

BASES FOR RIEMANN-ROCH SPACES OF CYCLIC CURVES

D. JOYNER, A. KSIR, AND T. SHASKA

ABSTRACT. Let C denote an algebraic curve with equation $y^n = f(x)$ and D an effective divisor on C . We give an explicit constructive method for computing a basis B of $L(D)$. In particular, it is done in such a way that if $E < D$ is another effective divisor, the basis B_E of $L(E)$ so constructed will be a subset of B . We plan to use this in future work to compute quotient representations, with applications to AG codes. We use **SAGE** to compute an example in some detail for a hyperelliptic curve.

In this paper¹, we give a simple procedure for computing bases of Riemann-Roch spaces of divisors on cyclic curves, which we call the “pivot method”. The method does not depend on the size of the genus of the curve, and strongly resembles the Gauss elimination method for matrices. Though it is probably known to experts, the formulation we present does not seem to have appeared explicitly in the literature. It seems to be a very specific version of Coates’ algorithm (see Coates [C], Davenport [D], and Berry [B1]). Also, there are strong similarities to ideas discussed in §3 of Berry [B2], though our calculations allow a more general class of divisors.

A cyclic curve is an algebraic curve C such that there exist a normal cyclic subgroup $C_m \triangleleft \text{Aut}(C)$ such that $g(C/C_m) = 0$. An equation of such curve can be given by $y^n = f(x)$. In the first section, we give a brief introduction to normal cyclic curves and describe a simple algorithm to construct functions with prescribed poles on such curves. This generalizes previous work of the first two authors for hyperelliptic curves.

In the second section we use this construction to compute bases for Riemann-Roch spaces on cyclic curves. In particular, for effective divisors D and E with $E < D$, we compute bases B_1 of $L(E)$ and B_2 of $L(D)$ such that $B_1 \subset B_2$.

The third section discusses the implementation of such algorithm in **SAGE**. Furthermore, it contains two examples for hyperelliptic curves: one general example on an interesting curve, and one more specific example where the calculations are partially done using **SAGE** [S]. The algorithm described here is included in the file `rrbasis3.sage` (implemented by the first author [J]), in the case of hyperelliptic curves where the divisors are effective and the support of D does not contain any points fixed by the hyperelliptic involution. We intend to implement the full version of the algorithm in **SAGE**.

Notation: Throughout this paper C denotes a cyclic curve defined over a field k of characteristic not equal to 2. $\text{Aut}(C)$ denotes the group of automorphisms defined over the algebraic closure of k .

¹This paper is licensed under the Attribution-ShareAlike Creative Commons license, <http://creativecommons.org/about/licenses/meet-the-licenses>.

1. GENERAL BACKGROUND

This section both defines notation and recalls well-known facts about cyclic curves.

A cyclic curve is an algebraic curve C such that there exist a normal cyclic subgroup $C_m \triangleleft \text{Aut}(C)$ such that $g(C/C_m) = 0$. Then $\bar{G} = G/C_m$ embeds as a finite subgroup of $PGL(2, \mathbb{C})$. The equation of cyclic curve can be given by the following

$$(1.1) \quad y^m = h(x) = \prod_{i=1}^s (x - \alpha_i)^{d_i}, \quad 0 < d_i < m.$$

Specifically, let C be a smooth curve defined in affine coordinates by $y^m = h(x)$, where $h(x)$ is a polynomial of degree $d > 3$. Then the discriminant of $h(x)$ is non-zero. We denote by n be the projective degree of the curve.

Let $\iota : C \rightarrow C$ denote the order m normal automorphism such that $C_m = \langle \iota \rangle$, sending a point $P = (x, y) \in C$ to $\iota(P) = P^* = (x, \xi_m y)$, where ξ_m is the m -th primitive root of unity. Let $\rho : C \rightarrow \mathbb{P}^1 = C/C_m$ denote the projection defined in affine coordinates by $(x, y) \mapsto x$, so $\rho^{-1}(\rho(P)) = \{P, \iota(P)\}$. A point P on C is ramified with respect to ρ if and only if it is a fixed point of ι .

When we say ‘‘ramification point’’, we always mean ramification point with respect to ρ , and when we say a point is ‘‘unramified’’, we always mean that it is not a ramification point with respect to ρ .

If $h(x)$ has odd degree, then there is one ramified point at infinity, which we label P_0 ; if $h(x)$ has even degree then there are two unramified points at infinity, which we label P_0 and P_0^* . For simplicity of notation, let $P_0^* = P_0$ in the odd degree case.

The following result summarizes some of what is known about the function field $F(C)$ and the affine coordinate ring $F[C] = F[x, y]/(y^m - h(x))$.

Proposition 1. (a) $F[C]$ is finitely generated as an $F[x]$ -module and is integral over $F[x]$. Moreover, as an F -vector space

$$F(C) = F(x) \oplus yF(x).$$

(b) $F[C]$ is finitely generated as an $F[y]$ -module and is integral over $F[y]$. Moreover, as an F -vector space

$$F(C) = F(y) \oplus xF(y) \oplus \cdots \oplus x^{d-1}F(y).$$

(c) If d is odd, the pole x_0 of $y \in F(y)$ has a unique extension P_0 to a totally ramified place of degree 1 of C with ramification index $e(P_0/x_0) = d$. Moreover,

$$\text{div}_\infty(x) = 2P_0, \quad \text{div}_{P_0}(y) = dP_0.$$

(d) If d is even, the pole x_0 of $y \in F(y)$ has two extensions P_0, P_0^* to unramified places of degree 1 of C with ramification indices $e(P_0^*/x_0) = e(P_0/x_0) = d/2$. Moreover,

$$\text{div}_\infty(x) = P_0 + P_0^*, \quad \text{div}_\infty(y) = (d/2)P_0 + (d/2)P_0^*.$$

(e) If d is odd,

$$L(rP_0) = \text{Span}\{x^i y^j \mid 2i + dj \leq r, 0 \leq i, 0 \leq j \leq d-1\}.$$

2. FUNCTIONS WITH PRESCRIBED POLES ON CYCLIC CURVES

We use the notation of the previous section. Let $\mathcal{P} = \{x_0, x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}\} \subset \mathbb{P}^1$ denote a finite set, where x_{r+1}, \dots, x_{r+s} are branch points of ρ , x_1, \dots, x_r are not branch points, and $x_0 = \infty \in \mathbb{P}^1$. For each $p \in \rho^{-1}(\mathcal{P})$, let $e_p \geq 0$ be an integer. Let D be the effective divisor on C defined by

$$D = \sum_{x \in \mathcal{P}} \sum_{p \in \rho^{-1}(x)} e_p \cdot p.$$

If $x = x_i \in \mathcal{P}$ and if $\rho^{-1}(x)$ contains two points, let $e_i^* = \min_{p \in \rho^{-1}(x)} e_p$ and let $e_i = \max_{p \in \rho^{-1}(x)} e_p$. If $\rho^{-1}(x_i) = \{p\}$ is a singleton, let $e_i^* = 0$ and $e_i = e_p$. In this case, we have

$$D = e_0 P_0 + e_1 P_1 \dots + e_r P_r + e_0^* P_0^* + e_1^* P_1^* \dots + e_r^* P_r^* \\ + e_{r+1} P_{r+1} + \dots + e_{r+s} P_{r+s}$$

where P_1, \dots, P_r are finite unramified points, $e_i \geq e_i^*$ for $i = 0, \dots, r$, and P_{r+1}, \dots, P_{r+s} are finite ramified points. (Recall $e_0^* = 0$ if d is odd.) Let (x_i, y_i) be the coordinates of P_i , $1 \leq i \leq r$. Note if $1 \leq i \leq r$ then $(x_i, -y_i)$ are the coordinates of P_i^* , and if $i > r$ then $y_i = 0$.

Proposition 2. *Let C be as above. Let D be an effective divisor on C as above with the following properties:*

- (1) y_1, \dots, y_r are all distinct
- (2) $e_i \geq e_i^*$ for $i = 0, \dots, r$
- (3) $e_1 + \dots + e_r \geq d/2$
- (4) e_{r+1}, \dots, e_{r+s} , and e_0 if d is odd, are either all even or all odd.

Then there is a function g with polar divisor D which is a linear combination of functions of the form:

- (a) $\frac{y}{\prod_{i=0}^{s-1} (x-x_i)^{e_i}}$,
- (b) $\frac{1}{(x-x_i)^m}$ ($0 < m \leq e_i$),
- (c) the monomial functions $x^i y^j$ ($i \geq 0, j = 0, 1$),
- (d) the ‘‘mixed’’ functions $\frac{y x^a}{\prod_{i=0}^{s-1} (x-x_i)^{d_i}}$ ($d_i < e_i$).

Remark 1. (a) If $P = (a, b)$ is an affine ramification point for ρ then

- (i) $b = 0$ and a is a root of h ,
- (ii) $1/(x-a)$ has a pole of order 2 at P .

If $P = (a, b)$ is an unramified affine point for ρ then

- (i) $b \neq 0$ and a is not a root of h ,
- (ii) $1/(x-a)$ has a pole of order 1 at P and a pole of order 1 at P^* .

(b) When d is even, C embeds into projective space using the $(1, g+1, 1)$ -weighted projective model with coordinates (X, Y, Z) and equation

$$Y^2 = h(X/Z)Z^d,$$

where $x = X/Z$, $y = Y/Z^{d/2}$. Assume $h(x)$ is monic. Let $\infty_+ = [1 : 1 : 0]$ and $\infty_- = [1 : -1 : 0]$ denote the two points at infinity. The coordinate x

has a pole of order 1 at ∞_+ and ∞_- ; y has a pole of order $d/2$ at each of these points. In particular,

$$g_+(x, y) = \frac{y - x^{d/2}}{x^{d/2}}$$

has a zero of order 1 at ∞_+ and

$$g_-(x, y) = \frac{y + x^{d/2}}{x^{d/2}}$$

has a zero of order 1 at ∞_- .

- (c) When d is odd, C has equation

$$Y^2 = h(X/Z)Z^{d+1},$$

where $x = X/Z$, $y = Y/Z^{\frac{d+1}{2}}$. In this case,

$$g(x, y) = \frac{y}{x^{\frac{d+1}{2}}},$$

has a zero of order 1 at ∞ . Let $\infty = [1 : 0 : 0]$ denote the point at infinity. At ∞ , x has a pole of order 2 and y has a pole of order d .

- (d) If d is odd, the ramification divisor R has degree $d + 1$ (it is the effective divisor given by the sum of the point at infinity plus all the affine points $(x, y) = (\alpha, 0)$, where α denotes a root of $h(x) = 0$). In this case, the canonical divisor has degree $d - 3$.
- (e) If d is even, the ramification divisor R has degree d (it is the same as in the odd case above, but without the point at infinity). In this case, the canonical divisor has degree $d - 4$.

Proof: Properties (1) and (3) ensure that for any point P , $\dim L(D - P) = \dim L(D) - 1$, so there is a function with polar divisor D . We will construct such a function out of the types of functions mentioned in the statement of the theorem. Our method is reminiscent of row reduction for matrices.

First we consider some special cases.

- If (a) the support of D does not contain a point at infinity, (b) $e_i = e_i^*$ for all unramified points and (c) e_i is even for all ramified points (except possibly at infinity), then D is the pullback (via ρ) of a divisor on \mathbb{P}^1 . Indeed, let

$$a = \sum_{P_i \text{ unramified}} e_i + \sum_{P_i \text{ ramified}} \frac{e_i}{2},$$

and let $p(x)$ be a polynomial of degree a with no roots among x_1, \dots, x_{r+s} . Then the function

$$(2.1) \quad f(x, y) = \frac{p(x)}{\prod_{i=1}^r (x - x_i)^{e_i} \prod_{i=r+1}^{r+s} (x - x_i)^{e_i/2}}$$

will have polar divisor D .

- If (a) the support of D does not contain a point at infinity, (b) $e_i = e_i^*$ for all unramified points and (c) e_i is odd for all ramified points (except possibly at infinity), then let

$$a = \sum_{P_i \text{ unramified}} e_i + \sum_{P_i \text{ ramified}} \frac{e_i + 1}{2} - \frac{d}{2},$$

if d is even, and

$$a = \sum_{P_i \text{ unramified}} e_i + \sum_{P_i \text{ ramified}} \frac{e_i + 1}{2} - \frac{d + 1}{2},$$

if d is odd. Let $p(x)$ be a polynomial of degree a with no roots among x_1, \dots, x_{r+s} . Then the function

$$(2.2) \quad f(x, y) = \frac{p(x)y}{\prod_{i=1}^r (x - x_i)^{e_i} \prod_{i=r+1}^{r+s} (x - x_i)^{(e_i+1)/2}}$$

will have polar divisor D .

In the general case, where $e_i > e_i^*$ for at least one unramified point P_i , let

$$a = \begin{cases} \sum_{i=1}^r e_i + \frac{e_0 - d}{2}, & d \text{ odd and } e_0 \text{ even,} \\ \sum_{i=1}^r e_i + \frac{e_0 + 1 - d}{2}, & d \text{ odd and } e_0 \text{ odd,} \\ \sum_{i=0}^r e_i - \frac{d}{2}, & d \text{ even,} \end{cases}$$

and let $p(x)$ be a polynomial of degree a in x with no roots among the x -coordinates of the points in the support of D . Let

$$\beta_i(x) = \begin{cases} (x - x_i)^{e_i}, & 1 \leq i \leq r, \\ (x - x_i)^{e_i/2}, & i \geq r, e_i \text{ even,} \\ (x - x_i)^{(e_i+1)/2}, & i \geq r, e_i \text{ odd.} \end{cases}$$

We define a **seed function** as follows. Choose an initial index $i_0 > 0$ such that P_{i_0} is an affine unramified point on C and $e_{i_0} > e_{i_0}^*$ ². Let

$$f_{0,D}(x, y) = \frac{(y + y_{i_0})p(x)}{\prod_{i=1}^{r+s} \beta_i(x)}.$$

Because of this, if e_i is even for all ramified P_i then $\text{div}_\infty(f_{0,D}(x, y))$ is

$$\begin{aligned} \text{div}_\infty(f_{0,D}(x, y)) &= e_0 P_0 (+e_0 P_0^*) + e_1 P_1 + e_1 P_1^* + \dots \\ &\quad + e_{i_0} P_{i_0} + (e_{i_0} - 1) P_{i_0}^* + \dots + e_r P_r + e_r P_r^* \\ &\quad + \sum_{i=1}^s e_{r+i} P_{r+i}. \end{aligned}$$

If e_i is odd for all ramified P_i , then $\text{div}_\infty(f_{0,D}(x, y))$ is

²For future reference, by analogy with Gauss elimination/row reduction, we call the point $P_{i_0}^*$ a **pivot point**.

$$\begin{aligned} \operatorname{div}_\infty(f_{0,D}(x,y)) &= e_0P_0(+e_0P_0^*) + e_1P_1 + e_1P_1^* + \dots \\ &\quad + e_{i_0}P_{i_0} + (e_{i_0} - 1)P_{i_0}^* + \dots + e_rP_r + e_rP_r^* \\ &\quad + \sum_{i=1}^s (e_{r+i} + 1)P_{r+i}. \end{aligned}$$

Now if $e_{i_0}^* < e_{i_0} - 1$, we will **pivot** until the pole at $P_{i_0}^*$ is $e_{i_0}^*$. Observe that the function

$$f_{i,m}(x,y) = \frac{1}{(x - x_i)^m}$$

has

$$\operatorname{div}_\infty(f_{i,m}(x,y)) = mP_i + mP_i^*.$$

We call the $f_{i_0,m}$ the **pivot functions** ($m > 0$).

It follows from an expansion in terms of a local coordinate or from the usual partial fraction decomposition of rational functions (see for example §5.11 in [GG]) that there is a constant $c \neq 0$ such that the divisor of $g = f_{0,D} - cf_{i_0,e_{i_0}-1}$ is

$$\begin{aligned} \operatorname{div}_\infty(g) &= e_0P_0(+e_0P_0^*) + e_1P_1 + e_1P_1^* + \dots \\ &\quad + e_{i_0}P_{i_0} + (e_{i_0} - 2)P_{i_0}^* + \dots + e_rP_r + e_rP_r^* \\ &\quad + \sum_{i=1}^s e_{r+i}P_{r+i}. \end{aligned}$$

if e_{r+i} is even, or

$$\begin{aligned} \operatorname{div}_\infty(g) &= e_0P_0(+e_0P_0^*) + e_1P_1 + e_1P_1^* + \dots \\ &\quad + e_{i_0}P_{i_0} + (e_{i_0} - 2)P_{i_0}^* + \dots + e_rP_r + e_rP_r^* \\ &\quad + \sum_{i=1}^s (e_{r+i} + 1)P_{r+i}. \end{aligned}$$

if e_{r+i} is odd. Thus we have reduced the multiplicity of the pole at $P_{i_0}^*$ by one.

The constant c is determined by the following calculation: choose a local parameter t such that $t = 0$ when $(x,y) = P_{i_0}^*$; for example $t = x - x_{i_0}$. Expand $f_{0,D}$ and $f_{i_0,e_{i_0}-1}$ as power series in t , so $f_{0,D}(x,y) = a \cdot t^{-e_{i_0}+1} + \text{higher order terms}$, and $f_{i_0,e_{i_0}-1}(x,y) = b \cdot t^{-e_{i_0}+1} + \dots$ then $c = a/b$.

Using the other pivot functions, we may compute constants c_i such that the function

$$\begin{aligned} f_{1,D}(x,y) &= f_0(x,y) - c_1f_{i_0,e_{i_0}-1}(x,y) \\ &\quad - c_2f_{i_0,e_{i_0}-2}(x,y) - \dots - c_{e_{i_0}}f_{i_0,0}(x,y) \end{aligned}$$

has divisor

$$\begin{aligned} \operatorname{div}_\infty(f_{1,D}(x, y)) &= e_0P_0(+e_0P_0^*) + e_1P_1 + e_1P_1^* + \dots \\ &\quad + e_{i_0}P_{i_0} + (e_{i_0}^*)P_{i_0}^* + \dots + e_rP_r + e_rP_r^* \\ &\quad + \sum_{i=1}^s e_{r+i}P_{r+i}, \end{aligned}$$

if e_{r+i} is even, or

$$\begin{aligned} \operatorname{div}_\infty(f_{1,D}(x, y)) &= e_0P_0(+e_0P_0^*) + e_1P_1 + e_1P_1^* + \dots \\ &\quad + e_{i_0}P_{i_0} + (e_{i_0}^*)P_{i_0}^* + \dots + e_rP_r + e_rP_r^* \\ &\quad + \sum_{i=1}^s (e_{r+i} + 1)P_{r+i}, \end{aligned}$$

if e_{r+i} is odd. In other words, we have reduced the order of the pole at the pivot point $P_{i_0}^*$ from e_{i_0} to $e_{i_0}^*$.

Now, if there is one, choose a new index i_1 , $1 \leq i_1 \leq r$, where P_{i_1} is unramified and $e_{i_1} \neq e_{i_1}^*$. Using $f_{1,D}$ and proceeding as above, we may compute $f_{2,D}$, reducing the order of the pole at the new pivot point $P_{i_1}^*$ to $e_{i_1}^*$. Proceeding inductively, in this way we may reduce the orders of all of the poles at the finite unramified pivot points. If d is even, and $e_0^* \neq e_0$, then we may use P_0^* as a pivot point with powers of x as the pivot functions. By this procedure, we find a function which we will call $f_{r,D}$ such that

$$\begin{aligned} \operatorname{div}_\infty(f_{r,D}(x, y)) &= e_0P_0(+e_0^*P_0^*) + e_1P_1 + e_1^*P_1^* + \dots \\ &\quad + e_rP_r + e_r^*P_r^* + \sum_{i=1}^s e_{r+i}P_{r+i}, \end{aligned}$$

if e_{r+i} is even, or

$$\begin{aligned} \operatorname{div}_\infty(f_{r,D}(x, y)) &= e_0P_0(+e_0^*P_0^*) + e_1P_1 + e_1^*P_1^* + \dots \\ &\quad + e_rP_r + e_r^*P_r^* + \sum_{i=1}^s (e_{r+i} + 1)P_{r+i}, \end{aligned}$$

if e_{r+i} is odd. In the first case, we are done: $\operatorname{div}_\infty(f_{r,D}(x, y)) = D$. In the second case, we pivot once at each of the ramified points P_{r+1}, \dots, P_{r+s} using the pivot function $f_{r+i, \frac{e_{r+i}+1}{2}}$ to remove the one excess pole.

Summarizing, we have constructed an element $g_D \in L(D)$ with pole divisor D , as desired. \square

3. BASES OF RIEMANN-ROCH SPACES FOR CYCLIC CURVES

Let C be a smooth hyperelliptic curve $y^2 = h(x)$, as in section 2 and

$$D = e_0P_0 + e_1P_1 \dots + e_rP_r(+e_0^*P_0^*) + e_1^*P_1^* \dots + e_r^*P_r^*(+e_{r+1}P_{r+1})$$

be a divisor on C , where as in section 2, P_1, \dots, P_r are finite unramified points, and $e_i \geq e_i^*$ for $i = 0, \dots, r$. In this section we only consider divisors D with at

most one ramified point in the support of D . Thus if the degree d of $h(x)$ is even, we may have one finite ramified point P_{r+1} in the support of D ; otherwise if d is odd, omit both terms in parentheses in the above expression.

If D satisfies the conditions of Proposition 2, then D is non-special, so by the Riemann-Roch theorem, we have

$$\dim L(D) = \deg(D) + 1 - g.$$

Theorem 3. *Let C and D be as above, and assume that D satisfies the conditions of Proposition 2. Then there is a basis of $L(D)$ consisting of functions which are linear combinations of*

- (a) $\frac{y}{\prod_{i=0}^{s-1} (x-x_i)^{f_i}}$,
- (b) $\frac{1}{(x-x_i)^m}$ ($0 < m \leq f_i$),
- (c) the monomial functions $x^i y^j$ ($i \geq 0, j = 0, 1$),
- (d) the "mixed" functions $\frac{yx^a}{\prod_{i=0}^{s-1} (x-x_i)^{f_i}}$.

Proof: By Proposition 2, we can construct an element b_0 in $L(D)$ of the required form with polar divisor D . Now suppose that

- (1) $e_i^* = 0$ for $i = 0, \dots, r$,
- (2) $e_{r+1} = 0$, and
- (3) $e_1 + \dots + e_r = \lfloor \frac{d+1}{2} \rfloor$.

We will call such a divisor "minimal." If D is minimal, $\deg(D) = \lfloor \frac{d+1}{2} \rfloor = g + 1$, so $\dim L(D) = 2$. The functions $b_0, 1$ form a basis for $L(D)$.

Now suppose that D is not minimal. Then we can subtract a point P from D in such a way that $D - P$ still satisfies the conditions of Proposition 2. Then there is a function b_1 with polar divisor $D - P$. Because b_0 and b_1 have different polar divisors, they are independent. Now if $D - P$ is minimal, $\deg(D) = 1 + \lfloor \frac{d+1}{2} \rfloor = g + 2$, so $\dim L(D) = 3$. In this case the functions $b_0, b_1, 1$ form a basis for $L(D)$. If $D - P$ is not minimal, we again subtract a point and continue in the same manner. In the end, if $\deg D = m + \lfloor \frac{d+1}{2} \rfloor$, we will have subtracted m points and constructed $m + 1$ independent functions b_0, \dots, b_m . Since $\dim L(D) = m + 2$, the function $b_0, \dots, b_m, 1$ form a basis for $L(D)$. □

As an immediate consequence of the above proof, we have the following results.

Corollary 4. *Let C and D be as above, so*

$$D = e_0 P_0 + e_1 P_1 \dots + e_r P_r (+e_0^* P_0^*) + e_1^* P_1^* \dots + e_r^* P_r^* (+e_{r+1} P_{r+1}).$$

Let $E < D$ be an effective divisor, so that $\text{Supp}(E) \subseteq \text{Supp}(D)$, and if E is written as

$$E = a_0 P_0 + a_1 P_1 \dots + a_r P_r (+a_0^* P_0^*) + a_1^* P_1^* \dots + a_r^* P_r^* (+a_{r+1} P_{r+1}),$$

assume that $a_i \geq a_i^$ for $i = 0, \dots, r$. Then we can find bases B_1 of $L(E)$ and B_2 of $L(D)$ such that $B_1 \subset B_2$ and each function is of the form described in Theorem 3.*

Remark 2. *Note that the condition $a_i \geq a_i^*$ may not be true a priori, even if E satisfies the conditions of Proposition 2.*

Proof: Construct a basis of $L(D)$ as in the proof of Theorem 3, but subtracting the points in $D - E$ first. □

4. IMPLEMENTATION AND EXAMPLES

In this section we explicitly compute both by hand and using SAGE, showing how the syntax can be used. You need the file `rrbasis3.sage`, which also has examples included.

4.1. $y^2 = x^9 + x$ **over** $GF(5)$. Consider the genus $g = 4$ curve

$$(4.1) \quad C : y^2 = x^9 + x, \quad F = GF(5),$$

which has rational points

$$C(F) = \{\infty, (0, 0), (2, 2), (2, 3), (3, 1), (3, 4)\}.$$

Let $P_1 = (2, 2)$, $P_1^* = (2, 3)$, $P_2 = (3, 1)$, $P_2^* = (3, 4)$. Consider the divisors $D = 4P_1 + 2P_2$ and $E = 3P_1 + 2P_2$. We will use the above construction to compute a basis of $L(D)$ which contains a basis of $L(E)$.

Taking P_1^* as our pivot point, we use the local coordinate $t = x - 2$, which vanishes at P_1^* . We can compute the expansion of y in two ways: (a) from the power series of $y = -(x+x^9)^{1/2}$ or (b) by plugging a general power series expansion with unknown coefficients into (4.1) and solving the “upper triangular” system of equations recursively for the coefficients. This can be done using method (b) in SAGE [S], as is shown below.

We will need local parameters about P_1^* and P_2^* .

Lemma 5. • *Local parameters about $P_1^* = (2, 3)$: We have*

$$(4.2) \quad x = t + 2, \quad y = 3 + 3t^2 + t^3 + 3t^4 + 3t^6 + 3t^7 + t^8 + 2t^9 + O(t^{10}).$$

• *Local parameters about $P_2^* = (3, 4)$: We have*

$$(4.3) \quad x = t + 3, \quad y = 4 + 3t^2 + t^3 + 3t^4 + 3t^6 + 3t^7 + t^8 + 2t^9 + O(t^{10}).$$

Proof: This can be verified by a direct computation, plugging each set of equations into $y^2 - x^9 - x$. □

Using method (b) and SAGE we have:

```

SAGE
sage: attach "rrbasis3.sage"
sage: F = GF(5)
sage: pt = (2,3)
sage: A2 = AffineSpace(2, F, names = 'xy')
sage: R = A2.coordinate_ring()
sage: x, y = R.gens()
sage: f = y^2 - x^9 - x
sage: C = AffineCurve_GF(A2,f)
sage: C.local_coordinates(pt,9)
[2 + t, 3 + 3*t^2 + t^3 + 3*t^4 + 3*t^6 + 3*t^7 + t^8 + 2*t^9 + 3*t^11 + 3*t^12]
sage: pt=(3,4)
sage: C.local_coordinates(pt,9)
[3 + t, 4 + 4*t^2 + 2*t^3 + 4*t^4 + 4*t^6 + t^7 + 3*t^8 + 4*t^9 + t^11 + t^12]
```

This is obtained by plugging in a power series with arbitrary coefficients into $f(x, y) = 0$, thus obtaining an “upper triangular” system of non-linear equations. This system can be imported into Singular [Si], which comes with SAGE, and solved using Gröbner bases techniques.

Now that we have computed the local coordinates, we proceed to find bases of $L(D)$ and $L(E)$. We have $\dim L(D) = \dim L(4P_1 + 2P_2) = 3$ and $\dim L(E) = \dim L(3P_1 + 2P_2) = 2$, so we need to find one function with polar divisor D and one function with polar divisor E .

First we find a function with polar divisor D . With P_1^* as the pivot point, the seed function is

$$f_0(x, y) = f_{0,D}(x, y) = \frac{y-3}{(x-2)^4(x-3)^2},$$

with polar divisor $\operatorname{div}_\infty(f_0) = 4P_1 + 3P_1^* + 2P_2 + 2P_2^*$, and the pivot functions are

$$f_{2,m}(x, y) = \frac{1}{(x-2)^m},$$

each with polar divisor $mP_1 + mP_1^*$, for $m = 1, 2, 3$.

We use the previously calculated local coordinates and SAGE to calculate

$$\operatorname{div}(f_{0,D} - 3f_{2,2} - 2f_{2,1}) = 4P_1 + 2P_2 + 2P_2^*,$$

eliminating the excess pole at P_1^* . Now we pivot at the point P_2^* . Let the new seed be

$$f_{1,D}(x, y) = f_{0,D}(x, y) - 3f_{2,2}(x, y) - 2f_{2,1}(x, y).$$

The new pivot functions are $f_{3,m}(x, y) = \frac{1}{(x-3)^m}$, which has divisor $mP_2 + mP_2^*$, for $i = 1, 2$. A similar SAGE calculation implies

$$\operatorname{div}(f_{1,D}(x, y) - f_{3,2}(x, y) - f_{3,1}(x, y)) = 4P_1 + 2P_2.$$

This has eliminated the excess pole at P_2^* . We take

$$\begin{aligned} b_0(x, y) &= f_{0,D}(x, y) - 3f_{2,2}(x, y) - 2f_{2,3}(x, y) - f_{3,2}(x, y) - f_{3,1}(x, y) \\ &= \frac{y-3}{(x-2)^4(x-3)^2} - \frac{3}{(x-2)^2} - \frac{2}{x-2} - \frac{1}{(x-3)^2} - \frac{1}{x-3} \end{aligned}$$

to be our first basis element in $L(D) = L(4P_1 + 2P_2)$.

Now, we wish to find a function b_1 with polar divisor E . Again we will first pivot on P_1^* . Let

$$f_{0,E}(x, y) = \frac{y-3}{(x-2)^3(x-3)^2} \in L(3P_1 + 2P_1^* + 2P_2 + 2P_2^*),$$

be the seed function and let $f_{2,m}(x, y) = \frac{1}{(x-2)^m}$ be the pivot functions. We again use the expansion for x and y in terms of t given in (4.3). A SAGE calculation (omitted) shows that $\operatorname{div}(f_{0,E} - f_{2,m}) = 3P_1 + 2P_1 + 2P_2^*$, so we have removed the excess pole at P_1^* . We now pivot around the point P_2^* . Let the new seed be

$$f_{1,E}(x, y) = f_{0,E}(x, y) - f_{2,1}(x, y) \in L(3P_1 + 2P_1 + 2P_2^*)$$

and let $f_{3,m}(x, y) = \frac{1}{(x-3)^m}$ be the new pivot functions. Another SAGE calculation (omitted) shows that

$$f_{1,E}(x, y) - 4f_{3,2}(x, y) - f_{3,1}(x, y) \in L(3P_1 + 2P_2).$$

This has removed the excess pole at P_2^* , so we are done. The new basis element is

$$\begin{aligned} b_1(x, y) &= f_{0,E}(x, y) - f_{2,1}(x, y) - 4f_{3,2}(x, y) - f_{3,1}(x, y) \\ &= \frac{y-3}{(x-2)^3(x-3)^2} - \frac{1}{x-2} - \frac{4}{(x-3)^2} - \frac{1}{x-3}. \end{aligned}$$

Since the dimension of $L(4P_1 + 2P_2)$ is 3, we have only the constants left, so we take $\{b_0, b_1, 1\}$ as a basis for $L(D)$. As a consequence of the method, the subset $\{b_1, 1\}$ is a basis for $L(E)$.

In fact, this can be computed in SAGE using the commands:

```

SAGE
-----
sage: F = GF(5)
sage: A2 = AffineSpace(2, F, names = 'xy')
sage: R = A2.coordinate_ring()
sage: x, y = R.gens()
sage: f = y^2 - x^9 - x
sage: C = AffineCurve_GF(A2, f)
sage: pts = C.rational_points(); pts
[(0, 0), (2, 2), (2, 3), (3, 1), (3, 4)]
sage: D = C.divisor([(0, pts[1]), (0, pts[3])])
sage: E = C.divisor([(2, pts[1]), (4, pts[3])])
sage: b = riemann_roch_space(C, D, E)
sage: b

[(2 + y + x + x^2 + 2*x^3 + 3*x^4)/(4 + 4*x + 4*x^2 + 3*x^3 + x^4 + 4*x^5 + x^6),
 (2 + y + x + x^2 + 2*x^3 + 3*x^4)/(2 + x + 4*x^2 + 2*x^3 + 2*x^4 + x^5)]
sage: C.divisor_of_function(b[0])
-2*(3 + y, 3 + x) - 4*(2 + x, 4 + y)
sage: C.divisor_of_function(b[1])
(1 + y, 2 + x) - 2*(3 + y, 3 + x) - 3*(2 + x, 4 + y)

```

The functions in \mathbf{b} represent the basis elements of $L(4P_1 + 2P_2)$ given by the functions b_0 and b_1 above. In future versions of SAGE, some of these commands may have a different syntax.

5. CONCLUDING REMARKS

We thank T. Berry for useful email communications and the NARC for partial research support.

REFERENCES

- [A] J. Alperin, **Local representation theory** Cambridge Univ. Press, 1986.
- [B1] T. Berry, *On Coates' algorithm*, ACM SIGSAM Bulletin, Volume 17, Issue 2, May (1983)12 - 17.
<http://portal.acm.org/citation.cfm?id=1089330.1089333>
- [B2] —, *Construction of linear systems on hyperelliptic curves*, J. Symbolic Comp. **26**(1998)315-327.
- [C] J. Coates, *Construction of rational functions on a curve*, Proc. Cambridge Phil. Soc. **68** (1970)105-123.
- [D] H. J. Davenport, **On the integration of algebraic functions**, Lecture Notes in Comp. Sci., vol 102 (1981), Springer-Verlag.
- [G] N. Göb, *Computing the automorphism groups of hyperelliptic function fields*, available at <http://front.math.ucdavis.edu/math.NT/0305284>.
- [GG] J. von zur Gathen and J. Gerhard, **Modern computer algebra**, 2nd ed., Cambridge Univ. Press, 2003.
- [GJK] D. Glass, D. Joyner and A. Ksir, *Basis of Riemann-Roch G -modules for $y^2 = x^p - x$ over $GF(p)$* , preprint, 2007.
- [J] D. Joyner, `rrbasis3.sage`, at <http://sage.math.washington.edu/home/wdj/research/rrbasis3.sage>.
- [JK] D. Joyner and A. Ksir, *Decomposing representations of finite groups on Riemann-Roch spaces*, Proc. Amer. Math. Soc. **135** (2007), 3465-3476.
- [Si] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern (2005). <http://www.singular.uni-kl.de>.
- [S] William Stein, **SAGE: An open source mathematical software package**, <http://www.sagemath.org/>, <http://sage.scipy.org/>
- [Sti] H. Stichtenoth, **Algebraic function fields and codes**, Springer-Verlag, 1993.

MATHEMATICS DEPARTMENT, UNITED STATES NAVAL ACADEMY, ANNAPOLIS, MD 21402
E-mail address: `wdj@usna.edu`

MATHEMATICS DEPARTMENT, UNITED STATES NAVAL ACADEMY, ANNAPOLIS, MD 21402
E-mail address: `ksir@usna.edu`

546 SCIENCE AND ENGINEERING BUILDING, DEPARTMENT OF MATHEMATICS, OAKLAND UNIVERSITY, ROCHESTER, MI, 48309
E-mail address: `shaska@oakland.edu`