A New Proof of a Theorem by Ginsburg and Spanier

Marcus Kracht
Department of Linguistics, UCLA
405 Hilgard Avenue
PO Box 951543
Los Angeles, CA 90095–1543
kracht@humnet.ucla.edu

December 18, 2002

Abstract

In [2], Ginsburg and Spanier showed that the semilinear subsets of $\mathbb{N}^n$ are exactly the sets that are definable in Presburger Arithmetic. The proof relied on two results shown in [1]: (1) that linear equations define semilinear sets, and (2) that the complement of a semilinear set is and the intersection of semilinear sets is again semilinear. Here we offer a much simpler proof of this fact. Basically, using quantifier elimination for Presburger Arithmetic we avoid having to show closure under negation. Instead, this will now follow from the results. Second, closure under intersection will be shown using standard techniques from linear algebra.

1 Preliminaries

Let $\mathbb{N}^n$ be the set of n–tuples of natural numbers. A tuple is denoted by an arrow, eg $\vec{v}$, whose coordinates are v^i, $i < n$. Put $\vec{0} := \langle 0, 0, \ldots, 0 \rangle$. Define $\vec{v} + \vec{w}$ by

$$(\vec{v} + \vec{w})(i) = \vec{v}(i) + \vec{w}(i)$$

Denote the structure $\langle \mathbb{N}^n, \overline{0}, + \rangle$ also by $\mathbb{N}^n$. The unit vector which is 0 except at place number i, where it is 1, is denoted by $\vec{e}_i$. We define $n\vec{v}$ inductively as follows. $0\vec{v} := \overline{0}$, $(n+1)\vec{v} := n\vec{v} + \vec{v}$. We write $\mathbb{N}\vec{v}$ for the set $\{n\vec{v} : n \in \mathbb{N}\}$. Finally, for two subsets $V, W \subseteq \mathbb{N}^A$ write $\vec{v} + W := \{\vec{v} + \vec{w} : \vec{w} \in W\}$ and $V + W := \{\vec{v} + \vec{w} : \vec{v} \in V, \vec{w} \in W\}$. A nonempty subset of $\mathbb{N}^n$ is called **linear** if it can be written as

$$\vec{v}_0 + \mathbb{N}\vec{v}_1 + \mathbb{N}\vec{v}_2 + \cdots + \mathbb{N}\vec{v}_m$$

for some m (which may be zero, in which case we get the singleton $\{\vec{v}_0\}$). Likewise, a subset of $\mathbb{Z}^n$ ($\mathbb{Q}^n$) is called **linear** if it has the form

$$\vec{v}_0 + \mathbb{Z}\vec{v}_1 + \mathbb{Z}\vec{v}_2 + \cdots + \mathbb{Z}\vec{v}_m$$

for subsets of $\mathbb{Z}^n$ as well as

$$\vec{v}_0 + \mathbb{Q}\vec{v}_1 + \mathbb{Q}\vec{v}_2 + \cdots + \mathbb{Q}\vec{v}_m$$

for subsets of $\mathbb{Q}^n$. The linear subsets of $\mathbb{Q}^n$ are nothing but the affine subspaces.

A subset of $\mathbb{N}^n$ ($\mathbb{Z}^n$, $\mathbb{Q}^n$) is called **semilinear** if it is the finite union of semilinear sets. We employ the following notation.

Definition 1.1 *Let M and N be finite subsets of $\mathbb{N}^n$. Then $\Sigma(M; N)$ denotes the set of vectors of the form $\vec{u} + \sum_{i<p} k_i \vec{v}_i$ such that $\vec{u} \in M$, $k_i \in \mathbb{N}$ and $\vec{v}_i \in N$ for all $i < p$.*

Presburger Arithmetic is defined as follows. The basic symbols are $\mathtt{0}$, $\mathtt{1}$, $+$, $<$ and $\equiv_m$, $m \in \mathbb{N} - \{0, 1\}$. Then Presburger Arithmetic is the first order theory of the structure $\underline{\mathbb{Z}} := \langle \mathbb{Z}, 0, 1, +, <, \langle \equiv_m : 1 < m \in \mathbb{N} \rangle \rangle$, where $a \equiv_m b$ iff $a - b$ is divisible by m.

Negation can be eliminated.

$$\begin{array}{lcl} \neg(x \doteq y) & \leftrightarrow & x < y \vee y < x \\ \neg(x < y) & \leftrightarrow & x \doteq y \vee y < x \\ \neg(a \equiv_m b) & \leftrightarrow & \bigvee_{0<i<m} a \equiv_m b + \underline{n} \end{array}$$

where $\underline{n}$ is defined by $\underline{0} := \mathtt{0}$, $\underline{n+1} := \underline{n} + \mathtt{1}$. We shall occasionally use $x \leq y$ for $x < y \vee x \doteq y$. Moreover, multiplication by a given natural number also is definable: put $0t := \overline{0}$, and $(n+1)t := nt + t$. Every term in the variables

x_i, $i < n$, is equivalent to $b + \sum_{i<n} a_i x_i$, where $b, a_i \in \mathbb{N}$, $i < n$. A subset S of $\mathbb{Z}^n$ is **definable** if there is a formula $\varphi(x_0, x_1, \ldots, x_{n-1})$ such that

$$S = \{\langle k_i : i < n\rangle \in \mathbb{Z}^n : \underline{\mathbb{Z}} \vDash \varphi[k_0, k_1, \ldots, k_{n-1}]\}$$

The definable subsets of $\mathbb{Z}^n$ are closed under union, intersection and complement and permutation of the coordinated. Moreover, if $S \subseteq \mathbb{Z}^{n+1}$ is definable, so is its projection

$$\pi_n[S] := \{\langle k_i : i < n\rangle : \text{ there is } k_n \in \mathbb{Z} : \langle k_i : i < n+1\rangle \in S\}$$

The same holds for definable subsets of $\mathbb{N}^n$, which are simply those definable subsets of $\mathbb{Z}^n$ that are included in $\mathbb{N}^n$. Clearly, if $S \subseteq \mathbb{Z}^n$ is definable, so is $S \cap \mathbb{N}^n$.

2 Linear Equations

Lemma 2.1 *Suppose that $a + \sum_{i<n} p_i x_i = b + \sum_{i<n} q_i x_i$ is a linear equation with rational numbers a, b, p_i and q_i ($i < n$). Then there is an equivalent equation $g + \sum_{i<n} u_i x_i = h + \sum_{i<n} v_i x_i$ with positive integer coefficients such that $g \cdot h = 0$ and for every $i < n$: $v_i u_i = 0$.*

Proof. First, multiply with the least common denominator to transform the equation into an equation with integer coefficients. Next, for every $i < n$, substract $q_i x_i$ from both sides $p_i > q_i$ and $p_i x_i$ otherwise. □

Call an equation **reduced** if it has the form

$$g + \sum_{i<m} k_i x_i = \sum_{m \le i < n} k_i x_i$$

with positive integer coefficients g and k_i, $i < n$. Likewise for an inequation. Evidently, modulo renaming of variables we can transform every rational equation into reduced form.

Lemma 2.2 *The set of solutions of a reduced equation is semilinear.*

Proof. Let μ be the least common multiple of the k_i. Consider a vector of the form $\vec{c}_{i,j} = (\mu/k_i)\vec{e}_i + (\mu/k_j)\vec{e}_j$, where $i < m$ and $m \le j < n$. Then if $\vec{v}$

is a solution, so is $\vec{v}+\vec{c}_{i,j}$ and conversely. Put $C := \{\vec{c}_{i,j} : i < m, m \leq j < n\}$ and let

$$P := \left\{ \vec{u} : g + \sum_{i<m} k_i \vec{u}(i) = \sum_{m \leq j < n} k_i \vec{u}(i), \text{ for all } i < n : \vec{u}(i) < \mu/k_i \right\}$$

Both P and C are finite. Moreover, the set of solutions is exactly $\Sigma(P; C)$.

Lemma 2.3 *The set of solutions of a reduced inequation is semilinear.*

Proof. Assume that the inequation has the form

$$g + \sum_{i<m} k_i x_i \leq \sum_{m \leq i < n} k_i x_i$$

Define C and P as before. Let $E := \{\vec{e}_i : m \leq i < n\}$. Then the set of solutions is $\Sigma(P; C \cup E)$. If the inequation has the form

$$g + \sum_{i<m} k_i x_i \geq \sum_{m \leq i < n} k_i x_i$$

the set of solutions is $\Sigma(P; C \cup F)$ where $F := \{\vec{e}_i : i < m\}$. □

Lemma 2.4 *Let $M \subseteq \mathbb{Q}^n$ be an affine subspace. Then $M \cap \mathbb{Z}^n$ is a semilinear subset of $\mathbb{Z}^n$.*

Proof. Let $\vec{v}_i$, $i < n+1$, be vectors such that

$$M = \vec{v}_0 + \mathbb{Q}\vec{v}_1 + \mathbb{Q}\vec{v}_2 + \cdots + \mathbb{Q}\vec{v}_{m-1}$$

We can assume that the $\vec{v}_i$ are linearly independent. Clearly, since $\mathbb{Q}\vec{w} = \mathbb{Q}(\lambda\vec{w})$ for any nonzero rational number λ, we can assume that $\vec{v}_i \in \mathbb{Z}^n$, $i < m$. Now, let $V := \{\vec{v}_0 + \sum_{0<i<m} \lambda_i \vec{v}_i : 0 \leq \lambda_i < 1\}$. $V \cap \mathbb{Z}^n$ is finite. Moreover, if $\vec{v}_0 + \sum_{0<i<m} \kappa_i \vec{v}_i \in \mathbb{Z}^n$ then also $\vec{v}_0 + \sum_{0<i<m} \kappa'_i \vec{v}_i \in \mathbb{Z}^n$ if $\kappa_i - \kappa'_i \in \mathbb{Z}$. Hence,

$$M = \bigcup_{\vec{w} \in V} \vec{w} + \mathbb{Z}\vec{v}_1 + \ldots \mathbb{Z}\vec{v}_m$$

This is a semilinear set. □

Lemma 2.5 *Let $M \subseteq \mathbb{Z}^n$ be a semilinear subset of $\mathbb{Z}^n$. Then $M \cap \mathbb{N}^n$ is semilinear.*

Proof. It suffices to show this for linear subsets. Let $\vec{v}_i$, $i < n+1$, be vectors such that

$$M = \vec{v}_0 + \mathbb{Z}\vec{v}_1 + \mathbb{Z}\vec{v}_2 + \cdots + \mathbb{Z}\vec{v}_{m-1}$$

Put $\vec{w}_i := -\vec{v}_i$, $0 < i < m$. Then

$$M = \vec{v}_0 + \mathbb{N}\vec{v}_1 + \mathbb{N}\vec{v}_2 + \cdots + \mathbb{N}\vec{v}_{m-1} + \mathbb{N}\vec{w}_1 + \ldots + \mathbb{N}\vec{w}_{m-1}$$

Thus, we may without loss of generality assume that

$$M = \vec{v}_0 + \mathbb{N}\vec{v}_1 + \mathbb{N}\vec{v}_2 + \cdots + \mathbb{N}\vec{v}_{m-1}$$

Notice, however, that these vectors are not necessarily in $\mathbb{N}^n$. For i starting at 1 until n we do the following.

Let $x^i_j := \vec{v}_j(i)$. Assume that for $0 < j < p$, $x^i_j \geq 0$, and that for $p \leq j < m$, $x^i_j > 0$. (A renaming of the variables can achieve this.) We introduce new cyclic vectors $\vec{c}_{j,k}$ for $0 < j < p$ and $p \leq k < m$. Let μ the least common multiple of the $|x^i_s|$, for all $0 < s < m$ where $x^i_s \neq 0$:

$$\vec{c}_{i,j} := (\mu/x^i_j)\vec{v}_j + (\mu/x^i_k)\vec{v}_k$$

Notice that the s–coordinates of these vectors are positive for $s < i$, since this is a positive sum of positive numbers. The ith coordinate of these vectors is 0. Suppose that the ith coordinate of

$$\vec{w} = \vec{v}_0 + \sum_{0<j<m} \lambda_j \vec{v}_j$$

is ≥ 0, where $\lambda_j \in \mathbb{N}$ for all $0 < j < m$. Suppose further that for some $k \geq p$ we have $\lambda_k \geq v^i_0 + m(\mu/|x^i_k|)$. Then there must be a $j < p$ such that $\lambda_j \geq (\mu/x^i_j)$. Then put $\lambda'_r := \lambda_r$ for $r \neq j, k$, $\lambda'_j := \lambda_j - (\mu/x^i_j)$ and $\lambda'_k := \lambda_k + (\mu/x^i_k)$. Then

$$\vec{w} = \vec{c}_{j,k} + \sum_{0<j<m} \lambda'_j \vec{v}_j$$

Moreover, $\lambda'_j \leq \lambda_j$ for all $j < p$, and $\lambda'_k < \lambda_k$. Thus, by adding these cyclic vectors we can see to it that the coefficients of the $\vec{v}_k$ for $p \leq k < m$ are bounded. Now define P to be the set of

$$\vec{w} = \vec{v}_0 + \sum_{0<j<m} \lambda_j \vec{v}_j \in \mathbb{N}^n$$

where $\lambda_j < v_0^j + m|\mu/x_j^i|$ for all $0 < j < m$. Then

$$M \cap \mathbb{N}^n = \bigcup_{\vec{u} \in P} \vec{u} + \sum_{0<j<p} \lambda_j \vec{v}_j + \sum_{0<j<p \leq k<m} \kappa_{j,k} \vec{c}_{j,k}$$

with all λ_j, $\kappa_{j,k} \geq 0$. Now we have achieved that all jth coordinates of vectors are positive. □

The following is now immediate.

Lemma 2.6 *Let $M \subseteq \mathbb{Q}^n$ be an affine subspace. Then $M \cap \mathbb{N}^n$ is a semilinear subset of $\mathbb{N}^n$.*

Lemma 2.7 *The intersection of two semilinear sets is again semilinear.*

Proof. It is enough to show the claim for linear sets. So, let $C_0 = \{\vec{u}_i : i < m\}$, $C_1 = \{\vec{v}_i : i < n\}$ and $S_0 := \Sigma(\{\vec{v}_0\}; C_0)$ and $S_1 := \Sigma(\{\vec{v}_1\}; C_1)$ be linear. We will show that $S_0 \cap S_1$ is semilinear. To see this, notice that $\vec{w} \in S_0 \cap S_1$ iff there are natural numbers κ_i $(i < m)$ and λ_j $(j < n)$ such that

$$\vec{w} = \vec{c} + \sum_{i<m} \kappa_i \vec{u}_i = \vec{e} + \sum_{i<n} \lambda_i \vec{v}_i$$

So, we have to show that the set of these $\vec{w}$ is semilinear.

The equations are now taken as linear equations with κ_i, $i < m$ and λ_i, $i < n$, as variables. Thus we have equations for $m + n$ variables. We solve these equations first in $\mathbb{Q}^{m+n}$. They form an affine subspace of $\mathbb{Q}^{m+n} \cong \mathbb{Q}^m \oplus \mathbb{Q}^n$. By the Lemma 2.6, the intersection of the set with $\mathbb{N}^{m+n}$ is semilinear, and so is its projection onto $\mathbb{N}^m$ (or to $\mathbb{N}^n$ for that matter). Let it be $\bigcup_{i<p} L_i$, where for each $i < p$, $L_i \subseteq \mathbb{N}^m$ is linear. Thus there is a representation of L_i as

$$L_i = \vec{\theta} + \mathbb{N}\vec{\eta}_0 + \ldots \mathbb{N}\vec{\eta}_{\gamma-1}$$

Now put

$$W_i := \{\vec{v}_0 + \sum_{i<m} \vec{\kappa}(i)\vec{u}_i : \vec{\kappa} \in L_i\}$$

From the construction we get that

$$S_0 \cap S_1 = \bigcup_{i<p} W_i$$

Define vectors $\vec{q}_i := \sum_{j<m} \vec{\eta}(j)_i \vec{u}_i$, $i < \gamma$ and $\vec{r} := \vec{c} + \sum_{j<m} \vec{\theta}(j)\vec{u}_i$. Then

$$W_i = \vec{r} + \mathbb{N}\vec{q}_0 + \ldots + \mathbb{N}\vec{q}_{\gamma-1}$$

So, W_i is linear. This shows the claim. □

Lemma 2.8 *If $S \subseteq \mathbb{N}^n$ is semilinear, so is its projection $\pi_n[S]$.*

2.1 The Theorem

We need one more prerequisite. Say that a first–order theory T has **quantifier elimination** if for every formula $\varphi(\vec{x})$ there exists a quantifier free formula $\chi(\vec{x})$ such that $T \vdash \varphi(\vec{x}) \leftrightarrow \chi(\vec{x})$. We follow the proof of [3].

Theorem 2.9 (Presburger) *Presburger Arithmetic has quantifier elimination.*

Proof. It is enough to show that for every formula $(\exists x)\varphi(\vec{y}, x)$ with $\varphi(\vec{y}, x)$ quantifier free there exists a quantifier free formula $\chi(\vec{y})$ such that

$$\mathbb{Z} \vDash (\forall \vec{y})((\exists x)\varphi(\vec{y}, x) \leftrightarrow \chi(\vec{y}))$$

Now, we may further eliminate negation (see the remarks above) and disjunctions inside $\varphi(\vec{y}, x)$ (since $(\exists x)(\alpha \vee \beta) \leftrightarrow (\exists x)\alpha \vee (\exists x)\beta)$). Finally, we may assume that all conjuncts contain x. For if α does not contain x free, $(\exists x)(\alpha \wedge \beta)$ is equivalent to $\alpha \wedge (\exists x)\beta$. So, φ can be assumed to be a conjunction of atomic formulae of the following form:

$$(\exists x)(\bigwedge_{i<p} n_i x \doteq t_i \wedge \bigwedge_{i<q} n'_i x < t'_i \wedge \bigwedge_{i<r} n''_i x > t''_i \wedge \bigwedge_{i<s} n'''_i x \equiv_{m_i} t'''_i)$$

Now, $s \equiv t$ is equivalent with $ns \equiv nt$, so after suitable multiplication we may see to it that all the n_i, n'_i, n''_i and n'''_i are the same number ν.

$$(\exists x)(\bigwedge_{i<p} \nu x \doteq \tau_i \wedge \bigwedge_{i<q} \nu x < \tau'_i \wedge \bigwedge_{i<r} \nu x > \tau''_i \wedge \bigwedge_{i<s} \nu x \equiv_{m_i} \tau'''_i)$$

We may rewrite the formula in the following way (replacing νx by x and the condition that x is divisible by ν).

$$(\exists x)(x \equiv_\nu 0 \wedge \bigwedge_{i<p} x \doteq \tau_i \wedge \bigwedge_{i<q} x < \tau'_i \wedge \bigwedge_{i<r} x > \tau''_i \wedge \bigwedge_{i<s} x \equiv_{m_i} \tau'''_i)$$

Assume that $p > 0$. Then the first set of conjunctions is equivalent with the conjunction of $\bigwedge_{i<j<p} \tau_i \equiv \tau_j$ (which does not contain x) and $x \doteq \tau_0$. We may therefore eliminate all occurrences of x by τ_0 in the formula.

Thus, from now on we may assume that $p = 0$. Also, notice that $x < \sigma \wedge x < \tau$ is equivalent to $(x < \sigma \wedge \sigma \leq \tau) \vee (x < \tau \wedge \tau < \sigma)$. This means that we can assume $q \leq 1$, and likewise that $r \leq 1$. Next we show that we can actually have $s \leq 1$. To see this, notice the following.

> Let u, v, w, x be integers, $w, x > 1$, and let p be the least common multiple of w and x. Then $gcd(p/w, p/x) = 1$, and so there exist integers m, n such that $1 = m \cdot p/w + n \cdot p/x$. It follows that the following are equivalent.
>
> 1. $y \equiv u \pmod{w}$ and $y \equiv v \pmod{x}$
> 2. $u \equiv v \pmod{gcd(w,x)}$ and $y \equiv m(p/w)u + n(p/x)v \pmod{p}$.

Using this equivalence we can reduce the congruence statements to a conjunction of congruences where only one involves x.

This leaves us with 8 possibilities. If $r = 0$ or $s = 0$ the formula is actually trivially true. That is to say, $(\exists x)(x < \tau)$, $(\exists x)(v < x)$, $(\exists x)(x \equiv_m \xi)$, $(\exists x)(x < \tau \wedge x \equiv_m \xi)$ and $(\exists x)(v < x \wedge x \equiv_m \xi)$ are equivalent to $\top$. Finally, it is verified that

$$\begin{array}{lcl} (\exists x)(x < \tau \wedge v < x) & \leftrightarrow & v\mathtt{+1} < \tau \\ (\exists x)(x < \tau \wedge v < x \wedge x \equiv_m \xi) & \leftrightarrow & \bigvee_{i<m}(\tau\mathtt{+1+}i < v \wedge \tau\mathtt{+1+}i \equiv_m \xi) \end{array}$$

□

Theorem 2.10 (Ginsburg & Spanier) *A subset of $\mathbb{N}^n$ is semilinear iff it is definable in Presburger Arithmetic.*

Proof. ($\Rightarrow$) Every semilinear set is definable in Presburger Arithmetic. To see this it is enough to show that linear sets are definable. For if M is a union of N_i, $i < p$, and each N_i is linear and hence definable by a formula $\varphi_i(\vec{x})$, then M is definable by $\bigvee_{i<p} \varphi_i(\vec{x})$. Now let $M = \vec{v} + \mathbb{N}\vec{v}_0 + \ldots + \mathbb{N}\vec{v}_{m-1}$ be linear. Then put

$$\varphi(\vec{x}) := (\exists y_0)(\exists y_1)\ldots(\exists y_{m-1})\left(\bigwedge_{i<m} \mathtt{0} \leq y_i \wedge \bigwedge_{i<n}(\vec{v}(i) \mathtt{+} \sum_{j<m} y_i \vec{v}(i)_j \doteq x_i)\right)$$

$\varphi(\vec{x})$ defines M. ($\Rightarrow$) Let $\varphi(\vec{x})$ be a formula defining S. By Theorem 2.9, there exists a quantifier free formula $\chi(\vec{x})$ defining S. Moreover, as we have remarked above, χ can be assumed to be negation free. Thus, χ is a disjunction of conjunctions of atomic formulae. By Lemma 2.7, the set of semilinear subsets of $\mathbb{N}^n$ is closed under intersection of members, and it is also closed under union. Thus, all we need to show is that atomic formulae define semilinear sets. Now, observe that $x_0 \equiv_m x_1$ is equivalent to $(\exists x_2)(x_0 \doteq x_1 + mx_2)$, which is semilinear, as it is the projection of $x_0 \doteq x_1 + mx_2$ onto the first two components. □

Corollary 2.11 *The complement of a semilinear set is again semilinear.*

References

[1] Seymour Ginsburg and Edwin H. Spanier. Bounded ALGOL–Like Languages. *Transactions of the American Mathematical Society*, 113:333 – 368, 1964.

[2] Seymour Ginsburg and Edwin H. Spanier. Semigroups, Presburger Formulas, and Languages. *Pacific Journal of Mathematics*, 16:285 – 296, 1966.

[3] J. Donald Monk. *Mathematical Logic*. Springer, Berlin, Heidelberg, 1976.