

RESEARCH STATEMENT

ERIC LANDQUIST

1. INTRODUCTION

My primary research interests are computational algebraic number theory and cryptography. More specifically, these interests include integer factorization and the discrete logarithm problem in various groups, but my current research focuses on cubic function fields of large prime characteristic. In particular, my research centers on the computation of certain invariants of these fields: the divisor and ideal class numbers, regulator, and the fundamental units of the maximal order. The computation of these invariants of number fields and function fields are central problems in algorithmic algebraic number theory. One of the main reasons for their importance, especially the class numbers, is that they are the order of certain groups that have potential application to cryptography. Any cryptographic setting requires, among other things, a group of large non-smooth order. Although it is possible that cubic function fields will be of direct use for cryptography, it is more likely that insights gained from their study may be applied for use in protocols based on quadratic, i.e. elliptic and hyperelliptic, function fields, which do have serious potential for use today. Aside from these applications, these fields do give rise to some very interesting theoretical problems which we have only begun to understand.

In this statement, I will begin with a brief overview of the notation and terminology of this subject, along with some historical points of interest. In the third section, I will describe results of my thesis, followed in the next section by some remaining problems and projects that I plan to work on for my post-doctoral work. Lastly I will conclude with some career research goals based on my current interests and directions.

2. BACKGROUND

Let $\mathbb{F}_q(x)$ be the field of rational functions with coefficients in \mathbb{F}_q , where $q > 3$ is prime. Analogously to number fields, we may define a finite algebraic extension K over $\mathbb{F}_q(x)$. Let $F(x, y)$ be an absolutely irreducible cubic polynomial in y with coefficients in $\mathbb{F}_q[x]$. We can write $F(x, y) = y^3 - A(x)y + B(x) = 0$, where $B(x)$ is nonzero, and there does not exist a polynomial $Q(x) \in \mathbb{F}_q[x]$ such that $Q^2(x) \mid A(x)$ and $Q^3(x) \mid B(x)$. Then $K = \mathbb{F}_q(x, y)$ is a separable extension of $\mathbb{F}_q(x)$ of degree 3. If $A(x) = 0$, then K is said to be a purely cubic function field. We define h to be the divisor class number of K , or in other words, the order of the divisor class group, or Jacobian, of K . The Hasse-Weil Theorem tells us that h lies in the interval $\left[(\sqrt{q} - 1)^{2g}, (\sqrt{q} + 1)^{2g} \right]$, where g is the genus of K .

Let \mathcal{O}_K be the maximal order of K , let $\mathcal{O}_K^* \cong \mathbb{F}_q \times \mathbb{Z}^r$ be the unit group of \mathcal{O}_K , and let h_K denote the (ideal) class number of \mathcal{O}_K , that is the order of the (ideal) class group of \mathcal{O}_K . If the unit rank r is positive, then we define any generating set of the free part of \mathcal{O}_K^* as the fundamental units of \mathcal{O}_K (or K). We denote this set $\{\epsilon_1, \dots, \epsilon_r\}$. We note that in the unit

rank 1 case, ϵ is unique up to constant multiples and inversion, but in the unit rank 2 case, the set of fundamental units is not uniquely determined in this way.

The ϵ_i are doubly exponential in the size of K , so fundamental units cannot be computed in fields of large characteristic or genus. For fields of large characteristic or genus, we instead wish to compute a related, but more tractable quantity called the regulator, R . We will define this for the various unit ranks based on the splitting of infinity. If the place at infinity splits $\infty = \infty_0 \cdots \infty_r$, then let v_i be the additive discrete valuation corresponding to ∞_i . In unit rank 0, $R = 1$; in unit rank 1, $R = |v_1(\epsilon)| = |v_0(\epsilon)|/2$; and finally in unit rank 2,

$$R = \left| \det \begin{pmatrix} v_0(\epsilon_1) & v_0(\epsilon_2) \\ v_1(\epsilon_1) & v_1(\epsilon_2) \end{pmatrix} \right| .$$

Despite the fact that the set of fundamental units is not unique, R is independent of these choices in any unit rank.

To relate these quantities, if f is the greatest common divisor of the inertia degrees of the ∞_i , then $fh = Rh_K$. In most cases, $f = 1$ so that $h = Rh_K$. For positive unit rank, h_K will generally be very small, usually trivial, so that h is a small multiple of R .

In the unit rank 1 and 2 cases, the ideal class group is not very interesting, but in the principal ideal class, we instead find a very curious object of study that in addition aids us in computing the fundamental units and regulator. This is the infrastructure of the principal ideal class, which we denote

$$\mathcal{R} = \{ \mathfrak{f} \in [\mathcal{O}] \mid \mathfrak{f} \text{ is reduced} \} .$$

This set almost forms a group under ideal composition, i.e. ideal multiplication followed by reduction; it is nonassociative. In fact, any function field or number field of positive unit rank exhibits an infrastructure. The infrastructure was first discovered in real quadratic number fields by Shanks [5], and provides the framework for the fastest known algorithms to compute the desired invariants in many of these fields. Infrastructure in unit rank 1 fields is a cycle with an additional operation called a baby step that maps an ideal to an adjacent ideal on the cycle. This baby step is similar to addition by 1 in $\mathbb{Z}/n\mathbb{Z}$. In unit rank 2 however, the infrastructure is toroidal in structure, bicyclic, but irregular; there are baby steps in two directions in this situation. (There are baby steps in three possible directions in fact, but we are mainly concerned with the two.) The unit rank 2 situation is very interesting mathematically, and presents us with some unique problems because we must now study how two cycles behave and interact. This is one of the main motivations for my research.

3. CURRENT RESEARCH

My thesis research is divided into three components. The first component develops ideal arithmetic in purely cubic function fields and the second gives results on optimizing class number computation in unit rank 0 fields. The last component lays a divisor theoretic foundation for infrastructure in cubic function fields. This has helped us to understand the structure and arithmetic of infrastructure, in particular the unit rank 2 case, and has led to insights into how general infrastructure behaves in function fields of higher degree and higher unit rank. This understanding will allow us to then compute class numbers and regulators in unit rank 2 fields much faster than current methods allow. In fact, there is evidence that class numbers can be computed faster in the unit rank 2 setting than in the other cases.

The first contribution of my thesis work describes the ideal arithmetic of all purely cubic function fields. In [3], Scheidler described ideal squaring and the multiplication of two

ideals that do not share any factors. Later, Bauer [1] described this arithmetic for all fields defined by a nonsingular polynomial. Therefore my thesis extends this work to describe the multiplication of any two ideals in the singular case as well, completing the description of ideal arithmetic in purely cubic function fields of characteristic at least 5. This arithmetic was then implemented in order to compute divisor class numbers.

A method due to Scheidler and Stein [4] computes divisor class numbers in time roughly $O(q^{(2g-1)/5})$, an improvement over previous techniques for $g \geq 3$. They use an Euler product form of the L -polynomial of a cubic function field K to find an estimate E of h and an upper bound U on the error $|h - E|$ so that h lies in the interval $[E - U, E + U]$. For fields of genus at least 3, this interval is smaller than the Hasse-Weil interval. One of two methods then searches for h , either Shanks' baby step-giant step algorithm or the parallelized kangaroo method due to Pollard. My work in this area centers on looking for ways to improve either the estimation phase or the search phase, and then implementing these methods and improvements. The most fruitful results thus far have been in the search phase. Class numbers are not evenly distributed in the interval $[E - U, E + U]$, so I have collected data to find the average error $\frac{|h-E|}{U}$ for various genera. This has allowed us to make near optimal parameter selections and speed up overall running times. Using these techniques, 25-digit class numbers have been computed for imaginary cubic fields of genus 3 and 4.

It is not yet known how to apply the aforementioned technique to compute regulators of unit rank 2 fields, so the last portion of my thesis work seeks to understand this case. My approach to this involves explaining the theory of infrastructure in terms of divisor arithmetic rather than ideal arithmetic. This has provided an explanation of infrastructure that is clearer and more intuitive than the traditional approach, which is based on ideals. In unit rank 1 fields, the place at infinity splits $\infty = \infty_0 \infty_1$, where $\deg(\infty_1) = 2$. Thus $\text{div}(\epsilon) = R(\infty_1 - 2\infty_0)$. Elements of \mathcal{R} are principal ideals typically written $\mathfrak{f} = \langle \theta^{-1} \rangle$, where θ can be chosen so that $0 \leq \deg(\theta) < R/2$. We define the distance of \mathfrak{f} to be $\delta(\mathfrak{f}) = \deg(\theta)$. Baby steps are shown to produce ideals in which the distance increases until a fundamental unit (or regulator) is reached. Likewise the distance of the composition of two ideals is roughly the sum of the distances of the individual ideals. In unit rank 2, ∞ splits completely and we have two fundamental units, which are of the form

$$\text{div}(\epsilon_i) = v_1(\epsilon_i)(\infty_1 - \infty_0) - v_2(\epsilon_i)(\infty_0 - \infty_2) ,$$

for $i = 1, 2$. Thus the two baby step directions are shown to produce reduced ideals whose divisor is incremented by $\infty_1 - \infty_0$ or by $\infty_0 - \infty_2$, depending on which direction the step is taken in. We nevertheless define the distance of an ideal $\mathfrak{f} = \langle \theta \rangle$ to be the ordered triple $\delta(\mathfrak{f}) = (\deg(\theta), \deg(\theta'), \deg(\theta''))$. Using this language of divisors, my thesis extends the results and algorithms of unit rank 1 infrastructure in [3] to unit rank 2 infrastructure and improves many of the bounds as well, such as those on the norms of ideals in \mathcal{R} and the maximum length of a baby step.

4. FUTURE RESEARCH

My goals for postdoctoral research are to use this divisor theoretic understanding of \mathcal{R} to significantly improve the running time of class number and regulator computations in cubic function fields and implement algorithms for unit rank 1 and 2 models of cubic function fields. With the arithmetic now in place, implementing a unit rank 1 baby step-giant step or kangaroo regulator algorithm will be a straightforward extension of methods used in

hyperelliptic infrastructure. (See [6].) The unit rank 2 situation is more complicated. A procedure to compute the regulator and fundamental units of a cubic function field was developed by Scheidler et al. in [2]. This approach only uses baby steps to find the two periods of \mathcal{R} , however. There are a couple obstructions to incorporating giant steps in order to speed up the computations. First, the composition of two ideals on one period is not necessarily on the same period. Secondly, the period corresponding to the second baby step has a twisting behavior around the torus and intersects the first period in a currently unpredictable location. I therefore plan to learn more about the behavior of unit rank 2 infrastructure and the properties of the periods such as the respective lengths of the two periods and the length and existence of preperiods in particular. Once this is accomplished, I will be able to apply Scheidler and Stein's class number computation method to the unit rank 2 setting. By splitting their interval $[E - U, E + U]$ into two, significant speed gains should be realized. At first, however, only fields with certain characteristics will be investigated to determine criteria for these properties.

Another goal is to generalize the arithmetic of purely cubic function fields to arbitrary cubic function fields of characteristic greater than 3. I wish to develop libraries that perform arithmetic in cubic function fields as well, building on the package that I am currently using. When it is completed, this library will be available for public use. A deeper knowledge and understanding of infrastructure of arbitrary unit rank will also be sought.

5. CAREER RESEARCH GOALS

Understanding unit rank 2 infrastructure in cubic function fields is a pivotal step to understanding infrastructure of fields of higher degree and of greater unit rank because of the presence of multiple periods and structural dimensions. One of my long term visions is therefore to work towards the development of a general infrastructure theory spanning global fields of all unit ranks. This will have to be a team effort, and I have contact with a number of other researchers working in this area, so this goal is certainly attainable. After sufficient progress has been made in cubic fields of unit rank 2, the next step in this generalization will be to consider quartic function fields of unit rank 2 and 3. This theory will be applied to computing class numbers and regulators, with explorations into improved techniques for effective computations. This area of study as a whole is relatively unexplored, but is a mathematically fascinating area of research with consequences that cannot yet be imagined.

REFERENCES

- [1] M. Bauer. The Arithmetic of certain cubic function fields. *Math. Comp.*, **73**:387–413, 2004.
- [2] Y. Lee, R. Scheidler, and C. Yarrish. Computation of the fundamental units and the regulator of a cyclic cubic function field. *Exp. Math.*, **12**(2):211–225, 2003.
- [3] R. Scheidler. Ideal arithmetic and infrastructure in purely cubic function fields. *J. Théor. Nombres Bordeaux*, **13**:609–631, 2001.
- [4] R. Scheidler and A. Stein. Class number approximation in cubic function fields. *Contrib. Discrete Math.*, **2**:107–132, 2007.
- [5] D. Shanks. The infrastructure of a real quadratic field and its applications. *Proc. 1972 Number Theory Conference*, Boulder, 217–224, 1972.
- [6] A. Stein and E. Teske. The parallelized Pollard kangaroo method in real quadratic function fields. *Math. Comp.*, **71**: 793–814, 2002.