On Integral Basis Reduction in Global Function Fields

M. E. Pohst and M. Schörnig

Technische Universität Berlin, Sekr. MA 8-1, FB 3 Mathematik
Straße des 17. Juni 136, D–10623 Berlin, F.R.G.
pohst@ and schoern@math.tu-berlin.de

1 Introduction

Global fields F are either finite extensions of $\mathbb{Q}$ or of $\mathbb{F}_q(x)$, a rational function field in one variable over a finite constant field. The integral closure o_F of $R = \mathbb{Z}$ or $R = \mathbb{F}_q[x]$, respectively, in F is a Dedekind domain and a free R-module of full rank, i.e. $o_F = \bigoplus_{i=1}^n R\omega_i$, where n denotes the degree of the extension and $\omega_i, 1 \leq i \leq n$, an integral basis.

In case F being a number field, o_F can be identified via the Minkowski map with a lattice in the Hilbert space $\mathbb{R}^n$. The most famous and efficient algorithm for basis reduction, the LLL-algorithm (cf. [6]), uses the existence of the inner product in $\mathbb{R}^n$ extensively in a sophisticated way.

Unfortunately, when F is a function field, there is no identification of o_F with a lattice in a Hilbert space because all valuations on F are discrete. Therefore, it is impossible to adapt the LLL-reduction to the function field case.

In this paper we sketch a reduction algorithm for integral bases in function fields where the infinite place P_∞ is tamely ramified. This algorithm allows us, e.g., to compute an integral basis $\omega_1, \ldots, \omega_n \in o_F$ with $B(\omega_i) = M_i, 1 \leq i \leq n$, where B is a special length function on F and the M_i's are generalized successive minima of o_F with respect to B. Furthermore, we give some applications to the unit group computation of o_F in fields of degree ≥ 3.

For proofs and a more detailed description we refer to a forthcoming paper.

2 Preliminaries

Let $q := p^r$ be a prime power, x transcendental over $\mathbb{F}_q$ and

$$F := \mathbb{F}_q(x, \rho) \text{ with } f(x, \rho) = 0,$$

where $\rho \in \overline{\mathbb{F}_q(x)}$ and $f \in \mathbb{F}_q[x, y]$ is an irreducible polynomial with $\deg_y(f) = n$ which is monic and separable in y.

The exact constant field $\widetilde{\mathbb{F}}_q$ is defined to be the set of all elements of F which are algebraic over $\mathbb{F}_q$. $\widetilde{\mathbb{F}}_q$ is a finite extension of $\mathbb{F}_q$ with $[\widetilde{\mathbb{F}}_q : \mathbb{F}_q] =: l \mid n$.

For $K \in \{\mathbb{F}_q(x), F\}$, we denote by $\mathbb{P}(K)$ ($\mathrm{Div}(K)$) the set of all places (divisors) of K. With $P \in \mathbb{P}(K)$ we associate the corresponding valuation ring $\mathcal{O}_P$, the surjective valuation $v_P : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ and the absolute value

$|\cdot|_P := q^{-v_P(\cdot)}, q^{-\infty} := 0$. The quotient $\mathcal{O}_P/P$ is isomorphic to a finite extension of $\mathbb{F}_q$. We define $\deg(P)$ to be the degree of this extension.

Especially, when $K = \mathbb{F}_q(x)$ we set $\mathcal{O}_\infty := \{g/h \in \mathbb{F}_q(x) \mid g, h \in \mathbb{F}_q[x], h \not\equiv 0, \deg(g) \le \deg(h)\}$ and denote by $P_\infty \quad (= x^{-1}\mathcal{O}_\infty)$, v_∞ and $|\cdot|_\infty := q^{-v_\infty(\cdot)}$ the corresponding place, surjective valuation and absolute value, respectively. By o_F ($o_{F,\infty}$) we denote the integral closure of $\mathbb{F}_q[x]$ ($\mathcal{O}_\infty$) in F. Furthermore, we set $U_F := o_F^*$.

Then there exists $s \in \{1, \dots, n\}$, and pairwise distinct $P_1, \dots, P_s \in \mathbb{P}(F)$ with $P_\infty o_{F,\infty} = \prod_{i=1}^s P_i^{e_i}$, where $e_i := e(P_i|P_\infty)$ is the ramification index and $f_i := f(P_i|P_\infty)$ the relative degree of P_i over P_∞, $(1 \le i \le s)$. We enumerate P_i, e_i and f_i subject to

$$e_i \le e_j \text{ and if } e_i = e_j : f_i \le f_j \text{ for all } 1 \le i < j \le s,$$

and call the $2s$-tuple $(e_1, f_1; \dots; e_s, f_s) \in \mathbb{N}^{2s}$ the signature of $F/\mathbb{F}_q(x)$.

Finally, we set $e := \mathrm{lcm}(e_1, \dots, e_s)$, $n_i := e_i f_i$ and denote by $v_i := v_{P_i}$ ($|\cdot|_i := q^{-v_i(\cdot)}, q^{-\infty} := 0$) the extensions of v_∞ ($|\cdot|_\infty$) to F, $(1 \le i \le s)$.

3 Geometry of Numbers

As in the number field case the efficiency of algorithmic methods applied to o_F strongly relies on the choice of a "good" integral basis with respect to a special length function. In this section we generalize the notion of length functions, lattices and successive minima given by K. Mahler [7]. We start with some definitions.

Definition 1. For a finite extension $E/\mathbb{F}_q$ and $k \in \mathbb{N}$ let

$$E\langle x^{-1/k}\rangle := \Big\{ \sum_{i=m}^{\infty} a_i x^{-i/k} \mid m \in \mathbb{Z}, a_i \in E \Big\}$$

denote the field of Puiseux series in $x^{-1/k}$ and by

$$V_k : E\langle x^{-1/k}\rangle \longrightarrow \mathbb{Z} \cup \{\infty\} : \alpha = \sum_{i=m}^{\infty} a_i x^{-i/k} \longmapsto \begin{cases} \infty & \alpha = 0, \\ \min\{i \in \mathbb{Z} \mid a_i \neq 0\} & \text{else,} \end{cases}$$

a surjective valuation on $E\langle x^{-1/k}\rangle$.

For the remaining of the section we fix $E/\mathbb{F}_q$ with $d := [E : \mathbb{F}_q] \in \mathbb{N}$, $k \in \mathbb{N}$ and set $L := E\langle x^{-1/k}\rangle$.

Definition 2. A function $G : L^n \to \mathbb{R}^{\ge 0}$ ($G : F \to \mathbb{R}^{\ge 0}$) with

1. $G(\alpha) = 0 \Leftrightarrow \alpha = 0$,
2. $G(\lambda\alpha) = |\lambda| G(\alpha)$ ($G(\lambda\alpha) = |\lambda|_\infty G(\alpha)$) and
3. $G(\alpha \pm \beta) \le \max\{G(\alpha), G(\beta)\}$

for all $\lambda \in L, \alpha, \beta \in L^n$ ($\lambda \in \mathbb{F}_q(x), \alpha, \beta \in F$) is called a length function on L^n (F).

Definition 3. Let R be a subring of $E[x^{1/k}]$ and $M \in \mathrm{GL}(n, L)$. Then $\Lambda = \Lambda(M, R) := \{M\alpha \mid \alpha \in R^n\}$ is called an R-lattice in L^n.

With these definitions at hand we remark an analogue to lattices in $\mathbb{R}^n$.

Remark. The ring R is a discrete subset of L equipped with the topology induced by the absolute value $q^{-dV_k(\cdot)}$. Therefore, an R-lattice $\Lambda \subset L^n$ is a discrete, additive subgroup of L^n with the product topology.

We generalize the notion of the successive minima.

Definition 4. Let R be a subring of $E[x^{1/k}]$, $\Lambda \subset L^n$ an R-lattice and G a length function on L^n. For $i \in \{1, \ldots, n\}$ the value

$$\begin{aligned} M_i(\Lambda, R, G) := \min\{\ \lambda \in \mathbb{R} \mid\ & \text{there exist } R\text{-linear independent} \\ & a_1, \ldots, a_i \in \Lambda \text{ with } G(a_j) \leq \lambda, \quad 1 \leq j \leq i\} \end{aligned}$$

is called the i-th successive minimum of Λ (with respect to R and G).

Replacing G by a length function on F and Λ by o_F, we define for $R := \mathbb{F}_q[x]$ analogously the i-th successive minimum $M_i(o_F, R, G)$ of o_F (with respect to R and G).

In [7], K. Mahler proved that $E[x^{1/k}]$-lattice bases can always be chosen to achieve the successive minima.

Theorem 5. *Let G be a length function on L^n, $M \in GL(n, L)$, $R := E[x^{1/k}]$, $\Lambda := \Lambda(M, R)$ and $M_i := M_i(\Lambda, R, G), 1 \leq i \leq n$.*

Then there exists a $T \in GL(n, R)$ with $V_k(\det T) = 0$ and

$$G(b_i) = M_i, \quad 1 \leq i \leq n, \ \text{where } (b_1, \ldots, b_n) := MT.$$

We now consider a special length function which will become important concerning algorithms for global function fields.

Definition and Lemma 1. *The function*

$$B : F \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto \max_{i=1}^{s} |\alpha|_i^{1/e_i}$$

is a length function on F with $B(\cdot) = q^{B^*(\cdot)}$ where

$$B^* : F \longrightarrow \{a/e \mid a \in \mathbb{Z}\} \cup \{-\infty\} : \alpha \longmapsto -\min_{i=1}^{s} v_i(\alpha)/e_i \ \text{and } B^*|_{o_F^\times} \geq 0.$$

Remark. The analogue of B in number fields is as follows: Let $K = \mathbb{Q}(\tau)$ with $g(\tau) = 0$ where $\tau \in \overline{\mathbb{Q}}$ and $g \in \mathbb{Z}[t]$ is a monic, irreducible polynomial of degree n. The roots $\tau_1, \ldots, \tau_n$ of g are sorted according to $\tau_i \in \mathbb{R}, 1 \leq i \leq r_1$, and $\tau_i = \overline{\tau}_{i+r_2} \in \mathbb{C} \backslash \mathbb{R}, r_1+1 \leq i \leq r_1+r_2$ with suitable $r_1, r_2 \in \mathbb{N}_0$. Then $|\cdot| : \mathbb{Q} \to \mathbb{R}$ has r_1+r_2 non-equivalent extensions, namely $|\cdot^{(i)}|, 1 \leq i \leq r_1$, and $|\cdot^{(i)}|^2, r_1+1 \leq i \leq r_1+r_2$ where $\cdot^{(i)}$ denotes the the mapping onto the i-th conjugate (cf. [13, Proposition 5-1-2.]). By definition, $f_i = 1, 1 \leq i \leq r_1 + r_2, \quad e_i = 1, 1 \leq i \leq r_1$, and $e_i = 2, r_1 + 1 \leq i \leq r_1 + r_2$ (cf. [3, p. 57]). Therefore, the analogue of B in number fields takes the form: $\alpha \mapsto \max_{i=1}^{r_1+r_2} |\alpha^{(i)}|$ for $\alpha \in K$.

Concerning the successive minima $M_i := M_i(o_F, \mathbb{F}_q[x], B), 1 \leq i \leq n$, we obtain

Theorem 6. *There exists an integral basis $\omega_1, \ldots, \omega_n \in o_F$ with $M_i = B(\omega_i), 1 \leq i \leq n$.*

When P_∞ is tamely ramified in F, i.e. $p \nmid e$, we will compute an integral basis satisfying Theorem 6 in section 5.

The structure of the successive minima depends on the exact constant field as we can see from

Lemma 7. *For $l = [\widetilde{\mathbb{F}}_q : \mathbb{F}_q]$ we have*

$$1 = M_1 = \ldots = M_l < M_{l+1} = \ldots = M_{2l} \leq \ldots \leq M_{n-l+1} = \ldots M_n.$$

4 Integral Basis Reduction

For many constructive problems concerning F it is important to compute elements $\alpha \in F$ with prescribed lower bounds for $v_1(\alpha), \ldots, v_s(\alpha)$ or, equivalently, elements with upper bounds for $|\alpha|_1, \ldots, |\alpha|_s$.

When we are dealing with number fields, this corresponds to the computation of elements with prescribed upper bounds for the absolute values of the conjugates; usually, this is done by enumeration of a weighted positive definite quadratic form (cf. [9, Chapter 5, Lemma (3.11)]).

For function fields, we do this in a different way, as we will show in the sequel. We start with the definition of a suitable Riemann-Roch space which goes back to W. M. Schmidt [11]:

Definition 8. For $D = \sum_{i=1}^{s} c_i P_i \in \mathrm{Div}(F)$ with $c_i \in \mathbb{Z}, 1 \leq i \leq s$, and $t \in \mathbb{R}$ we define the $\widetilde{\mathbb{F}}_q$-vector space

$$\mathcal{L}(D, t) := \{\alpha \in o_F \mid v_i(\alpha) \geq -c_i - te_i \quad (1 \leq i \leq s)\}.$$

Remark. By the product formula, we have $\mathcal{L}(D, t) = \{0\}$ whenever $\sum_{i=1}^{s} f_i(-c_i - te_i) > 0$.

For function fields over $\mathbb{C}(x)$ there is a deterministic algorithm for determining a basis for $\mathcal{L}(D,t)$ (cf. [11]) which is based on [2]. This algorithm uses Puiseux expansions of all roots of f over P_∞ which causes no problems since the constant field $\mathbb{C}$ has characteristic zero and is algebraically closed.

Before we can give a suitable modification of the algorithm which works over finite constant fields, we first have to deal with Puiseux expansions of the roots $\rho_1, \ldots, \rho_n$ of f over P_∞.

Recalling the definition of the fields of Puiseux series from the last section we can describe the roots of f in the case when P_∞ is tamely ramified:

Theorem 9. *If $p \nmid e$, then there exist*

$$d_1, \ldots, d_n \in \{1, \ldots, n\}, \quad d \in \{1, \ldots, lcm(d_1, \ldots, d_n)\}$$

and an enumeration of $\rho_1, \ldots, \rho_n$ with

$$(\rho_1, \ldots, \rho_n) = (\rho_{1,1}, \ldots, \rho_{1,n_1}, \rho_{2,1}, \ldots, \rho_{2,n_2}, \ldots, \rho_{s,1}, \ldots, \rho_{s,n_s})$$

such that $\rho_{i,j} \in \mathbb{F}_{q^d}\langle x^{-1/e_i}\rangle \subset \mathbb{F}_{q^d}\langle x^{-1/e}\rangle$, $\quad 1 \leq j \leq n_i$, are Puiseux expansions at $P_i, 1 \leq i \leq s$. Furthermore, $\mathbb{F}_{q^d}$ contains all e_i-th roots of unity, $1 \leq i \leq s$.

Remark. 1) The Puiseux expansions can be obtained via the Newton-Puiseux method (cf. [12, Chapter IV]).

2) If $p \mid e$, then the expansions obtained via the Newton-Puiseux method are not necessarily of Puiseux type but generally of Hamburger-Noether type (cf. [1, Chapter II], [10] and [4]).

3) If we are not interested in $F/\mathbb{F}_q(x)$ but in $F/\mathbb{F}_q$, and there is a place $P \in \mathbb{P}(\mathbb{F}_q(x))$ of degree one which is tamely ramified, it is possible to interchange the places P_∞ and P. Of course, this leads to a transformation of x into an x' and we study $F/\mathbb{F}_q(x')$ instead of $F/\mathbb{F}_q(x)$ but now with tamely ramified $P_\infty \in \mathbb{P}(\mathbb{F}_q(x'))$.

From now on let

$$(\rho_1, \ldots, \rho_n) = (\rho_{1,1}, \ldots, \rho_{s,n_s}) \in (\mathbb{F}_{q^d}\langle x^{-1/e}\rangle)^n =: (E\langle x^{-1/e}\rangle)^n =: L^n$$

be sorted according to Theorem 9 and $D = \sum_{i=1}^s c_i P_i \in \mathrm{Div}(F)$ with $c_i \in \mathbb{Z}, 1 \leq i \leq s$.

Before we introduce the notion of a D-reduced integral basis, we define the following four mappings (embedding, transformation, projection and order function):

$$\bar{\cdot} : F \to L^n : \alpha = \sum_{j=1}^n \lambda_j \rho^{j-1} \mapsto \overline{\alpha} := \big(\sum_{j=1}^n \lambda_j \rho_i^{j-1}\big)_{1 \leq i \leq n},$$

$$\cdot^D : L^n \to L^n : \beta = \big(\sum_{j=m_i}^\infty a_{i,j} x^{-j/e}\big)_{1 \leq i \leq n} \mapsto$$

$$\beta^D := \begin{pmatrix} \big(\sum_{j=m_i+c_1e/e_1}^{\infty} a_{i,j}x^{-j/e}\big)_{1\le i\le n_1} \\ \vdots \\ \big(\sum_{j=m_i+c_se/e_s}^{\infty} a_{i,j}x^{-j/e}\big)_{n-n_s+1\le i\le n} \end{pmatrix},$$

$$\theta_k : L^n \to E^n : \beta = \big(\sum_{j=m_i}^{\infty} a_{i,j}x^{-j/e}\big)_{1\le i\le n} \mapsto (a_{i,k})_{1\le i\le n}, \text{ for } k\in\mathbb{Z},$$

$$V : L^n \to \mathbb{Z}\cup\{\infty\} : \beta \mapsto \begin{cases} \infty & \beta = 0, \\ \min\{k\in\mathbb{Z} \mid \theta_k(\beta)\ne 0\} & \text{else.}\end{cases}$$

Definition 10. An integral basis $\omega_1,\ldots,\omega_n$ is called D-reduced, if for all $j \in \{0,\ldots,\ e-1\}$ the following set is $\mathbb{F}_q$-linearly independent (by definition, $\emptyset$ is linearly independent):

$$\{\theta_{V(\overline{\omega}_i^D)}(\overline{\omega}_i^D) \in E^n \mid i\in\{1,\ldots,n\} \text{ with } V(\overline{\omega}_i^D) \equiv j \mathrm{mod} e\}.$$

Remark. 1) Note, that for $\alpha \in F$:

$$V(\overline{\alpha}) = \min_{i=1}^{n} V_e(\alpha_i) = e\min_{i=1}^{s} v_i(\alpha)/e_i = -eB^*(\alpha).$$

2) The set

$$\bigoplus_{i=1}^{n} \mathbb{F}_q[x]\overline{\omega}_i \subset L^n$$

is an $\mathbb{F}_q[x]$-lattice in L^n. Therefore, the embedding $\bar{\cdot}$ can be seen as a function field analogue to the Minkowski map, and the transformation $\cdot^D$ is a lattice transformation with $V_e(det(\cdot^D)) = e\sum_{i=1}^{s} n_ic_i/e_i$.

With these definitions at hand we have (cf. [11]):

Lemma 11. *Let $\omega_1,\ldots,\omega_n$ be an integral basis. Then there exist $T\in GL(n,\mathbb{F}_q[x])$ and a D-reduced integral basis $(\tilde{\omega}_1,\ldots,\tilde{\omega}_n) = (\omega_1,\ldots,\omega_n)T$. The computation of T takes at most $V_e(\det(\overline{\omega}_1^D,\ldots,\overline{\omega}_n^D)) - \sum_{i=1}^{n} V(\overline{\omega}_i^D)$ simple reduction steps.*

Lemma 12. *Let $\omega_1,\ldots,\omega_n$ be a D-reduced integral basis and set $t_i := V(\overline{\omega}_i^D)/e \in \mathbb{Q}, 1\le i\le n$. Then the following holds for all $t\in\mathbb{R}$ (with $\deg(0) = -\infty$):*

$$\mathcal{L}(D,t) = \big\{\sum_{i=1}^{n}\lambda_i\omega_i \mid \lambda_i\in\mathbb{F}_q[x] \text{ with } \deg(\lambda_i)\le t_i+t \quad (1\le i\le n)\big\}.$$

Corollary 13. *Let $\mathcal{L}(D,t)$ and $t_i, 1\le i\le n$, as above. Then*

$$l|\dim_{\mathbb{F}_q}(\mathcal{L}(D,t)) = \sum_{i=1}^{n}\max\{0, 1+\lfloor t_i+t\rfloor\}$$

and $l\dim_{\widetilde{\mathbb{F}}_q}(\mathcal{L}(D,t)) = \dim_{\mathbb{F}_q}(\mathcal{L}(D,t))$.

Before we state the reduction algorithm, we define

$$\psi : \Omega := \{(\overline{\omega}_1^D, \ldots, \overline{\omega}_n^D) \in L^{n\times n} \mid \omega_1, \ldots, \omega_n \text{ is an integral basis } \} \longrightarrow \mathbb{Z}$$

$$(\phi_1, \ldots, \phi_n) \longmapsto V_e(\det(\phi_1, \ldots, \phi_n)) - \sum_{i=1}^{n} V(\phi_i)$$

and note $\psi(\Omega) \subset \mathbb{N}_0$.

Algorithm 14. *(D-reduction of an integral basis)*
Input: $(\phi_1, \ldots, \phi_n) := (\overline{\omega}_1^D, \ldots, \overline{\omega}_n^D) \in \Omega$.
Output: $T \in GL(n, \mathbb{F}_q[x])$ *subject to* $(\omega_1, \ldots, \omega_n)T$ *being a D-reduced integral basis.*

1: Initialize $T \leftarrow Id_n(\mathbb{F}_q[x])$.
2: ***Repeat***
  3: Compute $T_0 \in GL(n, \mathbb{F}_q[x])$ *with* $V(\widetilde{\phi}_1) \leq \ldots \leq V(\widetilde{\phi}_n)$ *where* $(\widetilde{\phi}_1, \ldots, \widetilde{\phi}_n) := (\phi_1, \ldots, \phi_n)T_0$. *Set* $(\phi_1, \ldots, \phi_n) \leftarrow (\phi_1, \ldots, \phi_n)T_0, T \leftarrow TT_0$ *and* $b \leftarrow 0$.
  4: ***For*** $\kappa = 0, \ldots, e-1$
    5: Compute $k = \#\{i \in \{1, \ldots, n\} \mid V(\phi_i) \equiv \kappa mod e\}$ *and* $i_1 < \ldots < i_k$ *with* $V(\phi_{i_m}) \equiv \kappa mod e, 1 \leq m \leq k$.
    6: ***If*** *((*$k > 1$*) and (*$\{\theta_{V(\phi_{i_m})}(\phi_{i_m}) \in E^n \mid 1 \leq m \leq k\}$ *is* $\mathbb{F}_q$*-linear dependent))*
      7: (reduction step) There exist $j \in \{1, \ldots, k-1\}$ *and* $(0, \ldots, 0, \alpha_j, \ldots, \alpha_k)^t \in \mathbb{F}_q^k, \alpha_j = 1$ *with* $\sum_{m=j}^{k} \alpha_m \theta_{V(\phi_{i_m})}(\phi_{i_m}) = 0$.
      Set $\xi \leftarrow \phi_{i_j} + \sum_{m=j+1}^{k} \alpha_m x^{(V(\phi_{i_m}) - V(\phi_{i_j}))/e} \phi_{i_m}$ *and compute* $T_1 \in GL(n, \mathbb{F}_q[x])$ *with* $(\phi_1, \ldots, \phi_{i_j - 1}, \xi, \phi_{i_j+1}, \ldots, \phi_n) = (\phi_1, \ldots, \phi_n)T_1$.
      Set $\phi_{i_j} \leftarrow \xi, T \leftarrow TT_1$ *and* $b \leftarrow 1$.
    8: ***end-If***
  9: ***end-For***
10: ***until*** *(*$b = 0$*)*
11: Output T *and terminate.*

Remark. The algortihm terminates, because only two situations can occur at the end of the repeat-loop: Either the flag b is zero, then the algorithm terminates immediately, or the flag b equals one, then a reduction step has taken place and the ψ-value of the current vector $(\phi_1, \ldots, \phi_n)$ has decreased. Furthermore, $\psi(\Omega) \subset \mathbb{N}_0$ and $\psi(\phi_1, \ldots, \phi_n) = 0$ implies that the corresponding integral basis is D-reduced. Therefore, the algorithm terminates after at most $\psi(\overline{\omega}_1^D, \ldots, \overline{\omega}_n^D)$ steps.

5 Applications of Reduced Integral Bases

We are now able to state applications of D-reduced integral bases when P_∞ is tamely ramified in F. We start with 0-reduced integral bases, i.e. D-reduced integral bases with respect to $D = 0 \in \mathrm{Div}(F)$:

Theorem 15. *Let* $\omega_1, \ldots, \omega_n$ *be a* 0*-reduced integral basis with* $B(\omega_1) \leq \ldots \leq B(\omega_n)$*. Then* $M_i = B(\omega_i), 1 \leq i \leq n$*.*

Remark. Considering lattices Λ in $\mathbb{R}^n, n > 4$, there are examples that bases cannot be chosen to achieve the successive minima of Λ with respect to $\|\cdot\|_2$ (cf. [9, Chapter 3, Example (3.31) and Theorem (3.32)]).

According to Dirichlet the structure of the unit group is given by

$$U_F = TU_F \times \langle \varepsilon_1 \rangle \times \ldots \times \langle \varepsilon_r \rangle \cong \mathbb{F}_{q^l}^\times \times \mathbb{Z}^r,$$

where TU_F is the group of the torsion units, r denotes the unit rank and $\varepsilon_1, \ldots, \varepsilon_r$ are fundamental units.

The torsion units are exactly the elements of $\widetilde{\mathbb{F}}_q^\times \cong \mathbb{F}_{q^l}^\times$, and recalling Lemma 7 we have

Lemma 16. *Let* $\omega_1, \ldots, \omega_n$ *be a* 0*-reduced integral basis with* $B^*(\omega_1) \leq \ldots \leq B^*(\omega_n)$*. Then* $0 = B^*(\omega_1) = \ldots = B^*(\omega_l) < B^*(\omega_{l+1})$*.*

Remark. Note that l depends only on $F/\mathbb{F}_q$ (and not on $F/\mathbb{F}_q(x)$). Therefore, we can calculate l via a 0-reduced integral basis when there is at least one place $P \in \mathbb{P}(F)$ with $\deg(P) = 1$ which is tamely ramified (cf. remark (3) after Theorem 9).

In order to compute fundamental units we adapt the "relation method" from number fields. Therefore, we construct elements of (small) bounded norm which can be done easily because of

Lemma 17. *Let* $\omega_1, \ldots, \omega_n$ *be a* 0*-reduced integral basis and* $t \in \mathbb{R}$*. Then* $\alpha \in \mathcal{L}(0, t)$ *implies* $\deg(N_{F/\mathbb{F}_q(x)}(\alpha)) \leq tn$*.*

An easy consequence of the product formula is

Lemma 18. *Let* $D = \sum_{i=1}^s c_i P_i$ *with* $\sum_{i=1}^s c_i f_i = 0$ *(i.e.* $\deg(D) = 0$*). Then we have the following equivalence:*

$$\alpha \in \mathcal{L}(D, 0)^\times \iff \alpha \in U_F \text{ and } v_i(\alpha) = -c_i \quad (1 \leq i \leq s),$$

and $\dim_{\widetilde{\mathbb{F}}_q}(\mathcal{L}(D, 0)) \in \{0, 1\}$*.*

Remark. The last lemma allows us to test whether there is an $\varepsilon \in U_F$ with prescribed $v_1(\varepsilon), \ldots, v_s(\varepsilon)$. This is particulary useful when having a unit $\varepsilon \in U_F$ at hand and trying to decide whether there exists an $\eta \in U_F$ with $\eta^m = \varepsilon$ for $m \in \mathbb{N}$: First, we test $m | v_i(\varepsilon), 1 \leq i \leq s$. After a successful test, we compute $\mathcal{L}(D, 0)$ for $D = \sum_{i=1}^s (v_i(\varepsilon)/m) P_i$. If $\dim_{\widetilde{\mathbb{F}}_q}(\mathcal{L}(D, 0)) = 0$, there is no m-th root of ε; if $\dim_{\widetilde{\mathbb{F}}_q}(\mathcal{L}(D, 0)) = 1$, the l basis elements are m-th roots of ε modulo torsion units, i.e. modulo $\widetilde{\mathbb{F}}_q^\times$.

6 Examples

In this section we give illustrative examples of the results mentioned above.

First, we consider $F = \mathbb{F}_5(x, \rho)$, where

$$f(x, \rho) = \rho^3 + (4x^3 + 4x^2 + 2x + 2)\rho^2 + (3x + 3)\rho + 2 = 0.$$

Then P_∞ splits into P_1 and P_2 with $e_1 = f_1 = 1$ and $e_2 = 2, f_2 = 1$. Therefore, $s = 2$, the signature is $(1,1;2,1)$, $5 \nmid e = 2$ and $(\rho_1, \rho_2, \rho_3) = (\rho_{1,1}, \rho_{2,1}, \rho_{2,2})$ have Puiseux expansions in $\mathbb{F}_{5^2}\langle z\rangle$, where $z := x^{-1/2}$. With a suitable primitive element $w \in \mathbb{F}_{5^2}^\times$, we have

$$\begin{aligned}
\rho_1 &= z^{-6} + z^{-4} + 3z^{-2} + 3 + 2z^4 + 4z^8 + z^{12} + z^{16} + \dots \\
\rho_2 &= w^{15}z^3 + 4z^4 + w^{15}z^5 + w^{15}z^7 + 3z^8 + w^{15}z^9 + \dots \\
\rho_3 &= w^3z^3 + 4z^4 + w^3z^5 + w^3z^7 + 3z^8 + w^3z^9 + \dots
\end{aligned}$$

For the integral basis $\omega_1 := 1, \quad \omega_2 := \rho, \quad \omega_3 := \rho^2$, we obtain

$$B^*(\omega_1) = 0, \quad B^*(\omega_2) = 3, \quad B^*(\omega_3) = 6$$

and for a 0-reduced integral basis $\tilde\omega_1 := 1, \quad \tilde\omega_2 := (2x^3 + 2x^2 + x + 1)\rho + 3\rho^2, \quad \tilde\omega_3 := (4x^3 + 4x^2 + 2x)\rho + \rho^2$:

$$B^*(\tilde\omega_1) = 0, \quad B^*(\tilde\omega_2) = 3/2, \quad B^*(\tilde\omega_3) = 3.$$

This implies $1, \sqrt{125}, 125$ being the successive minima of o_F with respect to B and $l = [\widetilde{\mathbb{F}}_5 : \mathbb{F}_5] = 1$. Furthermore, there is an element $\varepsilon \in U_F$ with $v_1(\varepsilon) = 3 = -v_2(\varepsilon)$. Since $\dim_{\mathbb{F}_q}(\mathcal{L}(P_1 - P_2, 0)) = 0$ there is no 3-rd root of ε. Therefore, ε is a fundamental unit and the regulator is 3.

This example took less than 4 seconds on a Pentium 90 with 16 MB RAM and a modified KASH software (cf. [5]).

Now we compute 0-reduced integral bases for all polynomials of the form

$$f(x,y) = y^3 + a_2(x)y^2 + a_1(x)y + a_0(x) \in \mathbb{F}_3[x,y]$$

with $\deg(a_i) \in \{-\infty, 0, 1\}, 0 \le i \le 2$, where the associated global function field $F/\mathbb{F}_q(x)$ is a separable extension of degree 3 in which P_∞ is tamely ramified.

In the following table the values

$$\begin{aligned}
\Sigma := \sum_{i=1}^n B^*(\omega_i),\ \ \widetilde\Sigma := \sum_{i=1}^n B^*(\widetilde\omega_i),\ \ \Delta\Sigma := \Sigma - \widetilde\Sigma, \\
M := \max_{i=1}^n B^*(\omega_i),\ \widetilde M := \max_{i=1}^n B^*(\widetilde\omega_i),\ \Delta M := M - \widetilde M.
\end{aligned}$$

are given with respect to the signature of all 428 polynomials (out of $3^6 = 729$) satisfying the restrictions mentioned above. Here $\omega_1, \dots, \omega_n \in o_F$ denotes an integral basis obtained with a modified Round-Two method (cf. [8, Ch. V.2]), and $\widetilde\omega_1, \dots, \widetilde\omega_n \in o_F$ is a 0-reduced integral basis.

The computations have been carried out on IBM RS6000 workstations with 64 MB RAM using a modified KASH software. The value $\overline{T}$ in the last column is the average running time in seconds. Values in () are absolute numbers.

Signatur	$[E:\mathbb{F}_3]$	Σ	M	$\tilde{\Sigma}$	$\tilde{M}$	$\Delta\Sigma$	ΔM	$\overline{T}$
$(1,3)$ (8)	3	0	0	0	0	0	0	0,017
$(1,1;1,2)$ (144)	2	3	2	2	1	1	1	3,028
$(1,1;2,1)$ (204)	1 (102) 2 (102)	3/2 (96) 3 (108)	1 (96) 2 (108)	3/2	1	0 (96) 3/2 (108)	0 (96) 1 (108)	7,672
$(1,1;1,1;1,1)$ (72)	1	3	2	2	1	1	1	5,736

Finally, we compute a fundamental unit of the quintic field defined by

$$f(x,y) = y^5 + (2x+3)y^2 + 3y + 1 \in \mathbb{F}_5[x,y].$$

In this example the signature is $(2,1;3,1)$ and ρ is a fundamental unit with $v_1(\rho) = -v_2(\rho) = 1$. The computation took 28 seconds on one of the IBM workstations mentioned above.

References

1. Campillo, A.: *Algebroid curves in positive characteristic*; Springer-Verlag; Berlin - Heidelberg - New York; 1980
2. Coates, J.: *Construction of rational functions on a curve*; Proc. Camb. Phil. Soc., No. 68; 1970; 105 - 123
3. Cohn, P. M.: *Algebraic numbers and algebraic functions*; Chapman & Hall; London - New York - Tokyo - Melbourne - Madras; 1991
4. Griffiths, D.: *Series expansion of algebraic functions*; in: Bosma, W.; van der Poorten, A. (eds.): *Computational algebra and number theory*; Kluwer Academic Publishers; Boston - Dordrecht - London; 1995
5. KANT group: *KANT V4*; submitted to J. Symb. Comput.
6. Lenstra, A. K.; Lenstra, H. W. Jr.; Lovász, L.: *Factoring polynomials with rational coefficients*; Math. Ann., Vol. 261; 1982; 515 - 534
7. Mahler, K.: *An analogue to Minkowski's geometry of numbers in a field of series*; Ann. Math., Vol. 42; No. 2; 1941; 488 - 522
8. Pohst, M. E.: *Computational algebraic number theory*; Birkh"auser Verlag; Basel - Boston - Berlin; 1993
9. Pohst, M.; Zassenhaus, H.: *Algorithmic algebraic number theory*; Cambridge University Press; Cambridge - New York - Melbourne; 1989
10. Ribowicz, M.: *Calcul de paramétrisation de courbes algébriques: Les développements de Hamburger-Noether*; Rapport de recherche RR 798-M; TIM 3/IMAG Informatique et Mathématiques Appliquées de Grenoble; 1989
11. Schmidt, W. M.: *Construction and estimation of bases in function fields*; J. Number Th. 39, No. 2; 1991; 181 - 224
12. Walker, R. J.: *Algebraic curves*; Springer-Verlag; New York - Heidelberg - Berlin; 1978
13. Weiss, E.: *Algebraic number theory*; Chelsea Publishing Company; New York; 1976

This article was processed using the LaTeX macro package with LLNCS style