The Euclide algorithm in dimension n

Loïc Pottier*

November 7, 1996

Introduction

We present in this paper an algorithm which is a natural extension in dimension n of the Euclide algorithm computing the greatest common divisor of two integers.

Let H be a sub-group of Z^n, given by a system of generators. This algorithm computes the union of bases of all monoids obtained as intersection of H with the 2^n orthants of Z^n.

As a consequence, this algorithm can be used for example to compute minimal solutions of linear Diophantine systems, the basis of the monoid of integer points of a rational simplicial convex cone (called the Hilbert basis of the monoid), the Hilbert serie of a graded algebra, or integer points of a rational simplex.

This is a *completion* algorithm, i.e. similar to Buchberger algorithm (Grobner bases), and to Knuth-Bendix algorithm (canonical rewriting systems), also parent with the Euclide algorithm.

In dimension 2, it is different of the Gaussian algorithm (see for example [3]).

The Euclide algorithm in Z

The Euclide algorithm makes successive Euclidean divisions :

$$a_1 = q_1 a_2 + a_3, \;\; a_2 = q_2 a_3 + a_4, \;\; ,\ldots, a_{n-1} = q_{n-1} a_n$$

giving finally the gcd a_n of a_1 and a_2.

More generally, given $g_1, \ldots, g_n$ generating a sub-group H of Z, divide them with each other, replacing them by remainders of divisions, while it is possible. Then we obtain a basis of H, i.e. the gcd of the g_i. Remark that this gcd is, in absolute value, a basis of the monoid $H \cap N$.

The Euclide algorithm appears then as a *completion algorithm*, as Buchberger algorithm, which makes divisions on multivariate polynomials.

*Projet SAFIR. (Université de Nice-Sophia Antipolis, INRIA, C.N.R.S), 2004 route des Lucioles, Sophia Antipolis, 06565 Valbonne CEDEX, FRANCE. Email : pottier@sophia.inria.fr

Generalization to Z^n

Naturally, let us generalize the Euclidean division to vectors of Z^n :

Definition:

a non zero vector v *divides* a vector v' iff for all $i \in [1;n]$, $v_i v'_i \geq 0$ and $|v_i| \leq |v'_i|$.

The *remainder* of the division of v' by v is $v' - qv$, where q is the greatest natural number such that qv divides v' if v divides v', else $q = 0$.

Note that the remainder is in the same orthant of Z^n than v', and also than v if q is not zero.

The remainder $R(v, F)$ of the division of a vector v by a family F of vectors is obtained by successive divisions by vectors of F or by their opposites. This remainder cannot be divided by any vector of $F \cup -F$ but it is not unique in general, and depends on the order in which vectors of F are used.

In other words, the division by F is not a *confluent* relation in general. To make it confluent, it is necessary to complete F, according to the principle shared by algorithms of Buchberger and Knuth-Bendix.

The Euclide algorithm in dimension n

From a generating system G of a sub-group H of Z^n, we build incrementally a family F of vectors in H, by adding at each step the non zero remainders of divisions by F of sums and differences of vectors of F (sums and differences are analog to *S-polynomials* of Buchberger and *critical pairs* of Knuth-Bendix). A last step divides vectors between them.

- Procedure Completion(G)
- $F := G \cup -G$
- $SD := \{v + v' | v, v' \in F\} - \{0\}$
- While $SD \neq \emptyset$
-     let $v \in SD$
-     $SD := SD - \{v, -v\}$
-     $v := R(v, F)$
-     if $v \neq 0$ then
-         $SD := SD \cup \{v' + v | v' \in F\} \cup \{v' - v | v' \in F\}$
-         $F := F \cup \{v, -v\}$
- Return F

- Procedure Reduction(F)
- While there exists v and v' in F, not equal, v' dividing v
-     $F := F - \{v, -v\} \cup \{R(v, \{v'\}), -R(v, \{v'\})\}$
- Return F

- Procedure HilbertBasis(G)
- Return Reduction(Completion(G))

Theorem

(i) these three procedures always end.
(ii) $v \in H \Leftrightarrow R(v,\text{Completion}(G)) = 0$
(iii) for all orthant $\mathcal{O}$ of Z^n, $\mathcal{O}\cap$HilbertBasis(G) is the basis of the monoid $\mathcal{O} \cap H$.

It is a well-known fact that the monoid of lattice points of a convexe rationnal polyedral cone of R^n is finitely generated, and has a unique basis of non-decomposable elements (see for example [8]).

The name of the procedure HilbertBasis comes from the fact that this basis is frequently called the *Hilbert basis* of this monoid (see [7] for example).

In our case, the cone is generated by $H \cap R_+^n$.

Proof

(i)

The procedure Reduction always ends, because dividing a vector of F strictly decreases the sum of absolute values of coordinates of vectors of F.

The procedure Completion builds a sequence of vectors, such that a vector cannot be divided by its predecessors. If this sequence is infinite, it must contain a sub-sequence of vectors with non-negative and nondecreasing (or non-positive and nonincreasing) first coordinate. The same remark applies inductively for other coordinates. So we get a sub-sequence of vectors dividing their successor, and we have a contradiction (this argument is similar to those of Hilbert basis theorem, and Dixon lemma).

Then, the last procedure also ends QED

(ii)

Let F:=Completion(G). Let v a vector of H irreducible by F. F is a generating system of H (it contains G), it contains opposites of its elements, then we can write $v = v_1 + \ldots + v_p$ where the v_i are in F.

Let us note u^+ the non-negative part of the vector u, and u^- the opposite of its non-positive part. Then $u = u^+ - u^-$.

If $v^+ = v_1^+ + \ldots + v_p^+$, then $v^- = v_1^- + \ldots + v_p^-$, and v is divisible by the v_i's, which contradict the hypothesis that v is irreducible.

Then there exists two vectors, say v_1 and v_2, such that $(v_1+v_2)^+ \neq v_1^+ + v_2^+$, i.e. $(v_1 + v_2)^+ < v_1^+ + v_2^+$. Because F= Completion(G), sums and differences of vectors in F reduce to 0 when divided by F.

So, we can write $v_1 + v_2 = v_{p+1} + \ldots + v_q$ where the v_j are in F (and in the same orthant than $v_1 + v_2$), and we have $v = v_3 + \ldots + v_q$. We have also $(v_1 + v_2)^+ = v_{p+1}^+ + \ldots + v_q^+$.

But $(v_1 + v_2)^+ \neq v_1^+ + v_2^+$: the sum of coordinates of $(v_1 + v_2)^+$ is strictly lesser than the sum of coordinates of v_1^+ and v_2^+. Then, in $v = v_3 + \ldots + v_q$, the sum of coordinates of positive parts is strictly lesser than in $v = v_1 + \ldots + v_p$: we have $v_3^+ + \ldots + v_q^+ < v_1^+ + \ldots + v_p^+$.

Iterating this reasonning, we find $v = 0$.

Then every vector of H reduces to 0 by F. Conversely, it is clear that if a vector reduces to 0 by F, then it is a sum of vectors of F, and is in H QED.

(iii)

Let B:=HilbertBasis(G). The procedure Reduction keeps the property (ii) valid, then a vector is in H if and only if it reduces to 0 with B. The remainders of successive divisions of a vector remain in its orthant, with divisors in its orthant, then a vector of $H \cap \mathcal{O}$ can be written as a sum of vectors of $B \cap \mathcal{O}$. Then $B \cap \mathcal{O}$ is a generating system of the monoid $H \cap \mathcal{O}$. Vectors of B do not divide between themselves, then $B \cap \mathcal{O}$ is the basis of $H \cap \mathcal{O}$ QED.

Improvements of the algorithm

We can improve this algorithm by avoiding to add to F remainders of some sums and differences, as it is done by criterions 1 and 2 of Buchberger and by the "middle rule" in Kunth-Bendix algorithm.

Criterion 1

If v and v' lies in the same orthant, then $v + v'$ reduces to 0 by division by v, and v' (similarly, if v and v' are in opposite orthants, $v - v'$ reduces to 0). Then it is not necessary to add their sum to SD (resp. their difference).

Criterion 2

Let v_1, v_2, and v_3 in F such that $v_1 - v_3$ and $v_3 - v_2$ are in the same orthant. Then it is not necessary to add $v_1 - v_2$ to SD if we add $v_1 - v_3$ and $v_3 - v_2$. Indeed, the remainders of $v_1 - v_3$ and $v_3 - v_2$ allow to reduce $v_1 - v_2$ to 0.

More generally:

the difference $v_1 - v_2$ is unuseful if there exists in F a vector v_3 different from v_1 and v_2 such that $v_1 - v_3$ and $v_3 - v_2$, or $v_1 + v_3$ and $-v_3 - v_2$, are in the same orthant.

the sum $v_1 + v_2$ is unuseful if there exists in F a vector v_3 different from v_1 and v_2 such that $v_1 - v_3$ and $v_3 + v_2$, or $v_1 + v_3$ and $v_2 - v3$, are in the same orthant.

In practice, these criterions are very useful, avoiding many divisions.

Some applications

1. Let $Ax = 0, \ , x \geq 0$ be a linear diophantine system, where A is a matrix with integer coefficients, and x is an integer vector. Its minimal solutions are by definition solutions which are not sum of two others (cf [1], [2], [6] for algorithms computing such minimal solutions).

Let G be a basis of the kernel of the map $x \mapsto Ax$ from Z^n to Z^m (note that such a basis is easy to obtain, by Hermite normal form computation for example [5]).

Then HilbertBasis(G)$\cap N^n$ is the set of minimal solutions of the system.

2. (Dual of application 1) Let C be a rational simplicial convex cone of R^n : C is the convex hull of half lines $R_+a_1, \ldots, R_+a_n$, where the a_i are in Z^n, and independent. Let A be the square matrix whose columns are the a_i, and H the sub-group of Z^n generated by the family G of columns of the matrix $det(A)A^{-1}$.

The image by the map $x \mapsto \frac{A}{det(A)}x$ of HilbertBasis(G)$\cap N^n$ is the basis of the monoid of integer points of C.

3. Let S be a rational simplex in R^n: S is the convex hull of $n+1$ independent points $a_1, \ldots, a_{n+1}$, with rational coordinates. Embed S in R^{n+1} by the map $\phi \ : x \mapsto (x, 1)$ from Z^n to Z^{n+1} : $\phi(S)$ generates a convex cone C, which is rational and simplicial.

In the basis of integer points of C, elements having 1 as last coordinate project bijectively on integer points of S (by the map $(x, y) \mapsto x$).

4. We can generalize to the case of discrete sub-groups of R^n.

In this case, the procedure Completion may not end : the monoids $H \cap \mathcal{O}$ are not longer necessary of finite type. But their intersections with every compact is finite. Then if we choose in the set SD always the vector with the least norm, we can enumerate all the bases of the monoids.

The same reasonning applies to the problem of computing the basis of integer points of a simplicial cone. Recent results of Lachaud ([4]) allows to approximate the normal to the faces of a simplical cone, using the faces of the sail of the cone (the sail is the boundary of the convex hull of non zero integer points of the cone).

As the vertices of this sail are in particular in the basis of integer points of the cone, the Euclide algorithm in dimension n should provide a method to approximate irrational vectors.

It is in fact what happens in dimension 1, where the Euclide algorithm gives the coefficients of the continued fraction of the first two numbers. These coefficients can be obtained as lenghts of the faces of the sails of two cones in the plane.

Can it be generalized in dimension n, in order to give sense to continued fractions in this context? Another question is to understand if the important fact is that we use vextices of the sails, or if we use a basis of integer points of cones (these two notions coincide in the plane, not in general).

5. The Hilbert basis of H is an universal Grobner basis of the toric ideal associated to H, which is the ideal generated by all the differences of monomials $X^{v^+} - X^{v^-}$, where v is in H (because every binomial of a reduced Grobner basis of this ideal correspond to an element of the Hilbert basis of H). Note that this universal Grobner basis is not minimal in general.

6. An implementation of this algorithm can be tested through the Web at URL:
`http://www.inria.fr/safir/SAFIR/Loic/Bastat/monoid.html`

References

[1] Contejean, E. and Devie, H. *Solving systems of linear diophantine equations.* In *UNIF'89*, Lambrecht, RFA, 1990.

[2] Domenjoud, E. *Outils pour la Déduction Automatique dans les Théories Associatives-Commutatives.* PhD thesis, Université de Nancy I, 1991.

[3] Flajolet, P., Daudé, H., and Vallée, B. *An average-case analysis of the Gaussian algorithm for lattice reduction* . Research report 2798, INRIA, feb. 1996.

[4] Lachaud, G. *Polyèdre d'Arnol'd et voile d'un cône simplicial: analogues du théorème de Lagrange.* Comptes rendus de l'Académie des Sciences de Paris, t.317, Série I, p. 711-716 1993.

[5] Kannan, R., and Bachem, A. *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix.* SIAM J. Comp. 8 (1979), 499-507.

[6] Pottier, L. *Gröbner bases of toric ideals.* Rapport de recherche 2224, INRIA, March 1994.

[7] Schrijver, A. *Theory of Linear and Integer Programming.* Wiley-Interscience, 1986.

[8] Tessier, B. *Variétés toriques et polytopes.* Séminaire Bourbaki exp. 565 (nov. 80) Lect. Notes in Math. 901, 1981, 71-84.