Semi-Linear Sets

Goal: • Show that semi-linear sets are precisely the sets of numbers that are Presburger-definable.

• Next step: Parikh-images.

$$\begin{tikzcd} \text{semi-linear} \arrow[rr, bend left, "\text{Closure under } *"] \arrow[rr, phantom, "="] & & \text{Presburger-definable} \arrow[ll, bend left, "\text{Closure under } \neg"] \end{tikzcd}$$

Consequences: • Closure of semi-linear sets under complement (cool)

• Closure of Presburger-definable sets under iteration.

Definition (Semi-linear sets)

Let $c \in \mathbb{N}^n$ be a vector and $P \subseteq \mathbb{N}^n$ a finite set of vectors.

Define $\mathcal{L}(c, P) := \{ v \in \mathbb{N}^n \mid \exists k_1, \ldots, k_n \in \mathbb{N} : v = c + \sum_{i=1}^{n} k_i p_i$ with $p_1, \ldots, p_n \in P \}$.

Here, c is called <u>constant</u> and P is called set of <u>periods</u>

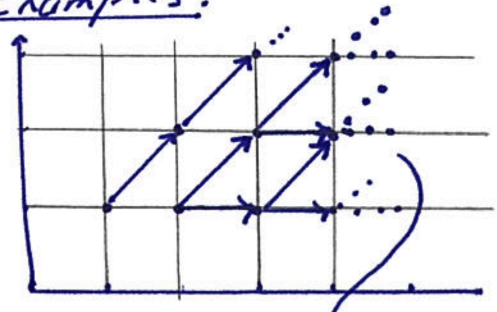
A set $M \subseteq \mathbb{N}^n$ is <u>linear</u> if

$M = \mathcal{L}(c, P)$ for some $c \in \mathbb{N}^n$, $P \subseteq \mathbb{N}^n$ finite.

A set $S \subseteq \mathbb{N}^n$ is <u>semi-linear</u> if it is a finite union of linear sets.

Examples:

$\mathcal{L}(\binom{1}{1}, \{\binom{1}{1}\})$



$\mathcal{L}(\binom{2}{1}, \{\binom{1}{0}, \binom{1}{1}\})$

Remark:

(1) Given a linear set $\mathcal{L}(c, P) \subseteq \mathbb{N}^n$ and a vector $v \in \mathbb{N}^n$, it is decidable whether $v \in \mathcal{L}(c, P)$ holds.

The same decidability holds for semi-linear sets.

(2) Linear sets are <u>not</u> closed under any of the Boolean operations, i.e., if $M \subseteq \mathbb{N}^n$ is linear, then $\overline{M}$ need not be linear.

$M_1, M_2 \subseteq \mathbb{N}^n$ $\qquad M_1 \cap M_2$

(3) The class of semi-linear sets properly includes the linear sets (every linear set is semi-linear).

Closure Properties of Semi-Linear Sets

Definition (Linear functions)

A function $f: \mathbb{N}^n \to \mathbb{N}^m$ is linear, if

$f(x+y) = f(x) + f(y)$ and $f(kx) = k f(x)$ with $k \in \mathbb{N}$.

Lemma (Semi-linear sets are closed under linear mappings)

Let $S \subseteq \mathbb{N}^n$ be semi-linear

and $f: \mathbb{N}^n \to \mathbb{N}^m$ be linear.

Then $f(S) \subseteq \mathbb{N}^m$ is semi-linear.

Definition (Iteration)

Let $A \subseteq \mathbb{N}^n$. Define

$$A^* := \{ v_1 + \dots + v_k \in \mathbb{N}^n \mid k \in \mathbb{N} \text{ and } v_1, \dots, v_k \in A \}.$$

Lemma (Semi-linear sets are closed under iteration):

If $S \subseteq \mathbb{N}^n$ is semi-linear, so is S^*.

Proof:

Let $S = \mathcal{L}(c_1, P_1) \cup \dots \cup \mathcal{L}(c_l, P_l)$.

One can show that

$$S^* = \bigcup_{I \subseteq \{1,\dots,l\}} \mathcal{L}\Big(\sum_{i \in I} c_i, \bigcup_{i \in I} P_i \cup \{c_i\} \Big).$$

$\square$

Lemma:

If $S \subseteq \mathbb{N}^n$ is semi-linear and $c \in \mathbb{N}^n$,

then $c + S := \{ c + x \mid x \in S \}$ is semi-linear.

<u>Theorem</u> (Semi-linear sets are closed under $\cup$ and $\cap$)

Let S_1 and S_2 be semi-linear.

Then $S_1 \cup S_2$ and $S_1 \cap S_2$ are semi-linear.

<u>Proof:</u>

„$\cup$" There is nothing to do. ✓

„$\cap$" It is sufficient to show that the intersection of linear sets is semi-linear.

<u>Why:</u>

$$M_1 \cap (M_2 \cup M_3) = (M_1 \cap M_2) \cup (M_1 \cap M_3).$$

↳ Consider

$$\mathcal{L}(c, \{u_1, \dots, u_m\}) \text{ and } \mathcal{L}(d, \{v_1, \dots, v_n\})$$

↳ Define

$$A := \{(x_1, \dots, x_m, y_1, \dots, y_n) \in \mathbb{N}^{m+n} \mid c + \sum x_i u_i = d + \sum y_i v_i\}$$

$$B := \{(x_1, \dots, x_m, y_1, \dots, y_n) \in \mathbb{N}^{m+n} \mid \sum x_i u_i = \sum y_i v_i\}$$

<u>Intuition:</u>

A = Coefficients for period vectors that lead to elements in $\mathcal{L}(c, \{u_1, \dots, u_m\}) \cap \mathcal{L}(d, \{v_1, \dots, v_n\})$.

B = Coefficients for period vectors that do not leave the intersection.

↳ Show that A and B are semi-linear.

Define

$S_A :=$ minimal elements of A

$S_B :=$ minimal elements of $B \setminus \{0\}$.

These sets are

- computable and
- guaranteed to be finite.

<u>Claim:</u>

$$\mathcal{A} = \bigcup_{s \in S_{\mathcal{A}}} \mathcal{L}(s, S_{\mathcal{B}})$$

$$\mathcal{B} = \mathcal{L}(0, S_{\mathcal{B}})$$

Hence, both $\mathcal{A}$ and $\mathcal{B}$ are semi-linear.

↳ Consider now $f : \mathbb{N}^{m+n} \longrightarrow \mathbb{N}^m$ with

$$f(x_1, \dots, x_m, y_1, \dots, y_n) := x_1 u_1 + \dots + x_m u_m .$$

This function f is linear.

Hence, by lemma above,

$f(\mathcal{A})$ is semi-linear.

Hence, by lemma above

$c + f(\mathcal{A})$ is semi-linear.

This is it, by definition of $\mathcal{A}$:

$$c + f(\mathcal{A})$$
$$= \mathcal{L}(c, \{u_1, \dots, u_m\}) \cap \mathcal{L}(d, \{v_1, \dots, v_n\}).$$

<u>It remains to prove the claim about</u> $=$:

Show equality for $\mathcal{A}$, uses equality for $\mathcal{B}$:

„$\supseteq$" Show that $\mathcal{L}(s, S_{\mathcal{B}}) \subseteq \mathcal{A}$

by induction on structure of $\mathcal{L}(s, S_{\mathcal{B}})$.

<u>IA:</u> s is a minimal element of $\mathcal{A}$, hence $s \in \mathcal{A}$.

<u>IS:</u> Suppose $q \in \mathcal{L}(s, S_{\mathcal{B}})$ satisfies

$$c + \sum_{1 \le i \le m} q(i) u_i = d + \sum_{1 \le j \le n} q(m+j) v_j$$

Consider $q + p$ with $p \in S_{\mathcal{B}}$.

For $p \in S_B$, we have

$$\sum_{1 \le i \le m} p(i) u_i = \sum_{1 \le j \le n} p(m+j) v_j .$$

Hence:

$$c + \sum_{1 \le i \le m} (q(i) + p(i)) u_i$$

$$= c + \sum_{1 \le i \le m} q(i) u_i + \sum_{1 \le i \le m} p(i) u_i$$

(IV & Obs) $$= d + \sum_{1 \le j \le n} q(m+j) v_j + \sum_{1 \le j \le n} p(m+j) v_j .$$

$$= d + \sum_{1 \le j \le n} (q(m+j) + p(m+j)) v_j .$$

This means $q + p \in A$.

„$\subseteq$" Show that $A = \bigcup_{s \in S_A} \mathcal{L}(s, S_B)$.

Let $p \in A$.
By definition of minimality, there is $q \le p$ with $q \in S_A$.
Hence:

$$\sum_{1 \le i \le m} (p(i) - q(i)) u_i$$

$$= \sum_{1 \le i \le m} p(i) u_i - \sum_{1 \le i \le m} q(i) u_i$$

(Since $p, q \in A$) $$= \overbrace{(d-c) + \sum_{1 \le j \le n} p(m+j) v_j}^{=} - \left((d-c) + \sum_{1 \le j \le n} q(m+j) v_j\right)$$

$$= \sum_{1 \le j \le n} p(m+j) v_j - \sum_{1 \le j \le n} q(m+j) v_j$$

$$= \sum_{1 \le j \le n} (p(m+j) - q(m+j)) v_j$$

This means $p - q \in B$.

Since
$$B = \mathcal{L}(0, S_B),$$
we get
$$q + (p-q) \in \mathcal{L}(q, S_B)$$
Hence,
$$p \in \mathcal{L}(q, S_B) \subseteq \bigcup_{s \in S_A} \mathcal{L}(s, S_B).$$
$\square$

An application of this result:

<u>Lemma</u> (Semi-linear sets are closed under inverse linear mappings)

Let $S \subseteq \mathbb{N}^n$ be semi-linear and
$f : \mathbb{N}^m \to \mathbb{N}^n$ a linear function.
Then $f^{-1}(S) \subseteq \mathbb{N}^m$ is semi-linear.

<u>Proof</u>:

Let $x = (x_1, \dots, x_a)$ and $y = (y_1, \dots, y_b)$. We use the notation $x.y := (x_1, \dots, x_a, y_1, \dots, y_b)$.

Define
$$g : \mathbb{N}^m \longrightarrow \mathbb{N}^{m+n} \text{ by}$$
$$g(x) := x.f(x).$$
By linearity of f, also g is linear.
Thus, by lemma above,
$$g(\mathbb{N}^m) \text{ is semi-linear.}$$
Moreover,
$$\mathbb{N}^m.S \text{ is semi-linear.}$$
Since semi-linear sets are closed under intersection:
$$\underbrace{g(\mathbb{N}^m) \cap \mathbb{N}^m.S}_{x.f(x) \text{ so that } f(x) \in S} \text{ is semi-linear.}$$

Let $h: \mathbb{N}^{m+n} \to \mathbb{N}^m$ by $h(x,y) := x$.

This h is linear and thus

$$h\left(g(\mathbb{N}^m) \cap \mathbb{N}^m . S\right) = f^{-1}(S)$$

is semi-linear. $\square$