

ON THE COMPUTATION OF INTEGRAL CLOSURES OF CYCLIC EXTENSIONS OF FUNCTION FIELDS

ROBERT FRAATZ

Abstract

Let \mathcal{S} be a non-empty proper subset of the set of places of a global function field F and E a cyclic Kummer or Artin–Schreier–Witt extension of F . We present a method of efficiently computing the ring of elements of E which are integral at all places of \mathcal{S} . As an important tool, we include an algorithmic version of the strong approximation theorem. We conclude with several examples.

1. *Introduction*

Work by the Russian mathematician Goppa (see, for instance, [7, 8]) showed that function fields with a large number of places of degree one can be used to define good error-correcting codes. Such fields may be constructed by taking a small field F where the number of places is known, and constructing extensions of F such that the splitting behaviour of the places is known in advance from theory. Class field theory is the most powerful technique currently available for building such extensions. To be able to work efficiently with the resulting Abelian extensions of large degree, it is important to develop explicit techniques for the fast computation of integral closures of Kummer extensions, Artin–Schreier–Witt extensions and their composita. In particular Artin–Schreier–Witt extensions have never been the focus of algorithmic investigation.

2. *Preliminaries*

Let $k = \mathbb{F}_q$ be a finite (in particular, perfect) field, q a power of a rational prime p , and F/k an algebraic function field over k ; that is, $F = k(x, \rho)$ with $f(x, \rho) = 0$ for some irreducible polynomial $f \in k[x, t]$ which is monic and separable with respect to t . Let E/F be an extension of function fields, let P be a place of F , and let $\emptyset \neq \mathcal{S}$ be a proper subset of the set \mathbb{P}_F of places of F . If P' is an extension of P to E , then $e(P'|P)$ denotes the ramification index of P' over P . Let \mathcal{O}_P be the valuation ring of P in F , v_P the corresponding valuation and $\mathcal{O}_{\mathcal{S}} := \bigcap_{P \in \mathcal{S}} \mathcal{O}_P$. We denote by $\mathcal{O}_P(E)$ and $\mathcal{O}_{\mathcal{S}}(E)$ the integral closure of \mathcal{O}_P and $\mathcal{O}_{\mathcal{S}}$ in E . If y is an element of E , then we write $\chi_{(y, E/F)}(T) \in F[T]$ for the minimal polynomial of y over F . For a divisor D of F , we denote by $\mathcal{L}(D)$ the Riemann–Roch space, and by $\mathcal{A}_F(D)$ the adèle space of D , the latter being a k -subspace of the adèle space \mathcal{A}_F of F . For details on notation and background, we refer to the book by Stichtenoth [14].

This article was written while the author visited the Computational Algebra Group at the University of Sydney in October–December 2004.

Received 9 September 2005, revised 9 November 2006; *published* 30 March 2007.

2000 Mathematics Subject Classification 11Yxx, 11Y40.

© 2007, Robert Fraatz

The main result of this paper is the development of procedures and algorithms to compute a finite set Ω of $\mathcal{O}_{\mathcal{S}}$ -generators of $\mathcal{O}_{\mathcal{S}}(E)$, where E is a cyclic Kummer (Section 4) or Artin–Schreier–Witt extension (Section 5) of F . This is done by first splitting \mathcal{S} into finitely many disjoint subsets and then computing, for each P in each of these sets, a set Ω_P of \mathcal{S} -integral generators of $\mathcal{O}_P(E)$ over \mathcal{O}_P . Proposition 2.1 assures us that the set, which consists of the union of all Ω_P , is the sought-after set Ω of $\mathcal{O}_{\mathcal{S}}$ -generators of $\mathcal{O}_{\mathcal{S}}(E)$. The set Ω is finite since the sets Ω_P will be equal for all but finitely many $P \in \mathcal{S}$. In Section 3 we give an algorithmic version of the strong approximation theorem which we have developed and which we will use frequently in the later sections. We finish by giving examples which demonstrate the efficiency of our method for computing integral closures by comparing it with the general method, which is based on the Round-2 algorithm.

The following proposition gives us one of the basic tools for our purpose of computing the generators of all \mathcal{S} -integral elements of E .

PROPOSITION 2.1. *Let E be an extension of a function field F/k , and let $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$. Suppose that there is a subset Ω of $\mathcal{O}_{\mathcal{S}}(E)$ which consists of \mathcal{O}_P -generators of $\mathcal{O}_P(E)$ for each $P \in \mathcal{S}$; that is,*

$$\mathcal{O}_P(E) = \mathcal{O}_P[\Omega] \quad \forall P \in \mathcal{S}.$$

Then Ω is a set of generators of $\mathcal{O}_{\mathcal{S}}(E)$ over $\mathcal{O}_{\mathcal{S}}$; that is,

$$\mathcal{O}_{\mathcal{S}}(E) = \mathcal{O}_{\mathcal{S}}[\Omega].$$

Proof. We have $\mathcal{O}_P[\Omega] = (\mathcal{O}_{\mathcal{S}}[\Omega])_{P \cap \mathcal{O}_{\mathcal{S}}}$ and $\mathcal{O}_P(E) = (\mathcal{O}_{\mathcal{S}}(E))_{P \cap \mathcal{O}_{\mathcal{S}}}$, where the modules on the right-hand side are the localizations of the $\mathcal{O}_{\mathcal{S}}$ -modules $\mathcal{O}_{\mathcal{S}}[\Omega]$ and $\mathcal{O}_{\mathcal{S}}(E)$, respectively, at the prime ideal $P \cap \mathcal{O}_{\mathcal{S}}$. Thus our assumption means that $(\mathcal{O}_{\mathcal{S}}(E))_{\mathfrak{p}} = (\mathcal{O}_{\mathcal{S}}[\Omega])_{\mathfrak{p}}$ for all maximal ideals \mathfrak{p} of $\mathcal{O}_{\mathcal{S}}$. This implies the result. \square

The next two results will help us to compute, for a place P of a function field F , a local integral basis for some field extension of F .

COROLLARY 2.2. *Let $E_0 \subseteq E_1 \subseteq \dots \subseteq E_n$ be a tower of field extensions of a function field E_0 , let P be a place of E_0 and let $\mathcal{S}_i \subset \mathbb{P}_{E_i}$ be all the places of E_i above P . Suppose, for all $0 \leq i \leq n-1$ and all $Q \in \mathcal{S}_i$, that there is $\Delta_Q \subset \mathcal{O}_P(E_{i+1})$ such that $\mathcal{O}_Q(E_{i+1}) = \mathcal{O}_Q[\Delta_Q]$. Then*

$$\mathcal{O}_P(E_n) = \mathcal{O}_P[\Delta], \quad \text{where } \Delta = \bigcup_{\substack{Q \in \mathcal{S}_i \\ 0 \leq i \leq n-1}} \Delta_Q.$$

Proof. This requires repeated application of Proposition 2.1 and the fact that $\mathcal{O}_{\mathcal{S}_i}(E_{i+1}) = \bigcap_{Q \in \mathcal{S}_{i+1}} \mathcal{O}_Q = \mathcal{O}_{\mathcal{S}_{i+1}}$. \square

PROPOSITION 2.3. *Let E be a finite separable extension of a function field F of degree n , and let $P \in \mathbb{P}_F$.*

(i) *Suppose that $E = F(y)$ and $\chi(T)$ is the minimal polynomial of y . If $\chi(T) \in \mathcal{O}_P[T]$ and $v_{P'}(\chi'(y)) = 0$ for all $P' \in \mathbb{P}_E$ with $P'|P$, then P is unramified in E and $\{1, y, \dots, y^{n-1}\}$ is a local integral basis for P in E/F .*

(ii) *Suppose that $P'|P$ (where $P' \in \mathbb{P}_E$) is totally ramified in E/F , and π is a prime element for P' . Then $\{1, \pi, \dots, \pi^{n-1}\}$ is a local integral basis for P in E/F .*

Proof. See [14, III.5.11 and III.5.12]. □

REMARK 2.4. Let F be a function field over the rational function field $k(x)$ and $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$. Define $s := \{p \in \mathbb{P}_{k(x)} \mid \exists P \in \mathcal{S} \text{ with } P|p\}$ and $\mathcal{S}' := \{P \in \mathbb{P}_F \mid P|p \text{ for some } p \in s\}$. Then for each $a \in F$ there exists a unique representation $a = \text{num}(a)/\text{den}(a)$ satisfying $\text{num}(a) = a_1\omega_1 + \dots + a_m\omega_m \in \mathcal{O}_{\mathcal{S}'}$ (here $a_i \in \mathcal{O}_s$ and $\omega_1, \dots, \omega_m$ is a basis of $\mathcal{O}_{\mathcal{S}'}$ over \mathcal{O}_s), $\text{den}(a) \in \mathcal{O}_s$ and $\gcd(\text{den}(a), a_1, \dots, a_m) = 1$. (Note that \mathcal{O}_s is a unique factorization domain.)

Using this notation, we now can state the following proposition.

PROPOSITION 2.5. *Let E/F be a function field extension, $0 \neq \beta \in E$, and let $\chi_{(\beta, E/F)}(T) = \sum_{i=0}^m \alpha_i T^i$ be the minimal polynomial of β over F . Let $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$. For*

$$\delta_\beta := \text{lcm} \left\{ \text{den} \left(\frac{\alpha_i}{\alpha_j} \right) \mid 0 \leq i < j \leq m, \alpha_i, \alpha_j \neq 0 \right\},$$

we have $\beta\delta_\beta \in \mathcal{O}_{\mathcal{S}}(E)$.

Proof. From the Newton polygon of $\chi_{(\beta, E/F)}$ we know that there exist $0 \leq r < s \leq m$ such that $0 \neq \alpha_r, \alpha_s$ and

$$v_{P'}(\beta) = e(P'|P) \frac{v_P(\alpha_r) - v_P(\alpha_s)}{s - r}$$

(see for instance [3, Chapter 6.3]). The result now follows easily. □

3. Strong approximation

A main tool for all the results presented in this paper is the strong approximation theorem. Since it is also of independent interest, we give an algorithmic solution in this section.

THEOREM 3.1 (STRONG APPROXIMATION). *Let F/\mathbb{F}_q be a function field, $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$ and $P_1, \dots, P_r \in \mathcal{S}$. Suppose that there are given $a_1, \dots, a_r \in F$ and $n_1, \dots, n_r \in \mathbb{Z}$. Then there exists an element $z \in F$ such that*

$$\begin{aligned} v_{P_i}(z - a_i) &= n_i & 1 \leq i \leq r, & \quad \text{and} \\ v_P(z) &\geq 0 & \text{for all } P \in \mathcal{S} \setminus \{P_1, \dots, P_r\}. \end{aligned} \tag{3.1}$$

Our proof follows Stichtenoth's [14], but is constructive. We need the following lemma.

LEMMA 3.2. *Suppose that we are in the situation of the theorem. Then there exists an element $y \in F$ such that*

$$\begin{aligned} v_{P_i}(y - a_i) &> n_i & 1 \leq i \leq r, & \quad \text{and} \\ v_P(y) &\geq 0 & \text{for all } P \in \mathcal{S} \setminus \{P_1, \dots, P_r\}. \end{aligned} \tag{3.2}$$

Proof. For $1 \leq i \leq r$ we set $\tilde{n}_i := n_i + 1$. We take a divisor A of positive degree whose support is disjoint to \mathcal{S} . Then there exists $l \in \mathbb{N}$ such that the divisor $D := lA - \sum_{j=1}^r \tilde{n}_j P_j$ is non-special (see [14, I.6.8.]).

We now describe how to find, for each $1 \leq i \leq r$, an element $y_i \in F$ with

$$\begin{aligned} v_{P_i}(y_i - a_i) &\geq \tilde{n}_i & 1 \leq i \leq r, \\ v_{P_j}(y_i) &\geq \tilde{n}_j & 1 \leq i \leq r, j \neq i \quad \text{and} \\ v_P(y_i) &\geq 0 & \text{for all } P \in \mathcal{S} \setminus \{P_1, \dots, P_r\}. \end{aligned} \quad (3.3)$$

The element $y = \sum_{i=1}^r y_i$ then satisfies (3.2).

If $v_{P_i}(a_i) \geq \tilde{n}_i$, we can set $y_i := 0$ and are done.

Suppose now that $v_{P_i}(a_i) < \tilde{n}_i$. The non-speciality of D implies that $\mathcal{A}_F = \mathcal{A}_F(D) + F$; see [14, I.5.4.]. Therefore there exists $\beta \in F$ such that $(\beta - \alpha_i) \in \mathcal{A}_F(D)$, where $\alpha_i \in \mathcal{A}_F$ is the adele whose P_i -component equals a_i and which is zero at all other components. This implies that $v_{P_i}(\beta - a_i) \geq \tilde{n}_i > v_{P_i}(a_i)$. The strict triangle equation then yields $v_{P_i}(\beta) = v_{P_i}(a_i)$; therefore

$$\beta \in \mathcal{L} := \mathcal{L} \left(lA - \sum_{j=1}^r \tilde{n}_j P_j + \tilde{n}_i P_i - v_{P_i}(a_i) P_i \right)$$

and $y_i := \beta$ satisfies (3.3). We finish the proof by showing how to actually compute β .

- (i) Let $\mathcal{B} := b_1, \dots, b_s$ be a basis of \mathcal{L} (for the computation of the Riemann–Roch spaces we refer to [10]).
- (ii) For each element $\gamma \in \{a_i\} \cup \mathcal{B}$ we compute a (finite) series expansion in the following sense. Let π be a prime element of P_i and $\omega_1, \dots, \omega_l$ a set of representatives of an \mathbb{F}_q -basis of the residue class field of P_i . We set $\tilde{\gamma} := \gamma \pi^{-v_{P_i}(a_i)}$ and then, iteratively for $v_{P_i}(a_i) \leq w \leq \tilde{n}_i$, we lift $\tilde{\gamma}(P_i)$ to $\gamma_w = \sum_{\mu=1}^l \gamma_{w,\mu} \omega_\mu$ and do $\tilde{\gamma} \leftarrow (\tilde{\gamma} - \gamma_w) / \pi$. This yields the expansion

$$\sum_{w=v_{P_i}(a_i)}^{\tilde{n}_i} \gamma_w \pi^w$$

of γ . (Here, $\tilde{\gamma}(P_i)$ denotes the residue class of $\tilde{\gamma}$ modulo P_i .)

- (iii) We construct a matrix M over \mathbb{F}_q whose columns contain the coefficients of the series expansion (as described in (ii)) of the elements of \mathcal{B} . Let $c = (c_1, \dots, c_s)$ be such that $Mc = a_i$ (from what was said above, it is clear that c exists.)
- (iv) Set $\beta := \sum_{v=1}^s c_v b_v$. □

We summarize the proof of the lemma in the following algorithm.

ALGORITHM 3.3.

Input: $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$, $P_1, \dots, P_r \in \mathcal{S}$, $a_1, \dots, a_r \in F$, $n_1, \dots, n_r \in \mathbb{Z}$.

Output: $y \in F$ such that $v_{P_i}(y - a_i) > n_i$ for all $1 \leq i \leq r$ and $v_P(y) \geq 0$ for all $P \in \mathcal{S} \setminus \{P_1, \dots, P_r\}$.

1. **for** $1 \leq i \leq r$ **do**
2. $\tilde{n}_i := n_i + 1$
3. **end for**

4. Choose a divisor A with $\deg A > 0$ whose support is disjoint to \mathcal{S} .
5. Compute $l \in \mathbb{N}$ such that $D := lA - \sum_{j=1}^r \tilde{n}_j P_j$ is non-special.
6. **for** $1 \leq i \leq r$ **do**
7. **if** $v_{P_i}(a_i) \geq \tilde{n}_i$ **then**
8. $y_i := 0$
9. **else**
10. Compute β as described in (i)–(iv) in the above proof.
11. $y_i := \beta$
12. **end if**
13. **end for**
14. **return** $y = \sum_{i=1}^r y_i$.

Proof of Theorem 3.1. We use algorithm 3.3 to compute $y \in F$ with

$$\begin{aligned} v_{P_i}(y - a_i) &> n_i & 1 \leq i \leq r, & \quad \text{and} \\ v_P(y) &\geq 0 & \text{for all } P \in \mathcal{S} \setminus \{P_1, \dots, P_r\} \end{aligned}$$

and $\tilde{y} \in F$ with

$$\begin{aligned} v_{P_i}(\tilde{y} - \pi_i^{n_i}) &> n_i & 1 \leq i \leq r, & \quad \text{and} \\ v_P(\tilde{y}) &\geq 0 & \text{for all } P \in \mathcal{S} \setminus \{P_1, \dots, P_r\}. \end{aligned}$$

The strict triangle equation then shows that the element $z := y + \tilde{y}$ satisfies definitions (3.1). \square

4. Kummer extensions

Let n be a natural number, and suppose that F contains the set μ_n of all n th roots of unity, where the characteristic of F is zero or coprime to n . A cyclic extension of F of degree n is called a *Kummer extension*. The following statements are equivalent.

- (i) E/F is a Kummer extension (of degree n).
- (ii) $E = F(y)$, where $y^n = u \in F^*$ and $u^l \neq x^n$ for all $x \in F$, $l \mid n$ and $l < n$.
- (iii) $E = F(y)$ where $y^n = u \in F^*$ and $u \neq w^d$ for all $w \in F$, $d \mid n$ and $d > 1$.

Each element $y \in E$ satisfying one of the conditions (ii) or (iii) is called a *Kummer generator* of E/F .

The following proposition helps us to determine the ramification behaviour of places in Kummer extensions of function fields.

PROPOSITION 4.1. *Let F/k be a function field and E/F a Kummer extension of degree n with generator $y \in E$ and $y^n = u \in F^*$. If P is a place of F and P' an extension of P in E , then*

$$e_E(P) := e(P'|P) = \frac{n}{r_{P,E}}, \quad (4.1)$$

where $r_{P,E} := \gcd(n, v_P(u)) > 0$.

Proof. See [9, Section 3]. □

For the rest of this section we fix a Kummer extension E of F of degree n with generator y , $y^n = u \in F$. Let $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$. The task of this section is to find a set of $\mathcal{O}_{\mathcal{S}}(F)$ generators of $\mathcal{O}_{\mathcal{S}}(E)$. Let us first consider the unramified places. We set

$$\begin{aligned} A &:= \{P \in \mathcal{S} \mid P \text{ unramified in } E/F\} \\ &= \{P \in \mathcal{S} \mid nj_P =: v_P(u) \equiv 0 \pmod{n}\} \end{aligned}$$

and $A_0 := \{P \in A \mid v_P(u) = 0 \text{ and } v_P(\delta_y) = 0\}$ (δ_y was defined in Proposition 2.5). Then

$$A \setminus A_0 = \{P \in A \mid v_P(u) \neq 0 \text{ or } v_P(\delta_y) > 0\}. \quad (4.2)$$

PROPOSITION 4.2 (\mathcal{S} -INTEGRAL \mathcal{O}_P -GENERATORS OF $\mathcal{O}_P(E)$ FOR $P \in A$).

(i) We have $y\delta_y \in \mathcal{O}_{\mathcal{S}}(E)$.

(ii) For all $P \in A_0$, we have $\mathcal{O}_P(E) = \mathcal{O}_P[y\delta_y]$.

Using strong approximation we choose $\tau \in F$ with $v_P(\tau) = -(j_P + v_P(\delta_y))$ for all $P \in A \setminus A_0$ and $v_Q(\tau) \geq 0$ for all $Q \in \mathcal{S} \setminus (A \setminus A_0)$. Then the following statements also hold.

(iii) We have $y\delta_y\tau \in \mathcal{O}_{\mathcal{S}}(E)$.

(iv) $\mathcal{O}_P(E) = \mathcal{O}_P[y\delta_y\tau]$ for all $P \in A \setminus A_0$.

Proof. Part (i) follows from Proposition 2.5. Let $P \in A_0$. Since $\chi_{(y, E/F)}(T) = T^n - u \in \mathcal{O}_P[T]$ and $v_{P'}(\chi'_{(y, E/F)}(y)) = v_{P'}(n \cdot y^{n-1}) = (n-1)v_{P'}(y) = 0$ for all $P' \in \mathbb{P}_E$ above P , Proposition 2.3(i) gives $\mathcal{O}_P(E) = \mathcal{O}_P[y]$. Since $v_P(\delta_y) = 0$ for all $P \in A_0$, this shows part (ii).

The element $\tilde{y} := y\delta_y\tau$ is a Kummer generator of E/F with $\tilde{y}^n = u\delta_y^n\tau^n =: \tilde{u}$ and minimal polynomial $\chi_{(\tilde{y}, E/F)}(T) = T^n - \tilde{u}$. Now Proposition 2.5 and the definition of τ yield $v_{Q'}(\tilde{y}) \geq 0$ for all $Q' \mid Q$, $Q \in \mathcal{S} \setminus (A \setminus A_0)$. From $v_P(\tilde{u}) = 0$ it follows that $v_{P'}(\tilde{y}) = 0$ for all $P' \in \mathbb{P}_E$ above P , $P \in A \setminus A_0$, and thus statement (iii) holds. Moreover, we get $\chi_{(\tilde{y}, E/F)}(T) \in \mathcal{O}_P[T]$ and $v_{P'}(\chi'(\tilde{y})) = v_{P'}(n \cdot \tilde{y}^{n-1}) = (n-1)v_{P'}(\tilde{y}) = 0$ for all $P' \in \mathbb{P}_E$ above P , $P \in A \setminus A_0$, and therefore (by Proposition 2.3(i)) $\mathcal{O}_P(E) = \mathcal{O}_P[\tilde{y}]$ for all $P \in A \setminus A_0$. □

Let us now consider the ramified places, that is, the set

$$B := \mathcal{S} \setminus A = \{P \in \mathcal{S} \mid v_P(u) \not\equiv 0 \pmod{n}\}.$$

We define

$$\begin{aligned} B_1 &:= \{P \in B \mid e_E(P) = n\} \\ &= \{P \in B \mid r_{P,E} = \gcd(n, v_P(u)) = 1\} \end{aligned} \quad (4.3)$$

and

$$B_2 := \{P \in B \mid 1 < e_E(P) < n\} = B \setminus B_1. \quad (4.4)$$

If $P \in B_1$, then P is totally ramified in E/F and there exist integers s_P and l_P with $l_P > 0$ such that $ns_P + l_P v_P(u) = 1$. Using strong approximation we choose $\gamma_P \in F$ satisfying

$$\begin{aligned} v_P(\gamma_P) &= s_P - l_P v_P(\delta_y) \quad \text{and} \\ v_Q(\gamma_P) &\geq 0 \quad \text{for all } Q \in \mathcal{S} \setminus \{P\}. \end{aligned} \quad (4.5)$$

PROPOSITION 4.3 (\mathcal{S} -INTEGRAL \mathcal{O}_P -GENERATORS OF $\mathcal{O}_P(E)$ FOR $P \in B_1$). *If $P \in B$ has ramification index $n = [E : F]$ (which is the case if and only if $r_{P,E} = \gcd(n, v_P(u)) = 1$) and γ_P is as in (4.5), then*

- (i) $\gamma_P(y\delta_y)^{l_P} \in \mathcal{O}_S(E)$ and
- (ii) $\mathcal{O}_P(E) = \mathcal{O}_P[\gamma_P(y\delta_y)^{l_P}]$.

Proof. Since $l_P > 0$, by Proposition 2.5 we get $v_{Q'}(\gamma_P(y\delta_y)^{l_P}) \geq 0$ for all $Q'|Q$, $Q \in \mathcal{S} \setminus \{P\}$. Moreover, if P' is the place of E above P , then $v_{P'}(\gamma_P(y\delta_y)^{l_P}) = 1$. The result now follows using Proposition 2.3(ii). \square

Suppose now that $P \in B_2$; that is, P is ramified in E with ramification index $e := e_E(P)$, where $1 < e < n$. Hence

$$r := r_{P,E} = \frac{n}{e} = \gcd(n, v_P(u)). \quad (4.6)$$

Consider the intermediate field $E_r := F(y^e)$ of E/F and let $P_{r,1}, \dots, P_{r,s}$ be all the places of E_r above P . Then E_r/F is a Kummer extension of degree r with Kummer generator y^e and defining polynomial $T^r - u$, and E/E_r is a Kummer extension of degree e with Kummer generator y and defining polynomial $T^e - y^e$. From (4.6) we get $r_{P,E_r} = \gcd(r, v_P(u)) = \gcd(n, v_P(u)) = r$, and hence (see (4.1))

$$e_{E_r}(P) = \frac{r}{r_{P,E_r}} = 1. \quad (4.7)$$

This implies that

$$e = e_E(P) = e_{E_r}(P) \cdot e_E(P_{r,i}) = e_E(P_{r,i}) \quad (4.8)$$

for each $1 \leq i \leq s$; that is, E_r is the inertia field of P in E . Let $P_{E,1}, \dots, P_{E,s}$ be all the places of E above P and $P_{E,i}|P_{r,i}$.

The unramified case (4.7) was dealt with in Proposition 4.2. Applied to our situation, this means that we take $j_P \in \mathbb{Z}$ with $v_P(u) = rj_P$, use strong approximation to choose $\tau_P \in F$ with $v_P(\tau_P) = -(j_P + v_P(\delta_{y^e}))$ and $v_Q(\tau_P) \geq 0$ for all $Q \in \mathcal{S} \setminus \{P\}$ and set

$$\alpha_P := y^e \delta_{y^e} \tau_P. \quad (4.9)$$

Proposition 4.2 then yields

$$\alpha_P \in \mathcal{O}_S(E_r) \quad \text{and} \quad \mathcal{O}_P(E_r) = \mathcal{O}_P[\alpha_P]. \quad (4.10)$$

On the other hand, the case (4.8) of total ramification was discussed in Proposition 4.3: for all $1 \leq i \leq s$ we have $v_{P_{E,i}}(y^n) = v_{P_{E,i}}(u) = ev_P(u)$ and therefore $v_{P_{r,i}}(y^e) = (v_P(u))/r$. Moreover, $1 = r_{P_{r,i},E} = \gcd(e, v_{P_{r,i}}(y^e))$. Hence there exist integers s_P and l_P with $l_P > 0$ such that $es_P + l_P(v_P(u))/r = 1$. We use strong approximation to find $\gamma_P \in F$ satisfying $v_P(\gamma_P) = s_P - l_P v_P(\delta_y)$ and $v_Q(\gamma_P) \geq 0$ for all $Q \in \mathcal{S} \setminus \{P\}$, and we define

$$\beta_P := \gamma_P(y\delta_y)^{l_P}. \quad (4.11)$$

Now $v_{P_{E,i}}(\beta_P) = 1$ for all $1 \leq i \leq s$ and, since $l_P > 0$, by Proposition 2.5 we get $v_{Q'}(\beta_P) \geq 0$ for all $Q'|Q$, $Q \in \mathcal{S} \setminus \{P\}$. By Proposition 2.3(ii) it then follows that

$$\beta_P \in \mathcal{O}_S(E) \quad \text{and} \quad \mathcal{O}_{P_{r,i}}(E) = \mathcal{O}_{P_{r,i}}[\beta_P] \quad (4.12)$$

for all $1 \leq i \leq s$. Putting together (4.10) and (4.12) we get the following proposition (by Corollary 2.2).

PROPOSITION 4.4 (\mathcal{S} -INTEGRAL \mathcal{O}_P -GENERATORS OF $\mathcal{O}_P(E)$ FOR $P \in B_2$). *Let P be in B_2 . With the notation just defined, we get*

- (i) $\alpha_P, \beta_P \in \mathcal{O}_{\mathcal{S}}(E)$ and
- (ii) $\mathcal{O}_P(E) = \mathcal{O}_P[\alpha_P, \beta_P]$. □

We are now able to give an algorithm which computes, for a Kummer extension E of a function field F and each $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$, a set of $\mathcal{O}_{\mathcal{S}}$ -generators of $\mathcal{O}_{\mathcal{S}}(E)$.

ALGORITHM 4.5.

Input: A Kummer extension E/F with generator y and $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$.

Output: A finite set Ω of $\mathcal{O}_{\mathcal{S}}$ -generators of $\mathcal{O}_{\mathcal{S}}(E)$.

1. Compute the sets $A \setminus A_0$, B_1 and B_2 (see (4.2), (4.3) and (4.4)).
2. Compute $\Omega_{A_0} := \{y\delta_y\}$, where δ_y is as in Proposition 2.5.
3. Compute τ (see Proposition 4.2) and set $\Omega_{A \setminus A_0} := \{y\delta_y\tau\}$.
4. For each $P \in B_1$ compute γ_P satisfying (4.5) and set

$$\Omega_{B_1} := \{\gamma_P(y\delta_y)^{l_P} \mid P \in B_1\}.$$

5. For each $P \in B_2$ compute α_P and β_P as in (4.9) and (4.11), respectively, and set

$$\Omega_{B_2} := \{\alpha_P, \beta_P \mid P \in B_2\}.$$

6. **return** $\Omega := \Omega_{A_0} \cup \Omega_{A \setminus A_0} \cup \Omega_{B_1} \cup \Omega_{B_2}$.

The correctness of this algorithm follows from $\mathcal{S} = A_0 \cup A \setminus A_0 \cup B_1 \cup B_2$ and Proposition 2.1. The set Ω is finite and contained in $\mathcal{O}_{\mathcal{S}}(E)$, since this is true for each of the sets Ω_{A_0} , $\Omega_{A \setminus A_0}$, Ω_{B_1} and Ω_{B_2} . (Note that $A \setminus A_0$, B_1 and B_2 are finite.)

5. Artin–Schreier–Witt extensions

Let F be a function field of characteristic $p > 0$, and let \bar{F} be the separable closure of F in some algebraic closure of F . Then \bar{F} is the maximal Galois extension of F . In this section we study cyclic extensions of degree p^n , $n \geq 1$.

We begin with the special case $n = 1$. Let $\wp : \bar{F} \rightarrow \bar{F}$ be defined by $\wp(x) := x^p - x$. Then the following assertions for a field extension E/F with $E \subseteq \bar{F}$ are equivalent.

- (1) E/F is cyclic of degree p .
- (2) $E = F(y)$, $\wp(y) = y^p - y = u \in F$ and $u \neq \alpha^p - \alpha$ for all $\alpha \in F$.

An extension for which (1) or (2) holds is called an *Artin–Schreier extension*. The elements of $\text{Gal}(E/F)$ are given by $\sigma(y) = y + \nu$, $\nu \in \mathbb{F}_p$. Each $y' \in E$ with $E = F(y')$ and $\wp(y') = y'^p - y' \in F$ is called an *Artin–Schreier generator* of E/F . An element $y' \in E$ is an Artin–Schreier generator if and only if there exist $\mu \in \mathbb{F}_p \subset F$ and $\zeta \in F$ such that $y' = \mu y + \zeta$ and $y'^p - y' = u' = \mu u + (\zeta^p - \zeta)$; that is, if and only if $y' \in \wp^{-1}(u')$ with $u' \in F$ and $u' - \mu u \in \wp(F)$ for some $\mu \in \mathbb{F}_p$. The minimal polynomial of y' over F is $T^p - T - u' \in F[T]$.

PROPOSITION 5.1. *Let F/k be a function field of characteristic $p > 0$, k perfect and $P \in \mathbb{P}_F$ a place of F .*

(i) *For each $u \in F$ we can define a unique*

$$\lambda_P(u) := \begin{cases} \lambda & \text{if there exists an element } \zeta := \zeta(P, u) \in F \text{ with} \\ & v_P(u + (\zeta^p - \zeta)) = -\lambda < 0, \lambda \not\equiv 0 \pmod{p} \\ 0 & \text{if there exists an element } \zeta := \zeta(P, u) \in F \text{ with} \\ & v_P(u + (\zeta^p - \zeta)) \geq 0. \end{cases}$$

(ii) *If E/F is an Artin–Schreier extension and $y \in E$ an Artin–Schreier generator of E/F with $\wp(y) = u \in F$, then*

- *P is unramified in E if and only if $\lambda_P(u) = 0$, and*
- *P is totally ramified in E if and only if $\lambda_P(u) > 0$.*

Moreover, from (i) it follows that, if y' is another Artin–Schreier generator of E/F with $\wp(y') = u' \in F$, then $\lambda_P(u) = \lambda_P(u')$.

Proof. See [14, III.7.7 and III.7.8]. □

For later applications it will be important to compute $\lambda_P(u)$ from Proposition 5.1(i). We describe the procedure for doing this in the following algorithm. We retain the notation of Proposition 5.1.

ALGORITHM 5.2. *Reduction-AS*

Input: $P \in \mathbb{P}_F$, $u \in F$, $\text{char } F = p > 0$.

Output: $\zeta := \zeta(P, u) \in F$ and $\lambda = \lambda_P(u) \in \mathbb{Z}$ (see Proposition 5.1(i)) with either
 $v_P(u + (\zeta^p - \zeta)) \geq 0$ (in this case $\lambda := 0$)
 or
 $v_P(u + (\zeta^p - \zeta)) = -\lambda < 0$, $\lambda \not\equiv 0 \pmod{p}$.

1. $\zeta \leftarrow 0$, $\lambda \leftarrow v_P(u)$, $x \leftarrow u$
2. **while** $\lambda < 0$ **and** $\lambda \equiv 0 \pmod{p}$ **do**
3. $l \leftarrow \lambda/p$
4. Choose $t \in F$ with $v_P(t) = l$.

5. Choose $\alpha \in \mathcal{O}_P^*$ with

$$\frac{x}{t^p} + P = (\alpha + P)^p = \alpha^p + P. \quad (5.1)$$

(In the paragraph following the statement of this algorithm we show how to find α .)

6. $\zeta \leftarrow \zeta - \alpha t$

7. $x \leftarrow u + (\zeta^p - \zeta)$

8. $\lambda \leftarrow v_P(x)$

9. **end while**

10. **if** $\lambda < 0$ **then**

11. $\lambda := -\lambda$

12. **else**

13. $\lambda := 0$

14. **end if**

15. **return** ζ, λ .

We proceed by showing the correctness of this algorithm (following the proof of [14, III.7.7]). First we note that $x = u + (\zeta^p - \zeta)$ and t^p are non-zero. Since $v_P(t^p) = v_P(x)$, we have $v_P(x/t^p) = 0$; hence $0 \neq x/t^p + P \in \mathcal{O}_P/P$. Then there exists an $\alpha \in \mathcal{O}_P$ satisfying (5.1), since \mathcal{O}_P/P is perfect. Moreover, $\alpha \in \mathcal{O}_P^*$ since $v_P(\alpha^p) = v_P(x/t^p) = 0$.

Now (5.1) implies $(x/t^p - \alpha^p) \in P$; that is, $v_P(x/t^p - \alpha^p) > 0$. This implies that

$$v_P(x - (\alpha t)^p) > v_P(t^p) = \lambda. \quad (5.2)$$

It now remains to show that

$$\begin{aligned} v_P(u + ((\zeta - \alpha t)^p - (\zeta - \alpha t))) &> v_P(u + (\zeta^p - \zeta)) \\ &= v_P(x) = \lambda, \end{aligned} \quad (5.3)$$

because it follows that λ strictly increases in every step of the ‘while’ loop, and so the algorithm terminates with the correct result. Since

$$\begin{aligned} v_P(u + ((\zeta - \alpha t)^p - (\zeta - \alpha t))) &= v_P(u + (\zeta^p - \zeta) - ((\alpha t)^p - \alpha t)) \\ &= v_P(x - ((\alpha t)^p - \alpha t)), \end{aligned}$$

(5.3) follows from $v_P(\alpha t) = v_P(t) = l > lp = \lambda$ and (5.2). (Note that during the ‘while’ loop, λ — and therefore l — is negative.)

We now generalize the above to powers of p . Let n be a fixed natural number. For a field L we denote by $W_n(L)$ the ring of Witt vectors over L of length n . We define the homomorphism

$$\wp : W_n(\bar{F}) \longrightarrow W_n(\bar{F}), \quad (x_1, \dots, x_n) \longmapsto (x_1^p, \dots, x_n^p) - (x_1, \dots, x_n). \quad (5.4)$$

The proofs of the following two statements can be found in [11] or [4].

THEOREM 5.3. *The following statements are equivalent.*

(i) E/F is a cyclic extension of degree p^n .

(ii) $E = F(y)$ for some $y \in W_n(\bar{F})$, where $\wp(y) = u \in W_n(F)$ and $p^{n-1}u \notin \wp(W_n(F))$.

(iii) $E = F(y)$ for some $y \in W_n(\bar{F})$, where $u = (u_1, \dots, u_n) \in W_n(F)$ with $\wp(y) = u$ and $u_1 \neq \alpha^p - \alpha$ for all $\alpha \in F$.

(Here, $F(y)$ is the subfield of \bar{F} which is obtained by adjoining all the coordinates of y to F .) An extension E of F satisfying the above conditions is called an Artin–Schreier–Witt extension and y an Artin–Schreier–Witt generator of E/F .

PROPOSITION 5.4. *Suppose that E/F is an Artin–Schreier–Witt extension with generator $y \in \wp^{-1}(u)$ for some $u \in W_n(F)$. Then, for $y' \in W_n(\bar{F})$, the following assertions are equivalent.*

(i) y' is an Artin–Schreier–Witt generator of E/F .

(ii) $y' \in \wp^{-1}(u')$ with $u' \in W_n(F)$ and $u' - \lambda u \in \wp(W_n(F))$ for some $\lambda \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

(iii) $y' = \lambda y + \zeta$ for some $\lambda \in (\mathbb{Z}/p^n\mathbb{Z})^*$ and $\zeta \in W_n(F)$.

For the rest of this section we fix an Artin–Schreier–Witt extension E/F with generator $y = (y_1, \dots, y_n) \in \wp^{-1}(u)$ for some $u \in W_n(F)$. We set $E_0 := F$, $E_n := E$ and $E_i := F(y_1, \dots, y_i)$ for each $1 \leq i \leq n$. Note that, since E_i/F is cyclic, E_1, \dots, E_{i-1} are the only intermediate fields of E_i/F , and therefore $E_i = F(y_1, \dots, y_i) = F(y_i)$.

REMARK 5.5. We have the following recursive formulas:

$$\begin{aligned} u_1 &= y_1^p - y_1, \\ u_2 &= y_2^p - y_2 - z_1, \\ &\vdots \\ u_n &= y_n^p - y_n - z_{n-1}, \end{aligned}$$

where $z_0 = 0$ and $z_i \in E_i$ are polynomial expressions in y_l, u_l and z_{l-1} ($1 \leq l \leq i$) with coefficients in the prime field of F (see, for instance, [13]). Each extension E_i/E_{i-1} is an Artin–Schreier extension with generator y_i .

Let $\emptyset \neq \mathcal{S} \subseteq \mathbb{P}_F$. Now we have all the necessary tools to compute a set of generators of $\mathcal{O}_{\mathcal{S}}(E)$ over $\mathcal{O}_{\mathcal{S}}$. We will give a brief survey of the rest of this section. Let $P \in \mathbb{P}_F$. We begin by defining a vector $\Lambda_P \in \mathbb{Z}^n$, a vector $\zeta_P \in W_n(F)$ and a natural number t_P which will give us information about the ramification behaviour of P in E . We use these vectors to split \mathcal{S} in finitely many disjoint subsets. Then we compute for each P in each of these sets a set of \mathcal{S} -integral generators of $\mathcal{O}_P(E)$ over \mathcal{O}_P . As mentioned above, Proposition 2.1 then guarantees that the set Ω , which consists of all these generators and will turn out to be finite, has the desired properties.

We define Λ_P, ζ_P and t_P with the following algorithm, which essentially applies the reduction algorithm 5.2 successively to the coordinates of the vector $u \in W_n(F)$.

ALGORITHM 5.6. *Reduction-ASW*

Input: $P \in \mathbb{P}_F$.

Output: $\zeta_P \in W_n(F)$, $\Lambda_P \in \mathbb{Z}^n$ and $t_P \in \mathbb{N}$.

1. $\zeta_P \leftarrow (0, \dots, 0)$, $\Lambda_P \leftarrow (0, \dots, 0)$, $\lambda \leftarrow 0$, $i \leftarrow 0$
2. **while** $\lambda = 0$ **and** $i < n$ **do**
3. $i \leftarrow i + 1$
4. $\zeta, \lambda \leftarrow \text{Reduction-AS}(P, u_i)$
5. $u \leftarrow u + \wp(Z)$, where $Z \in W_n(F)$ is given by

$$Z_j = \begin{cases} \zeta & j = i \\ 0 & \text{else} \end{cases}$$

6. $(\zeta_P)_i \leftarrow \zeta$
7. **end while**
8. $(\Lambda_P)_i \leftarrow \lambda$
9. **if** $i = n$ **and** $\lambda = 0$ **then**
10. $t_P \leftarrow n$
11. **else**
12. $t_P \leftarrow i - 1$
13. **end if**
14. **return** ζ_P, Λ_P, t_P

The new Artin–Schreier–Witt generator of E/F which is obtained by the above procedure is

$$y_P := y + \zeta_P \tag{5.5}$$

with

$$u_P := \wp(y_P) = u + \wp(\zeta_P); \tag{5.6}$$

that is, $E_j = E_{j-1}((y_P)_j)$ and

$$(y_P)_j^p - (y_P)_j = (u_P)_j + z_{P,j-1},$$

where $z_{P,j-1} \in E_{j-1}$ is as in Remark 5.5.

REMARK 5.7. Let $P \in \mathbb{P}_F$.

(i) We denote by P_j an arbitrary place of E_j over P . Since the E_j ($0 \leq j \leq n$) are the only subfields of E_n , the inertia field of P_n over P equals E_t for some $0 \leq t \leq n$. We claim that

$$t = t_P. \tag{5.7}$$

From Proposition 5.1 we know that P_{j-1} is unramified in E_j/E_{j-1} if and only if $\lambda_{P_{j-1}}((u_P)_j + z_{P,j-1}) = 0$. Therefore we will have established (5.7) if we show that

$$(\Lambda_P)_j = \lambda_{P_{j-1}}((u_P)_j + z_{P,j-1}) \quad \text{for } 1 \leq j \leq t + 1. \tag{5.8}$$

Since $(\Lambda_P)_1 = \dots = (\Lambda_P)_t = 0$ and $z_{P,j-1}$ is a polynomial expression in $(y_P)_l$, $(u_P)_l$ and $z_{P,l-1}$ ($1 \leq l < j-1$) with coefficients in the prime field of F , we have

$$v_{P_{j-1}}(z_{P,j-1}) \geq 0, \quad 1 \leq j \leq t+1. \quad (5.9)$$

For $1 \leq j \leq t$ we have $(\Lambda_P)_j = 0$ and $v_P((u_P)_j) \geq 0$. Therefore

$$v_{P_{j-1}}((u_P)_j + z_{P,j-1}) \geq 0 \quad (5.10)$$

and thus $\lambda_{P_{j-1}}((u_P)_j + z_{P,j-1}) = 0$. It follows that P is unramified in E_t/E .

On the other hand, if $t < n$ and $j = t+1$ (that is, $v_P((u_P)_{t+1}) = -(\Lambda_P)_{t+1} < 0$), then strict triangularity and (5.9) yield

$$v_{P_t}((u_P)_{t+1} + z_{P,t}) = v_{P_t}((u_P)_{t+1}) = v_P((u_P)_{t+1}) \quad (5.11)$$

and we have proved (5.8) and hence (5.7).

(ii) For each $1 \leq i \leq t_P$ consider the minimal polynomial

$$\chi_i(T) := \chi_{((y_P)_i, E_i/E_{i-1})}(T) = T^p - T - ((u_P)_i + z_{P,i-1})$$

of $(y_P)_i \in E_i$ over E_{i-1} . For each $P_{i-1} \in \mathbb{P}_{E_{i-1}}$ with $P_{i-1}|P$ we know from (5.10) that $\chi_i(T) \in \mathcal{O}_{P_{i-1}}[T]$. This implies that for each $1 \leq i \leq t_P$ the element $(y_P)_i$ is integral at P . Moreover, $v_{P_i}(\chi'_i((y_P)_i)) = 0$ for all $P_i \in \mathbb{P}(E_i)$ with $P_i|P_{i-1}$. Proposition 2.3(i) then yields

$$\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}[(y_P)_i]. \quad \square$$

For later reference we note the following: since $P_{t+1}|P_t$ is totally ramified and $P_t|P$ is unramified, we have

$$\begin{aligned} 0 > p \cdot v_{P_t}((u_P)_{t+1} + z_{P,t}) &= v_{P_{t+1}}((u_P)_{t+1} + z_{P,t}) \\ &\geq \min\{v_{P_{t+1}}((y_P)_{t+1}^p), v_{P_{t+1}}((y_P)_{t+1})\} \\ &= p \cdot v_{P_{t+1}}((y_P)_{t+1}); \end{aligned}$$

that is, (together with (5.11))

$$-(\Lambda_P)_{t+1} = v_P((u_P)_{t+1}) = v_{P_t}((u_P)_{t+1} + z_{P,t}) = v_{P_{t+1}}((y_P)_{t+1}). \quad (5.12)$$

Note that all the above expressions do not depend on the choice of the place P_j over P for all $1 \leq j \leq t+1$.

We now split \mathcal{S} into subsets. We define

$$\begin{aligned} A &:= \{P \in \mathcal{S} \mid v_P(u_i) \geq 0 \text{ for all } 1 \leq i \leq n\}, \\ B &:= B_{n+1} := \{P \in \mathcal{S} \setminus A \mid t_P = n\} \\ &= \{P \in \mathcal{S} \setminus A \mid (\Lambda_P)_i = 0 \text{ for all } 1 \leq i \leq n\}, \end{aligned}$$

and for $1 \leq j \leq n$,

$$\begin{aligned} B_j &:= \{P \in \mathcal{S} \mid t_P = j-1\} \\ &= \{P \in \mathcal{S} \mid (\Lambda_P)_i = 0 \text{ for } 1 \leq i < j \text{ and } (\Lambda_P)_j > 0\}. \end{aligned}$$

Note that all the above sets are pairwise disjoint, their union equals \mathcal{S} and that $A \cup B$ equals the set of places of \mathcal{S} which are unramified in E/F . Moreover, $\bar{A} := \mathcal{S} \setminus A = \bigcup_{j=1}^{n+1} B_j$.

REMARK 5.8. The sets B_1, \dots, B_{n+1} can be computed in the following way:

- Compute, for each $1 \leq i \leq n$,

$$\begin{aligned} \bar{A}_i &:= \{P \in \mathcal{S} \mid v_P(u_i) < 0 \text{ and } v_P(u_j) \geq 0 \text{ for all } 1 \leq j < i\} \\ &= \{P \in \mathcal{S} \mid v_P(u_i) < 0 \text{ and } P \notin \bar{A}_j \text{ for all } 1 \leq j < i\}. \end{aligned}$$

These sets are also pairwise disjoint and their union equals \bar{A} . Moreover, they can easily be derived from the vector u .

- For each $P \in \bar{A}_l$, $1 \leq l \leq n$, compute t_P using algorithm 5.6.

For each P we can now also compute y_P and u_P as in (5.5) and (5.6). Of course, $y_P = y$ and $u_P = u$ for all $P \in A$.

In the following propositions we will show how to compute \mathcal{S} -integral generators of $\mathcal{O}_P(E)$ over \mathcal{O}_P successively for the places P in the sets A, B_1, \dots, B_{n+1} .

Using the definition in Proposition 2.5 we define the following subset of A :

$$A' := \{P \in A \mid v_P(\delta_{y_i}) > 0 \text{ for some } 1 \leq i \leq n\}. \quad (5.13)$$

PROPOSITION 5.9. *Let $\Omega_{A \setminus A'} := \{y_i \delta_{y_i} \mid 1 \leq i \leq n\}$. Then*

- $y_i \delta_{y_i} \in \mathcal{O}_{\mathcal{S}}(E)$ for each $1 \leq i \leq n$;
- for all $P \in A \setminus A'$ we have $\mathcal{O}_P(E) = \mathcal{O}_P[\Omega_{A \setminus A'}]$.

Proof. Part (i) follows from Proposition 2.5. Let $P \in A \setminus A'$. For all $1 \leq i \leq n$ we have $v_P(\delta_{y_i}) = 0$, and hence δ_{y_i} is a unit in \mathcal{O}_P . Therefore (by Remark 5.7(ii)) $\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}[y_i \delta_{y_i}]$ for each place P_{i-1} of E_{i-1} over P . Part (ii) then follows from Corollary 2.2. \square

PROPOSITION 5.10. *Let $P \in A' \cup B_1 \cup \dots \cup B_{n+1}$. For each $1 \leq i \leq t_P$ we use strong approximation to find $\gamma_{P,i} \in F$ with $v_P(\gamma_{P,i}) = -v_P(\delta_{(y_P)_i})$ and $v_Q(\gamma_{P,i}) \geq 0$ for all $Q \in \mathcal{S} \setminus \{P\}$. Then*

- $(y_P)_i \delta_{(y_P)_i} \gamma_{P,i} \in \mathcal{O}_{\mathcal{S}}(E)$ for each $1 \leq i \leq t_P$;
- $\mathcal{O}_P(E_{t_P}) = \mathcal{O}_P[\tilde{\Omega}_P]$, where $\tilde{\Omega}_P := \{(y_P)_i \delta_{(y_P)_i} \gamma_{P,i} \mid 1 \leq i \leq t_P\}$.

In particular, for $P \in A' \cup B$ we have $\mathcal{O}_P(E) = \mathcal{O}_P[\Omega_P]$, where $\Omega_P := \tilde{\Omega}_P$.

Proof. Part (i) follows from Proposition 2.5. For part (ii) we use the same argument as in the proof of Proposition 5.9(ii): for each $1 \leq i \leq t_P$ we have $v_P(\delta_{(y_P)_i} \gamma_{P,i}) = 0$; hence $\delta_{(y_P)_i} \gamma_{P,i}$ is a unit in \mathcal{O}_P . From Remark 5.7(ii) we then get $\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}[\delta_{(y_P)_i} \gamma_{P,i}]$ for each place P_{i-1} of E_{i-1} over P , and the result follows, by Corollary 2.2. \square

PROPOSITION 5.11. *Let $P \in B_n$. Since for all $P_n \in \mathbb{P}_{E_n}$ with $P_n | P$ we have $v_{P_n}((y_P)_n) = -(\Lambda_P)_n \not\equiv 0 \pmod{p}$ (which was shown in (5.12)), there exist l_P and $s_P \in \mathbb{Z}^{\geq 0}$ such that $s_P \cdot p - l_P \cdot (\Lambda_P)_n = 1$. Using strong approximation we choose $\theta_{P,n} \in F$ with $v_P(\theta_{P,n}) = s_P - l_P \cdot v_P(\delta_{(y_P)_n})$ and $v_Q(\theta_{P,n}) \geq 0$ for all $Q \in \mathcal{S} \setminus \{P\}$. Then*

- $\theta_{P,n} ((y_P)_n \delta_{(y_P)_n})^{l_P} \in \mathcal{O}_{\mathcal{S}}(E)$;
- $\mathcal{O}_P(E_n) = \mathcal{O}_P[\Omega_P]$, where $\Omega_P := \tilde{\Omega}_P \cup \{((y_P)_n \delta_{(y_P)_n})^{l_P} \theta_{P,n}\}$.

Proof. (i) Since $l_P \geq 0$, it follows from Proposition 2.5 and the definition of $\theta_{P,n}$ that $v_{Q'}(\theta_{P,n}((y_P)_n \delta_{(y_P)_n})^{l_P}) \geq 0$ for all places Q' of E over Q with $Q \in \mathcal{S} \setminus \{P\}$. Moreover, $v_{P_n}(\theta_{P,n}((y_P)_n \delta_{(y_P)_n})^{l_P}) = 1$ for all places P_n of E over P . This gives part (i) and (using Proposition 2.3(ii)) we have

$$\mathcal{O}_{P_t}(E_n) = \mathcal{O}_{P_t} \left[\theta_{P,n}((y_P)_n \delta_{(y_P)_n})^{l_P} \right] \quad (5.14)$$

for all $P_t \in \mathbb{P}_{E_t}$ with $P_t|P$. Part (ii) follows with Corollary 2.2 from (5.14) and Proposition 5.10. \square

We are now left with the task of finding a set of generators for $\mathcal{O}_P(E)$, $P \in B_r$, $1 \leq r < n$. Let $P_{t_P,1}, \dots, P_{t_P,r}$ be all the places of E_{t_P} , $P_{n-1,1}, \dots, P_{n-1,r}$ be all the places of E_{n-1} and $P_{n,1}, \dots, P_{n,r}$ be all the places of E_n above P with $P_{n,j}|P_{n-1,j}|P_{t_P,j}$. We recall from Remark 5.5 that for the generator y_n of the Artin-Schreier extension E_n/E_{n-1} , it holds that $y_n^p - y_n = u_n + z_{n-1} \in E_{n-1}$. Since each $P_{n-1,j}$ is totally ramified in E_n/E_{n-1} , there exists an element $\rho_{P,j}$ of E_{n-1} such that

$$v_{P_{n-1,j}}(u_n + z_{n-1} + (\rho_{P,j}^p - \rho_{P,j})) = \lambda_{P_{n-1,j}}(u_n + z_{n-1}) =: -m_{P,j} < 0$$

with $m_{P,j} \not\equiv 0 \pmod{p}$ (see Proposition 5.1). Therefore we can choose $l_{P,j}$ and $s_{P,j} \in \mathbb{Z}^{\geq 0}$ such that $s_{P,j} \cdot p^{n-t_P} - l_{P,j} \cdot m_{P,j} = 1$. (Note that $p^{n-t_P} = e(P_{n,j}|P_{t_P,j}) = e(P_{n,j}|P)$.) Now $y_n + \rho_{P,j}$ is an Artin-Schreier generator of E_n/E_{n-1} with

$$(y_n + \rho_{P,j})^p - (y_n + \rho_{P,j}) = u_n + z_{n-1} + (\rho_{P,j}^p - \rho_{P,j})$$

and

$$v_{P_{n,j}}(y_n + \rho_{P,j}) = \frac{1}{p} \cdot v_{P_{n,j}}(u_n + z_{n-1} + (\rho_{P,j}^p - \rho_{P,j})) = -m_{P,j}.$$

Select $\theta_{P,n,j} \in F$ with

$$\begin{aligned} v_P(\theta_{P,n,j}) &= s_{P,j} - l_{P,j} \cdot v_P(\delta_{(y_n + \rho_{P,j})}) \quad \text{and} \\ v_Q(\theta_{P,n,j}) &\geq 0 \quad \text{for all } Q \in \mathcal{S}, Q \neq P. \end{aligned}$$

PROPOSITION 5.12. *Suppose that we are in the situation just described. Then*

- (i) $\theta_{P,n,j}((y_n + \rho_{P,j})\delta_{(y_n + \rho_{P,j})})^{l_{P,j}} \in \mathcal{O}_{\mathcal{S}}(E)$ for all $1 \leq j \leq r$;
- (ii) $\mathcal{O}_P(E_n) = \mathcal{O}_P[\Omega_P]$, where

$$\Omega_P := \tilde{\Omega}_P \cup \left\{ ((y_n + \rho_{P,j})\delta_{(y_n + \rho_{P,j})}\theta_{P,n,j})^{l_{P,j}} \mid 1 \leq j \leq r \right\}.$$

Proof. This is similar to the proof of Proposition 5.11. For all $1 \leq j \leq r$, we get

$$v_{Q'} \left(\theta_{P,n,j}((y_n + \rho_{P,j})\delta_{(y_n + \rho_{P,j})})^{l_{P,j}} \right) \geq 0$$

for all places Q' of E over Q with $Q \in \mathcal{S} \setminus \{P\}$ and

$$v_{P_{n,j}} \left(\theta_{P,n,j}((y_n + \rho_{P,j})\delta_{(y_n + \rho_{P,j})})^{l_{P,j}} \right) = 1.$$

This gives part (i) and

$$\mathcal{O}_{P_{t_P,j}}(E_n) = \mathcal{O}_{P_{t_P,j}} \left[\theta_{P,n,j}((y_n + \rho_{P,j})\delta_{(y_n + \rho_{P,j})})^{l_{P,j}} \right] \quad (5.15)$$

for all $1 \leq j \leq r$.

Part (ii) follows using Corollary 2.2 from (5.15) and Proposition 5.10. \square

To finish this section we now summarize the above results and give an algorithm which computes, for an Artin–Schreier–Witt extension E of a function field F and each $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$, a set of $\mathcal{O}_{\mathcal{S}}$ -generators of $\mathcal{O}_{\mathcal{S}}(E)$.

ALGORITHM 5.13.

Input: An Artin–Schreier–Witt extension E/F with generator y and $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$.

Output: A finite set Ω of $\mathcal{O}_{\mathcal{S}}$ -generators of $\mathcal{O}_{\mathcal{S}}(E)$.

1. Compute the set A' (see (5.13)).
2. Compute the sets B_1, \dots, B_{n+1} (see Remark 5.8).
3. Compute $\Omega_{A \setminus A'}$ as in Proposition 5.9.
4. For each $P \in A' \cup B$ compute Ω_P (see Proposition 5.10) and

$$\Omega_{A' \cup B} := \bigcup_{P \in A' \cup B} \Omega_P.$$

5. For each $1 \leq i \leq n$ and each $P \in B_i$ compute Ω_P (see Propositions 5.11 and 5.12) and set

$$\Omega_{B_i} := \bigcup_{P \in B_i} \Omega_P.$$

6. **return** $\Omega := \Omega_{A \setminus A'} \cup \Omega_{A' \cup B} \cup \Omega_{B_1} \cup \dots \cup \Omega_{B_n}$.

The correctness of this algorithm follows from $\mathcal{S} = A \setminus A' \cup A' \cup B \cup B_1 \cup \dots \cup B_n$ and Proposition 2.1. We have shown that the sets $\Omega_{A \setminus A'}$, $\Omega_{A' \cup B}$ and Ω_{B_i} , $1 \leq i \leq n$, are contained in $\mathcal{O}_{\mathcal{S}}(E)$. They are finite since A' , B and B_i , $1 \leq i \leq n$, are finite. Therefore Ω is a finite subset of $\mathcal{O}_{\mathcal{S}}(E)$.

6. Examples

The set of places of the rational function field $k(x)/k$ consists of the *infinite* place $P_{\infty} := \{g/h \mid g, h \in k[x], \deg g < \deg h\}$ and the *finite* places $P_{\pi} := \{g/h \mid g, h \in k[x], h \neq 0, \pi \mid g, \pi \nmid h\}$, $\pi \in k[x]$ irreducible. Let F be a global function field, and let \mathcal{S} be the set of places of F lying above the finite places.

In this final section we examine a list of examples and compare our method to compute the finite maximal order $\mathcal{O}_E := \mathcal{O}_{\mathcal{S}}(E)$ of a Kummer or Artin–Schreier–Witt extension E of F with the Round-2-based method (see for instance [12], [5] and [6]). A comparison of the complexity analysis of the two approaches is beyond the scope of this paper since the complexity of the ideal arithmetic in relative extensions has yet to be analyzed. What we can say is that our method uses only linear algebra over \mathbb{F}_q , whereas the Round-2 algorithm needs $\mathbb{F}_q[t]$.

We use the following notation. We denote by T_1 the time that our algorithm needed for the computation (all times are given in seconds), and by T_2 the time which the Round-2 algorithm needed to compute \mathcal{O}_E as an overorder of $\mathcal{O}_{E,eq}$, where $\mathcal{O}_{E,eq}$ is defined in the following way. Let F/k be a function field with finite maximal order \mathcal{O}_F and let $E = F(y)$, $g(y) = 0$ for some irreducible polynomial

$$g(t) = t^n + \frac{a_{n-1}}{b_{n-1}}t^{n-1} + \dots + \frac{a_0}{b_0} \in F[t],$$

where $a_i, b_i \in \mathcal{O}_F$. If d is a (lowest) common multiple of b_0, \dots, b_{n-1} , then dy is a zero of the irreducible polynomial

$$(dt)^n + \frac{a_{n-1}}{b_{n-1}}d(dt)^{n-1} + \dots + \frac{a_0}{b_0}d^n,$$

which has coefficients in \mathcal{O}_F . We set $\mathcal{O}_{E,eq} := \mathcal{O}_F[dy]$. Since in our cases the index of \mathcal{O}_E over $\mathcal{O}_{E,eq}$ is an ideal which has prime factors of fairly high degree, this method soon reaches its limits. To overcome this problem and get more realistic times with which to compare our algorithm, in most of the examples we also include the time T_3 , which the Round-2 algorithm needed to compute \mathcal{O}_E as an overorder of another order $\mathcal{O}_{E,1} \supseteq \mathcal{O}_{E,eq}$, whose index in \mathcal{O}_E has fewer prime factors with smaller powers. To get $\mathcal{O}_{E,1}$, we set $h := gd/(t - y) \in E[t]$. Then g is a polynomial with coefficients $\beta_0, \dots, \beta_{n-1} \in \mathcal{O}_E$ and

$$\mathcal{O}_{E,1} := \mathcal{O}_F[\beta_0, \dots, \beta_{n-1}]$$

is an overorder of $\mathcal{O}_{E,eq}$ (see [1, p. 88]).

We write ‘???’ in the cases where the computation of the maximal order was not finished after more than two days. All computations have been carried out using the computer algebra system MAGMA V2.11 [2] on a Pentium IV, 2.8 GHz, 1024 MB-RAM.

6.1. Kummer extensions

Here we look at some examples of Kummer extensions E/F . We examine the runtime of both methods with increasing degree n of the extension E/F , where E and F are defined in the following way. We start with the field k of $p = 3$ elements, adjoin a primitive n th root of unity to k to get the field \mathbb{F}_q , q a power of p , and construct $F = \mathbb{F}_q(x, \rho)$ with $\rho^2 + 2\rho + x^3 + x + 1 = 0$. The field $E = F(y)$ is then the Kummer extension given by $y^n - ((1/x^2)\rho + x^2) = 0$. See Table 1.

Table 1: Examples of Kummer extensions.

n	q	T_1	T_2	T_3
28	3^6	5	2581	539
31	3^{30}	14	15989	4160
40	3^4	15	6894	1720
61	3^{10}	37	???	29264
100	3^{20}	975	???	???
122	3^{10}	367	???	???
140	3^{12}	1751	???	???
160	3^8	3276	???	???

6.2. Artin–Schreier–Witt extensions

We begin by presenting a small example in detail. Let $F = \mathbb{F}_5(x, \rho)$, where $\rho^3 - \rho^2 + 2x\rho - x^4 = 0$, and let $E = F(y)$ be the Artin–Schreier extension with

$$y^p - y = \frac{4}{x^5}\rho^2 + \frac{x^2 + 4x + 2}{x^4}\rho + \frac{4}{x} =: u.$$

Then $P_1 := (x, 4\rho + 1)$ is the only finite place of F where u has a negative valuation, $v_{P_1}(u) = -5$. (Note that every place has a two-element representation; see for instance [12, Theorem 5.39(d)].) Therefore $A = \mathcal{S} \setminus \{P_1\}$. We compute $\delta_y = x^5$ (see Proposition 2.5) and get $\Omega_{A \setminus A'} = \{yx^5\}$ (Proposition 5.9) and

$$A' = \left\{ \left(x, \frac{3}{x}\rho^2 + \frac{x+2}{x}\rho + 1 \right), \left(x, \frac{2}{x}\rho^2 + \frac{3}{x}\rho + x \right) \right\}$$

(see (5.13)).

Now we calculate B and B_1 using Algorithm 5.6 (see Remark 5.8). In our case this essentially means applying the reduction algorithm 5.2 to (P_1, u) . This yields $\zeta = (1/x)\rho$ and $v_{P_1}(u + (\zeta^p - \zeta)) = -4 \not\equiv 0 \pmod{5}$. Therefore $B_1 = \{P_1\}$ and $B = \emptyset$.

We finish the example by computing (see Proposition 5.10)

$$\Omega_{A' \cup B} = \left\{ yx^5 \frac{3(\rho+2)(\rho+3)(\rho^2+(2x+4)\rho+x^2)}{(x+2)x(\rho^2+(2x+4)\rho+4x^3+x^2+2x)}, yx^5 \frac{(\rho+2)(\rho+3)(\rho+2x+4)(\rho+3x)}{(x+2)x(\rho^2+4\rho+3x^3)} \right\}$$

and (using Proposition 5.11)

$$\Omega_{B_1} = \{(4x\rho^2 + 2x^2\rho)y + (2x + 4)\rho^2 + 2x\rho + 4x^4\}.$$

Next we compute the finite maximal order of different Artin–Schreier extensions E/F . In every step we increase the degree p of the extension. The fields E and F are defined in the following way: $F = \mathbb{F}_p(x, \rho)$ is the extension of $\mathbb{F}_p(x)$ given by $\rho^3 - (x + 1)\rho^2 + 2x\rho - x^5 = 0$ and $E = F(y)$ is the Artin–Schreier extension with

$$y^p - y = \frac{x^5}{x^3 - 1}\rho^2 + \frac{x^6 + x^2 + 1}{x^6 - 1}\rho + \frac{1}{x^5}.$$

See Table 2.

Table 2: Examples of Artin–Schreier–Witt extensions of degree p .

p	T_1	T_2	T_3
5	3	22	16
7	4	77	18
11	5	499	63
13	9	1141	192
23	20	15073	1829
31	36	57512	4240
53	475	691322	35290
61	300	???	79350
71	488	???	???
83	1859	???	???
97	62226	???	???

In the last group of examples we compute the finite maximal order of Artin–Schreier–Witt extensions E/F of degree p^2 for $p = 3, 5, 7$ and p^3 for $p = 2, 3$, respectively. Here $\wp : W_n(\bar{F}) \rightarrow W_n(\bar{F})$, $n = 2, 3$, is the Artin–Schreier–Witt map which was defined in (5.4); see Tables 3 and 4.

Table 3: Examples of Artin–Schreier–Witt extensions of degree p^2 .

$p = 3$	$F = \mathbb{F}_p(x, \rho)$, where $\rho^2 + x^3 + x + 1 = 0$ $E = F((y_1, y_2))$: $\wp((y_1, y_2)) = (\frac{1}{x^2}\rho + x^2, \frac{1}{x-1}\rho + x)$	T1 = 3	T2 = 33
$p = 5$	$F = \mathbb{F}_p(x, \rho)$, where $\rho^2 + x^3 + x + 1 = 0$ $E = F((y_1, y_2))$: $\wp((y_1, y_2)) = (\frac{1}{x^2+3}\rho + x^2, \frac{1}{x-1}\rho + x)$	T1 = 658	T2 = 2175
$p = 7$	$F = \mathbb{F}_p(x, \rho)$, where $\rho^2 + x^3 + x + 1 = 0$ $E = F((y_1, y_2))$: $\wp((y_1, y_2)) = (\frac{1}{x^2+3}\rho + x^2, \frac{1}{x-1}\rho + x)$	T1 = 542	T2 = ???

Table 4: Examples of Artin–Schreier–Witt extensions of degree p^3 .

$p = 2$ T1 = 451 T2 = ???	$F = \mathbb{F}_p(x, \rho)$, where $\rho^3 - \rho^2 + 2x\rho - x^5 = 0$ $E = F((y_1, y_2, y_3))$: $\wp((y_1, y_2, y_3)) = ((x + 1)\rho^2 + \frac{1}{x^2+1}\rho + x^2, (x^3 + x^2)\rho^2 + \frac{1}{x+1}\rho + x, \frac{1}{x^2+1}\rho^2 + (x^6 + 1)\rho + \frac{1}{x^{12}})$
$p = 3$ T1 = 34586 T2 = ???	$F = \mathbb{F}_p(x, \rho)$, where $\rho^2 + x^3 + x + 1 = 0$ $E = F((y_1, y_2, y_3))$: $\wp((y_1, y_2, y_3)) = ((x + 2)\rho + \frac{1}{x^2}, (x^3 + x^2)\rho + \frac{1}{x+2}, \frac{1}{x^2}\rho + x^6 + 2)$

References

1. J. P. BUHLER, H. W. LENSTRA, JR. and CARL POMERANCE, ‘Factoring integers with the number field sieve’, *The development of the number field sieve*, Lecture Notes in Math. 1554 (Springer, Berlin, 1993) 50–94. 157
2. J. CANNON *et al.*, *The computer algebra system MAGMA* (University of Sydney, 2004), <http://magma.maths.usyd.edu.au/magma/>. 157
3. J. W. S. CASSELS, *Local fields*, London Mathematical Society Student Texts 3 (Cambridge University Press, Cambridge, 1986). 143
4. R. FRAATZ, ‘Computation of maximal orders of cyclic extensions of function fields’, Dissertation, Technische Universität Berlin, 2005, http://www.math.tu-berlin.de/~kant/publications/diss/diss_Robert-Fraatz.pdf. 150

5. C. FRIEDRICH, ‘Bestimmung relativer Ganzheitsbasen mit dem Round-2-Algorithmus’, Diplomarbeit, Technische Universität Berlin, 1997, <http://www.math.tu-berlin.de/~kant/publications/diplom/friedrichs.ps.gz>. 156
6. C. FRIEDRICH, ‘Berechnung von Maximalordnungen über Dedekindringen’, Dissertation, Technische Universität Berlin, 2000, http://www.math.tu-berlin.de/~kant/publications/diss/diss_fried.pdf. 156
7. V. D. GOPPA, ‘Codes on algebraic curves’, *Dokl. Akad. Nauk SSSR* 259 (1981) 1289–1290. 141
8. V. D. GOPPA, *Geometry and codes*, Mathematics and its Applications (Soviet Series) 24 (Kluwer, Dordrecht, 1988). 141
9. H. HASSE, ‘Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper’, *J. Reine Angew. Math.* 172 (1934) 37–54. 146
10. F. HESS, ‘Computing Riemann–Roch spaces in algebraic function fields and related topics’, *J. Symbolic Comput.* 33 (2002) 425–445. 144
11. F. LORENZ, *Einführung in die Algebra. Teil II* (Bibliographisches Institut, Mannheim, 1990). 150
12. M. POHST and H. ZASSENHAUS, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications 30 (Cambridge University Press, Cambridge, 1997). 156, 158
13. H. L. SCHMID, ‘Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p ’, *J. Reine Angew. Math.* 175 (1936) 108–123. 151
14. H. STICHTENOTH, *Algebraic function fields and codes*, Universitext (Springer, Berlin, 1993). 141, 143, 144, 149, 150

Robert Fraatz fraatz@math.tu-berlin.de
<http://www.math.tu-berlin.de/~fraatz>

Technische Universität Berlin
Fakultät II
Institut für Mathematik MA 8-1
Straße des 17. Juni 136
10623 Berlin
Germany