Computation of toric Gröbner bases and successive minima of lattices

Loïc Pottier

Institut National de Recherche en Informatique et Automatique,
Projet S.A.F.I.R.,
2004 route des Lucioles, Sophia Antipolis,
06565 Valbonne CEDEX, FRANCE.
Email : `pottier@sophia.inria.fr`

April 13, 1994

1 Introduction

This directory `Bastat-Sun` contains two C programs working on Sun machines. Mathematical bases of these programs can be found in [4], and also in [5] for the first program.

- First program, `bastat`, computes a reduced Gröbner basis of a defining ideal of a monomial variety, its dimension, and its degree if the variety is homogeneous.
- Second program, `minima`, computes Minkowski successive minima of a lattice for the -1 norm $\|x\|_1 = sup(\sum_{x_i>0} x_i, \sum_{x_i<0} -x_i)$. When the lattice is homogeneous (i.e. verifying $\sum_i x_i = 0$), it is the half of the 1 norme $\|x\|_1 = \sum_i |x_i|$, so the successive minima are also those with the 1 norme.

If any of these programs does not work directly, it must be recompiled. For this type `make bastat` or `make minima` (in case of problem, send me computer answers by email...).

2 Program `bastat`

Let X be a variety parametrized by monomials (with exponents possibly negative) :

$$\{X_i = Y^{m_1}, \ldots, X_n = Y^{m_n}\}$$

Let I be the kernel of the morphism from $k[X]$ in $k[Y, Y^{-1}]$ sending X_i to Y^{m_i}. Let A be the matrix with m_i as columns, and H be its kernel, which is a sub-lattice of Z^n. Let $\{v_1, \ldots, v_p\}$ be a basis of H.
The ideal I is the trace on $k[X]$ of

$$J = (TX_1 \ldots X_n - 1, X^{{v_1}^+} - X^{{v_1}^-}, \ldots, X^{{v_p}^+} - X^{{v_p}^-})$$

Program `bastat` computes the reduced Gröbner basis of I for a given order (in fact a Gröbner basis of J, intersected with $k[X]$), and the dimension of X.
If the parameters of X is homogeneous (monomials Y^{m_i} have the same degree), it ask if it must compute the degree of X, what is done if one type any word but `0` (it can take a long time).
The program ask for the following inputs:

1. **the monomial order and the way the ideal is given:**

   0: lexicographic order, the ideal is given by the matrix A.

   1: reverse lexicographic order, the ideal is given by the matrix A.

   2: lexicographic order, the ideal is given by a basis of the kernel of A.

   3: reverse lexicographic order, the ideal is given by a basis of the kernel of A.

2. **a matrix** A of exponents of monomials Y^{m_i} (orders 0 or 1), or a matrix whose rows form a basis of the kernel of A (orders 2 or 3).

The binomials of the Gröbner basis of I are printed as vector of dimension n, positive coordinates corresponding to exponents of leading monomial, negative to tail monomial.
During the computation, are printed pairs of numbers: first is the current number of binomials in the basis, second is the current number of S-polynomials to be reduced.
Limits: the program is limited by the number of elements in the Gröbner bases (10000), the number of S-polynomials to be reduced (1000000), and the size of integers (32 bits). Overcrossing these bounds will cause the program to wildly end ...

2.1 Comparing with `macaulay`

In each session, the program creates a file `input-macaulay` containing a `macaulay` script computing a reverse lexicographic Gröbner basis for I (again by a Gröbner basis of J and elimination).

To make this computaion, type `macaulay<input-macaulay`. The trace of the `macaulay` session is recorded in the file `output-macaulay`.
Comparizon of execution times beetwen `bastat` and `macaulay` is very favourable to `bastat`, particulary in the cases when degrees or number of variables exceed bounds of `macaulay`.
When we give as input the variety by monomials of parameters, a second file `input-mat-macaulay` is created, where the ideal J becomes

$$J = (TY_1 \dots Y_m X_1 \dots X_n - 1, X_1 Y^{m_1^-} - Y^{m_1^+}, \dots, X_1 Y^{m_n^-} - Y^{m_n^+})$$

The Gröbner basis of I is then obtained by a Gröbner basis of J and by elimination of variables $T, Y_1, \dots, Y_m$. This method can allow `macaulay` to achieve its computation when degrees a too big in the first definition of J.

2.2 Example 1

This example is due to M.Morales et P.Gimenez (Institut Fourier, Grenoble, France).
Executions times are those of Sun SPARC10/51 machine.
`macaulay` computes it in 0.48 second (with `input-macaulay`, it fails with too big degrees with `input-mat-macaulay`).
The method of Morales [3], effective in codimension 2, computes it immediately.
`bastat` computes it in 0.32 second (this time contains an uncompressible part of memory allocation, which becomes non significant with bigger examples).
The curve is parametrized with:

$$\{y = s^{281}t^{500}, z = st^{780}, x = s^{781}, w = t^{781}\}$$

Run `bastat`:

```
[C/Bastat-Sun]bastat<Ex/mg-revlex

          CALCUL DE BASES STANDARD D'IDEAUX TORIQUES
------------------------------------------------------------------------------
Loi(tre(accent aigu)ma)c Pottier

Projet SAFIR (Systemes Algebriques Formels pour l'Industrie et la Recherche)
INRIA Sophia Antipolis
2004 route des Lucioles
06565 Valbonne Cedex FRANCE
Tel: 93 65 78 19
Fax: 93 65 77 66
Courrier electronique: pottier@sophia.inria.fr
------------------------------------------------------------------------------
```

avril 1994

```
Ordre sur les monomes:1
Matrice des monomes (= colonnes) definissant la variete:
Nombre de colonnes: 4
Nombre de lignes: 2
Donnez les coefficients de la matrice ligne par ligne:
281 1   781 0
500 780 0   781
Matrice:
-39  25  14   0
 14 -29  -5  20
[3,3][4,4][5,4][6,3][7,7][8,9][9,15][10,12][11,7][12,6][13,9][14,7][15,11]
[16,8][17,13][18,14]
Base standard de l'ideal
(
[-1 281 0 -280]
[2 219 -1 -220]
[5 157 -2 -160]
[8 95 -3 -100]
[-3 62 1 -60]
[11 33 -4 -40]
[39 -25 -14 0]
[-14 29 5 -20]
[25 4 -9 -20]
)
Temps: 0.32s
Nombre de binomes dans la base standard: 9
Dimension de la variete: 2
L'ideal est homogene.
Calcul du degre de la variete?(repondre par 0 ou 1):1
Degre 781
Temps: 0.00s
```

With `macaulay`:

```
[C/Bastat-Sun] macaulay<input-macaulay
                          Macaulay
        A computer algebra system for algebraic geometry

    This program, Macaulay, may be freely copied for others.  We
request that you write us to join a mailing list of Macaulay users,
so that we can keep you informed of updates to Macaulay.
```

Dave Bayer
Department of Mathematics
Barnard College
New York, NY 10027
(212)854-2643, 864-4235
dab@math.columbia.edu

Mike Stillman
Department of Mathematics
Cornell University
Ithaca, NY 14853
(607)255-7240, 277-1835
mike@mssun7.msi.cornell.edu

```
Macaulay version 3.0, created 8/14/89

% ring R
! characteristic (if not 31991)       ?
! number of variables                 ? 5
!   5 variables, please               ? x[0]x[1]x[2]x[3]x[4]
! variable weights (if not all 1)     ?
! monomial order (if not rev. lex.)   ? 1 4
;   largest degree of a monomial        : 512 512

%
ideal I
! number of generators ? 3
! (1,1) ? x[0]1x[1]1x[2]1x[3]1x[4]1-1
! (1,2) ? x[2]29x[3]5-x[1]14x[4]20
! (1,3) ? x[1]39-x[2]25x[3]14

% <inhomog_std I J

% elim J H

% putstd H
; 1
; 9
; x[2]29x[3]5-x[1]14x[4]20
; x[2]62x[3]-x[1]3x[4]60
; x[2]281-x[1]x[4]280
; x[1]2x[2]219-x[3]x[4]220
; x[1]5x[2]157-x[3]2x[4]160
; x[1]8x[2]95-x[3]3x[4]100
; x[1]11x[2]33-x[3]4x[4]40
; x[1]25x[2]4-x[3]9x[4]20
; x[1]39-x[2]25x[3]14

% end of file ($) received, exiting Macaulay
```

2.3 Example 2

This example is taken from [1].
`bastat` computes it in 0.33 second.
`macaulay` fails with `input-macaulay`, degrees are too big, and succeed with `input-mac-macaulay`, in 10.93 seconds.
With `bastat`:

```
Ordre sur les monomes:1
Matrice des monomes (= colonnes) definissant la variete:
Nombre de colonnes: 5
Nombre de lignes: 3
Donnez les coefficients de la matrice ligne par ligne:
2 5 -3 1 -2
1 7 2 3 1
4 -2 -1 -5 3
Matrice:
-125  74  -3 -129   0
6590 -3901 159 6800  -1
[3,5][3,3][4,3][4,2][5,4][6,7][7,10][8,14][9,15][10,11][11,17][12,24][13,17]
[14,22][15,30][16,18][17,25][18,9]
Base standard de l'ideal
(
[35 -21 0 37 1]
[0 -7 -21 22 25]
[5 -8 -15 21 18]
[20 -11 3 18 -3]
[10 -9 -9 20 11]
[15 -10 -3 19 4]
[5 -1 6 -1 -7]
)
Temps: 0.25s
Nombre de binomes dans la base standard: 7
Dimension de la variete: 3
```

With `macaulay`:

```
% ring R
! characteristic (if not 31991)       ?
! number of variables                 ? 9
!   9 variables, please               ? ut[1]t[2]t[3]x[1]x[2]x[3]x[4]x[5]
```

```
! variable weights (if not all 1)     ?
! monomial order (if not rev. lex.)   ? 4 5
;   largest degree of a monomial        : 512 217

%
ideal I
! number of generators ? 6
! (1,1) ? x[1]-t[1]2t[2]1t[3]4
! (1,2) ? x[2]t[3]2-t[1]5t[2]7
! (1,3) ? x[3]t[1]3t[3]1-t[2]2
! (1,4) ? x[4]t[3]5-t[1]1t[2]3
! (1,5) ? x[5]t[1]2-t[2]1t[3]3
! (1,6) ? ut[1]t[2]t[3]x[1]x[2]x[3]x[4]x[5]-1

% <inhomog_std I J

% elim J H

% putstd H
; 1
; 7
; x[4]22x[5]25-x[2]7x[3]21
; x[1]5x[4]21x[5]18-x[2]8x[3]15
; x[1]5x[3]6-x[2]x[4]x[5]7
; x[1]10x[4]20x[5]11-x[2]9x[3]9
; x[1]15x[4]19x[5]4-x[2]10x[3]3
; x[1]20x[3]3x[4]18-x[2]11x[5]3
; x[1]35x[4]37x[5]-x[2]21

% end of file ($) received, exiting Macaulay
```

2.4 Other examples

Other more complex examples, not computable with `macaulay`, are in the directory `Ex` (magic matrices, Leech lattice, ...)
For example the variety parametrized by columns of matrix of the system of equations defining an order 6 magic matrix:

```
1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -1
0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -1
0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 -1
```

```
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 -1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 -1
1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 -1
0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 -1
0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 -1
0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 -1
0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 -1
0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 -1
```

`bastat` computes the Gröbner basis for lexicographic order in 14 seconds, which has 214 binomials, in 37 variables. For reverse lexicographic order, time is 16 seconds, with 308 binomials.
For the corresponding variety of order 7 magic matrices, `bastat` computes the Gröbner basis for lexicographic order in 5 minuts and 12 seconds. It has 497 binomials in 50 variables.

3 Program `minima`

3.1 Problem

To a sub-lattice H of Z^n with basis $\{v_1, \ldots, v_p\}$, we associate ideal I which is the trace on $k[X]$ of ideal

$$J = (TX_1 \ldots X_n - 1, X^{{v_1}^+} - X^{{v_1}^-}, \ldots, X^{{v_p}^+} - X^{{v_p}^-})$$

The successive minima of H for the -1 norm $\|x\|_1 = sup(\sum_{x_i>0} x_i, \sum_{x_i<0} -x_i)$ are then given by some binomials of a reduced Gröbner basis of I for a degree order on monomials [4].
When the lattice is homogeneous (i.e. included in $\sum_i x_i = 0$), this -1 norme is the half of the 1 norme $\|x\|_1 = \sum_i |x_i|$, and the successive minima are also those for the 1 norm.

3.2 Algorithm

The program `minima` has the same input as program `bastat` (see section 2) and give as output the Gröbner basis, with vectors whose norm are the successive minima (they are taken in the Gröbner basis).

3.3 Example

The lattice is a Craig lattice [2] (then homogeneous). Computation time is 52 seconds.

```
[C/Bastat-Sun] minima<Ex/noy56
Ordre sur les monomes:
3
Dimension du reseau:
6
Rang du reseau:
5
Donnez les generateurs ligne par ligne:
2 -6 15 -20 15 -6
-6 2 -6 15 -20 15
15 -6 2 -6 15 -20
-20 15 -6 2 -6 15
15 -20 15 -6 2 -6
reseau:
{
[15 -20 15 -6 2 -6]
[-20 15 -6 2 -6 15]
[15 -6 2 -6 15 -20]
[-6 2 -6 15 -20 15]
[2 -6 15 -20 15 -6]
}
[6,29]
...
[598,699]
ideal
(
norme 32 [17 -7 8 -17 7 -8]
...
norme 2 [-1 0 1 1 0 -1]
)
Plus grande norme dans la base standard: 32
Nombre de binomes dans la base standard: 300
Minima successifs:
(les normes sont les valeurs de la norme -1,
a doubler pour obtenir la norme 1 dans le cas d'un reseau homogene)
ideal
(
norme 32 [0 -5 0 0 32 -27]
norme 18 [0 -9 0 18 0 -9]
norme 18 [0 0 -9 9 9 -9]
norme 2 [0 1 1 0 -1 -1]
norme 2 [-1 0 1 1 0 -1]
)
```

References

[1] P.Conti,C.Traverso "Buchberger algorithm and integer programming", Proc. AAECC-9 1991, LNCS 539 pp130-139, Springer Verlag ed.

[2] J.H.Conway, N.J.A.Sloane "Sphere packings, lattices and groups", Springer verlag ed., p222-224.

[3] M.Morales "Equations des variétés monomiales", pre-print, Université de Grenoble I, France.

[4] L.Pottier "Gröbner bases of toric ideals", rapport de recherche INRIA 2224, INRIA Sophia Antipolis ed., avril 1994.

[5] B.Sturmfels "Gröbner bases of toric varieties", Tohoku Mathematical journal 43 (1991) p 249-261.)