Journal of Symbolic Computation 47 (2012) 552–567

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Efficient computation of maximal orders in radical (including Kummer) extensions

Nicole Sutherland[1]

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

ARTICLE INFO

Article history:
Received 23 December 2010
Accepted 23 December 2011
Available online 30 December 2011

Keywords:
Maximal orders
Kummer extensions
Radical extensions

ABSTRACT

We describe an algorithm, linear in the degree of the field, for computing a (pseudo) basis for P-maximal orders of radical (which includes Kummer) extensions of global arithmetic fields. We construct our basis in such a way as to further improve maximal order computations in these radical extensions. Using this algorithm for the similar problem of computing maximal orders of class fields is discussed. We give examples of both function fields and number fields comparing the running time of our algorithm to that of the Round 2 or 4 and Fraatz (2005).

1. Introduction

Maximal order computations usually use algorithms like Round 2 (Cohen, 2000) and Round 4 (Baier, 1996; Ford and Letard, 1994) which are polynomial complexity in the degree of the field. However, for some special types of extensions, like radical extensions, we can find a more efficient algorithm for maximal order computations (linear complexity in the degree of the field). Kummer extensions are a special case of radical extensions. An efficient algorithm for maximal orders of Kummer extensions is important in class field theory and coding theory which use such computations heavily. Radical extensions occur as both algebraic function fields or number fields. We state our results generally as they apply to both but note that we gain most in the case of function fields.

To compute maximal orders we factor the discriminant of the input order and compute P-maximal orders for every prime P dividing the discriminant. Note that the computation of a maximal order is polynomial time equivalent to finding the largest squarefree factor of the discriminant (Chistov, 1989) and factoring an integer discriminant is a sub-exponential time algorithm, so in a number field this initial computation may dominate the whole computation. For a radical extension by $x^n - a$ we know

E-mail address: nicole.sutherland@sydney.edu.au.

[1] Tel.: +61 2 9351 5776; fax: +61 2 9351 4534.

0747-7171/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2011.12.053

the discriminant is $n^n a^{n-1}$, so we need only factorize n and a, hence we can avoid both computing and factoring the whole discriminant. These P-maximal orders we compute are then added together to gain the maximal order itself. We can gain most then by considering the computation of the P-maximal orders.

We have implemented our algorithms in Magma V2.16 (Cannon et al., 2009) (and later) and provide a comparison of timings in Section 7. For a discussion of number fields and function fields in Magma please see Fieker (2006).

We follow Stichtenoth (1993) in notation. Here we give the key definitions and results which are based on those in Stichtenoth (1993) as noted but extended to include algebraic number fields.

Definition 1. Let F be a algebraic field, $n > 1$ and let $u \in F$ be such that $u \neq w^d$ for all $w \in F$ and $d > 1, d|n$. Then $F' = F(\alpha)$ with $\alpha^n = u$ is a radical extension of F.

An important special case of radical extensions are Kummer extensions. It is only these which Stichtenoth considers.

Definition 2 (*Stichtenoth, 1993 III.7.3*)**.** Let F be a algebraic field containing a primitive nth 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 $d > 1, d|n$. Then $F' = F(\alpha)$ with $\alpha^n = u$ is a Kummer extension of F.

Definition 3. Let O be an order in a field F'/F with coefficient ring $\mathbb{Z}_F$, a maximal order of F, and let P be a prime of $\mathbb{Z}_F$. A *P-maximal order of O* is an order ${}_PO$ such that O is a submodule of ${}_PO$, ${}_PO \subseteq \mathbb{Z}_F$ and, as $\mathbb{Z}_F$ modules, ${}_PO/O$ is P-primary and $\mathbb{Z}_{F'}/{}_PO$ has no P-primary component (where $\mathbb{Z}_{F'}$ is a maximal order of F').

Note that Cohen (2000) gives a definition of an order being P-maximal (Definition 2.4.1(1)) however his definition concentrates on the difference between a P-maximal order and a maximal order and does not have any reference to a suborder as our definition does. The suborder is important to us as it will be the input into our algorithm and the P-maximal order we will compute will be the minimal such one containing the input order.

Let F'/F be a finite separable extension of the algebraic field F/K and $P \in \mathbb{P}_F$ be a place of F/K. We recall from Stichtenoth (1993) Corollary III.3.5 that the integral closure O'_P of O_P in F' is

$$O'_P = \bigcap_{P'|P} O_{P'}$$

where $O_{P'}$ is the valuation ring at the place P'. We also have from this corollary that there is a basis $\{a_i\}$ of F'/F such that

$$O'_P = \sum_{i=1}^{n} O_P a_i$$

and we call such a basis $\{a_i\}$ an integral basis of O'_P over O_P or a P-integral basis.

Therefore we have that O'_P contains those elements of F' with non–negative valuation at all primes $P'|P$.

Definition 4. We call an order O in F'/F an equation order if $O = C[\alpha]$ where α is a root of a monic integral polynomial over the order C of the algebraic field F.

The orders we are interested in will be extensions of the maximal order of the algebraic field F, so C will be a maximal order.

Without loss of generality we assume u is an integral element of F so that the defining polynomial of F' is monic and integral and therefore the P-maximal order will contain the equation order.

Definition 5. We call F'/F a relative extension if F itself is an extension (of finite degree) of some field. If F is a rational function field or $\mathbb{Q}$ then F'/F is called an absolute extension.

1.1. Previous work

Earlier work on computing maximal orders of radical extensions has concentrated on computations in Kummer extensions.

Let P be a prime in an algebraic field F . Generators of P-maximal orders of Kummer extensions of F are well known (for number fields (Daberkow, 1995; Pohst, 1996; Daberkow, 2001), for function fields (Fraatz, 2005)). However, it is expensive to construct a P-maximal order from those generators as this is constructing a minimal order containing a set of elements which is expensive, at least $O(n^3)$ where n is the degree of the field, because of the use of normal form.

Daberkow and Pohst have considered Kummer extensions in Daberkow (1995), Pohst (1996) and Daberkow (2001). In these publications they provide a system of generators for the maximal order of a Kummer extension (Daberkow (1995) Theorem 3.29 and Pohst (1996) Theorem 2.3). They restrict to Kummer extensions of prime degree and reduction of generators is required. After reduction they have at most twice the prime degree number of generators. Pohst notes that a relative integral basis only exists under certain conditions. Daberkow (1995) and Pohst (1996) state Hecke's Theorem (Hecke, 1954, 1981). They are also interested in relative discriminants (of maximal orders) of Kummer extensions.

Fraatz (2005) also computes generators for a maximal order of Kummer extensions of function fields. There is no restriction on the degree of the extension and the number of generators is related to the number of ramified primes. We will compare timings from our implementation with his.

Cohen (2000) also states Hecke's Theorem. In his proof of Hecke's Theorem (Theorem 10.2.9) he gives elements which are Kummer equivalent (Definition 10.2.8) to the primitive element of the Kummer extension but generate a P-integral power basis of the Kummer extension (Stichtenoth (1993) Propositions III.5.11 and 12) when P is either totally ramified or unramified in the extension. At the end of Section 5.3.6 he claims that computing an integral pseudo basis of a Kummer extension is easy. We shall show here that it indeed is a very efficient computation.

Stichtenoth (1993) states and proves the values of the ramification degrees and different exponents of primes of a Kummer extension of F over P in Proposition III.7.3 and its proof. Elements generating a P-integral power basis of a Kummer extension can be deduced from this proof and this is where we started.

In this paper we derive a pseudo basis for a P-maximal order of a radical extension in a way such that the computation of the maximal order from these P-maximal orders is efficient. This does not require the minimal order computation required to compute an order from generators. We extend our work on Kummer extensions to the computation of maximal orders of class fields.

2. A (local) P-integral power basis

Stichtenoth (1993) (Theorem III.7.3 and its proof) suggests, for a Kummer extension $F' = F(\alpha)$, an isomorphic field $E = F(\beta)$ such that a root of the defining polynomial of E defines a (local) P-integral power basis for F' where β is Kummer equivalent to α. We used this β as the basis of our first algorithm to compute a P-maximal order of a radical extension. Note that Stichtenoth does not use the existence of a primitive n-th root of unity in the coefficient field so we state our theorem for radical extensions.

Theorem 6 (*P-Integral Power Basis of a Radical Extension*). *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 prime of F with $v_P(n) = 0$ and abbreviate $v_P(u)$ to $v(u)$. Set g, k, j such that $g = kv(u) + nj$, $0 \le g < n$ and g is minimal (i.e. $g = \gcd(v(u), n) \bmod n$).*

- *If $g \le 1$ then $\{\beta^i\}_{0 \le i < n}$ where $\beta = \alpha^k \pi^j$ and π is a uniformizing element for P is a (local) P-integral power basis for F'.*
- *If $g > 1$ then $\{\beta_1^i \beta_2^l\}_{0 \le i < g, 0 \le l < n/g}$ where*

$$\beta_1 = \alpha^{(n/g)} \pi^{(-v(u)/g)}, \qquad \beta_2 = \alpha^{k'} \pi^{j'} \quad \text{with } \frac{v(u)}{g} k' + \frac{n}{g} j' = 1$$

is a (local) P-integral power basis for F'. (That is β_1 is a root of $x^g - \beta_1^g = x^g - u\pi^{(-v(u))}$ and β_2 is a root of $x^{(n/g)} - (\alpha^{k'}\pi^{j'})^{(n/g)}$).

Proof. For any prime P' of F', $P'|P$, we know P' has ramification degree n/g over P (Stichtenoth, 1993) for $g > 0$ and ramification degree 1 for $g = 0$.

We consider 3 cases :

(1) $P'|P$ is totally ramified : $g = 1$,

$$v_{P'}(\beta) = kv_{P'}(\alpha) + jv_{P'}(\pi) = kv_{P'}(\alpha) + j\frac{n}{g} = 1.$$

Therefore β is a P' prime element so by Stichtenoth (1993) Proposition III.5.12, $\{\beta^i\}_{0\le i<n}$ is a (local) P-integral basis for F'.

(2) $P'|P$ is unramified : $g = 0, k = 1, j = -v(u)/n$

$$v_{P'}(\beta) = k\frac{v(u)}{n} + j = \frac{v(u)}{n} - \frac{v(u)}{n} = 0.$$

The minimal polynomial of β is $\phi = x^n - \beta^n = x^n - u^k\pi^{jn}$ and $v_P(u^k\pi^{jn}) = kv(u) + jnv_P(\pi) = 0$ so the minimal polynomial is integral at P and $v_{P'}(\phi'(\beta)) = v_{P'}(n\beta^{n-1}) = v_{P'}(n) + (n-1)v_{P'}(\beta) = 0$ so that $\{\beta^i\}_{0\le i<n}$ is a (local) P-integral basis for F' by Stichtenoth (1993) Proposition III.5.11. Note that this does not hold when $v_P(n)$ is not zero, i.e. when P is a critical prime.

(3) When $g > 1$, $P'|P$ is ramified but not totally. We split F' into a tower of extensions and consider $F'/F_0/F$ where $F_0 = F(\alpha_0)$ and $F' = F_0'(\alpha)$ and $\alpha_0 = \alpha^{n/g}$. Let $P_0 = P' \cap F_0'$ then $\gcd(g, v(u)) = g \equiv 0 \bmod g$ so $P_0|P$ is unramified and $\beta_1 = \alpha_0^k\pi^j$ with $k = 1$ and $j = -v(u)/g$, $v_{P_0}(\beta_1) = 0$ as for case (2) above. Therefore $\{\beta_1^i\}_{0\le i<g}$ is a (local) P-integral basis for F_0/F.

Consider $P'|P_0$. This is totally ramified since

$$\gcd(n/g, v_{P_0}(\alpha^{n/g})) = \gcd(n/g, v_P(\alpha^{n/g})) = \gcd(n/g, v(u)/g) = 1.$$

Therefore we have $\beta_2 = \alpha^{k'}\pi^{j'}$ as in case (1) above with $v_{P'}(\beta_2) = 1$ so $\{\beta_2^l\}_{0\le l<n/g}$ is a (local) P-integral power basis for F'/F_0.

We have then that $\{\beta_1^i\beta_2^l\}_{0\le i<g, 0\le l<n/g}$ is a basis for F'/F. Since $v_{P'}(\beta_2) = 1$ and $v_{P'}(\beta_1) = \frac{n}{g}v_{P_0}(\beta_1) = 0$ both β_1 and β_2 are P'-integral and so $\{\beta_1^i\beta_2^l\}$ is a (local) P-integral basis for F'/F. □

3. A pseudo basis

A (local) P-integral power basis is an improvement on generators but we found we can do better than this. There are a few more requirements for a basis of a P-maximal order and there are ways in which we can construct our P-maximal order more efficiently. We would like to avoid certain denominators, the P-maximal order to contain the equation order and as we are interested in computing maximal orders we want it to be easy to add the P-maximal orders we compute. And as Pohst (1996) notes a relative integral basis does not exist in every extension.

This led to the use of pseudo bases. We will give Cohen's (Cohen, 2000) Definition 1.4.1 of pseudo elements and bases and Hoppe's (Hoppe, 1998) Definition 4.1.1 of a pseudo matrix.

Definition 7 (*Cohen, 2000, Definition 1.4.1*)**.** Let M be a finitely generated torsion-free R-module and set $V = FM$ where R is a Dedekind domain and F is its field of fractions.

(1) A pseudo-element of V is a sub-R-module of V of the form $\mathfrak{a}\omega$ with $\omega \in V$ and $\mathfrak{a}$ a fractional ideal of R, or equivalently an equivalence class of pairs $(\omega, \mathfrak{a})$ formed by an element of V and a fractional ideal of R under the equivalence relation $(\omega, \mathfrak{a})\mathcal{R}(\omega', \mathfrak{a}')$ if and only if $\mathfrak{a}\omega = \mathfrak{a}'\omega'$ as sub-R-modules of rank 1 of V.

(2) The pseudo-element $\mathfrak{a}\omega$ is said to be integral if $\mathfrak{a}\omega \subset M$.

(3) If $\mathfrak{a}_i$ are fractional ideals of R and ω_i are elements of V, we say that $(\omega_i, \mathfrak{a}_i)_{1\le i\le k}$ is a pseudo-generating set for M if

$$M = \mathfrak{a}_1\omega_1 + \cdots + \mathfrak{a}_k\omega_k.$$

(4) We say that $(\omega_i, \mathfrak{a}_i)_{1\le i\le k}$ is a pseudo-basis of M if

$$M = \mathfrak{a}_1\omega_1 \oplus \cdots \oplus \mathfrak{a}_k\omega_k.$$

From a pseudo-generating set or basis we can construct a pseudo matrix by putting the vectors w_i into the columns (or rows) of a matrix.

Definition 8 (Hoppe, 1998, *Definition 4.1.1*)**.** Let O be an order of a field F and let $m, n \in \mathbb{N}$ and A be an $(n \times m)$-matrix over F with column vectors $A_1, \ldots, A_m$ in F^n. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ be fractional ideals of O. Then $[(\mathfrak{a}_1, \ldots, \mathfrak{a}_m), A]$ is a pseudo matrix over O with n rows and m columns.

A pseudo matrix constructed from a pseudo basis for an order O in a field F' of degree n will have n rows and n columns. We use a pseudo matrix $[(\mathfrak{a}_j), (\omega_j)]$ as a transformation matrix expressing the basis of O as a linear combination of the basis of its suborder S. Let $\{s_j\}$ be a basis for the field of fractions of S such that $s_j\mathfrak{s}_j \subseteq S$ where $\mathfrak{s}_j$ are the ideals in a pseudo basis of S. Then $\{b_i\}$ with $b_i = \sum_j w_{ij}s_j$ is a basis for the field of fractions of O with $b_i\mathfrak{a}_i \subseteq O$ where w_{ij} is the ij-th entry of the matrix whose columns are ω_j.

These pseudo bases meet all the above requirements. They allow us to handle denominators, include the equation order and create the order with a diagonal matrix which makes the additions more efficient. To compute the sum of 2 orders constructed as transformations of a common suborder usually involves a union (or join) of their bases followed by a hermite form calculation, which is cheaper when applied to the join of two diagonal matrices. We can arrange our pseudo bases such that the corresponding pseudo matrices are identity matrices and addition becomes taking the GCDs of the coefficient ideals $\mathfrak{a}_j$.

We can construct a pseudo basis from the P-integral power basis of Theorem 6 in each case. We will show that the pseudo basis we construct is a pseudo basis for an order (i.e. it contains 1 and is closed under multiplication) which is at least as large as the order the basis is a transformation of. We prove P-maximality later.

Proposition 9. *Suppose we satisfy the hypothesis of* Theorem 6*. Let O be an order of F' and let P now denote $P \cap C$ where $C \subset F$ is the coefficient order of O.*

- *If $P'|P$ is either totally ramified or unramified then*

$$(\omega_i, \mathfrak{a}_i)_i = (\alpha^{k_i}, P^{ji+v(u)t_i})_{0\le i<n}, \qquad ki = k_i + t_in, \quad 0 \le k_i < n$$

is a pseudo basis for an order containing the equation order of O,

- *Otherwise*

$$(\omega_{il}, \mathfrak{a}_{il})_i = (\alpha^{k_{il}}, P^{-iv(u)/g+j'l+v(u)t_{il}})_{0\le i<g, 0\le l<n/g}, \quad in/g + k'l = k_{il} + t_{il}n, 0 \le k_{il} < n$$

is a pseudo basis for an order containing the equation order of O.

These pseudo bases are derived from the P-integral power basis as follows.

- $P'|P$ is totally ramified or unramified, a P-integral basis is $\{\beta^i\}_{0\le i<n}$, $\beta = \alpha^k\pi^j, kv(u)+nj = g, g = 0, 1$. Using pseudo elements,

$$\begin{aligned}
(\alpha^kP^j)^i &= \alpha^{k_i}\alpha^{t_in}P^{ji} && \text{where } ki = k_i + t_in \text{ and } 0 \le k_i < n\\
&= \alpha^{k_i}u^{t_i}P^{ji}\\
&= \alpha^{k_i}\pi^{v(u)t_i}u'^{t_i}P^{ji} && \text{where } u = \pi u'\\
& && \text{and } \pi \text{ is a uniformizing element for } P \text{ or is } P.
\end{aligned}$$

We group the P parts together and note that multiplication by u' does not change the power of P to get the pseudo basis $(\alpha^{k_i}, P^{ji+v(u)t_i})_{0\le i<n}$.

We also note that since k is coprime to n ($k = 1$ or $g = 1$) and $k_{i_1} = k_{i_2} \implies k(i_1 - i_2) = (t_{i_1} - t_{i_2})n$ we have $k_{i_1} = k_{i_2} \implies i_1 = i_2$. So the values k_i are unique and since there are n different k_i values, for each $0 \le z < n$ there is some i such that $k_i = z$.

- $P'|P$ is partially ramified, a P-integral basis is $\{\beta_1^i \beta_2^l\}_{0 \le i < g, 0 \le l < n/g}$, where $\beta_1 = \alpha^{n/g}\pi^{-v(u)/g}$, $\beta_2 = \alpha^{k'}\pi^{j'}$ and $\frac{v(u)}{g}k' + \frac{n}{g}j' = 1$. Using pseudo elements,

$$\begin{aligned}(\alpha^{n/g}P^{-v(u)/g})^i(\alpha^{k'}P^{j'})^l &= \alpha^{k_{il}}\alpha^{t_{il}n}P^{-iv(u)/g+j'l} \quad \text{where} \\ &\qquad in/g + k'l = k_{il} + t_{il}n \quad \text{and} \quad 0 \le k_{il} < n \\ &= \alpha^{k_{il}}u'^{t}P^{-iv(u)/g+j'l+v(u)t_{il}}.\end{aligned}$$

We note that multiplication by u' does not change the power of P to get the pseudo basis $(\alpha^{k_{il}}, P^{-iv(u)/g+j'l+v(u)t_{il}})_{0 \le i < g, 0 \le l < n/g}$.

Here again the k_{il} are unique. If $k_{i_1 l_1} = k_{i_2 l_2}$ then $(l_1 - l_2)k' = n/g((t_{i_1 l_1} - t_{i_2 l_2})g - (i_1 - i_2))$ and since k' and n/g are coprime $n/g | l_1 - l_2 < n/g$ so $l_1 = l_2$. Let $t_m = t_{i_m l_m}$. Then we have $g(t_1 - t_2) = i_1 - i_2$ so $g | i_1 - i_2 < g$ and $i_1 = i_2$. Therefore, since there are n different k_{il} values, for each $0 \le z < n$ there is some i and l such that $k_{il} = z$.

Proof. We will show that $(\omega_i, \mathfrak{a}_i)_i$ is a pseudo basis for an order when $P'|P$ is either totally ramified or unramified and note that the partially ramified case can be proven similarly.

When $i = 0$, $\omega_0 = 1$, $\mathfrak{a}_0 = 1$ so 1 is contained in the span of $(\omega_i, \mathfrak{a}_i)_i$. We now use pseudo elements and check that $\mathfrak{a}_i\omega_i \times \mathfrak{a}_{i'}\omega_{i'}$ is in the span of $(\omega_i, \mathfrak{a}_i)_i$. For $i, i' < n$ we have $i + i' = mn + i''$, $i'' < n$, $m = 0, 1$ so

$$\mathfrak{a}_i\omega_i \times \mathfrak{a}_{i'}\omega_{i'} = P^{j(i+i')+v(u)(t_i+t_{i'})}\alpha^{k_i+k_{i'}}.$$

But $k_i + k_{i'} = k_{i''} + (t_{i''} + km - (t_i + t_{i'}))n$ so

$$\begin{aligned}\mathfrak{a}_i\omega_i \times \mathfrak{a}_{i'}\omega_{i'} &= P^{j(mn+i'')+v(u)(t_i+t_{i'})}\alpha^{k_{i''}}u^{(t_{i''}+km-(t_i+t_{i'}))} \\ &= P^{ji''+jmn+v(u)(t_i+t_{i'})+v(u)(t_{i''}+km-(t_i+t_{i'}))}\alpha^{k_{i''}} \\ &= P^{ji''+v(u)t_{i''}+jmn+v(u)km}\alpha^{k_{i''}} \\ &= \mathfrak{a}_{i''}\omega_{i''}P^{jmn+v(u)km} \\ &\subseteq \mathfrak{a}_{i''}\omega_{i''} \text{ since } jmn + v(u)km = mg \ge 0.\end{aligned}$$

Therefore $\mathfrak{a}_i\omega_i \times \mathfrak{a}_{i'}\omega_{i'}$ is in the span of $(\omega_i, \mathfrak{a}_i)_i$.

To check that the order with pseudo basis $(\omega_i, \mathfrak{a}_i)_i$ contains O we check that the exponents of P are non-positive. When

$g = 0,$

$$ji + v(u)t_i = \frac{-v(u)}{n}i + v(u)t_i = v(u)\left(t_i - \frac{i}{n}\right) \le 0 \quad \text{since } t_i = \lfloor ki/n \rfloor \quad \text{and} \quad k = 1$$

$g = 1,$

$$\begin{aligned}kv(u) + jn = 1, &\quad \text{so } ikv(u) + ijn = i, \\ i &= ikv(u) - t_inv(u) + ijn + t_inv(u) \\ &= v(u)(ki - t_in) + n(ji + v(u)t_i) \\ &= v(u)k_i + n(ji + v(u)t_i), \\ n(ji + v(u)t_i) &= i - v(u)k_i \le i.\end{aligned}$$

$$\text{Therefore } ji + v(u)t_i \le i/n < 1, \ \text{so } ji + v(u)t_i \le 0.$$

$1 < g < n,$

$$v_{P'}(\alpha^{k_{il}}P^{-iv(u)/g+j'l+v(u)t_{il}}) = v_{P'}((\alpha^{n/g}P^{-vu/g})^i(\alpha^{k'}P^{j'})^l) = 0i + 1l = l.$$

$$\text{Therefore,} \quad l = k_{il}v_{P'}(\alpha) + v_{P'}(P)\left(j'l - i\frac{v(u)}{g} + v(u)t_{il}\right)$$

$$\frac{n}{g}\left(j'l - i\frac{v(u)}{g} + v(u)t_{il}\right) = l - k_{il}v_{P'}(\alpha) \le l \text{ since } k_{il}v_{P'}(\alpha) \ge 0$$

$$j'l - i\frac{v(u)}{g} + v(u)t_{il} \le l\frac{g}{n} < 1 \quad \text{since } 0 \le l < \frac{n}{g}.$$

$$\text{Therefore } j'l - i\frac{v(u)}{g} + v(u)t_{il} \le 0 \text{ since the LHS is an integer.}$$

So we have in all cases that the exponents of P in the pseudo basis are non-positive. The order with pseudo basis $(\omega_i, \mathfrak{a}_i)_i$ will contain the equation order since for i such that $k_i = 1, \alpha = 1 \times \omega_i$ and $1 \in \mathfrak{a}_i$ since $(v(u)t_i + ji) \le 0$, so α, a primitive element for the equation order, is in the order with pseudo basis $(\omega_i, \mathfrak{a}_i)_i$.

In the partially ramified case, let i, l be such that $k_{il} = 1, \alpha = 1 \times \omega_i$ and $1 \in \mathfrak{a}_i$ since $(jl - iv(u)/g + v(u)t_{il}) \le 0$ so α is an element of the transformed order.

Therefore the order created using this pseudo basis will contain the equation order of O which it is constructed as a transformation of. □

Let O' be the order with pseudo basis $(\omega_i, \mathfrak{a}_i)_i$ we are constructing as a transformation of O. We form a transformation pseudo matrix expressing the basis of O' as a transformation of the basis of O. We use the ω_i, the powers of α, (as module elements) as the columns of the matrix and the powers of P as the ideals $\mathfrak{a}_j$. The order of the basis of O' does not matter so we reorder our pseudo basis to $(\alpha^i, P^{m_i})_{0 \le i < n}$ (since k_i takes all values $0 \le i < n$). If O is an equation order then as module elements the powers α^i are the standard basis vectors e_i and the matrix containing them as columns is the identity.

When O is not a relative extension and so an integral basis exists, we can simplify a little. Since the primes of F are elements of the integer ring of F each power of P is an element of F. Therefore we can multiply these into the matrix, first extracting the most negative power to use as a denominator for the transformation.

We summarize in this algorithm. Notation is as previously.

Algorithm 1 (*Computing a Pseudo Basis of a P-Maximal Order*)**.** We take as input an equation order O in a radical field extension F'/F with coefficient ring C and a prime $P \in C$ or $P \subset C$.

```
(1) Compute $v(u), g, k, j$ as in Theorem 6.
(2) Let $T$ be the transformation matrix of the $P$-maximal order we are computing
(3) if $g \le 1$ then
    (a) if $F$ is a relative extension
        (i) set $T$ to the identity matrix, let $I$ be an array of ideals
        (ii) for $i \in [0 \ldots n)$
                Put $P^{ji+v(u)t_i}$ in the $k_i$th entry of $I$
    (b) if $F$ is not a relative extension
        (i) Compute $\mu = \min_i\{ji + v(u)t_i\}$
        (ii) for $i \in [0 \ldots n)$
                Put $P^{ji+v(u)t_i-\mu}$ in the $k_i$th diagonal entry of $T$
    otherwise
        Compute $k', j'$ as in Theorem 6.
        (a') if $F$ is a relative extension
            (i) set $T$ to the identity matrix, let $I$ be an array of ideals
            (ii) for $i \in [0 \ldots n)$
                    Put $P^{-iv(u)/g+j'l+v(u)t_{il}}$ in the $k_{il}$th entry of $I$
        (b') if $F$ is not a relative extension
            (i') Compute $\mu = \min_{i,l}\{-iv(u)/g + j'l + v(u)t_{il}\}$
```

(ii′) for $i \in [0 \dots g), l \in [0 \dots n/g)$

Put $P^{-iv(u)/g+j'l+v(u)t_{il}-\mu}$ in the k_{il}th diagonal entry of T

(4) If F is a number field and P is a critical prime then handle as in Section 4.

We now analyse the complexity of the above algorithm. There are n powers $P^{ji+v(u)t_i}$ or $P^{ji+v(u)t_i-\mu}$ to compute where $0 \geq ji + v(u)t_i \geq -v(u)$ so $-v(u) \leq \mu \leq 0$ (and similarly for $g > 1$) so the powers we compute have exponents between 0 and $-v(u)$ or $-\mu$ which is at worst $v(u)$. Therefore the complexity is $O(n\log(v(u)) + \log(v(u)))$ since computing $v(u)$ has complexity $O(\log(v(u)))$.

3.1. Proof of P-maximality

Theorem 10. *The order with pseudo basis computed using Algorithm 1 is a P-maximal order of O.*

Proof. Let R be the order of F'/F with pseudo basis

$$(\omega_i, \mathfrak{a}_i)_i = (\alpha^{k_i}, P^{(v(u)t_i+ji)})_{0\leq i<n}$$

if P is totally ramified or unramified or

$$(\omega_{il}, \mathfrak{a}_{il})_{il} = (\alpha^{k_{il}}, P^{-iv(u)/g+jl+v(u)t_{il}})_{0\leq i<g,0\leq l<n/g}$$

otherwise.

To prove that R is the P-maximal order of the equation order O we need to prove that as $\mathbb{Z}_F$ modules R/O is P-primary and that R is maximal with these properties.

R/O is P-primary When F'/F is not a relative extension, we test whether R/O is P-primary by considering the determinant of the inverse of the transformation matrix. The transformation matrix is a diagonal matrix containing non-positive powers of P, therefore the inverse of the transformation matrix is a diagonal matrix containing non-negative powers of P. Therefore the determinant is a non-negative power of P.

When F'/F is a relative extension, we consider the principal ideal generated by the determinant of the inverse of the transformation matrix divided by the coefficient ideals, $\mathfrak{a}_i$. In this case the transformation matrix is the identity, so the principal ideal generated by the determinant of the inverse is $1\mathbb{Z}_F$. Dividing this by non-positive powers of P gives an ideal which is a non-negative power of P.

Therefore R/O is P-primary.

Maximality at P We take the elements from our (local) P-integral power basis in Theorem 6 and prove that they are in the localization of R at P. The localization of R at P is $R_{P\cap R}$, fractions of elements in R with no P in the denominator. It is contained in the integral closure O'_P.

Basis $\{b_i\} = \{(\alpha^k\pi^j)^i\}$

$$\begin{aligned}(\alpha^k\pi^j)^i &= \alpha^{k_i}\alpha^{t_in}\pi^j\\ &= \alpha^{k_i}u^{t_i}\pi^j \quad \text{where } u = \pi^{v(u)}u'\\ &= \omega_i u'^{t_i}\pi^{v(u)t_i+j}\\ &= u'^{t_i}r \quad \text{where } r \in R \text{ since } \pi^{v(u)t_i+j} \in \mathfrak{a}_i.\end{aligned}$$

Since $v_P(u') = 0$, $v_P(u'^{t_i}) = 0$ also, so there is no P in the denominator of $(\alpha^k\pi^j)^i$. Therefore $(\alpha^k\pi^j)^i$ is in the localization of R at P.

Basis $\{b_{il}\} = \{(\alpha^{n/g}\pi^{-v(u)/g})^i(\alpha^k\pi^j)^l\}$

$$\begin{aligned}(\alpha^{n/g}\pi^{-v(u)/g})^i(\alpha^k\pi^j)^l &= \alpha^{in/g+kl}\pi^{-iv(u)/g+jl}\\ &= \alpha^{k_{il}}\alpha^{t_{il}n}\pi^{-iv(u)/g+jl}\\ &= \alpha^{k_{il}}u^{t_{il}}\pi^{-iv(u)/g+jl}\\ &= \omega_{il}u'^{t_{il}}\pi^{-iv(u)/g+jl+v(u)t_{il}}\\ &= u'^{t_{il}}r \text{ where } r \in R \text{ since } \pi^{-iv(u)/g+jl+v(u)t_{il}} \in \mathfrak{a}_{il}\end{aligned}$$

Since $v_P(u') = 0$, $v_P(u'^{t_{il}}) = 0$ also, so there is no P in the denominator of $(\alpha^{n/g}\pi^{-v(u)/g})^i(\alpha^k\pi^j)^l$. Therefore $(\alpha^{n/g}\pi^{-v(u)/g})^i(\alpha^k\pi^j)^l$ is in the localization of R at P.

The basis $\{(\alpha^k\pi^j)^i\}$ or $\{(\alpha^{n/g}\pi^{-v(u)/g})^i(\alpha^k\pi^j)^l\}$ is an integral basis of F' at P, that is, it is a basis for the integral closure O'_P. Therefore the integral closure O'_P is contained in the localization of R at P. Since also the localization of R at P is contained in the integral closure O'_P the localization of R at P is the integral closure O'_P. Therefore we have that $v(\mathrm{disc}(R_{P\cap R})) = v(\mathrm{disc}(O'_P))$. But by Pohst and Zassenhaus (1989) p292 (invariance under localization) this means that $v_P(\mathrm{disc}(R)) = v_P(\mathrm{disc}(\mathbb{Z}_{F'}))$ since O'_P is the localization of $\mathbb{Z}_{F'}$ at P. Therefore R is P-maximal. □

3.2. The maximal order

Here we summarize the algorithm we use to compute a maximal order of a radical extension from the P-maximal order computed using Algorithm 1.

Algorithm 2 (*Computing Maximal Orders of Radical Extensions*)**.** We take as input an order O in a radical extension F'/F.

(1) Factorize the discriminant of O.
(2) If F'/F is a relative extension then
  (a) For each prime P in the factorization of the discriminant compute the array of ideals I_P as in Algorithm 1 Step 3(a) and 3(a′).
  (b) For $i \in [0 \dots n)$ Take the GCD of all the ith entries of the I_P arrays and collect the results in the array of ideals G.
  (c) Construct the order M with transformation pseudo matrix $[G, I_{n\times n}]$.
  (d) If O is not an equation order then set $M = M + O$ since there may have been primes O was already P-maximal at which do not appear in its discriminant.
  (e) If there are critical primes in the factorization of the discriminant compute the P-maximal order of the equation order of O using another algorithm (see Section 4) and add into M for each critical prime P.
  Otherwise
  (a′) Compute the sum M of O and all the P-maximal orders of O (computed using Algorithm 1 if P is non-critical) for each prime P in the factorization of the discriminant. If P is critical then apply another algorithm (see Section 4).
(3) M is the maximal order of O

4. Critical primes

We note a limitation of our algorithm for number fields only. Since critical primes do not occur in function fields our algorithm is complete for function fields.

Definition 11. Let P be a prime of a number field F and let F' be an extension of F. If the minimum of P or the absolute minimum of P divides the degree of F'/F then P is a critical prime for F'/F.

Algorithm 1 does not compute a P-maximal order at critical primes which are not totally ramified. At critical primes $v_P(n) \neq 0$ which upsets our proof of Theorem 6 in case (2), the unramified primes and therefore also case (3) which uses the unramified case. The order it does compute may not be big enough so the Round 2 was called on the result which became very expensive in some examples. This only applies to equation orders which are not maximal since if the equation order is maximal this can be determined using the Dedekind test (Cohen, 2000).

In the small number of cases when $F = \mathbb{Q}$, Round 4 can be applied. In the case where F' can be completed we can factorize the defining polynomial of F' over the completion of F at P and use the two-element certificate returned along with the factorization (Pauli, 2001) to form a matrix over the completion which is mapped back to F and becomes the basis matrix of the P-maximal order. We also compute the exponents for the powers of P which are the coefficient ideals of the P-maximal order.

For number fields of prime degree there are techniques to compute a (local) P-integral basis when P is a critical prime (Daberkow, 1995). Such techniques could be extended to fields whose degree is the product of 2 primes, however they involve a congruence that is difficult and so far time consuming to solve so we have not done any further work in this direction.

5. Other uses of the algorithm

There are some computations other than (P-)maximal orders of radical extensions which we hoped could benefit from the use of Algorithm 2. We identified or constructed Kummer extensions in these computations, computed a pseudo basis for the maximal order in that Kummer extension then mapped that maximal order basis back to the original. This was found to be very advantageous for computing maximal orders of class fields.

5.1. Dual and intersection

Let E be an equation order of the field extension F'/F of degree n. Let $E^\#$ denote the dual of E with respect to the trace and K be a radical extension containing F'. Once we have a maximal order for K we need to intersect that maximal order with F' to gain a maximal order of F' since K is larger than F'. To do this we compute the dual of the equation order of the original field where the dual is defined as

$$E^\# = \{x \in F' | \mathrm{Tr}(xE) \in \mathbb{Z}_F\}.$$

For all $x \in \mathbb{Z}_{F'}$ we have $xe \in \mathbb{Z}_{F'}$ for all $e \in E$ so $x \in E^\#$ and $\mathbb{Z}_{F'} \subseteq E^\#$.

Note that this holds for all orders O of F' but our interest is in equation orders.

In parallel to Cohen (2000) Definition 2.3.16 and Proposition 2.3.18 and more generally we have

Proposition 12. *Let $(\omega_i, \mathfrak{a}_i)_i$ be a pseudo basis of an order O where $\omega_i \in O$ and $\mathfrak{a}_i$ are fractional ideals of the coefficient ring of O which is maximal. If $T = \mathrm{Tr}_{L/K}(\omega_i\omega_j)$, the pseudo matrix $[T^{-1}, \mathfrak{a}_i^{-1}]$ represents a pseudo basis of $O^\#$.*

The proof follows similarly to Cohen's proof of Proposition 2.3.18 in Cohen (2000).

We do not construct the order $E^\#$ as it is more efficient to work with the pseudo basis only. To compute the intersection of the maximal order of K with $E^\#$, we find the basis of the maximal order of K with respect to the coefficient ring of E. We map the pseudo basis of $E^\#$ into K and express both bases as pseudo matrices with respect to the coefficient ring of E. We intersect these two bases as pseudo matrices and create the maximal order of F' as a transformation of E.

5.2. A Kummer approach to radical extensions

We began by following a similar approach to Daberkow (1995), Section 4.3. For a radical extension F'/F of degree n we computed a cyclotomic extension F_c/F which contained the nth roots of unity and then extended this by the defining polynomial of F'/F to gain a Kummer extension K/F_c. After computing the maximal order of K using Algorithm 2 we intersected this with the dual of the equation order of F' to gain the maximal order of F'/F.

Unfortunately this was quite expensive for some examples. However, Stichtenoth (1993) Remark III.7.5 notes that he does not use the presence of the roots of unity in the coefficient field. So we wrote Theorem 6 and Algorithms 1 and 2 for radical extensions rather than Kummer extensions.

It turns out that the algorithm following Daberkow (1995) can be faster than Round 2 for some examples requiring only small degree cyclotomic extensions but Algorithm 2 is faster still. For a comparison of timings see Section 7.4.

5.3. Use of Kummer algorithm to compute maximal orders of class fields

A similar approach can be taken to compute maximal orders of class fields. Here we can decompose the field into a compositum of cyclic fields C_i/k of prime power degree. A generator β inside a Kummer extension can be found for each C_i so there is known a Kummer extension $K_i = k(\zeta_{p^r})(\beta)$ and some $\alpha \in K_i$ such that $C_i = k(\alpha)$. We do similar to as we did originally in the radical case above—compute the maximal order of the Kummer extension K_i then intersect this with the dual of the class field to gain a maximal order, see Section 5.1.

Algorithm 3 (*Maximal Orders of Class Fields Using Kummer Extensions*)**.** We take as input an abelian field A. For each cyclic field component C we do

(1) Get the associated Kummer extension K of C.
(2) If C is a Kummer extension then compute the maximal order of C using Algorithm 2.
(3) Otherwise create a Kummer extension K_a isomorphic to K but defined as an extension of the coefficient ring of K represented as an absolute extension.
(4) Compute the maximal order of K_a using Algorithm 2.
(5) Find a basis of the maximal order of K_a with respect to the coefficient ring of K. This is a basis for the maximal order of K.
(6) Find a dual basis for (the equation order of) C.
(7) Take the intersection of the bases in (5) and (6) and construct the (mostly) maximal order M of C using it.
(8) If there are critical primes which are not totally ramified in the discriminant of K then we do not handle them in Algorithm 2 so M is not maximal and we handle all the critical primes as discussed in Section 4 to get the maximal order of C.

The maximal orders of the components C are then combined together (algorithm by Dr. Claus Fieker). Since it is easy to compute the discriminant of A from the class field theoretic input it is easy to determine whether this order is maximal and if it is not to compute its maximal order using the Discriminant algorithm (Buchmann and Lenstra, 1994).

6. Examples

We show calculations for a few simple examples. The first example has one ramified and one unramified prime.

Example 1. Consider $K/\mathbb{Q}$ given by $K = \mathbb{Q}[x]/\langle x^2 + 11\rangle, u = 11$. There are 2 primes dividing the discriminant of K. The prime 2 is critical and does not ramify in K, the prime 11 ramifies in K. We have $vu = 0$ at 2 and $vu = 1$ at 11. At the prime 2 we have $g = 0, k = 1, j = 0$. At the prime 11 we have $g = 1, k = -1, j = 1$. So we have a local 2-integral basis $\{\alpha^i\}_{i=0,1}$ and a local 11-integral basis $\{(\alpha^{-1}11)^i\}_{i=0,1}$ where $\alpha^2 = 11$. We compute the pseudo basis $(\{1, \alpha\}, \{1, 1\})$ at 2 using $k_0 = 0, t_0 = 0, k_1 = 1, t_1 = 0$ and $(\{1, \alpha\}, \{1, 11^{1-1}\})$ at 11 using $k_0 = 0, t_0 = 0, k_1 = 1, t_1 = -1$. So as far as we can compute $\{\alpha^i\}_i$ is an integral basis for K. This is unfortunately not the case since 2 is a critical prime and a 2-maximal order can be computed using the Round 4 algorithm, but at least we have a basis for the 11-maximal order.

We give an example of a function field which is a Kummer extension. This example contains primes which are neither totally ramified nor unramified.

Example 2. Consider $F/\mathbb{Q}(\zeta_8)(t)$ given by $F = \mathbb{Q}(\zeta_8)(t)[x]/\langle x^8 + 3t^4\rangle$. There is 1 prime dividing each of the finite and the infinite discriminants. Both primes, t and $1/t$, have $vu = 4$ and also $g = 4$. So we have a local t integral basis $\{(\alpha^2 t^{-1})^i(\alpha^{-1}t)^l\}_{0\le i<4, 0\le l<2}$ where $\alpha^8 = -3t^4$ and a local $1/t$ integral basis $\{(\gamma^2(1/t)^{-1})^i(\gamma^{-1}1/t)^l\}_{0\le i<4, 0\le l<2}$ where $\gamma^8 = -3/t^4$. We compute the pseudo basis

$$(\{1, \alpha^7, \alpha^2, \alpha, \alpha^4, \alpha^3, \alpha^6, \alpha^5\}, \{t^0, t^{-3}, t^{-1}, t^0, t^{-2}, t^{-1}, t^{-3}, t^{-2}\})$$

at t and

$$(\{1, \gamma^7, \gamma^2, \gamma, \gamma^4, \gamma^3, \gamma^6, \gamma^5\},$$
$$\{(1/t)^0, (1/t)^{-3}, (1/t)^{-1}, (1/t)^0, (1/t)^{-2}, (1/t)^{-1}, (1/t)^{-3}, (1/t)^{-2}\})$$

at $1/t$. At t we form the matrix with diagonal $\{1, 1, t^{-1}, t^{-1}, t^{-2}, t^{-2}, t^{-3}, t^{-3}\}$ which we multiply by (and pair with) the denominator t^3 to gain the transformation matrix of the (t) maximal order of F as a transformation of the finite equation order of F having basis $\{\alpha^i\}$ over a maximal coefficient ring. At $1/t$ we form the matrix with diagonal

$$\{1, 1, (1/t)^{-1}, (1/t)^{-1}, (1/t)^{-2}, (1/t)^{-2}, (1/t)^{-3}, (1/t)^{-3}\}$$

which we multiply by (and pair with) the denominator $(1/t)^3$ to gain the transformation matrix of the $(1/t)$ maximal order of F as a transformation of the infinite equation order having basis $\{\gamma^i\}$.

Note that the calculations here are identical for each prime since they share the same value of vu and the rest is substitution of primitive elements and primes.

The next example is represented as a relative extension. It contains 2 primes which are ramified and 5 which are partially ramified.

Example 3. Consider $F'/F(t)$ given by $F = \mathbb{F}_7(t)[x]/\langle x^3 + x + (t+1)/t^2\rangle, F' = F[x]/\langle x^6 + (t+1)(t+2)^3/t\rangle$. There are 5 primes dividing the finite discriminant and 2 primes dividing the infinite discriminant. These primes are ideals of either the finite maximal order of F or the infinite maximal order of F. There is 1 prime above t and 2 primes above each of $t+1$ and $t+2$, and we shall call these $P_0, P_{11}, P_{12}, P_{21}$ and P_{22} respectively. There are 2 primes above $1/t$ which shall call P_{1i} and P_{2i}—we consider these as infinite primes. We have $vu_0 = 15$, $vu_1 = 1$, $vu_2 = 3$ and $vu_i = 45$ (the valuation of u is the same for both primes lying over $t+1$, $t+2$ and $1/t$).

Let α be such that $\alpha^6 + t^5(t+1)(t+2)^3 = 0$, γ such that $\gamma^6 + (t+1)(t+2)^3/t^{49} = 0$ and let π_r be a uniformizing element for P_r. We compute a local P_0-integral basis $\{(\alpha^2\pi_0^{-5})^i(\alpha\pi_0^{-2})^l\}_{0\le i<3, 0\le l<2}$, a local P_{11} integral basis $\{\alpha^i\}$, a local P_{21} integral basis $\{(\alpha^2\pi_{21}^{-1})^i\alpha^l\}_{0\le i<3,0\le l<2}$ and a local P_{1i}-integral basis $\{(\gamma^2\pi_{1i}^{-15})^i(\gamma\pi_{1i}^{-7})^l\}_{0\le i<3,0\le l<2}$. We note that the P_{12}-integral basis differs to the P_{11}-integral basis only in the uniformizer, the P_{22}-integral basis differs to the P_{22}-integral basis only in the uniformizer and the P_{2i}-integral basis differs to the P_{1i}-integral basis only in the uniformizer because of their common values of vu.

We compute the pseudo bases

$$(\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}, \{1, P_0^{-2}, P_0^{-5}, P_0^{-7}, P_0^{-10}, P_0^{-12}\}) \text{ at } P_0,$$

$$(\{\alpha^i\}_{0\le i<6}, \{1\}_{0\le i<6}) \text{ at } P_{11} \text{ and } P_{12},$$

$$(\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}, \{1, 1, P_2^{-1}, P_2^{-1}, P_2^{-2}, P_2^{-2}\}) \text{ at } P_{21} \text{ and } P_{22}$$

and

$$(\{1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5\}, \{1, P_i^{-7}, P_i^{-15}, P_i^{-22}, P_i^{-30}, P_i^{-37}\}) \text{ at } P_{1i} \text{ and } P_{2i}$$

where we use the short hand P_1 to refer to either P_{11} or P_{12}, P_2 to refer to either P_{21} or P_{22} and P_i to refer to either P_{1i} and P_{2i}. Since F'/F is a relative representation we set the transformation matrices to the identity. The coefficient ideals in the pseudo matrix for P_0 are $\{1, P_0^{-2}, P_0^{-5}, P_0^{-7}, P_0^{-10}, P_0^{-14}\}$, for P_{11} and P_{12} are $\{1\}_{0\le i<6}$, for P_{21} and P_{22} are $\{1, 1, P_2^{-1}, P_2^{-1}, P_2^{-2}, P_2^{-2}\}$ and for P_{1i} and P_{2i} are $\{1, P_i^{-7}, P_i^{-15}, P_i^{-22}, P_i^{-30}, P_i^{-37}\}$.

7. Results

We give timings showing that Algorithms 2 and 3 are faster than previous algorithms for a range of fields. Note that the Round 2 algorithm involves randomness so timings for this algorithm may differ depending on seed.

Timings are given for an Intel(R) Core(TM)2 Extreme CPU X9650 3GHz (4GB RAM) machine running Magma V2.17-12 under Linux.

7.1. *Maximal orders of number fields*

Computing maximal orders of degree n Kummer extensions of the cyclotomic field of order n showed that Algorithm 2 could be 10 times as fast even for some small examples. A comparison of timings is given in Table 1.

Table 1
Maximal order computation timings for Kummer extensions of cyclotomic fields.

$\mathbb{Q}(\zeta_n)/\langle x^n - a\rangle$	Algorithm 2	Round 2 or 4	Algorithm 2 is
$x^3 - 5^4$	0.01 s	0.02 s	2 times faster
$x^6 - 7^5$	0.07 s	0.11 s	1.5 times faster
$x^9 - 2^4$	0.42 s	4.26 s	10 times faster
$x^{12} - 5^7$	0.35 s	3.21 s	9 times faster

Table 2
Maximal order computation timings for Kummer extensions of function fields.

Field	Algorithm 2	Round 2	Algorithm 2 is
$\mathbb{Q}(\zeta_8)(t)[x]/\langle x^8 - 3t^4\rangle$ (finite)	0.00 s	0.04 s	
$\mathbb{Q}(\zeta_8)(t)[x]/\langle x^8 - 3t^4\rangle$ (infinite)	0.01 s	0.09 s	9 times faster
$\mathbb{Q}(\zeta_{20})(t)[x]/\langle x^{20} - 7t^{11}\rangle$ (finite)	0.02 s	1.21	60 times faster
$\mathbb{Q}(\zeta_{20})(t)[x]/\langle x^{20} - 7t^{11}\rangle$ (infinite)	0.02 s	3.59	179 times faster
$\mathbb{Q}(t)(\zeta_7)[x]/\langle x^7 + t\zeta_7\rangle$ (finite)	0.00 s	0.06 s	
$\mathbb{Q}(t)(\zeta_7)[x]/\langle x^7 + t\zeta_7\rangle$ (infinite)	0.01 s	163.56 s	16 000 times faster

Table 3
Maximal order computation timings for Kummer extensions of function fields occurring in abelian extensions.

Algorithm	Maximum time	Average time
Algorithm 2 (Finite)	2.38 s	0.696s
Round 2 (Finite)	211.45 s	56.54 s
Algorithm 2 (Infinite)	5.33 s	0.167s
Round 2 (Infinite)	117.74 s	4.855 s

7.2. *Maximal orders of function fields*

We give the timings from some simple examples in Table 2.

We ran a batch of maximal order computations for function fields related to abelian extensions. Let $F = \mathbb{F}_9(t)[x]/\langle x^3 + x + 1/t + 1/t^2\rangle$. We form a divisor D by adding together some places of F of degree 2, compute its ray class group R and form the quotient Q of R by $8R$. We compute the subgroups of Q and compute an abelian extension for D and each subgroup. Let F_i' be the extension of F defined by the defining polynomial of the ith abelian extension (of degree 8). There were 448 fields F_i'. Some timings for the computations of the finite and infinite maximal orders of F_i' are given in Table 3.

We also ran Algorithm 2 on the Kummer extensions given as examples in Fraatz (2005) Section 5.1. In Table 4 we give the averages of times from our implementation and that of Fraatz (2005) for comparison. Fraatz (2005) divided his Kummer extension examples into 3 groups, we compute an average for each of those groups. The first group of examples are of the form $F' = F[y]/\langle y^n - u\rangle$ where $F = \mathbb{F}_q(t)[x]/\langle x^5 + 4x^4 + t^2x^3 + 2x^2 + t^5x + t + 1\rangle$, ρ is a primitive element of F, q is a power of 5 and $u = \frac{t^{11}+4t^{10}+t^8+4t^7+t^5+4t^4+t^2+4t+1}{t^4+4t^3+t+4}\rho^4 + \frac{1}{t^2+3}\rho + t^2$. The second group are of the form $F' = F[y]/\langle y^n - u\rangle$ where $F = \mathbb{F}_q(t)[x]/\langle x^2 + 2x + t^3 + t + 1\rangle$, ρ is a primitive element of F, q is a power of 3 and $u = 1/t^2\rho + t^2$. The third group are of the form $F' = F[y]/\langle y^n - u\rangle$ where $F = \mathbb{F}_q(t)[x]/\langle x^3 - (t+1)x^2 + 2tx - t^5\rangle$, ρ is a primitive element of F, q is a power of 3 and $u = (t^3+2)\rho^2 + (t^2+1)\rho + 1$. Fraatz (2005) gave timings for finite maximal order computations for the first group of examples and timings for infinite maximal order computations for the third group of examples. We will do likewise. As in Fraatz (2005) we consider the finite primes as those which lie

Table 4
Comparison of average times for examples from Fraatz (2005).

Examples	n	Algorithm 2	Round 2	Fraatz (2005)
1–6	11–24	1.52 s	737.06 s	117.89 s
7–14	28–160	236.64 s	188 309 s (e.g. 7–11 only)	1948.9 s (805 s)
15–20	5–29	0.308 s	185.79s	5.49 s

Table 5
Comparison of average timings of maximal order computations for abelian fields.

Degree	Algorithm 3	Round 2	Difference
8	24.615 s	33.888 s	1.3 times faster
9	1.34 s	133.37 s (27 s)	99 (20) times faster
11	7 s	573.839 s (411.66 s)	81 (58) times faster
16	25.98 s	3964.19 s (2048.59 s)	152 (78) times faster

Table 6
Comparison of timings for maximal order computations of radical extensions.

Extension	Algorithm 2	Round 2	Similar to Daberkow (1995)
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{12}+\sqrt{-t}\rangle$ (finite)	0.00 s	0.1 s	0.03 s
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{12}+\sqrt{-t}\rangle$ (infinite)	0.03 s	11.4 s	0.78 s
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (finite)	0.01 s	0.13 s	564.42
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (infinite)	0.04 s	15.88 s	2461.82 s
$\mathbb{F}_{101}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (finite)	0.00 s	0.00 s	0.1 s
$\mathbb{F}_{101}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (infinite)	0.03 s	14.34 s	1.73 s

above polynomials in t and the infinite primes as those which lie above $1/t$. Since we cannot reproduce or better the timings given in Fraatz (2005) for group 2 we give an average of the times given in Fraatz (2005) in brackets.

7.3. *Maximal orders of abelian fields*

Let $F = \mathbb{Q}[x]/\langle x^2 - 2\rangle$. We compute the ray class group R of a divisor in F and take the quotient Q of R by nR where n will be the degree of the resulting number fields. For some subgroups of Q we compute an abelian extension A and compute the maximal order of A using both Algorithm 3 and the default Round 2 algorithm. Some average times are given in Table 5.

There was 1 degree 9 example which took over 1000 s, 1 degree 11 example which took over 2000 s and 1 degree 16 example which took over 100 000 s using the Round 2 or Discriminant (Buchmann and Lenstra, 1994) algorithms. Removing these times from the average computations resulted in averages of 27 s, 411.66 s and 2048.59 s (respectively) for the rest.

In Fieker (2006) Section 3.4 there is a genus computation which took almost 9000 s. This computation takes less than 0.1 s using the techniques described in this paper.

7.4. *Maximal orders of radical extensions*

We compare times of implementations of Algorithm 2, Round 2 and the approach similar to Daberkow (1995) for radical extensions in Tables 6 and 7, as much as practical.

In Table 7 we use extensions of $\mathbb{F}_{101}(t)[y]/\langle y^3 + y^2 + y + t\rangle$ of a range of degrees and give average times for 10 random radical extensions of each degree 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 is a random integer in the range $[1 \ldots 5]$ randomly multiplied by either 1 or 2.

Table 7
Comparison of average timings for maximal order computations of radical extensions.

Degree	Algorithm 2	Round 2	Similar to Daberkow (1995)
11 (finite)	0.125 s	12.77 s	148.45 s
11 (infinite)	0.029 s	11.44 s	1305.34 s
12 (finite)	0.074 s	19.53 s	0.291 s
12 (infinite)	0.035 s	28.32 s	0.557 s
13 (finite)	0.152 s	24.8 s	33.31 s
13 (infinite)	0.042 s	23.39 s	27.93 s
14 (finite)	0.082 s	34.85 s	9.57 s
14 (infinite)	0.048 s	36.53 s	25.12 s
15 (finite)	0.123 s	40.5 s	0.679 s
15 (infinite)	0.05 s	52.53 s	0.733 s
19 (finite)	0.384 s	115.538 s	221.02 s
19 (infinite)	0.1 s	203.455 s	771.646 s
21 (finite)	0.35 s	183.28 s	92 s
21 (infinite)	0.099 s	349.21	52 s
22 (finite)	0.157 s	237.6 s	253.64 s
22 (infinite)	0.14 s	439.38 s	3176.34 s
23 (finite)	0.387 s	275.149 s	406.5 s
23 (infinite)	0.148 s	530.516 s	6569 s
27 (finite)	0.951 s	614.88 s	>2440 s
27 (infinite)	0.179 s	1303.3 s	>52825 s
28 (finite)	0.255 s	739.9 s	56 s
28 (infinite)	0.271 s	1759.23 s	72 s
29 (finite)	0.643 s	835.2 s	>7467 s
29 (infinite)	0.248 s	2083 s	>112 062 s
30 (finite)	0.188 s	1013.4 s	2.55 s
30 (infinite)	0.22 s	1957 s	6.86 s
31 (finite)	0.703 s	1130.83 s	91.6 s
31 (infinite)	0.571 s	2245.44 s	38.3 s

Acknowledgement

The author would like to thank Dr Claus Fieker for his help in implementing the algorithms described in this paper.

References

Baier, G., Zum Round 4 Algorithmus, Master's Thesis, Technische Universit Berlin, 1996.

Buchmann, Johannes A., Lenstra Jr., Hendrik W., 1994. Approximating rings of integers in number fields. J. Théor. Nombres Bordeaux 6 (2), 221–260.

J.J. Cannon, W. Bosma, C. Fieker, and A. Steel (Eds.), Handbook of Magma functions (V2.16), Computational Algebra Group, University of Sydney, 2009. http://magma.maths.usyd.edu.au.

Chistov, A.L., 1989. The complexity of constructing the ring of integers of a global field. Soviet Math. Dokl. 597–600 (English translation).

Cohen, H., 2000. Advanced Topics in Computational Number Theory. Springer.

Daberkow, M., Über die Bestimmung der ganzen Elemente in Radikalerweiterungen algebraischer Zahlkörper, Ph.D. Thesis, TU-Berlin, 1995.

Daberkow, M., 2001. On computations in Kummer extensions. J. Symbolic Comput. 31 (1–2), 113–131.

Fieker, C., 2006. Class theory of global fields. In: Cannon, J.J., Bosma, W. (Eds.), Discovering Mathematics with Magma. Springer.

Ford, D., Letard, P., 1994. Implementing the round four maximal order algorithm. J. Théor. Nombres Bordeaux (6), 39–80. http://almira.math.u-bordeaux.fr:80/jtnb/1994-1/jtnb6-1.html.

Fraatz, R., Computation of maximal orders of cyclic extensions of function fields, Ph.D. Thesis, TU-Berlin, 2005.

Hecke, E., 1954. Vorlesung über die Theorie der Algebraischen Zahlen. Akademische Verlags-gesellschaft Geest & Portig K.-G.

Hecke, E., 1981. Lectures on the Theory of Algebraic Numbers. Springer-Verlag.

Hoppe, A., Normal forms over Dedekind domains—efficient implementation in the computer algebra system KANT, Ph.D. Thesis, TU-Berlin, 1998.

Pauli, S., 2001. Factoring polynomials over local fields. J. Symbolic Comput. 32, 533–547.

Pohst, M.E., 1996. Computational aspects of Kummer theory. In: Cohen, Henri (Eds.), Algorithmic Number Theory. Second International Symposium, ANTS-II, Talence, France, May 18–23, 1996. Proceedings. In: Lect. Notes Comput. Sci., 1122. Springer, Berlin, pp. 259–272. 1996.

Pohst, M., Zassenhaus, H., 1989. Algorithmic Algebraic Number Theory. Cambridge University Press.

Stichtenoth, H., 1993. Algebraic Function Fields and Codes. Springer-Verlag.