Lattice basis reduction in function fields

Sachar Paulus
Institute of Theoretical Computer Science
Darmstadt University of Technology
64283 Darmstadt
Germany

January 13, 1998

Abstract

We present an algorithm for lattice basis reduction in function fields. In contrast to integer lattices, there is a simple algorithm which provably computes a reduced basis in polynomial time. Moreover, this algorithm works only with the coefficients of the polynomials involved, so there is no polynomial arithmetic needed. This algorithm can be generically extended to compute a reduced lattice basis starting from a generating system. Moreover, it can be applied to lattices of integral determinant over the field of puiseux expansions of a function field. In that case, this algorithm can be used for computing in Jacobians of curves.

1 Previous work

In [4], A. Lenstra published a work on factoring multivariate polynomials over finite fields. Part of the problem was solved by computing a smallest vector of a lattice in a polynomial ring. To solve this problem, he formulated an algorithm which works "only" with coefficients of the finite field. The "only" means that except addition and substraction no polynomial arithmetic is performed; every reduction step consists in the solution of a triangular linear system of equations with coefficients in the finite field.

A. Lenstra proposed this algorithm for lattice bases which are not necessarily of full rank. We argue that this algorithm can also be used (with some minor changes) for computing a reduced basis starting from a generating system.

The main argument for its correctness is analogous to the MLLL justification. Moreover, there is no need to restrict it to polynomials over finite fields. Since for arithmetical operations on approximations of puiseux expansions there is no precision loss, one can easily apply this algorithm on generating systems of "real" lattices, at least the determinant of the lattice is an integer, as used in [8]. By this way, one can develop an arithmetic on divisor classes of curves of higher degree.

2 Reduced lattice bases in function fields

Let n be a positive integer and K a field. For a function $g \in K[X]$ we denote by $|g|$ its degree in X. The *norm* $|a|$ of a n-dimensional vector $a = (a_1, \ldots, a_n) \in K[X]$ is defined as $\max\{|a_j| : 1 \leq j \leq n\}$.

Let $b_1, b_2, \ldots, b_n \in K[X]^n$ be linearly indpendent over $K(X)$. The *lattice* $L \subset K[X]^n$ of *rank* n spanned by $b_1, \ldots, b_n$ is defined as

$$L = \sum_{j=1}^{n} K[X]b_j = \left\{ \sum_{j=1}^{n} r_j b_j : r_j \in K[X](1 \leq i \leq n) \right\}.$$

The *determinant* $d(L) \in K[X]$ of L is defined as the determinant of the $n \times n$ matrix B having the vectors $b_1, \ldots, b_n$ as columns. The value of $d(L)$ does not depend on the choice of a basis of L up to units of K. The *orthogonality defect* $OD(b_1, \ldots, b_n)$ of a basis $b_1, \ldots, b_n$ for a lattice L is defined as

$$\sum_{i=1}^{n} |b_i| - |d(L)|.$$

Clearly $OD(b_1, \ldots, b_n) \geq 0$.

For $1 \leq j \leq n$ a j-th *successive minimum* $|m_j|$ of L is defined as the norm of a vector m_j of smallest norm in L that is linearly independent of $m_1, \ldots, m_{j-1}$ over $K(X)$. $|m_j|$ is independent of the particular choice of $m_1, \ldots, m_{j-1}$. See [5].

Proposition 2.1 *Let $b_1, \ldots, b_n$ be a basis for a lattice L satisfying $OD(b_1, \ldots, b_n) = 0$ ordered in such a way that $|b_i| \leq b_j$ for $1 \leq i < j \leq n$. Then $|b_j|$ is a j-th successive minimum of L for $1 \leq j \leq n$.*

Proof: See [4]. □

We say that the basis $b_1, \ldots, b_n$ is *reduced* if $OD(b_1, \ldots, b_n) = 0$.

Proposition 2.2 *Let $b_1, \ldots, b_n$ be a basis for a lattice L and denote $b_{i,j}$ the j-th coordinate of b_i. If the coordinates of the vectors $b_1, \ldots, b_n$ can be permuted in such a way that they satisfy*

1. $|b_i| \leq |b_j|$ *for* $1 \leq i < j \leq n$ *and*
2. $|b_{i,j}| < |b_{i,i}| \leq |b_{i,k}|$ *for* $1 \leq j < i < k \leq n$,

then the basis $b_1, \ldots, b_n$ is reduced.

Proof: The second condition implies that $d(L) = \sum_{j=1}^{n} |b_j|$, so $b_1, \ldots, b_n$ is reduced. □

The second condition is illustrated by the following figure, where the i-th column of the matrix is b_i. The j-th position in the i-th column gives the condition that holds for $|b_{i,j}|$:

$$\begin{pmatrix} = |b_1| & < |b_2| & < |b_3| & \cdots & < |b_n| \\ \leq |b_1| & = |b_2| & < |b_3| & \cdots & < |b_n| \\ \leq |b_1| & \leq |b_2| & = |b_3| & \cdots & < |b_n| \\ \vdots & \vdots & \vdots & & \vdots \\ \leq |b_1| & \leq |b_2| & \leq |b_3| & \cdots & = |b_n| \end{pmatrix}$$

We extend this theory to the case of a lattice whose rank is smaller than n. Let m be a positive integer $< n$, let $b_1, \ldots, b_m \in K[X]$ be linearly independent over $K(X)$ and let L be the lattice in $K[X]^n$ of rank m spanned by $b_1, \ldots, b_m$. Denote by B the $n \times m$ matrix having the b_i as columns. We define the determinant $d(L)$ of L to be the maximum of the norms of the determinants of the $m \times m$ submatrices of B. The orthogonality defect is again defined as $OD(b_1, \ldots, b_m) = \sum_{i=1}^{m} |b_i| - d(L)$. A basis is called *reduced* if $OD(b_1, \ldots, b_m) = 0$. If the vectors are sorted according to their norm, then $|b_i|$ is a i-th successive minimum of L.

We have an analogous proposition to the one above:

Proposition 2.3 *Let $b_1, \ldots, b_m$ be a basis for a lattice L of rank $m < n$ and denote $b_{i,j}$ the j-th coordinate of b_i. If the coordinates of the vectors $b_1, \ldots, b_m$ can be permuted in such a way that they satisfy*

1. $|b_i| \leq |b_j|$ *for* $1 \leq i < j \leq m$ *and*
2. $|b_{i,j}| < |b_{i,i}| \leq |b_{i,k}|$ *for* $1 \leq j < i \leq m$ *and* $i < k \leq n$,

then the basis $b_1, \ldots, b_m$ *is reduced.*

Proof: The second condition implies that $d(L) = \sum_{j=1}^{n} |b_j|$, so $b_1, \ldots, b_n$ is reduced. □

The second condition is illustrated by the following figure, where the i-th column of the matrix is b_i. The j-th position in the i-th column gives the condition that holds for $|b_{i,j}|$:

$$\begin{pmatrix} = |b_1| & < |b_2| & < |b_3| & \cdots & < |b_m| \\ \leq |b_1| & = |b_2| & < |b_3| & \cdots & < |b_m| \\ \leq |b_1| & \leq |b_2| & = |b_3| & \cdots & < |b_m| \\ \vdots & \vdots & \vdots & & \vdots \\ \leq |b_1| & \leq |b_2| & \leq |b_3| & \cdots & = |b_m| \\ \leq |b_1| & \leq |b_2| & \leq |b_3| & \cdots & \leq |b_m| \\ \vdots & \vdots & \vdots & & \vdots \\ \leq |b_1| & \leq |b_2| & \leq |b_3| & \cdots & \leq |b_m| \end{pmatrix}$$

Finally, we want to compute a reduced basis starting from a generating system. Therefore we need the following

Proposition 2.4 *Let* $b_1, \ldots, b_m$ *be a generating system for a lattice* L *and denote* $b_{i,j}$ *the* j*-th coordinate of* b_i*. If the coordinates of the vectors* $b_1, \ldots, b_m$ *can be permuted in such a way that they satisfy*

1. $|b_i| \leq |b_j|$ *for* $1 \leq i < j \leq m$ *and*
2. $|b_{i,j}| < |b_{i,i}| \leq |b_{i,k}|$ *for* $1 \leq j < i \leq m$ *and* $i < k \leq n$,

then the system $b_1, \ldots, b_m$ *forms a (reduced) basis of* L*.*

Proof: The determinant of the submatrix $(b_{i,j})_{i,j=1,\ldots,m}$ has the largest degree of all $m \times m$ submatrices, namely $\prod_{i=1}^{m} |b_i|$ and is obviously $\neq 0$. If $b_1, \ldots, b_m$ were linear dependent, then the vectors resulting from cutting the last $n - m$ coefficients were also linear dependent and the determinant were 0 which is a contradiction. Thus $b_1, \ldots, b_m$ are linear independent over $K(X)$ and so form a basis. □

3 The algorithm

We will now describe an algorithm which will compute a reduced basis of a lattice of full rank given by a generating system of vectors. In the course of the algorithm the coordinates of the vectors will be permuted several times. The original ordering of the coefficients can be restored by applying the appropriate permutation.

For a polynomial $b_{i,j}$ we denote by $b_{i,j,p}$ the coefficient of X^p.

Algorithm 3.1 ***Input:*** $b_1, \ldots, b_l \in K[X]$

Output: $a_1, \ldots, a_m$ *basis of* $\langle b_1, \ldots, b_l \rangle$

1. $k \leftarrow 0$
2. WHILE $k < l$ DO
   - 2.1. Choose $c \in \{b_{k+1}, \ldots, b_l\}$ such that $|c| = \min\{|b_j| : k+1 \leq j \leq l\}$, let i_c be the corresponding index, $swap(b_{k+1}, b_{i_c})$
   - 2.2. Solve $\sum_{i=1}^{k} a_{i,j,|a_i|} r_i = c_{j,|c|}$ for $1 \leq j \leq k$ in K
   - 2.3. $c' \leftarrow c - \sum_{i=1}^{k} r_i X^{|c|-|a_i|} \cdot a_i$
   - 2.4. IF $|c'| = |c|$ THEN
     - 2.4.a1 $a_{k+1} \leftarrow c$
     - 2.4.a2 Permute the coordinates $(k+1, \ldots, n)$ such that $|a_{k+1,k+1}| = |a_{k+1}|$
     - 2.4.a3 $k \leftarrow k+1$

     ELSE /* *We have found a shorter vector, possibly* 0 */
     - 2.4.b1 IF $c' = 0$ THEN
       - 2.4.b1.a1 eliminate b_{k+1}
       - 2.4.b1.a2 $l \leftarrow l-1$

       ELSE /* *Insert the new vector at the right place and restart from there* */
       - 2.4.b1.b1 $p \leftarrow \max\{0, \ldots, k : |a_l| \leq |c'|\}$
       - 2.4.b1.b2 FOR $j = k+1$ DOWNTO $p+2$ DO $b_j \leftarrow a_{j-1}$
       - 2.4.b1.b3 $b_{p+1} \leftarrow c'$
       - 2.4.b1.b4 $k \leftarrow p$

Remark: We have denoted the vectors which are assumed to be correct during the computation with a and those which are assumed to be reviewed with b. Some assignments have been done in the case where these sets are subject to change (2.4.a1, 2.4.b1.b2-3). Those are clearly not to be done in an implementation: an easy pointer arithmetic can produce the same effect very fast.

Correctness: The following invariants are easy to check to hold before step 2.1:

I1 $|a_i| \leq |a_j|$ for $1 \leq i < j \leq k$

I2 $|a_k| \leq b_j|$ for $k < j \leq l$

I3 $|a_{i,j}| < |a_{i,i}| \leq |a_{i,h}|$ for $1 \leq j < i \leq k$ and $i < h \leq n$

I4 $a_{i,i,|a_i|} \neq 0$ for $1 \leq i \leq k$

I5 $a_{i,j,|a_i|} = 0$ for $1 \leq j < i \leq k$

Note that I4 and I5 imply that the linear system to be solved in step 2.2. is in fact triangular with non-zero entries on the diagonal. Thus there exists a unique solution.

The algorithm terminates, since in step 2.4. either $\sum_{i=1}^{k} |a_i| + \sum_{i=k+1}^{l} |b_i|$ becomes smaller, where k becomes also smaller, or stays unchanged, in which case k is increased by 1. The algorithm terminates if $k = l$, so exactly when $\sum_{i=1}^{k} |a_i|$ equals the determinant of the lattice. Thus only a finite number of passes through 2.4. is possible.

If the algorithm terminates, then the vectors $a_1, \ldots, a_k$ fulfill I1,I2,I3 with $k = l$, thus with proposition 2.4 they form a reduced basis of the lattice. □

We will express the complexity of the algorithm in terms of arithmetical operations in K. By an arithmetical operation in K, we mean addition, subtraction, multiplication or division of two elements of K. We will first study the case where the input of the algorithm is a basis $b_1, \ldots, b_l$. In that case, the number of passes of step 2.4. of the algorithm is bounded by $(l+1) \cdot (OD(b_1, \cdots, b_l)+1)$, since either $\sum_{i=1}^{l} |b_i|$ decreases by at least 1 or stays unchanged, in which case at most $l + 1$ passes are possible, since then k is increased by 1. Now every pass of the main loop consists of $O(k^2)$ operations in K for step 2.2. and $O(k \cdot n \cdot \max |b_i|)$ operations in K for step 2.3. Thus we get the following result:

Proposition 3.2 *Algorithm 3.1 takes $O(l^2 \cdot n \cdot \max |b_i| \cdot OD(b_1, \ldots, b_k))$ arithmetical operations in K to compute a reduced basis starting from a basis $b_1, \ldots, b_l$.*

Now if the input of the algorithm is not a basis, the analysis stays unchanged, but the upper bound given by $OD(b_1, \ldots, b_l)$ makes no longer sense. In that case, we use as upper bound for the number of passes trough the main loop $(l+1) \cdot (\sum_{i=1}^{l} |b_i| - d(L) + 1)$. We get the following

Proposition 3.3 *Algorithm 3.1 takes* $O(l^3 \cdot n \cdot (\max |b_i|)^2)$ *arithmetical operations in* K *to compute a reduced basis starting from a generating system* $b_1, \ldots, b_l$.

If the lattice is "real"-valued and has an integral determinant, then given a sufficient accurate precision p, the algorithm above can be used without changes. The complexity of the algorithm is then $O(l \cdot (l+p) \cdot n \cdot \max |b_i| \cdot OD(b_1, \ldots, b_k))$. If the determinant is not integral, then the termination of the algorithm is not as easy.

4 An application in divisor class groups

There exist several applications for this algorithm. E.g. A.K. Lenstra used it for factoring multivariate polynomials over finite fields. It can also be used for the presentation of large simple groups. We will give a new application in the context of divisor class groups.

As described in [6], the (degree zero) divisor class group of a hyperelliptic curve can be uniquely represented by reduced ideals in an imaginary quadratic function field. In the composition algorithm of reduced ideals, the reduction process of non-reduced ideals plays an important role.

It is a major goal in function field theory to have a reasonably fast arithmetic for the divisor class group of function fields of degree > 2. One hopes that this arithmetic also works with "reduced" ideals. In contrast to the number field case, there may exist a better analogy to imaginary quadratic function fields, namely function fields where the (chosen) infinite prime is totally ramified. In this situation, first results concerning uniqueness of representation of divisor classes are obtained (see [2]). In that model, one needs an algorithm which computes for a given ideal an equivalent ideal of smallest degree. This can be achieved by the puiseux expansions version of the algorithm proposed in this paper analogously to the integral basis reduction in [8]. One applies the algorithm to the image of the ideal basis in the puiseux expansions field and transports the modifications done on the original basis. The first vector of the resulting basis will be the shortest vector of the ideal. Thus dividing the ideal basis elements by this vector will yield a reduced basis.

References

[1] J. Coates: *Construction of rational functions on a curve.* Proc. Camb. Phil. Soc. **68** (1970).

[2] S. Galbraith, S. Paulus: *Unique representation of divisor class groups of function fields of degree* > 2. In preparation.

[3] A. K. Lenstra, H. W. Lenstra Jr., L. Lovasz: *Factoring polynomials with rational coefficients.* Math. Ann. **261** (1982).

[4] A. K. Lenstra: *Factoring multivariate polynomials over finite fields.* J. Computer & System Sciences **30** (1985) No. 2.

[5] K. Mahler: *An analogue of Minkowski's geometry of numbers in a field of series.* Annals of Math. **42** (1941).

[6] S. Paulus, H. G. Rück: *Real and imaginary quadratic representations of hyperellitptic function fields.* To appear in Mathematics of Computation.

[7] M. E. Pohst, H. Zassenhaus: *Algorithmic algebraic number thoery.* Cambrigde University Press: Cambridge 1989.

[8] M. E. Pohst, M. Schörning: *On integral basis reduction in global function fields.* Proceedings of ANTS II. Lecture Notes in Computer Science **1122**. Springer Verlag 1996.