On Diophantine systems coming from AC-unification of higher-order patterns: exploiting symmetries

Ana Paula Tomás, Evelyne Contejean

Technical Report Series: DCC-97-15

Departamento de Ciência de Computadores – Faculdade de Ciências

&

Laboratório de Inteligência Artificial e Ciência de Computadores

Universidade do Porto

Rua do Campo Alegre, 823 4150 Porto, Portugal

Tel: +351+2+6078830 – Fax: +351+2+6003654

http://www.ncc.up.pt/fcup/DCC/Pubs/treports.html

On Diophantine systems coming from AC-unification of higher-order patterns: exploiting symmetries*

Ana Paula Tomás
DCC & LIACC, Univ. do Porto
R. do Campo Alegre, 823
4150 Porto, Portugal
apt@ncc.up.pt

Evelyne Contejean
LRI, CNRS URA 410
Bât. 490, Univ. Paris-Sud
91405 Orsay Cedex, France
contejea@lri.fr

December 1997

Abstract

We study systems of linear Diophantine equations that arise when performing AC-unification of higher-order patterns by the algorithm recently proposed by A. Boudet and E. Contejean [1]. Their solution space presents symmetries which can be exploited to solve them more efficiently.

1 Introduction

We investigate the problem of solving systems of linear Diophantine equations of the form (1) in naturals,

$$\bigwedge_{\pi' \in \Pi} \sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,\pi}\, z_{i,\pi' \circ \pi^{-1}} \quad = \quad \sum_{i=n_1+1}^{n_2} \sum_{\pi \in \Pi} a_{i,\pi}\, z_{i,\pi' \circ \pi^{-1}} \tag{1}$$

in $N \times n_2$ variables $z_{i,\theta}$, with $1 \leq i \leq n_2$, $\theta \in \Pi = \{\pi_1, \ldots, \pi_N\}$, being $(\Pi, \circ)$ a given group of permutations, where the operation $\circ$ is composition. Each coefficient $a_{i,\pi} \in \mathbb{N}$. We assume that π_1 is the identity element.

The motivation comes from problems of unification of higher-order patterns modulo an associative-commutative theory. Systems of the form (1) arise while solving the AC-unification problem (2) by the algorithm proposed by A. Boudet and E. Contejean in [1],

$$\lambda \overline{x}. \sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,\pi} F_i(\overline{x}^{\pi}) = \lambda \overline{x}. \sum_{i=n_1+1}^{n_2} \sum_{\pi \in \Pi} a_{i,\pi} F_i(\overline{x}^{\pi}) \tag{2}$$

where $\Pi = \{\pi_1, \ldots, \pi_N\}$ denotes the group of permutations over the sequences of variables in $\overline{x}$. Basically (please refer to [1] for precise details) the system of Diophantine equations (1) states that the number of occurrences of a term $t(\overline{x}^{\pi'})$ must be the same in both sides of the equation. In fact, let a substitution σ be a solution to (2), that introduces some term $t(\overline{x})$. If $z_{i,\pi'}$ denotes the number of times a term $t(\overline{x}^{\pi'})$ is introduced by $F_i(\overline{x})\sigma$, then $z_{i,\pi'}$ is the number of times $t(\overline{x}^{\pi' \circ \pi})$ is introduced by $F_i(\overline{x}^{\pi})\sigma$. Thus, the number of times $F_i(\overline{x}^{\pi})\sigma$ introduces term $t(\overline{x}^{\pi'})$ equals the number of times $F_i(\overline{x})\sigma$

*This work was partly supported by CNRS and IICT (project 4312), and it was mainly developed during the visit of A. P. Tomás to LRI (Orsay).

introduces $t(\overline{x}^{\pi' \circ \pi^{-1}})$, which is denoted by $z_{i,\pi' \circ \pi^{-1}}$. Therefore, $a_{i,\pi}\, z_{i,\pi' \circ \pi^{-1}}$ gives the number of occurrences of $t(\overline{x}^{\pi'})$ coming from $a_{i,\pi} F_i(\overline{x}^{\pi})$. Since the number of occurrences of a term $t(\overline{x}^{\pi'})$ must be the same in both sides of the equation, the system of Diophantine equations (1) must hold.

It is not difficult to see that (1) can be given the form (3) by re-ordering the terms in each equation.

$$\bigwedge_{\pi' \in \Pi} \sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,\pi^{-1} \circ \pi'}\, z_{i,\pi} \quad = \quad \sum_{i=n_1+1}^{n_2} \sum_{\pi \in \Pi} a_{i,\pi^{-1} \circ \pi'}\, z_{i,\pi} \tag{3}$$

Before proceeding we present some examples.

Example 1 *Let the unification equation be*

$$\lambda\, xyz.\, 2F_1(x,y,z) + F_1(y,z,x) = \lambda\, xyz.\, F_2(z,y,x) + F_2(x,y,z)$$

In this case, $\Pi = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$, *that is,* Π *is in fact the group of permutations over the sequences of variables in* $\overline{x}$, *being* $\pi_1(xyz) = xyz$, $\pi_2(xyz) = yxz$, $\pi_3(xyz) = xzy$, $\pi_4(xyz) = zyx$, $\pi_5(xyz) = yzx$, *and* $\pi_6(xyz) = zxy$. *The system of Diophantine equations given by (1) is*

$$\left\{ \begin{array}{rcl} 2z_{1,\pi_1} + z_{1,\pi_6} & = & z_{2,\pi_4} + z_{2,\pi_1} \\ 2z_{1,\pi_2} + z_{1,\pi_3} & = & z_{2,\pi_5} + z_{2,\pi_2} \\ 2z_{1,\pi_3} + z_{1,\pi_4} & = & z_{2,\pi_6} + z_{2,\pi_3} \\ 2z_{1,\pi_4} + z_{1,\pi_2} & = & z_{2,\pi_1} + z_{2,\pi_4} \\ 2z_{1,\pi_5} + z_{1,\pi_1} & = & z_{2,\pi_2} + z_{2,\pi_5} \\ 2z_{1,\pi_6} + z_{1,\pi_5} & = & z_{2,\pi_3} + z_{2,\pi_6} \end{array} \right.$$

Example 2 *Let the unification equation be*

$$\lambda\, xyz.\, 2F_1(x,y,z) + F_1(y,z,x) = \lambda\, xyz.\, 2F_2(x,y,z)$$

In this case, $\Pi = \{\pi_1, \pi_2, \pi_3\}$ *is a subgroup of the group of all permutations over the sequences of variables in* $\overline{x}$, *being* $\pi_1(xyz) = xyz$, $\pi_2(xyz) = yzx$, *and* $\pi_3(xyz) = zxy$. *In general,* Π *is the least subgroup containing the permutations occurring in the given problem. The Diophantine system is*

$$\left\{ \begin{array}{rcl} 2z_{1,\pi_1} + z_{1,\pi_3} & = & 2z_{2,\pi_1} \\ 2z_{1,\pi_2} + z_{1,\pi_1} & = & 2z_{2,\pi_2} \\ 2z_{1,\pi_3} + z_{1,\pi_2} & = & 2z_{2,\pi_3} \end{array} \right.$$

Property 1 *The set of solutions of (1) is invariant under the permutations in the subgroup* $\Pi = \{\pi_1, \ldots, \pi_N\}$, *in the sense that*

$$s = (z_{1,\pi_1}, \ldots, z_{1,\pi_N}, \ldots, z_{n_2,\pi_1}, \ldots, z_{n_2,\pi_N})$$

is a solution of (1) if and only if

$$(z_{1,\pi \circ \pi_1}, \ldots, z_{1,\pi \circ \pi_N}, \ldots, z_{n_2,\pi \circ \pi_1}, \ldots, z_{n_2,\pi \circ \pi_N}),$$

which we denote by s^{π}, *is also a solution of (1), for all* $\pi \in \Pi$.

Proof. From (1) we have that for any $\theta \in \Pi$,

$$\bigwedge_{\pi' \in \Pi} \sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,\pi}\, z_{i,(\theta \circ \pi') \circ \pi^{-1}} \quad = \quad \sum_{i=n_1+1}^{n_2} \sum_{\pi \in \Pi} a_{i,\pi}\, z_{i,(\theta \circ \pi') \circ \pi^{-1}}$$

so that

$$\bigwedge_{\pi'\in\Pi} \sum_{i=1}^{n_1}\sum_{\pi\in\Pi} a_{i,\pi^{-1}\circ\pi'}\, z_{i,\theta\circ\pi} \;=\; \sum_{i=n_1+1}^{n_2}\sum_{\pi\in\Pi} a_{i,\pi^{-1}\circ\pi'}\, z_{i,\theta\circ\pi}$$

since $a_{i,\pi^{-1}\circ\pi'}$ is the coefficient of $z_{i,(\theta\circ\pi')\circ(\pi^{-1}\circ\pi')^{-1}}$, that is, of $z_{i,(\theta\circ\pi)}$. □

Given any tuple $\mathbf{x} = (z_{1,\pi_1}, \ldots, z_{1,\pi_N}, \ldots, z_{n_2,\pi_1}, \ldots, z_{n_2,\pi_N}) \in \mathbb{R}^{N\times n_2}$, let us define $\mathbf{x}^\pi$, with $\pi \in \Pi$, by

$$\mathbf{x}^\pi = (z_{1,\pi\circ\pi_1}, \ldots, z_{1,\pi\circ\pi_N}, \ldots, z_{n_2,\pi\circ\pi_1}, \ldots, z_{n_2,\pi\circ\pi_N}).$$

The (i,π_j)–component of $\mathbf{x}^\pi$ is the $(i,\pi\circ\pi_j)$–component of $\mathbf{x}$, and reciprocally, the (i,π_j)–component of $\mathbf{x}$ is the $(i,\pi^{-1}\circ\pi_j)$–component of $\mathbf{x}^\pi$, for all $\pi_j \in \Pi$, and $1 \le i \le n_2$.

Property 2 *For all* $\mathbf{x} \in \mathbb{R}^{N\times n_2}$*, and* $\pi_k, \pi_m \in \Pi$*, we have* $(\mathbf{x}^{\pi_k})^{\pi_m} = \mathbf{x}^{\pi_k\circ\pi_m}$.

Proof. The (i,π_j)–component of $(\mathbf{x}^{\pi_k})^{\pi_m}$ is the $(i,\pi_m\circ\pi_j)$–component of $\mathbf{x}^{\pi_k}$, which is the $(i,\pi_k\circ(\pi_m\circ\pi_j))$–component of $\mathbf{x}$. Thus, the (i,π_j)–component of $(\mathbf{x}^{\pi_k})^{\pi_m}$ is the (i,π_j)–component of $\mathbf{x}^{\pi_k\circ\pi_m}$. □

What we are going to present applies to any system of linear Diophantine equations for which Property 1 holds. In view of Property 1, we are able to design more efficient methods to solve such systems than the general ones. In particular, we are able to adapt both the *Algorithm by Contejean and Devie* [2] and the *Slopes Algorithm* [3, 4] which compute the minimal solutions of systems in the general form, in order to find more efficiently the minimal solutions of these kind of systems.

We shall now recall some notions and results that are needed in the sequel.

2 On the solutions of Diophantine systems

It is known that the set $\mathcal{M}$ of the solutions of the system of linear Diophantine equations (4)

$$AX \;=\; 0,\;\; A\in\mathbb{Z}^{m\times n},\;\; X \in \mathbb{N}^n \tag{4}$$

is completely described by the finite set of minimal solutions of (4). These solutions are the nonnull solutions of (4) that are minimal in $\mathcal{M}$ for the component-wise ordering $\preceq$ given by $(u_1, \ldots, u_n) \preceq (v_1, \ldots, v_n)$ iff $u_i \le v_i$ for all i. Each solution in $\mathcal{M}$ is a linear *nonnegative integral* combination of the minimal solutions.

The solutions in *real* numbers of $AX = 0, X \succeq 0$, define a pointed convex polyhedral cone $\mathcal{C}$. When $\mathcal{C}$ is non-degenerated, $\mathcal{C}$ is the convex hull of its extreme rays (i.e., 1-dimensional faces) which are finitely many. A unique minimal solution $\mathbf{r}_i$ of (4) defines each extreme ray of $\mathcal{C}$. These minimal solutions, say $\mathbf{r}_1, \ldots, \mathbf{r}_p$, are the minimal solutions of minimal support of (4), which are well-characterized. The support of x is supp $x = \{i \mid x_i \neq 0\}$. Similarly, if $X \subseteq \mathbb{R}^n$, then supp $X = \bigcup_{x\in X}$ supp x. For simplicity, we often just call $\mathbf{r}_i$ an extreme ray of $\mathcal{C}$, rather than saying that it generates an extreme ray of $\mathcal{C}$.

It is known that the faces of $\mathcal{C}$, together with the improper face $\mathcal{C}$, form a lattice under inclusion, the so-called face lattice. This lattice is isomorphic to the lattice of the supports of the faces under inclusion. Each face $\mathcal{F}$ of $\mathcal{C}$ is a pointed convex polyhedral cone whose extreme rays are extreme rays of $\mathcal{C}$. That is, if $\mathcal{R}_\mathcal{C} = \{\mathbf{r}_1, \ldots, \mathbf{r}_p\}$ is the set of minimal solutions of minimal support, then $\mathcal{C} = cone\mathcal{R}_{\mathcal{C}} = \{\sum_{i=1}^{p} \alpha_i \mathbf{r}_i \mid \alpha_i \in \mathbb{R}_0^+\}$, and for each face $\mathcal{F} \subset \mathcal{C}$ we have $\mathcal{F} = cone\mathcal{R}_{\mathcal{F}}$ for some $\mathcal{R}_{\mathcal{F}} \subset \mathcal{R}_{\mathcal{C}}$. The dimension of $\mathcal{F}$, denoted by $dim\mathcal{F}$, is the dimension of the linear subspace generated by $\mathcal{R}_{\mathcal{F}}$. If $\mathcal{R}_{\mathcal{F}}$ is some subset of $\mathcal{R}_{\mathcal{C}}$, then $cone\mathcal{R}_{\mathcal{F}}$ is a face of $\mathcal{C}$ if and only if there exists no $r \in \mathcal{R}_{\mathcal{C}} \backslash \mathcal{R}_{\mathcal{F}}$ such that $\text{supp}\mathcal{R}_{\mathcal{F}} = \text{supp}(\mathcal{R}_{\mathcal{F}} \cup \{r\})$. Moreover, if $\mathcal{F}'$ is a face of $\mathcal{F}$, and $\mathcal{F}'$ precedes immediately $\mathcal{F}$ in the face lattice, then $\mathcal{F}'$ is called a facet of $\mathcal{F}$ and $\dim \mathcal{F} = \dim \mathcal{F}' + 1$. These latter properties are of use while computing the face lattice from the extreme rays of $\mathcal{C}$, and the dimensions of the faces of $\mathcal{C}$.

3 Solving the current problem

3.1 About the solution cone

Let $\mathbf{r}$ be a minimal solution of minimal support of (1). From Property 1, we have that each $\mathbf{r}^\pi$ gives a distinct extreme ray of the solution cone $\mathcal{C}$ of (1), for all $\pi \in \Pi$. Moreover, if $\mathcal{F}$ is a face of $\mathcal{C}$, then $\mathcal{F}^\pi$ is a face of $\mathcal{C}$, for all $\pi \in \Pi$, where $\mathcal{F}^\pi = \{s^\pi \mid s \in \mathcal{F}\}$, although these faces $\mathcal{F}^\pi$ are not necessarily pairwise distinct. Clearly, the solutions in $\mathcal{F}$ determine the solutions in $\mathcal{F}^\pi$, for $\pi \in \Pi$.

Example 3 *Let us consider the Diophantine system in Example 1, whose system matrix is as follows.*

$$\begin{bmatrix} 2 & 0 & 1 & -2 & 0 & 0 \\ 1 & 2 & 0 & 0 & -2 & 0 \\ 0 & 1 & 2 & 0 & 0 & -2 \end{bmatrix}$$

The solution cone is 3-dimensional, with three extreme rays r_1, r_2, r_3 given by $r_1 = (2,0,0,2,1,0)$, $r_2 = (0,2,0,0,2,1)$, and $r_3 = (0,0,2,1,0,2)$, the 2-dimensional faces being $cone\{r_1, r_2\}$, $cone\{r_1, r_3\}$, and $cone\{r_2, r_3\}$.

In this case, $(\Pi, \circ)$ is an abelian group, with $\Pi = \{\pi_1, \pi_2, \pi_3\}$, π_1 being the identity element, $\pi_2 \circ \pi_2 = \pi_3$, $\pi_3 \circ \pi_3 = \pi_2$, and $\pi_2 \circ \pi_3 = \pi_1$. It can be seen that, $r_2 = r_1^{\pi_3}$ and $r_3 = r_1^{\pi_2}$. Furthermore, let $\mathcal{F} = cone\{r_1, r_2\}$, that is, $\mathcal{F} = cone\{r_1, r_1^{\pi_3}\}$. Then, $\mathcal{F}^{\pi_2} = cone\{r_1^{\pi_2}, r_1^{\pi_1}\} = cone\{r_1, r_3\}$, and $\mathcal{F}^{\pi_3} = cone\{r_2, r_3\}$. As a conclusion, all the solutions in 2-dimensional faces are determined by the solutions in $\mathcal{F}$.

Property 3 *If s is a minimal solution then s^π is also a minimal solution of (1), for all $\pi \in \Pi$.*

Minimal coverings of the face lattice. To compute the minimal solutions of (1), we can restrict the search to a proper subset of the faces of its solution cone $\mathcal{C}$. We refer to such a subset as *a minimal covering of the face lattice*. In section 3.2, we present a completion algorithm that finds such a covering given the extreme rays of $\mathcal{C}$.

Specific versions of the *Algorithm by Contejean and Devie* (C-D algorithm, for short) and the *Slopes Algorithm* can be designed to solve (1), in which the search is restricted to a minimal covering of the face lattice. This is quite immediate for Slopes, since Slopes computes the set of minimal solutions in a monotonic way, by visiting all faces of $\mathcal{C}$ in increasing order of dimension, searching for minimal solutions lying in the interior of each face $\mathcal{F}$ of $\mathcal{C}$ (including $\mathcal{C}$ itself).

Although the C-D algorithm does not explore the face lattice in a similar way, we can nevertheless think of algorithm based on it which restricts the search to a minimal covering of that lattice. To find minimal solutions in the interior of each face $\mathcal{F}$ in the covering, it would run just as C-D algorithm while solving $A_{\mathcal{F}} X_{\mathcal{F}} = 0$, except that it would start from the all 1's tuple, and consider the minimal solutions already found in subfaces of $\mathcal{F}$. Here, $A_{\mathcal{F}}$ stands for the matrix resulting from A by keeping just the columns A^i such that $i \in \text{supp}\mathcal{F}$, and $X_{\mathcal{F}}$ results from X in a similar way. Clearly, whenever some minimal solution s is found in $\mathcal{F}$, s^π must be added to the set of minimal solutions, for $\pi \in \Pi$ such that $\mathcal{F} \neq \mathcal{F}^\pi$. This applies also to Slopes.

If a face $\mathcal{F}$ is invariant under some permutations in Π, say for $\pi \in \Pi_0 \subseteq \Pi$, and s is a minimal solution found in the interior of $\mathcal{F}$, then so are s^π, for $\pi \in \Pi_0$. Moreover, if some upper bound on the components of the minimal solutions in $\mathcal{F}$ is introduced by s, then s^π may also set other upper bounds on the other minimal solutions in $\mathcal{F}$, for $\pi \in \Pi_0$. Implementing search pruning by minimal solutions in an efficient way can be crucial in this kind of problem. Some further study will be devoted to this topic.

3.2 Computing a minimal covering of the face lattice

If the solution cone $\mathcal{C}$ has p extreme rays, then they may be grouped into p/N pairwise disjoint ordered sets $\{\mathtt{r}_i^{\pi_1}, \ldots, \mathtt{r}_i^{\pi_N}\}$, each $\mathtt{r}_i$ being some minimal solution of minimal support of (1), for $1 \leq i \leq p/N$. Only these $\mathtt{r}_i$'s need to be computed. Rather than $\{\mathtt{r}_i^{\pi_1}, \ldots, \mathtt{r}_i^{\pi_N}\}$ we use either the notation $(\{\mathtt{r}_i^{\pi_1}\}, \ldots, \{\mathtt{r}_i^{\pi_N}\})$ or the abbreviated form $[\,\{\mathtt{r}_i\}\,]$.

More generally, by

$$[\,\{\mathtt{r}_{i_1}^{\pi_{j_1}}, \ldots, \mathtt{r}_{i_k}^{\pi_{j_k}}\}\,]$$

we refer to

$$(\,\{\mathtt{r}_{i_1}^{\pi_{j_1}\circ\pi_1}, \ldots, \mathtt{r}_{i_k}^{\pi_{j_k}\circ\pi_1}\},\ \ldots,\ \{\mathtt{r}_{i_1}^{\pi_{j_1}\circ\pi_N}, \ldots, \mathtt{r}_{i_k}^{\pi_{j_k}\circ\pi_N}\}\,).$$

The idea behind this notation is that if $\mathcal{F} = cone\{\mathtt{r}_{i_1}^{\pi_{j_1}}, \ldots, \mathtt{r}_{i_k}^{\pi_{j_k}}\}$ then $[\,\{\mathtt{r}_{i_1}^{\pi_{j_1}}, \ldots, \mathtt{r}_{i_k}^{\pi_{j_k}}\}\,]$ denotes $\{\mathcal{F}^\pi \mid \pi \in \Pi\}$. We recall that, as said above, π_1 stands for the identity element of $(\Pi, \circ)$.

Furthermore, we suppose that the first element in such a tuple is ordered by $<_{lex}$, being $\mathtt{r}_{i_1}^{\pi_{j_1}} <_{lex} \ldots <_{lex} \mathtt{r}_{i_k}^{\pi_{j_k}}$, where $<_{lex}$ is defined by

$$\mathtt{r}_i^{\pi_k} <_{lex} \mathtt{r}_j^{\pi_m} \quad \text{if and only if} \quad \text{either } i < j, \text{ or } i = j \text{ and } k < m$$

for $1 \leq i, j \leq p/N$, and $1 \leq k, m \leq N$.

Property 4 *For all $\pi \in \Pi$, $\{\mathtt{r}_{i_i}^{\pi_{j_i}} \mid 1 \leq i \leq k\} = \{\mathtt{r}_{i_i}^{\pi_{j_i}\circ\pi^{-1}} \mid 1 \leq i \leq k\}^\pi$. In particular,*

$$\{\mathtt{r}_{i_i}^{\pi_{j_i}} \mid 1 \leq i \leq k\} \in [\,\{\mathtt{r}_{i_i}^{\pi_{j_i}\circ\pi_{j_1}^{-1}} \mid 1 \leq i \leq k\}\,],$$

that is, $\{\mathtt{r}_{i_i}^{\pi_{j_i}} \mid 1 \leq i \leq k\} \in [\,\{\mathtt{r}_{i_1}, \mathtt{r}_{i_2}^{\pi_{j_2}\circ\pi_{j_1}^{-1}}, \ldots, \mathtt{r}_{i_k}^{\pi_{j_k}\circ\pi_{j_1}^{-1}}\}\,]$.

From Property 4, a relevant subset of the 2-dimensional faces is a subset of the set consisting of

$$\begin{array}{ll} cone\{\mathtt{r}_i, \mathtt{r}_i^\pi\}, & \text{with } \pi \in \Pi \setminus \{\pi_1\},\ \ 1 \leq i \leq p/N, \text{ and} \\ cone\{\mathtt{r}_i, \mathtt{r}_j^\pi\}, & \text{with } \pi \in \Pi,\ \ 1 \leq i < j \leq p/N. \end{array}$$

Possibly, not all such cones are faces of $\mathcal{C}$, and for all $\pi \in \Pi \setminus \{\pi_1\}$, either $cone\{\mathtt{r}_i, \mathtt{r}_i^\pi\}$ or $cone\{\mathtt{r}_i, \mathtt{r}_i^{\pi^{-1}}\}$ may be needed. We are going to consider $\{\mathtt{r}_i, \mathtt{r}_j^\pi\}$ as a representative of $[\,\{\mathtt{r}_i, \mathtt{r}_j^\pi\}\,]$, for $j \geq i$.

Property 5 *For all $\pi_j, \pi \in \Pi$, $1 \leq i, j \leq N$, and face $\mathcal{F}$, it holds that $(i, \pi_j) \in supp\mathcal{F}$ if and only if $(i, \pi^{-1}\circ\pi_j) \in supp\mathcal{F}^\pi$.*

Given $X \subseteq \mathbb{R}^n$, we can represent supp X by a 0/1-tuple $(\xi_1, \ldots, \xi_n)$, with $\xi_i = 1$ when $i \in \text{supp } X$, and $\xi_i = 0$ when $i \notin \text{supp } X$. In this way, if $\mathcal{F}$ is a face of $\mathcal{C}$, its support may be given by a 0/1-tuple $(\xi_{1,\pi_1}, \ldots, \xi_{1,\pi_N}, \ldots, \xi_{n_2,\pi_1}, \ldots, \xi_{n_2,\pi_N})$, with $\xi_{i,\pi} \in \{0,1\}$, for $1 \leq i \leq n_2$, and $\pi \in \Pi$. From Property 1, we have that, $(\xi_{1,\pi_1}, \ldots, \xi_{1,\pi_N}, \ldots, \xi_{n_2,\pi_1}, \ldots, \xi_{n_2,\pi_N})$ gives supp $\mathcal{F}$ if and only if

$$(\xi_{1,\pi\circ\pi_1}, \ldots, \xi_{1,\pi\circ\pi_N}, \ldots, \xi_{n_2,\pi\circ\pi_1}, \ldots, \xi_{n_2,\pi\circ\pi_N})$$

gives supp $\mathcal{F}^\pi$, for all $\pi \in \Pi$.

The following completion procedure computes a minimal covering of the face lattice of $\mathcal{C}$. It is based on the algorithm given by M. Filgueiras and A. P. Tomás [4] for computing the face lattice of the solution cone of a system in the general form (4).

```
create [Top], Top consisting of all extreme rays;
for each i with 1 ≤ i ≤ p/N create [ {r_i} ] of dimension 1;
combine each ray r (in <_lex) with each created [R] ≠ [Top]
   if supp(R ∪ {r}) = supp(Top) do nothing
   else if supp(R ∪ {r}) = suppR, replace [R] by [R ∪ {r}]
   else if supp(R ∪ {r}) = suppR_0^π, for some [R_0] and π ∈ Π
     if dim [R_0] < 1 + dim [R]
     then set dim [R_0] to 1 + dim [R]
     else do nothing;
   else (resulting face is new)
     create new [R'] where R' = R ∪ {r};
     set dim [R'] to
       1 + max{dim [R_0] | supp(R') ⊃ suppR_0^π, for some π ∈ Π};
     for each [R_0] with supp(R') ⊂ suppR_0^π for some π ∈ Π
       set dim [R_0] to max(1 + dim[R'], dim[R_0]);

set all layers to empty;
for each [R] ≠ [Top]
   insert [R] into Layer[dim [R] ];
set dim[Top] to 1+maximum dimension found;
```

Lemma 1 *Whatever* $[\mathcal{R}]$ *is,* $[\mathcal{R}]$ *is removed when combined with* r *if and only if* supp $\mathcal{R} = \text{supp}(\mathcal{R} \cup \{r\})$, *being replaced by* $[\mathcal{R} \cup \{r\}]$.

Lemma 1 results immediate from the algorithm, and as a corollary we have Lemma 2.

Lemma 2 *Suppose that* $[\mathcal{R}]$ *exists when the algorithm is starting the combinations with* r_m*, and that* $[\mathcal{R}]$ *no longer exists when combinations with* $r_m^{\pi_N}$ *terminate, for some* $1 \leq m \leq p/N$. *Then, there are* $\pi_{\iota_1}, \ldots, \pi_{\iota_k} \in \Pi$, *(with* $1 \leq k \leq N$*) such that* $[\mathcal{R} \cup \{r_m^{\pi_{\iota_1}}, \ldots, r_m^{\pi_{\iota_k}}\}]$ *exists when the combinations with* $r_m^{\pi_N}$ *terminate, being* supp $\mathcal{R} = \text{supp}(\mathcal{R} \cup \{r_m^{\pi_{\iota_1}}, \ldots, r_m^{\pi_{\iota_k}}\})$.

Proposition 1 *Let* $\mathcal{R}$ *be a subset of the set of extreme rays of the solution cone* $\mathcal{C}$. *There exists some* $[\mathcal{R}_\mathcal{F}]$ *(possibly* `[Top]`*) in the minimal covering found by the completion procedure, such that* $\mathcal{R} \subseteq \mathcal{R}_\mathcal{F}^\pi$ *for some* $\pi \in \Pi$.

Corollary 1.1 *Let* $\mathcal{F}$ *be a face of the solution cone* $\mathcal{C}$, $\mathcal{R}_\mathcal{F}$ *denoting the set of its extreme rays. There exists* $[\mathcal{R}]$ *in the minimal covering found by the completion procedure, such that* $\mathcal{R}_\mathcal{F} = \mathcal{R}^\pi$ *(as unordered sets), for some* $\pi \in \Pi$. *Furthermore,* $\mathcal{R} = \mathcal{R}_\mathcal{F}^{\pi^{-1}}$.

References

[1] Boudet, A., Contejean E.: AC-unification of higher-order patterns. In G. Smolka (Ed), *Proc. Principles and Practice of Constraint Programming – CP'97*, Lecture Notes in Computer Science 1330, Springer-Verlag, 267–282, 1997.

[2] Boudet, A., Contejean E., and Devie, H.: A new *AC* Unification algorithm with an algorithm for solving systems of Diophantine equations. In Proceedings of the 5th Conference on Logic and Computer Science, IEEE, 289–299, 1990.

[3] Tomás, A. P., Filgueiras, M.: Solving linear Diophantine equations using the geometric structure of the solution space. In H. Common (Ed.), *Proceedings of the 8th Conf. on Rewriting Techniques and Applications – RTA'97*, Lecture Notes in Computer Science 1232, Springer-Verlag, 269–283, 1997.

[4] Tomás, A. P., Filgueiras, M.: An Algorithm for Solving Systems of Linear Diophantine in Naturals. In E. Costa, A. Cardoso (Eds.), *Proc. of the 8th Portuguese Conference on Artificial Intelligence, EPIA'97*, Lecture Notes in Artificial Intelligence 1323, Springer-Verlag, 73–84, 1997.