Cutting Planes and the Elementary Closure in Fixed Dimension

Alexander Bockmayr
Friedrich Eisenbrand

MPI–I–99–2-008 December 1999

Authors' Addresses

Alexander Bockmayr
Université Henri Poincaré, LORIA
Campus scientifique, B.P. 239
F-54506 Vandœuvre-lès-Nancy, France
bockmayr@loria.fr

Friedrich Eisenbrand
Max-Planck-Institut für Informatik
Im Stadtwald
D-66123 Saarbrücken, Germany
eisen@mpi-sb.mpg.de

Abstract

The elementary closure P' of a polyhedron P is the intersection of P with all its Gomory-Chvátal cutting planes. P' is a rational polyhedron provided that P is rational. The known bounds for the number of inequalities defining P' are exponential, even in fixed dimension. We show that the number of inequalities needed to describe the elementary closure of a rational polyhedron is polynomially bounded in fixed dimension. If P is a simplicial cone, we construct a polytope Q, whose integral elements correspond to cutting planes of P. The vertices of the integer hull Q_I include the facets of P'. A polynomial upper bound on their number can be obtained by applying a result of Cook et al. Finally, we present a polynomial algorithm in varying dimension, which computes cutting planes for a simplicial cone that correspond to vertices of Q_I.

1 Introduction

Integer programming is concerned with the optimization problem

$$\max\{c^T x \mid Ax \leq b,\, x \in \mathbb{Z}^n\}, \text{ where } A \in \mathbb{Z}^{m\times n} \text{ and } b \in \mathbb{Z}^m.$$

It is well-known that integer programming is NP-hard. However, the situation is different if the number of variables, here n, is fixed. Lenstra (1983) showed that integer programming in fixed dimension is solvable in polynomial time. Lenstra's algorithm relies on results from the geometry of numbers like Khintchine's *flatness theorem*, *lattice basis reduction*, and the *ellipsoid method*. Lovász & Scarf (1992) found a way to avoid the ellipsoid method. However, present algorithms for integer programming in fixed dimension are still far from being elementary.

The *cutting plane method* pioneered by Gomory (1958) computes iteratively tighter approximations of the integer hull P_I of a polyhedron P, until P_I is finally obtained. We shortly describe the method. An inequality $c^T x \leq \lfloor \delta \rfloor$, with $c \in \mathbb{Z}^n$ and $\delta = \max\{c^T x \mid x \in P\}$, is called a Gomory-Chvátal *cutting plane*. The set of vectors P' satisfying all cutting planes for P is called the *elementary closure* of P. Let $P^{(0)} = P$ and $P^{(i+1)} = (P^{(i)})'$, for $i \geq 0$. Chvátal (1973) showed that every polytope P satisfies $P^{(t)} = P_I$ for some $t \in \mathbb{N}_0$. Schrijver (1980) extended this result to rational polyhedra. The number of iterations t until $P^{(t)} = P_I$ is not polynomial in the size of the description of P, even in fixed dimension (Chvátal 1973). Yet, if $P_I = \emptyset$ and $P \subseteq \mathbb{R}^n$, Cook, Coullard & Turán (1987) showed that there exists a number $t(n)$, such that $P^{(t(n))} = \emptyset$. Cook (1990) proved the existence of cutting plane proofs for integer infeasibility that can be carried out in polynomial space. These results raise the question whether it is possible to come up with a polynomial cutting plane algorithm for integer infeasibility in fixed dimension. Using binary search this would also yield a polynomial cutting plane algorithm for integer programming in fixed dimension.

In this context we are motivated to investigate the complexity of the elementary closure in fixed dimension. More precisely, we will study the question whether, in fixed dimension, the elementary closure P' of a polyhedron $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$, with A and b integer, can be defined by an inequality system whose size is polynomial in the size of A and b.

It is well-known that the elementary closure P' can be defined by cutting planes of the form $\lambda^T Ax \leq \lfloor \lambda^T b \rfloor$, where $\lambda \in [0,1)^m$ (see e.g. (Cook, Cunningham, Pulleyblank & Schrijver 1998, Lemma 6.34)). This leads to the insight that P' is a rational polyhedron again, if P is rational. Carathéodory's theorem implies that the vectors λ can be further restricted such that at most $\mathrm{rank}(A)$ many components of λ are strictly positive.

Proposition 1. *Let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}, A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$, be a rational polyhedron. The elementary closure P' is the polyhedron defined by $Ax \leq b$ and the set of all inequalities $\lambda^T Ax \leq \lfloor \lambda^T b \rfloor$, where λ has at most $\mathrm{rank}(A)$ positive components, $\lambda \in [0,1)^m$ and $\lambda^T A \in \mathbb{Z}^n$.*

It follows that P' can be described by at most $(\|A^T\|_\infty)^n$ many inequalities, since this is a straightforward upper bound on the number of integer vectors of the form $\lambda^T A$, $\lambda \in [0,1]^m$. This upper bound is exponential in the encoding length of A, even in fixed dimension. One can further restrict the cutting planes $c^T x \leq \lfloor \delta \rfloor$ to those corresponding to a *totally dual integral* (TDI) system defining P (Edmonds & Giles 1977, Giles & Pulleyblank 1979, Schrijver 1980). The number of inequalities of a minimal TDI-system for a polyhedron P can still be exponential in the size of P, even in fixed dimension (Schrijver 1986, p. 317).

The contributions of this paper are twofold. In the first part, we prove that in fixed dimension the number of inequalities needed to describe P' is polynomial in the encoding length of P. Based on this result, we develop in the second part a polynomial algorithm in varying dimension for computing Gomory-Chvátal cutting planes of simplicial cones. Our approach uses techniques from integer linear algebra like the Hermite and the Howell normal form of matrices. While the Hermite normal form has been applied to cut generation before (see e.g. (Hung & Rom 1990, Letchford 1999)), the cutting planes that we derive here are not only among those of maximal possible violation in a natural sense, but also belong to the polynomial description of P' developed in the first part of our paper. Caprara, Fischetti & Letchford (1999) apply Gaussian elimination to find mod k-cuts, for k prime, which are violated by $(k-1)/k$. We present a framework that captures all Gomory-Chvátal cuts in an algebraic structure, namely the kernel of a matrix and one solution of an inhomogeneous system of linear equalities over some residue ring $\mathbb{Z}_d$, where d is not necessarily prime. This structure comfortably allows for local search techniques to improve on various criteria for the quality of cuts, like the Euclidean distance, norm or sparsity.

2 Notation and definitions

A *polyhedron* P is a set of vectors of the form $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$, for some matrix $A \in \mathbb{R}^{m \times n}$ and some vector $b \in \mathbb{R}^m$. We write $P = P(A, b)$. The polyhedron is *rational* if both A and b can be chosen to be rational. If P is bounded, then P is called a *polytope*. The *integer hull* P_I of a polytope P is the convex hull of the integral vectors in P. If P is rational, then P_I is a rational polyhedron again. The *dimension* of P is the dimension of the affine hull of P. An inequality $c^T x \leq \delta$ defines a *face* $F = \{x \in P \mid c^T x = \delta\}$ of P, if $\delta \geq \max\{c^T x \mid x \in P\}$. F is called a *facet* of P, if $\dim(F) = \dim(P) - 1$. If $F \neq \emptyset$ and $\dim(F) = 0$, then F is called a *vertex* of P. If P is full-dimensional, then P has a unique (up to scalar multiplication) minimal set of inequalities defining P. They correspond to the facets of P. We refer to (Nemhauser & Wolsey 1988) and (Schrijver 1986) for further basics of polyhedral theory.

The *size* of an integer z is the number

$$\text{size}(z) = \begin{cases} 1 & \text{if } z = 0 \\ 1 + \lfloor \log_2(|z|) \rfloor & \text{if } z \neq 0 \end{cases}$$

Likewise, the size of a matrix $A \in \mathbb{Z}^{m \times n}$, $\text{size}(A)$ is the number of bits needed to encode A, i.e., $\text{size}(A) = mn + \sum_{i,j} \text{size}(a_{i,j})$, (see (Schrijver 1986, p. 29)). If P is given as $P(A, b)$, then we denote $\text{size}(A) + \text{size}(b)$ by $\text{size}(P)$.

A *lattice* $\mathcal{L} \subseteq \mathbb{R}^n$ is a subgroup of $\mathbb{R}^n$ of the form $\{Ax \mid x \in \mathbb{Z}^n\}$, where A is a nonsingular square matrix. We write $\mathcal{L} = \mathcal{L}(A)$. The *dual lattice* $\mathcal{L}^*(A)$ of $\mathcal{L}(A)$ is the lattice $\mathcal{L}^*(A) = \{x \in \mathbb{R}^n \mid x^T y \in \mathbb{Z}, \forall y \in \mathcal{L}(A)\}$. One has $\mathcal{L}^*(A) = \mathcal{L}((A^{-1})^T)$ (see e.g. (Schrijver 1986, p. 50)).

If P is a rational polyhedron, then the number of extreme points of P_I can be polynomially bounded by size(P) in fixed dimension. This follows from a generalization of a result by Hayes & Larman (1983), see (Schrijver 1986, p. 256). The following upper bound on the number of vertices of P_I was proved by Cook, Hartmann, Kannan & McDiarmid (1992). Bárány, Howe & Lovász (1992) show that this bound is tight.

Theorem 2. *If $P \subseteq \mathbb{R}^n$ is a rational polyhedron which is the solution set of a system of at most m linear inequalities whose size is at most φ, then the number of vertices of P_I is at most $2m^d(6n^2\varphi)^{d-1}$, where $d = \dim(P_I)$ is the dimension of the integer hull of P.*

Last we recall some basic number theory (see e.g. (Niven, Zuckerman & Montgomery 1991)). $\mathbb{Z}_d$ denotes the *ring of residues* modulo d, i.e., the set $\{0, \dots, d-1\}$ with addition and multiplication modulo d. We will often identify an element of $\mathbb{Z}_d$ with the natural number in $\{0, \dots, d-1\}$ to which it corresponds. $\mathbb{Z}_d$ is a commutative ring but not a field if d is not a prime. However $\mathbb{Z}_d$ is a *principal ideal ring*, i.e., each ideal is of the form $\langle g \rangle = \{gx \mid x \in \mathbb{Z}_d\} \lhd \mathbb{Z}_d$. Since $\langle d \rangle = \langle eg \rangle$ for each unit $e \in \mathbb{Z}_d^*$ and since $g/\gcd(d,g)$ is a unit of $\mathbb{Z}_d$, it follows that $\langle g \rangle = \langle \gcd(d,g) \rangle$. Therefore we can assume that g divides d, $g \mid d$. Thus each ideal of $\mathbb{Z}_d$ has a unique generator dividing d, call it the *standard generator*. The standard generator g of an ideal $\langle a_1, \dots, a_k \rangle \lhd \mathbb{Z}_d$ is easily computed with the Euclidean algorithm.

3 The elementary closure of a rational simplicial cone

Consider a *rational simplicial cone*, i.e., a polyhedron $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$, where $A \in \mathbb{Z}^{n \times n}$, $b \in \mathbb{Z}^n$ and A has full rank. Observe that P, P' and P_I are all full-dimensional. The elementary closure P' is given by the inequalities

$$(\lambda^T A)x \leq \lfloor \lambda^T b \rfloor, \text{ where } \lambda \in [0,1]^n, \text{ and } \lambda^T A \in \mathbb{Z}^n. \tag{1}$$

Since P' is full-dimensional, there exists a unique (up to scalar multiplication) minimal subset of the inequalities in (1) that suffices to describe P'. These inequalities are the facets of P'. We will come up with a polynomial upper bound on their number in fixed dimension.

The vectors λ in (1) belong the dual lattice $\mathcal{L}^*(A)$ of $\mathcal{L}(A)$. Recall that each element in $\mathcal{L}^*(A)$ is of the form μ/d, where $d = \det(\mathcal{L}(A)) = |\det(A)|$ is the absolute value of the determinant of A. It follows from the Hadamard inequality that size(d) is polynomial in size(A), even for varying n. Now (1) can be rewritten as

$$\frac{\mu^T A}{d}\, x \leq \left\lfloor \frac{\mu^T b}{d} \right\rfloor, \text{ where } \mu \in \{0, \dots, d\}^n, \text{ and } \mu^T A \in (d \cdot \mathbb{Z})^n. \tag{2}$$

Notice here that $\mu^T b/d$ is a rational number with denominator d. There are two cases: either $\mu^T b/d$ is an integer, or $\mu^T b/d$ misses the nearest integer by at least $1/d$. Therefore $\lfloor \mu^T b/d \rfloor$ is the only integer in the interval

$$\left[\frac{\mu^T b - d + 1}{d}, \frac{\mu^T b}{d}\right].$$

These observations enable us to construct a polytope Q, whose integral points will correspond to the inequalities (2). Let Q be the set of all (μ, y, z) in $\mathbb{R}^{2n+1}$ satisfying the inequalities

$$\begin{array}{rcl} \mu & \geq & 0 \\ \mu & \leq & d \\ \mu^T A & = & d\, y \\ (\mu^T b) - d + 1 & \leq & d\, z \\ (\mu^T b) & \geq & d\, z. \end{array} \tag{3}$$

If (μ, y, z) is integral, then $\mu \in \{0, \dots, d\}^n$, $y \in \mathbb{Z}^n$ enforces $\mu^T A \in (d \cdot \mathbb{Z})^n$ and z is the only integer in the interval $[(\mu^T b + 1 - d)/d,\, \mu^T b/d]$. It is not hard to see that (3) defines indeed a polytope.

The correspondence between inequalities (their syntactic representation) in (2) and integral points in Q is obvious. The facets of P' are among the vertices of Q_I.

Proposition 3. *Each facet of P' is represented by an integral vertex of Q_I.*

Proof. Consider a facet $c^T x \leq \delta$ of P'. If we remove this inequality (possibly several times, because of scalar multiples) from the set of inequalities in (2), then the polyhedron defined by the resulting set of inequalities differs from P', since P' is full-dimensional. Thus there exists a point $\hat{x} \in \mathbb{Q}^n$ that is violated by $c^T x \leq \delta$, but satisfies any other inequality in (2). Consider the following integer program:

$$\max\{(\mu^T A/d)\, \hat{x} - z \mid (\mu, y, z) \in Q_I\}. \tag{4}$$

Since $\hat{x} \notin P'$ there exists an inequality $(\mu^T A/d)x \leq \lfloor \mu^T b/d \rfloor$ in (2) with

$$(\mu^T A/d)\hat{x} - \lfloor \mu^T b/d \rfloor > 0.$$

Therefore, the optimal value will be strictly positive, and an integral optimal solution (μ, y, z) must correspond to the facet $c^T x \leq \delta$ of P'. Since the optimum of the integer linear program (4) is attained at a vertex of Q_I, the assertion follows. $\square$

Remark 4. Not each vertex of Q_I represents a facet of P'. In particular, if P is defined by nonnegative inequalities only, then $\mathbf{0}$ is a vertex of Q_I but not a facet of P'.

Theorem 5. *The elementary closure of a rational simplicial cone $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$, where A and b are integral, is polynomially bounded in* $\text{size}(P)$ *when the dimension is fixed.*

Proof. Each facet of P' corresponds to a vertex of Q_I by Proposition 3. Recall from the Hadamard bound (see e.g. (Schrijver 1986, p. 7)) that $d \leq \|a_1\| \cdots \|a_n\|$, where a_i are the columns of A. Thus the number of bits needed to encode d is in $\mathrm{O}(n \,\text{size}(P))$. Therefore the size of Q is in $\mathrm{O}(n \,\text{size}(P))$. It follows from Theorem 2 that the number of vertices of Q_I is in $\mathrm{O}(\text{size}(P)^n)$ for fixed n, since the dimension of Q is $n+1$. $\square$

It is possible to explicitly construct in polynomial time a minimal inequality system defining P' when the dimension is fixed. As noted in (Cook et al. 1992), one can construct the vertices of Q_I in polynomial time. This works as follows. Suppose one has a list of vertices $v_1, \ldots, v_k$ of Q_I. Let Q_k denote the convex hull of these vertices. Find an inequality description of Q_k, $Cx \leq d$. For each row-vector c_i of C, find with Lenstra's algorithm a vertex of Q_I maximizing $\{c^T x \mid x \in Q_I\}$. If new vertices are found, add them to the list and repeat the preceding steps, otherwise the list of vertices is complete. The list of vertices of Q_I yields a list of inequalities defining P'. With the ellipsoid method or your favorite linear programming algorithm in fixed dimension, one can decide for each individual inequality, whether it it is necessary. If not, remove it. What remains are the facets of P'.

4 The elementary closure of rational polyhedra

Let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$, with integral A and b, be a rational polyhedron. If A does not have full column rank, then there exists a unimodular matrix U transforming A from the right into a matrix with only $\text{rank}(A)$ many nonzero columns. Since unimodular transformations applied to A from the right and the elementary closure operation are compliant (see e.g. (Schrijver 1986, p. 341)), we can assume that A has full column rank. Such a unimodular matrix U can be found in polynomial time. Simply choose $\text{rank}(A)$ linearly independent rows $\hat{A}$ of A with Gaussian elimination and compute U transforming $\hat{A}$ into its *Hermite normal form* (Schrijver 1986, p. 45). Recall that the Hermite normal form of an integral matrix $A \in \mathbb{Z}^{m \times n}$ with full row rank is a nonnegative, nonsingular lower triangular matrix H, such that there exists a unimodular matrix U with $(H \mid 0) = AU$, where each row of H has a unique maximal entry, located at the diagonal $h_{i,i}$. Polynomial algorithms for computing the Hermite normal form have been given by Kannan & Bachem (1979), Hafner & McCurley (1991), and Storjohann & Labahn (1996), among others.

It follows from Proposition 1 that any Gomory-Chvátal cut can be derived from a set of n inequalities out of $Ax \leq b$ where the corresponding rows of A are linear independent. Such a choice represents a simplicial cone C and it follows from Theorem 5 that the number of inequalities of C' is polynomially bounded by $\text{size}(C) \leq \text{size}(P)$.

Theorem 6. *The number of inequalities needed to describe the elementary closure of a rational polyhedron $P = P(A, b)$ with $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$, is polynomial in* size(P) *in fixed dimension.*

Proof. As we observed, we can assume that A has full column rank. An upper bound on the number of inequalities that are necessary to describe P' follows from the sum of the upper bounds on the number of facets of C' where C is a simplicial cone, formed by n inequalities of $Ax \leq b$. There are at most $\binom{m}{n} \leq m^n$ ways to choose n linear independent rows of A. Thus the number of necessary inequalities describing P' is $\mathrm{O}(m^n \mathrm{size}(P)^n)$ for fixed n. □

Following the discussion at the end of Section 3 and using again Lenstra's algorithm, it is now easy to come up with a polynomial algorithm for constructing the elementary closure of a rational polyhedron $P(A, b)$ in fixed dimension. As we observed, we can assume that A has full column rank. For each choice of n rows of A defining a simplicial cone C, compute the elementary closure C' and put the corresponding inequalities in the partial list of inequalities describing P'. At the end, redundant inequalities can be deleted.

5 Finding cuts for simplicial cones

In Section 3 we saw that the vertices of Q_I include the facets of the elementary closure P' of a simplicial cone $P(A, b)$. In practice the following situation often occurs. One wants to find a cutting plane that cuts of the extreme point of P, $\hat{x} = A^{-1}b$. It is easy to see that the scenario of Gomory's corner polyhedron (Gomory 1967) (see also (Schrijver 1986, p. 364)), is of this nature. In this section, we will show how to generate such cutting planes. Following Section 3, they will have the special property that they correspond to vertices of Q_I and thus belong to a family of inequalities which grows only polynomially in fixed dimension. While the separation problem for the elementary closure is NP-hard (Eisenbrand 1999) in general, these cutting planes can be computed in polynomial time in varying dimension.

Let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ again be a rational simplicial cone, where $A \in \mathbb{Z}^{n \times n}$ and $b \in \mathbb{Z}^n$. Let $d = |\det(A)|$ denote the absolute value of the determinant of A. Let Q be defined by the inequalities in (3). We will find a face-defining inequality of Q_I that represents the cutting planes with a maximal rounding effect. This relates to the study of maximally violated mod k-cuts by Caprara et al. (1999). A cutting plane

$$(\mu/d)^T Ax \leq \lfloor (\mu/d)^T b \rfloor$$

can be found by solving the following linear system over $\mathbb{Z}_d$.

$$\mu^T (A \mid b) = (0, \ldots, 0, \nu), \tag{5}$$

where ν/d for $\nu \in \{0, \ldots, d-1\}$ is the desired value for the rounding effect $(\mu^T b)/d - \lfloor (\mu^T b)/d \rfloor$. If P is a simplicial cone, then this rounding effect is the *amount of violation* of the cutting plane by the extreme point $\hat{x}$ of P. Caprara et al. (1999) fix ν in the system (5) to the maximal possible value $d-1$. However, there does not have to exist a solution to (5) when ν is set to $d-1$. We show here that the maximal ν, denote it by $\nu_{\max}$, for which a solution to (5) exists, can be computed efficiently.

For this we have to reach a little deeper into the linear algebra tool-box. In the following we will make extensive use of the Hermite and Howell normal form of an integer matrix. The Hermite normal form belongs to the standard tools in integer programming. Hung & Rom (1990) for example use a variant of the Hermite normal form to generate cutting planes of simplicial cones P, such that the outcome $\tilde{P}$ has in integral vertex. Letchford (1999) uses the Hermite normal form to cut off the minimal face of a cone $P(A, b)$ where A has full row rank. We use the Hermite normal form because it allows us to represent the image and kernel of matrices $A \in \mathbb{Z}_d^{m\times n}$ in a convenient way. Notice that $\mathbb{Z}_d$ is not a field if d is not a prime. Therefore, standard Gaussian elimination does not apply for these tasks in general.

5.1 The Howell and Hermite normal form

Let us study the column-span of a matrix $B \in \mathbb{Z}_d^{m\times n}$

$$\operatorname{span}(B) = \{x \in \mathbb{Z}_d^m \mid \exists y \in \mathbb{Z}_d^n,\, By = x\}.$$

The column-span of an integral matrix $B \in \mathbb{Z}^{m\times n}$ is defined accordingly. We write $\operatorname{span}_{\mathbb{Z}_d}(B)$ and $\operatorname{span}_{\mathbb{Z}}(B)$ to distinguish if necessary. The span of an empty set of vectors is the submodule $\{\mathbf{0}\}$ of $\mathbb{Z}_d^m$.

Consider the set of vectors $S(i) \subseteq \operatorname{span}(B)$, $i = 0, \dots, m$, whose first i components are 0. Clearly $S(i)$ is a $\mathbb{Z}_d$-submodule of $\operatorname{span}(B)$. We say that a nonzero matrix B is in *canonical form* if

i. B has no zero column, i.e., a column containing zeroes only,

ii. B is in *column-echelon form*, i.e., if the first occurrence of a nonzero entry in column j is in row i_j, then $i_j < i_{j'}$, whenever $j < j'$ (the columns form a staircase “downwards”),

iii. $S(i)$ is generated by the columns of B belonging to $S(i)$.

We shortly motivate this concept. If $B \in \mathbb{Z}_d^{m\times n}$ is in canonical form and $y \in \mathbb{Z}_d^m$ is given, then it is easy to decide whether $y \in \operatorname{span}_{\mathbb{Z}_d}(B)$. For this, let i be the number of leading zeroes of y. Clearly $y \in \operatorname{span}_{\mathbb{Z}_d}(B)$ if and only if $y \in S(i)$. Conditions ii) and iii) imply that if $y \in S(i)$, then there exists a unique column b of B with exactly i leading zeroes and

$$b_{i+1} \cdot x = y_{i+1} \tag{6}$$

being a solvable equation in $\mathbb{Z}_d$. It is an elementary number theory task to decide, whether such an x exists and if so to find one (see e.g. (Niven et al. 1991,

p. 62)). Now subtract $x\, b_{i+1}$ times column b from y. The result is in $S(i+1)$. One proceeds until the outcome is in $S(n)$, which implies that $y \in \operatorname{span}_{\mathbb{Z}_d}(B)$, or the conditions discussed above fail to hold, which implies that $y \notin \operatorname{span}_{\mathbb{Z}_d}(B)$.

Storjohann & Mulders (1998) show how to compute a canonical form of a matrix A with $\mathrm{O}(mn^{\omega-1})$ basic operations in $\mathbb{Z}_d$, where $\mathrm{O}(n^\omega)$ is the time required to multiply two $n \times n$ matrices. The number ω is less then or equal to 2.37 as found by Coppersmith & Winograd (1990). In the rest of this paper, we use the O-notation to count basic operations in $\mathbb{Z}_d$ like addition, multiplication, or (extended)-gcd computation of numbers in $\{0, \ldots, d-1\}$. The bit-complexity of a basic operation in $\mathbb{Z}_d$ is $\mathrm{O}(\operatorname{size}(d) \log \operatorname{size}(d) \log\log \operatorname{size}(d))$ as found by Schönhage & Strassen (1971) (see also (Aho, Hopcroft & Ullman 1974)). Recall that $\operatorname{size}(d) = \mathrm{O}(n \operatorname{size}(A))$.

Storjohann & Mulders (1998) give Howell (1986) credit for the first algorithm and the introduction of the canonical form and call it *Howell normal form*. However, there is a simple relation to the *Hermite normal form* already used in Section 4.

Proposition 7. *Let $A \in \mathbb{Z}_d^{m \times n}$ be a nonzero matrix and let H be the Hermite normal form of $(A \mid d \cdot I)$ where $(A \mid d \cdot I)$ is interpreted as an integer matrix. Then a canonical form of A is the matrix H' which is obtained from H by deleting the columns $h^{(i)}$ with $h_{i,i} = d$ (notice that $h_{i,i} \mid d$).*

Proof. Clearly, $\operatorname{span}_{\mathbb{Z}_d}(H') \subseteq \operatorname{span}_{\mathbb{Z}_d}(A)$ and H' is in column-echelon form. We need to verify iii). Let $u \in \operatorname{span}_{\mathbb{Z}_d}(A)$ with $u \in S(i)$, where i is maximal. Property iii) is guaranteed if $i = m$. If $i < m$, then $u_{i+1} \neq 0$. Interpreted over $\mathbb{Z}$, this means that $0 < u_{i+1} < d$. Clearly $u \in \operatorname{span}_{\mathbb{Z}}(H)$, and since $u_{i+1} \in h_{i+1,i+1} \cdot \mathbb{Z}$ (recall that H is a lower triangular matrix with nonzero diagonal elements and that u_{i+1} is the first nonzero entry of u), it follows that the column $h^{(i+1)}$ appears in H'. After subtracting $u_{i+1}/h_{i+1,i+1}$ times the column $h^{(i+1)}$ from u, the result will be in $S(i+1)$ and, by induction, the result will be in the span of the columns of H' belonging to $S(i+1)$. All together we see that u is in the span of the vectors of H' belonging to $S(i)$. $\square$

It is now easy to see that the canonical forms of a matrix A have a unique representative B that, using the notation of ii), satisfies the following additional conditions that we will assume for the rest of the paper:

iv. the elements of row i_j are reduced modulo $b_{i_j,j}$ (interpreted over the integers) and

v. the natural number $b_{i_j,j}$ divides d.

5.2 Determining the maximal amount of violation

We now apply the canonical form to determine the maximal amount of violation $\nu_{\max}/d$. Notice that $P \neq P_I$ if and only if there exists a $\nu \neq 0$ such that (5) has a solution. If $(A \mid b)^T$ consist in $\mathbb{Z}_d$ of zeroes only, then $P = P_I$. Otherwise let H be the canonical form of $(A \mid b)^T$, which can be found with $\mathrm{O}(n^\omega)$ basic operations in $\mathbb{Z}_d$ (Storjohann & Mulders 1998). Since $P \neq P_I$, the last column of H is of the form $(0,\dots,0,g)^T$, for some $g \neq 0$. The ideal $\langle g \rangle \triangleleft \mathbb{Z}_d$ generated by g is exactly the set of ν such that (5) is solvable for μ. Since $g \mid d$, the largest $\nu \in \{1,\dots,d-1\} \cap \langle g \rangle$ is

$$\nu_{\max} = d - g.$$

Thus we can compute $\nu_{\max}$ in $\mathrm{O}(n^\omega)$ basic operations in $\mathbb{Z}_d$ and the inequality

$$(b^T, \mathbf{0}^T, -1)(\mu, y, z) = b^T\mu - z \leq \nu_{\max} \tag{7}$$

will be valid for Q_I, defining a nonempty face of Q_I,

$$F = (Q_I \cap (b^T\mu - z = \nu_{\max})). \tag{8}$$

Theorem 8. *Let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ be a rational simplicial cone, where $A \in \mathbb{Z}^{n\times n}$ is of full rank, $b \in \mathbb{Z}^n$ and $d = |\det(A)|$. Then one can compute in $\mathrm{O}(n^\omega)$ basic operations of $\mathbb{Z}_d$ the maximal possible amount of violation $\nu_{\max}/d$. Here, $\nu_{\max}$ is the maximum number $\nu \in \{0,\dots,d-1\}$ for which there exists a cutting plane $(\mu/d)^T Ax \leq \lfloor(\mu^T b)/d\rfloor$ separating $A^{-1}b$ with $(\mu^T b)/d - \lfloor(\mu^T b)/d\rfloor = \nu/d$.*

5.3 Computing vertices of Q_I

We proceed by computing a vertex of F, which will also be a vertex of Q_I. First we find in $\mathrm{O}(n^\omega)$ basic operations of $\mathbb{Z}_d$, a solution $\hat\mu$ to

$$\mu^T(A \mid b) = (0,\dots,0,\nu_{\max}). \tag{9}$$

Let $K \in \mathbb{Z}_d^{n\times k}$ represent the kernel of $(A \mid b)^T$, i.e.,

$$\mathrm{span}_{\mathbb{Z}_d}(K) = \{x \in \mathbb{Z}_d^n \mid x^T(A \mid b) = (0,\dots,0)\}.$$

The canonical form of K again can be computed in time $\mathrm{O}(n^\omega)$ (Storjohann & Mulders 1998). The solution set of (9) is the set of vectors

$$\mathcal{S} = \{\hat\mu + \bar\mu \mid \bar\mu \in \mathrm{span}_{\mathbb{Z}_d}(K)\}. \tag{10}$$

Notice that $\mathcal{S}$ is the set of integral vectors in F. Vertices of Q_I will be obtained as minimal elements of $\mathcal{S}$ with respect to some ordering on $\mathcal{S}$. For $i = 1,\dots,n$ and a permutation σ of $\{1,\dots,n\}$, we define a quasi-ordering $\leq_\sigma^i$ on $\mathcal{S}$ by

$$\mu \leq_\sigma^i \tilde\mu \quad \text{iff} \quad (\mu_{\sigma(1)},\dots,\mu_{\sigma(i)}) \leq_{\text{lex}} (\tilde\mu_{\sigma(1)},\dots,\tilde\mu_{\sigma(i)}).$$

Here, $\leq_{lex}$ denotes the lexicographic ordering on $\{0,\dots,d-1\}^i$.

Proposition 9. *If $\mu \in \mathcal{S}$ is minimal with respect to $\leq_\sigma^n$, then (μ, y, z) is a vertex of Q_I, where y and z are determined by μ according to (3).*

Proof. Assume without loss of generality that $\sigma = \mathrm{id}$. Let $\mu \in \mathcal{S}$ be minimal with respect to $\leq_\sigma^n$ and suppose that $\mu = \sum_{j=1,\dots,l} \alpha_j \mu^{(j)}$ is a convex combination of vertices of Q_I, where each $\mu^{(j)} \neq \mu$ and $\alpha_j > 0$. Clearly, each $\mu^{(j)}$ is in $\mathcal{S}$. Therefore, there exists an index $i \in \{1,\dots,n\}$ such that $\mu_i \leq \mu_i^{(j)}$, for all $j \in \{1,\dots,l\}$, and $\mu_i < \mu_i^{(j)}$, for some $j \in \{1,\dots,l\}$. Since $\alpha_j \geq 0$ and $\sum_{i=1,\dots,l} \alpha_j = 1$, we have $\sum_{j=1,\dots,l} \alpha_j \mu_i^{(j)} > \mu_i$, a contradiction. □

We now show how to compute a minimal element $\mu \in \mathcal{S}$ with respect to $\leq_\sigma^n$. For simplicity we assume that $\sigma = \mathrm{id}$, but the algorithm works equally well for any other permutation. For $\mu \in \mathcal{S}$, we call $(\mu_1,\dots,\mu_i)$ the *i-prefix* of μ. We will construct a sequence $\mu^{(i)}, i = 0,\dots,n$, of elements of $\mathcal{S}$ with the property that the i-prefix of $\mu^{(i)}$ is minimal among all i-prefixes of elements in $\mathcal{S}$ with respect to the $\leq_{\mathrm{lex}}$ order. Since $\leq_{\mathrm{lex}}$ is a total order, the i-prefix of $\mu^{(i)}$ is unique and the i-prefix of $\mu^{(j)}$ is the i-prefix of $\mu^{(i)}$, for all $j \geq i$. In other words, the j-prefix of $\mu^{(j)}$ coincides with the i-prefix of $\mu^{(i)}$ except possibly in the last $(j-i)$ components.

Define $K(i) \subseteq \mathrm{span}_{\mathbb{Z}_d}(K)$ as the $\mathbb{Z}_d$-submodule of $\mathrm{span}_{\mathbb{Z}_d}(K)$ consisting of those elements having a zero in their first i components. For $j \geq i$, the vector $\mu^{(j)}$ is obtained from $\mu^{(i)}$ by adding an element of $K(i)$. Suppose that K is in canonical form and let $K^{(i)}$ be the submatrix of K consisting of those columns of K that lie in $K(i)$. Notice that $K^{(i)}$ is in canonical form, too, and that $\mathrm{span}_{\mathbb{Z}_d}(K^{(i)}) = K(i)$.

We initialize $\mu^{(0)}$ with an arbitrary element of $\mathcal{S}$. Suppose we have constructed $\mu^{(i)}$. By the preceding discussion, $\mu^{(i+1)}$ is of the form $\mu^{(i)} + \mu$, for some $\mu \in K(i)$. We have to take care of the $(i+1)$-st component. Let κ be the first column of $K^{(i)}$ and let g be the $(i+1)$-st component of κ. If $g = 0$, then $\mu^{(i)}$ is minimal with respect to $\leq^{i+1}$. Otherwise the smallest component that we can get in the $(i+1)$-st position is is the least positive remainder r of the division of $\mu_{i+1}^{(i)}$ by g (remember that $g \mid d$). We have $\mu_{i+1}^{(i)} = qg + r$ with an appropriate natural number q and some $r \in \{1,\dots,g-1\}$. Thus, by subtracting $q\kappa$ from $\mu^{(i)}$, we obtain a vector $\mu^{(i+1)}$ that is minimal with respect to $\leq^{i+1}$. Notice that the computation of $\mu^{(i+1)}$ from $\mu^{(i)}$ involves $\mathrm{O}(n)$ elementary operations in $\mathbb{Z}_d$. Repeating this construction n times we get the following theorem.

Theorem 10. *Let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ be a rational simplicial cone, where $A \in \mathbb{Z}^{n \times n}$ is of full rank, $b \in \mathbb{Z}^n$ and $d = |\det(A)|$. Then one can compute in $\mathrm{O}(n^\omega)$ basic operations of $\mathbb{Z}_d$ a vertex of Q_I corresponding to a cutting plane $(\mu/d)^T Ax \leq \lfloor (\mu/d)^T b \rfloor$ separating $A^{-1}b$ with maximal possible amount of violation $\nu_{\max}/d$.*

In practice one would want to generate several cutting planes for P. Here is a simple heuristic to move from one cutting plane corresponding to a vertex of Q_I to the next. If one has computed some $\mu \in \mathcal{S}$ then it can be easily checked, whether a component of μ can be individually decreased. This works as follows. Suppose we are interested in the i-th component μ_i. Compute the standard generator g of the ideal of the i-th components of $\mathrm{span}_{\mathbb{Z}_d}(K)$. Recall that $g \mid d$. Now μ_i can be individually decreased, if $g < \mu_i$. In this case we swap rows i and 1 of K and components i and 1 of μ and proceed as discussed in the previous paragraph. This "swapping" corresponds to another permutation. It results in a new order $\leq_\sigma$ and a new vertex of Q_I.

References

Aho, A., Hopcroft, J. & Ullman, J. (1974), *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading.

Bárány, I., Howe, R. & Lovász, L. (1992), 'On integer points in polyhedra: a lower bound', *Combinatorica* **12**(2), 135 – 142.

Caprara, A., Fischetti, M. & Letchford, A. N. (1999), 'On the separation of maximally violated mod-k cuts', *Mathematical Programming* . To appear. (Extended abstract: Integer Programming and Combinatorial Optimization, IPCO'99, Springer LNCS 1610. See also: `http://www.or.deis.unibo.it/abs96-97.html`).

Chvátal, V. (1973), 'Edmonds polytopes and a hierarchy of combinatorial problems', *Discrete Mathematics* **4**, 305 – 337.

Cook, W. (1990), 'Cutting-plane proofs in polynomial space', *Mathematical Programming* **47**, 11–18.

Cook, W., Coullard, C. R. & Turán, G. (1987), 'On the complexity of cutting plane proofs', *Discrete Applied Mathematics* **18**, 25 – 38.

Cook, W., Cunningham, W. H., Pulleyblank, W. R. & Schrijver, A. (1998), *Combinatorial Optimization*, John Wiley.

Cook, W., Hartmann, M., Kannan, R. & McDiarmid, C. (1992), 'On integer points in polyhedra', *Combinatorica* **12**(1), 27 –37.

Coppersmith, D. & Winograd, S. (1990), 'Matrix multiplication via arithmetic progressions.', *J. Symb. Comput.* **9**(3), 251–280.

Edmonds, J. & Giles, R. (1977), A min-max relation for submodular functions on graphs, *in* 'Stud. Integer Program.', Ann. Discrete Math. 1, pp. 185–204.

Eisenbrand, F. (1999), 'On the membership problem for the elementary closure of a polyhedron', *Combinatorica* **19**(2), 297–300.

Giles, F. R. & Pulleyblank, W. R. (1979), 'Total dual integrality and integer polyhedra', *Linear Algebra and its Applications* **25**, 191 – 196.

Gomory, R. E. (1958), 'Outline of an algorithm for integer solutions to linear programs', *Bull. AMS* **64**, 275 – 278.

Gomory, R. E. (1967), 'Faces of an integer polyhedron', *Proc. Nat. Acad. Sci.* **57**, 16 – 18.

Hafner, J. L. & McCurley, K. S. (1991), 'Asymptotically fast triangularization of matrices over rings', *SIAM J. Comput.* **20**(6), 1068–1083.

Hayes, A. C. & Larman, D. G. (1983), 'The vertices of the knapsack polytope', *Discrete Applied Mathematics* **6**, 135 – 138.

Howell, J. A. (1986), 'Spans in the module $(Z_m)^s$', *Linear and Multilinear Algebra* **19**, 67–77.

Hung, M. S. & Rom, W. O. (1990), 'An application of the Hermite normal form in integer programming', *Linear Algebra and its Applications* **140**, 163–179.

Kannan, R. & Bachem, A. (1979), 'Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix', *SIAM J. Comput.* **8**(4), 499–507.

Lenstra, H. W. (1983), 'Integer programming with a fixed number of variables', *Mathematics of Operations Research* **8**(4), 538 – 548.

Letchford, A. N. (1999), Totally tight rank-1 Chvátal-Gomory cuts. Manuscript, `http://www.lancs.ac.uk/staff/letchfoa/pubs.htm`.

Lovász, L. & Scarf, H. E. (1992), 'The generalized basis reduction algorithm', *Mathematics of Operations Research* **17**(3), 751 – 764.

Nemhauser, G. L. & Wolsey, L. A. (1988), *Integer and Combinatorial Optimization*, John Wiley.

Niven, I., Zuckerman, H. S. & Montgomery, H. L. (1991), *An Introduction to the Theory of Numbers, Fifth edition*, Wiley.

Schönhage, A. & Strassen, V. (1971), 'Schnelle Multiplikation grosser Zahlen. (Speedy multiplication of great numbers).', *Computing* **7**, 281–292.

Schrijver, A. (1980), 'On cutting planes', *Annals of Discrete Mathematics* **9**, 291 – 296.

Schrijver, A. (1986), *Theory of Linear and Integer Programming*, John Wiley.

Storjohann, A. & Labahn, G. (1996), Asymptotically fast computation of Hermite normal forms of integer matrices, *in* Y. N. Lakshman, ed., 'ISSAC 96', ACM Press, pp. 259–266.

Storjohann, A. & Mulders, T. (1998), Fast algorithms for linear algebra modulo N, *in* 'European Symposium on Algorithms, ESA'98', Vol. 1461 of *Lecture Notes in Computer Science*, Springer, pp. 139–150.

INFORMATIK

Below you find a list of the most recent technical reports of the Max-Planck-Institut für Informatik. They are available by anonymous ftp from `ftp.mpi-sb.mpg.de` under the directory `pub/papers/reports`. Most of the reports are also accessible via WWW using the URL `http://www.mpi-sb.mpg.de`. If you have any questions concerning ftp or WWW access, please contact `reports@mpi-sb.mpg.de`. Paper copies (which are not necessarily free of charge) can be ordered either by regular mail or by e-mail at the address below.

Max-Planck-Institut für Informatik
Library
attn. Anja Becker
Im Stadtwald
66123 Saarbrücken
GERMANY
e-mail: `library@mpi-sb.mpg.de`

MPI-I-2000-1-001	E. Althaus, O. Kohlbacher, H. Lenhof, P. Müller	A branch and cut algorithm for the optimal solution of the side-chain placement problem
MPI-I-1999-3-005	T.A. Henzinger, J. Raskin, P. Schobbens	Axioms for Real-Time Logics
MPI-I-1999-3-004	J. Raskin, P. Schobbens	Proving a conjecture of Andreka on temporal logic
MPI-I-1999-3-003	T.A. Henzinger, J. Raskin, P. Schobbens	Fully Decidable Logics, Automata and Classical Theories for Defining Regular Real-Time Languages
MPI-I-1999-3-002	J. Raskin, P. Schobbens	The Logic of Event Clocks
MPI-I-1999-3-001	S. Vorobyov	New Lower Bounds for the Expressiveness and the Higher-Order Matching Problem in the Simply Typed Lambda Calculus
MPI-I-1999-2-007	G. Delzanno, J. Raskin	Symbolic Representation of Upward-closed Sets
MPI-I-1999-2-006	A. Nonnengart	A Deductive Model Checking Approach for Hybrid Systems
MPI-I-1999-2-005	J. Wu	Symmetries in Logic Programs
MPI-I-1999-2-004	V. Cortier, H. Ganzinger, F. Jacquemard, M. Veanes	Decidable fragments of simultaneous rigid reachability
MPI-I-1999-2-003	U. Waldmann	Cancellative Superposition Decides the Theory of Divisible Torsion-Free Abelian Groups
MPI-I-1999-2-001	W. Charatonik	Automata on DAG Representations of Finite Trees
MPI-I-1999-1-007	C. Burnikel, K. Mehlhorn, M. Seel	A simple way to recognize a correct Voronoi diagram of line segments
MPI-I-1999-1-006	M. Nissen	Integration of Graph Iterators into LEDA
MPI-I-1999-1-005	J.F. Sibeyn	Ultimate Parallel List Ranking ?
MPI-I-1999-1-004	M. Nissen, K. Weihe	How generic language extensions enable "open-world" desing in Java
MPI-I-1999-1-003	P. Sanders, S. Egner, J. Korst	Fast Concurrent Access to Parallel Disks
MPI-I-1999-1-002	N.P. Boghossian, O. Kohlbacher, H.-. Lenhof	BALL: Biochemical Algorithms Library
MPI-I-1999-1-001	A. Crauser, P. Ferragina	A Theoretical and Experimental Study on the Construction of Suffix Arrays in External Memory
MPI-I-98-2-018	F. Eisenbrand	A Note on the Membership Problem for the First Elementary Closure of a Polyhedron
MPI-I-98-2-017	M. Tzakova, P. Blackburn	Hybridizing Concept Languages
MPI-I-98-2-014	Y. Gurevich, M. Veanes	Partisan Corroboration, and Shifted Pairing
MPI-I-98-2-013	H. Ganzinger, F. Jacquemard, M. Veanes	Rigid Reachability
MPI-I-98-2-012	G. Delzanno, A. Podelski	Model Checking Infinite-state Systems in CLP

MPI-I-98-2-011	A. Degtyarev, A. Voronkov	Equality Reasoning in Sequent-Based Calculi
MPI-I-98-2-010	S. Ramangalahy	Strategies for Conformance Testing
MPI-I-98-2-009	S. Vorobyov	The Undecidability of the First-Order Theories of One Step Rewriting in Linear Canonical Systems
MPI-I-98-2-008	S. Vorobyov	AE-Equational theory of context unification is Co-RE-Hard
MPI-I-98-2-007	S. Vorobyov	The Most Nonelementary Theory (A Direct Lower Bound Proof)
MPI-I-98-2-006	P. Blackburn, M. Tzakova	Hybrid Languages and Temporal Logic
MPI-I-98-2-005	M. Veanes	The Relation Between Second-Order Unification and Simultaneous Rigid E-Unification
MPI-I-98-2-004	S. Vorobyov	Satisfiability of Functional+Record Subtype Constraints is NP-Hard
MPI-I-98-2-003	R.A. Schmidt	E-Unification for Subsystems of S4
MPI-I-98-2-002	F. Jacquemard, C. Meyer, C. Weidenbach	Unification in Extensions of Shallow Equational Theories
MPI-I-98-1-031	G.W. Klau, P. Mutzel	Optimal Compaction of Orthogonal Grid Drawings
MPI-I-98-1-030	H. Brönniman, L. Kettner, S. Schirra, R. Veltkamp	Applications of the Generic Programming Paradigm in the Design of CGAL
MPI-I-98-1-029	P. Mutzel, R. Weiskircher	Optimizing Over All Combinatorial Embeddings of a Planar Graph
MPI-I-98-1-028	A. Crauser, K. Mehlhorn, E. Althaus, K. Brengel, T. Buchheit, J. Keller, H. Krone, O. Lambert, R. Schulte, S. Thiel, M. Westphal, R. Wirth	On the performance of LEDA-SM
MPI-I-98-1-027	C. Burnikel	Delaunay Graphs by Divide and Conquer
MPI-I-98-1-026	K. Jansen, L. Porkolab	Improved Approximation Schemes for Scheduling Unrelated Parallel Machines
MPI-I-98-1-025	K. Jansen, L. Porkolab	Linear-time Approximation Schemes for Scheduling Malleable Parallel Tasks
MPI-I-98-1-024	S. Burkhardt, A. Crauser, P. Ferragina, H. Lenhof, E. Rivals, M. Vingron	q-gram Based Database Searching Using a Suffix Array (QUASAR)
MPI-I-98-1-023	C. Burnikel	Rational Points on Circles
MPI-I-98-1-022	C. Burnikel, J. Ziegler	Fast Recursive Division
MPI-I-98-1-021	S. Albers, G. Schmidt	Scheduling with Unexpected Machine Breakdowns
MPI-I-98-1-020	C. Rüb	On Wallace's Method for the Generation of Normal Variates
MPI-I-98-1-019		2nd Workshop on Algorithm Engineering WAE '98 - Proceedings
MPI-I-98-1-018	D. Dubhashi, D. Ranjan	On Positive Influence and Negative Dependence
MPI-I-98-1-017	A. Crauser, P. Ferragina, K. Mehlhorn, U. Meyer, E. Ramos	Randomized External-Memory Algorithms for Some Geometric Problems
MPI-I-98-1-016	P. Krysta, K. Loryś	New Approximation Algorithms for the Achromatic Number
MPI-I-98-1-015	M.R. Henzinger, S. Leonardi	Scheduling Multicasts on Unit-Capacity Trees and Meshes
MPI-I-98-1-014	U. Meyer, J.F. Sibeyn	Time-Independent Gossiping on Full-Port Tori
MPI-I-98-1-013	G.W. Klau, P. Mutzel	Quasi-Orthogonal Drawing of Planar Graphs
MPI-I-98-1-012	S. Mahajan, E.A. Ramos, K.V. Subrahmanyam	Solving some discrepancy problems in NC*
MPI-I-98-1-011	G.N. Frederickson, R. Solis-Oba	Robustness analysis in combinatorial optimization