THE JOURNAL OF SYMBOLIC LOGIC
Volume 76, Number 4, Dec. 2011

THE ADDITIVE GROUP OF THE RATIONALS DOES NOT HAVE AN AUTOMATIC PRESENTATION

TODOR TSANKOV

Abstract. We prove that the additive group of the rationals does not have an automatic presentation. The proof also applies to certain other abelian groups, for example, torsion-free groups that are p-divisible for infinitely many primes p, or groups of the form $\bigoplus_{p\in I} \mathbf{Z}(p^\infty)$, where I is an infinite set of primes.

§1. Introduction. Consider the basic algorithm for adding two integers that we are taught in elementary school: write the two numbers in decimal, align them on the right, and add them digit by digit (using an addition table), carrying only one bit of information from one position to the next. What is remarkable about this procedure is that we can add two very long integers, digit by digit, using only local information and a bounded amount of memory. It becomes interesting to understand what other mathematical structures admit an encoding such that one can perform the operations using a similarly simple algorithm. This idea is formalized by the notion of an *automatic* (or *FA-presentable*) structure which is defined as follows.

Fix a finite alphabet Σ and denote by Σ^* the set of all finite words formed by letters of Σ. A *language* is a subset of Σ^*. A language is called *regular* if there exists a finite automaton that recognizes it. The following definition was first considered by Hodgson [5] and the basic theory of automatic structures was later developed by Khoussainov and Nerode [7].

DEFINITION 1. A countable, relational structure $(M; R_1, \dots, R_k)$, where M is the universe of the structure and $R_1, \dots, R_k$ are the relations, is called *automatic* if there exists a regular language $D \subseteq \Sigma^*$ and a bijection $g\colon D \to M$ such that the relations $g^{-1}(R_1), \dots, g^{-1}(R_k)$ are also regular.

In order to make sense of what it means for $g^{-1}(R_i)$ to be regular, one has to specify how to represent $(\Sigma^*)^n$ as a set of words in a finite alphabet. The standard approach is to use *padding*: add a special symbol $\diamond$ to the alphabet and embed $(\Sigma^*)^n$ into $((\Sigma \cup \{\diamond\})^n)^*$ by appending $\diamond$s at the end of the shorter words in the n-tuple so that all words become of equal length. Everywhere below where we mention regular subsets of $(\Sigma^*)^n$, we are using this convention. For more details, see any of the papers [7, 9, 6]. In Definition 1, one can relax the condition on g and allow

Received May 24, 2010.
Key words and phrases. automatic structures, FA-presentable, abelian groups, additive combinatorics.

© 2011, Association for Symbolic Logic
0022-4812/11/7604-0013/$2.10

it to be only a surjection but then equality in M has to be regular. Also, one can include in the definition structures with function symbols by considering the graphs of the functions as relations. This will be important for us because we will be mostly concerned with algebraic structures.

Automatic structures are also attractive from another point of view: since the class of regular languages is stable under Boolean operations and projections, one readily sees that for any first order formula $\phi(\bar{x})$, the set $\{\bar{a} \in D^n : D \models \phi(\bar{a})\}$ is a regular language and, moreover, one can construct algorithmically an automaton recognizing it starting from the formula ϕ and the automata for the basic relations. In particular, the first order theories of automatic structures are decidable. One can also extend the first order language by the additional quantifiers "there exist infinitely many" and "there exist m modulo n" and keep this decidability property. For all of this and some additional background, see Rubin's thesis [14] or the recent survey Khoussainov–Minnes [6].

The condition of admitting an automatic presentation turns out to be rather restrictive. If one allows rich algebraic structure in the language, then often the only automatic structures are the trivial ones. For example, every automatic Boolean algebra is either finite or a finite power of the algebra of finite and co-finite subsets of $\mathbf{N}$ and all automatic integral domains (in the language of rings) are finite (Khoussainov–Nies–Rubin–Stephan [9]; for more detailed information on automatic rings, see also Nies–Thomas [12]).

Even if one considers simpler algebraic structures such as groups, the definition is still too restrictive: Oliver and Thomas [13] observed, as a consequence of Gromov's theorem about finitely generated groups of polynomial growth and a theorem of Romanovskiĭ classifying the virtually polycyclic groups with decidable first order theory, that a finitely generated group has an automatic presentation (in the sense of Definition 1) iff it is virtually abelian. This was extended by Nies and Thomas [12] who showed that every finitely generated subgroup of an automatically presentable group is virtually abelian.

However, for finitely generated groups, there is a convenient alternative. A different notion of an *automatic group*, in which the alphabet is a set of generators for the group, each word represents the corresponding product of generators, and one further requires that equality in the group and right multiplication by a generator be verifiable by automata, was introduced by Cannon and Thurston in the 1980s (see Epstein et al. [1] for the precise definition and more details) and has led to a rich and interesting theory. In order to avoid confusion, we will adopt the terminology from [12] and call a group with an automatic presentation in the sense of Definition 1 *FA-presentable*.

In view of the remarks above, it seems that the natural class of groups for which one wants to consider FA-presentability is the class of abelian groups and this is where we will concentrate our attention from now on. There are already some interesting known examples. Finite groups are of course FA-presentable and an infinite direct sum of copies of $\mathbf{Z}/p\mathbf{Z}$ is also FA-presentable. By using the idea of "addition with carry," one can construct presentations for $\mathbf{Z}$ and $\mathbf{Z}(p^\infty) = \{x \in \mathbf{Q}/\mathbf{Z} : \exists k\ p^k x = 0\}$. The class of FA-presentable groups is stable under finite sums (so all finitely generated abelian groups are FA-presentable) and one can combine a presentation of $\mathbf{Z}$ with a presentation of $\bigoplus_{p|n} \mathbf{Z}(p^\infty)$ to construct

a presentation of $\mathbf{Z}[1/n] = \{a/n^k \in \mathbf{Q}\colon a, k \in \mathbf{Z}\}$. The class of FA-presentable abelian groups is also stable under taking finite extensions and, more interestingly, under "automatic amalgamation" (Nies–Semukhin [11]) which provides some further examples. Currently, there are fairly few known ways to show that an abelian group does not admit an automatic presentation: the only abelian groups with a decidable first order theory known to not be FA-presentable were the ones containing a free abelian group of infinite rank [9]. In this paper, we describe some new restrictions on possible automatic presentations of abelian groups. The following is our main theorem which answers a question of Khoussainov (see, e.g., [8]).

THEOREM 2. *The following groups are not FA-presentable*:

(i) $(\mathbf{Q}, +)$, *or, more generally, any torsion-free abelian group that is p-divisible for infinitely many primes p*;

(ii) $(\mathbf{Q}/\mathbf{Z}, +)$, *or, more generally, any group of the form* $\bigoplus_{p\in I} \mathbf{Z}(p^\infty)$, *where I is an infinite set of primes.*

Some partial results providing restrictions on possible automatic presentations of $\mathbf{Q}$ and $\mathbf{Q}/\mathbf{Z}$ had been proved by F. Stephan (see [10]).

The ideas for the proof of Theorem 2 are combinatorial. Our main tool is Freiman's structure theorem for sets with a small doubling constant.

The organization of the paper is as follows. In Section 2, we discuss some preliminary notions and facts from additive combinatorics; in Section 3, we prove Theorem 2 for the case of the rationals; and finally, in Section 4, we indicate how to modify the proof in order to obtain the other instances of Theorem 2.

Below, $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{R}$ will denote the sets of the natural numbers, the integers, the rationals, and the reals, respectively. If A is a finite set, $|A|$ denotes its cardinality.

Acknowledgements. I am grateful to B. Khoussainov for pointing out an error in a preliminary draft of this paper, making many useful comments, and suggesting some references.

Addendum. Recently, Braun and Strüngmann, using the methods introduced in this paper, have shown that every FA-presentable, torsion-free, abelian group is an extension of a finite rank free group by a sum of finitely many $\mathbf{Z}(p^\infty)$. In particular, this characterizes exactly the FA-presentable subgroups of $\mathbf{Q}$.

§2. Preliminaries from additive combinatorics.

Our main reference for results in additive combinatorics is the book by Tao and Vu [16].

Let Z be an abelian group. We will be interested in finite sets $A \subseteq Z$ such that their doubling $A + A = \{a_1 + a_2\colon a_1, a_2 \in A\}$ is small, i.e., $|A + A| \leq C|A|$ for some constant C (such sets naturally arise from automatic presentations of Z as we shall see shortly). Typical sets with this property are arithmetic progressions and, more generally, multi-dimensional arithmetic progressions. By a remarkable theorem of Freiman [2], these are essentially the only examples. In order to state the theorem, we recall a few basic definitions. A *generalized arithmetic progression* (or just a progression, for short) in an abelian group Z is a pair (P, ϕ), where P is a finite subset of Z and ϕ is an affine map from a parallelepiped in $\mathbf{Z}^d$ onto P, i.e.,

$$P = \{v_0 + \sum_{i=1}^{d} a_i v_i\colon 0 \leq a_i < N_i \text{ for } i = 1, \ldots, d\},$$

where $v_0, v_1, \ldots, v_d \in Z$ and $N_1, \ldots, N_d \in \mathbf{N}$ (and of course, $\phi(a_1, \ldots, a_d) = v_0 + \sum_{i=1}^{d} a_i v_i$). We will often suppress ϕ if it is clear from the context. The number d is called the *rank* of the progression. Progressions of rank 1 are just ordinary arithmetic progressions. A progression is called *proper* if ϕ is injective. Also, if $N = (N_1, \ldots, N_d)$, we will write $[0, N)$ for the parallelepiped $\prod_{i=1}^{d} [0, N_i)$ in $\mathbf{Z}^d$ (and similarly for $(-N, N)$, etc.). If we put $v = (v_1, \ldots, v_d)$ and $a = (a_1, \ldots, a_d) \in \mathbf{Z}^d$, then we will write $a \cdot v$ for the sum $\sum_{i=1}^{d} a_i v_i \in Z$. With this notation, we can concisely write the progression P as $v_0 + [0, N) \cdot v$.

THEOREM (Freiman's theorem). *Let Z be a torsion-free abelian group and $C > 0$ be a constant. Then there exist constants K and d such that whenever a finite set $A \subseteq Z$ satisfies $|A + A| \leq C|A|$, there exists a proper progression P of rank at most d that contains A and $|P|/|A| \leq K$.*

The original proof of the theorem can be found in [2]; for a modern treatment due to Ruzsa, see Ruzsa [15], Tao–Vu [16, Chapter 5], or the self-contained exposition Green [3].

We will also need some basic notions and facts from the geometry of numbers. Recall that a *lattice* in $\mathbf{R}^d$ is a discrete subgroup. The *rank* of a lattice is the dimension of the subspace of $\mathbf{R}^d$ that it spans. A subset $B \subseteq \mathbf{R}^d$ is *symmetric* if $B = -B$. We denote by vol the d-dimensional Lebesgue measure. The following lemma goes back to Minkowski and follows for example from [16, Theorem 3.30]; in order to avoid introducing additional notation, we supply the easy proof.

LEMMA 3. *Let $B \subseteq \mathbf{R}^d$ be a bounded, open, symmetric, convex set and $\Gamma < \mathbf{R}^d$ be a lattice of full rank. If $\mathrm{vol}(B) < (2^d/d!)\,\mathrm{vol}(\mathbf{R}^d/\Gamma)$, then $\dim \mathrm{span}\, B \cap \Gamma < d$.*

PROOF. Suppose, towards contradiction, that $B \cap \Gamma$ contains d linearly independent vectors $v_1, \ldots, v_d$. By applying an invertible linear transformation of $\mathbf{R}^d$ (which will scale both sides of the given inequality by the same factor), we can assume that $(v_1, \ldots, v_d)$ is in fact the standard basis of $\mathbf{R}^d$. In particular, after this transformation, Γ will contain $\mathbf{Z}^d$ and hence, $\mathrm{vol}(\mathbf{R}^d/\Gamma) \leq 1$. On the other hand, B, being convex and symmetric, will contain the polyhedron with vertices $\pm v_1, \ldots, \pm v_d$ which has volume $2^d/d!$. This contradicts the hypothesis. ⊣

One last fact which we will need is that the intersection of a convex set with a lattice can be efficiently contained in a progression of rank equal to the rank of the lattice. More precisely, the following holds (see [16, Lemma 3.36]).

LEMMA 4. *Let B be a bounded, convex, symmetric, open set in $\mathbf{R}^d$ and let $\Gamma < \mathbf{R}^d$ be a lattice of rank r. Then there exist a tuple $w = (w_1, \ldots, w_r) \in \Gamma^r$ of linearly independent vectors in $\mathbf{R}^d$ and a tuple $N = (N_1, \ldots, N_r)$ of positive integers such that*

$$(-N, N) \cdot w \subseteq B \cap \Gamma \subseteq (-r^{2r}N, r^{2r}N) \cdot w.$$

§3. Proof for the case of the rationals. Let Σ be a finite alphabet. If $L \subseteq \Sigma^*$, denote by $L^{\leq n}$ the set of words in L of length not greater than n. We will need the following two basic lemmas (for proofs, see, for example, [9]). The first one is a general fact about the growth of regular languages and the second is a version of the pumping lemma particularly suitable for studying automatic structures.

LEMMA 5. *Let $L \subseteq \Sigma^*$ be a regular language. Then there exists a constant C such that $|L^{\leq n+1}| \leq C|L^{\leq n}|$ for all n.*

LEMMA 6. *Let L_1, L_2 be languages over a finite alphabet and $R \subseteq L_1 \times L_2$ be a regular relation such that the sections $R_x = \{y \in L_2 : (x, y) \in R\}$ are finite. Then for all $(x, y) \in R$, $\mathrm{len}(y) \leq \mathrm{len}(x) + k$, where k is the number of states of an automaton recognizing R.*

Suppose now that $(Z, +)$ is an FA-presentable abelian group and fix some automatic presentation of it; that is, fix a regular language $D \subseteq \Sigma^*$ and a bijection $g : D \to Z$ such that the preimage under g of the graph of addition is recognizable by an automaton with, say, r states. We will often identify Z and D via g. For example, when we write $A + B$ for some $A, B \subseteq D$, we mean the set $\{g^{-1}(g(a)+g(b)) : a \in A, b \in B\}$. By applying Lemma 6 to the graph of addition, one immediately obtains that $D^{\leq n} + D^{\leq n} \subseteq D^{\leq n+r}$. Also, the graph of the homomorphism $M_p : Z \to Z$ defined by $M_p(x) = px$, where p is an integer, is regular. Let $h(p)$ be the minimal number of states of an automaton recognizing the graph of M_p. (Using the fact that one can compute $M_p(x)$ using no more than $O(\log p)$ additions, one sees that $h(p) = p^{O(1)}$ but we will not need this.) If $A \subseteq Z$, denote by $p^{-1}A$ the set $M_p^{-1}(A)$. If M_p has finite kernel (for example, if Z is torsion-free), Lemma 6 implies that $p^{-1}D^{\leq n} \subseteq D^{\leq n+h(p)}$.

Let $l_0 = \min\{l \in \mathbf{N} : 0 \in D^{\leq l} \text{ and } |D^{\leq l}| \geq 2\}$ and put $A_n = D^{\leq l_0+nr}$ for $n = 0, 1, \ldots$. We summarize the properties of the sets A_n that we have established so far (under the assumption that the homomorphism M_p has a finite kernel). There exist a constant C_1 and a function $h : \mathbf{N} \to \mathbf{N}$ such that:

(i) $0 \in A_0$ and $|A_0| \geq 2$;
(ii) $A_n + A_n \subseteq A_{n+1}$;
(iii) $|A_{n+1}| \leq C_1|A_n|$;
(iv) $p^{-1}A_n \subseteq A_{n+h(p)}$.

The property (iii) follows from Lemma 5. In particular (ii) and (iii) imply that

$$|A_n + A_n| \leq C_1|A_n| \quad \text{for all } n. \tag{3.1}$$

Now we can formulate our main combinatorial result which, by the above observations, implies Theorem 2 for the case of the rationals.

THEOREM 7. *There does not exist a sequence $\{A_n\}_{n\in\mathbf{N}}$ of finite subsets of $\mathbf{Q}$ that satisfy the conditions* (i)–(iv) *above.*

PROOF. We will obtain a contradiction with Freiman's theorem. To that end, we will need a quantitative measure of how efficiently a given additive set is contained in a progression. For a finite additive set A and a rank d, define

$$\theta(A, d) = \min\{|P|/|A| : P \supseteq A \text{ and } P \text{ is a proper progression of rank } \leq d\}.$$

If there is no d-dimensional progression covering A (for example, if $d = 0$), put $\theta(A, d) = \infty$. One property of θ, obvious from the definition, is the following:

$$B \subseteq A \Longrightarrow \theta(A, d) \geq \frac{|B|}{|A|}\theta(B, d). \tag{3.2}$$

The next lemma quantitatively formalizes the observation that if we have a progression of integers all of whose elements are divisible by p for some large prime p and add to it a single element not divisible by p, then in order to contain the resulting set efficiently in a progression, we need to increase its rank. In order to state the

lemma in a slightly more general form that will be useful later, we introduce some notation. If A is a subset of an abelian group, denote by $\langle A\rangle$ the group generated by A.

Recall that if p is a prime, the *p-adic norm* $\|x\|_p$ of $x \in \mathbf{Q}\setminus\{0\}$ is defined by

$$\|x\|_p = p^m \iff x = p^{-m}a/b, \text{ where } a,b \in \mathbf{Z}\setminus p\mathbf{Z} \text{ and } m \in \mathbf{Z},$$

and $\|0\|_p = 0$. Note that the p-adic norm on $\mathbf{Q}$ has the following properties:

$$\begin{aligned} &\{\|x\|_p : x \in \mathbf{Q}\} \text{ has no accumulation points} \\ &\qquad\qquad \text{other than 0 and } \forall x \lim_{m\to\infty} \|p^m x\|_p = 0; \end{aligned} \tag{3.3}$$

$$\|x\|_p = \|-x\|_p \text{ and } \|x+y\|_p \le \max\{\|x\|_p, \|y\|_p\}; \tag{3.4}$$

$$\forall a \in \mathbf{Z} \quad \|ax\|_p < \|x\|_p \Longrightarrow p \mid a. \tag{3.5}$$

For a set $A \subseteq \mathbf{Q}$, let $\|A\|_p = \sup\{\|a\|_p : a \in A\}$. If $V \le \mathbf{Q}$ and $0 < \|V\|_p < \infty$, let $V_{(p)}$ denote the subgroup $\{x \in V : \|x\|_p < \|V\|_p\}$. Note that (3.3)–(3.5) imply the following:

$$\text{for all } A \subseteq \mathbf{Q}, \quad \|\langle A\rangle\|_p = \|A\|_p; \tag{3.6}$$

$$\|x\|_p > \|y\|_p \Longrightarrow \|x+y\|_p = \|x\|_p; \tag{3.7}$$

$$0 < \|V\|_p < \infty \Longrightarrow [V : V_{(p)}] \ge p. \tag{3.8}$$

To see that (3.8) holds, note that if $v \in V$ is such that $\|v\|_p = \|V\|_p$ (which exists by (3.3)), then, by (3.5), the elements $0, v, 2v, \ldots, (p-1)v$ of V are in distinct cosets of the subgroup $V_{(p)}$.

LEMMA 8. *Let $d \ge 1$ be an integer and $p > d!$ be prime. Let Z be an abelian group equipped with a norm $\|\cdot\|_p$ satisfying* (3.3)–(3.5). *Let $A \subseteq Z$ be a finite set with at least 2 elements, and $z \in Z$ be such that $\|z\|_p > \|A\|_p$. Then*

$$\theta(A\cup\{z\}, d) \ge \min\{\frac{p^{1/d}}{4d}, \frac{\theta(A, d-1)}{d^{C_0 d^3}}\}, \tag{3.9}$$

where C_0 is an absolute constant.

PROOF. If $\theta(A\cup\{z\}, d) = \infty$, there is nothing to prove, so suppose that $\theta(A\cup\{z\}, d) < \infty$. Let

$$P = \{v_0 + \sum_{i=1}^{d} a_i v_i : 0 \le a_i < N_i \text{ for } i = 1, \ldots, d\},$$

where $v_0, \ldots, v_d \in Z$, be a proper progression of rank d covering $A\cup\{z\}$ such that $|P|/|A\cup\{z\}| = \theta(A\cup\{z\}, d)$. We will first show that for some $i \ge 1$, $\|v_i\|_p \ge \|z\|_p$. Denote by V_1 the group generated by $v_1, \ldots, v_d$ and suppose, towards a contradiction, that $\|V_1\|_p < \|z\|_p$. We have two cases: either $\|v_0\|_p < \|z\|_p$ or $\|v_0\|_p \ge \|z\|_p > \|V_1\|_p$. In the first case, we obtain that, since $P \subseteq v_0 + V_1$, $\|P\|_p \le \|v_0 + V_1\|_p < \|z\|_p$ which contradicts the fact that $z \in P$. In the second, by (3.7), for every $x \in v_0 + V_1$, $\|x\|_p = \|v_0\|_p > \|A\|_p$ which contradicts the fact that $A \subseteq v_0 + V_1$ and A is non-empty.

Now by reordering $v_1, \ldots, v_d$, we can assume that there exists $k \geq 1$ such that

$$\|v_1\|_p, \ldots, \|v_k\|_p \geq \|z\|_p \text{ and } \|v_{k+1}\|_p, \ldots, \|v_d\|_p < \|z\|_p.$$

Put $M = N_1 N_2 \cdots N_k$. We distinguish the following two cases which will correspond to the two different quantities on the right-hand side of (3.9).

CASE 1. $M < p/k!$. Note that this case is impossible if $d = 1$. Indeed, we showed that $\|v_1\|_p > \|A\|_p$ and since A contains at least two elements, it is easy to see, using (3.5), that if $d = 1$, the interval $[0, N_1)$ must contain two integers whose difference is divisible by p and hence, $M = N_1 \geq p + 1$ (for a similar argument, see Case 2 below). Hence, we can assume that $d \geq 2$.

Write v for the vector $(v_1, \ldots, v_k)$ and N for $(N_1, \ldots, N_k)$. Let $f: \mathbf{Z}^k \to Z$ be the homomorphism $f(x) = x \cdot v$. Put $V = \langle v_1, \ldots, v_k \rangle = f(\mathbf{Z}^k)$. Let

$$\Lambda = \{y \in Z: \|y\|_p < \|z\|_p\}$$

and note that Λ is a subgroup of Z and $A \subseteq \Lambda$. Let also Γ be the lattice in $\mathbf{R}^k$ given by

$$\Gamma = \{x \in \mathbf{Z}^k: f(x) \in \Lambda\}$$

and note that since by (3.3), for all large enough m, $p^m \mathbf{Z}^k \leq \Gamma$, Γ has full rank. Let B be the open, symmetric, convex box $\prod_{i=1}^k (-N_i, N_i)$ in $\mathbf{R}^k$. We have $\mathrm{vol}(B) = (2N_1) \cdots (2N_k) = 2^k M$ and

$$\mathrm{vol}(\mathbf{R}^k/\Gamma) = \mathrm{vol}(\mathbf{R}^k/\mathbf{Z}^k)[\mathbf{Z}^k : \Gamma] \geq p.$$

The first equality follows from the fact that if A is a fundamental domain for $\mathbf{R}^k/\mathbf{Z}^k$ and B is a system of coset representatives for $\mathbf{Z}^k/\Gamma$, then $A + B$ is a fundamental domain for $\mathbf{R}^k/\Gamma$ and the sets $A + b_1$ and $A + b_2$ are disjoint for distinct $b_1, b_2 \in B$. To see that the inequality holds, note that Γ is contained in the kernel of the composition of the surjective homomorphisms

$$\mathbf{Z}^k \xrightarrow{f} V \to V/V_{(p)}$$

and apply (3.8). Applying Lemma 3 and our hypothesis about M yields that $\Gamma \cap B$ is contained in a sublattice of Γ of rank $r < k$. (For the moment, suppose that $k > 1$, so that we can take $r > 0$. We will explain how to deal with the case $k = 1$ later.) By Lemma 4, there exist tuples $N' = (N'_1, \ldots, N'_r)$ of positive integers and $w = (w_1, \ldots, w_r) \in \Gamma^r$ such that $w_1, \ldots, w_r$ are independent in $\mathbf{R}^k$ and

$$(-N', N') \cdot w \subseteq \Gamma \cap B \subseteq (-r^{2r} N', r^{2r} N') \cdot w.$$

From the first inclusion and the independence of $w_1, \ldots, w_r$, we have

$$|(-N', N')| = |(-N', N') \cdot w| \leq |B \cap \Gamma| \leq |B \cap \mathbf{Z}^k| < 2^k M. \tag{3.10}$$

Let P_0 be the progression $\{\sum_{i=k+1}^d a_i v_i : 0 \leq a_i < N_i\}$ and note that $P_0 \subseteq \Lambda$. Then $P = v_0 + P_0 + f([0, N))$. Note that by the properness of P, $|P| = |P_0| \cdot |[0, N)| = M|P_0|$. Let $a^0 = (a_1^0, \ldots, a_k^0) \in [0, N)$ be such that $v_0 + a^0 \cdot v \in \Lambda$ and put $v_0' = a^0 \cdot v$ (since $A \subseteq P \cap \Lambda$, such an a^0 always exists). We have

$$P = v_0 + P_0 + f([0, N)) = v_0 + P_0 + v_0' + f([-a^0, N - a^0)).$$

Note that $v_0 + v_0' + P_0 \subseteq \Lambda$. Hence,

$$\begin{aligned} A \subseteq P \cap \Lambda &= v_0 + v_0' + P_0 + f([-a^0, N - a^0)) \cap \Lambda \\ &= v_0 + v_0' + P_0 + f([-a^0, N - a^0) \cap \Gamma) \\ &\subseteq v_0 + v_0' + P_0 + f(B \cap \Gamma) \\ &\subseteq v_0 + v_0' + P_0 + f((-r^{2r}N', r^{2r}N') \cdot w) \\ &\subseteq v_0 + v_0' + P_0 + (-r^{2r}N', r^{2r}N') \cdot f(w), \end{aligned} \tag{3.11}$$

where $f(w) = ((f(w_1), \dots, f(w_r))$. Denote by Q the progression (3.11). We have that $A \subseteq Q$, $\operatorname{rank} Q = \operatorname{rank} P_0 + r = d - k + r < d$, and by (3.10),

$$\begin{aligned} |Q| &\leq |P_0| \cdot |(-r^{2r}N', r^{2r}N')| \\ &< |P_0| 2^r r^{2r^2} |(-N', N')| \\ &< |P_0| 2^r r^{2r^2} 2^k M < 4^k k^{2k^2} |P|. \end{aligned} \tag{3.12}$$

Now note that if we had $k = 1$ in the beginning, then $B \cap \Gamma = \{0\}$, so if we take $Q = v_0 + v_0' + P_0$, we will again have $A \subseteq Q$, $\operatorname{rank} Q < d$, and the estimate (3.12) will still hold.

Of course, the progression Q need not be proper. However, properness can be achieved at the price of increasing its size. Applying [16, Theorem 3.40] yields that we can include Q in a proper progression Q' of equal or lesser rank and size at most $d^{C_0' d^3}|Q|$ for some absolute constant C_0'. This allows us to conclude that in this case,

$$\begin{aligned} \theta(A \cup \{z\}, d) = \frac{|P|}{|A \cup \{z\}|} &\geq \frac{|Q|}{2|A| 4^k k^{2k^2}} \\ &\geq \frac{|Q'|}{2|A| d^{C_0' d^3} 4^k k^{2k^2}} \\ &\geq \frac{\theta(A, d-1)}{d^{C_0 d^3}} \end{aligned}$$

for an appropriately chosen C_0.

Case 2. $M \geq p/k!$. Then for some $i \leq k$, $N_i \geq (p/k!)^{1/k} \geq (p/d!)^{1/d}$. Without loss of generality, we can assume that $N_1 \geq (p/d!)^{1/d}$. Now fix some $(a_2, \dots, a_d) \in \mathbf{Z}^{d-1}$ and consider the following condition on a_1:

$$a_1 v_1 + v_0 + \sum_{i=2}^{d} a_i v_i \in \Lambda. \tag{3.13}$$

Let $a_1', a_1'' \in \mathbf{Z}$ be two values of a_1 satisfying (3.13). Since $\|v_1\|_p > \|\Lambda\|_p$, by (3.5), we obtain that $p \mid a_1' - a_2''$. Hence the proportion of the numbers a_1 in the interval $[0, N_1)$ for which (3.13) holds is not greater than $\lceil N_1/p \rceil / N_1 \leq \max\{1/N_1, 2/(p+1)\}$. Therefore, by properness,

$$|P \cap \Lambda| / |P| \leq \max\{(p/d!)^{-1/d}, 2/(p+1)\} \leq (p/(2d!))^{-1/d}.$$

Hence in this case,

$$\theta(A \cup \{z\}, d) = \frac{|P|}{|A \cup \{z\}|} \geq \frac{|P|}{2|A|} \geq \frac{|P|}{2|P \cap \Lambda|} \geq \frac{(p/(2d!))^{1/d}}{2} \geq \frac{p^{1/d}}{4d}. \quad \dashv$$

Now we can proceed with the proof of the theorem. Suppose, towards a contradiction, that a sequence of subsets $\{A_n\}$ of $\mathbf{Q}$ satisfying (i)–(iv) does exist. Let $C = \max\{C_0, C_1\}$, where C_0 is the constant from Lemma 8 and C_1 is the constant from (iii). By (3.1) and Freiman's theorem, there exist constants K and d such that $\theta(A_n, d) \leq K$ for all n. Pick inductively a sequence of primes $p_d < p_{d-1} < \cdots < p_0$ satisfying the conditions

$$p_d > (4dCK)^d \quad \text{and} \quad p_{i-1} > p_i C^{h(p_i)d} d^{Cd^4} \text{ for } i = d, d-1, \ldots, 1. \tag{3.14}$$

Define inductively the sequence of integers $n_0 < n_1 < \cdots < n_d$ by

$$n_0 = 0 \quad \text{and} \quad n_i = \min\{n\colon \|A_n\|_{p_i} > \|A_{n_{i-1}}\|_{p_i}\} \quad \text{for } i = 1, \ldots, d.$$

Note that by the properties of the family $\{A_n\}$, $n_i \leq n_{i-1} + h(p_i)$ (indeed, if the norm $\|A_{n_{i-1}}\|_{p_i}$ is achieved for $z \in A_{n_{i-1}}$, then $\|p_i^{-1}z\|_{p_i} > \|z\|_{p_i} = \|A_{n_{i-1}}\|_{p_i}$ and $p_i^{-1}z \in A_{n_{i-1}+h(p_i)}$). Hence,

$$|A_{n_i-1}| \leq C^{h(p_i)-1}|A_{n_{i-1}}|. \tag{3.15}$$

We will prove by induction on i that

$$\theta(A_{n_i}, i) > C^{-1}p_i^{1/d}/(4d) \quad \text{for all } i = 0, \ldots, d. \tag{3.16}$$

Applied for $i = d$, (3.16) will yield a contradiction with the choice of p_d. The case $i = 0$ follows trivially from the definition of θ. Suppose now that $i \geq 1$ and (3.16) holds for $i - 1$ in order to prove it for i. By the induction hypothesis, (3.15), and (3.2),

$$\theta(A_{n_i-1}, i-1) \geq C^{-h(p_i)+1}\theta(A_{n_{i-1}}, i-1) > C^{-h(p_i)}p_{i-1}^{1/d}/(4d). \tag{3.17}$$

By the choice of n_i, there exists $z \in A_{n_i}$ such that $\|z\|_{p_i} > \|A_{n_i-1}\|_{p_i}$. Apply Lemma 8 to the set $A_{n_i-1} \cup \{z\}$ and the prime p_i to obtain

$$\begin{aligned}\theta(A_{n_i}, i) &> C^{-1}\theta(A_{n_i-1} \cup \{z\}, i) \\ &\geq C^{-1}\min\{p_i^{1/d}/(4d), \theta(A_{n_i-1}, i-1)/d^{Cd^3}\}.\end{aligned}$$

The choice of p_{i-1} and (3.17) allow us to conclude that

$$p_i^{1/d}/(4d) \leq \theta(A_{n_i-1}, i-1)/d^{Cd^3}$$

which completes the induction and the proof. $\dashv$

Remark 9. Note that Freiman's theorem gives another way to see that a torsion-free abelian group of infinite rank is not FA-presentable (originally proved in [9]). Indeed, if one considers the sets $D^{\leq n}$ as above, by applying Freiman's theorem, one obtains that there is a constant d such that each $D^{\leq n}$ is contained in a progression of rank d. Since the group generated by a progression of rank d has rank at most $d + 1$, this leads to a contradiction. In fact, for this argument, instead of Freiman's theorem, one can use the much simpler version [16, Lemma 5.13].

§4. Other groups.

4.1. The torsion-free case. The proof above can be used to show that certain other torsion-free abelian groups also do not have an automatic presentation. Recall that an abelian group Z is called *p-divisible* if all of its elements are divisible by p, i.e., for all $x \in Z$, there exists $y \in Z$ such that $py = x$. It is easy to extend the proof in Section 3 to cover all torsion-free groups that are p-divisible for infinitely many p. Let Z be such a group. If Z has infinite rank, then Z is not FA-presentable by [9] (cf. Remark 9 above). Otherwise, Z can be embedded as a subgroup of $\mathbf{Q}^k$ for some finite k. For $x = (x_1, \ldots, x_k) \in \mathbf{Q}^k$, define its p-adic norm by

$$\|x\|_p = \max\{\|x_1\|_p, \ldots, \|x_k\|_p\}.$$

It is easy to check that this norm satisfies (3.3)–(3.5), hence Lemma 8 applies. In order to complete the rest of the proof of Theorem 7, one just has to choose the primes $p_1, \ldots, p_d$ in (3.14) so that Z is p_i-divisible for each i. That can be done because, by assumption, there are infinitely many such primes. This completes the proof of Theorem 2 (i).

4.2. The torsion case. One has to be slightly more careful in the torsion case but the proof in Section 3 still goes through for some torsion groups. Let I be some infinite set of primes and put $T_I = \bigoplus_{p \in I} \mathbf{Z}(p^\infty)$. (In the special case when I is the set of all primes, $T_I = \mathbf{Q}/\mathbf{Z}$.) For $p \in I$, one can define the p-adic norm for $x \in T_I$ by

$$\|x\|_p = \operatorname{ord} \pi_p(x),$$

where $\pi_p \colon T_I \to \mathbf{Z}(p^\infty)$ is the natural projection and $\operatorname{ord} z$ denotes the order of z (with the special agreement that $\operatorname{ord} 0 = 0$). This is not really a norm (in the sense that $\{x \in T_I \colon \|x\|_p = 0\}$ is a non-trivial subgroup of T_I) but it still satisfies (3.3)–(3.5) which is all we need for Lemma 8 to hold.

Freiman's theorem is also available for arbitrary abelian groups (Green–Ruzsa [4]; see also [16, Theorem 5.44]). The only difference is that now in the conclusion of the theorem, one obtains coset progressions instead of ordinary progressions. A *coset progression* in an abelian group Z is a subset of the form $H + P$, where H is a finite subgroup of Z, P is a proper progression as defined previously, and the sum is direct, i.e., every element of $H + P$ can be represented in a unique fashion as a sum $h + p$, where $h \in H$ and $p \in P$. Since every finite subgroup of T_I is cyclic and every finite cyclic group is a one-dimensional progression, every coset progression of rank d in T_I can be written as a proper progression of rank $d + 1$.

The conditions (i)–(iv) for the sets A_n are still satisfied because the homomorphisms $M_p \colon T_I \to T_I$, $x \mapsto px$ have finite kernels for all primes p . Also, one has to ensure that the primes $p_1, \ldots, p_d$ in (3.14) are in the set I which can be achieved because I is infinite. The rest of the proof goes through unchanged.

REFERENCES

[1] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston, ***Word processing in groups***, Jones and Bartlett Publishers, Boston, MA, 1992.

[2] G. A. Freiman, ***Nachala strukturnoi teorii slozheniya mnozhestv***, Kazan. Gosudarstv. Ped. Inst, 1966.

[3] Ben Green, *Structure theory of set addition*, lecture notes available at `http://www.dpmms.cam.ac.uk/~bjg23/notes.html`, 2002.

[4] Ben Green and Imre Z. Ruzsa, *Freiman's theorem in an arbitrary abelian group*, ***Journal of the London Mathematical Society. Second Series***, vol. 75 (2007), no. 1, pp. 163–175.

[5] Bernard R. Hodgson, *On direct products of automaton decidable theories*, ***Theoretical Computer Science***, vol. 19 (1982), no. 3, pp. 331–335.

[6] Bakhadyr Khoussainov and Mia Minnes, *Three lectures on automatic structures*, ***Logic Colloquium 2007*** (F. Delon, U. Kohlenbach, P. Maddy, and F. Stephan, editors), Lecture Notes in Logic, vol. 35, Association for Symbolic Logic, 2010, pp. 132–176.

[7] Bakhadyr Khoussainov and Anil Nerode, *Automatic presentations of structures*, ***Logic and computational complexity*** (***Indianapolis, IN, 1994***), Lecture Notes in Computer Science, vol. 960, Springer, Berlin, 1995, pp. 367–392.

[8] ———, *Open questions in the theory of automatic structures*, ***Bulletin of the European Association for Theoretical Computer Science***, vol. 94 (2008), pp. 181–204.

[9] Bakhadyr Khoussainov, André Nies, Sasha Rubin, and Frank Stephan, *Automatic structures: richness and limitations*, ***Logical Methods in Computer Science***, vol. 3 (2007), no. 2:2, 18 pp. (electronic).

[10] André Nies, *Describing groups*, ***The Bulletin of Symbolic Logic***, vol. 13 (2007), no. 3, pp. 305–339.

[11] André Nies and Pavel Semukhin, *Finite automata presentable abelian groups*, ***Logical foundations of computer science*** (A. Nerode and S. Artemov, editors), Lecture Notes in Computer Science, vol. 4514, Springer, Berlin, 2007, pp. 422–436.

[12] André Nies and Richard M. Thomas, *FA-presentable groups and rings*, ***Journal of Algebra***, vol. 320 (2008), no. 2, pp. 569–585.

[13] Graham P. Oliver and Richard M. Thomas, *Automatic presentations for finitely generated groups*, ***STACS 2005*** (V. Diekert and B. Durand, editors), Lecture Notes in Computer Science, vol. 3404, Springer, Berlin, 2005, pp. 693–704.

[14] Sasha Rubin, ***Automatic structures***, Ph.D. thesis, 2004.

[15] I. Z. Ruzsa, *Generalized arithmetical progressions and sumsets*, ***Acta Mathematica Hungarica***, vol. 65 (1994), no. 4, pp. 379–388.

[16] Terence Tao and Van Vu, ***Additive combinatorics***, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006.

ANALYSE FONCTIONNELLE, BOÎTE 186
UNIVERSITÉ PARIS 6
4 PLACE JUSSIEU
75252 PARIS CEDEX 05, FRANCE

Current address: Equipe de Logique, UFR de Mathématiques, Université Paris Diderot, 75205 Paris CEDEX 13, France

E-mail: todor@math.jussieu.fr