Computing Maximal Orders in Cyclic Extensions of Global Algebraic Fields

Nicole Sutherland

Computational Algebra Group, School of Mathematics and Statistics, The University of Sydney

Definitions

A *pseudo element* can be thought of simply as a pairing of an ideal with an element. An element is in the span of a set of pseudo elements if it can be written as a linear combination of the elements in the pseudo elements in the set with coefficients lying in the correponding ideals. A *pseudo basis* is a set which spans a module and contains the correct number of pseudo elements.

([Sti93] Proposition III.7.3) Let F be a algebraic field containing a primitive n-th root of unity, where $n > 1$ is coprime to the characteristic of F, and let $u \in F$ be such that $u \neq w^d$ for all $w \in F$ and $d > 1, d \mid n$. Then $F' = F(\alpha)$ with $\alpha^n = u$ is a *Kummer extension* of F.

([Sti93] Proposition III.7.8) Let F be a function field of characteristic $p > 0$ with perfect constant field and let $u \in F$ be such that $u \neq w^p - w$ for all $w \in F$. Then $F' = F(\alpha)$, where $\alpha^p - \alpha = u$, is an *Artin–Schreier* extension of F.

Let F be a function field of characteristic $p > 0$ with perfect constant field and $\bar{F}$ the separable closure of F in some algebraic closure. An *Artin–Schreier–Witt extension* of F is an abelian extension $E \subseteq \bar{F}$ of F of degree p^n.

Kummer Extensions

Kummer extensions are an important special case of radical extensions.

Theorem (Radical)

Let F'/F be a radical extension defined by the polynomial $x^n - u$ and let α be a root of this polynomial, a primitive element for F'. Let P be a place of F with $v_P(n) = 0$. Set g_P, k_P, j_P such that $g_P = k_P v_P(u) + n j_P, 0 \le g_P < n$ and g_P is minimal (i.e. $g_P = \gcd(v_P(u), n) \bmod n$). Set k'_P, j'_P such that $v_P(u)/g_P k'_P + n/g_P j'_P = 1$. Let $\mathcal{O} = \mathbb{Z}_F[\alpha]$ be an order of F' and S be a set of primes of $\mathbb{Z}_F$. Then

$$(\omega_i, \mathfrak{a}_i)_{0 \le i < n} = (\alpha^i, \prod_{P \in S} P^{\mu_{P,i}})_{0 \le i < n}$$

is a pseudo basis for an S-maximal overorder $\mathcal{R}$ of $\mathcal{O}$ where

$$\mu_{P,i} = \begin{cases} j_P i_P + v_P(u) t_{P,i_P}, & \text{if } P \text{ is unramified or totally ramified in } F',\ i_P \text{ is such that } i = k_{P,i_P}, 0 \le i_P < n \text{ and } t_{P,i_P} = \lfloor k_P i_P / n \rfloor \\ -i_P v_P(u)/g_P + j'_P l_P + v_P(u) t_{P,i_P l_P}, & \text{otherwise with } i_P, l_P \text{ such that } i = k_{P,i_P l_P}, 0 \le i_P < g_P, 0 \le l_P < n/g_P, t_{P,i_P l_P} = \lfloor (i_P n/g_P + k'_P l_P)/n \rfloor \end{cases}$$

The construction of a maximal order from this pseudo basis is efficient and this can be used to great advantage to compute maximal orders of class fields of number fields.

Some Comparisons

Table 1 contains average times for computing maximal orders of 10 random radical extensions of $\mathbb{F}_{101}(t)[y]/\langle y^3 + y^2 + y + t\rangle$ whose defining polynomials are of the form $x^n - \prod_{i=1}^3 p_i^{e_i}$, where p_i is a random prime polynomial and $e_i \in [1 \dots 6, 8, 10]$ is chosen randomly.

Degree	Algorithm (ECMO) using Theorem (Radical)	Round 2
28	0.125s	475.416s
30	0.112s	648.358s
31	0.409s	727.231s

Table 1: Comparison of average timings for maximal order computations of radical extensions

Let $F = \mathbb{Q}[x]/\langle x^2 - 2\rangle$. Let A be an abelian extension of F of degree 16. The average time to compute the maximal order of some extensions A using Algorithm (ECMO) was 8.86s. This is 245 times faster than the average of 36.3min for the Round 2 algorithm to compute the maximal orders.

Overview

Cyclic extensions of global algebraic fields occur as Kummer extensions of algebraic number fields and as Kummer and Artin–Schreier–Witt extensions of global algebraic function fields. Since maximal orders of global algebraic fields are also modules over Dedekind domains, we present 3 similar pseudo bases from which maximal orders of these cyclic extensions can be efficiently computed. An advantage of our approach is that the factorization of a discriminant is not necessary in most cases. For detailed information please see [Sut12], [Sut13], [Sut14] and [Sut15].

Efficient Construction of a Maximal Order

Algorithm (ECMO)

INPUT:

- *A cyclic extension $E/F = F(\alpha)$ of a global field F and an integral closure $\mathbb{Z}_F \subset F$.*

OUTPUT:

- *A maximal order of E over $\mathbb{Z}_F$.*

STEPS:

1. *Compute a set S of primes of $\mathbb{Z}_F$ at which $\mathbb{Z}_F[d\alpha]$ is not maximal, where $d \in \mathbb{Z}_F$ is such that $d\alpha$ is integral and d has smallest valuation.*
2. *Compute a pseudo basis for an S-maximal order of E over $\mathbb{Z}_F$ using the corresponding Theorem for the type of cyclic extension E/F is.*
3. *Construct the maximal order of E over $\mathbb{Z}_F$ from the pseudo basis.*

Artin–Schreier Extensions

Let F be a function field of characteristic $p > 0$ with separable closure $\bar{F}$. The *Artin–Schreier operator* $\wp : \bar{F} \to \bar{F}$ is the $\mathbb{F}_p$-linear homomorphism $\wp : x \mapsto x^p - x$.

Let $P \in \mathbb{P}_F$ and $u \in F$. An *Artin–Schreier quotient* of u modulo P is an element $z_P \in F$ satisfying $v_P(u - \wp(z_P)) \ge 0$ or $p \nmid v_P(u - \wp(z_P)) < 0$.

Let $S \subset \mathbb{P}_F$. If z is an Artin–Schreier quotient of u modulo P for all $P \in S$ then we call z an *Artin–Schreier quotient* of u modulo S.

Theorem (AS)

Let F'/F be an Artin–Schreier extension, $\mathcal{O} = \mathbb{Z}_F[d\alpha]$ an order of F', S be a set of primes of $\mathbb{Z}_F$ and $z \in F$ an Artin–Schreier quotient of u modulo S. Then

$$(\omega_j, \mathfrak{a}_j)_j = \left((d(\alpha - z))^j, \prod_{P \in S} P^{\mu_{P,j} - j v_P(d)} \right)_{0 \le j < p},$$

is a pseudo basis over $\mathbb{Z}_F$ for an S-maximal overorder of $\mathcal{O}$, where $\mu_{P,j}$ is the smallest non-negative integer such that $v_{P'}(\mathfrak{a}_j \omega_j) \ge 0$ for all $P' \mid P$.

Some Comparisons

Table 2 contrasts timings for the computation of maximal orders in Artin–Schreier extensions. All examples are given by $F' = F[y]/\langle y^p - y - u\rangle$ where $F = \mathbb{F}_p(t)[x]/\langle x^3 - (t+1)x^2 + 2xt - t^5\rangle$, ρ is a primitive element of F and $u = \frac{t^5}{t^3-1}\rho^2 + \frac{t^6+t^2+1}{t^6-1}\rho + \frac{1}{t^5}$.

p	Algorithm (ECMO) using Theorem (AS)	Round 2	p	Algorithm (ECMO) using Theorem (AS)	Round 2
31	0.9s	73min	53	3.81s	13hrs
61	5.98s	> 20hrs	71	9.78s	-

Table 2: Comparison of times for examples from [Fra05]

Artin–Schreier–Witt Extensions

Let A be a commutative ring and let $n > 0$. The ring $W_n(A)$ of *Witt vectors* of length n is the set of all vectors of length n with entries in A with addition and multiplication given by [Has80] Section 10.4. The zero element is $(0, \dots, 0)$ and a multiplicative identity is $(1, 0, \dots, 0)$.

Let $\wp : W_n(\bar{F}) \to W_n(\bar{F})$ be given by $\wp(x_1, \dots, x_n) \mapsto (x_1^p, \dots x_n^p) - (x_1, \dots, x_n)$. Let $P \in \mathbb{P}_F$ and $u \in W_n(F)$. An *Artin–Schreier–Witt quotient* of u modulo P is an element $\zeta_P \in W_n(F)$ satisfying $v_P((u - \wp(\zeta_P))_i) \ge 0$ or $p \nmid v_P((u - \wp(\zeta_P))_i) < 0$ for all $1 \le i \le n$.

Let $S \subset \mathbb{P}_F$. If ζ is an Artin–Schreier–Witt quotient of u modulo P for all $P \in S$ then we call ζ an *Artin–Schreier–Witt quotient* of u modulo S.

Theorem (ASW)

Let k be a field with prime characteristic p, F be an extension of $k(t)$, and $u \in W_n(F)$. Let $E = F(\alpha) = F(\wp^{-1}(u))$ be an Artin–Schreier–Witt extension of degree p^n and S a set of primes of $\mathbb{Z}_F$ with the same ramification degree p^{n-t}. Let $\zeta \in F$ be an Artin–Schreier–Witt quotient of u modulo S. Let $\rho \in E_{n-1} = F(\wp^{-1}((u_1, \dots, u_{n-1}))$ be an Artin–Schreier quotient of the constant coefficient of the defining polynomial of E/E_{n-1} modulo $\{P' : P' \mid P, P \in S \mid e(P'|P) > p\}$ such that $v_Q(\rho) \ge 0$ for all $Q \notin \{P' : P' \mid P, P \in S \mid e(P'|P) > p\} \cup \{X\}$ for some place X with $X \cap \mathbb{Z}_F = k$. Let d_l be such that $v_{P_l}(d_l \alpha_l) \ge 0$ for all $P_l \mid P$, P a prime ideal of $\mathbb{Z}_F$ and let $v_{P,ij} = j v_P(d) + \sum_{l=1}^t i_l v_P(d_l)$. Then

$$(\omega_{ij}, \mathfrak{a}_{ij})_{ij} = ((d_1(\alpha - \zeta)_1)^{i_1} \dots (d_t(\alpha - \zeta)_t)^{i_t} (d(\alpha_n - \rho))^j, \prod_{P \in S} P^{\mu_{P,j} - v_{P,ij}})_{0 \le i_1, \dots, i_t < p, 0 \le j < p^{n-t}}$$

or, without computing ρ when the ramification index $p^{n-t} = p$,

$$(\omega_{ij}, \mathfrak{a}_{ij})_{ij} = ((d_1(\alpha - \zeta)_1)^{i_1} \dots (d_{n-1}(\alpha - \zeta)_{n-1})^{i_{n-1}} (d(\alpha - \zeta)_n)^j, \prod_{P \in S} P^{\mu_{P,j} - v_{P,ij}})_{0 \le i_1, \dots, i_{n-1} < p, 0 \le j < p}$$

is a pseudo basis for an S-maximal order of E over $\mathbb{Z}_F$, where $\mu_{P,j}$ is the smallest non-negative integer such that $v_{P'}(\mathfrak{a}_{ij} \omega_{ij}) \ge 0$ for all $P' \mid P \in S$ and all i.

For a set S of primes of $\mathbb{Z}_F$ containing primes of several ramification degrees we can split the set S into a disjoint union of sets $S_i, 0 \le i \le n$ containing primes of ramification degree p^i. For each of these sets we can compute an S_i-maximal order $\mathcal{S}_i$. The sum $\sum_i \mathcal{S}_i$ calculated using addition of modules is then an S-maximal order of E containing $\mathbb{Z}_F$.

A Comparison

For 30 randomly generated degree 7^2 ASW extensions of $\mathbb{F}_7(t)$ the average time to compute a maximal order using Algorithm (ECMO) and Theorem (ASW) was 31.129s. Using Round 2 the average time was 1.4hrs.

Acknowledgements

The author would like to thank her supervisors, Claus Fieker and Stephen Donnelly.

References

[Fra05] R. Fraatz, *Computation of maximal orders of cyclic extensions of function fields*, Ph.D. thesis, Technische Universität Berlin, 2005.

[Has80] H. Hasse, *Number theory*, Springer Verlag, 1980.

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Springer–Verlag, 1993.

[Sut12] N. Sutherland, *Efficient computation of maximal orders in radical (including Kummer) extensions*, Journal of Symbolic Computation **47** (2012), 552–567.

[Sut13] N. Sutherland, *Efficient computation of maximal orders in Artin–Schreier extensions*, Journal of Symbolic Computation **53** (2013), 26–39.

[Sut14] N. Sutherland, *Efficient computation of maximal orders in Artin–Schreier–Witt extensions*, Journal of Symbolic Computation **77** (2016), 189–216.

[Sut15] N. Sutherland, *Algorithms for Galois extensions of global function fields*, PhD Thesis, University of Sydney, 2015.

Contact: nicole.sutherland@sydney.edu.au