On Symmetries in Systems Coming from AC-unification of Higher-Order Patterns*

Ana Paula Tomás[1] and Evelyne Contejean[2]

[1] DCC-FC & LIACC, Universidade do Porto
R. do Campo Alegre, 823,
4150-180 Porto, Portugal
apt@ncc.up.pt
[2] LRI, CNRS URA 410
Bât. 490, Univ. Paris-Sud
91405 Orsay Cedex, France
contejea@lri.fr

Abstract. We study systems of linear Diophantine equations that arise when performing AC-unification of higher-order patterns by the algorithm proposed by A. Boudet and E. Contejean [2]. Some preliminary results are presented on exploiting their highly symmetrical solution spaces in order to design efficient problem specific solvers. Symmetry is induced by the group of permutations that defines the problem.

1 Introduction

Solving general linear Diophantine systems $AX = 0$, with $A \in \mathbb{Z}^{m\times n}$, $X \in \mathbb{N}^n$, is an NP-complete problem. The set of solutions $\mathcal{M}$ of such a problem is completely described by the finite set $\mathcal{H}(\mathcal{M})$ of its minimal solutions [13]. These are the non-null solutions in $\mathcal{M}$ that are minimal for the component-wise ordering: $(u_1, \ldots, u_n) \preceq (v_1, \ldots, v_n)$ iff $u_i \leq v_i$ for all i. Each solution in $\mathcal{M}$ is a linear non-negative integral combination of the minimal solutions. The set $\mathcal{H}(\mathcal{M})$ is called the Hilbert Basis [9] of $\mathcal{M}$. The problem of finding $\mathcal{H}(\mathcal{M})$, that is in general computationally intractable, has been investigated by Elliott [7] and MacMahon [10] in the beginning of 1900, and more recently by several other researchers with different interests, although many works concern applications to term rewriting, especially to AC-unification [1, 3–6, 8, 11, 12, 14, 16–18]. Even for small problems, it is not the case that one of the existing algorithms is always more efficient than the others, so that there is still a strong interest in studying the structure of the problem so as to design new algorithms [11]. In this work, we investigate the problem of solving Diophantine systems of the form (1)

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

* Work partly supported by CNRS and IICT (project 4312) and by funds granted to LIACC through the Programa de Financiamento Plurianual, Fundação para a Ciência e Tecnologia and Programa POSI.

in $N \times n_2$ variables $z_{i,\theta}$, which range over natural numbers, with $1 \leq i \leq n_2$ and $\theta \in \Pi = \{\pi_1, \pi_2, \ldots, \pi_N\}$, where $(\Pi, \circ)$ is a given group of permutations, $\circ$ denotes composition and π_1 the identity element. Each coefficient $a_{i,\pi} \in \mathbb{N}$.

The motivation comes from problems of unification of higher-order patterns modulo an AC-theory. Systems of the form (1) arise while solving the AC-unification problem (2) by the algorithm proposed by Boudet and Contejean in [2], $\Pi = \{\pi_1, \pi_2, \ldots, \pi_N\}$ being actually the group of permutations over the sequences of variables in $\overline{x}$.

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

Further technical details may be found in [2]. The idea is that if a substitution σ is a solution to (2), that introduces some term $t(\overline{x})$, and $z_{i,\pi'}$ 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 $t(\overline{x}^{\pi'})$ equals the number of times $F_i(\overline{x})\sigma$ 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, (1) must hold. By re-ordering the terms in each equation, (1) can be rewritten as (3).

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

Given $\mathtt{x} = (z_{1,\pi_1}, z_{1,\pi_2}, \ldots, z_{1,\pi_N}, \ldots, z_{n_2,\pi_1}, z_{n_2,\pi_2}, \ldots, z_{n_2,\pi_N}) \in \mathbb{R}^{N \times n_2}$ and $\pi \in \Pi$, let us define $\mathtt{x}^{\pi}$ by (4).

$$\mathtt{x}^{\pi} = (z_{1,\pi \circ \pi_1}, z_{1,\pi \circ \pi_2}, \ldots, z_{1,\pi \circ \pi_N}, \ldots\ldots, z_{n_2,\pi \circ \pi_1}, z_{n_2,\pi \circ \pi_2}, \ldots, z_{n_2,\pi \circ \pi_N}) \tag{4}$$

Property 1. The (i, π_j)–element of $\mathtt{x}$ is the $(i, \pi^{-1} \circ \pi_j)$–element of $\mathtt{x}^{\pi}$, for all $\pi_j \in \Pi$, and $1 \leq i \leq n_2$.

The solution set of (3) is highly symmetrical as stated by Property 2. Our goal is to exploit it so as to design better algorithms to compute the Hilbert basis (3).

Property 2. The solution set of (3) is invariant under the permutations in Π: for all $\theta \in \Pi$, s is a solution of (3) if and only if s^{θ} is also a solution of (3).

Proof. $\sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,\pi^{-1} \circ \pi'}\, z_{i,\theta \circ \pi} = \sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,\pi^{-1} \circ \theta \circ \theta^{-1} \circ \pi'}\, z_{i,\theta \circ \pi}$
$= \sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,(\theta \circ \pi)^{-1} \circ (\theta \circ \pi')}\, z_{i,\theta \circ \pi}$. By (3), $\sum_{i=1}^{n_1} \sum_{\pi \in \Pi} a_{i,(\theta \circ \pi)^{-1} \circ (\theta \circ \pi')}\, z_{i,\theta \circ \pi} =$
$\sum_{i=n_1+1}^{n_2} \sum_{\pi \in \Pi} a_{i,(\theta \circ \pi)^{-1} \circ (\theta \circ \pi')}\, z_{i,\theta \circ \pi} = \sum_{i=1}^{n_2} \sum_{\pi \in \Pi} a_{i,\pi^{-1} \circ \pi'}\, z_{i,\theta \circ \pi}$, for all π'.

The emphasis is put on the analysis of the structure of face lattice of the convex polyhedron that is defined by the solutions of the linear relaxation of the problem. In the next section we recall some useful results.

2 On the solutions of Diophantine systems

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 $\mathtt{r}_i$ of (5) defines each extreme ray of $\mathcal{C}$.

$$AX = 0, \quad A \in \mathbb{Z}^{m \times n}, \quad X \in \mathbb{N}^n, \tag{5}$$

Notice that each $\mathtt{r}_i$ is a multiple of an unique feasible basic solution (vertex) of $AX = 0, \sum_{j=1}^{n} X_j = 1, X_j \in \mathbb{R}_0^+$, for all j. Therefore, these minimal solutions, say $\mathtt{r}_1, \ldots, \mathtt{r}_p$, are the minimal solutions of minimal support of (5), that 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 $\mathtt{r}_i$ 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 [15]. 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 $\mathcal{R}_\mathcal{C} = \{\mathtt{r}_1, \ldots, \mathtt{r}_p\}$ is the set of minimal solutions of minimal support, then $\mathcal{C} = cone\mathcal{R}_\mathcal{C} = \{\sum_{i=1}^{p} \alpha_i \mathtt{r}_i \mid \alpha_i \in \mathbb{R}_0^+\}$, 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 $\mathcal{R}_\mathcal{F}$. A cone $\mathcal{C}$ is called simplicial if $\mathcal{R}_\mathcal{C}$ is a free set. Given $\mathcal{R}_\mathcal{F} \subseteq \mathcal{R}_\mathcal{C}$, $cone\mathcal{R}_\mathcal{F}$ 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 supp$\mathcal{R}_\mathcal{F}$ = 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 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 Some Examples

Example 1. Let the unification equation be

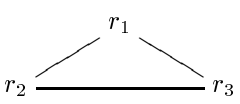
$$\lambda\, xyz.\ 2F_1(x,y,z) + F_1(y,z,x) = \lambda\, xyz.\ 2F_2(x,y,z)$$

In this case, $\Pi = \{\pi_1, \pi_2, \pi_3\}$ is a subgroup of the group of all permutations of xyz, 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. We have $\pi_2 \circ \pi_2 = \pi_3$, $\pi_3 \circ \pi_3 = \pi_2$, $\pi_2 \circ \pi_3 = \pi_3 \circ \pi_2 = \pi_1$ and so the system is

$$\begin{cases} 2z_{1,\pi_1 \circ \pi_1^{-1}} + z_{1,\pi_1 \circ \pi_2^{-1}} = 2z_{2,\pi_1 \circ \pi_1^{-1}} \\ 2z_{1,\pi_2 \circ \pi_1^{-1}} + z_{1,\pi_2 \circ \pi_2^{-1}} = 2z_{2,\pi_2 \circ \pi_1^{-1}} \\ 2z_{1,\pi_3 \circ \pi_1^{-1}} + z_{1,\pi_3 \circ \pi_2^{-1}} = 2z_{2,\pi_3 \circ \pi_1^{-1}} \end{cases} \Leftrightarrow \begin{cases} 2z_{1,\pi_1} + z_{1,\pi_3} = 2z_{2,\pi_1} \\ 2z_{1,\pi_2} + z_{1,\pi_1} = 2z_{2,\pi_2} \\ 2z_{1,\pi_3} + z_{1,\pi_2} = 2z_{2,\pi_3} \end{cases}$$

A sketch of a cross section of its solution cone is shown below on the right.

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



The solution cone is a 3-dimensional *simplicial* cone (the cross section is a simplex). Its three extreme rays r_1, r_2, r_3 are given by $r_1 = (2,0,0,2,1,0)$, $r_2 = (0,2,0,0,2,1)$, and $r_3 = (0,0,2,1,0,2)$, and it has three 2-dimensional faces ($cone\{r_1, r_2\}$, $cone\{r_1, r_3\}$ and $cone\{r_2, r_3\}$). By (4), we have $r_2 = r_1^{\pi_3}$ 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 $\mathcal{F}^{\pi_3} = cone\{r_2, r_3\}$. This means that all the solutions in 2-dimensional faces are determined by the solutions in $\mathcal{F}$.

Notation. $\mathcal{F}^{\pi}$ stands for $\{\mathtt{x}^{\pi} \mid \mathtt{x} \in \mathcal{F}\}$. We call $\mathcal{F}_1$ and $\mathcal{F}_2$ *equivalent faces* if and only if $\mathcal{F}_2 = \mathcal{F}_1^{\theta}$, for some $\theta \in \Pi$. For any given face $\mathcal{F}$, the equivalence class of $\mathcal{F}$, which we shall denote by $[\mathcal{R}_{\mathcal{F}}]$ is $[\mathcal{R}_{\mathcal{F}}] = \{\mathcal{F}^{\pi} \mid \pi \in \Pi\}$. Three classes were found in the previous example: $[\{r_1\}]$, $[\{r_1, r_1^{\pi_3}\}]$, $[\{r_1, r_1^{\pi_2}, r_1^{\pi_3}\}]$.

Property 3. For all $\mathtt{x} \in \mathbb{R}^{N \times n_2}$ and $\pi_k, \pi_m \in \Pi$, $(\mathtt{x}^{\pi_k})^{\pi_m} = \mathtt{x}^{\pi_k \circ \pi_m}$. So, for all $\mathcal{F} \subseteq \mathbb{R}^{N \times n_2}$, it holds $(\mathcal{F}^{\pi_k})^{\pi_m} = \mathcal{F}^{\pi_k \circ \pi_m}$.

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

The face lattice is well-characterized for simplicial cones. If $\mathcal{C}$ is a simplicial cone of dimension N, with $\mathcal{R}_{\mathcal{C}} = \{\mathtt{r}_i \mid 1 \leq i \leq N\}$, each k-dimensional face of $\mathcal{C}$ is defined by an unique subset of $\mathcal{R}_{\mathcal{C}}$ of order k, and conversely. Thus, the number of k-dimensional faces is $\mathrm{C}_k^N = \frac{N!}{(N-k)!k!}$, with $1 \leq k \leq N$. If, one side of (1) contains a single variable per equation (e.g., $z_{n_1+1,\pi' \circ \pi^{-1}}$ is the single variable on the right-hand side of the π'–equation), the solution cone is simplicial.

Example 2. Let the unification equation be

$$\lambda\, xyz.\ 2F_1(x,y,z) + F_1(y,z,x) = \lambda\, xyz.\ 3F_2(z,y,x)$$

In this case, $\Pi = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$ is the group of permutations of xyz, 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 and $(\Pi, \circ)$ are as follows.

$$\begin{cases} 2z_{1,\pi_1} + z_{1,\pi_6} = 3z_{2,\pi_4} \\ 2z_{1,\pi_2} + z_{1,\pi_3} = 3z_{2,\pi_5} \\ 2z_{1,\pi_3} + z_{1,\pi_4} = 3z_{2,\pi_6} \\ 2z_{1,\pi_4} + z_{1,\pi_2} = 3z_{2,\pi_1} \\ 2z_{1,\pi_5} + z_{1,\pi_1} = 3z_{2,\pi_2} \\ 2z_{1,\pi_6} + z_{1,\pi_5} = 3z_{2,\pi_3} \end{cases}$$

$\circ$	π_1	π_2	π_3	π_4	π_5	π_6
π_1	π_1	π_2	π_3	π_4	π_5	π_6
π_2	π_2	π_1	π_6	π_5	π_4	π_3
π_3	π_3	π_5	π_1	π_6	π_2	π_4
π_4	π_4	π_6	π_5	π_1	π_3	π_2
π_5	π_5	π_3	π_4	π_2	π_6	π_1
π_6	π_6	π_4	π_2	π_3	π_1	π_5

The nonnegative real solutions define a 6-dimensional simplicial cone.

$$\begin{array}{ll} r_1 = (3,0,0,0,0,0,\ 2,0,0,0,1,0) & r_1^{\pi_2} = (0,3,0,0,0,0,\ 0,2,0,1,0,0) \\ r_1^{\pi_3} = (0,0,3,0,0,0,\ 0,1,2,0,0,0) & r_1^{\pi_4} = (0,0,0,3,0,0,\ 0,0,1,2,0,0) \\ r_1^{\pi_6} = (0,0,0,0,3,0,\ 0,0,0,0,2,1) & r_1^{\pi_5} = (0,0,0,0,0,3,\ 1,0,0,0,0,2) \end{array}$$

Note that, for instance, $cone\{r_1^{\pi_3}, r_1^{\pi_5}, r_1^{\pi_6}\} = cone\{r_1, r_1^{\pi_5 \circ \pi_3^{-1}}, r_1^{\pi_6 \circ \pi_3^{-1}}\}^{\pi_3}$, so that $cone\{r_1^{\pi_3}, r_1^{\pi_5}, r_1^{\pi_6}\} \in \{cone\{r_1, r_1^{\pi_2}, r_1^{\pi_4}\}^{\theta} \mid \theta \in \Pi\}$. This means that if we search for solutions in the faces that contain r_1 we are able to deduce the whole solution set by performing permutations. Another interesting point is that, for all $\pi_j \in \Pi$, $cone\{r_1, r_1^{\pi_j}\} = cone\{r_1, r_1^{\pi_j}\}^{\theta}$ if and only if $\theta = \pi_j$ and $\pi_j = \pi_j^{-1}$ (i.e., π_j is a transposition).

Therefore, if $\mathcal{C}$ is simplicial, and Π is the group of permutations of $\overline{x}$ (a string of n variables), the number of faces of dimension 2 is $N(N-1)/2$ but we should only explore $(N-1+n(n-1)/2)/2$. Note that $N = |\Pi|$ and $n(n-1)/2$ is the number of transpositions.

When $N = 6$, the number of faces is $2^N - 1 = 63$, six being extreme rays, but there are only 15 equivalence classes.

Example 3. 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

$$\begin{cases} 2z_{1,\pi_1} + z_{1,\pi_6} = z_{2,\pi_4} + z_{2,\pi_1} \\ 2z_{1,\pi_2} + z_{1,\pi_3} = z_{2,\pi_5} + z_{2,\pi_2} \\ 2z_{1,\pi_3} + z_{1,\pi_4} = z_{2,\pi_6} + z_{2,\pi_3} \\ 2z_{1,\pi_4} + z_{1,\pi_2} = z_{2,\pi_1} + z_{2,\pi_4} \\ 2z_{1,\pi_5} + z_{1,\pi_1} = z_{2,\pi_2} + z_{2,\pi_5} \\ 2z_{1,\pi_6} + z_{1,\pi_5} = z_{2,\pi_3} + z_{2,\pi_6} \end{cases}$$

For simplicity, let us write z_{ik} instead of z_{i,π_k}. Property 2 says that

$$(z_{11},\, z_{12},\, z_{13},\, z_{14},\, z_{15},\, z_{16},\quad z_{21},\, z_{22},\, z_{23},\, z_{24},\, z_{25},\, z_{26})$$

is a solution if and only if the following tuples are solutions.

$$\begin{array}{ll} (z_{12},\, z_{11},\, z_{16},\, z_{15},\, z_{14},\, z_{13}, & z_{22},\, z_{21},\, z_{26},\, z_{25},\, z_{24},\, z_{23}) \\ (z_{13},\, z_{15},\, z_{11},\, z_{16},\, z_{12},\, z_{14}, & z_{23},\, z_{25},\, z_{21},\, z_{26},\, z_{22},\, z_{24}) \\ (z_{14},\, z_{16},\, z_{15},\, z_{11},\, z_{13},\, z_{12}, & z_{24},\, z_{26},\, z_{25},\, z_{21},\, z_{23},\, z_{22}) \\ (z_{15},\, z_{13},\, z_{14},\, z_{12},\, z_{16},\, z_{11}, & z_{25},\, z_{23},\, z_{24},\, z_{22},\, z_{26},\, z_{21}) \\ (z_{16},\, z_{14},\, z_{12},\, z_{13},\, z_{11},\, z_{15}, & z_{26},\, z_{24},\, z_{22},\, z_{23},\, z_{21},\, z_{25}) \end{array}$$

Notice also that, by adding up the system equations, we conclude that

$$2\left(\sum_{\pi_k \in \Pi} z_{1k}\right) + \left(\sum_{\pi_k \in \Pi} z_{1k}\right) = \left(\sum_{\pi_k \in \Pi} z_{2k}\right) + \left(\sum_{\pi_k \in \Pi} z_{2k}\right)$$

that is, $3\sum_k z_{1k} = 2\sum_k z_{2k}$ so that, e.g. $(2,2,2,2,2,2,3,3,3,3,3,3)$ is a solution. This illustrates one of the interesting properties that can be exploited.

4 Finding the Hilbert Basis

What we are going to present applies to any system of linear Diophantine equations for which Property 2 holds. In order to compute the minimal solutions of (1), we can restrict the search to a proper subset of the faces of its solution cone $\mathcal{C}$. Each face in the subset identifies a particular equivalence class. We call such a subset *a minimal covering of the face lattice*. We are going to 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*[3] (C-D algorithm, for short) and the *Slopes Algorithm*[16–18] 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 $i \in \mathrm{supp}\mathcal{F}$, 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.

Property 4. If s is a minimal solution then s^π is also a minimal solution of (1), for all $\pi \in \Pi$.

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.

4.1 Minimal covering of the face lattice

If the solution cone $\mathcal{C}$ has p extreme rays, then they may be grouped into pairwise disjoint ordered sets $\{\mathtt{r}_i^{\pi_1}, \ldots, \mathtt{r}_i^{\pi_N}\}$ (clearly, repetitions should be excluded) each $\mathtt{r}_i$ being some minimal solution of minimal support of (1). For simplicity, let us assume that there are p/N such sets (meaning that $r_i^\pi \neq r_i^{\pi'}$ if $\pi \neq \pi'$). Only these $\mathtt{r}_i$'s need to be computed. Rather than $\{\mathtt{r}_i^{\pi_1}, \ldots, \mathtt{r}_i^{\pi_N}\}$ we shall use $[\,\{\mathtt{r}_i\}\,]$, because it represents the equivalence class of $cone\{\mathtt{r}_i\}$.

We recall that, as said above, π_1 stands for the identity element of $(\Pi, \circ)$. Let us define $<_{lex}$ as $\mathtt{r}_i^{\pi_k} <_{lex} \mathtt{r}_j^{\pi_m}$ if and only if either $i < j$, or $i = j$ and $k < m$, for $1 \leq i, j \leq p/N$, and $1 \leq k, m \leq N$.

Property 5. For all $\pi \in \Pi$, $\{\mathbf{r}_{i_i}^{\pi_{j_i}} \mid 1 \le i \le k\} = \{\mathbf{r}_{i_i}^{\pi_{j_i} \circ \pi^{-1}} \mid 1 \le i \le k\}^{\pi}$, so that $[\{\mathbf{r}_{i_i}^{\pi_{j_i}} \mid 1 \le i \le k\}] = [\ \{\mathbf{r}_{i_1}, \mathbf{r}_{i_2}^{\pi_{j_2} \circ \pi_{j_1}^{-1}}, \ldots, \mathbf{r}_{i_k}^{\pi_{j_k} \circ \pi_{j_1}^{-1}}\ \}\ ]$.

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 [18] for computing the face lattice of the solution cone of a system in the general form (5), and can be improved.

```
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;
```

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 $i \in$ supp X, and $\xi_i = 0$ when $i \notin$ supp X. In this way, if $\mathcal{F}$ is a face of $\mathcal{C}$, its support may be given by a 0/1-tuple. The relation between supp$\mathcal{F}$ and supp$\mathcal{F}^{\pi}$ is established by Properties 1 and 2.

Example 4. With Π defined as in Example 3, let the system be

$$\begin{cases} 2z_{11} + z_{16} + z_{13} = z_{24} + z_{23} \\ 2z_{12} + z_{13} + z_{16} = z_{25} + z_{26} \\ 2z_{13} + z_{14} + z_{11} = z_{26} + z_{21} \\ 2z_{14} + z_{12} + z_{15} = z_{21} + z_{25} \\ 2z_{15} + z_{11} + z_{14} = z_{22} + z_{24} \\ 2z_{16} + z_{15} + z_{12} = z_{23} + z_{22} \end{cases}$$

It can be checked that the reduced face lattice has 37 faces whereas the actual face lattice has 189. The 18 extreme rays are in 4 classes, which are identified by $(0,0,1,0,0,1,0,0,2,0,0,2)$, $(0,0,0,0,1,1,0,2,1,0,1,0)$, $(0,0,0,1,0,1,1,1,1,0,1,0)$, and $(0,0,1,0,4,1,2,6,0,2,2,0)$.

Conclusions. Some properties of the structure of the solution set of some Diophantine systems, with an highly symmetrical solution set, were discussed. An algorithm that finds a minimal covering of the face lattice is given. Ongoing study aims at a better characterization of such coverings, by inspecting the algebraic properties of the group of symmetries $(\Pi, \circ)$. In particular, this may lead to an exact characterization of the minimal covering of the face lattice for simplicial cones.

References

1. Abdulrab, H., Pécuchet, J.-P.: Solving Systems of Linear Diophantine Equations and Word Equations. *Proc. RTA'89*, LNCS 355, 530–532. Springer-Verlag, 1989.
2. Boudet, A., Contejean E.: AC-unification of higher-order patterns. *Proc. CP'97*, LNCS 1330, Springer-Verlag, 267–282, 1997.
3. Boudet, A., Contejean E., and Devie, H.: A new *AC* Unification algorithm with an algorithm for solving systems of Diophantine equations. In *Proc. LICS'90*, IEEE, 289–299, 1990.
4. Clausen, M., Fortenbacher, A.: Efficient solution of linear Diophantine equations. *J. Symbolic Computation*, 8:201–216, 1989.
5. Domenjoud, E.: *Outils pour la Déduction Automatique dans les Théories Associatives-Commutatives*. Thése de doctorat d'Université, Univ. Nancy I, 1991.
6. Domenjoud, E., Tomás, A.P. (1995). From Elliott-MacMahon to an Algorithm for General Linear Constraints on Naturals, *Proc. CP'95*, Lecture Notes in Computer Science 976, 18–35, Springer-Verlag.
7. Elliott, E. B: On linear homogenous Diophantine equations. *Quart. J. Pure Appl. Math.*, 34:348–377, 1903.
8. Huet, G.: An algorithm to generate the basis of solutions to homogeneous linear Diophantine equations. *Information Processing Letters*, 7(3):144–147, 1978.
9. Hilbert, D.: Ueber die Theorie der algebraischen Formen. *Math. Ann.*, 36:473–534, 1890.
10. MacMahon, P.: *Combinatory Analysis*, 2. Chelsea Publishing Co., 1918.
11. Pasechnik, D. V. : On computing Hilbert bases via the Elliot-MacMahon algorithm, *Theoretical Computer Science*, 263:37–46, 2001.
12. Pottier, L.: Minimal solutions of linear diophantine systems: bounds and algorithms. *Proc. RTA'91*, LNCS 488, Springer-Verlag, 162–173, 1991.
13. Schrijver, A.: *Theory of Linear and Integer Programming*, Wiley-Interscience, 1986.
14. Stanley, R. P.: Linear homogeneous Diophantine equations and magic labelings of graphs. *Duke Math. J.*, 40:607–632, 1973.
15. Stanley, R. P.: *Enumerative Combinatorics*, Vol I, The Wadsworth & Brooks/Cole Mathematics Series, 1986.
16. Tomás, A. P.: *On Solving Linear Diophantine Constraints*. Ph.D Thesis, Faculty of Sciences, University of Porto, 1997.
17. Tomás, A. P., Filgueiras, M.: Solving linear Diophantine equations using the geometric structure of the solution space. *Proc. RTA'97*, LNCS 1232, Springer-Verlag, 269–283, 1997.
18. Tomás, A. P., Filgueiras, M.: An Algorithm for Solving Systems of Linear Diophantine in Naturals. *Proc. EPIA'97*, LNAI 1323, Springer-Verlag, 73–84, 1997.