On expansions of the group of integers

Françoise Point (UMons)

BPGMTC, january 14^{th} 2022.

Finite automata

A finite automaton M is a finite state machine given by (Σ, Q, q_0, F, T), where Σ is a finite alphabet, q_0 an initial state, Q a finite set of states, $F \subset Q$ a set of accepting states and T a transition function from $Q \times \Sigma \to Q$ with the convention that $T(q, \lambda) = q$ for λ the empty word.

Let Σ^* be the set of all finite words on Σ. Let $\sigma \in \Sigma^*$ and $a \in \Sigma$, one extends T to $T : Q \times \Sigma^* \to Q$ by setting $T(q, \sigma a) := T(T(q, \sigma), a)$.

The automaton accepts $\sigma \in \Sigma^*$ if $T(q_0, \sigma) \in F$. (We will say that M works on Σ.)

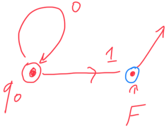
A subset $L \subset \Sigma^*$ is recognized/accepted by M if $L = \{\sigma \in \Sigma^* \colon T(q_0, \sigma) \in F\}$.

Definability and finite automata in the natural numbers

Each natural number n can be written in base $d \geq 2$, so as a finite word in the alphabet $\Sigma := \{0, \ldots, d-1\}$. A subset of $\mathbb{N}$ is d-automatic if it is recognized by a finite automaton M working on Σ.

Let $d = 2$. The study of 2-automatic subsets of $\mathbb{N}$ has been marked by a result of R. Buchi who showed that the sets definable in $(\mathbb{N}, +, V_2)$, where $V_2(n)$ is the highest power of 2 dividing n, are exactly the 2-automatic sets.

Example



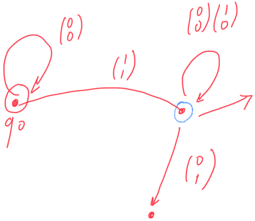
$n \in P_2$ iff $n = 0 \dots 01$

$(n, m) \in graph(V_2)$

iff

$n = 0 \cdots 01010 \dots$

$V_2(n) = 0 \cdots 0100000$



Definability and finite automata in the natural numbers

In fact the original statement of R. Buchi is about $(\mathbb{N}, +, P_2)$, where P_2 is the set of powers of 2, which is incorrect as observed, for instance, by Semenov.

Also, in his review, McNaughton suggested to consider instead the structure $(\mathbb{N}, +, \epsilon_2)$, where $\epsilon_2(n, m)$ holds iff n is a power of 2 which occurs in the binary expansion of m.

This last structure is interdefinable with $(\mathbb{N}, +, V_2)$.

A proof of the corrected result may be found in the master thesis of V. Bruyère.

Regular languages

The class $\mathcal{R}$ of *regular* languages is the smallest class of languages on Σ that contains all finite languages and closed under the following operations: if $L_1, L_2 \in \mathcal{R}$, then

1. $L_1 \cup L_2 \in \mathcal{R}$,
2. $L_1 L_2 := \{\sigma\tau\colon \sigma \in L_1, \tau \in L_2\} \in \mathcal{R}$,
3. $L_1^* := \{\sigma_1 \dots \sigma_n\colon n \in \mathbb{N}, \sigma_i \in L_1, 1 \leq i \leq n\} \in \mathcal{R}$.

Fact: A subset $L \subset \Sigma^*$ is *regular* iff it is accepted by an automaton M working on Σ.

Using that correspondence, one can show that indeed a subset of $(\mathbb{N}, +, 0)$ is recognized by a finite automaton working on $\{0, 1\}$ iff it is definable in $(\mathbb{N}, +, 0, V_2)$. Furthermore that last structure is decidable. Also one can easily replace $(\mathbb{N}, +, 0)$ by $(\mathbb{Z}, +, -, 0, <)$.

Finite-automaton presentable structures, following B. Hodgson and A. Nies

Let $\mathcal{L}$ be a finite language. A first-order (countable) $\mathcal{L}$-structure $\mathcal{M}$ is *FA*-presentable (Finite Automaton) if there is a finite alphabet Σ and a regular language $D \subset \Sigma^*$ such that the elements of the domain can be represented by D and some finite automata can check whether the atomic relations hold in $\mathcal{M}$.

Theorem (Hodgson, 1976)

If a countable structure is *FA*-presentable, then it is decidable.

One uses that the emptiness problem for finite automata is decidable.

Remark: One can extend results on the ring $\mathbb{Z}$ to other Euclidean rings, for instance polynomial rings or rings of formal power series over a finite field. (To treat that last example one needs to work with finite automata accepting infinite words).

Expansions of $(\mathbb{Z}, +, <)$ and of $(\mathbb{R}, +, \cdot, <)$

The theory of $(\mathbb{Z}, +, 0, <)$ satisfies different notions of minimality. Its theory is NIP, dp-minimal, coset-minimal and quasi-o-minimal.
Recall that an ordered group G (non necessarily abelian) is coset-minimal if every definable subset of G is a finite union of cosets of definable subgroups intersected with intervals.
A totally ordered structure is *quasi-o-minimal* if in every elementarily equivalent structure every definable set is a boolean combination of intervals and $\emptyset$-definable sets. It is *essentially quasi-o-minimal* if it has an expansion by constants which is quasi-o-minimal.
Fact: (Point-Wagner) Let G be an ordered group. Then the following is equivalent:

1. $Th(G)$ is essentially quasi-o-minimal.
2. $Th(G)$ is coset-minimal.
3. Every definable subset of a model $\mathcal{G}$ of $Th(G)$ is a finite union of cosets of nG intersected with intervals, for some $n < \omega$.

NIP expansions

Note that $(\mathbb{Z}, +, <, V_2)$ has IP (one can define any finite subset of P_2 using ϵ_2).

$(\mathbb{Z}, +, <, P_2)$ is NIP (see later).

(van den Dries, 1985) $Th(\mathbb{Z}, +, <, P_2)$ is model-complete in the language $\{+, -, <, \mod_n, \lambda_2 \colon n \in \mathbb{N} \setminus \{0, 1\}\}$, where $\lambda_2(x)$ is the largest power of 2 smaller than x.

(Moosa-Scanlon, 2004) $Th(\mathbb{Z}, +, P_2)$ is stable and its definable subsets can be described as follows.

$(\mathbb{Z}, +, P_2)$

Let $(\Gamma, +, -, 0)$ a finitely generated abelian group and F an injective endomorphism of Γ. Let Σ be a finite symmetric subset of Γ containing 0 and denote by Σ^* the set of finite words on Σ. We say that the finite word $\sigma := a_0 \cdots a_n$ represents $a \in \Gamma$ if $a = a_0 + F(a_1) + \ldots + F^n(a_n)$. We use the notation $a = [\sigma]_F$.

Definition (Bell-Moosa/Hawthorne)

Let Σ be as above. Then Σ is a F-spanning set for Γ if

1. any element of Γ can be represented by an element of Σ^*,
2. if $a_1, a_2, a_3 \in \Sigma$, then $a_1 + a_2 + a_3 \in \Sigma + F(\Sigma)$,
3. if $a_1, a_2 \in \Sigma$ are such that for some $b \in \Gamma$, $a_1 + a_2 = F(b)$, then $b \in \Sigma$.

Proposition (Hawthorne)

The structure $(\Gamma, +, F)$ is FA-presentable.

Let $L \subset \Sigma^*$, then L is sparse if L is regular and if the set of words in L of length smaller than or equal to x is bounded by a polynomial function of x. A subset $A \subset \Gamma$ is F-sparse if $A = [L]_{F^r}$ for some sparse $L \subset \Sigma^*$ with Σ a F^r-spanning set, $r > 0$.

Let $a \in \Gamma$, then set $K(a, F) := \{a + F(a) + \cdots + F^n(a) \colon n \in \mathbb{N}\}$.

An elementary F-set is a subset of Γ of the form $a_0 + K(a_1, F^{n_1}) + \ldots + K(a_m, F^{n_m})$, for some $a_0, \ldots, a_m \in \Gamma$ and $n_1, \ldots, n_m \in \mathbb{N}$.
Example: the F-orbit of a
$F^{\mathbb{N}}(a) = \{F^n(a) : n \in \mathbb{N}\} = a + K(Fa - a)$ is an elementary F-set.

Theorem (Moosa-Scanlon 2004/Hawthorne 2021)

Let $A \subset \Gamma$ be F-sparse. Then A is stable in Γ iff A is a boolean combination of elementary F-sets.

Back to expansions of $(\mathbb{Z}, +, -, 0)$

As a consequence, one obtains:

Theorem (Hawthorne 2021–case $d = 2$)

Let $A \subset \mathbb{Z}$. Then A is 2-automatic and stable in $(\mathbb{Z}, +)$ iff A is a boolean combination of elementary 2-sets and cosets of subgroups of $\mathbb{Z}$ iff A is definable in $(\mathbb{Z}, +, P_2)$. In particular the theory of $(\mathbb{Z}, +, P_2)$ is stable.

Independently, Poizat (2014) and then Palacin-Sklinos (2018) proved that:

Theorem (Poizat/Palacin-Sklinos)

The theory of $(\mathbb{Z}, +, P_2)$ is superstable of U-rank ω.

Expansions of fields by multiplicative subgroups

The result of L. van den Dries on the expansion $Th(\mathbb{Z}, +, \leq, P_2)$ was proven using a similar analysis as for $(\mathbb{R}, +, \cdot, 0, 1, \leq, P_2)$ (adding a multiplicative group to the field structure) which was extended later by van den Dries and Gunaydin to expansions of the form $(\mathbb{R}, +, \cdot, 0, 1, \leq, P_2.P_3)$.

Theorem (van den Dries, Gunaydin, 2006, Theorem 1.3)

Let Γ be a dense subgroup of $(\mathbb{R}^{>0})$ and suppose it has the Mann property. Then one can (explicitely) axiomatize the theory of $(\mathbb{R}, \Gamma) := (\mathbb{R}, +, -, \cdot, 0, 1, \Gamma, \{\gamma : \gamma \in \Gamma\})$.

Mann property

Let K be a field and G a subgroup of the multiplicative group of K. Consider equations of the form:

$$r_1x_1 + ... + r_nx_n = 1,$$

withr_i,$1 \leq i \leq n$, in the prime field of K and its solutions in G. A tuple $(g_1, ..., g_n) \in G^n$ is called a non-degenerate solution if for all proper subsets J of of $\{1, ..., n\}$, $\sum_{j \in J} r_j g_j \neq 0$. The group G has the Mann property in K if such equations have only finitely many non-degenerate solutions.

Fact [van der Poorten-Schlickewei, Evertse, Laurent] Any multiplicative group of finite rank in a field of characteristic 0 has the Mann property.

Theorem

Let K be an algebraically closed field of characteristic 0 and let Γ be a finitely generated subgroup of the K-points of some semi-abelian variety defined over K, then the theory of (K, Γ) is stable (Γ is stably embedded).

Theorem (Scanlon-Moosa, 2004)

Consider the structure $(K, +, \cdot, \Gamma)$, where K is an algebraically closed field of characteristic p and Γ is a finitely generated Frobenius submodule of a semi-abelian variety X defined over a finite field. Then the induced structure on Γ is stable and so the theory of (K, Γ) is stable.

How special is P_2?

Let $A \subset \mathbb{N}$, A infinite. Enumerate A as a strictly increasing sequence $A = (a_n)_{n \geq 0}$.
Consider the expansions $(\mathbb{Z}, +, A)$, or $(\mathbb{Z}, +, -A \cup A)$, or $(\mathbb{Z}, +, 0, <, A)$. Which ones are tame?

How does the sequence grows?
Consider the sequence $(\frac{a_{n+1}}{a_n})_{n \in \mathbb{N}}$ and $\limsup_{n \in \mathbb{N}} \frac{a_{n+1}}{a_n}$.
If it is > 1, say that A is lacunary. If $\lim_{n \in \mathbb{N}} \frac{a_{n+1}}{a_n}$ exists in $\mathbb{R} \cup \{+\infty\}$, denote it by θ and call it the Kepler limit.

Recall that (a_n) is a linear recurrence sequence if there are $r_0, \ldots, r_{k-1} \in \mathbb{Q}$, with $k \in \mathbb{N}^{\geq 1}$ minimal, such that for all $n \in \mathbb{N}$,

$$a_{n+k} = \sum_{i=0}^{k-1} r_i a_{n+i}.$$

The polynomial P_A defined by $P_A(X) = X^k - \sum_{i=0}^{k-1} r_i X^i$ is called the *characteristic polynomial* and the elements $a_0, \ldots, a_{k-1}$ the initial conditions.

Lacunary sequences (G. Conant)

A subset $B \subset \mathbb{R}^{>0}$ is geometric if $\{\frac{a}{b} \colon a \geq b \;\&\; a, b \in B\}$ is closed and discrete.

The sequence $A = (a_n) \subset \mathbb{Z}$ is a geometric sparse sequence if

1. there is a function $f : A \to \mathbb{R}^{>0}$ such that $f(A)$ is geometric, and
2. $\sup \{|a - f(a)| \colon a \in A\} \in \mathbb{R}$.

Theorem (G. Conant, 2019)

Let A be a geometric sparse sequence (in $\mathbb{Z}$). Then, the theory of $(\mathbb{Z}, +, A)$ is superstable of Lascar rank ω.

Lacunary sequences: the Kepler limit is > 1

Let $A := (a_n)_{n\in\mathbb{N}} \subset \mathbb{N}$. Then A is a regular (sparse) sequence if it has a Kepler limit exists and $\theta > 1$ and either

1. θ is transcendental or
2. θ is algebraic (over $\mathbb{Q}$) and (a_n) is a linear recurrence sequence whose characteristic polynomial is the minimal polynomial of θ

Theorem (Semenov(1979) /P.(2000); P.-Lambotte(2020))

Suppose A is a regular (sparse) sequence. Then,
the theory of $(\mathbb{Z}, +, <, A)$ is model-complete and NIP,
the theory of $(\mathbb{Z}, +, A)$ is superstable of Lascar rank ω and model-complete.

Decidability issues.

Sparse sequences following A.L. Semenov

Let S be the successor function on A and consider $Q(S(x)) := \sum_{i=0}^{n} r_i S^i(x)$ with $r_i \in \mathbb{Z}$, $0 \leq i \leq n$. We associate to such term a polynomial in $\mathbb{Z}[S]$.

Definition (A.L. Semenov)

$A \subset \mathbb{N}$ is a sparse sequence if for any $Q(S) \in \mathbb{Z}[S] \setminus \{0\}$, either for all $a_m \in A$, $Q(a_m) = 0$, or $Q >_{pp} 0$ or $-Q >_{pp} 0$,
and if $Q >_{pp} 0$, then there exists a natural number ℓ such that $Q(S^\ell) - Q > 0$.

One shows that if A is regular, then A is sparse following Semenov and that the theory T of $(\mathbb{Z}, +, -, 0, A, <)$ admits q.e. in the language of ordered abelian groups, together with $\{mod_n; n \in \mathbb{N}^*, \lambda_A, S, S^{-1}\}$. One can give an explicit axiomatisation and in case A is a linear recurrence sequence give conditions under which T is decidable.

Comparison between regular sequence and geometrically sparse sequences.

Again one can show that the theory of $(\mathbb{Z}, +, -, 0, A)$ admits q.e. in $\{+, -, 0, A\} \cup \{S, S^{-1}, c_0\} \cup \{\Sigma_{\bar{Q}} \colon \bar{Q} \in \mathbb{Z}[S]^n\}$, where $\Sigma_{\bar{Q}}$ are predicates that express that a tuple belongs to the images of $\bar{Q}(S)$.

(See the thesis of Q. Lambotte). There are regular sequences (a_n) which are not geometrically sparse. And among the linear recurrence sequences with a Kepler limit, one can characterize those which are geometrically sparse.

Non-lacunary sequences

Theorem (Conant, 2018)

Let Γ be a finitely generated monoid of $(\mathbb{N}, \cdot)$ and $A \subset \Gamma$ be infinite. Then the theory of $(\mathbb{Z}, +, A)$ is superstable of U-rank ω.

If there are $a, b \in \Gamma$ with $\log_a(b)$ is irrational, then Γ is non-lacunary (Furstenberg).

Non-lacunary sequences

Let $r \in \mathbb{R} \setminus \mathbb{Q}$, $r > 1$ and let $B_r := (\lfloor nr \rfloor)_{n \in \mathbb{N}^*}$ be a Beatty sequence.

Theorem (Gunaydin-Ozsahakyan, 2021)

$(\mathbb{Z}, +, -, 0, 1, B_r)$ is NIP (unstable), decidable, admits q.e. adding countably many predicates $D_{n,1}, D_{n,0}$, $n \in \mathbb{N} \setminus \{0, 1\}$, and there is no intermediate structure betwen $(\mathbb{Z}, +)$ and $(\mathbb{Z}, +, B_r)$, where $D_{n,1}(x) := \exists y \in B_r \; ny = x$ and $D_{n,0}(x) := \exists y \notin B_r \; ny = x$.

They use the following tool. Let

$$e : \mathbb{Z} \to S^1 : z \mapsto e^{\frac{i2\pi z}{r}},$$

where S^1 is the circle of center $(0, 0)$ and radius 1 in $\mathbb{R}^2$. Let C be the (anti-clockwise) cyclic order on S^1 and $Z_r := e(\mathbb{Z})$. Denote by $(e(-1)\, 1)$ the (cyclic) interval in S^1.

Gunaydin and Ozsahakyan show that $(\mathbb{Z}, +, -, 0, 1, B_r)$ is isomorphic to $(e(\mathbb{Z}), \cdot, {}^{-1}, 1, e(1), (e(-1)\, 1) \cap e(\mathbb{Z}))$.

A detour: cyclically ordered groups

Let G be any dense subgroup of $(\mathbb{R}, +, 0, <)$, for instance take a subgroup generated by $\langle \mathbb{Z}, \mathbb{Z}/r \rangle$, where $r \in \mathbb{R} \setminus \mathbb{Q}$.
Robinson and Zakon showed that the theory of $(G, +, -, 0, <)$ can be axiomatized as an ordered abelian group which is *regularly dense*, namely for each positive integer n, $x < y$ implies that there is an element z such that $x < nz < y$, and where for each $n \geq 2$, the indices $[G : nG]$ (finite or infinite), are specified.

Theorem (Giraudet, Leloup, Lucas; Bélair, P.)

Let $\mathcal{G} := (G \cap [0\,1[, +_1, <)$. Then $Th(\mathcal{G})$ is model-complete (in some extension of the language by infinitely many constants symbols), NIP and decidable if is r.e.

Non-lacunary sequences

Let $\mathcal{P}$ be the set of prime numbers. Recall Dickson hypothesis (or the linear Schnitzel hypothesis):

(D) Let $f_1(x), \ldots, f_n(x)$ be irreducible linear polynomials over $\mathbb{Z}$, each having a positive leading coefficient. Suppose that there is no prime p which divides $\prod_{i=1}^{n} f_i(x)$ for all $x \in \mathbb{N}$. Then there exist infinitely many $x \in \mathbb{N}$ such that such that $f_1(x), \ldots, f_n(x)$ are all prime.

Theorem (Bateman-Jockusch-Woods, 1993)

$(\mathbb{Z}, +, 0, <, \mathcal{P})$ is undecidable if Dickson hypothesis holds.

The proof shows that multiplication is definable, using a theorem of Buchi on the undecidability of $(\mathbb{Z}, +, <, 0, \{g(n) : n \in \mathbb{N}\})$, where $g(x) \in \mathbb{N}[x]$ is a polynomial of degree at least 2.

Theorem (Bateman-Jockusch-Woods, 1993)

$(\mathbb{Z}, +, 0, <, V_2, \{2^n : n \in \mathcal{P})$ is decidable if Dickson hypothesis holds.

Theorem (Kaplan-Shelah, 2017)

$(\mathbb{Z}, +, 0, 1, -\mathcal{P} \cup \mathcal{P})$ is unstable, supersimple of rank 1 and decidable if Dickson hypothesis holds.

Note that in $(\mathbb{Z}, +, \mathcal{P})$ one may define the order (since any sufficiently large positive integer is a sum of at most 4 prime numbers).