USING CLASS FIELD THEORY TO CONSTRUCT CURVES WITH MANY POINTS

KRISTIN LAUTER AND MICHAEL ZIEVE

The Weil bound says that the number of $\mathbb{F}_q$-rational points on a genus-g curve is at most $q + 1 + 2g\sqrt{q}$. Various improvements to this bound are due to Stark, Manin, Ihara, Serre, Drinfeld-Vladut, Oesterlé, Stöhr-Voloch, Lauter, and others. In order to test whether these improved bounds are best possible, it is necessary to construct curves with many points.

We need a supply of curves for which we can quickly compute the basic invariants (genus, number of rational points). In this project the curves we use are abelian covers of the projective line. Class field theory provides a description of all such covers, so the steps of this project are:

1. Compute the invariants of curves beginning from the class field theoretic description;
2. Make choices of the class field theoretic data which will yield curves with many points;
3. Compute explicit equations for the corresponding curves, by means of Carlitz modules.

In the second step, by 'curves with many points' we mean curves whose number of $\mathbb{F}_q$-rational points comes close to the best known upper bound for that choice of g and q. Of course, the closer the better!

We will split into two groups; one group will focus on the first two steps, the other will focus on the third. These steps are described in more detail in the next three sections. The fourth section discusses further directions we can pursue if time permits.

1. Class field theory

For a detailed introduction to class field theory constructions of curves with many rational points, see [8] and [6].

In this section we recall the relevant facts from class field theory. For convenience, we use the language of function fields (for which a basic

Date: February 17, 2000.

reference is [10]). Let $K = \mathbb{F}_q(t)$ and $R = \mathbb{F}_q[t]$. We often identify irreducible polynomials in R with the corresponding places of K.

Theorem. *For any nonconstant polynomial $M \in R$, there exists an abelian extension L_M/K with these properties:*

1. $\mathrm{Gal}(L_M/K) \cong (R/M)^*/{\mathbb{F}_q}^*$.
2. *The infinite place of K splits completely in L_M; in particular, $\mathbb{F}_q$ is the full constant field of L_M.*
3. *If $P \in R$ is irreducible and coprime to M, then the place P is unramified in L_M/K, and its decomposition group is generated by the image of P in $(R/M)^*/{\mathbb{F}_q}^*$.*
4. *Let $P \in R$ be an irreducible factor of M with multiplicity r, and let $G^n(P)$ be the n-th ramification group of P in L_M/K (in the upper numbering, cf. [9]). If $n > r-1$ then $G^n(P) = 1$; if $0 \le n \le r-1$ then $G^n(P)$ is the subgroup of $(\mathbb{F}_q[x]/M)^*/{\mathbb{F}_q}^*$ generated by polynomials congruent to 1 mod $M/P^{r-\lceil n \rceil}$.*

In fact, the above conditions uniquely determine L_M.[1] Moreover, if L/K is any finite abelian extension in which the infinite place splits completely, there is an M for which L_M contains L. But we will not need these last two facts in what follows.

If L is a function field over $\mathbb{F}_q$, let $N(L)$ denote the number of degree-one places on L (equivalently, the number of $\mathbb{F}_q$-rational points on the curve corresponding to L). For any finite abelian extension L/K, we have $N(L) \ge [L:K]n_s + n_r$, where n_s (resp., n_r) denotes the number of degree-one places of K which split completely (resp., are totally ramified) in L/K. As a warm-up exercise, write down an exact formula for n. Recall the definition of decomposition field: if L/K is a finite abelian extension and P is a place of K, then the maximal subextension of L/K in which P splits completely is the subfield of L fixed by the decomposition group of P.

Our strategy for producing curves with many points is as follows: choose a set S of degree-one places of K which contains the infinite place, and choose a nonconstant polynomial $M \in R$. Let L be the subfield of L_M fixed by (the group generated by) the decomposition groups at all the places in S. Then $N(L) \ge [L:K] \cdot \#S$. The genus of L can be computed via the Riemann-Hurwitz formula and Hilbert's theory of ramification groups (cf. [9, pp. 61–76] and [6, Prop. 1]).

Problem: for various choices of q, S, and M, compute the genus and number of degree-one places on the corresponding field L.

[1] Terminology: L_M is the maximal abelian extension of K in which the conductor divides M and the infinite place splits completely.

2. Choosing the parameters

In the previous section we constructed certain extensions $L/\mathbb{F}_q(x)$ depending on three parameters: q, S, and M. Now try to find choices of these parameters for which $N(L)$ comes close to the known upper bounds for that choice of q and g. For small g and q, tables of best known upper and lower bounds can be found in [3]. Tables of the curves obtained by letting S contain all places of degree one except one can be found in [7].

3. Carlitz modules

The Carlitz module enables one to write down explicit equations for the fields L_M in the above Theorem. The basic idea is as follows: starting from $M(t) \in R = \mathbb{F}_q[t]$, there is a recipe for writing down an associated polynomial $\Psi_M(u) \in R[u]$ together with a natural action of $(R/M)^*$ on the roots of Ψ_M. It turns out that this action induces an isomorphism $\mathrm{Gal}(\widehat{L_M}/K) \cong (R/M)^*$, where $\widehat{L_M}$ is the splitting field of Ψ_M over K. Then L_M is the subfield of $\widehat{L_M}$ fixed by ${\mathbb{F}_q}^*$. The polynomials Ψ_M and the action of $(R/M)^*$ are defined in [4, p. 79].

For this part of the project, begin by reading the first four sections of [4]. In those seven pages, Hayes gives a self-contained proof of most of our Theorem. First problem: complete the proof of the Theorem.

Now compute some examples of fields $\widehat{L_M}$. Then compute examples of L_M, and then examples of quotients of L_M by decomposition groups over rational places of K. Finally, compute equations for the fields described by the other group of students (these will be quotients of certain fields L_M).

4. Further directions

You may have noticed that, when applying the Theorem for fixed q, it is difficult to produce curves which have large genus and which have many $\mathbb{F}_q$-rational points (relative to their genus). Try to find infinite families of curves over $\mathbb{F}_q$, for fixed q, which have as many points as possible (relative to their genus). It turns out that, if we fix q and only consider genus-g curves which are abelian covers of the projective line, then as g grows the number of $\mathbb{F}_q$-rational points on such a curve cannot grow linearly in g (whereas all the upper bounds of Weil et al. are linear in g) – in fact, this number of points is at most $c_q g/\log g$ (where c_q is a constant depending only on q). This result is due to Frey, Perret, and Stichtenoth; read their elegant proof in [2] (hint: first trace through their proof in case all ramification is tame, to see the key ideas). For fixed q, can you find abelian covers of the projective line which have any prescribed genus $g > 1$ and which have at least $g/\log g$ rational points over $\mathbb{F}_q$? (Such covers do exist, for every q and g.)

One can also study abelian covers of curves other than the projective line. For an explicit treatment of class field theory in this case, see [5]; for a non-explicit treatment, see [1]. If there is time and interest, carry out any of the above steps in this more general setting.

References

[1] R. Auer, *Ray class fields of global function fields with many rational places*, math.AG/9803065

[2] G. Frey, M. Perret, and H. Stichtenoth, *On the different of abelian extensions of global fields*, pp. 26–32 in: Coding Theory and Algebraic Geometry (H. Stichtenoth and M. A. Tsfasman, eds.), Springer-Verlag, New York, 1992.

[3] G. van der Geer, M. van der Vlugt, Tables of curves with many points, to appear in Mathematics of Computation. available at: `http://www.wins.uva.nl/~geer/publications.html`

[4] D. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 74–91.

[5] D. Hayes, *A brief introduction to Drinfeld modules*, pp. 1–32 in: The Arithmetic of Function Fields (D. Goss et al., eds.), W. de Gruyter, Berlin, 1992.

[6] K. Lauter, *Deligne-Lusztig curves as ray class fields*, available at: `http://www.mpim-bonn.mpg.de/cgi-bin/preprint/preprint_search.pl`

[7] K. Lauter, *A Formula for Constructing Curves over Finite Fields with Many Rational Points*, Journal of Number Theory **74**, 56-72 (1999). available at: `http://www.mpim-bonn.mpg.de/cgi-bin/preprint/preprint_search.pl`

[8] R. Schoof, Algebraic curves and coding theory,, UTM 336, Univ. of Trento, 1990.

[9] J.-P. Serre, Local Fields, Springer-Verlag, New York, 1979.

[10] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

E-mail address: `klauter@microsoft.com`

E-mail address: `zieve@math.usc.edu`