Group Reducts of Presburger Arithmetic

Gabriel Conant
Notre Dame

April 9, 2016
17th Graduate Student Conference in Logic
University of Notre Dame

Presburger arithmetic

Presburger arithmetic is the complete theory of the ordered group of integers $(\mathbb{Z}, +, <, 0)$.

This theory was first axiomatized by Presburger in 1927. An alternate presentation uses the monoid of nonnegative integers $(\mathbb{N}, +, 0)$.

Presburger arithmetic has quantifier elimination in the definitional expansion $\mathcal{L}_{\text{Pr}} = \{+, -, 0, 1, <, (n\mathbb{Z})_{n<\omega}\}$.

Definable sets in Presburger arithmetic

Sets $A \subseteq \mathbb{Z}^n$, which are definable in Presburger arithmetic, have a very nice structure. For example, if $A \subseteq \mathbb{Z}$ is definable in Presburger arithmetic then

$$A = F \cup L_1 \cup \ldots \cup L_k,$$

where F is some finite set and each L_i is an arithmetic progression.

In particular, sets like

- $\Pi_q = \{q^n : n \in \mathbb{N}\}$, where $q > 1$,
- $\mathrm{Fac} = \{n! : n \in \mathbb{N}\}$,
- $\mathrm{Perf}(k) = \{n^k : n \in \mathbb{N}\}$, where $k > 0$,
- Primes,

are not definable in Presburger arithmetic.

Expansions of Presburger arithmetic

Question

Suppose $\mathcal{Z} = (\mathbb{Z}, +, <, 0, \dots)$ is some expansion of Presburger arithmetic. How easy is it to recognize that $\mathcal{Z}$ is a *proper* expansion?

Theorem (Michaux-Villemaire 1996)

Suppose $\mathcal{Z} = (\mathbb{Z}, +, <, 0, \dots)$ *is a proper expansion of Presburger arithmetic. Then there is a subset* $A \subseteq \mathbb{Z}$*, which is definable in* $\mathcal{Z}$*, but not in* $(\mathbb{Z}, +, <, 0)$*.*

By contrast: $(\mathbb{C}, =)$ and $(\mathbb{C}, +, \cdot, 0, 1)$ define the same subsets of $\mathbb{C}$.

Expansions of Presburger arithmetic

Theorem (Michaux-Villemaire 1996)

Suppose $\mathcal{Z} = (\mathbb{Z}, +, <, 0, \ldots)$ is a proper expansion of Presburger arithmetic. Then there is a subset $A \subseteq \mathbb{Z}$, which is definable in $\mathcal{Z}$, but not in $(\mathbb{Z}, +, <, 0)$.

Applications:

- (Belegradek-Peterzil-Wagner 2000) There are no proper **quasi-o-minimal** expansions of Presburger arithmetic.
- (Dolich-Haskell-Macpherson-Starchenko 2011) There are no proper **dp-minimal** expansions of Presburger arithmetic.
- (Dolich-Goodrick 2015) There are no proper **strong** expansions of Presburger arithmetic.

Reducts of Presburger arithmetic

There are lots, *for example*,

- $(\mathbb{Z}, =)$
- $(\mathbb{Z}, x \mapsto x + 1)$
- $(\mathbb{Z}, x \mapsto -x)$
- $(\mathbb{Z}, x \mapsto x + 1, x \mapsto -x)$
- $(\mathbb{Z}, +, 0)$
- $(\mathbb{Z}, <)$
- $(\mathbb{Z}, <, x \mapsto -x)$
- $(\mathbb{Z}, +, <, 0)$

Definition

A structure $\mathcal{Z}$, with universe $\mathbb{Z}$, is a **group reduct of Presburger arithmetic** if $\mathcal{Z}$ is a reduct of $(\mathbb{Z}, +, <, 0)$ and an expansion of $(\mathbb{Z}, +, 0)$.

The Main Result

Theorem (C. 2016)

There are no proper group reducts of Presburger arithmetic. In other words, if $\mathcal{Z}$ is a group reduct of Presburger arithmetic then $\mathcal{Z}$ is interdefinable with either $(\mathbb{Z}, +, 0)$ or $(\mathbb{Z}, +, <, 0)$.

Motivation: stable expansions of $(\mathbb{Z},+,0)$

Until recently, it was unknown if $(\mathbb{Z},+,0)$ had any proper stable expansions.

Theorem (Palacín-Sklinos; Poizat 2014)

For any $q>0$, $(\mathbb{Z},+,0,\Pi_q)$ is a proper stable expansion of $(\mathbb{Z},+,0)$.

Palacín-Sklinos prove the same for $(\mathbb{Z},+,0,\mathrm{Fac})$.

- $(\mathbb{Z},+,0,\mathrm{Perf}(2))$ defines the ordering by the four-square theorem (Lagrange 1770).
- $(\mathbb{Z},+,0,\mathrm{Primes})$ defines the ordering by Goldbach-type theorems (e.g. Tao 2012 or Helfgott 2015).

Digression on Primes

Let $P = \{p \in \mathbb{Z} : |p| \text{ is prime }\}$. Then $(\mathbb{Z}, +, 0, P)$ is again unstable (in fact, has the independence property by Kaplan-Shelah 2016). However, it is possible that $(\mathbb{Z}, +, 0, P)$ *does not* define the ordering.

Dickson's Conjecture (1904)

Fix finitely many linear forms $(a_i x + b_i)_{i \leq k}$, with $a_i \geq 1$. Then there are infinitely many n such that $a_i n + b_i$ is prime for all $i \leq k$, *provided that*

$$\gcd\left(\prod_{i \leq k} a_i n + b_i : n > 0\right) = 1.$$

- The $k = 1$ case is known (Dirichlet 1837).
- The $k = 2$ case would imply infinitely many twin primes: $(x, x+2)$, and infinitely many Sophie Germain primes: $(x, 2x+1)$.

Kaplan-Shelah show that if this conjecture is true, then $(\mathbb{Z}, +, 0, P)$ is supersimple (and so, in particular, does not define the ordering).

Tame Expansions of $(\mathbb{Z}, +, 0)$

Problem

Characterize the subsets $A \subseteq \mathbb{Z}^n$ (even just $A \subseteq \mathbb{Z}$) such that $(\mathbb{Z}, +, 0, A)$ is stable.

What about expansions of $(\mathbb{Z}, +, 0)$ satisfying other "tameness" properties (e.g. finite dp-rank)?

Question (Asch-Dol-Hask-Mac-Star 2013)

Is every dp-minimal expansion of $(\mathbb{Z}, +, 0)$ a reduct of $(\mathbb{Z}, +, <, 0)$?

The same could be asked about finite dp-rank expansions in general.

Theorem (C.-Pillay 2016)

Any proper finite dp-rank expansion of $(\mathbb{Z}, +, 0)$ *is unstable.*

Group reducts of Presburger arithmetic

Question

Is every finite dp-rank expansion of $(\mathbb{Z}, +, 0)$ a reduct of $(\mathbb{Z}, +, <, 0)$?

Definition

A structure $\mathcal{Z}$, with universe $\mathbb{Z}$, is a **group reduct of Presburger arithmetic** if $\mathcal{Z}$ is a reduct of $(\mathbb{Z}, +, <, 0)$ and an expansion of $(\mathbb{Z}, +, 0)$.

Theorem (C. 2016)

There are no proper group reducts of Presburger arithmetic.

So the initial question is equivalent to:
Is $(\mathbb{Z}, +, <, 0)$ the *only* proper finite dp-rank expansion of $(\mathbb{Z}, +, 0)$?

Restatement of main result

Fix $A \subseteq \mathbb{Z}^n$.

- A is **Presburger-definable** if it is definable in $(\mathbb{Z}, +, <, 0)$.
- A is **group-definable** if it is definable in $(\mathbb{Z}, +, 0)$.
- A **defines the ordering** if $\mathbb{N}$ is definable in $(\mathbb{Z}, +, 0, A)$.

Main Theorem (restated)

Suppose $A \subseteq \mathbb{Z}^n$ is Presburger-definable. Then either A defines the ordering or A is group-definable.

Structure of Presburger-definable sets

- A partial function $f : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ is **$\mathbb{Z}$-linear** if it is of the form

$$f(\bar{x}) = u + \sum_{i=1}^{n} a_i \left(\frac{x_i - r_i}{m_i} \right)$$

  for some $\bar{m}, \bar{r} \in \mathbb{N}^n$, $\bar{a} \in \mathbb{Z}^n$, and $u \in \mathbb{Z}$ (note: $\mathrm{dom}(f) = \bar{m}\mathbb{Z}^n + \bar{r}$).
- A subset of $\mathbb{Z}$ is a **Presburger cell** if it is of the form

$$[a, b]^r_m := \{x \in \mathbb{Z} : a \leq x \leq b,\ x \equiv_m r\},$$

  where $r, m \in \mathbb{N}$ and $a, b \in \mathbb{Z} \cup \{\pm\infty\}$.
- A subset of $\mathbb{Z}^{n+1}$ is a **Presburger cell** if it is of the form

$$C[f, g]^r_m := \{(\bar{x}, y) \in \mathbb{Z}^{n+1} : \bar{x} \in C,\ f(\bar{x}) \leq y \leq g(\bar{x}),\ y \equiv_m r\},$$

  where $C \subseteq \mathbb{Z}^n$ is a Presburger cell, $c, m \in \mathbb{N}$, and each of f and g is either constant $\pm\infty$ or a $\mathbb{Z}$-linear function whose domain contains C.

Structure of Presburger-definable sets

Theorem (Cluckers 2003)

$A \subseteq \mathbb{Z}^n$ is Presburger-definable if and only if it can be written as a finite union of Presburger cells in $\mathbb{Z}^n$.

Structure of group-definable sets

Fact (folklore)

$A \subseteq \mathbb{Z}^n$ is group-definable if and only if it is a finite Boolean combination of cosets of subgroups of $\mathbb{Z}^n$.

Recall that any subgroup $H \leq \mathbb{Z}^n$ is isomorphic to $\mathbb{Z}^k$ for some $0 \leq k \leq n$. The **rank** of H is k.

- If C is a coset of a rank k subgroup of $\mathbb{Z}^n$ then the **rank** of C is k.
- The **rank** of a set $A \subseteq \mathbb{Z}^n$ is the minimal $k \leq n$ such that A is contained in a finite union of cosets of rank at most k.
- $A \subseteq \mathbb{Z}^n$ is a **quasi-coset** if $A = C \backslash Z$ where C is a coset and Z is group-definable with $\text{rk}(Z) < \text{rk}(C)$ (by convention, $\text{rk}(\emptyset) = \text{-1}$).

Theorem

$A \subseteq \mathbb{Z}^n$ is group-definable if and only if it can be written as a finite union of quasi-cosets in $\mathbb{Z}^n$.

Proof of the main result

Main Theorem (restated)

Suppose $A \subseteq \mathbb{Z}^n$ is Presburger-definable. Then either A defines the ordering or A is group-definable.

We proceed by induction on n.

The base case $n = 1$ is straightforward from quantifier elimination.

Assume the main result for Presburger-definable subsets of $\mathbb{Z}^n$, and fix a Presburger-definable subset $A \subseteq \mathbb{Z}^{n+1}$. Assume A *does not define the ordering*. We want to show A is group-definable.

Let $\pi(A)$ denote the projection of A to $\mathbb{Z}^n$. Then $\pi(A)$ is group-definable by induction and the assumption on A.

Technical reductions

Notation: Fix $m > 0$ and $a, b \in \mathbb{Z}$ with $a \leq b$.

- $[a, b]_m = [a, b] \cap m\mathbb{Z}$ (i.e. $[a, b]^0_m$)
- $a \leq_m b$ if $[a, b] \cap m\mathbb{Z} \neq \emptyset$
- $a <_m b$ if $(a, b) \cap m\mathbb{Z} \neq \emptyset$

A set $B \subseteq \mathbb{Z}^{n+1}$ has **sorted fibers** if there is an integer $m > 0$ and tuples of $\mathbb{Z}$-linear functions $\bar{f} = (f_1, \ldots, f_k)$ and $\bar{g} = (g_1, \ldots, g_k)$ on $\mathbb{Z}^n$ satisfying the following properties:

- $\pi(B) \subseteq \mathrm{dom}(f_i) \cap \mathrm{dom}(g_i)$ for all $1 \leq i \leq k$,
- for all $\bar{x} \in \pi(B)$ there are $\sigma, \tau \in S_k$ such that

$$B_{\bar{x}} = \textstyle\bigcup_{i=1}^{k} \left[f_{\sigma(i)}(\bar{x}), g_{\tau(i)}(\bar{x})\right]_m$$

  and

$$f_{\sigma(1)}(\bar{x}) \leq_m g_{\tau(1)}(\bar{x}) <_m \ldots <_m f_{\sigma(k)}(\bar{x}) \leq_m g_{\tau(k)}(\bar{x}).$$

Technical reductions

$A \subseteq \mathbb{Z}^{n+1}$ is Presburger-definable and does not define the ordering.

Main Technical Work

(*a*) *A* is interdefinable with a finite sequence of Presburger-definable sets with sorted fibers.

(*b*) Suppose *A* has sorted fibers, witnessed by *k*-tuples $\bar{f}$ and $\bar{g}$. Suppose further that $f_s = g_t + c$ for some $s, t \leq k$ and $c \in \mathbb{Z}$. Then *A* is interdefinable with a finite sequence of Presburger-definable sets in $\mathbb{Z}^{n+1}$, each of which has sorted fibers witnessed by some *proper* subtuples of $\bar{f}$ and $\bar{g}$.

Altogether, we may assume *A* has sorted fibers and induct on the length of the witnessing tuples of $\mathbb{Z}$-linear functions.

Technical reductions

$A \subseteq \mathbb{Z}^{n+1}$ is Presburger-definable, does not define the ordering, and has sorted fibers witnessed by $\bar{f}$, $\bar{g}$.

One last reduction: We may assume $\pi(A)$ is a single quasi-coset.

For simplicity, assume $\pi(A) = \mathbb{Z}^n \backslash X$, where $X \subseteq \mathbb{Z}^n$ is group-definable with $\mathrm{rk}(X) < n$.

*After certain linear transformations, the general case essentially reduces to this.

Goal: Prove that some f_s and g_t are parallel.

Polyhedra in $\mathbb{R}^n$

- Given non-parallel affine functions f, g on $\mathbb{R}^n$, define the **half-spaces**

$$H(f \leq g) := \{\bar{x} \in \mathbb{R}^n : f(\bar{x}) \leq g(\bar{x})\},$$
$$H(f < g) := \{\bar{x} \in \mathbb{R}^n : f(\bar{x}) < g(\bar{x})\},$$

  as well as the **hyperplane** $H(f = g) := \{\bar{x} \in \mathbb{R}^n : f(\bar{x}) = g(\bar{x})\}$.
- Set $H(f \leq g)^* = H(g \leq f)$ and $H(f < g)^* = H(g < f)$.
- A **polyhedron** in $\mathbb{R}^n$ is the intersection of finitely many half-spaces.
- If $P = H_1 \cap \ldots \cap H_k$ is a polyhedron, where each H_i is a half-space, then the **opposite polyhedron** is

$$P^* = H_1^* \cap \ldots \cap H_k^*.$$

- The **inradius** of a polyhedron P is

$$r(P) := \sup\{r \geq 0 : P \text{ contains a closed ball of radius } r\}.$$

Polyhedra in $\mathbb{R}^n$

Theorem (Kadets 2005)

If $P, Q_1, \ldots, Q_n$ are polyhedra and $P \subseteq Q_1 \cup \ldots \cup Q_n$ then

$$r(P) \leq r(Q_1) + \ldots + r(Q_n).$$

Corollary

Suppose P is a polyhedra with infinite inradius.

(a) P^* has infinite inradius.

(b) If $X \subseteq \mathbb{Z}^n$ has $\mathrm{rk}(X) < n$ then $(\mathbb{Z}^n \backslash X) \cap P$ cannot be covered by finitely many polyhedra of finite inradius.

Back to the proof

$A \subseteq \mathbb{Z}^{n+1}$ is Presburger-definable, does not define the ordering, has sorted fibers witnessed by $\bar{f}$, $\bar{g}$, and $\pi(A) = \mathbb{Z}^n \backslash X$ with $\mathrm{rk}(X) < n$.

Suppose no f_s, g_t are parallel.

Given $\sigma, \tau \in S_k$, define the following polyhedron in $\mathbb{R}^n$,

$$P(\sigma, \tau) = \bigcap_{i \leq k} H\left(f_{\sigma(i)} \leq g_{\tau(i)}\right) \cap \bigcap_{i<k} H\left(g_{\tau(i)} < f_{\sigma(i+1)}\right).$$

By assumption, $\pi(A) \subseteq \bigcup_{\sigma,\tau} P(\sigma, \tau)$.

So we may fix $\mu, \nu \in S_k$ such that $P(\mu, \nu)$ has infinite inradius.

End of the proof

- $A \subseteq \mathbb{Z}^{n+1}$ has sorted fibers witnessed by $\bar{f}$, $\bar{g}$,
- $\pi(A) = \mathbb{Z}^n \backslash X$ where $\mathrm{rk}(X) < n$,
- $\pi(A) \subseteq \bigcup_{\sigma,\tau} P(\sigma,\tau)$, and $\mu,\nu \in S_k$ are such that $r(P(\mu,\nu)) = \infty$.

Then $P(\mu,\nu)^*$ has infinite radius. Set

$$C = \pi(A) \cap P(\mu,\nu)^*.$$

For any $\bar{x} \in C$, we have

- $g_{\nu(k)}(\bar{x}) \leq f_{\mu(k)}(\bar{x}) < \ldots < g_{\nu(1)}(\bar{x}) \leq f_{\mu(1)}(\bar{x})$, and
- $f_{\sigma(1)}(\bar{x}) \leq g_{\tau(1)}(\bar{x}) < \ldots < f_{\sigma(k)}(\bar{x}) \leq g_{\tau(k)}(\bar{x})$ for some $\sigma,\tau \in S_k$.

Chasing inequalities: $f_{\mu(k)}(\bar{x}) = g_{\nu(k)}(\bar{x})$ for all $\bar{x} \in C$.

Then $f_{\mu(k)} = g_{\nu(k)}$, since otherwise C is contained in the hyperplane

$$H(f_{\mu(k)} = g_{\mu(k)}).$$

Matthias Aschenbrenner, Alf Dolich, Deirdre Haskell, Dugald Macpherson, and Sergei Starchenko, *Vapnik-Chervonenkis density in some theories without the independence property, II*, Notre Dame J. Form. Log. **54** (2013), no. 3-4, 311–363.

Oleg Belegradek, Ya'acov Peterzil, and Frank Wagner, *Quasi-o-minimal structures*, J. Symbolic Logic **65** (2000), no. 3, 1115–1132.

Raf Cluckers, *Presburger sets and p-minimal fields*, J. Symbolic Logic **68** (2003), no. 1, 153–162.

Gabriel Conant, *There are no intermediate structures between the group of integers and Presburger arithmetic*, arXiv:1603.00454 [math.LO], 2016.

Gabriel Conant and Anand Pillay, *Stable groups and expansions of* $(\mathbb{Z}, +, 0)$, arXiv:1601.05692 [math.LO], 2016.

Alf Dolich, Deirdre Haskell, Dugald Macpherson, and Sergei Starchenko, *Vapnik-Chervonenkis density in some theories without the independence property, I*, Trans. Amer. Math. Soc. **368** (2016), no. 8, 5889–5949.

Alfred Dolich and John Goodrick, *Strong theories of ordered abelian groups*, arXiv:1511.08274 [math.LO], 2015.

Vladimir Kadets, *Coverings by convex bodies and inscribed balls*, Proc. Amer. Math. Soc. **133** (2005), no. 5, 1491–1495 (electronic).

Itay Kaplan and Saharon Shelah, *Decidability and classification of the theory of integers with primes*, arXiv:1601.07099 [math.LO], 2016.

Christian Michaux and Roger Villemaire, *Presburger arithmetic and recognizability of sets of natural numbers by automata: new proofs of Cobham's and Semenov's theorems*, Ann. Pure Appl. Logic **77** (1996), no. 3, 251–277.

Daniel Palacín and Rizos Sklinos, *Superstable expansions of free abelian groups*, Notre Dame J. Form. Log., to appear, available: arXiv 1405.0568.

Bruno Poizat, *Supergénérix*, J. Algebra **404** (2014), 240–270, À la mémoire d'Éric Jaligot. [In memoriam Éric Jaligot].