Weakening Presburger Arithmetic

Christian Choffrut

Laboratoire LIAFA, Université de Paris 7
2, pl. Jussieu, 75251, Paris Cedex 05
cc@liafa.jussieu.fr,
http://www.liafa.jussieu.fr/~cc

Abstract. We consider logics on $\mathbb{Z}$ and $\mathbb{N}$ which are weaker than Presburger Arithmetic and we settle the following decision problem: given a k-ary relation on $\mathbb{Z}$ and $\mathbb{N}$ which is first order definable in Presburger Arithmetic, is it definable in these weaker logics? These logics, intuitively, are obtained in two different ways. First by introducing modulo and threshold counting predicates on the difference of two variables and second by depriving $\mathbb{Z}$ from the ordering.

1 Background and definitions

Presburger arithmetic is the first order theory of integers $\mathbb{Z}$ with the operation of addition and the usual ordering, though the same term might also refer to the first order theory of nonnegative integers with the addition and the equality. Whichever arithmetic is meant should be clear from the context. The validity of a closed formula in this structure is proved decidable via quantifier elimination in the extension including all predicates $x = b \mod a$ with $a \in \mathbb{N}$ and $0 \leq b < a$, see e.g., [8, Chap. III.4]. Though long underestimated, this result is nowadays one of the main tools available in model-checking and program verification and the number of papers refereeing to it exceed several hundreds. Here we are concerned with definability in various, strictly weaker substructures on the same domain or possibly on the domain of nonnegative integers. The general question is as follows: given an arbitrary Presburger formula with n free variables defining an n-ary relation, is it first order definable in the weaker structure? E., g., the binary relation in $\mathbb{Z}$ defined by the formula $\phi(x, y) = ((x > 0) \vee (x < 0)) \wedge ((y > 0) \vee (y < 0))$ is definable without the ordering but the relation $\phi(x, y) = x < y$ is not.

The substructures we investigate are summarized in table 1. The integers a, b, c satisfy the conditions $0 \leq b < a$ and $c \in \mathbb{Z}$ or $c \in \mathbb{N}$, depending on which structure it refers to. The subscripts used should suggest the general idea of *modulo* and *threshold* counting. Observe that the first structure has no predicate (except equality) while the remaining structures have no operations.

Some of these structures were studied earlier from different points of view. In [5] the author studies the complexity of the validity of a closed expression in $\mathcal{Z}_{\text{thresh}}$ and of the quantifier elimination. A precise estimate is given and compared to the similar problems in full Presburger arithmetic. The same questions

structure	domain	functions	predicates
$\mathcal{Z}$	$\mathbb{Z}$	$x+y$	$x<y$
$\mathcal{N}_p$	$\mathbb{N}$	$x+y$	$=$
$\mathcal{Z}^W$	$\mathbb{Z}$	$x+y$	$=$
$\mathcal{Z}_{\mathrm{thresh}+\mathrm{mod}}$	$\mathbb{Z}$	none	$(x \geq c)_{c\in\mathbb{Z}}, (x \pm y \geq c)_{c\in\mathbb{Z}}, (x = b \mod a)_{0\leq b<a}$
$\mathcal{N}_{\mathrm{thresh}+\mathrm{mod}}$	$\mathbb{N}$	none	$(x \geq c)_{c\in\mathbb{N}}, (x - y \geq c)_{c\in\mathbb{N}}, (x = b \mod a)_{0\leq b<a}$
$\mathcal{Z}_{\mathrm{mod}}$	$\mathbb{Z}$	none	$x \pm y \geq 0, (x = b \mod a)_{0\leq b<a}$
$\mathcal{N}_{\mathrm{mod}}$	$\mathbb{N}$	none	$x - y \geq 0, (x = b \mod a)_{0\leq b<a}$
$\mathcal{Z}_{\mathrm{thresh}}$	$\mathbb{Z}$	none	$(x \geq c)_{c\in\mathbb{Z}}, (x \pm y \geq c)_{c\in\mathbb{Z}}$
$\mathcal{N}_{\mathrm{thresh}}$	$\mathbb{N}$	none	$(x \geq c)_{c\in\mathbb{N}}, (x - y \geq c)_{c\in\mathbb{N}}$

Table 1. The different structures studied in this paper.

are solved when substituting the additive group of rationals $\mathbb{Q}$ for the group of integers. In [6] the structure $\mathcal{N}_{\mathrm{thresh}+\mathrm{mod}}$ is not obtained as a reduction of the Presburger arithmetics but rather as an extension of the first order logic of the successor. A characterization is given but no decidability issue is tackled.

Our main result is the following, cf. [2] and [1].

Theorem *Given a relation over $\mathbb{Z}$ (resp. $\mathbb{N}$) which is first order definable in Presburger Arithmetic, for each one of the structures of table 1 whose domain is $\mathbb{Z}$ (resp. $\mathbb{N}$), it is recursively decidable whether or not this relation is first order definable in this structure.*

2 The ingredients of the proof

In this section we intend to give an idea of the ingredients for the proof of the main result. We concentrate on the two structures $\mathcal{Z}^W$ and $\mathcal{Z}_{\mathrm{thresh}+\mathrm{mod}}$. In other words we are given a relation in $\mathbb{Z}^k$ defined by a $\mathcal{Z}$-formula with k free variables and we want to decide whether or not it is $\mathcal{Z}^W$- (resp. $\mathcal{Z}_{\mathrm{thresh}+\mathrm{mod}}$-) definable. The proof for the remaining structures does not require essentially different arguments.

The following is the basic result on first order definable subsets in Presburger arithmetic, see [4, 3, 7].

Theorem 1. *Given a subset $X \subseteq \mathbb{Z}^k$ (resp. $X \subseteq \mathbb{N}^k$) the following conditions are equivalent*

1. *X is a finite union of $\mathbb{Z}$-linear (resp. $\mathbb{N}$-linear) subsets, i.e, of subsets of the form $x_0+\mathbb{N}x_1+\cdots+\mathbb{N}x_n$ for some $n \geq 0$ and some $x_0, x_1, \ldots x_n \in \mathbb{Z}^k$ (resp. $\mathbb{N}^k$)*
2. *X is a finite union of $\mathbb{Z}$-simple (resp. $\mathbb{N}$-simple) subsets, i.e, of subsets of the form $x_0 + \mathbb{N}x_1 + \cdots + \mathbb{N}x_n$ for some $n \geq 0$ and some $x_0, x_1, \ldots x_n \in \mathbb{Z}^k$ (resp. $\mathbb{N}^k$) which are linearly independent as $\mathbb{Q}$-vectors.*
3. *X is first order definable in the structure $\langle \mathbb{Z}, =, <, +, 0, 1\rangle$ (resp. $\langle \mathbb{N}, =, <, +, 0, 1\rangle$)*

Furthermore, there exists a procedure which converts one form into another

2.1 The case $\mathcal{Z}_{\mathbf{thresh}+\mathbf{mod}}$

The $\mathcal{Z}_{\mathrm{thresh}+\mathrm{mod}}$-definable relations have a simple decomposition in terms of norm one vectors. Here is a precise definition. We consider the set $\{0,1,-1\}^k \cap (\mathbb{Z}^k - \{0\}^k)$ of (L_∞-) norm one vectors and we provide it with a partial ordering by writing $e \geq f$ if the following condition holds: if the i-th component of f is nonzero, then f and e have the same i-th component. These vectors are not linearly independent, however we have the disjoint union

$$\mathbb{Z}^k = \bigcup_E \left(\sum_{e \in E} (\mathbb{N} - \{0\})e \right) \tag{1}$$

where E ranges over all strictly decreasing sequences of norm one vectors and where by convention the empty sequence represents the null vector.

The decomposition mentioned above involves the family of recognizable relations in $\mathbb{N}^k$ which is an important subfamily of the Presburger definable relations. We recall its definition.

Definition 1. *A subset $X \subseteq \mathbb{N}^k$ is* recognizable *if it is a finite union of direct products such as*

$$X_1 \times \cdots \times X_k$$

where for $i = 1, \ldots, k$, X_i is a finite union of arithmetic sequences, i.e., sequences of the form $\{a + kp \mid k \in \mathbb{N}\}$ for some $a, b \in \mathbb{N}$.

We are now able to state the main characterization of the family of $\mathcal{Z}_{\mathrm{thresh}+\mathrm{mod}}$-definable relations on which the decidability result is based: indeed, recognizability in $\mathcal{Z}$ is decidable as proved in [4, Corollary 4.5].

Theorem 2. *A relation $X \subseteq \mathbb{Z}^k$ is definable in $\mathcal{Z}_{\mathrm{thresh}+\mathrm{mod}}$ if and only if it is a finite union of relations of the form*

$$X_1 e_1 + \cdots + X_p e_p$$

where $0 < p \leq k$, $e_1 > \cdots > e_p$ is a strictly decreasing sequence of norm one vector and $X_1 \times \cdots \times X_p$ is recognizable.

2.2 The case $\mathcal{Z}^W$

We proceed top-down. We are given a subset in $\mathbb{Z}^k$ defined by a $\mathcal{Z}$-formula with k free variables and we transform it into a finite union of simple sets as asserted in Theorem 1. Call the integer n appearing in the expression of the simple set its *dimension* and observe that n is at most equal to k. By applying a simple geometric transformation of the space, we show that we can always assume that this union possesses at least one element of the dimension of the space, i.e., without loss of generality equal to k. The crux of the proof is the following result.

Theorem 3. *Let $X \subseteq \mathbb{Z}^k$ be a $\mathcal{Z}$-definable set of the form $X = T \cup \bigcup_{i=1}^{m} Y_i$ where $Y_i = a^{(i)} + \sum_{j=1}^{k} \mathbb{N} b_j^{(i)}$ for some linearly independent vectors $b_j^{(i)}$ (i.e. it is a simple set of dimension k) and T is a finite union of $\mathbb{N}$-simple sets of dimension less than k. Then X is $\mathcal{Z}^W$-definable if, and only if, it can be decomposed as $S \cup (P \setminus R)$, where:*

1. $P = \bigcup_{1 \leq i \leq m} (a^{(i)} + \sum_{j=1}^{k} \mathbb{Z} b_j^{(j)})$;
2. *R and S are $\mathcal{Z}^W$-definable sets which are included in a finite union of $\mathbb{Z}$-simple sets of dimension less than k;*
3. $R \subseteq P$ *and* $S \cap P = \emptyset$.

Indeed, given X, we can compute P, test equality *1* and obtain $S = X \setminus P$ and $R = P \setminus X$. The result applies recursively to R and S.

References

1. C. Choffrut. Deciding whether a relation defined in Presburger logic can be defined in weaker logics. submitted.
2. C. Choffrut and A. Frigeri. Definable sets in weak Presburger arithmetic. submitted.
3. S. Eilenberg and M.-P. Schützenbeger. Rational sets in commutative monoids. *Journal of Algebra*, 13(2):173–191, 1969.
4. S. Ginsburg and E.H. Spanier. Bounded regular sets. In *Proc. of the Amer. Math. Soc. 17*, pages 1043–1049, 1966.
5. M. Koubarakis. The complexity of query evaluation in indefinite temporal constraint databases. *Theor. Comput. Sci.*, 171(1-2):25–60, 1997.
6. P. Péladeau. Logically defined subsets of $\mathbb{N}^k$. *Theoret. Comput. Sci.*, 93:169–193, 1992.
7. J. Sakarovitch. *Eléments de théorie des automates*. Vuibert Informatique, 2003.
8. C. Smoryński. *Logical Number Theory I: An Introduction*. Springer Verlag, 1991.