INSTITUT DE RECHERCHE EN INFORMATIQUE ET SYSTÈMES ALÉATOIRES

PUBLICATION INTERNE
N° 1016

ON MANIPULATING Z-POLYHEDRA

PATRICE QUINTON, SANJAY RAJOPADHYE, TANGUY RISSET

ISSN 1166-8687

IRISA
CAMPUS UNIVERSITAIRE DE BEAULIEU - 35042 RENNES CEDEX - FRANCE

IRISA

INSTITUT DE RECHERCHE EN INFORMATIQUE ET SYSTÈMES ALÉATOIRES
Campus de Beaulieu – 35042 Rennes Cedex – France
Tél. : (33) 99 84 71 00 – Fax : (33) 99 84 71 71

On Manipulating Z-polyhedra

Patrice Quinton, Sanjay Rajopadhye, Tanguy Risset

Thème 1 — Réseaux et systèmes
Projet API

Publication interne n° 1016 — Juillet 1996 — 21 pages

Abstract: We address the problem of computation upon $\mathbb{Z}$-polyhedra which are intersections of polyhedra and integral lattices. We introduce a canonic representation for $\mathbb{Z}$-polyhedra which allow to perform comparisons and transformations of $\mathbb{Z}$-polyhedra with the help of a computational kernel on polyhedra. This contribution is a step toward the manipulation of images of polyhedra by affine functions, and has application in the domain of automatic parallelization and parallel VLSI synthesis.

Key-words: regular parallelism, polyhedron, lattices, loop nest, Automatic synthesis methodology, vlsi

(Résumé : tsvp)

CNRS INRIA

Centre National de la Recherche Scientifique
(URA 227) Université de Rennes 1 – Insa de Rennes

Institut National de Recherche en Informatique
et en Automatique – unité de recherche de Rennes

Manipulations de Z-polyèdres

Résumé : Nous nous intéressons au problème du calcul sur les $\mathbb{Z}$-polyèdres (intersections entre des polyèdres et des treillis entiers). Nous introduisons une représentation canonique pour les $\mathbb{Z}$-polyèdres qui permet, avec l'aide d'un outils de calcul sur les polyèdres, d'effectuer des comparaisons et des transformations sur les $\mathbb{Z}$-polyèdres. Cette contribution est un pas vers la manipulation d'images de polyèdres par des fonctions affines. Les résultats présentés ici ont des applications dans le domaine de la parallélisation automatique et la synthèse d'architecture VLSI parallèles

Mots-clé : polyèdre, treillis, parallelisme régulier, nids de boucles, méthodologie de synthèse automatique, vlsi

1 Introduction

Research in parallel VLSI synthesis and automatic parallelization pay particular attention to the efficient treatment of loop nests which are the time consuming structures of programs. Manipulation of loop nests led to the study of convex polyhedra which represent their iteration spaces (in this paper, a *convex polyhedron* is in fact the set of integral points contained in a convex polyhedron). Recently, it became obvious that efficient tools were necessary to provide computational kernel on convex polyhedra ([Pug92, Fea92, Bal95, Tei93, Wil93]).

Manipulating upon these structures is not easy, and the mathematical foundation of the so-called *polyhedral theory*, has its roots in theory of linear and integer programming ([MRTT53, Che68, Sch86, NW88]). A convex polyhedron has two dual representations: intersection of half spaces or convex combinations of vertices. These representations were introduced by Motzkin ([MRTT53]), and Chernikova showed how to go from one to the other ([Che68]). Successive improvements of the Chernikova algorithm ([FQ88, Ver92]) provided a very efficient computational kernel on convex polyhedra.

Using this kernel, Wilde implemented a public domain polyhedral library ([Wil93]) which provided basic operations (intersection, union, image and preimage by integral functions, comparison tests, ...) of *domains* (sets of integral points contained in unions of finitely many convex polyhedra). The library has been useful in the field of regular parallelism for many researchers.

However, the polyhedral model is too restrictive when we target problems like, for instance, partitioning ([TT93]), multi-rate arrays modeling ([LR96]) or loop nests with non-unit stride ([Hel94]). In [TT93], Teich and Theile formally introduced (as *linearly bounded lattices* or LBL) the images of polyhedra by affine mappings. This class is very large and difficult to deal with, especially because the affine mappings considered are generally not invertible. Le Verge ([Ver94]) proposed a partial solution to this problem by introducing a *generalized inverse* in some particular cases. Some computation procedures were proposed by Teich in [Tei93].

In fact, for many problems for which the polyhedral model is too restrictive, the LBL model is too much general. One usually needs to manipulate convex with holes such that the remaining index points are regularly spaced. This notion (which corresponds to LBL with invertible mapping) has been introduced by Ancourt in [Anc91] as a *$\mathbb{Z}$-polyhedron*. However, no complete computational library for $\mathbb{Z}$-polyhedra was described. This paper is intended to give the theoretical background necessary to describe precisely such a library. For this, we need first to choose a representation for $\mathbb{Z}$-polyhedra, and then to describe valid operations on this representation.

This work was motivated by the desire to extend Alpha [Mau89, Wil93, QRR96]. Alpha is a functional language for synthesizing of parallel VLSI architectures from high level specification ([WS94]). In Alpha, representing two clocks, one being three times faster than the other must by done with $\mathbb{Z}$-polyhedra ([QRR96]). To obtain a coherent language which preserve the semantics and other important static analysis properties of Alpha, the new domains ($\mathbb{Z}$-polyhedra) must be closed under intersection, image by invertible affine function and preimage by an affine function. The results presented here provide the theoretical foundations for this extension. However, we believe that they have applications in other areas (such as loop transformations). For this reason, we make a conscious decision to separate it from the context of Alpha and simply present the theoretical results for manipulating $\mathbb{Z}$-polyhedra.

2 Definitions and preliminary results

The purpose of this section is to introduce the notations and the basic results needed in the paper.

Definition 1 (rational polyhedron) *A rational polyhedron is a subset of $\mathbb{Q}^k$ defined by a finite set of affine inequalities.*

We will call *polyhedron* a set of integral points contained in a rational polyhedron. If P is a rational polyhedron, we will note P^{int} the polyhedron consisting of the set of integer points in P ($P \cap \mathbb{Z}^n$), and if Q is a polyhedron, we will note Q^{rat} the rational polyhedron whose convex hull is the convex hull of Q.

Definition 2 (lattice) *A lattice is a subset of $\mathbb{Q}^k$ defined by integral linear combinations of linearly independent rational vectors of $\mathbb{Q}^k$, called generating vectors (or the basis of the lattice).*

An *integral lattice* is a lattice whose generating vectors are integral.

Definition 3 (true dimension) *The true dimension of a subset S of $\mathbb{Z}^n$ is the dimension of the minimum vector space that contains the convex hull of S. A subset of $\mathbb{Z}^n$ is* full dimensional *if its true dimension is n.*

Note here that we only deal with *linear* lattices (i.e. lattices containing 0. In section 5, we explain how all this work can be extended to affine integral lattices (affine integral combination of linearly independent integral vectors).

Definition 4 ($\mathbb{Z}$-polyhedron) *A $\mathbb{Z}$-polyhedron is the intersection of a polyhedron and an integral full dimensional lattice.*

Definition 5 (Hermite normal form) *A matrix of full row rank is said to be in Hermite normal form (HNF) if it has the form $[B\ 0]$ where B is a non singular, lower triangular, non negative matrix, in which each row has a unique maximum entry located on the main diagonal of B.*

Theorem 1 (Hermite normal form) *for any rational matrix M of full row rank, there exists a unique matrix H in Hermite normal form and a unimodular matrix U such that $M = HU$.*

Proof: [Sch86, pp. 45-46] □

Proposition 1 *Let A be a rational $n \times k$ matrix of full row rank. The set:*

$$L(A) = \{x \in \mathbb{Q}^n \mid x = Ay, \quad y \in \mathbb{Z}^k\}$$

is a lattice.

Proof: Let $[B\ 0]$ be the Hermite normal form of A. Since A is full row rank, B is $n \times n$ non singular. Thus $L(B) = \{x \mid x = By,\ y \in \mathbb{Z}^n\} = \{x \mid x = [B\ 0]y, \quad y \in \mathbb{Z}^k\} = L(A)$ and the columns of B are the linearly independent vectors generating $L(A)$ □

Proposition 2 (uniqueness of the Hermite normal form) *Let A and A' be rational matrices of full row rank, with Hermite normal forms $[B\ 0]$ and $[B'\ 0]$, respectively. Then the columns of A generate the same lattice as those of A', if and only if $B = B'$.*

Proof: [Sch86, p.48] □

In the following, we will say that a linear function is in Hermite normal form with respect to a basis (by default the canonical basis) if its matrix in the basis is in Hermite normal form. Now we can state the following important property:

Proposition 3 (lattice normal form) *Given a full dimensional lattice L, there exists a unique matrix H in Hermite normal form such that $L = L(H)$. Equivalently, there exists a unique linear function f in Hermite normal form such that*

$$L = f(\mathbb{Z}^k) = \{x \mid x = f(y),\ y \in \mathbb{Z}^k\}.$$

Proof: suppose that the lattice is defined by $L = \{x \mid x = My,\ y \in \mathbb{Z}^n\}$. M is full row rank. Let H_1 be the Hermite normal form of M, we have seen in the proof of Proposition 1 that $L(M) = L(H_1)$. Moreover, if H_2 is another matrix in Hermite normal form generating L, by Proposition 2, H_1=H_2 □

Remark: In this paper, we will only consider full dimensional lattices. In other words, when we speak of a lattice in $\mathbb{Q}^n$, then its generating vectors span the whole space $\mathbb{Q}^n$.

3 $\mathbb{Z}$-polyhedra canonic form

So far, we have defined a $\mathbb{Z}$-polyhedron as the intersection of a polyhedron and a lattice. For the purpose of compatibility with the existing polyhedral library, we will use an alternate representation, namely the image of a polyhedron by a non singular integral (not necessarily unimodular) linear function. Now, we will show that a $\mathbb{Z}$-polyhedron has a unique representation called its canonic form. We first consider the full dimensional case (section 3.1), then we look at the general case (section 3.2).

3.1 Full dimensional $\mathbb{Z}$-polyhedra

We prove that, if we represent of a full dimensional $\mathbb{Z}$-polyhedron by the intersection of a lattice and a rational polyhedron, the lattice is unique. We first prove (Lemma 1) that this is true if the $\mathbb{Z}$-polyhedron contains a basis of the lattice, then we prove that a $\mathbb{Z}$-polyhedron always contains a basis of the underlying lattice (theorem 2).

Lemma 1 *For every full dimensional $\mathbb{Z}$-polyhedron Z_1 in $\mathbb{Z}^n$, assume that there are two representations of Z_1: $Z_1 = T_1 \cap P_1$ and $Z_1 = T_2 \cap P_2$ where T_1, T_2 are lattices and P_1, P_2 are rational polyhedra. If Z_1 contains a basis of T_1 and a basis of T_2 then $T_1 = T_2$.*

Proof: Call H_1 and H_2 the Hermite normal form matrices that define T_1 and T_2. Let B_1 be the matrix whose columns are the vectors of the basis of T_1 in Z_1. As each column of B_1 is in T_1, there exists an integral matrix B'_1 such that $B_1 = H_1 B'_1$. Moreover, as B_1 is a basis of T_1 (every point of T_1 can be described by integral combinations of the columns of B_1), B'_1 is a basis of $\mathbb{Z}^n$ and thus is unimodular. Now, as all the columns of B_1 are in Z_1, they are also in T_2 thus $H_2^{-1} B_1$ is an integral matrix. As a consequence, there exists an integral matrix X_1 such that $H_2^{-1} H_1 B'_1 = X_1$, which is equivalent to say: there exists an integral matrix X'_1 such that: $H_1 = H_2 X'_1$.

Applying a similar argument to the basis of T_2, we can deduce that there exists an integral matrix X'_2 such that:$H_2 = H_1 X'_2$. As H_1 and H_2 are square and non singular, it follows that $X'_1 = X_2^{'-1}$ and thus the matrices X_1 and X_2 are unimodular. This means that H_1 and H_2 differ only by a unimodular transformation, and hence (as they are in Hermite normal form) they are equal. We can conclude that $T_1 = T_2$. □

Theorem 2 (uniqueness of the lattice of a $\mathbb{Z}$-polyhedron) *Given a full dimensional $\mathbb{Z}$-polyhedron Z_1 in $\mathbb{Z}^n$, assume that there are two representations of Z_1: $Z_1 = T_1 \cap P_1$ and $Z_1 = T_2 \cap P_2$ where T_1, T_2 are lattices and P_1, P_2 rational polyhedra. Then $T_1 = T_2$.*

Proof: Let H_1 and H_2 be the HNF matrices that define lattices T_1 and T_2. We will prove that $H_1 = H_2$. As Z_1 is full dimensional, there exist $n+1$ linearly independent points in Z_1, thus n linearly independent vectors starting from the same point z_0 of Z_1 and reaching n points of Z_1. Let B_1 be the integral matrix whose columns are these n vectors. Each column of B_1 belongs to T_1 and T_2, thus $M_1 = H_1^{-1}(B_1)$ and $M_2 = H_2^{-1}(B_1)$ are integral matrices. If M_1 and M_2 are unimodular, the result holds because of Lemma 1.

Suppose that one of the two matrices (say M_1) is not unimodular. Let C_1^M be the convex polyhedron generated by the columns of M_1 (that is the convex polyhedron whose vertices are $H_1^{-1}(z_0)$ and the points reached by the columns of M_1 from $H_1^{-1}(z_0)$, see figure 1-(b)). We will prove that there always exists an integral point strictly inside C_1^M (i.e inside and not equal to one of the vertices), this is illustrated on figure 1. To see that, just take the Smith Normal Form of M_1 [Sch86]: $M_1 = V_1^M S_1^M U_1^M$. Note that $det(S_1^M) = det(M_1) > 1$ since M_1 non unimodular. The transformations U_1^M and V_1^M are linear thus they preserve rational convexity and as they are unimodular, they also preserve the number of integral points present in the polyhedron generated by the columns of M_1 (C_1^M) and S_1^M (C_1^S). Thus if there

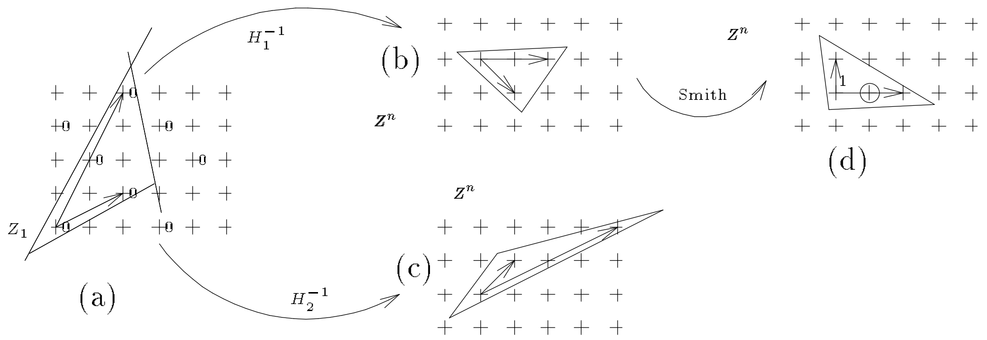


Figure 1: Principle of the proof of the unique representation of $\mathbb{Z}$-polyhedra: independent vectors of Z_1 (a) are sent to $\mathbb{Z}^n$ and normalized by the smith decomposition (d). If the result is not a basis of $\mathbb{Z}^n$, we can find a set of vectors defining a *smaller* basis (d)

is an integral point strictly inside C_1^S, it comes from a point strictly inside C_1^M. Now, As the determinant of S_1^M is greater than one, one of its diagonal coefficients is greater than one. If we set this coefficient to 1, we obtain a new integral diagonal matrix $S_1^{'M}$ which represents a convex polyhedron which is obviously included in C_1^M (see the surrounded point in figure 1-(d)), and such that $det(S_1^{'M}) < det(S_1^M)$. Thus, Matrix: $M_1' = V_1^M S_1^{'M} U_1^M$ represents a convex polyhedron which is strictly included in C_1^M (i.e included and $det(M_1') < det(M_1)$). Define $B_1' = H_1 M_1'$ which is included in Z_1 and thus there exists M_2' such that $B_1' = H_2 M_2'$. Note that $|det(M_2')| = \left|\frac{det(B_1')}{det(B_1)} det(M_2)\right| < |det(M_2)|$.

Thus we have defined a procedure that decreases by at least 1 the absolute value of the determinant of M_1 and M_2, if one of them is not unimodular. As these determinants can take only integral non zero values (we always keep independent vectors), they will be set to 1 in a finite time. Thus there always exists a basis of the lattice in a full dimensional $\mathbb{Z}$-polyhedron and (by Lemma 1) the lattice is unique: $T_1 = T_2$ □

The previous uniqueness result is one of the key result of this paper, it will permit (as explained later) to define a canonic representation of any $\mathbb{Z}$-polyhedra. We introduce here the canonic form for a full dimensional $\mathbb{Z}$-polyhedron using the representation of $\mathbb{Z}$-polyhedron by image of a polyhedron by a linear integral non singular function.

Proposition 4 *For every full dimensional $\mathbb{Z}$-polyhedron $Z_1 = L_1 \cap Q_1$ in $\mathbb{Z}^n$, where L_1 is a lattice and Q_1 a polyhedron, there exists a polyhedron P_1 and a unique integral non singular linear function f in Hermite normal form such that:*

$$Z_1 = f(P_1) = \{x \mid x = Fy, \quad y \in P_1\}.$$

Proof: As Z_1 is full dimensional, by theorem 2, L_1 is unique. We also know that there is a unique HNF matrix H_1 such that $L(H_1) = L_1$ (H_1 is integral invertible because L_1

is an integral full dimensional lattice). If f is the function represented by H_1, we take $P_1 = f^{-1}(Q_1)$, and it is easy to see that $Z_1 = f(P_1)$. Indeed, for each integral point $p \in P_1$, $f(p) \in L_1$ and $f(p) \in Q_1$ thus $f(P_1) \subset Z_1$. Conversely, for any point q of Z_1, $f^{-1}(q)$ is integral and $f^{-1}(q) \in P_1$, thus $Z_1 = f(P_1)$.

Conversely, Let f_2 in Hermite normal form and P_2 be such that $Z_1 = f_2(P_2)$. Then $Z_1 = f_2(\mathbb{Z}^n) \cap (f_2(P_2))^{rat}$. By theorem 2, we have $L_1 = f_2(\mathbb{Z}^n)$ and as f_2 is in HNF, by Proposition 2 we have $f_2 = f_1$. □

From now on, we will denote (f, P) the $\mathbb{Z}$-polyhedron which is the image by the integral non singular function f of the polyhedron P. The following proposition ensures the existence of a normal form for full dimensional polyhedra.

Proposition 5 *Let $Z_1 = (f_1, P_1)$ and $Z_2 = (f_2, P_2)$ be two full dimensional $\mathbb{Z}$-polyhedra in normal form (f_1 and f_2 in Hermite normal form), then $Z_1 = Z_2$ if and only if $f_1 = f_2$ and $P_1^{int} = P_2^{int}$.*

Proof: If $Z_1 = Z_2$, then (Proposition 4) $f_1 = f_2$. Suppose that $P_1^{int} \neq P_2^{int}$. There exists an integral point p in, say P_1, which is not in P_2. $f_1(p) \in Z_1$ thus $f_2^{-1}(f_1(p)) \in P_2$. As $f_1 = f_2$, $f_2^{-1}(f_1(p)) = p$ and we have a contradiction, thus we must have $P_1^{int} = P_2^{int}$.

Conversely, it is obvious that, if $f_1 = f_2$ and $P_1^{int} = P_2^{int}$ then $(f_1, P_1) = (f_2, P_2)$. □

3.2 General case

In the previous section, we provided a unique canonic form for a full dimensional $\mathbb{Z}$-polyhedron. In this section we define a canonic form for a $\mathbb{Z}$-polyhedron which is not full dimensional (called a degenerate $\mathbb{Z}$-polyhedron). If $Z_1 = f_1(P_1)$ is a degenerate $\mathbb{Z}$-polyhedron, we denote $Vect(Z_1)$ the vector space generated by Z_1. In our canonic form, we will force f_1 to be the identity on the subspace orthogonal to $Vect(Z_1)$.

Lemma 2 *Let Z_1 be a $\mathbb{Z}$-polyhedron of true dimension k in $\mathbb{Z}^n$. There exists a unimodular basis $B = (b_1, \ldots, b_n)$ such that $Z_1 = Z_1 \cap Vect(b_1, \ldots, b_k)$ (i.e, all components of the points of Z_1 on $(b_{k+1}, \ldots, b_n)$ are 0).*

Proof: Consider k linearly independent vectors that define a basis of the linear space $Vect(Z_1)$. Consider the $k \times n$ full row rank matrix M whose rows are these vectors. The Hermite normal form of M provide M' ($k \times n$ HNF matrix) and U ($n \times n$ unimodular matrix) such that $M = M'U$. The rows of U are exactly the basis that we are looking for. Indeed, $M = M'U = [H\ 0]U$, which means that the k rows of M are obtained from the k first rows of U. Thus $Vect(Z_1) \subset Vect(u_1, \ldots, u_k)$. The components of the points of Z_1 on the vectors $(u_{k+1}, \ldots, u_n)$, are constant. We just have to provide a translation so that they are all zero □

To compute such a basis, one can look for the HNF of a matrix composed of the set of vertices of the domain. We will now introduce our canonic form of a degenerate $\mathbb{Z}$-polyhedron.

Theorem 3 ($\mathbb{Z}$-polyhedron canonic form) *Let $Z_1 = L_1 \cap Q_1$ be a $\mathbb{Z}$-polyhedron of true dimension k in $\mathbb{Z}^n$ (L_1 is a full dimensional lattice, Q is a dense rational polyhedron), and let B be a unimodular basis such that $Z_1 \subset Vect(b_1, \ldots, b_k)$ (as defined in Lemma 2 for instance). There exists a unique integral non singular function f and a polyhedron $P_1 \subset Vect(b_1, \ldots, b_k)$ such that $Z_1 = f(P_1)$ and the matrix of f in basis B is of the form $\begin{pmatrix} H & 0 \\ 0 & Id \end{pmatrix}$ where H is in Hermite normal form. Moreover, given B, if P_1 is equal to its integral hull then P_1 is unique.*

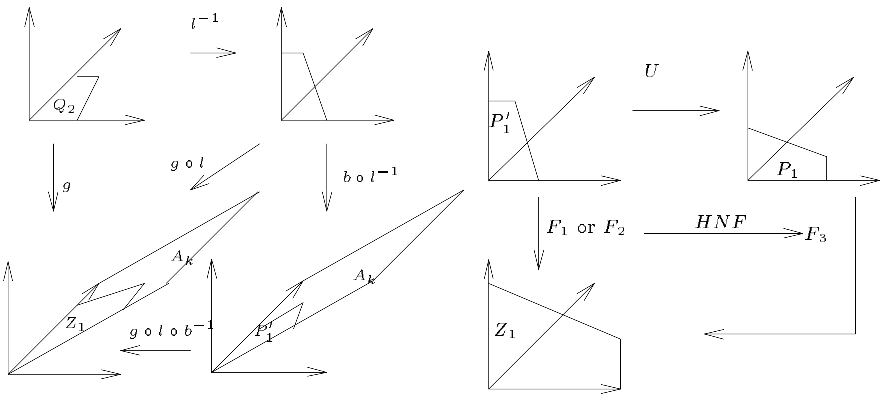
Proof: Let $A_k = Vect(b_1, \ldots, b_k)$. First, we prove the uniqueness of f. Let h be the function $\mathbb{Z}^k \to \mathbb{Z}^k$ whose matrix in the canonical basis of $\mathbb{Z}^k$ is H. If the function f exists, then f is completely defined by its restriction h to A_k. If we consider the $\mathbb{Z}$-polyhedron $Z_2 = Z_1 \cap A_k$ of $\mathbb{Z}^k$, and $P_2 = P_1 \cap A_k$, then $Z_2 = h(P_2)$. Z_2 is full dimensional in A_k, h is in Hermite normal form, thus by theorem 2, h is unique. Thus f is unique. Now, if P_3 is such that $f(P_1) = f(P_3)$ then the sets of integer points of P_1 and P_3 are equal because f is invertible.

Now we construct f. Let $Z_1 = L_1 \cap Q_1$ be the original representation of Z_1, and let g be a function defining the lattice L_1 (L_1 is full dimensional thus g is non singular). If we take $Q_2 = (g^{-1}(Q_1)))^{int}$, we have $Z_1 = g(Q_2)$. g is non singular thus the true dimension of Q_2 is k. Let $L = (l_1, \ldots, l_n)$ be a basis of $\mathbb{Z}^n$ such that $Q_2 \subset Vect(l_1, \ldots, l_k)$ (b and l are the functions whose matrices in the canonical basis are B and L). Consider $P'_1 = b \circ l^{-1}(Q_2)$, we have $P'_1 \subset A_k$. Considering $f_1 = g \circ l \circ b^{-1}$, we have $f_1(P'_1) = g \circ l \circ b^{-1} \circ b \circ l^{-1}(Q_2) = Z_1$. Now, if we consider the matrix F_1 of f_1 in basis B (that is the matrix of function $b^{-1} \circ g \circ l$ in the canonical basis), it has the form: $F_1 = \begin{pmatrix} F_{11} & X \\ 0 & Y \end{pmatrix}$ where F_{11} is a $k \times k$ matrix. As $P'_1 \subset A_k$, if we consider f_2 whose matrix in B is $F_2 = \begin{pmatrix} F_{11} & 0 \\ 0 & Id_{n-k} \end{pmatrix}$, we have $f_2(P'_1) = f_1(P'_1)$. Finally, if we take the Hermite normal form of F_{11}: $F_{11} = HU$, we can find $P_1 = \begin{pmatrix} U & 0 \\ 0 & Id_{n-k} \end{pmatrix} P'_1$ and $F_3 = \begin{pmatrix} H & 0 \\ 0 & Id_{n-k} \end{pmatrix}$. If f is the function whose matrix in basis B is F_3, we have: $Z_1 = f(P_1)$. Thus the existence is proved. □

The construction performed in the previous proof defines a way to set a $\mathbb{Z}$-polyhedron $Z_1 = g(Q_2)$ in canonic form. The process is illustrated in figure 2 with the notations of the proof. The first part of the construction consists in unimodular transformations on the source polyhedron Q_2 to obtain P'_1 (figure 2-(a)), then modifications of function g and P'_1 are performed simultaneously to obtain $f(P_1)$ (from F_1 to F_2 and from F_2 to F_3 figure 2-(b)).

We have introduced a *canonic form* for a general $\mathbb{Z}$-polyhedron. The canonic form of a $\mathbb{Z}$-polyhedron Z_1 will be (F, P, B) where the matrix F is expressed in basis B, (i.e. $Z_1 = BF(P)$ in the canonical basis) and has the properties described in Theorem 3 and P is equal to its integral hull. We will describe in section 5 a procedure for finding a canonic form of a $\mathbb{Z}$-polyhedron $Z_1 = f_1(P_1)$. The first phase consists in choosing a correct basis B and then the second phase derives the representation $f_2(P_2)$ as in figure 2. This canonic form has the following properties:

- P_2 is obtained from P_1 by unimodular basis changes.



(a)
Unimodular basis change on the source polyhedron Q_2 to bring it into the space of the $\mathbb{Z}$-polyhedron Z_1. The polyhedra are represented in the canonical basis of Z^3.

(b)
Hermit normalization to obtain the $\mathbb{Z}$-polyhedron canonic form. The polyhedra are represented in basis B.

Figure 2: Construction procedure for $\mathbb{Z}$-polyhedron canonic form

- Z_1 has exactly the same number of points as P_2.

4 Closure properties of $\mathbb{Z}$-polyhedra

In this section, we state some closure properties of $\mathbb{Z}$-polyhedra necessary to provide a complete computationnal kernel for $\mathbb{Z}$-polyhedra.

Proposition 6 *The intersection of two $\mathbb{Z}$-polyhedra is a $\mathbb{Z}$-polyhedron*

Proof: by taking the original representation, this is obvious: $Z_1 = L_1 \cap P_1$, $Z_2 = L_2 \cap P_2$. $L_1 \cap L_2$ is a full dimensional integral lattice (remember that we consider linear lattices), and $P_1 \cap P_2$ is a rational polyhedron, hence the result. $\square$

Image and preimage of a $\mathbb{Z}$-polyhedron by a function are defined in the following way:

- if $f : \mathbb{Q}^n \rightarrow \mathbb{Q}^l$ is a linear rational mapping

$$f(Z_1) = \{x \in \mathbb{Z}^l \mid (\exists y \in Z_1) \;\; f(y) = x\}.$$

- and if Z_1 is a $\mathbb{Z}$-polyhedron in $\mathbb{Z}^n$, and $g : \mathbb{Q}^k \rightarrow \mathbb{Q}^n$ is a linear rational mapping then:

$$Pre(Z_1, g) = \{x \in \mathbb{Z}^k \mid g(x) \in Z_1\},$$

Note that this is not the classical notion of image and preimage, we impose the condition that these sets contain integral points because we will use rational functions. note also that if f is non singular, $Pre(Z_1, f) = f^{-1}(Z_1)$.

From the definition of Pre, it is clear that the preimage of a $\mathbb{Z}$-polyhedron by a rational invertible function is a $\mathbb{Z}$-polyhedron. Indeed, if g is invertible, the preimage by g of the underlying lattice is a rational full dimensional lattice intersected with $\mathbb{Z}^k$, thus it is an integral full dimensional lattice. And we know that the preimage of the polyhedron is a polyhedron ([Mau89, Wil93]), thus the preimage of a $\mathbb{Z}$-polyhedron by a non singular function is a $\mathbb{Z}$-polyhedron. In section 5, we introduce a procedure that uses the Smith decomposition of the function defining the lattice to compute the preimage (and image) of a $\mathbb{Z}$-polyhedron by a non singular function. The preimage by any (possibly singular) function is less obvious. The following Proposition ensures that it is always a $\mathbb{Z}$-polyhedron.

Proposition 7 *If Z_1 is a $\mathbb{Z}$-polyhedron of $\mathbb{Z}^k$ and $g : \mathbb{Q}^n \rightarrow \mathbb{Q}^k$ is a rational linear mapping, then the preimage of Z_1 by g is a $\mathbb{Z}$-polyhedron.*

Proof: Consider the representation of Z_1: $Z_1 = L_1 \cap Q_1$

$$\begin{aligned} Pre(Z_1, g) &= \{x \in \mathbb{Z}^n \mid (\exists y \in Z_1)\ \ g(x) = y\} \\ &= \{x \in \mathbb{Z}^n \mid (\exists y \in L_1)\ \ g(x) = y\} \cap \{x \in \mathbb{Q}^n \mid (\exists y \in Q_1)\ \ g(x) = y\} \\ &= Pre(L_1, g) \cap \{x \in \mathbb{Q}^n \mid (\exists y \in Q_1)\ \ g(x) = y\}. \end{aligned}$$

As $\{x \in \mathbb{Q}^n \mid (\exists y \in Q_1)\ \ g(x) = y\}$ is the preimage of a rational polyhedron by a linear function, it is a rational polyhedron. We will now prove that $Pre(L_1, g)$ is a lattice. Let $Im(g) = g(\mathbb{Q}^n)$, $Ker(g) = \{x \in \mathbb{Q}^n \mid g(x) = 0\}$ and $k_1 = dim(Ker(g))$. We know that we can find a basis B of $\mathbb{Z}^n$ such that $Ker(g) = Vect(b_1, \ldots, b_{k_1})$ (Lemma 2). Let $Source(g) = Vect(b_{k_1+1}, \ldots, b_n)$, then $\mathbb{Q}^n = Ker(g) \oplus Source(g)$. Moreover, if we call g' the restriction of g to $Source(g)$, we know that g' is a one to one mapping from $Source(g)$ to $Im(g)$.

We first prove that every point x of $Pre(L_1, g)$ can be decomposed in an unique manner into $x_1 + x_2$ with $x_1 \in Pre(L_1, g')$, $x_2 \in Ker(g)$, x_1 and x_2 integral. For any $x \in Pre(L_1, g)$ there exists a unique pair $(x_1, x_2) \in Source(g) \times Ker(g)$ such that $x = x_1 + x_2$. If we express this decomposition on basis B defined above, we can easily see that x_1 and x_2 have integral coordinates in this basis, thus they are integral point as B is a basis of $\mathbb{Z}^n$. As there exists $y \in L_1$ such that $g(x) = y$, we have: $y = g(x) = g(x_1) = g'(x_1)$, thus $x_1 \in Pre(L_1, g')$. Conversely, for any $(x_1, x_2) \in Pre(L_1, g') \times Ker(g)$, if x_1 and x_2 are integral $x = x_1 + x_2 \in Pre(L_1, g)$ because $g(x) = g'(x_1) \in L_1$. We now prove that $Pre(L_1, g')$ is a lattice in $Source(g)$. Just remark that, if $L_1 = f(\mathbb{Z}^k)$, $L_2 = L_1 \cap Im(g)$ is a lattice in $Im(g)$, $L_2 = f_2(\mathbb{Z}^{n-k_1})$, thus $Pre(L_1, g') = {g'}^{-1}(f_2(\mathbb{Z}^{n-k_1}))$ which is a lattice in $Source(g)$.

Every point of $Pre(L_1, g')$ can be described by a linear integral combination of $n - k_1$ independent integral vectors $(v_{k_1+1}, \ldots, v_n)$. As every integral point of $Ker(g)$ can be described by a linear integral combination of k_1 independent integral vectors $(b_1, \ldots, b_{k_1})$ and as $Ker(g) \cap Source(g) = 0$, every integral vectors of $Pre(L_1, g)$ can be described by a linear integral combination of $(b_1, \ldots, b_{k_1}, v_{k_1+1}, \ldots, v_n)$. Thus $Pre(L_1, g)$ is a lattice.

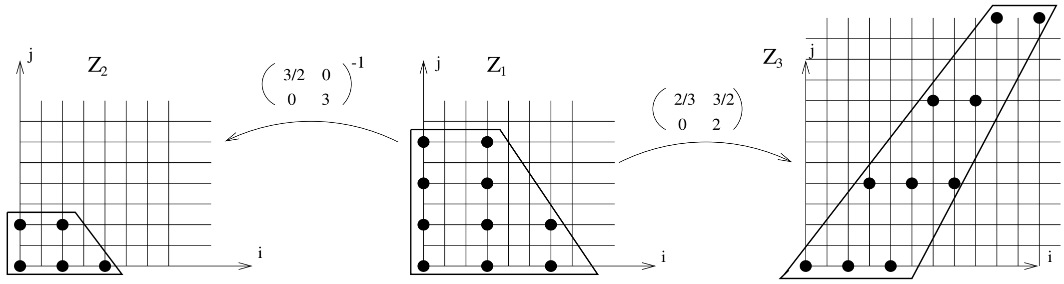


Figure 3: Preimage and image of a $\mathbb{Z}$-polyhedron by non singular functions. The transformation on the right is pseudo-unimodular, the left one is not.

Finally, $Pre(Z_1, g)$ is the intersection of a lattice and a rational polyhedron, it is a $\mathbb{Z}$-polyhedron. □

Note that the full dimensionality of the $\mathbb{Z}$-polyhedron may not be preserved, even if we consider non singular function. The following Proposition gives necessary and sufficient conditions that an invertible function must satisfy to preserve the number of points. This property defines exactly the set of functions for which taking the image of a $\mathbb{Z}$-polyhedron can be considered as a *pseudo-unimodular* change of basis (see figure 3). A transformation applied to a $\mathbb{Z}$-polyhedron is pseudo-unimodular with respect to this $\mathbb{Z}$-polyhedron if, by applying its inverse to the image of the $\mathbb{Z}$-polyhedron, we get exactly the original $\mathbb{Z}$-polyhedron.

Proposition 8 *Let $Z_1 = (f_1, P_1)$ be a $\mathbb{Z}$-polyhedron of true dimension k in $\mathbb{Z}^n$ and let (F_2, P_2, B_2) be the canonic form of Z_1. Let g be rational invertible matrix and G_2 be the matrix of g expressed in B_2. Then g is pseudo-unimodular with respect to Z_1 if and only if the first k columns of G_2F_2 are integral.*

Proof: First, remember that P_2 is obtained from P_1 by a unimodular transformation thus both have the same number of points. Suppose that the condition is met. As g is invertible, points of $f_1(P_1)$ are mapped by g to different points. The canonic form imposes that every point of P_2 is mapped in $Vect(b_1, \ldots, b_k)$ by F_2 ($(b_i)_i$ are the vectors of B_2). Hence, the condition ensures that every point of P_2 is mapped to an integral point by G_2F_2 (each of these points are different because G_2F_2 is invertible). By applying G_2^{-1} on the image, we get back to Z_1.

Conversely, suppose now that the condition is not met. Let h be the first $k \times k$ sub-matrix of F_2. We have proved (theorem 2) that we can find a basis of the lattice generating Z_1 such that it corresponds to the image by h of a basis Z^k included in P_2 (these vectors can be obtained by starting from a point of P_2 and reaching k different points of P_2). Let $\begin{pmatrix} B \\ 0 \end{pmatrix}$ be the matrix whose columns are these k vectors expressed in basis B_2. The first k columns of

$G_2F_2 \begin{pmatrix} B & 0 \\ 0 & Id \end{pmatrix}$ are the images of these k vectors by $g \circ f$ (in basis B_2). Now remark that saying that one of the coefficient of the first k columns of G_2F_2 is not integral is equivalent to say that one of the coefficient of the first k columns of $G_2F_2 \begin{pmatrix} B & 0 \\ 0 & Id \end{pmatrix}$. Indeed, B is unimodular and the columns are conserved because of the form of the matrix $\begin{pmatrix} B & 0 \\ 0 & Id \end{pmatrix}$. If one of the coefficients of these columns is not integral, it implies that an integral point of P_2 is mapped to a rational point by G_2F_2. Thus this point is lost. Moreover, because of the definition of the image of a $\mathbb{Z}$-polyhedron, no new point may be created by G_2F_2 (i.e for every point $p_1 \in P_2$ there exists at most one integral point $p_2 \in G_2F_2(P_2)$ such that $p_2 = G_2F_2(p_1)$). Thus the number of points in $G_2F_2(P_2)$ may not be equal to the number of points in P_2 which is the number of points of $F_2(P_2)$. Thus we have the result. □

Note that a sufficient condition is that $g \circ f_1$ is an integral affine function. As we have defined image and preimage in a slightly non-standard manner (by intersecting with the canonical lattice), we must redefine the usual compatibility rules between the function composition and the operations on $\mathbb{Z}$-polyhedra (intersection and union).

Lemma 3 *If Z_1 and Z_2 are two $\mathbb{Z}$-polyhedra in $\mathbb{Z}^n$ and $f : \mathbb{Q}^k \to \mathbb{Q}^n$ a rational linear mapping, $Pre(Z_1 \cap Z_2, f) = Pre(Z_1, f) \cap Pre(Z_2, f)$*

Proof: Let $x \in Pre(Z_1 \cap Z_2, f)$, there exists $y \in Z_1 \cap Z_2$ such that $f(x) = y$. As x is integral, $x \in Pre(Z_1, f)$ and $x \in Pre(Z_2, f)$. Conversely, let $x \in Pre(Z_1, f) \cap Pre(Z_2, f)$, there exists $y_1 \in Z_1$ and $y_2 \in Z_2$ such that: $f(x) = y_1$ and $f(x) = y_2$. As f is a function, $y_1 = y_2$ thus $x \in Pre(Z_1 \cap Z_2, f)$ □

Lemma 4 *If Z_1 and Z_2 are two $\mathbb{Z}$-polyhedra in $\mathbb{Z}^n$ and $f : \mathbb{Q}^k \to \mathbb{Q}^n$ a rational linear mapping, $Pre(Z_1 \cup Z_2, f) = Pre(Z_1, f) \cup Pre(Z_2, f)$*

Proof: Let $x \in Pre(Z_1 \cup Z_2, f)$, there exists $y \in Z_1 \cup Z_2$ such that $f(x) = y$. Say, without loss of generality that $y \in Z_1$, as x is integral, $x \in Pre(Z_1, f)$ thus $x \in Pre(Z_1, f) \cup Pre(Z_2, f)$. Conversely, let $x \in Pre(Z_1, f) \cup Pre(Z_2, f)$, Say, without loss of generality that $x \in Pre(Z_1, f)$, there exists $y_1 \in Z_1$ such that: $f(x) = y_1$. $y_1 \in Z_1 \cup Z_2$ and x integral thus $x \in Pre(Z_1 \cup Z_2, f)$. □

These two lemma can also be applied to images of $\mathbb{Z}$-polyhedra by invertible functions. The major difference implied by the notion of preimage and image we use appears when we introduce the composition of functions.

Proposition 9 *Let Z_1 be a $\mathbb{Z}$-polyhedron of $\mathbb{Z}^n$ and f, g rational linear mappings $f : \mathbb{Q}^k \to \mathbb{Q}^n$ and $g : \mathbb{Q}^l \to \mathbb{Q}^k$. Then $Pre(Pre(Z_1, f), g) = Pre(Z_1, f \circ g) \cap Pre(\mathbb{Z}^k, g)$*

Proof: If $f^{-1}(Z_1) = \{x \in \mathbb{Q}^k \mid \exists y \in Z_1 \quad f(x) = y\}$ (the classical notion of preimage), by definition of Pre, we have: $Pre(Z_1, f) = f^{-1}(Z_1) \cap \mathbb{Z}^k$. Thus $Pre(Pre(Z_1, f), g) = g^{-1}(f^{-1}(Z_1) \cap \mathbb{Z}^k) \cap \mathbb{Z}^l$. The classical notion of preimage has the properties of lemma 3 and 4), thus $g^{-1}(f^{-1}(Z_1)\cap \mathbb{Z}^k) = g^{-1}(f^{-1}(Z_1))\cap g^{-1}(\mathbb{Z}^k)$. As $f\circ g : \mathbb{Q}^l \rightarrow \mathbb{Q}^n$, $Pre(Z_1, f\circ g) = (f\circ g)^{-1}(Z_1)\cap \mathbb{Z}^l = g^{-1}\circ f^{-1}(Z_1)\cap \mathbb{Z}^l$. Thus $Pre(Pre(Z_1, f), g) = (g^{-1}(f^{-1}(Z_1))\cap \mathbb{Z}^l)\cap (g^{-1}(\mathbb{Z}^k)\cap \mathbb{Z}^l) = Pre(Z_1, f\circ g)\cap Pre(\mathbb{Z}^k, g)$. □

5 Algorithms

In this section, we describe algorithms that are derived from the results of previous sections. This explains how one can implement a computation library on $\mathbb{Z}$-polyhedra. We suppose that we have all the functionalities of the polyhedral library [Wil93]. We also have procedure for finding the Hermite normal form and the Smith normal form of a matrix. These algorithms have been implemented in the MMAlpha environnement based on Mathematica and the polyhedral library.

5.1 On affine Lattices

All the previous results where proved under the assumption that the lattices where linear lattices (i.e. contain 0). In the algorithms presented hereafter, the lattices are *affine* (it is usually the case). We briefly explain here how previous results can be extended to the case where the lattices are affine integral combination of integral independent vectors (the constant part being integral too).

The first problem concern the generalization of Proposition 3, which gives a canonic form for a linear lattice. Every full dimensional linear lattice has a unique representation as $L(H)$ where H is in Hermite normal form. This is no more true for affine lattice. For instant, the lattices $\{2i+2, 3j \mid i, j \in \mathbb{Z}\}$ and $\{2i, 3j \mid i, j \in \mathbb{Z}\}$ are exactly the same and the linear part of the underlying matrices H are in Hermite normal form. This problem is solved with the following extension of Proposition 3:

Proposition 10 (affine lattice normal form) *Given a full dimensional affine lattice L, there exists a unique matrix H in Hermite normal form and a unique vector h such that such that $L = L(H) + h$, with the property $0 \leq h_i < H_{i,i}$ $\forall i$.*

Proof: An affine Lattice of $\mathbb{Z}^n$ is defined by $L(H) + l = \{x \mid x = Hy + l \;\; y \in \mathbb{Z}^n\}$. we will suppose that H is in Hermite normal form, If it is not the case, just perform the transformation as if the lattice was linear and change the constant accordingly. It is easy to see that $L_2 = \{x \mid x = H_2 y + l_2 \;\; y \in \mathbb{Z}^n\} = L$ if and only if $H = H_2$ (otherwise they do not contain the same vectors) and $H^{-1}(l - l_2)$ is integral. Indeed, if $H^{-1}(l-l_2)$ is integral, for each $x \in L$, $x = Hy + l = H_2(y - (H^{-1}(l_2 - l))) + l_2$ thus $x \in L_2$ and the reciprocal is proved the same way.

The existence of h is proved recursively. Suppose that there exists a index k ($k \geq 1$) such that for $i < k$, $0 \leq l_i \leq H_{i,i}$. Consider a point x of L: $x = Hy_1 + l$. If $l_k > H_{k,k}$, let $l_k = qH_{k,k} + r$ be the Euclidean division of l_k by $H_{k,k}$. We call v^k the vector such that $v^k_j = 0$ for $j \neq k$ and $v^k_j = q$ and $V^k = Hv^k$ (The $k-1$ first component of V^k are zero). Now just note that $x = Hy_1 + l = H(y_1 + v_k) + l - V^k$. If we call $l' = l - V_k$, the first $k-1$

components of l' are the first $k-1$ components of l and the k^{th} component is r which is between 0 and $H_{k,k}-1$. As v_k and V_k do not depend of x, we have found a new expression for lattice L: $L = \{x \mid x = Hy + l' \; y \in \mathbb{Z}^n\}$ such that for all $i \leq k$, $0 \leq l'_i < H_{i,i}$. Hence the existence of h is recursively proved.

For he uniqueness, consider h_1 and h_2 having the property requested. As $L(H) + h^1 = L(H) + h^2$, $H^{-1}(h^1 - h^2)$ is integral. Again, we prove recursively that $h^1 = h^2$. Let $m = H^{-1}(h^1 - h^2)$, first note that $m_1 = (h^1_1 - h^2_1)/H_{1,1}$. As m_1 is integral and $0 \leq h^1_1, h^2_1 < H_{1,1}$ we must have $h^1_1 = h^2_1$. Now suppose that there exists a $k \geq 1$ such that for all $i < k$, $h^1_i = h^2_i$. We have: $m_k = \sum_{j=1}^{k}(H^{-1}_{k,j}(h^1_j - h^2_j)) = H^{-1}_{k,k}(h^1_k - h^2_k) = (h^1_k - h^2_k)/H_{k,k}$. As m_k is integral and $0 \leq h^1_k, h^2_k < H_{k,k}$, we must have $h^1_k = h^2_k$. Hence the result. □

This result allow to generalize Theorem 2, Proposition 4 and also Theorem 3 for canonic form of degenerate $\mathbb{Z}$-polyhedra.

Some generalization must be done for the closure properties. First, the intersection of two affine lattices can be empty. Hence, we need to provide special procedure to handle that case. In fact, we can prove the following proposition:

Proposition 11 *The intersection of Two full dimensional affine lattices is either empty or full dimensional.*

Proof: Consider $L_1 = L(A) + a$ and $L_2 = L(B) + b$. Suppose that the intersection $L = L_1 \cap L_2$ contain at least one point t. $t = Ax + a = By + b$ thus $x = A^{-1}By + A^{-1}(b-a)$ is integral. Consider now, if we note e_i the i^{th} vector of the canonical basis, the n vectors $z_i = y + \Lambda_i e_i$ where Λ_i is an integer such that $A^{-1}(\Lambda_i e_i)$ is integral (Λ_i always exists). And consider the other n vectors $z'_i = A^{-1}Bz_i + A^{-1}(b-a)$. First note that each z'_i is integral because $z'_i = x + \Lambda A^{-1} e_i$. Then note that $Az'_i + a = Bz_i + b$ thus $Bz_i + b$ belongs to L_1 and L_2 for all i. Finally, note that, as B is invertible, $(y - z_i)_{i=1..n}$ are n linearly independent vectors thus, so are $(t - Bz_i - b)_{i=1..n}$ thus the intersection is full dimensional. □

Image and preimage have been computed with linear mapping. Adding a constant part to deal with affine mappings does not change the results presented in section 4.

The main difficulties appear when implementing computations. Dealing with affine mapping needs special procedure (special Hermite normal form, ...). In the polyhedral library, the constant part is assimilated to an additional dimension ξ, which always has the value $\xi = 1$. In the rest of this section, we provide algorithm for the general case: $\mathbb{Z}$-polyhedra with affine lattices in the representation chosen by the polyhedral library.

5.2 Finding a Hermite basis

This algorithm finds, given a set of integral vectors $(v_i)_{i=1..k}$ of $\mathbb{Z}^n$, the dimension l of $Vect(v_i)_{i=1..k}$ and a unimodular basis U such that $Vect(v_i)_{i=1..k} = Vect(u_1, \ldots, u_l)$. Here the u_i are the columns of U such that the first l vectors of U span $Vect(v_i)_{i=1..k}$.

`FindHermiteBasis(`$(v_1)_{i=1..k}$`)`
  `Let` M `be the` $k \times n$ `matrix whose rows are the` v_i`.`

```
  Let M' be a subset of the rows of M spanning the same subspace
  Let M' = HU be the Hermite decomposition of M'.
  Let l be the number of non zero column in H.
  Return(l, U)
```

Note that we must start with a full row rank matrix otherwise the algorithm does not give the correct l. In the following, this algorithm is used with a polyhedron or a $\mathbb{Z}$-polyhedron as input provided we know a system of vector spanning exactly the same space as it (this is easy to build with the internal polyhedral library representation). This procedure consist of linear transformation (not affine). If we want to use it on affine objects (polyhedron or points), the coordinates of the objects in the new basis will be constant. There remains to perform a translation so that the coordinate of the polyhedron in the new basis are zero.

5.3 Finding the canonic form of a $\mathbb{Z}$-polyhedron

This procedure returns, given a $\mathbb{Z}$-polyhedron represented by $Z_1 = (F_1, P_1)$ the canonic form (F_2, P_2, B_2) of Z_1: F_2 is in Hermite normal form, P_2 is included in the first coordinates, the representation is expressed in basis B_2 (that is: $B_2F_2(P_2) = F_1(P_1)$).

FindNormalForm(F_1, P_1)
  Let (l_1, B_1)=FindHermiteBasis(P_1)
  Let (l_2, B_2)=FindHermiteBasis($F_1(P_1)$)
    /* we have $l_1 = l_2$ */
  Let $T_1 = B_2^{-1}F_1B_1$
  If $T_1 = \begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} + \begin{pmatrix} T_{c,1} \end{pmatrix}$, Let $(H_{11}, U_{11}) = HNF(T_{11})$
    /* T_{11} is $k \times k$ where k is the true dimension of Z_1 */
  Let $T_2 = \begin{pmatrix} H_{11} & 0 \\ 0 & Id_{n-k} \end{pmatrix} + \begin{pmatrix} T_{c,1} \end{pmatrix}$
  Let $P_2 = \begin{pmatrix} U_{11} & 0 \\ 0 & Id_{n-k} \end{pmatrix} B_1^{-1}(P_1)$
  return(T_2, P_2, B_2)

Note that we have:
$B_2T_2(P_2) = B_2\left(\begin{pmatrix} H_{11} & 0 \\ 0 & Id_{n-k} \end{pmatrix}\right)\left(\begin{pmatrix} U_{11} & 0 \\ 0 & Id_{n-k} \end{pmatrix} B_1^{-1}(P_1)\right) + T_{c,1}\Big)$,
and $B_2(\begin{pmatrix} T_{11} & 0 \\ 0 & Id_{n-k} \end{pmatrix} B_1^{-1}(P_1) + T_{c,1}) = B_2T_1B_1^{-1}(P_1)$ because both $B_1^{-1}(P_1)$ and $T_1B_1^{-1}(P_1)$ have their last $n-k$ coordinates set to zero. Thus: $B_2F_2(P_2) = B_2T_1B_1^{-1}(P_1) = F_1(P_1)$.

5.4 Intersection of two $\mathbb{Z}$-polyhedra

This algorithm provides the intersection of 2 $\mathbb{Z}$-polyhedra (with underlying linear lattices). As suggested in proposition 6, we intersect the lattices (the result is full dimensional or empty) and then we get the polyhedron. When dealing with affine lattices, one way to implement the intersection it to consider the constant part as an additional dimension which must be equal to one (homogeneous system [Wil93]). In that case, once the linear lattices are intersected, we must still solve another linear Diophantine equation which says that the constant part is equal to one.

`IntersectZpols(`$(F_1, P_1), (F_2, P_2)$`)`

`/* First we intersect the full dimensional lattices */`

`/* That is: we solve (in` $\mathbb{Z}^n$`) z=f1(x),z=f2(y) in z */`

`Let` HU `be the Hermite decomposition of` $M = \begin{pmatrix} Id_n & -F_1 & 0 \\ Id_n & 0 & -F_2 \end{pmatrix}$

`/* The` n `last columns of` H `are null */`

`/* they correspond to free variable of the solution of`

`If` $\begin{pmatrix} z \\ x \\ y \end{pmatrix} = U^{-1} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix}$ `then`

$$M \begin{pmatrix} z \\ x \\ y \end{pmatrix} = H \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} = 0 \Leftrightarrow t_1 = t_2 = 0$$

`Let` U_2 `be the upper right` $n \times n$ `sub-matrix of` U^{-1}`, if` $t_1 = t_2 = 0$ `then` $z = U_2(t_3)$

`thus the lattice of the intersection is given by` $\{x \mid \exists z \quad x = U_2 z\}$`*/`

`Let` $F_3 = U_2$

`/* Now, compute the polyhedron */`

`Let` $P_3 = F_3^{-1}(F_1(P_1) \cap F_2(P_2))$

`return(`F_3, P_3`)`

5.5 Image and preimage by an invertible function

This procedure provides the image of a $\mathbb{Z}$-polyhedron by a rational invertible function. It can also be used to compute the preimage of a $\mathbb{Z}$-polyhedron by a rational invertible function.

`ZpolImage(`$(F_1, P_1), G$`)`

`If` GF_1 `integral return(`(GF_1, P_1)`)`

`Else`

`Let` $\Delta = UGF_1V$ `be the Smith normal form of` GF_1`.`

`Let` Δ' `be the diagonal matrix composed of the denominators of` Δ

`Let` $F_2 = U^{-1}\Delta\Delta'$

`Let` $P_2 = \Delta'^{-1}V^{-1}(P_1)$

`return(`(F_2, P_2)`)`

```
  EndIf
```

5.6 Preimage by a function

This algorithm explain how to compute the preimage of a $\mathbb{Z}$-polyhedron by a rational linear mapping. To the treatment of section 5.5, we must add the intersection of the $\mathbb{Z}$-polyhedron by the space image of the function (which is not necessarily the whole space), and the extension of the result by the kernel of the function (which is not necessarily limited to 0). This procedure works with linear transformation, it is easy to extend it to affine transformations.

ZpolPreimage((F_1, P_1),G)
      /* we suppose $G : \mathbb{Q}^l \to \mathbb{Q}^n$ and we note l_1 the rank of G */
  If G nonsingular return ZpolImage($(F_1, P_1), G^{-1}$)
  Else
      Let C=FindHermiteBasis($Ker(G)$)
      Let $D = (c_{l-l_1+1}, \ldots, c_l, c_1, \ldots, c_{l-l_1})$ /* reorder the vectors of C */
      Let B=FindHermiteBasis($G(\mathbb{Z}^l)$)
      Let $G_2 = B^{-1}GD = \begin{pmatrix} G_{21} & 0 \\ 0 & 0 \end{pmatrix}$ /* G_{21} is $l_1 \times l_1$ invertible */
      Let $G_3 = \begin{pmatrix} G_{21} & 0 \\ 0 & Id_{n-l_1} \end{pmatrix}$ /* G_3 is a non singular function of $\mathbb{Q}^n$ */
      let (F_2, P_2)=IntersectZpols($(B^{-1}F_1, (P_1)), (G_3, \mathbb{Z}^{l_1})$)
      Let (F_3, P_3)=ZpolImage((F_2, P_2),G_3^{-1})
          /* (F_3, P_3) is a $\mathbb{Z}$-polyhedron of $\mathbb{Z}^n$ which is included in the first
          l1 coordinate */
      Let (F_4, P_4, B_4)= zpolNormalForm((F_3, P_3))
          /* B_4 is of shape $\begin{pmatrix} B_{41} & B_{42} \\ 0 & B_{43} \end{pmatrix}$ */
      Let P_5=DomExtend(DomProject(P_4,$l1$),l)
          /* complete the preimage by the kernel of G */
      Let $F_5 = \begin{pmatrix} Fbis_{41} & 0 \\ 0 & Id_{l-l1} \end{pmatrix}$ where $Fbis_{41} = B_{41}F_{41}$
          /* this description is expressed in basis D */
      return((DF_5D^{-1}, DP_5))
  Endif

5.7 Union of $\mathbb{Z}$-polyhedra

In general, the union of two $\mathbb{Z}$-polyhedra (F_1, P_1) and (F_2, P_2) will treated as such ($(F_1, P_1) \cup (F_2, P_2)$). However, there are some special cases that can be detected:

- If one of them is included in the other: $P_1 \subset P_2$ and $F_2^{-1}F_1$ integral, return((F_2, P_2))

- If the lattice are the same: $F_1 = F_2$, return$((F_1, P_1 \cup P_2))$.

6 Conclusion

We have presented theoretical background for implementing a computational kernel on $\mathbb{Z}$-polyhedra. We have proved that the class of $\mathbb{Z}$-polyhedra is stable by intersection, preimage by a linear rational function and image by a linear invertible rational function. The compatibility rules between function composition and $\mathbb{Z}$-polyhedra operations is not as simple as for the classical notion of image and preimage but we can easily express the preimage of the preimage in terms of the preimage of the composition. Moreover, we know exactly, for every $\mathbb{Z}$-polyhedron Z_1 the condition that the invertible rational function f must satisfy so that the number of points in $f(Z_1)$ (resp. $f^{-1}(Z_1)$) is conserved. We will say that f is *pseudo-unimodular* with respect to Z_1. This is sufficient to provide a computational kernel on $\mathbb{Z}$-polyhedra.

We have provided algorithms for all the operations needed. these algorithms have been implemented in an α-version of the $\mathbb{Z}$-polyhedra library based on the polyhedral library and written in Mathematica. This first implementation confirmed, first the necessity of a canonic form for performing any kind of manipulation on $\mathbb{Z}$-polyhedra and second, that the additional complexity was not a very important. Extending the results of section 4 for dealing with union of $\mathbb{Z}$-polyhedra is straightforward. In order to implement a complete library working on $\mathbb{Z}$-polyhedra, there remains two problems.

- The computation of the canonic form uses the integer hull of a polyhedron. This is a very difficult operation which is currently not available in the polyhedral library. However, if the polyhedra tackled have small dimension (less than five, as it is often the case in Alpha), this problem is not completely intractable [Wür93, Har88].
- when dealing with union of $\mathbb{Z}$-polyhedra it is almost impossible to have a canonic form (indeed, a $\mathbb{Z}$-polyhedron can be written as union of $\mathbb{Z}$-polyhedra in many ways).

These problems where also present when dealing with polyhedra and they where not solved in the implementation provided in the polyhedral library. However, practical experiences from different sites proved that these cases occurred very rarely in the applications tested.

The main contribution of this work is the definition of a canonic form for a $\mathbb{Z}$-polyhedron. This canonic form allows us to perform crucial operations (equality test, intersection, etc ...) on $\mathbb{Z}$-polyhedra. Another new feature is the ability to take into account rational mappings when manipulating $\mathbb{Z}$-polyhedra (only integral mapping where usually allowed when dealing with polyhedra).

This work is a step towards the manipulation of image of polyhedra by arbitrary linear function (LBL in [TT93]). $\mathbb{Z}$-polyhedra will not be able to model all the sets met in the manipulation of loop iteration domains but it will really simplify the expression of an important subset.

References

[Anc91] C. Ancourt. *Génération automatique de codes de transfert pour multiprocesseurs à mémoires locales.* PhD thesis, Université de Paris VI, 1991.

[Bal95] F. Balasa. *Background Memory Allocation for Multi-Dimensional Signal Processing.* PhD thesis, Katholieke Universiteit Leuven, 1995.

[Che68] N.V. Chernikova. Algorithm for discovering the set of all the solution of a linear programming problem. *U.S.S.R Computational Mathematics and Mathematical Physics*, 8(6):282–293, 1968.

[Fea92] P. Feautrier. Some efficient solutions to the affine scheduling problem, part I, one dimensional time. *Int. J. of Parallel Programming*, 21(5):313–348, October 1992.

[FQ88] F. Fernández and P. Quinton. Extension of chernikova's algorithm for solving general mixed linear programming problems. Technical Report 437, IRISA - Rennes (France), 1988.

[Har88] M.E. Hartmann. *Cutting Planes and the Complexity of the Integer Hull.* PhD thesis, School Of Operations Research and Industrial Engineering, Cornell University, 1988.

[Hel94] P.C. Held. Hipars: a tool for automatic conversion of nested loop programs into single assignment programs. Technical Report Dept. Electrical Engineering, Delft University of Technology, 1994.

[LR96] P. Lenders and S. Rajopadhye. Multirate VLSI arrays and their synthesis. *IEEE Transactions on Computers*, (to appear) 1996.

[Mau89] C. Mauras. *Alpha : un langage équationnel pour la conception et la programmation d'architectures parallèles synchrones.* PhD thesis, Université de Rennes 1, IFSIC, December 1989.

[MRTT53] T.S. Motzkin, H. Raiffa, G.L. Thompson, and R.M. Thrall. The double description method. Theodore S. Motzkin: Selected Papers, 1953.

[NW88] G.L. Nemhauser and L.A. Wolsey. *Integer and Combinatorial Optimization.* Wiley-interscience, 1988.

[Pug92] William Pugh. The omega test: a fast and practical integer programming algorithm for depedence analysis. *Communications of the ACM*, 8:102–114, August 1992.

[QRR96] P. Quinton, S. V. Rajopadhye, and T. Risset. Extension of the ALPHA language to recurrences on sparse periodic domains. In *Int. Conf. on Application Specific Array Processors (To appear)*, 1996.

[Sch86] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley and Sons, New York, 1986.

[Tei93] J. Teich. *A compiler for Application-Specific Processor Arrays*. PhD thesis, Universität des Saarlandes, 1993.

[TT93] J. Teich and L. Thiele. Partitioning of processor arrays: A piecewise regular approach. *INTEGRATION: The VLSI Journal*, 14(3):297–332, Feb 1993.

[Ver92] H. Le Verge. A note on Chernikova's algorithm. RR 635, IRISA, IRISA, Campus de Beaulieu, 35042 Rennes Cedex, France, Feb 1992.

[Ver94] H. Le Verge. Computations on linearly bounded lattices. Personal communication, 1994.

[Wil93] D. Wilde. A library for doing polyhedral operations. Technical Report Internal Publication 785, IRISA, Rennes, France, Dec 1993. Also published as INRIA Research Report 2157.

[WS94] D. Wilde and O. Sie. Regular array synthesis using ALPHA. Technical Report Internal Publication 829, IRISA, Rennes, France, May 1994.

[Wür93] F. Würtz. Bestimmung der ganzzahligen Hülle eines rationalen Polyeders. Studienarbeit, Universität des Saarlandes, November 1993.