ is the only non-zero coordinate and it occurs in the $(j+1)$-st position). Let $m_{s,t}$ be the product of all factors $p_i^{h'_j - h_j}$ such that p_i, h'_j and h_j satisfy items 1 to 4; if there is no such factor, then set $m_{s,t} = 1$. M outputs an index e such that W_e enumerates all $\sigma \in \mathbb{Z}^{<\omega}$ such that for some $t \geq s$ and $t' \geq s$, $\sum_{i=0}^{|\sigma|-1} \sigma(i) b_{i,t} \in \left\langle \dfrac{q'}{m_{s,t'}} \right\rangle$.

It will be verified that M is indeed a behaviourally correct learner for $\mathcal{F}_\beta$. Let $F := \left\langle \dfrac{q}{m} \right\rangle$ be any finitely generated subgroup of G_R, where q and m are relatively prime natural numbers, and let T be any text for F_β. Since every integer in F is a multiple of q and T must contain (q), it follows that after seeing a sufficiently long segment $T[s_1]$ of T, M will always correctly guess that the numerator of the target subgroup's generating element is equal to q.

Suppose $m = r_0^{h_0} \ldots r_k^{h_k}$ for some positive integers $h_0, \ldots, h_k$ and primes $r_0, \ldots, r_k$ with $r_0 < \ldots < r_k$. For all $i \in \{0, \ldots, k\}$, T contains an element of the shape $\Big(0, \ldots, 0, qr_i^{h''_i}, 0, \ldots,$ $0)$, where, if the $(j+1)$-st coordinate of this element is the only non-zero entry, then $b_j = r_i^{-h'_i}$ for some h'_i with $h'_i - h''_i = h_i$. Consequently, for sufficiently large s_2, $r_0^{h_0} \ldots r_k^{h_k}$ divides $m_{s_2,t}$ whenever $t \geq s_2$ ($m_{s_2,t}$ may be divisible by other prime powers as well). Let $j_0, \ldots, j_k$ be such that for all $i \in \{0, \ldots, k\}$, $b_{j_i} = r_i^{-h'''_i}$ for some $h'''_i \geq 1$. Fix $s_3 > \max(\{s_1, s_2\})$ such that

i. for all $s \geq s_3$ and all $j \in \mathbb{N}$, if $b_{j,s} = p_i^{-e}$ for some $e \geq 1$ and prime $p_i \leq \max(\{q, r_k\})$, then $b_{j,s} = b_j$ (in other words, all entries of β that are equal to p_i^{-e} for some $e \geq 1$ and $p_i \leq \max(\{q, r_k\})$ have stabilised at stage s); in particular, $b_{j_i,s} = b_{j_i}$ for all $i \in \{0, \ldots, k\}$;
ii. $s_3 > \max(\{i, e\})$ for all prime powers p_i^e that are factors of either q or m.

First, it will be shown that $W_{M(T[s])} \subseteq F_\beta$ if $s \geq s_3$. Fix any $s \geq s_3$ and $t \geq s$. By the choice of s_3, $r_0^{h_0} \ldots r_k^{h_k}$ divides $m_{s,t}$. Suppose $m_{s,t} = r_0^{h_0} \ldots r_k^{h_k} g_0^{c_0} \ldots g_{\ell'}^{c_{\ell'}}$ for some positive integers $c_0, \ldots, c_{\ell'}$ and primes $g_0, \ldots, g_{\ell'}$ that do not divide q or m. Consider any $\sigma \in \mathbb{Z}^{<\omega}$ such that

$$\sum_{i=0}^{|\sigma|-1} \sigma(i) b_{i,s'} \in \left\langle q r_0^{-h_0} \cdots r_k^{-h_k} g_0^{-c_0} \cdots g_{\ell'}^{-c_{\ell'}} \right\rangle \tag{3}$$

for some $s' \geq s$. It may be assumed without loss of generality that for any $p' \in \{r_0, \ldots, r_k, g_0, \ldots, g_{\ell'}\}$, $\sum_{i=0}^{|\sigma|-1} \sigma(i) b_{i,s'} \notin \left\langle q p' r_0^{-h_0} \ldots r_k^{-h_k} g_0^{-c_0} \ldots g_{\ell'}^{-c_{\ell'}} \right\rangle$. Let $d_0, \ldots, d_{\ell'}$ be such that for all $i \in \{0, \ldots, \ell'\}$, $b_{d_i,s} = b_{d_i,s'} = g_i^{-c'_i}$ for some $c'_i \geq c_i$; by the preceding assumption, $d_i \in \{0, \ldots, |\sigma| - 1\}$ for all $i \in \{0, \ldots, \ell'\}$. We show that

$$\sum_{i=0}^{|\sigma|-1} \sigma(i) b_i \in \left\langle q r_0^{-h_0} \cdots r_k^{-h_k} \right\rangle; \tag{4}$$

this will establish that $W_{M(T[s])} \subseteq F_\beta$.

The following relation will be established:

$$\sum_{i=0}^{|\sigma|-1} \sigma(i) b_i \in \left\langle q r_0^{-h_0} \cdots r_k^{-h_k} g_0^{-c'_0} \ldots g_{\ell'}^{-c'_{\ell'}} \right\rangle. \tag{5}$$

It suffices to show that for every $i \in \{0, \ldots, |\sigma|-1\}$, $(b_i - b_{i,s'})\sigma(i) \in \left\langle q r_0^{-h_0} \cdots r_k^{-h_k} g_0^{-c'_0} \cdots g_{\ell'}^{-c'_{\ell'}} \right\rangle$; this fact, combined with (3), will establish (5).

Pick any $i \in \{0, \ldots, |\sigma| - 1\}$; without loss of generality, assume that $b_i \neq b_{i,s'}$. By the Martin-Löf randomness of R, it may be assumed that every $(i+1)$-st entry of β (for any $i \in \mathbb{N}$) is either equal to $p_j^{-n'_j}$ for some $n'_j \geq 1$ or equal to some integer p' such that the $(i+1)$-st coordinate of β is changed exactly once from some value $p_{j'}^{-n''_{j'}}$ (where $n''_{j'} \geq 1$) to p'; in addition, for any two terms of β of the shape $p_{i_1}^{-n'_{i_1}}$ and $p_{i_2}^{-n'_{i_2}}$, where $n'_{i_1} \geq 1$ and $n'_{i_2} \geq 1$, $i_1 \neq i_2$. Thus $b_{i,s'} = p_j^{-n'_j}$ and $b_i = w_i$ for some $j \in \mathbb{N}, n'_j \geq 1$ and $w_i \in \mathbb{Z}$.

Case 1: $p_j \notin \{r_0, \ldots, r_k, g_0, \ldots, g_{\ell'}\}$. Then

$$\begin{aligned}(b_i - b_{i,s'})\,\sigma(i) &= \left(w_i - p_j^{-n'_j}\right)\sigma(i) \\ &= \left(w_i p_j^{n'_j} - 1\right) \cdot \sigma(i) \cdot p_j^{-n'_j}.\end{aligned}$$

By Conditions i and ii, as well as by the choice of w_i (as given in the proof of Theorem 15), every prime power factor of q must divide $w_i p_j^{n'_j} - 1$; in particular, q divides $w_i p_j^{n'_j} - 1$. Furthermore, by (3) and the following two facts: (a) $p_j \notin \{r_0, \ldots, r_k, g_0, \ldots, g_{\ell'}\}$ and (b) p_j does not divide $b_{i',s'}^{-1}$ for all $i' \neq i$ with $b_{i',s'}^{-1} \in \mathbb{N}$, one has $\sigma(i) \cdot p_j^{-n'_j} \in \mathbb{Z}$. Therefore

$$\begin{aligned}(b_i - b_{i,s'})\,\sigma(i) &= \left(w_i p_j^{n'_j} - 1\right) \cdot \sigma(i) \cdot p_j^{-n'_j} \\ &\in \langle q \rangle \\ &\subseteq \left\langle q r_0^{-h_0} \cdots r_k^{-h_k} g_0^{-c'_0} \cdots g_{\ell'}^{-c'_{\ell'}} \right\rangle.\end{aligned}$$

Case 2: $p_j \in \{r_0, \ldots, r_k, g_0, \ldots, g_{\ell'}\}$. By Condition i, $p_j \in \{g_0, \ldots, g_{\ell'}\}$; suppose $p_j = g_{i'}$ for some $i' \in \{0, \ldots, \ell'\}$, so that $n'_j = c'_{i'}$. As in Case 1,

$$\begin{aligned}(b_i - b_{i,s'})\,\sigma(i) &= \left(w_i - g_{i'}^{-c'_{i'}}\right)\sigma(i) \\ &= \left(w_i g_{i'}^{c'_{i'}} - 1\right) \cdot \sigma(i) \cdot g_{i'}^{-c'_{i'}}.\end{aligned}$$

Conditions i and ii, together with the choice of w_i, imply that q divides $w_i g_{i'}^{-c'_{i'}} - 1$. Thus, as before,

$$\begin{aligned}(b_i - b_{i,s'})\,\sigma(i) &= \left(w_i g_{i'}^{c'_{i'}} - 1\right) \cdot \sigma(i) \cdot g_{i'}^{-c'_{i'}} \\ &\in \left\langle q g_{i'}^{-c'_{i'}} \right\rangle \\ &\subseteq \left\langle q r_0^{-h_0} \cdots r_k^{-h_k} g_0^{-c'_0} \cdots g_{\ell'}^{-c'_{\ell'}} \right\rangle.\end{aligned}$$

This establishes (5). Now if $\sum_{i=0}^{|\sigma|-1} \sigma(i)b_i \in \left\langle qr_0^{-h_0} \cdots r_k^{-h_k} g_0^{-c'_0} \ldots g_{\ell'}^{-c'_{\ell'}} \right\rangle \setminus \left\langle qr_0^{-h_0} \cdots r_k^{-h_k} \right\rangle$, then there must be a least $i'' \in \{0, \ldots, \ell'\}$ such that $b_{d_{i''},s'} = b_{d_{i''}} = g_{i''}^{-c'_{i''}}$. But since content$(T)$ contains $(0, \ldots, 0, qg_{i''}^{c''}, 0, \ldots, 0)$, where the $(d_{i''}+1)$-st position is the only non-zero entry and $c'_{i''} - c'' = c_{i''} \geq 1$, $g_{i''}^{c_{i''}}$ must then be a factor of m, a contradiction. Hence $\sum_{i=0}^{|\sigma|-1} \sigma(i)b_i \in \left\langle qr_0^{-h_0} \cdots r_k^{-h_k} \right\rangle$.

Furthermore, since $m_{s,t''} = m$ for sufficiently large $t'' \geq s$ and for any given l, there is some $t' \geq s$ with $b_{i,t'} = b_i$ whenever $i \leq l$, one also has that $F_\beta \subseteq W_{M(T[s])}$. Thus $W_{M(T[s])} = F_\beta$, as required. ◀

The next result shows, in contrast to Theorem 18, 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 19.** *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.*

Proof. Assume, by way of contradiction, that such a learner N did exist. By Proposition 14, one could then find a locking sequence γ for N on the set $\mathbb{Z}_\beta$ of representations of $\mathbb{Z}$ with respect to β. We show that this implies the existence of a strictly increasing recursive enumeration $i_0, i_1, i_2, \ldots$ such that for all j, $p_{i_j}^{-1} \in G_R$. The enumeration $i_0, i_1, i_2, \ldots$ is defined as follows. For each j, let i_j be the first ℓ' found such that $\ell' > i_{j'}$ for all $j' < j$ and there is a sequence $\delta \in (\mathbb{Z}^{<\omega})^*$ satisfying the following conditions.

1. $N(\gamma \circ \delta) \neq N(\gamma)$.
2. For all $\sigma \in$ content(δ), $p_{\ell'}\sigma \in \mathbb{Z}_\beta$.

Note that Condition 2 is semi-decidable because $\mathbb{Z}_\beta$ is r.e. By the Martin-Löf randomness of R, there exist infinitely many p such that $p^{-1} \in G_R$. For each such p, since N must explanatorily learn $\langle p^{-1} \rangle_\beta$, $W_{N(\gamma)} = \mathbb{Z}_\beta \subset \langle p^{-1} \rangle_\beta$ and content$(\gamma) \subseteq \mathbb{Z}_\beta \subset \langle p^{-1} \rangle_\beta$, there exists some $\delta \in \left(\langle p^{-1} \rangle_\beta\right)^*$ such that $N(\gamma \circ \delta) \neq N(\gamma)$. Furthermore, for each $\sigma \in$ content(δ), one has

$$\begin{aligned}
(p\sigma) \cdot \beta_{|\sigma|-1} &= p(\sigma \cdot \beta_{|\sigma|-1}) \\
&\in p\langle p^{-1} \rangle \\
&\subseteq \mathbb{Z}.
\end{aligned}$$

Thus i_j is defined for all j. It remains to show that for all j, $p_{i_j}^{-1} \in G_R$. To see this, one first observes that by the locking sequence property of γ, if δ is the sequence found together with i_j satisfying Conditions 1 and 2, then $N(\gamma \circ \delta) \neq N(\gamma)$ implies that there exists some $\sigma \in$ content(δ) with $\sigma \notin \mathbb{Z}_\beta$; in other words, $\sigma \cdot \beta_{|\sigma|-1} \notin \mathbb{Z}$. By Condition 2, $p_{i_j}\sigma \in \mathbb{Z}_\beta$ and therefore $\sigma \cdot \beta_{|\sigma|-1}$ must be of the shape $qp_{i_j}^{-1} \in G_R$ for some $q \in \mathbb{Z}$ that is coprime to p_{i_j}. Consequently, $p_{i_j}^{-1} \in G_R$, as required. But by Proposition 7, the existence of the enumeration $i_0, i_1, i_2, \ldots$ would contradict the fact that R is Martin-Löf random. Hence $\mathcal{F}_\beta$ cannot be explanatorily 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 10. Slightly abusing the notation defined in Notation 17, 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 20.** *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.*

Proof. We will use the fact that any finitely generated subgroup of $G_R/\mathbb{Z}$ is finite[3] (see, for example, [26, page 106]). Let $\beta := (b_i)_{i<\omega}$ be the generating sequence for $G_R/\mathbb{Z}$ constructed in the proof of Theorem 10; as was shown in the proof of this theorem, equality is r.e. with respect to β, that is, $E := \{(\sigma,\sigma') \in \mathbb{Z}^{<\omega}\times\mathbb{Z}^{<\omega} \mid \sum_{i=0}^{|\sigma|-1}\sigma(i)b_i - \sum_{j=0}^{|\sigma'|-1}\sigma'(j)b_j \equiv 0 \ (mod\ 1)\}$ is r.e. Then for any finitely generated subgroup F of $G_R/\mathbb{Z}$ with elements $x_0,\ldots,x_k$, if σ_i is a representation for x_i for all $i \in \{0,\ldots,k\}$, then $F_\beta = \bigcup_{0\leq i\leq k}\{\tau \in \mathbb{Z}^{<\omega} \mid (\sigma_i,\tau) \in E\}$ is r.e. Define a learner M on any text T as follows. On input $T[s]$, M outputs an r.e. index for the closure under equality of all $\sigma \in \text{content}(T[s])$, that is, $W_{M(T[s])} = \{\tau \in \mathbb{Z}^{<\omega} \mid (\exists\sigma \in \text{content}(T[s]))[(\sigma,\tau) \in E]\}$. Let F be any finitely generated subgroup of $G_R/\mathbb{Z}$, and suppose M is fed with a text T for F_β. By construction, M always conjectures a set that is contained in F_β. Furthermore, since F is finite, there is a sufficiently large s such that for all $x \in F$, content$(T[s])$ contains some σ with $\sum_{i=0}^{|\sigma|-1}\sigma(i)b_i \equiv x \ (mod\ 1)$. Thus, as M always conjectures a set that is closed under equality with respect to β, it follows that for all $s' \geq s$, M on $T[s']$ will conjecture F_β. ◀

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 19.

▶ **Theorem 21.** *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 19, 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 22.** *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* **Ex**$[K]$*-learnable.*

---

[3] This may be seen as follows. Suppose $F = \left\langle \frac{p}{q} \right\rangle$ for some relatively prime $p,q \in \mathbb{N}$. Then for all $n \in \mathbb{N}$, there are $n' \in \mathbb{Z}$ and r with $0 \leq r < q$ such that $\frac{np}{q} = \frac{n'q+r}{q} \equiv \frac{r}{q}$ $(mod\ 1)$.

Proof. Let β be any generating sequence for G_R satisfying the hypothesis of the theorem. Define an $\mathbf{Ex}[K]$ learner M as follows. On input $a_0 \circ \ldots \circ a_n$, where $a_i \in \mathbb{Z}^{<\omega} \cup \{\#\}$ for all $i \in \{0, \ldots, n\}$, oracle K is first used to determine a representation ρ of a generator for the subgroup generated by $\{a_i \cdot \beta_{|a_i|-1} \mid 0 \leq i \leq n \wedge a_i \notin \{\varepsilon, \#\}\}$. This can be done in a recursive fashion. We first identify the indices $i_0, \ldots, i_\ell \in \{0, \ldots, n\}$ (if any) such that $a_i \notin \{\varepsilon, \#\}$ and $(a_i, \mathbf{0}) \notin E_\beta$ (here $\mathbf{0}$ denotes any zero vector); if no such index exists, then let ρ be any representation of 0. Set $\rho_0 = a_{i_0}$. Having defined ρ_k, use oracle K to determine relatively prime integers i, j such that $(i\rho_k, ja_{i_{k+1}}) \in E_\beta$; without loss of generality, assume that $j \geq 1$. Then search for some $\rho' \in \mathbb{Z}^{<\omega}$ with $(j\rho', \rho_k) \in E_\beta$, and set $\rho_{k+1} = \rho'$. Assuming inductively that ρ_k represents a generator for the subgroup generated by $\{a_{i_p} \cdot \beta_{|a_{i_p}|-1} \mid 0 \leq p \leq k\}$, one deduces from the relations $(i\rho_k, ja_{i_{k+1}}) \in E_\beta$ and $(j\rho', \rho_k) \in E_\beta$ that

$$\begin{aligned} a_{i_{k+1}} \cdot \beta_{|a_{i_{k+1}}|-1} &= \frac{i}{j}\rho_k \cdot \beta_{||\rho_k||-1} \\ &= \frac{i}{j} j\rho' \cdot \beta_{|\rho'|-1} \\ &= i\rho' \cdot \beta_{|\rho'|-1}. \end{aligned}$$

Hence $a_{i_{k+1}} \cdot \beta_{|a_{i_{k+1}}|-1} \in \langle \rho' \cdot \beta_{|\rho'|-1} \rangle$. Since $\rho_k \cdot \beta_{|\rho_k|-1} \in \langle \rho' \cdot \beta_{|\rho'|-1} \rangle$, it follows from the induction hypothesis that for all $l \leq k$, $a_{i_l} \cdot \beta_{|a_{i_l}|-1} \in \langle \rho' \cdot \beta_{|\rho'|-1} \rangle$. Thus, setting $\rho = \rho_{k+1}$, $\rho \cdot \beta_{|\rho|-1}$ generates the subgroup generated by $\{a_i \cdot \beta_{|a_i|-1} \mid 0 \leq i \leq n \wedge a_i \notin \{\varepsilon, \#\}\}$.

M now outputs the least $e \leq n$ (if any such e exists) such that the following hold:

1. content$(a_0 \ldots a_n) \subseteq W_e$.
2. For all $\tau \in W_{e,n}$, there is some integer q such that $(\tau, q\rho) \in E_\beta$.

If there is no $e \leq n$ satisfying all of the above conditions, then M outputs a default index, say 0. Suppose M is fed with a text for the set of representations of some finitely generated subgroup F. Then M will identify a generator g such that $F = \langle g \rangle$ in the limit; Condition 1 ensures that in the limit, M will conjecture a set W_e such that $\langle g \rangle_\beta \subseteq W_e$, while Condition 2 ensures that in the limit, M will not overgeneralise, that is, it will not output a set containing elements not in $\langle g \rangle_\beta$. Hence M explanatorily learns F_β relative to oracle K. ◀

We recall from Theorem 10 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. Equivalently, we ask whether the collection of all r.e. sets of pairs (σ, σ') for which equality modulo 1 holds with respect to any given generating sequence for G_R can be learnt; it turns out that this class is not even behaviourally correctly learnable. 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 23.** *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.*

Proof. Assume, by way of contradiction, that $\mathcal{E}_0$ has a behaviourally correct learner N. Using a standard type of argument in inductive inference, we will build a limiting recursive generating sequence β for G_R and a text T for $E_\beta := \{(\sigma, \sigma') \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta_{|\sigma|-1} \equiv$

$\sigma' \cdot \beta_{|\sigma'|-1}$ $(mod\ 1)\}$ such that E_β is r.e. and N on T outputs some wrong conjecture for E_β infinitely often, that is, there are infinitely many s for which $W_{N(T[s])} \neq E_\beta$.

The basic construction of β follows the proof of Theorem 10, the main difference being that at various stages of the construction, one searches for some sequence Γ to extend the current text segment T_s such that N on $T_s \circ \Gamma$ conjectures some r.e. set containing a pair $(\sigma, \sigma') \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega}$ such that σ and σ' are both of the shape $(0, \ldots, 0, 1)$, where $|\sigma| \neq |\sigma'|$ and σ, σ' are both longer than any $\tau \in \text{content}(T_s \circ \Gamma)$; one may then ensure that $W_{N(T_s \circ \Gamma)}$ is a wrong conjecture by setting the $|\sigma'|$-th position of β to 0 and the $|\sigma|$-th position of β to p^{-1} for some fixed prime p with $p^{-1} \in G_R$. The constructions of β and T are given in more detail below. The approximations of β and T at stage s will be denoted by β^s and T_s respectively. Fix some prime p such that $p^{-1} \in G_R$.

1. Set $T_0 = \varepsilon$ and $\beta^0 = \varepsilon$.
2. At stage $s+1$, let γ be a generating sequence for G_R that extends a prefix of β^s and is defined as in Theorem 10, so that equality modulo 1 with respect to γ is r.e. In other words, one builds γ in increasing segments by searching at every stage t a new element $p_j^{-n_{j,t}} \in G_{R^t}$ such that $n_{j,t} \geq 1$, where R^t is the t-th approximation to R, and adding $p_j^{-n_{j,t}}$ as a new term to the current approximation of γ. Furthermore, for every ℓ such that the ℓ-th term of the current approximation of γ does not belong to G_{R^t}, the ℓ-th term of γ is permanently set to 0. Note that an r.e. index for E_γ can be uniformly computed from β^s. Now search for some $\delta \in (E_\gamma \cup \{\#\})^*$ such that $W_{N(T_s \circ \delta)}$ enumerates a pair (σ, τ) satisfying the following:
   a. $|\sigma| \neq |\tau|$.
   b. $|\sigma| > |\beta^s|$ and $|\tau| > |\beta^s|$.
   c. For all $(\eta, \eta') \in \text{content}(\delta)$, $|\sigma| > \max(\{|\eta|, |\eta'|\})$ and $|\tau| > \max(\{|\eta|, |\eta'|\})$.
   d. The first $|\sigma| - 1$ (resp. $|\tau| - 1$) terms of σ (resp. τ) are equal to 0 while the last term of σ (resp. τ) is equal to 1.

   Since E_γ is r.e. by construction, N must behaviourally correctly learn E_γ. Moreover, since every term of γ is either an element of G_R of the shape $p_i^{-n_i}$ for some $n_i \geq 1$ or equal to 0, Proposition 7 implies that γ has infinitely many terms equal to 0. Hence such δ and (σ, τ) must eventually be found.

   Without loss of generality, assume that $|\sigma| < |\tau|$. Now let β^{s+1} be the sequence of length $|\tau| + 1$ such that the $(|\tau| + 1)$-st position of β^{s+1} is equal to $p_i^{-n_{i,t}}$ for the least $t \geq s$ such that for some minimum i, $n_{i,t} \geq 1$ and β^s does not contain $p_i^{-n_{i,t}}$, the $|\tau|$-th position of β^{s+1} is p^{-1} and the terms of β^{s+1} between the $|\sigma|$-th and $(|\tau| - 1)$-st positions inclusive are all equal to 0, and the terms of β^{s+1} between the $(|\beta^s| + 1)$-st and the $(|\sigma| - 1)$-st positions inclusive are equal to the respective terms of the $(s+1)$-st approximation of γ; furthermore, all the terms of β^{s+1} are corrected up the $(s+1)$-st approximation, that is, every term of β^{s+1} belongs to $G_{R^{s+1}}$ and is either equal to 0 or is of the shape $p_i^{-n_i}$ for some $n_i \geq 1$. Let Γ be a string whose range consists of all $(\sigma, \sigma') \in \{-s-1, -s, \ldots, s, s+1\}^{<s+2} \times \{-s-1, -s, \ldots, s, s+1\}^{<s+2}$ such that $\sigma \cdot \beta^{s+1}_{|\sigma|-1} = \sigma' \cdot \beta^{s+1}_{|\sigma'|-1}$, and set $T_{s+1} = T_s \circ \delta \circ \Gamma$.

Set $T = \lim_{s\to\infty} T_s$ and $\beta = \lim_{s\to\infty} \beta^s$ (more precisely, for each $i \in \mathbb{N}$, $T(i) = \lim_{s\to\infty} T_s(i)$ and $\beta(i) = \lim_{s\to\infty} \beta^s(i)$). Arguing as in the proof of Theorem 10, the set E_β is r.e.; in addition, the range of T is precisely equal to E_β. On the other hand, by construction N on T infinitely often outputs an r.e. index for some set not equal to E_β. Hence N cannot be a behaviourally correct learner for $\mathcal{E}_0$. ◀

In contrast to Theorem 23, we present a positive learnability result for the collection of all co-r.e. sets of pairs of representations of G_R for which equality holds with respect to any generating sequence for G_R. 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 24.** *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.*

Proof. Define a K-recursive learner M for $\mathcal{E}_1$ as follows. On input γ, M first guesses the minimum e such that the $(e+1)$-st term of the generating sequence is non-zero; it takes e to be the smallest $e' \leq |\gamma|$ such that $(\mathbf{0}, I_{e'+1}(1)) \notin \mathrm{content}(\gamma)$ (where $\mathbf{0}$ denotes the zero vector of length 1; $I_{e+1}(1)$ denotes the vector of length $e+1$ whose first e coordinates are 0 and whose last coordinate is 1); if no such e' exists, then M outputs a default index, say an r.e. index for $\emptyset$. Based on the $(e+1)$-st term b_e of the generating sequence and content(γ), M calculates some of the remaining terms of this sequence as a multiple of b_e. For each $(\sigma,\tau) \in \mathrm{content}(\gamma)$ such that there are $d \in \mathbb{N}$, $q \in \mathbb{Z}$ and $r \in \mathbb{Z}^+$ with $\sigma = I_{e+1}(q)$, $\tau = I_{d+1}(r)$, $d \neq e$ and $\gcd(q,r) = 1$, the $(d+1)$-st term b_d of the generating sequence is $\frac{qb_e}{r}$. Let $e_0,\ldots,e_\ell$ be all the numbers such that for each $i \in \{0,\ldots,\ell\}$, M has determined a rational number q_i for which the (e_i+1)-st term of the generating sequence equals $q_i b_e$ (in particular, there is a j with $e_j = e$). M finds all pairs $(\sigma_0,\sigma'_0),\ldots,(\sigma_{\ell'},\sigma'_{\ell'}) \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega}$ for which all non-zero positions of σ_i and σ'_i belong to $\{e_0,\ldots,e_\ell\}$ and $\sum_{j=0}^{\ell} \sigma_i(e_j) \cdot q_j \neq \sum_{j=0}^{\ell} \sigma'_i(e_j) \cdot q_j$. M outputs the least index $c \leq |\gamma|$ satisfying the following conditions (if such a c exists).

1. $\mathrm{content}(\gamma) \cap W_c = \emptyset$.
2. For all $i \in \{0,\ldots,\ell'\}$, $(\sigma_i,\sigma'_i) \in W_c$.

If no such c exists, then M conjectures $\emptyset$.

Suppose M is presented with a text T for some $E_\beta \in \mathcal{G}_1$, where β is a generating sequence for G_R such that equality is co-r.e. with respect to β. Suppose $\beta = (b_i)_{i<\omega}$. Then M on T will find in the limit the least number e such that $b_e \neq 0$ (since for all $d < e$, $(\mathbf{0}, I_{d+1}(1)) \in \mathrm{content}(T)$). By Condition 1, M will, in the limit, always conjecture a set contained in $(\mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega}) \setminus E_\beta$. Furthermore, for all $(\sigma,\sigma') \notin E_\beta$ and every $i \leq \max(\{|\sigma|,|\sigma'|\})$, there are integers q_i, r_i with $r_i > 0$ and $\gcd(q_i,r_i) = 1$ such that $q_i b_e = r_i b_i$, and therefore content(T) must contain $(I_{e+1}(q_i), I_{i+1}(r_i))$. Since $b_e \neq 0$, one has

$$\sum_{j=0}^{|\sigma|-1} \sigma(j) \cdot \frac{q_j}{r_j} \neq \sum_{j=0}^{|\sigma'|-1} \sigma'(j) \cdot \frac{q_j}{r_j} \Leftrightarrow \sum_{j=0}^{|\sigma|-1} \sigma(j) \cdot \frac{q_j b_e}{r_j} \neq \sum_{j=0}^{|\sigma'|-1} \sigma'(j) \cdot \frac{q_j b_e}{r_j} \Leftrightarrow (\sigma,\sigma') \notin E_\beta,$$

and thus by Condition 2, M will, in the limit, always conjecture a set containing (σ,σ'). M will therefore converge to the least index c satisfying $E_\beta = (\mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega}) \setminus W_c$, as required. ◀

5 Random Subrings of Rationals and Random Joins of Prüfer Groups

We have seen in Section 3 that any Martin-Löf random sequence $R \leq_T K$ gives rise to a random subgroup G_R of rationals such that for some generating sequence β for G_R, equality with respect to β is co-r.e. and another β such that the set of representations of any non-trivial finitely generated subgroup of G_R with respect to β is r.e. The present section will define other random structures with similar properties in an entirely analogous manner.

We begin by defining random subrings of rationals based on Martin-Löf random sequences. First, one observes that for every subring A of $(\mathbb{Q}, +, \cdot)$, there is a set P of primes such that A consists of all fractions $\frac{q}{r}$ with q an integer and r a product of prime powers $p_{i_0}^{n_{i_0}}, p_{i_k}^{n_{i_k}}$ for some $p_{i_0}, \ldots, p_{i_k} \in P$.[4] Let R be any Martin-Löf random sequence that is Turing reducible to K, and let N_R be the subring of $(\mathbb{Q}, +, \cdot)$ such that for all i, $p_i^{-1} \in N_R$ iff $R(i) = 1$. By the preceding observation, N_R consists of all fractions $\frac{p}{q}$ such that p is any integer and q is any product of prime powers $p_{i_0}^{n_{i_0}}, \ldots, p_{i_k}^{n_{i_k}}$ with $R(i_j) = 1$ for all $j \in \{0, \ldots, k\}$ and $n_{i_0}, \ldots, n_{i_k} \geq 0$. By analogy to the definition of a generating sequence for G_R, a *generating sequence for* N_R is any infinite sequence $(b_i)_{i<\omega}$ such that $\langle b_i \mid i < \omega \rangle = N_R$. All the earlier definitions that applied to G_R will be adapted, mutatis mutandis, to the subring N_R.

▶ **Theorem 25.** *Let $R \leq_T K$ be Martin-Löf random w.r.t the Lebesgue measure on 2^ω. Then there is a generating sequence β for N_R such that*

(i) equality with respect to β is co-r.e.;
(ii) for any finitely generated subgroup F of N_R, the set of representations of F with respect to β is co-r.e.;
(iii) the class of all sets of representations of finitely generated subgroups of N_R with respect to β is explanatorily learnable using co-r.e. indices.

Proof. We follow the construction of β in the proof of Theorem 8 with a few modifications. Fix some prime p such that $p^{-1} \in N_R$; the Martin-Löf randomness of R implies that such a p exists. As before, R_s denotes the s-th approximation of R; without loss of generality, assume that for all $t > s$, $R(t) = 0$. The $(i+1)$-st term of β will be denoted by $\beta(i)$, while the s-th approximation of β will be denoted by β^s. For any $\alpha \in \mathbb{Q}^{<\omega}$, the $(i+1)$-st term of α will be denoted by $\alpha(i)$. The construction of β proceeds in stages. For any sequence γ, $i < |\gamma|$ and $r \in \mathbb{Q}$, $\gamma[i \to r]$ denotes the sequence obtained from γ by replacing its $(i+1)$-st term with r.

1. Stage 0. Set $\beta^0 = (1, p^{-1})$.
2. Stage $s + 1$.
   a. Compute $R_{s+1}, R_{s+2}, R_{s+3}, \ldots$ in succession until the least $s' \geq s + 1$ is found such that for some minimum $i \leq s'$, $R_{s'}(i) = 1$ and p_i^{-1} is not a term of β^s. (The Martin-Löf randomness of R implies that such s' and i exist.) Set $\beta^{s+1} \leftarrow \beta^s \circ (p_i^{-1})$. For each p_j such that $j = i$ or β^s contains a term equal to p_j^{-1}, and for $m = 1$ to $m = s + 1$, if p_j^{-m} is not a term of β^s, set $\beta^{s+1} \leftarrow \beta^{s+1} \circ (p_j^{-m})$. (This step ensures that for all $p_j^{-1} \in N_R$, β eventually contains all terms of the shape p_j^{-m}, where $m \geq 1$.) Then go to Step 2.b.
   b. Check for every $j \leq |\beta^{s+1}| - 1$ whether the $(j+1)$-st term of β^{s+1} equals p_ℓ^{-m} for some ℓ and $m \geq 1$ such that $R_{s+1}(\ell) = 0$. Suppose there is a least such j, say j'. Then the $(j' + 1)$-st term of β^{s+1} is replaced with p^{-n} for some $n > s + 1$ that is large enough so

[4] To see this, suppose A is non-trivial (otherwise the statement is immediate); then A must contain 0 as well as 1, and therefore by induction A contains all integers. Let P be the set of primes p such that p has a multiplicative inverse in A. Then for all $p_{i_0}, \ldots, p_{i_k} \in P$ and all integers $q, n_{i_0}, \ldots, n_{i_k}$, one has $qp_{i_0}^{-n_{i_0}} \ldots p_{i_k}^{-n_{i_k}} \in A$. Conversely, let p and q be relatively prime integers such that $q > 0$ and $\frac{p}{q} \in A$. Let x and y be integers with $xp + yq = 1$; then $\frac{1}{q} = \frac{xp+yq}{q} = \frac{xp}{q} + y \in A$. Thus for every prime factor r of q, $\frac{1}{r} \in A$ and so $r \in P$.

that $n > 2n' + s + 1$ for all $p^{-n'}$ occurring in β^{s+1} and all inequalities over the range $\{-s-1,\ldots,0,\ldots,s+1\}$ with respect to β^{s+1} are preserved; in other words, for all pairs $(\sigma,\sigma') \in \{-s-1,\ldots,0,\ldots,s+1\}^{<|\beta^{s+1}|+1} \times \{-s-1,\ldots,0,\ldots,s+1\}^{<|\beta^{s+1}|+1}$ such that $\sigma \cdot \beta^{s+1}_{|\sigma|-1} \neq \sigma' \cdot \beta^{s+1}_{|\sigma'|-1}$, one also has the relation $\sigma \cdot \beta'_{|\sigma|-1} \neq \sigma' \cdot \beta'_{|\sigma'|-1}$, where $\beta' = \beta^{s+1}[j' \to p^{-n}]$. Set $\beta^{s+1} \leftarrow \beta^{s+1}[j' \to p^{-n}]$, then go to Step 2.c.

c. Repeat Step 2.b until no term of β^{s+1} is equal to p_ℓ^{-m} for some $m \geq 1$ and ℓ with $R_{s+1}(\ell) = 0$, then go to Stage $s+2$.

Set $\beta = \lim_{s\to\infty} \beta^s$. Then by Step 2.a, for every $p_j^{-1} \in N_R$ and $n \geq 1$, β contains a term equal to p_j^{-n}. Since, as was observed earlier, every $x \in N_R$ is of the shape $qp_{i_0}^{-n_{i_0}} \ldots p_{i_k}^{-n_{i_k}}$ for some $p_{i_0}^{-1},\ldots,p_{i_k}^{-1} \in N_R$ and $q \in \mathbb{Z}$, β is a generating sequence for N_R. It remains to verify that β satisfies (i), (ii) and (iii).

(i) It suffices to show that $\mathrm{NE}_\beta := \{(\sigma,\sigma') \in \mathbb{Z}^{<\omega} \times \mathbb{Z}^{<\omega} \mid \sigma \cdot \beta_{|\sigma|-1} \neq \sigma' \cdot \beta_{|\sigma'|-1}\}$ is equal to the r.e. set $\bigcup_{s<\omega} \mathrm{NE}^s_\beta$, where $\mathrm{NE}^s_\beta := \{(\tau,\tau') \in \{-s,\ldots,0,\ldots,s\} \times \{-s,\ldots,0,\ldots,s\} \mid |\tau|,|\tau'| \leq |\beta^s| \wedge \tau \cdot \beta^s_{|\tau|-1} \neq \tau' \cdot \beta^s_{|\tau'|-1}\}$. Suppose $(\sigma,\sigma') \in \mathrm{NE}_\beta$. Since R is limiting-recursive, there is an $s_0 \geq \max(\mathrm{content}(\sigma) \cup \mathrm{content}(\sigma'))$ large enough so that whenever $t \geq s_0$, $|\beta^t| \geq \max(\{|\sigma|,|\sigma'|\})$ and the value of $\beta^t(i)$ for every i in the domain of σ or σ' has stabilised, i.e. $\beta^t(i) = \beta(i)$ for all $i < \max(\{|\sigma|,|\sigma'|\})$. It follows that $(\sigma,\sigma') \in \mathrm{NE}^{s_0}_\beta$.

Now suppose $(\tau,\tau') \in \mathrm{NE}^{s_1}_\beta$ for some $s_1 \in \mathbb{N}$, so that $\tau \cdot \beta^{s_1}_{|\tau|-1} \neq \tau' \cdot \beta^{s_1}_{|\tau|-1}$. By Steps 2.b and 2.c in the construction of β, one has $\tau \cdot \beta^t_{|\tau|-1} \neq \tau' \cdot \beta^t_{|\tau'|-1}$ for all $t \geq s_1$. In particular, if $s_2 \geq s_1$ is the least number such that for all $t' \geq s_2$, $\beta^{t'}(i) = \beta(i)$ whenever $i < \max(\{|\sigma|,|\sigma'|\}$, then $\tau \cdot \beta^{s_2}_{|\tau|-1} \neq \tau' \cdot \beta^{s_2}_{|\tau'|-1}$, which is equivalent to $\tau \cdot \beta_{|\tau|-1} \neq \tau' \cdot \beta_{|\tau'|-1}$. Therefore $(\tau,\tau') \in \mathrm{NE}_\beta$.

(ii) Let F be any finitely generated subgroup of N_R that is generated by $\dfrac{r}{r'}$ for some relatively prime integers r and r' with $r' > 0$. Note that every term of β is equal to 1 or is of the shape $p_i^{-m'}$ for some i and $m' \geq 1$, and that β is a one-one sequence. Hence there is a least s_0 such that for all $j \geq s_0$, $\beta(t) \notin F$; furthermore, the Martin-Löf randomness of R implies that s_0 can be chosen so that β_{s_0} contains a term of the shape $p^{-n'}$ for some $n' \in \mathbb{N}$ with $p^{n'} \nmid r'$. Fix some $s_1 \geq s_0$ such that for all $t' \geq s_1$, $|\beta^{t'}| \geq s_0 + 1$ and $\beta^{t'}(i) = \beta(i)$ whenever $i < s_0$. We claim that the complement of the set of representations of F with respect to β, denoted by $\overline{F}_\beta$, is equal to the r.e. set

$$\bigcup_{t \geq s_1} \{\sigma \in \{-t,\ldots,0,\ldots,t\} \times \{-t,\ldots,0,\ldots,t\} \mid |\sigma| \leq |\beta^t| \wedge \sigma \cdot \beta^t_{|\sigma|-1} \notin F\}.$$

That the latter set contains $\overline{F}_\beta$ follows from the fact that for all $\sigma \in \overline{F}_\beta$, there is an s_2 such that whenever $t \geq s_2$, $|\beta^t| \geq |\sigma|$ and $\beta^t(i) = \beta(i)$ for all $i < |\sigma|$.

Now consider any $\sigma \in \{-t,\ldots,0,\ldots,t\} \times \{-t,\ldots,0,\ldots,t\}$ and $t \geq s_1$ such that $|\sigma| \leq |\beta^t|$ and $\sigma \cdot \beta^t_{|\sigma|-1} \notin F$. It will be shown that $\sigma \in \overline{F}_\beta$. Consider all $i_0,\ldots,i_k \in \{0,\ldots,|\sigma|-1\}$ such that for each $j \in \{0,\ldots,k\}$, there is some $t' > t$ with $\beta^{t'}(i_j) \neq \beta^t(i_j)$. It may be assumed without loss of generality that $\sigma(i_j) \neq 0$ for all $j \in \{0,\ldots,k\}$ (for if $\sigma(i_j) = 0$, then any difference between the value of $\beta^t(i)$ and $\beta^{t'}(i)$ would have no effect on whether $\sigma \in \overline{F}_\beta$). By Steps 2.b and 2.c in the construction of β, there are $n_0,\ldots,n_k > t$ with $n_{i+1} > 2n_i + t$ for all $i \in \{0,\ldots,k-1\}$ such that $\{\beta(i_j) \mid 0 \leq j \leq k\} = \{p^{-n_i} \mid 0 \leq i \leq k\}$. Without loss of generality, assume that $\beta(i_j) = p^{-n_j}$ for all $j \in \{0,\ldots,k\}$. Then $\sum_{j=0}^k \sigma(i_j)\beta(i_j) = \sum_{j=0}^k \sigma(i_j)p^{-n_j}$. Since $0 < |\sigma(i_j)| \leq t$, $n_j > t$ and $n_{j+1} > 2n_j + t$, there is an $n'' \in \mathbb{N}$ such that $\sum_{j=0}^k \sigma(i_j)p^{-n_j}$ equals $qp^{-n''}$ for some $q \in \mathbb{Z}$ that is coprime to p and $n'' > 2n'''$ for the largest n''' such that $p^{-n'''}$ is a term of β^t (such a term exists by the choice of s_0).

Thus $\sigma \cdot \beta_{|\sigma|-1}$ is of the shape $\frac{r''}{r'''}$ for some relatively prime integers r'' and r''' such that $p^{n''}$ divides r'''. Since β^t contains a term $p^{-n'}$ such that $p^{n'} \nmid r'$ (where, as stated at the beginning of the proof, r and r' are relatively prime integers with $r' > 0$ such that $\frac{r}{r'}$ is a generator of F), it follows that $p^{n''} \nmid r'$ and therefore $\sigma \cdot \beta_{|\sigma|-1} \notin F$. Consequently, $\sigma \in \overline{F}_\beta$.

(iii) We first observe the following. Suppose T is any text for F_β, where $F = \langle rq^{-1} \rangle$ for some relatively prime integers r, q with $q > 0$.

(I) Since $\beta(0) = 1$, the value of r can be determined in the limit from T by taking the greatest common divisor of all elements w such that $(w) \in \mathrm{content}(T)$.

(II) For every prime power factor $p_i^{n_i}$ of q, there is some i' such that $\beta(i') = p_i^{-n_i}$, and therefore $I_{i'+1}(r) \in \mathrm{content}(T)$.

(III) There is a least j such that for all $j' > j$, $\beta(j')$ is of the shape $p_\ell^{-n'}$ for some prime p_ℓ and $n' \geq 1$ with $rp_\ell^{-n'} \notin F$; in particular, $I_{j'+1}(r) \notin \mathrm{content}(T)$.

(IV) By (ii), there is a minimum s_0 such that $\overline{F}_\beta = \bigcup_{t \geq s_0} \{\sigma \in \{-t, \ldots, 0, \ldots, t\} \times \{-t, \ldots, 0, \ldots, t\} \mid |\sigma| \leq |\beta^t| \wedge \sigma \cdot \beta^t_{|\sigma|-1} \notin F\}$.

Define a learner M as follows. On input δ, M determines the greatest common divisor d of the set of all w such that $(w) \in \mathrm{content}(\delta)$ (if no such w exists, then M just sets $d = 0$). Next, M identifies all $j_0, \ldots, j_\ell$ such that $I_{j_k+1}(d) \in \mathrm{content}(\delta)$ for all $k \in \{0, \ldots, \ell\}$, and it approximates $\beta(j_k)$ by determining the least $t' \geq |\delta|$ such that $|\beta^{t'}| \geq j_k + 1$ and setting the approximation to be $\beta^{t'}(j_k)$. For each $k \in \{0, \ldots, \ell\}$, let $p_{i_k}^{-n_{i_k}}$ be the current approximation of $\beta(j_k)$, where $n_{i_k} \geq 0$. M then takes $dp_{h_0}^{-m_0} \ldots p_{h_{\ell'}}^{-m_{\ell'}}$ to be its current guess for a generator of F, where $\{p_{h_0}, \ldots, p_{h_{\ell'}}\} = \{p_{i_0}, \ldots, p_{i_\ell}\}$ and for each $k \in \{0, \ldots, \ell'\}$, m_k is the largest number e' such that $p_{h_k}^{-e'} \in \{p_{i_0}^{-n_{i_0}}, \ldots, p_{i_\ell}^{-n_{i_\ell}}\}$. Having determined a guess for F, M finds the least $s_0 \leq |\delta|$ such that the $|\delta|$-th approximation of

$$G_{s_0} := \bigcup_{t \geq s_0} \{\sigma \in \{-t, \ldots, 0, \ldots, t\} \times \{-t, \ldots, 0, \ldots, t\} \mid |\sigma| \leq |\beta^t| \wedge \sigma \cdot \beta^t_{|\sigma|-1} \notin F\},$$

denoted by $G_{s_0,|\delta|}$, satisfies $G_{s_0,|\delta|} \cap \mathrm{content}(\delta) = \emptyset$. If no such s_0 exists, then M outputs a co-r.e. index for $\emptyset$; otherwise, M outputs a co-r.e. index for $\mathbb{Z}^{<\omega} \setminus G_{s_0}$. By (I), (II) and (III), M on T will correctly identify a generator for F in the limit. Furthermore, defining s_0 as in (IV), if $s_0 \geq 1$, then content(T) contains some element in $\bigcup_{t \geq s_0 - 1} \{\sigma \in \{-t, \ldots, 0, \ldots, t\} \times \{-t, \ldots, 0, \ldots, t\} \mid |\sigma| \leq |\beta^t| \wedge \sigma \cdot \beta^t_{|\sigma|-1} \notin F\}$; thus, for all $s' < s_0$, M will reject $\mathbb{Z}^{<\omega} \setminus G_{s'}$ and conjecture $\mathbb{Z}^{<\omega} \setminus G_{s_0}$ as the correct hypothesis in the limit. ◀

▶ Remark. The explanatory learner M in the proof of (iii) of Theorem 25 is also *conservative* in the sense that for any two text initial segments $T[n_1]$ and $T[n_2]$ for any F_β, where $n_1 < n_2$, $M(T[n_1]) \neq M(T[n_2])$ only if $\mathrm{content}(T[n_2]) \not\subseteq \overline{W}_{M(T[n_1])}$ (we assume that M's hypothesis space is some fixed numbering $\overline{W}_0, \overline{W}_1, \overline{W}_2, \ldots$ of co-r.e. subsets of $Z^{<\omega}$).

We recall that for any prime p, a *Prüfer p-group* (denoted by $\mathbb{Z}(p^\infty)$) may be defined as the quotient of the group of all rational numbers whose denominator is a power of p by $\mathbb{Z}$. Regarding $\mathbb{Z}(p^\infty)$ as a subgroup of $(\mathbb{Q}/\mathbb{Z}, +)$, we define a *random join of Prüfer groups* based on any given Martin-Löf random sequence R as follows. As before, suppose R is Martin-Löf random and is Turing reducible to K. Then the subgroup P_R is defined to be the join of all $\mathbb{Z}(p_{i_0}^\infty), \mathbb{Z}(p_{i_1}^\infty), \mathbb{Z}(p_{i_2}^\infty), \ldots$ such that for all $j \in \mathbb{N}$, the i_j-th bit of R is 1. In other words, P_R consists of every fraction (modulo 1) whose denominator is a product of finitely many powers of primes belonging to $\{p_{i_0}, p_{i_1}, p_{i_2}, \ldots\}$. The next result is the analogue of Theorem 25 for P_R; the proof is entirely similar to that of Theorem 25.

▶ **Theorem 26.** *Let $R \leq_T K$ be Martin-Löf random w.r.t the Lebesgue measure on 2^ω. Then there is a generating sequence β for P_R such that*

(i) equality with respect to β is co-r.e.;
(ii) for any finitely generated subgroup F of P_R, the set of representations of F with respect to β is co-r.e.;
(iii) the class of all sets of representations of finitely generated subgroups of P_R with respect to β is explanatorily learnable using co-r.e. indices.

By adapting the proofs of Theorems 10, 20 and 19, one obtains an almost "symmetrical" version of Theorem 26 for P_R.

▶ **Theorem 27.** *Let $R \leq_T K$ be Martin-Löf random w.r.t the Lebesgue measure on 2^ω. Then there is a generating sequence β for P_R such that*

(i) equality with respect to β is r.e.;
(ii) for any finitely generated subgroup F of P_R, the set of representations of F with respect to β is r.e.;
(iii) the class of all sets of representations of finitely generated subgroups of P_R with respect to β is **Bc***-learnable but not* **Ex***-learnable.*

6 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.

A question deserving further attention is the extent to which the choice of the generating sequence for a randomly generated subgroup G of rationals influences the learnability of its finitely generated subgroups; in particular, is there a generating sequence β for G such that every non-trivial finitely generated subgroup of G has an r.e. representation with respect to β and the class of all such representations with respect to β is not even behaviourally correctly learnable? We also did not 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 Janis M. Bārzdiņš. Two theorems on the limiting synthesis of functions. In Janis M. Bārzdiņš, editor, *Theory of Algorithms and Programs I*, volume 210 of *Proceedings of the Latvian State University*, pages 82–88. Latvian State University, Riga, 1974. In Russian.
2 Reinhold Baer. Abelian groups without elements of finite order. *Duke Mathematical Journal*, 3(1):68–122, 1937.
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 Rodney G. Downey and Denis R. Hirschfeldt. *Algorithmic randomness and complexity.* Theory and Applications of Computability. Springer, New York, 2010.

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

8 Mark Fulk. A study of inductive inference machines. Ph.D. Thesis, SUNY/Buffalo, 1985.

9 E. Mark Gold. Language identification in the limit. *Information and Control* 10:447–474, 1967.

10 Misha Gromov. Random walk in random groups. *Geometric and Functional Analysis* 13(1):73–146, 2003.

11 Matthew Harrison-Trainor, Bakhadyr Khoussainov and Daniel Turetsky. Effective aspects of algorithmically random structures. *Computability*, to appear. Manuscript available at http://homepages.ecs.vuw.ac.nz/ harrism1/papers/random-structures.pdf.

12 Asylkhan N. Khisamiev. Constructive Abelian groups. In: Yuri L. Ershov, Sergei S. Goncharov, Anil Nerode & Jeff B. Remmel (Eds.), *Handbook of Recursive Mathematics*, volume 2, *Studies in Logic and the Foundations of Mathematics*, volume 139. North-Holland, Amsterdam, 1998, pages 1177–1231.

13 Bakhadyr 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) (CSL-LICS '14)*, July 14–18, 2014, Vienna, Austria, pages 56:1–56:9.

14 Bakhadyr Khoussainov. A quest for algorithmically random infinite structures, II. *Logical Foundations of Computer Science - International Symposium, LFCS 2016*, Deerfield Beach, FL, USA, January 4–7, 2016. Proceedings. Springer Lecture Notes in Computer Science 9537, pages 159–173, 2016.

15 Ming Li and Paul Vitányi. A new approach to formal language theory by Kolmogorov complexity. *SIAM Journal on Computing*, 24(2):398–410, 1995.

16 Ming Li and Paul Vitányi. *An introduction to Kolmogorov complexity and its applications.* Third edition. Springer, 2008.

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

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

19 André Nies. *Computability and Randomness*, volume 51 of Oxford Logic Guides. Oxford University Press, Oxford, 2009.

20 André Nies and Volkher Scholz. Martin-Löf random quantum states. Manuscript. https://arxiv.org/pdf/1709.08422.pdf.

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

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

23 Hartley Rogers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, New York, 1967.

24 Claus-Peter Schnorr. A unified approach to the definition of a random sequence. *Mathematical Systems Theory,* 5(3):246–258, 1971.

25 Robert Soare. *Recursively Enumerable Sets and Degrees. A Study of Computable Functions and Computably Generated Sets.* Springer-Verlag, Heidelberg, 1987.

26 Elias M. Stein and Rami Shakarchi. Fourier Analysis: An Introduction (Princeton Lectures in Analysis, Volume 1). Princeton University Press, 41 William Street, Princeton, New Jersey 08540, 2003.

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

28 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.

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

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

31 Vladimir Vovk, Alexander Gammerman and Craig Saunders. Machine-learning applications of algorithmic randomness. *Proceedings of the Sixteenth International Conference on Machine Learning*, ICML 1999, Bled, Slovenia, June 27–30, 1999, pages 444–453, 1999.