Bull. Aust. Math. Soc. **93** (2016), 513–515
doi:10.1017/S0004972715001793

ALGORITHMS FOR GALOIS EXTENSIONS OF GLOBAL FUNCTION FIELDS

NICOLE SUTHERLAND

(Received 15 November 2015; first published online 17 February 2016)

2010 *Mathematics subject classification*: primary 11R58; secondary 11R32, 11R37, 11Y16, 11Y40, 14H05.

Keywords and phrases: function fields, cyclic Galois extensions, integral closures, maximal orders, Galois groups.

This thesis considers some computational problems in cyclic Galois extensions of global function fields. We investigate the efficient computation of integral closures, or maximal orders, in cyclic extensions of global fields and the determination of Galois groups for polynomials over global function fields.

Global function fields, which are finite separable extensions of a global rational function field, are interesting because they provide a basis for designing efficient algorithms for algebraic curves. Applications of curves and function fields arise in coding theory and cryptography. Efficient computation with curves or function fields is necessary for efficient construction of codes.

In this thesis, we consider function fields from the number theory point of view, and take advantage of algorithms for number fields (such as those in [2]), which can be used analogously for function fields. Algorithms are stated generally, so it is irrelevant whether the field is a number or a function field and whether or not it is represented as an extension of another algebraic (function) field.

Some tasks have a rich history for number fields but have only recently sparked interest for function fields. These include the development of methods to efficiently compute integral closures (an analogue of $\mathbb{Z}$), Galois groups, class groups and unit groups, which are the four most important tasks of number theory considered by Zassenhaus [6]. We investigate two of these. Integral closures can be used to compute class groups, unit groups and Galois groups, which are the other three important tasks.

Also interesting for function fields is the computation of Riemann–Roch spaces of divisors and the genus. The calculation of a basis for a Riemann–Roch space can use the representation of a divisor by ideals of integral closures. Improving the efficiency

Thesis submitted to the University of Sydney in September 2014; degree approved on 1 June 2015; supervisors Claus Fieker and Stephen Donnelly.

of the computation of integral closures can therefore improve the computation of the genus, Riemann–Roch spaces and divisor class groups.

Function fields defined over a finite field k (with characteristic $p > 0$), along with number fields, are *global fields*. Both types of global fields have a class field theory which allows abelian extensions to be classified completely. Abelian extensions allow us to construct families of fields where we can control the genus and the number of rational places and they provide a way of computing these values for such extensions relatively cheaply. In order to use these fields explicitly and compute the rational places, we need to be able to compute integral closures in these fields efficiently.

To construct an algebraic–geometric code from a function field involves the computation of some rational places of the function field, the construction of a divisor and the computation of a basis for its Riemann–Roch space. The minimum distance of a code is linked to the genus and the number of rational places of the function field. Algebraic–geometric codes are interesting because curves with many rational points tend to have high minimum distances, which is good for reliable transmission of information. Class field theory can be used to generate curves with many rational points compared to their genus [3].

Efficient algorithms make possible a wider range of applications. The construction of algebraic–geometric codes from much larger cyclic field extensions benefits from improved efficiency in the integral closure computation. To achieve this, efficient algorithms for computing integral closures specifically for Kummer, Artin–Schreier and Artin–Schreier–Witt extensions are investigated. These algorithms are efficient because they compute a global (pseudo) basis for such orders. We show that we have removed one of the barriers to constructing good codes from larger cyclic extensions.

In cyclic extensions, the combination of the local maximal orders can be done efficiently and a (pseudo) basis can be written down directly for the global maximal orders. Calculating a basis for the maximal orders 'by hand', which we show can be easily done, saves much computation time in computing a basis from generators. The special shape of the defining polynomials means that, in many cases, we can avoid, for the first time, any normal form computations. This is possible for cyclic extensions because of the relationship between the constant coefficient and the discriminant of the polynomial and also between the constant coefficient and the primitive element of the extension. Additionally, we compute integral closures without computing any other subrings of the function field (as the round 2 method does) and without factoring (or sometimes even computing) the discriminant of the defining polynomial.

For Kummer extensions (more generally, radical extensions), we give an efficient algorithm to compute a diagonal basis for integral closures. In Artin–Schreier extensions, our efficient algorithm computes a triangular basis for integral closures. In Artin–Schreier–Witt extensions, we have been able to compute a (pseudo) basis for S-maximal orders where S contains primes of the same ramification degree, rather than generators corresponding to each individual prime. To combine S-maximal orders for different ramification degrees, we minimise the number of pseudogenerators which are input to the normal form computation. We also compute a basis for a degree p^n extension rather than the Artin–Schreier–Witt tower of n extensions of

degree p, as in [5]. These cyclic extensions cover all possibilities for components of abelian extensions.

Since abelian and cyclic extensions are types of Galois extensions and computing Galois groups is also considered to be an important task of number theory, we describe an algorithm to compute Galois groups of polynomials of unrestricted degree over global function fields. Since Stauduhar developed an interesting practical algorithm [7] for the computation of Galois groups, there have been a number of other algorithms described but these have mostly been specific to irreducible polynomials over the rational field. We consider the recent algorithm of Fieker and Klüners [4] and describe how to adjust this algorithm so that it can be used to compute Galois groups of polynomials over characteristic p function fields, including when the characteristic is two (in which case replacement invariants were required). Further, we provide an algorithm to compute Galois groups of reducible polynomials, including those over function fields of characteristic p.

Most of the results in this thesis have been published in [8, 9, 11], or are being revised for publication in [10]. All of the algorithms described in this thesis have been implemented by the author in the Magma Computer Algebra System [1] (V2.16, V2.17, V2.18, V2.20 and later) and perform effectively as is shown by a number of examples and a collection of timings.

References

[1] J. J. Cannon, W. Bosma, C. Fieker and A. Steel (eds.), *Handbook of Magma Functions (V2.20)* (Computational Algebra Group, University of Sydney, 2013), http://magma.maths.usyd.edu.au, 2013.
[2] H. Cohen, *Advanced Topics in Computational Number Theory* (Springer, New York, 2000).
[3] V. Ducet and C. Fieker, 'Computing equations of curves with many points', in: *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, OBS (eds. E. Howe and K. Kedlaya) (Mathematical Sciences Publishers, Berkeley, 2012).
[4] C. Fieker and J. Klüners, 'Computation of Galois groups of rational polynomials', *London Math. Soc. J. Comput. Math.* **17**(1) (2014), 141–158.
[5] R. Fraatz, *Computation of Maximal Orders of Cyclic Extensions of Function Fields*, PhD Thesis, Technische Universität Berlin, 2005.
[6] M. Pohst, 'In memoriam: Hans Zassenhaus', *J. Number Theory* **47** (1994), 1–19.
[7] R. P. Stauduhar, 'The determination of Galois groups', *Math. Comput.* **27** (1973), 981–996.
[8] N. Sutherland, 'Efficient computation of maximal orders in radical (including Kummer) extensions', *J. Symbolic Comput.* **47** (2012), 552–567.
[9] N. Sutherland, 'Efficient computation of maximal orders in Artin–Schreier extensions', *J. Symbolic Comput.* **53** (2013), 26–39.
[10] N. Sutherland, 'Efficient computation of maximal orders in Artin–Schreier–Witt extensions', *J. Symbolic Comput.*, in revision.
[11] N. Sutherland, 'Computing Galois groups of polynomials (especially over function fields of prime characteristic)', *J. Symbolic Comput.* **71** (2015), 73–97.

NICOLE SUTHERLAND, Computational Algebra Group,
School of Mathematics and Statistics, University of Sydney,
NSW 2006, Australia
e-mail: nicole.j.sutherland@bigpond.com

https://doi.org/10.1017/S0004972715001793 Published online by Cambridge University Press