On expansions of $(\mathbb{Z}, +, 0)$.

Françoise Point

FNRS-FRS, UMons

March 24th 2017.

- Expansions of $(\mathbb{Z}, +, 0)$ versus of $(\mathbb{Z}, +, 0, <)$ (or $(\mathbb{N}, +)$) in the point of view of stability-like properties, definability, decidability.
- •• Comparison between expansions of $(\mathbb{Z}, +, 0, <)$ and of $(\mathbb{F}_p[X], +, 0)$, $(\mathbb{F}_p[X, X^{-1}], +, 0)$, $(\mathbb{F}_p[[X]], +, 0)$, \cdots .
- $\bullet \bullet \bullet \mathsf{Analogy}$ between expansions of $(\mathbb{Z},+,0,<)$ and $(\mathbb{R},+,.,0,1).$

• $(\mathbb{Z}, +, 0)$ is a torsion-free abelian group and $|\mathbb{Z}/n\mathbb{Z}| = n$, for each $n \in \mathbb{N}^*$. Define the unary predicate $D_n(x)$ by: $\exists y \ n.y = x$.

The theory of $(\mathbb{Z}, +, 0)$ admits quantifier-elimination in $\{+, -, 0, D_n; n \in \omega \setminus \{0, 1\}\}.$

The theory of $(\mathbb{Z}, +, 0)$ is superstable. (All modules are stable–definability of types–).

It is not ω -stable:one has an infinite chain of proper definable sugbroups: $n!\mathbb{Z}$, of finite index in one another.

View now $(\mathbb{Z}, +, <, 0)$ as a totally ordered abelian group. •• (Presburger) The theory of $(\mathbb{Z}, +, 0, <)$ admits quantifier-elimination in $\{+, -, 0, 1, <, D_n; n \in \omega \setminus \{0, 1\}\}$. In expansions of $(\mathbb{N}, +, 0)$ with a predicate, we have the following phenomenon: [Muchnik-Michaux-Villemaire] Let $A \subset \mathbb{N}^n$, then

 $A \notin Def(\mathbb{N}, +) \text{ iff } \exists X \subset \mathbb{N} \ (X \in Def(\mathbb{N}, +, A) \& X \notin Def(\mathbb{N}, +)).$

 \sim an analogy with o-minimal structures \mathcal{M} (e.g. the field of real numbers), where the structure of definable subsets in M^n is determined by how the definable subsets of M look like.

 \rightarrow notion of dimension and definition of *coset-minimality*.

(Belegradek, Peterzil, Wagner, 2000) $\mathcal{M} := (M, <, \cdots)$ is quasi-o-minimal if in any structure $\mathcal{N} \equiv \mathcal{M}$, any definable subset of N is a boolean combination of 0-definable sets and intervals. Example: $(\mathbb{Z}, +, 0, <, 1)$.

(P., Wagner) Let $\mathcal{G} := (G, \cdot, 1, \leq, ...)$ be a totally ordered group. Then \mathcal{G} is coset-minimal if every definable subset of G is a finite union of cosets of definable subgroups intersected with intervals.

• (P., Wagner) Let \mathcal{G} be coset-minimal, then one can identify its reduct as a pure ordered group.

Namely, assume it is discretely ordered, then \mathcal{G} is abelian and there is a chain of convex subgroups $\{0\} = G_0 < G_1 < \cdots < G_{k+1} = G$ with $G_1 \equiv (\mathbb{Z}, +, 0, <)$ and either $G_{i+1}/G_i \equiv (\mathbb{Q}, +, 0, <)$ or $G_{i+1}/G_i \equiv (\mathbb{Z}, +, 0, <)$, $1 \le i \le k$.

Note that the group $(\mathbb{Z} \times \mathbb{Z}, +, \leq, c_1, c_2, f)$, where f((x, y)) = (0, x) is a coset-minimal group which does not satisfy the exchange property.

•• (P., Wagner) If \mathcal{M} is group, then it is quasi-o-minimal iff the theory of \mathcal{M} is coset-minimal (possibly after adding finitely many constants).

(In that case, one can show that in the above description of definable subsets, one can assume that all cosets are of the form: cosets of n.M, for a certain n, and these subgroups are of finite index in M.)

Decidability proven using automata theory of expansions of $(\mathbb{Z}, +, 0, <)$

- One way to prove decidability for expansions of $(\mathbb{Z},+,0,<)$ is to use automata theory.
- The strategy is to link definability in expansions of $(\mathbb{N}, +, 0)$ with recognisability by a finite automata (R. Buchi,...) and to use the following result of Kleene:
- [Kleene] The emptiness problem for finite automaton is decidable.

More generally, take \mathcal{M} a first-order (countable) \mathcal{L} -structure with \mathcal{L} be a finite relational language. Then \mathcal{M} is *finite automaton presentable* (for short, FA-presentable) if

if the elements of the domain can be represented by (finite) words in a regular language $D \subset A^*$ over some finite alphabet A

in such a way that for each relation R of \mathcal{L} , we have some finite automaton which recognizes the graph of R.

Example

Take $(\mathbb{N}, +)$ the natural numbers. Code any $n \in \mathbb{N}$ by its binary expansion $n = \sum_{i=0}^{s} 2^{i} \cdot \epsilon_{i}$, with $\epsilon_{i} \in A := \{0, 1\}$. In this case, D is the set of finite words in 0, 1 ending with a 1, the empty word representing 0.

Let $n \in \mathbb{N}$, then $V_2(n)$ is the highest power of 2 that divides n. So in the binary expansion of n, $V_2(n)$ is the smallest power of 2 that occurs with a non-zero coefficient.

Using finite automata theory, one can prove: [Büchi (1960), McNaughton, Bruyère (1985)] The theory of $(\mathbb{N}, +, V_2)$ is decidable; any subset of \mathbb{N}^n is definable if and only if it FA-recognizable. Moreover a definable subset of \mathbb{N}^n is $\forall \exists \forall$ -definable (Villemaire). One constructs three automata.

- One to recognise the relation $\{(a, b, a + b) : a, b \in \mathbb{N}\}$ and
- another one to recognise the relation $\{(a, b) : a < b\}$.
- another one to recognise the relation $\{(a, V_2(a)) : a, b \in \mathbb{N} \setminus \{0\}\}.$

The following automaton recognizes the graph of the function V_2 . The letter x designates any letter of our alphabet $A = \{0, 1\}$.

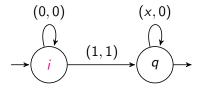


Figure: Büchi automaton for V_2 (accepting paths)

Automaton for $\cdot 2$

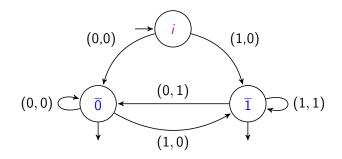


Figure: Büchi automaton for the graph of the function $\cdot 2$, namely it accepts all tuples of the form $\{(u, 0u)\}$

[Nies] FA-presentability is a *strong* condition on the structure:

- FA-presentable groups are locally abelian-by-finite,
- FA-presentable rings are locally finite and
- FA-presentable rings without zero-divisors are the finite fields.

[Hodgson,...] Any (countable) FA-presentable \mathcal{L} -structure is decidable. (He also considered \mathcal{L} -structures whose elements can be represented by infinite words \rightsquigarrow finite automaton accepting infinite words).

Undecidability of expansions of $(\mathbb{N}, +, V_2)$

The theory of $(\mathbb{N}, +, V_2, V_3)$ is undecidable (R. Villemaire).

The theory of $(\mathbb{N}, +, V_2, P_3)$ is also undecidable (A. Bès).

Both Villemaire's and Bès' results rely on a slight generalization of a result of C. Elgot and M. Rabin on weak monadic second-order theory of $(\mathbb{N}, Succ)$.

Let g be a strictly increasing function from P_2 to P_2 with the property that g skips at least one value between two consecutive arguments:

$$\forall n \forall m \ (n < m \rightarrow 2.g(n) < g(m)).$$

Then $\operatorname{Th}(\mathbb{N}, +, V_2, n \mapsto g(n))$ is undecidable. (One defines addition and multiplication on the exponents of powers of 2.)

Decidable expansions of polynomial rings

This strategy can be applied to other additive reducts of Euclidean rings. For instance,

On $\mathbb{F}_q[X]$, we have a partial order \prec induced by the degree function and let P_X be a unary predicate for the powers of X

[A. Sirokofskich, 2010] The structure $(\mathbb{F}_q[X], +, P_X, \prec, \cdot u; u \in \mathbb{F}_q[X])$ is model-complete.

Let $u \in \mathbb{F}_q[X] \setminus \mathbb{F}_q$, we define the unary function $V_u(x)$ sending x to the highest power of u dividing it.

[L. Waxweiler, 2009] The theory of $(\mathbb{F}_q[X], +, 0, \prec, V_u, .C; C \in \mathbb{F}_q[X])$, where .C denotes the scalar multiplication by C, is decidable and have a bound $(\forall \exists \forall)$ on the complexity of definable sets.

Euclidean rings setting:-joint work with M. Rigo and L. Waxweiler

One can use finite automata working on infinite words.

Let $\mathcal{F} := (\mathbb{F}_p[[X]], +, 0, V_X, \lambda_X, \prec, .C; C \in \mathbb{F}_q[X])$

Let $P \in \mathbb{F}_q[[X]]$, we define the unary function $V_P(x)$ sending x to the highest power of P dividing it.

THEOREM (Bélair, Gélinas, P.)

The theory of \mathcal{F} is decidable and $Def(\mathcal{F}) = \bigcup_n Rec(A_n^{\omega})$.

Let \mathcal{M} be an \mathcal{L} -structure and let $\phi(x; \bar{y})$ be an \mathcal{L} -formula. Then ϕ has the independence property (*IP*) (in M) if for every k there exist $b_0, \dots, b_{k-1} \in M$ such that for every subset E of $\{0, \dots, k-1\}$ there exists $\bar{a}(E) \in M$ such that the following equivalence holds:

$$\ell \in E \text{ iff } \mathcal{M} \models \phi(b_{\ell}; \bar{a}(E)). \quad (\star).$$

If no formula has (IP), then one says that \mathcal{M} is NIP.

 $(\mathbb{Z}, +, 0, <, V_2)$ has a formula with (IP), namely: $2^{\ell} \in n$ if $\exists u \exists v \ n = u + 2^{\ell} + v$, where $V_2(u) = V_2(n)$, $\lambda_2(u) < 2^{\ell}$, $2^{\ell} < V_2(v)$, $\lambda_2(v) = \lambda_2(n)$ (with special cases for the extremities).

Observation: Let T be the theory of a coset-minimal group. Then T has *NIP*.

Observation: Let T be the theory of a coset-minimal group. Then T has *NIP*.

Proof: Let $\mathcal{G} \models T$. By the way of contradiction, we may assume that a formula witnessing (*IP*) is of the form $\psi(x; y_1, \dots, y_N)$. For every k, there would exist $b_0, \dots, b_{k-1} \in G$ such that que for every subset A of $\{0, \dots, k-1\}$ there exist $\bar{a}_A \in G^N$ such that

 $i \in A$ iff $\mathcal{G} \models \phi(b_i; \bar{a}_A)$.

The definable set $\phi(G, \bar{y})$ is a finite union of cosets of n.Gintersected with intervals, and the number of intervals is bounded by ℓ , with n and ℓ independent from \bar{y} . Let f := [G : nG]. Consider $k := (2.\ell + 1).n$. By the pigeon-hole principle, in any finite set of elements $b_0, \dots, b_{k-1} \in G$, there are at least $2.\ell + 1$ of them in the same coset of n.G, among the indices of this subset, one can find a subset of $\ell + 1$ elements which cannot be selected using ℓ intervals. Question (Chernikov,Hils): Are there ordered modules whose theories are not NIP?

(P. Glivicky, P. Pudlak (2017)) There exists an ordered module \mathcal{M} over a ring of the form $\mathbb{Z}[a, b]$ in which one can define multiplication on a non-standard interval. Therefore the theory of \mathcal{M} is not NIP and its theory is undecidable.

(Penzin, 1973) Penzin has previously showed that for some n > 1, the universal theory of $(\mathbb{Z}, +, 0, <, \cdot d_1, \cdots, \cdot d_n)$ is undecidable.

[Hieronymi, Tychonievich, 2014] One can define multiplication in $(\mathbb{R}, +, 0, <, \alpha.\mathbb{N}, \beta.\mathbb{N}, \gamma.\mathbb{N})$, where α, β, γ are \mathbb{Q} -linearly independent.

Definability in expansions of $(\mathbb{Z}, +, <)$

Recall that $V_2(n)$ is the highest power of 2 that divides $n, n \in \mathbb{N}$.

Let P_2 be the set of powers of 2 and denote the corresponding unary predicate by the same letter,

then $(\mathbb{Z}, +, 0, <, P_2)$ is a reduct of $(\mathbb{Z}, +, 0, <, V_2)$: we have

 $P_2(x)$ iff $V_2(x) = x$.

[van den Dries, 1985] The structure $(\mathbb{Z}, +, -, 0, <, P_2)$, is model-complete and admits quantifier elimination in $\{+, -, 0, 1, \equiv_n; n \in \mathbb{N}^*, \lambda_2\}$, where $\lambda_2(x)$ is the largest power of 2 that occurs in the binary expansion of n.

(Byproduct of the methods used for his proof of the model-completeness of $(\mathbb{R}, +, ., 0, 1, 2^{\mathbb{Z}})$).

Mann property

Let K be a field of characteristic 0 and G a multiplicative subgroup of $(K^*, \cdot, 1)$.

Then G has the Mann property if every equation of the form

$$\sum_{i=1}^n a_i \cdot g_i = 1,$$

 $a_i \in \mathbb{Q}$, has only finitely many non-degenerate solutions in G.

 (g_1, \dots, g_n) is non-degenerate if for any proper subset J of indices, $\sum_{j \in J} a_j \cdot g_j \neq 0.$

\rightsquigarrow Mann axioms

Examples: (Mann) If $K = \mathbb{C}$ and G is the subgroup \mathbb{U} of roots of unity, then (\mathbb{C}, \mathbb{U}) has the Mann property. Let $a \in \mathbb{R}^{>0}$, then the subgroup $a^{\mathbb{Z}}$ has the Mann property. (van der Poorten, Schlickewei, 1991) Let K be a field of characteristic 0 and G a multiplicative subgroup of $(K^*, \cdot, 1)$. Suppose that G is of finite rank i.e. $\dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q}$ is finite. Then G has the Mann property.

• $(\mathbb{C}, \mathbb{U}), (\mathbb{R}, \mathbb{U})$, where \mathbb{U} is the group of roots of unity in \mathbb{C} (Zilber, 1993, 2003)

2 (
$$\mathbb{R}$$
, $< 2^{\mathbb{Z}}$, $3^{\mathbb{Z}} >$) (Gunaydin, van den Dries, 2006)

3 $(\mathbb{Q}_p, (1+p)^{\mathbb{Z}})$ (Mariaule, 2016)

In that last case, study of: $\rightarrow (\mathbb{Z}, +, v_p)$, namely induced structure on the value group of \mathbb{Q}_p .

Let Γ be a subgroup of $\mathbb{R}^{>0}$ with the Mann property.

(van den Dries, Gunaydin, 2006) Let K be a real closed ordered field, let G be a dense subgroup of $K^{>0}$, and let a group homomorphism $\gamma \to \gamma' : \Gamma \to G$.

Then $(K, G, (\gamma')_{\gamma \in \Gamma}) \equiv (\mathbb{R}, \Gamma, (\gamma)_{\gamma \in \Gamma})$ if and only if

(i) $(G, (\gamma')_{\gamma \in \Gamma}) \equiv (\Gamma, (\gamma)_{\gamma \in \Gamma})$ as ordered groups and; for all $a_1, ..., a_n \in \mathbb{Z}$ and $\gamma_1, ..., \gamma_n \in \Gamma$ $a_1\gamma_1 + ... + a_n\gamma_n > 0 \leftrightarrow a_1\gamma'_1 + ... + a_n\gamma'_n > 0$; (ii) $(K, G, (\gamma')_{\gamma \in \Gamma}$ satisfies the Mann axioms of Γ . Let p be a prime number bigger than 2 and let $v_p : (\mathbb{Z}, +, 0) \to (\mathbb{N}, \leq) : z \to n)$, where p^n is the highest power of p dividing n.

(Guignot/ Mariaule, 2016) The theory of $(\mathbb{Z}, +, v_p)$ is NIP and is model-complete (and admits quantifier-elimination).

One can also consider the one-sorted structure $(\mathbb{Z}, +, |_p)$, where $a|_p b$ iff $v_p(a) \leq v_p(b)$ (D'Elbée).

(Note that NIP-(ordered) groups/dp-minimal groups have been studied in details by Aschenbrenner, Dolich, Haskell, Macpherson, Starchenko/Simon/...).

Let us consider expansions of $(\mathbb{Z}, +, 0)$.

Recall that the theory of the free non abelian group F_2 on two generators is stable (Z. Sela, 2013).

Question (Pillay): which kind of structure the free non abelian group F_2 on two generators can induce on its proper definable subgroups? in particular on its centralisers?)

(Palacin-Sklinos 2017/Poizat) The theory of $(\mathbb{Z}, +, 0, 1, P_2)$ is superstable of *U*-rank ω . Moreover, there are no proper superstable expansions of $(\mathbb{Z}, +, 0)$ of finite *U*-rank.

(Palacin-Sklinos) The same proof works for $a^{\mathbb{N}}$, $a \in \mathbb{N}$, a > 2, also for fast growing sequences like $(n!)_{n \in \omega^*}$.

Method of P-S: Casanovas-Ziegler result on stable expansions by a predicate.

Question: for which sequences R, the expansion $(\mathbb{Z}, +, R)$ remains stable?

(Kaplan, Shelah 2017) Let \mathcal{P} be the set of prime numbers. Then, assuming Dickson conjecture (DC), the theory of $(\mathbb{Z}, +, 0, 1, \mathcal{P} \cup -\mathcal{P})$ is decidable, not stable but supersimple of rank 1.

In fact, the theory of $(\mathbb{Z}, +, 0, 1, \mathcal{P} \cup -\mathcal{P})$ admits quantifier elimination in $\{+, -, 0, 1, \mathcal{P}, D_n, Q_n; n \in \omega^*, n \ge 2\}$, where $\mathcal{P}(x)$ iff $x \in \mathcal{P} \cup -\mathcal{P}$ and Q_n is defined as $(D_n(x) \& \mathcal{P}(\frac{x}{n}))$.

DC (1904): Let $k \ge 1$ and $\overline{f} = \langle f_i : i < k \rangle$ where $f_i(x) = a_i x + b_i$ with a_i, b_i non-negative integers, $a_i \ge 1$ for all i < k. Assume that: there does not exist any integer n > 1 dividing all the products $\prod_{i < k} f_i(s)$ for every (non-negative) integer s. Then there exist infinitely many natural numbers m such that $f_i(m)$ is prime for all i < k.

Note that one can define \mathbb{N} in $(\mathbb{Z}, +, 0, \mathcal{P})$: any natural number bigger than 1 is a sum of a bounded number of primes. This is due to the fact that $\sigma(\mathcal{P} + \mathcal{P}) > 0$, where for $R \subset \mathbb{N}$,

$$\sigma(R) = \inf_{n \to +\infty} \frac{|R \cap [0 \ n]|}{n}$$

(Bateman, Jockusch, Woods, 1993) Under (DC), the theory of $(\mathbb{Z}, +, 0, 1, <, \mathcal{P})$ is undecidable.

They show that $\{n^2 + n : n \in \omega\}$ is definable in $(\mathbb{N}, +, \mathcal{P})$ and from this subset, one can define the graph of the square function and so the multiplication.

It gives an example of a unary predicate R such that $(\mathbb{Z}, +, 0, R)$ is decidable, whereas $(\mathbb{Z}, +, 0, <, R)$ is undecidable.

(Conant) A subset $A \subset \mathbb{R}^+$ is geometric if $\{\frac{a}{b}: a, b \in A; b \leq a\}$ is closed and discrete. A sequence $R \subset \mathbb{N}$ is geometrically sparse if there exists a function $f : R \to \mathbb{R}^+$ such that f(R) is geometric and $sup_{r \in R} |r - f(R)| < \infty$.

The theory of $(\mathbb{Z}, +, 0, 1, R)$ is superstable of *U*-rank ω , for any geometrically sparse sequence *R*.

(Lambotte, P.) Let $R := (r_n)_{n \ge 0}$, with $r_0 = 1$, be a strictly increasing sequence such that there exists $\theta > 1$ such that $\lim_{n \to +\infty} \frac{r_n}{\theta^n}$ exists and is nonzero. Moreover one assumes that R is given by a linear recurrence whose characteristic polynomial is the minimal polynomial of θ .

Then, the theory of $(\mathbb{Z}, +, 0, 1, R)$ is superstable of *U*-rank ω and it is model-complete.

(A.L. Semenov) A sequence *R* is sparse if the operators of the form $a_0.S^0(y) + \cdots + a_n.S^n(y)$ for $y \in R$, $a_i \in \mathbb{Z}$, are either = 0, eventually strictly positive or strictly negative and if $A >_{pp} 0$, then there exists Δ such that $A(S^{\Delta}y) - y > 0$.

[A.L. Semenov, 1979] Let R be an increasing sequence of natural numbers, which is sparse and periodic in each $\mathbb{Z}/n\mathbb{Z}$, then the theory of $(\mathbb{N}, +, R)$ is model-complete i.e. any definable set is existentially definable.

[P., 2000] Let *R* be an increasing sequence of natural numbers, which is sparse and periodic in each $\mathbb{Z}/n\mathbb{Z}$. Then, $(\mathbb{Z}, +, 0, 1, <, ./n, \lambda_R, S, S^{-1})$ admits quantifier elimination and is axiomatisable.

Examples of sparse sequences in \mathbb{N} : let $R := (r_n)_{n \ge 0}$, with $r_0 = 1$, be a strictly increasing sequence such that $\lim_{n \to +\infty} \frac{r_{n+1}}{r_n} = \theta > 1$ exists.

 $1 \quad \lim_{n \to +\infty} \frac{r_{n+1}}{r_n} := +\infty,$

2 θ is a transcendental number,

• there exists θ such that $\lim_{n\to+\infty} \frac{r_n}{\theta^n}$ exists and is nonzero, and if in addition, in cases (1) and (2) the limit is effective and Ris periodic in each $\mathbb{Z}/n\mathbb{Z}$, then get decidability. In case (3), one assumes in addition that R is given by a linear recurrence whose characteristic polynomial is the minimal polynomial of θ and one gives conditions under which $\lim_{n\to+\infty} \frac{r_n}{\theta^n}$ is effective.

An example of a non-sparse sequence is $(r_n := n + 2^n)$ but $(\mathbb{N}, +, R)$ is model-complete. It is bi-interpretable with $(\mathbb{N}, +, n \to 2^n)$.

[ADDMS] M. Aschenbrenner, A. Dolich, D. Haskell, D. Macpherson, and S. Starchenko, Vapnik?Chervonenkis Density in Some Theories without the Independence Property, II, Notre Dame Journal of Formal Logic Volume 54, Numbers 3-4, 2013.

[BGP] L. Bélair, M. Gélinas, F. Point, Ensembles reconnaissables de séries formelles sur un corps fini, C.R.Acad. Sci. Paris, Ser.I., volume 354, Issue 3, March 2016, 225-229.

[C] G. Conant, Stability and sparsity in sets of natural numbers, ArXiv january 2017.

[GP] P. Glivicky, P. Pudlak, Wild models of linear arithmetics, (to appear in MQL, 2017).

[H] B.R. Hodgson, Théories décidables par automate fini, Ph.D. Thesis, Université de Montréal, 1976.

[KS] I. Kaplan, S. Shelah, Decidability and classification of the theory of integers with primes, ArXiv 2016.

[P] Point F., On decidable extensions of Presburger arithmetic: from A. Bertrand numeration systems to Pisot numbers, J. Symbolic Logic 65 (2000), no. 3, 1347- 1374.

[PRW] F. Point, M. Rigo and L. Waxweiler, Defining multiplication in some additive ex- pansions of polynomial rings, Communications in Algebra, 44:5, 2075-2099, 2016.

[S] Semenov A.L., On certain extensions of the arithmetic of natural numbers with addition, Math. USSR Izvestiya **15**, no. 2, 401-418, 1980.