Introduction to Tree Language Theory

Hitoshi Ohsaki

National Institute of
Advanced Industrial Science and Technology (AIST)

seminar talk (7/10)

2009

VII. Parikh's theorem

Commutative image

Let L : language over T (terminals)

c(L) is the commutative image of L if $\forall u \in \Sigma^*$, $\exists u \in$ c(L) iff $\exists w \in L$: u, w are equivalent under the axiom $xy \approx yx$

Let $T = \{a_1, \ldots, a_n\}$

$\sharp_{a_i}(u)$ is the number of occurrences of a_i in a word u

$\sharp_T(u)$ is the vector $(\sharp_{a_1}(u), \ldots, \sharp_{a_n}(u))$

$\Psi_T(L)$ is $\{\, \sharp_T(u) \mid u \in L \,\}$, called Parikh image of L

Note

- $\Psi_T(L) = \Psi_T(\text{c}(L))$
- $\Psi_T(L) = \Psi_T(M)$ if and only if c(L) = c(M)

  $\because$ $\sharp_T(u) = \sharp_T(w)$ if and only if u, w are equivalent under the axiom $x\,y \approx y\,x$

Remark

$\mathbb{N}^{|T|}$ (vectors) and $T^*/_{\approx}$ (commutative words) are isomorphic :

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
T^* \arrow[r, "\mathsf{c}"] \arrow[d, "\Psi_T"] & T^*/_{\approx} \arrow[d, shift left, "h"] \\
\mathbb{N}^{|T|} \arrow[r, shift left, "g"] & \mathsf{mul}(T) \arrow[l, shift left, "g^{-1}"] \arrow[u, shift left, "h^{-1}"]
\end{tikzcd}
$$

$$g(v) = \bigcup_{i=1}^{|T|}{}_{\mathsf{mul}} \{ \overbrace{\mathsf{a}_i, \ldots, \mathsf{a}_i}^{v(i)} \}_{\mathsf{mul}}$$

$$g(u+v) = g(u) \cup_{\mathsf{mul}} g(v)$$

$$h(\varepsilon) = \varnothing$$

$$h(\mathsf{a}) = \{\mathsf{a}_i\}_{\mathsf{mul}}$$

$$h(xy) = h(x) \cup_{\mathsf{mul}} h(y)$$

$\mathsf{mul}(A)$: set of multisets over A, $\cup_{\mathsf{mul}}$: multiset union, $\{\cdot\}_{\mathsf{mul}}$: multiset

Non-negative vector addition systems (NNVAS)

NNVAS $V = (c, \{v_1, \ldots, v_k\})$ on $\mathbb{N}^n$

c	:	vector in $\mathbb{N}^n$,	called constant
$v_1, \ldots, v_k$	:	vectors in $\mathbb{N}^n$,	called periods

$*$ Originally, VAS [1] is equipped with vectors $v_1, \ldots, v_n$ from $\mathbb{Z}^n$ as periods.

predicate Φ_V of NNVAS V :

$$\Phi_V(v) \quad \Leftrightarrow \quad \exists x_1, \cdots, x_k, \in \mathbb{N} \colon v = c + (x_1 \times v_1) + \cdots + (x_k \times v_k)$$

set $[\![V]\!]$ generated by NNVAS V :

$$[\![V]\!] = \{ \, v \in \mathbb{N}^n \mid \Phi_V(v) \, \}$$

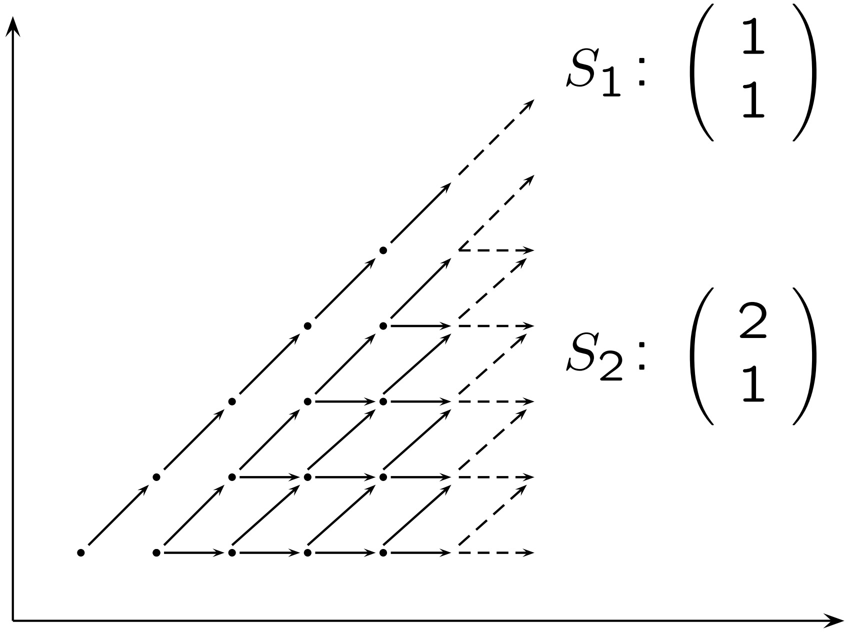
Note

$\Phi_V(v)$ if and only if $v \in [\![V]\!]$ ($\Phi_V(v) \stackrel{?}{\equiv}$ true is decidable, so $v \stackrel{?}{\in} [\![V]\!]$ is decidable)

[1] L.H. Landweber: *Properties of Vector Addition Systems*, technical report 258, University of Wisconsin-Madison, USA, June 1975.

Semi-linear sets

S is a linear set if $\exists$ NNVAS $V = (c, \{v_1, \ldots, v_k\})$ such that $S = [\![V]\!]$



$$S_1: \begin{pmatrix} 1 \\ 1 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$S_2: \begin{pmatrix} 2 \\ 1 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Semi-linear set is a finite union $S_1 \cup \cdots \cup S_n$ of linear sets

Note

- Linear sets are not closed under any Boolean operation. (Exercise)
- The class of semi-linear sets properly includes that of linear sets.

Closure properties

Semi-linear sets are closed under Boolean operations

Proof of $\cup$

Obvious by definition of semi-linearity.

Proof of $\cap$

Let $U = (c, \{u_1, \ldots, u_m\})$ and $V = (d, \{v_1, \ldots, v_n\})$. Define

$$A = \{(x_1, \ldots, x_m, y_1, \ldots, y_n) \in \mathbb{N}^{m+n} \mid c + \textstyle\sum_{1 \leqslant i \leqslant m} x_i u_i = d + \sum_{1 \leqslant j \leqslant n} y_j v_j\}$$
$$B = \{(x_1, \ldots, x_m, y_1, \ldots, y_n) \in \mathbb{N}^{m+n} \mid \textstyle\sum_{1 \leqslant i \leqslant m} x_i u_i = \sum_{1 \leqslant j \leqslant n} y_j v_j\}.$$

One can compute the sets S_A, S_B of minimal positive elements of A and $B - \mathbf{0}$, respectively, and S_A and S_B are finite (Appendix (C)-(1)), where $\mathbf{0}$ is the vector containing only 0. For each $s \in S_A$, define an NNVAS $W_s = (s, S_B)$. We show that $A = \bigcup_{s \in S_A} [\![W_s]\!]$ in the following.

For "$\supseteq$", use the induction on (the structure of) W_s. The base case is obvious, because s is a minimal element of A. For the induction step, suppose $p \in S_B$ and $q \in [\![W_s]\!]$ where $q = c + \sum_{1 \leqslant i \leqslant m} q(i) u_i = d + \sum_{1 \leqslant j \leqslant n} q(m+j) v_j$. Since p is a minimal element of B, it satisfies $\sum_{1 \leqslant i \leqslant m} p(i) u_i = \sum_{1 \leqslant j \leqslant n} p(m+j) v_j$. Then, $p + q = c + \sum_{1 \leqslant i \leqslant m} (p(i) + q(i)) u_i = d + \sum_{1 \leqslant j \leqslant n} (p(m+j) + q(m+j)) v_j$. Hence, $p + q \in A$.

For "$\subseteq$", suppose $p \in A$. From minimality, $q \leqslant p$ for some $q \in S_A$. (Proof cont'd)

Proof of $\cap$ (cont'd)

This implies that : $\sum_{1\leqslant i\leqslant m}(p(i)-q(i))u_i = \sum_{1\leqslant i\leqslant m}p(i)u_i - \sum_{1\leqslant i\leqslant m}q(i)u_i = (d-c)+\sum_{1\leqslant j\leqslant n}p(m+j)v_j - ((d-c)+\sum_{1\leqslant j\leqslant n}q(m+j)v_j) = \sum_{1\leqslant j\leqslant n}p(m+j)v_j - \sum_{1\leqslant j\leqslant n}q(m+j)v_j$, and thus, $p-q\in B$. Observe that $B=[\![(\mathbf{0},S_B)]\!]$: "$\supseteq$" is obvious, and "$\subseteq$" is shown by structural induction. Since $q+(p-q)\in[\![W_q]\!]$, $p\in[\![W_q]\!]$.

Let f be the function from $\mathbb{N}^{m+n}$ to $\mathbb{N}^m$ such that $f(p)=\sum_{1\leqslant i\leqslant m}p(i)u_i$. Obviously, $f(p+q)=f(p)+f(q)$, so f is a linear function (page 21). Since semi-linearity is closed under linear mapping, $\{f(w)\mid w\in A\}$ is semi-linear (Appendix (A)-(2)), and thus, $[\![U]\!]\cap[\![V]\!]=\{c+f(w)\mid w\in A\}$ is semi-linear. $\square$

Proof sketch of $(\,)^{\mathsf{c}}$

Suppose that S is a finite union of linear sets $T_1,\ldots,T_n$. By de Morgan's law, $(S)^{\mathsf{c}}=(T_1)^{\mathsf{c}}\cap\cdots\cap(T_n)^{\mathsf{c}}$. So it suffices to show that the complement of a linear set is semi-linear. Let $V=(c,\{v_1,\ldots,v_n\})$ be an NNVAS on $\mathbb{N}^k$, and define $V_0=(\mathbf{0},\{v_1,\ldots,v_n\})$. Then, (1) $([\![V_0]\!])^{\mathsf{c}}$ is semi-linear (Appendix (B)), (2) $X=\{x\in\mathbb{N}^k\mid c\not\leqslant x\}$ is semi-linear, (3) let $Y=\{y\in\mathbb{N}^k\mid c\leqslant y\}$, then $([\![V]\!])^{\mathsf{c}}=X\cup(Y-[\![V]\!])$. Let f be the function of $\mathbb{N}^k$ such that $f(x)=x+c$. Since f is a bijective function of $\mathbb{N}^k$ onto Y, $Y-[\![V]\!]$ is semi-linear if and only if $f^{-1}(Y-[\![V]\!])$ is semi-linear. Observe that $f^{-1}(Y-[\![V]\!])=f^{-1}(Y)-f^{-1}([\![V]\!])=\mathbb{N}^k-[\![V_0]\!]$. According to (1) & (2), $f^{-1}(Y-[\![V]\!])$, which is $([\![V_0]\!])^{\mathsf{c}}$, is semi-linear, and hence, $X\cup(Y-[\![V]\!])$ is semi-linear. $\square$

[1] S. Ginsburg: *Mathematical Theory of Context-Free Languages*, McGraw-Hill, 1966.

Parikh's theorem

Given CFG $\mathcal{G} = (\Sigma, T, N, \mathsf{q}_0, \Delta)$,

1. there exist NNVAS's $V_1, \ldots, V_k$ such that $\Psi_T(\mathcal{L}(\mathcal{G})) = \bigcup_{1 \leqslant i \leqslant k} [\![V_i]\!]$, and V_i $(1 \leqslant i \leqslant k)$ is effectively computable from $\mathcal{G}$
   (Parikh image of context-free language is effectively semi-linear)
2. there exists a regular language L such that $\mathsf{c}(\mathcal{L}(\mathcal{G})) = \mathsf{c}(L)$.
   (Commutative images of the classes of CFL and RL coincide)

Proof

First we show (1) : For each $Q \subseteq N$, define $\mathcal{L}_Q(\mathcal{G}) = \{\, w \in \Sigma^* \mid w$ is obtained from a derivation tree in which every non-terminal symbol of N appears$\}$. Observe that $\mathcal{L}(\mathcal{G}) = \bigcup_{Q \subseteq N} \mathcal{L}_Q(\mathcal{G})$, and thus, $\Psi_T(\mathcal{L}(\mathcal{G})) = \bigcup_{Q \subseteq N} \Psi_T(\mathcal{L}_Q(\mathcal{G}))$. Define the conditions

(a) all q in Q occur in the tree,

(b) no q in Q occurs more than $|N|$-times on any path from the root to a leaf.

And then, define the sets D_Q, $\tilde{D}_Q$ of derivation trees whose root is q_0 :

$D_Q = \{\, t \mid$ derivation tree t whose leaves are terminals and that satisfies (a) & (b) $\}$

$\tilde{D}_Q = \{\, t \mid$ derivation tree t whose leaves are terminals and that satisfies (a) $\}$

(Proof cont'd)

Proof (cont'd)

Moreover, define the set I_Q as follows :

$$I_Q = \left\{ t \;\middle|\; \begin{array}{l} \text{derivation tree } t \text{ whose root is } q \in Q \text{ and whose leaves contain exactly} \\ \text{one non-terminal } q \text{ and that satisfies (b)} \end{array} \right\}$$

Let

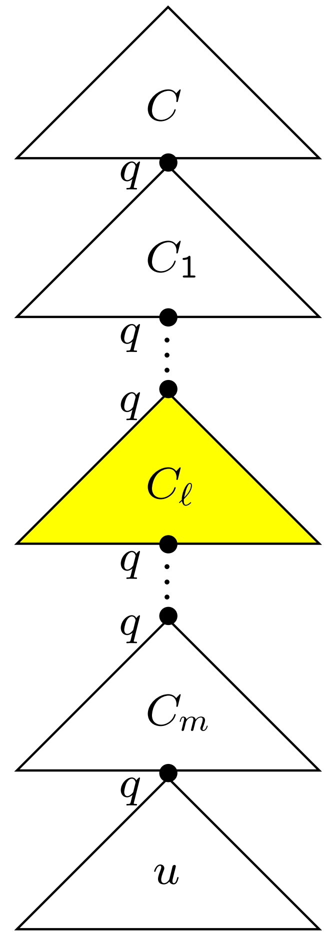
$$V_Q = \bigcup_{s \in D_Q} [\![\, (\sharp_T(\mathrm{leaf}(s)), \{\, \sharp_T(\mathrm{leaf}(t)) \mid t \in I_Q \,\}) \,]\!],$$

then we show that for each $Q \subseteq N$, $V_Q = \Psi_T(\mathcal{L}_Q(\mathcal{G}))$. For "$\subseteq$", use the induction on vectors in V_Q. In the base case, consider some $s \in D_Q$ such that $\sharp_T(\mathrm{leaf}(s))$ is a constant in V_Q. By definition, $\mathrm{leaf}(s) \in \mathcal{L}_Q(\mathcal{G})$, and thus, $\sharp_T(\mathrm{leaf}(s)) \in \Psi_T(\mathcal{L}_Q(\mathcal{G}))$. For induction step, suppose $v_1 \in V_Q$ and $v_2 = \sharp_T(\mathrm{leaf}(t))$ for some $t \in I_Q$. By induction hypothesis, $v_1 \in \Psi_T(\mathcal{L}_Q(\mathcal{G}))$, and thus, there exists a derivation tree $u \in \tilde{D}_Q$ such that $\mathrm{leaf}(u) \in \mathcal{L}_Q(\mathcal{G})$ and $\sharp_T(\mathrm{leaf}(u)) = v_1$. If the root of t is labeled by $q \in Q$ (so $\mathrm{leaf}(t) = w_1\, q\, w_2$), then $t = C[q]$. Since $u = C'[u']$ for some u' such that the root of u' is labeled by q, the tree $C'[C[u']]$ (obtained by inserting C in between C' and u') is a derivation tree in $\tilde{D}_Q$. Since $\sharp_T(\mathrm{leaf}(C'[C[u']])) = \sharp_T(\mathrm{leaf}(C'[u'])) + \sharp_T(\mathrm{leaf}(C)) = v_1 + \sharp_T(\mathrm{leaf}(t)) = v_1 + v_2$, we obtain $v_1 + v_2 \in \Psi_T(\mathcal{L}_Q(\mathcal{G}))$.

Next, for "$\supseteq$", use the induction on trees in $\tilde{D}_Q$. In the base case, consider $t \in D_Q$. By definition, $\sharp_T(\mathrm{leaf}(t)) \in V_Q$. For induction step, suppose $t \in \tilde{D}_Q$ and $t \notin D_Q$ such that every tree u in $\tilde{D}_Q$ smaller than t satisfies $\sharp_T(u) \in V_Q$. (Proof cont'd)

Proof (cont'd)

By assumption, t has a path (from the root to a leaf) that contains a non-terminal $q \in Q$ occurring more than $|Q|$-times. Let $n = |Q|$. Then, $t = C[C_1[\cdots C_m[u]\cdots]]$ such that the root of C_i ($1 \leqslant i \leqslant m$ & $n < m$) and the root of u are q. See the right figure. Here C is possibly the empty context. We will obtain a smaller tree from t by removing a context among $C_1, \ldots, C_m$. If some of non-terminals in Q appears only in C_i, C_i can not be a candidate, because the resulting tree is not in $\tilde{D}_Q$. However, since $|Q - \{q\}| = n - 1 < m$, there is at least a context, say C_ℓ (yellow part), such that $t' \in \tilde{D}_Q$ where $t' = C[C_1[\cdots C_{\ell-1}[C_{\ell+1}[\cdots C_m[u]\cdots]]\cdots]]$. By induction hypothesis, leaf$(t') \in V_Q$. If C_k satisfies the condition (b), leaf(t') + leaf$(C_\ell) \in V_Q$, because leaf$(C_\ell) \in I_Q$. If there is no such context in $C_1, \ldots, C_m$, find another non-terminal from Q that occurs more than $|Q|$-times in the same root-leaf path, because this path does not satisfy the condition (b). Repeating this process, one can eventually find a context satisfying (b).



For (2), take the regular grammar $\mathcal{G}_V$ with production rules $\mathsf{q}_0 \to \mathsf{a}_1^{c(1)} \cdots \mathsf{a}_n^{c(n)} \mid \mathsf{a}_1^{v_1(1)} \cdots \mathsf{a}_n^{v_1(n)} \mathsf{q}_0 \mid \cdots \mid \mathsf{a}_1^{v_k(1)} \cdots \mathsf{a}_n^{v_k(n)} \mathsf{q}_0$ for NNVAS $V = (c, \{v_1, \ldots, v_k\})$ on $\mathbb{N}^n$, where $v_i(j)$ is j-th element of vector v_i, then $\Psi_T(\mathcal{L}(\mathcal{G}_V)) = [\![V]\!]$. This implies that for every semi-linear set S, there exists a regular grammar $\mathcal{G}$ such that $\Psi_T(\mathcal{L}(\mathcal{G})) = S$. $\square$

Language inequations

Let Σ : alphabet with $T = \{a_1, \ldots, a_m\}$ and $N = \{x_1, \ldots, x_n\}$

L_Σ is a set of language components over Σ :

$$\varepsilon,\ a_1 \ldots, a_m,\ x_1, \ldots, x_n,\ \perp,\ uw,\ u + w \ \in\ \mathsf{L}_\Sigma \text{ if } u, w \in \mathsf{L}_\Sigma$$

$f(x_1, \ldots, x_n) \leq x_i$ is a language inequation if $f(x_1, \ldots, x_n) \in \mathsf{L}_\Sigma$

Let $L_1, \ldots, L_n$: languages over T

$f(x_1, \ldots, x_n)$: language components over Σ

$[f(x_1, \ldots, x_n)](L_1, \ldots, L_n)$ is value of $f(x_1, \ldots, x_n)$:

$$[\varepsilon](L_1, \ldots, L_n) = \{\varepsilon\} \qquad [\perp](L_1, \ldots, L_n) = \varnothing$$

$$[a_i](L_1, \ldots, L_n) = \{a_i\} \qquad [x_i](L_1, \ldots, L_n) = L_i$$

$$[uw](L_1, \ldots, L_n) = [u](L_1, \ldots, L_n) \cdot [w](L_1, \ldots, L_n)$$

$$[u + w](L_1, \ldots, L_n) = [u](L_1, \ldots, L_n) \cup [w](L_1, \ldots, L_n)$$

Solutions of language inequations

Let $f_i(x_1, \ldots, x_n) \leq x_i$: language inequations over Σ $(1 \leqslant i \leqslant n)$

$L_1, \ldots, L_n$: languages over T

$(L_1, \ldots, L_n)$ is a solution of $f_i(x_1, \ldots, x_n) \leq x_i$

if L_i is a minimal language satisfying $[f_i(x_1, \ldots, x_n)](L_1, \ldots, L_n) \subseteq L_i$

Note 1 (Ginsburg & Rice)

$(L_1, \ldots, L_n)$ is a solution of $f_i(x_1, \ldots, x_n) \leq x_i$ $(1 \leqslant i \leqslant n)$ iff $L_i = \mathcal{L}(\mathcal{G}_i)$ such that $\mathcal{G}_i = (\Sigma \cup \{\perp\}, P, \{x_1, \ldots, x_n, \perp\}, x_i, \{\, x_i \to f_i(x_1, \ldots, x_n) \mid 1 \leqslant i \leqslant n\colon f_i(x_1, \ldots, x_n) \leq x_i \,\})$

Note 2

We say $(L_1, \ldots, L_n)$ is a solution of $f_i(x_1, \ldots, x_n) \leq x_i$ over a commutative alphabet if L_i is a minimal language satisfying $\mathrm{c}([f_i(x_1, \ldots, x_n)](L_1, \ldots, L_n)) \subseteq \mathrm{c}(L_i)$. In this definition, L_i in $(L_1, \ldots, L_n)$ is always a regular language $(1 \leqslant i \leqslant n)$. However, this is not a consequence of Parikh's theorem. (Proof is explained later)

[1] S. Ginsburg & H.G. Rice: *Two Families of Languages Related to ALGOL*, Journal of Association for Computing Machinery (ACM) 9, pp.350–371, 1962.

Commutative Kleene algebra

Commutative Kleene algebra with variables X is $(A, X, \{+, \cdot, {}^*, 1, 0\})$

A : carrier set

X : finite set of variables

such that the following axioms hold for operators :

[Associativity]	[Commutativity of +]	[Commutativity of ·]
$(x+y)+z = x+(y+z)$	$x+y = y+x$	$x \cdot y = y \cdot x$
[Distributivity]	[Identity of +]	[Identity of ·]
$x \cdot (y+z) = x \cdot y + x \cdot z$	$x+0 = x$	$x \cdot 1 = x$
[Idempotency]	[Nullpotency]	[Kleene star]
$x+x = x$	$x \cdot 0 = 0$	$1 + x \cdot x^* = x^*$

Corollary

$(x+y)^* = x^* \cdot y^*$ $\quad$ $x + y \cdot z \leq z \Rightarrow x \cdot y^* \leq z$ $\quad$ $(x \leq y \Leftrightarrow x + y = y)$

Differential operator

Let $K[X]$: commutative Kleene algebra with variables X

D is mapping from $K[X]$ to $K[X]$ such that (called differential operator)

$$
\begin{aligned}
D(x+y) &= D(x) + D(y)\\
D(x \cdot y) &= x \cdot D(y) + y \cdot D(x)\\
D(x^*) &= x^* \cdot D(x)\\
D(1) &= D(0) = 0
\end{aligned}
$$

$\frac{\partial}{\partial x}$ is differential operator for $x \in X$ such that

$$
\begin{aligned}
\frac{\partial x}{\partial x} &= 1\\
\frac{\partial y}{\partial x} &= 0 \text{ if } y \in X - \{x\}\\
\frac{\partial a}{\partial x} &= 0 \text{ if } a \in A\\
\frac{\partial}{\partial x}(f(e)) &= \frac{\partial f}{\partial x}(e) \cdot \frac{\partial e}{\partial x}
\end{aligned}
$$

($\frac{\partial f}{\partial x}$ is denoted by $f'(x)$)

Solution of $f_i(x_1, \ldots, x_n) \leq x_i$ in $K[X]$

Let $f(x_1, \ldots, x_n)$: finite expression in $K[X]$

$e_1, \ldots, e_n$: finite expressions in $K[\varnothing]$

$(e_1, \ldots, e_n)$ is solution of $f(x_1, \ldots, x_n) \leq x_i$ in $K[X]$

if e_i is a minimal subset of A satisfying $f(e_1, \ldots, e_n) \subseteq e_i$

Proposition (Hopkins & Kozen 1999)

Every $f(x) \leq x$ in $K[\{x\}]$ has the unique solution $f'(f(0))^* \cdot f(0)$

Proof

First, we observe that for all polynomials e, g, h, k in $K[X]$,

(1) $e(x+g) = e(x) + e'(x+g) \cdot g$

$e(g) = e(0) + e'(g) \cdot g$ if $x = 0$

(2) $e \cdot h \leq g \cdot h \Rightarrow k(e) \cdot h \leq k(g) \cdot h$

Each statement can be shown by the induction on the structure of polynomials.

(Proof cont'd)

Proof (cont'd)

Let $e = g\cdot h$, $g = f(0)$, $h = f'(g)^*$ in the previous (2), then $e\cdot h = f(0)\cdot f'(g)^*\cdot f'(g)^* = f(0)\cdot f'(g)^*$ and $g\cdot h = f(0)\cdot f'(g)^*$. Thus, for any polynomial k, $k(g\cdot h)\cdot h \le k(g)\cdot h$ in this case. Therefore, one can conclude that $f'(f(0))\cdot f(0)$ satisfies $f(x) \le x$:

$$
\begin{array}{rcll}
f(f'(f(0))^*\cdot f(0)) & = & f(g\cdot h) & \\
 & = & f(0) + f'(g\cdot h)\cdot g\cdot h & \text{by (1)} \\
 & \le & f(0) + f'(g)\cdot g\cdot h & \text{by the above observation} \\
 & = & g + f'(g)\cdot g\cdot f'(g)^* & \\
 & = & (1 + f'(g)\cdot f'(g)^*)\cdot g & \\
 & = & f'(g)^*\cdot g & \text{by [Kleene star]} \\
 & = & f'(f(0))^*\cdot f(0) &
\end{array}
$$

For the "least" solution, we show that for every polynomial k in $K[\{x\}]$ that satisfies $f(k) \le k$, $f'(f(0))^*\cdot f(0) \le k$. According to Corollary in page 13, it suffices to show that $f(0) + f'(f(0))\cdot k \le k$: From monotonicity $f(0) \le f(k)$ (as $0 \le k$) and the assumption $f(k) \le k$, one can have $f'(f(0)) \le f'(k)$. Thus,

$$
\begin{array}{rcll}
f(0) + f'(f(0))\cdot k & \le & f(0) + f'(k)\cdot k & \\
 & \le & f(k) & \text{by (1)} \\
 & \le & k & \text{by assumption}
\end{array}
$$

Hence, uniqueness is justified by the fact that $f'(f(0))^*\cdot f(0)$ is the least solution. $\Box$

Corollary (Generalization of Parikh's theorem)

Every system of inequations $f_i(x_1, \ldots, x_n) \leq x_i$ $(1 \leqslant i \leqslant n)$ in $K[X]$ has the unique solution, and is effectively computable from $f_1, \ldots, f_n$

Proof

Suppose $X = \{x, y\}$, and let the system of inequations : $f(x, y) \leq x$ and $g(x, y) \leq y$. First, freeze x, meaning that we consider $K[\{x\}][\{y\}]$ instead of $K[\{x, y\}]$. According to the previous proposition, one can compute the (least) solution $h(x)$ of the inequation $g(x, y) \leq y$. And then, compute the solution of $f(x, h(x)) \leq x$ in $K[\{x\}]$. Let $(k, h(k))$ be the solution obtained by this computation. For the claim that $(k, h(k))$ is the least solution, let (p, q) be a solution of the above system. Since the least solution of $g(p, y) \leq y$ is $h(p)$ where x in $g(x, y)$ is instantiated by p, $h(p) \leq q$. By monotonicity and the assumption that (p, q) is a solution, $f(p, h(p)) \leq f(p, q) \leq p$. Because k is the least solution of $f(x, h(x))$, one can conclude that $k \leq p$. Therefore,

$$\begin{array}{rcll} (k, h(k)) & \leq & (k, h(p)) & \text{by monotonicity } (k \leq p) \\ & \leq & (p, q) & \text{by the above observation } (h(p) \leq q) \end{array}$$

Iteratively applying the above computation to the system S of inequations in $K[X]$, it results in the least solution of S. $\square$

Example

Consider the CFG $\mathcal{G}_1, \mathcal{G}_2$ with the following production rules :

$$\Delta_1 \; : \quad \mathsf{q}_0 \rightarrow \mathsf{a}\,\mathsf{q}_0\mathsf{b} \qquad \mathsf{q}_0 \rightarrow \varepsilon$$

$$\begin{array}{lllll} \Delta_2 \; : & \mathsf{q}_0 \rightarrow \mathsf{a}\,\mathsf{q}_1 & \mathsf{q}_0 \rightarrow \mathsf{b}\,\mathsf{q}_2 & \mathsf{q}_0 \rightarrow \varepsilon \\ & \mathsf{q}_1 \rightarrow \mathsf{a}\,\mathsf{q}_1\,\mathsf{q}_1 & \mathsf{q}_1 \rightarrow \mathsf{b}\,\mathsf{q}_0 & \\ & \mathsf{q}_2 \rightarrow \mathsf{a}\,\mathsf{q}_0 & \mathsf{q}_2 \rightarrow \mathsf{b}\,\mathsf{q}_2\,\mathsf{q}_2 & \end{array}$$

Then $\mathcal{L}(\mathcal{G}_1)$ and $\mathcal{L}(\mathcal{G}_2)$ are solutions for x of the following systems, respectively :

$$S_1 \; : \quad \mathsf{ab}x + 1 \leq x$$

$$S_2 \; : \quad \mathsf{a}y + \mathsf{b}z + 1 \leq x \qquad \mathsf{a}y^2 + \mathsf{b}x \leq y \qquad \mathsf{a}x + \mathsf{b}z^2 \leq z$$

For S_1, according to Proposition (Hopkins & Kozen 1999), let $f(x) = \mathsf{ab}x + 1$, $f'(f(0))^* \cdot f(0) = (\mathsf{ab})^* \cdot 1 = (\mathsf{ab})^*$ that is equivalent to $\mathcal{L}(\mathcal{G}_1)$ under commutativity.

For S_2, let $f(x,y,z) = \mathsf{a}y + \mathsf{b}z + 1$, $g(x,y,z) = \mathsf{a}y^2 + \mathsf{b}x$, $h(x,y,z) = \mathsf{a}x + \mathsf{b}z^2$. First, freeze x, y, meaning that consider $K[\{x\}][\{y\}][\{z\}]$ for $K[\{x,y,z\}]$: Let $\ell_h(z) = \mathsf{a}x + \mathsf{b}z^2$, then $z = \ell'_h(\ell_h(0))^* \cdot \ell_h(0) = (\mathsf{ab}x)^* \cdot \mathsf{a}x$. Next, let $\ell_g(y,z) = \mathsf{a}y^2 + \mathsf{b}x$, and then consider $\ell_g(y, (\mathsf{ab}x)^* \cdot \mathsf{a}x) = \mathsf{a}y^2 + \mathsf{b}x$. Similar to the previous step, we obtain $y = (\mathsf{ab}x)^* \cdot \mathsf{b}x$. Finally, consider $f(x, (\mathsf{ab}x)^* \cdot \mathsf{b}x, (\mathsf{ab}x)^* \cdot \mathsf{a}x) = (\mathsf{ab}x) \cdot (\mathsf{ab}x)^* + 1 = (\mathsf{ab}x)^*$. Let $p(x) = (\mathsf{ab}x)^*$, then computing $p'(x)$ and $p'(p(0))^* \cdot p(0)$ is Exercise.

Exercise

1. Show that the commutative image of a context-free language is not context-free.
2. Construct examples showing the claim in page 5 that the class of linear sets is not closed under union, intersection or complement.
3. Show that semi-linearity is closed under projection, meaning that for every projection f_i such that $f_i(v) = (v(1), \ldots, v(i-1), v(i+1), \ldots, v(k))$, if S is a semi-linear subset of $\mathbb{N}^k$, then $f_i(S) = \{f_i(v) \mid v \in S\}$ is semi-linear.
4. Show that semi-linearity is closed under $\times$, meaning that if S and T are semi-linear subsets of $\mathbb{N}^m$ and of $\mathbb{N}^n$, then $S \times T$ is semi-linear.
5. Construct an example showing that for a language L over T, $\Psi_T(L)$ is semi-linear but L is not context-free.
6. Show that $\{ w \in \{\mathsf{a}, \mathsf{b}\}^* \mid |w|_{\mathsf{a}} = (|w|_{\mathsf{b}})^2 \}$ is not context-free.
7. Show that every context-free language over a one-letter alphabet is regular.
8. Compute $p'(x)$ and the solution for x, y, z of S_2 in page 18.

Appendix (A) : Basic properties of semi-linear sets

(1) Every linear set on $\mathbb{N}^k$ is a finite union of linear sets on $\mathbb{N}^k$, each of which is linearly independent periods

Proof

Use the induction on the number of periods. The base case is obvious, because a linear set (obtained by an NNVAS) with one period satisfies (1). For induction step, let $L = [\![V]\!]$ where $V = (c, \{v_1, \ldots, v_n\})$, and suppose $v_1, \ldots, v_n$ is linearly dependent. Then, there exist a permutation π over $\{1, \ldots, n\}$, non-negative integers t_i $(1 \leqslant i \leqslant k)$ and positive integers t_j $(k < j \leqslant n)$ such that $\sum_{1 \leqslant i \leqslant k} t_i\, v_{\pi(i)} = \sum_{k+1 \leqslant j \leqslant n} t_j\, v_{\pi(j)}$ $(*)$. For each j $(k < j \leqslant n)$, define $C_j = \{c + xv_{\pi(j)} \mid 0 \leqslant x < t_j\}$ and $P_j = \{v_1, \ldots, v_n\} - \{v_{\pi(j)}\}$. Let $L_j = \bigcup_{0 \leqslant x < t_j} [\![(c + xv_{\pi(j)}, P_j)]\!]$, then by induction hypothesis, L_j is the finite union of linear sets, each of which satisfies (1).

Next, we show that $L = \bigcup_{k<j\leqslant n} L_j$. By construction, $L_j \subseteq L$ $(k < j \leqslant n)$, and thus, $\bigcup_{k<j\leqslant n} L_j \subseteq L$. For "$\supseteq$", let $v = c + \sum_{1 \leqslant i \leqslant n} d_i v_{\pi(i)}$ in $\mathbb{N}^k$. If $d_j \geqslant t_j$ $(k < j \leqslant n)$, then take $u_1 = c + \sum_{1 \leqslant i \leqslant k}(d_i + t_i)v_{\pi(i)} + \sum_{k<j\leqslant n}(d_j - t_j)v_{\pi(j)}$. From $(*)$, $v = u_1$. After ℓ-times application of the above procedure, one can obtain u_ℓ such that $v = u_\ell$ and a coefficient of $v_{\pi(j)}$ is less than t_j for some j $(k < j \leqslant n)$. Let $u_\ell = c + \sum_{1 \leqslant i \leqslant n} e_i v_{\pi(i)}$, then $u_\ell \in L_j$, because $c + e_j v_{\pi(j)} \in C_j$ and $\{v_1, \ldots, v_n\} - \{v_{\pi(j)}\} = P_j$. $\square$

As a corollary of (1), it follows that : every semi-linear set on $\mathbb{N}^k$ is a finite union of linear sets on $\mathbb{N}^k$, each of which is linearly independent periods.

Appendix (A) : Basic properties of semi-linear sets (cont'd)

A function f from $\mathbb{N}^m$ to $\mathbb{N}^n$ is linear if $f(x+y) = f(x) + f(y)$:

(2) Semi-linearity is closed under linear mapping, meaning that for every linear function f from $\mathbb{N}^m$ to $\mathbb{N}^n$, if S is a semi-linear subset of $\mathbb{N}^m$, then $f(S) = \{f(v) \mid v \in S\}$ is semi-linear.

Proof

It suffices to show that linearity is closed under linear mapping. Let $L = [\![V]\!]$ where $V = (c, \{v_1, \ldots, v_k\})$, then $f(L) = [\![V']\!]$ where $V' = (f(c), \{f(v_1), \ldots, f(v_k)\})$. So, for every $x \in L$, $f(x) \in f(L)$. Conversely, if $u \in f(L)$, then $u = f(c) + \sum_{1 \leqslant i \leqslant k} y_i f(v_i) = f(c + \sum_{1 \leqslant i \leqslant k} y_i v_i)$. Hence, $u = f(z)$ for some $z \in L$. $\square$

(3) Semi-linearity is closed under inverse linear-mapping, meaning that if S is a semi-linear subset of $\mathbb{N}^m$, then $f^{-1}(S) = \{v \in \mathbb{N}^m \mid \exists f(v) \in S\}$ is semi-linear.

Proof

For $p = (x_1, \ldots, x_a)$ and $q = (y_1, \ldots, y_b)$, we denote $p \times q$ for $(x_1, \ldots, x_a, y_1, \ldots, y_b)$. Let g be the function $g(x) = x \times f(x)$. From linearity of f, we have $g(x+y) = (x+y) \times (f(x) + f(y)) = (x \times f(x)) + (y \times f(y)) = g(x) + g(y)$. So, g is a linear function. From (2), $g(\mathbb{N}^m)$ is a semi-linear subset of $\mathbb{N}^{m+n}$. Moreover, since $\mathbb{N}^m \times S$ is semi-linear, $g(\mathbb{N}^m) \cap (\mathbb{N}^m \times S)$ is semi-linear, because semi-linearity is closed under intersection. Let h be the projection $h(x \times y) = x$, then $h(g(\mathbb{N}^m) \cap (\mathbb{N}^m \times S)) = f^{-1}(S)$. Hence, $f^{-1}(S)$ is semi-linear, because semi-linearity is closed under projection. $\square$

Appendix (B) : Complement of semi-linear sets

For every NNVAS $V = (\mathbf{0}, \{v_1, \ldots, v_n\})$ on $\mathbb{N}^k$ with linearly independent vectors $v_1, \ldots, v_n$, $([\![V]\!])^{\mathsf{C}}$ is semi-linear. ($\mathbf{0}$ is the vector containing only 0)

Proof

If $k > n$, then find a mapping π from $\{1, \ldots, k-n\}$ to $\{1, \ldots, k\}$ such that for unit vectors $e_{\pi(1)}, \ldots, e_{\pi(k-n)}$ (each e_i of which contains exactly one 1 at i-th position and the other elements are 0), $v_1, \ldots, v_n, e_{\pi(1)}, \ldots, e_{\pi(k-n)}$ are linearly independent. So one can take $V' = (\mathbf{0}, \{v_1, \ldots, v_k\})$ and $v_1, \ldots, v_k$ are linearly independent. Then, it holds that : there exists a positive integer $\ell_{V'}$ for V' such that $\mathbb{N}^k = \{\, u \mid \exists x \in \mathbb{N},\ \exists y_1, \ldots, y_k \in \mathbb{Z} : 1 \leqslant x \leqslant \ell_{V'}\ \&\ xu = \sum_{1 \leqslant i \leqslant k} y_i v_i \,\}$. First, we show that for each subset I of $\{1, \ldots, k\}$, $S_I = \{\, u \times (y_1, \ldots, y_k) \mid \exists x, y_1, \ldots, y_k \in \mathbb{N} : xu + \sum_{i \in I} y_i v_i = \sum_{j \notin I} y_j v_j \,\}$ is effectively semi-linear. Note that $S_I \subseteq \mathbb{N}^{2k}$. Define the function $f_{I,x}$ of $\mathbb{N}^{2k}$ such that $f_{I,x}(p \times q) = (xp + \sum_{i \in I} q(i) v_i) \times \sum_{j \notin I} q(j) v_j$, and define g from $\mathbb{N}^k$ to $\mathbb{N}^{2k}$ such that $g(r) = r \times r$. Let $F = f_{I,x}((p_1 \times q_1) + (p_2 \times q_2))$, then

$$
\begin{aligned}
F &= f_{I,x}((p_1 + p_2) \times (q_1 + q_2)) \\
&= ((xp_1 + \textstyle\sum_{i \in I} q_1(i) v_i) + (xq_1 + \sum_{i \in I} q_2(i) v_i)) \times (\sum_{i \notin I} q_1(i) v_i + \sum_{i \notin I} q_2(i) v_i) \\
&= ((xp_1 + \textstyle\sum_{i \in I} q_1(i) v_i) \times \sum_{i \notin I} q_1(i) v_i) + ((xq_1 + \sum_{i \in I} q_2(i) v_i) \times \sum_{i \notin I} q_2(i) v_i) \\
&= f_{I,x}(p_1 \times p_2) + f_I(q_1 \times q_2),
\end{aligned}
$$

so $f_{I,x}$ is a linear function. Moreover, g is a linear function, because $g(x+y) = (x+y) \times (x+y) = (x \times x) + (y \times y) = g(x) + g(y)$. (Proof cont'd)

Appendix (B) : Complement of semi-linear sets (cont'd)

From (1), $D = \{ g(p) \mid p \in \mathbb{N}^k \}$ is semi-linear. From (3), $f^{-1}_{I,x}(D)$ is semi-linear. Observe that $\bigcup_{1 \leqslant x \leqslant \ell_V} f^{-1}_{I,x}(D) = \bigcup_{1 \leqslant x \leqslant \ell_V} \{ p \in \mathbb{N}^{2k} \mid f_{I,x}(p) \in D \} = S_I$.

Next, for each non-empty subset I of $\{1, \ldots, k\}$, define $c_I = (0, \ldots, 0, a_1, \ldots, a_k)$ where $a_i = 1$ if $i \in I$; otherwise, $a_i = 0$. Let $E_I = (c_I, \{e_1, \ldots, e_{2k}\})$ such that e_i $(1 \leqslant i \leqslant 2k)$ is the unit vector whose i-th element is 1, and let $h(x \times y) = x$. For each $I \subseteq \{1 \leqslant x \leqslant \ell_V\}$ with $I \neq \varnothing$, define $K_I = \bigcup_{1 \leqslant x \leqslant \ell_V} [\![E_I]\!] \cap f^{-1}_{I,x}(D)$, then K_I is semi-linear, and thus, $h(K_I)$ is semi-linear, because h is a linear function. We take $T_I = h(K_I)$. Since $T_I = \{u \in \mathbb{N}^k \mid \exists x, y_1, \ldots, y_k \in \mathbb{N} \colon xu = \sum_{i \in I} (-y_i)v_i + \sum_{j \notin I} y_j v_j \;\&\; y_i > 0 \;(i \in I)\}$, $T_I \cap [\![V']\!] = \varnothing$ for all non-empty subset I.

Next, define an NNVAS P_i $(n < i \leqslant k)$ where $P_i = (e_{n+i}, \{e_1, \ldots, e_{2k}\})$ and n is the number of periods of V. Since $[\![P_i]\!]$ is semi-linear, $[\![P_i]\!] \cap K_I$ is semi-linear for each $I \subseteq \{1, \ldots, k\} - \{i\}$. Let $U_I = \bigcup_{n < i \leqslant k} h([\![P_i]\!] \cap K_I)$. If $I \subseteq \{1, \ldots, k\} - \{i\}$, then $U_I = \{u \in \mathbb{N}^k \mid \exists x, j \in \mathbb{N}, \exists y_1, \ldots, y_k \in \mathbb{Z} \colon xu = \sum_{i \in I} y_i v_i \;\&\; y_j > 0 \;\&\; j > n\}$. Hence, $U_I \cap [\![V']\!] = \varnothing$.

Next, for each x $(1 \leqslant x \leqslant \ell_V)$ and j $(1 \leqslant j \leqslant n)$, where n is the number of periods of V, let

$$
\begin{aligned}
Q_{x,j} &= \{ u \times y \mid \exists y \in \mathbb{N}^n \colon xu = \textstyle\sum_{1 \leqslant i \leqslant n} y(i) v_i \;\;\&\;\; y(j) \bmod x \neq 0 \} \\
R_x &= \{ u \times y \mid \exists y \in \mathbb{N}^n \colon xu = \textstyle\sum_{1 \leqslant i \leqslant n} y(i) v_i \;\;\&\;\; y \neq \mathbf{0} \}.
\end{aligned}
$$

We show that for every x and j, $Q_{x,j}$ is effectively semi-linear. The set $\min_{\geqslant}(R_x)$ of minimal solutions of R_x is finite and computable (Appendix (C)). (Proof cont'd)

Appendix (B) : Complement of semi-linear sets (cont'd)

Observe that $R_x = [\![(\mathbf{0}, \min_{\geqslant}(R_x))]\!]$. Moreover,

$$Q_{x,j} \;=\; R_x \cap \{\, p \times y \mid \exists p \in \mathbb{N}^k, y \in \mathbb{N}^n \colon 1 \leqslant y(j) < x \,\}$$

Since $\{\, p \times y \mid \exists p \in \mathbb{N}^k, y \in \mathbb{N}^n \colon 1 \leqslant y(j) < x \,\}$ is effectively semi-linear, $Q_{x,j}$ is so. Let h' be the function from $\mathbb{N}^{k+n}$ to $\mathbb{N}^k$ such that $h'(p \times y) = p$, then $h'(Q_{x,j})$ is semi-linear, because h' is a linear function.

Finally, we show that

$$([\![V']\!])^{\mathsf{C}} = \bigcup_{\varnothing \neq I \subseteq \{1,\ldots,\ell_V\}} T_I \;\cup \bigcup_{1 \leqslant i \leqslant k, I \subseteq \{1,\ldots,k\}-\{i\}} U_I \;\cup \bigcup_{1 \leqslant x \leqslant \ell_V, 1 \leqslant j \leqslant n} h'(Q_{x,j}).$$

By construction, "$\supseteq$" is obvious : We already verified for the first two cases. For the last case, suppose $v \in Q_{x,j}$ for some x ($1 \leqslant x \leqslant \ell_V$) and j ($1 \leqslant j \leqslant n$), which means that $xv = \sum_{1 \leqslant i \leqslant n} y(i) v_i$ and $y(j)$ cannot be divided by x. This implies that if $x = 1$, $y(j)$ cannot be an integer. Hence, $v \notin [\![V']\!]$.

For "$\subseteq$", suppose $v \in ([\![V']\!])^{\mathsf{C}}$, then there exists $x \in \mathbb{N}$, $y_1, \ldots, y_k \in \mathbb{Z}$ such that $1 \leqslant x \leqslant \ell_V$ and $xv = \sum_{1 \leqslant i \leqslant k} y_i v_i$. If $y_i < 0$ ($1 \leqslant i \leqslant k$), then $v \in T_I$ for some non-empty subset I of $\{1, \ldots, \ell_V\}$. If $y_i > 0$ ($n+1 \leqslant i \leqslant k$), then $v \in U_I$ for some $1 \leqslant j \leqslant k, I \subseteq \{1, \ldots, k\} - \{j\}$. So, assume $y_i \geqslant 0$ ($1 \leqslant i \leqslant n$). If for all i ($1 \leqslant i \leqslant n$), y_i is divided by x, $v \in [\![V']\!]$. Thus, there exists j such that y_j is not divided by x. Hence, $v \in h'(Q_{x,j})$. $\square$

Alternative proof is obtained by bijective correspondence to Presburger arithmetic, where negation can be eliminated, and so negation-free NNVAS formula is obtained.

Appendix (C) : Minimal solutions

Every semi-linear set $\bigcup_{1 \leqslant i \leqslant n} [\![(c_i, \{v_{p_i(q_i)}\})]\!]$ contains only finitely minimal elements c_i $(1 \leqslant i \leqslant n)$. This observation can be generalized as follows :

(1) Every set of incomparable vectors in $\mathbb{N}^k$ is finite.

Proof

Use the induction on k. The base case is obvious, because $k = 1$. For induction step, define the projection f_k from $\mathbb{N}^k$ to $\mathbb{N}^{k-1}$ such that $f_k(v) = (v(1), \ldots, v(k-1))$. Suppose for leading to the contradiction that there exists an infinite subset S of $\mathbb{N}^k$ whose elements are pairwise incomparable. For each $u, v \in S$, one of the following holds : (a) $f_k(u)$ and $f_k(v)$ are incomparable, (b) $f_k(u) > f_k(v)$ and $u(k) < v(k)$, (c) $f_k(u) < f_k(v)$ and $u(k) > v(k)$. By induction hypothesis, (a) holds for only finitely many pairs. If (b) holds for infinitely many pairs, there exists an infinite sequence $u_1, u_2, \ldots$ such that $f_k(u_i) < f_k(u_{i+1})$ and $u_i(k) > u_{i+1}(k)$. However, it contradicts to the well-foundedness of $>$ on $\mathbb{N}$. For the same reason, (c) does not hold for infinitely many pairs, and hence, our assumption leads to the contradiction. $\square$

As a corollary of (1), it holds that : Every subset of $\mathbb{N}^k$ contains only finitely many minimal elements.

In contrast, it holds that : If $k \geqslant 2$, for every subset of $\mathbb{N}^k$ containing m minimal elements, there exists a subset of $\mathbb{N}^k$ which contains more than m minimal elements (the number of incomparable minimal elements in $\mathbb{N}^k$ $(k \geqslant 2)$ is unbounded).

Appendix (C) : Minimal solutions (cont'd)

(2) One can compute the set S of minimal positive solutions of the equation :

$$w = \sum_{1\leqslant i\leqslant m} x_i u_i - \sum_{1\leqslant j\leqslant n} y_j v_j \quad (u_1,\dots,u_m,v_1,\dots,v_n \in \mathbb{N}^k,\ w\in\mathbb{Z}^k) \qquad (*1)$$

Proof

Let $V = \{\, u_i, v_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n \,\}$. First, we show that the question if there exists a positive solution of V is decidable. If $V \cup \{w\}$ is linear independent, there is no solution. If V is linear independent and $V\cup\{w\}$ is linear dependent, then one can compute the a unique solution p over $\mathbb{Q}^m$ and q over $\mathbb{Q}^n$ such that $w = \sum_{1\leqslant i\leqslant m} p(i)u_i - \sum_{1\leqslant j\leqslant n} q(j)v_j$, which means that the equation has the positive solution over $\mathbb{N}^{m+n}$ if and only if $p\in\mathbb{N}^m$ and $q\in\mathbb{N}^n$. Suppose that V is linear dependent. The following proof proceeds by induction on $m+n$. The base case (the case of $m+n=1$) is obvious, because there is no such V (the above equation forms $w = x_1u_1$ or $w = -y_1v_1$). For induction hypothesis, observe that one can compute subsets $I\subseteq\{1,\dots,m\}$ and $J\subseteq\{1,\dots,n\}$ and vectors $p\in\mathbb{N}^m$ and $q\in\mathbb{N}^n$ such that

$$\sum_{i\in I} p(i)u_i - \sum_{j\in J} q(j)v_j = \sum_{i\notin I} p(i)u_i - \sum_{j\notin J} q(j)v_j$$

with either $p(i)>0$ for some $i\in I$ or $q(j)>0$ for some $j\in J$. This implies that $(*1)$ has a positive solution x_i, y_j $(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n)$ if and only if it satisfies either $x_i \leqslant p(i)$ for some $i\in I$ or $y_j\leqslant q(j)$ for some $j\in J$. (Proof cont'd)

Appendix (C) : Minimal solutions (cont'd)

This is because if $(x_1, \ldots, x_m, y_1, \ldots, y_n) > (p \times q)$, then

$$w = \sum_{i \in I}(x_i - p(i))u_i + \sum_{i \notin I}(x_i + p(i))u_i - \sum_{j \in J}(y_j - q(j))v_j - \sum_{j \notin J}(y_j + q(j))v_j$$

such that $x_i - p(i) < x_i$ for some $i \in I$ or $y_j - q(j) < y_j$ for some $j \in J$. By repeating the above computation, we obtain a positive solution of $(*1)$ such that $x_i \leqslant p(i)$ for some $i \in I$ or $y_j \leqslant q(j)$ for some $j \in J$. Let $X = \{(k, a) \mid a \in I, k \leqslant p(i)\}$ and $Y = \{(\ell, b) \mid b \in J, \ell \leqslant q(j)\}$. Then, the equation $(*1)$ has a positive solution if and only if there exists $(k, a) \in X$ such that $w - ku_a = \sum_{i \in I - \{a\}} p(i)u_i - \sum_{j \in J} q(j)v_j$ $(*2)$ has a solution or $(\ell, b) \in Y$ such that $w + \ell v_b = \sum_{i \in I} p(i)u_i - \sum_{j \in J - \{b\}} q(j)v_j$ $(*3)$ has a solution. Here "$(*2)$ has a solution" means the equation $(*2)$ has a positive solution or the solution is $\mathbf{0}$ (where $k > 0$ and the other $p(i)$'s are 0). Similar to $(*3)$. By induction hypothesis, the question if $(*2)$ or $(*3)$ has a solution is decidable. Hence, since X, Y are finite, the question if $(*1)$ has a positive solution is decidable.

Next, we show our statement. According to the above observation, one can determine if there is a positive solution of $(*1)$. If there is no solution, the empty set is the answer. Otherwise, one can find a positive solution of $(*1)$. Since the number of vectors smaller than the solution is finite, one can find a minimal positive solution of $(*1)$, say s. If there is another minimal positive solution of $(*1)$, say t, then for some $c, d \in \{1, \ldots, m+n\}$, $t(c) < s(c)$ and $t(d) > s(d)$. So, if $1 \leqslant c \leqslant m$, consider the equation $(*2)$ where $k = c$ and $u_a = t(c)$. (Proof cont'd)

Appendix (C) : Minimal solutions (cont'd)

Similarly, if $m < c \leqslant n$, consider the equation $(*3)$ where $\ell = c$ and $v_b = t(c)$. Since the number of the candidates for the pairs of such $(c, t(c))$ is finite, by induction hypothesis, one can compute the set S_c of minimal positive solutions of $(*2)$ and the set T_c of minimal positive solutions of $(*3)$. Let $f_{x,c}$ be the function from $\mathbb{N}^{m+n-1}$ to $\mathbb{N}^{m+n}$ such that $f_{x,c}(w) = (w(1), \ldots, w(c-1), x, w(c), \ldots, w(m+n-1))$. Then, $S = \min_{\geqslant}(\bigcup_{1 \leqslant c \leqslant m+n} \bigcup_{0 \leqslant x \leqslant s(c)} \{f_{x,c}(w) \mid w \in S_c \cup T_c\})$. Hence, we can compute the set of minimal positive solutions of $(*1)$. $\square$

National Institute of Advanced Industrial Science and Technology (AIST) – Senri-site, AIST Kansai.

Office: Shin-Senri Nishi 1–2–14 (MSK bldg. 5th floor), Toyonaka, Osaka 560–0083, Japan

URL: **http://staff.aist.go.jp/hitoshi.ohsaki/**