ALBANIAN JOURNAL
OF MATHEMATICS
Volume 5, Number 1, Pages 31–40
ISSN 1930-1235: (2011)

GENUS CALCULATIONS FOR TOWERS OF FUNCTION FIELDS ARISING FROM EQUATIONS OF C_{ab} CURVES

CALEB MCKINLEY SHOR

Abstract. We give a generalization of error-correcting code construction from C_{ab} curves by working with towers of algebraic function fields. The towers are constructed recursively, using defining equations of C_{ab} curves. In order to estimate the parameters of the corresponding one-point Goppa codes, one needs to calculate the genus. Instead of using the Hurwitz genus formula, for which one needs to know about ramification behavior, we use the Riemann-Roch theorem to get an upper bound for the genus by counting the number of Weierstrass gap numbers associated to a particular divisor. We provide a family of examples of towers which meet the bound.

1. Introduction

Let K be a perfect field, and let a and b be positive integers with $a > b$ and $\gcd(a, b) = 1$. Consider the polynomial $f \in K[x, y]$ given by

$$f(x, y) = \alpha_{a,0}x^a + \alpha_{0,b}y^b + \sum_{i,j} \alpha_{i,j}x^i y^j,$$

where $\alpha_{i,j} \in K$, $\alpha_{a,0}\alpha_{0,b} \neq 0$, and the summation is taken over non-negative integers i and j such that $aj + bi < ab$. The plane curve C defined by the equation $f = 0$ is called a C_{ab} curve. Such curves can be thought of as generalizations of the Weierstrass form of elliptic and hyperelliptic curves.

One has the following results (see Section 3.3 in [4], Proposition 4.6 in [5], or [3]). C is irreducible, with a single point at infinity. Let F/K be the associated function field, so $F = K(x, y)/(f)$. (We will use the function field notation of [8].) Let P_∞ be the unique place at infinity. If the affine points of C are non-singular, then the genus of C is $(a - 1)(b - 1)/2$, and the Riemann-Roch space $\mathcal{L}(mP_\infty)$ is generated by monomials of the form $x^i y^j$ where $aj + bi \leq m$. (In fact, a basis is $\{x^i y^j : 0 \leq i, 0 \leq j < b, aj + bi \leq m\}$.)

We will be concerned with the case where $K = \mathbb{F}_q$, the finite field with q elements. For the construction of geometric Goppa codes (as in [8], Chapter II), one uses a function field $F/\mathbb{F}_q$ of transcendence degree 1. For some divisor D, one needs to calculate a basis of functions for $\mathcal{L}(D)$ and then evaluate these functions at other rational places in the function field. A lower bound for the sum of the dimension and minimum distance of a Goppa code is known in terms of the genus of F. Since we can calculate a basis for $\mathcal{L}(mP_\infty)$ and know the genus of the function field of a non-singular C_{ab} curve, constructing a code with a C_{ab} curve essentially amounts to calculating rational places. Importantly, decoding methods exist for such curves, as is seen in [7].

In this paper, we present towers of function fields that give a generalization of the C_{ab} curve code constructions. These towers arise recursively from the defining equations of C_{ab} curves, which is explained in Section 2. Because of the way these towers are constructed, bases for the spaces $\mathcal{L}(mP_\infty)$ are easy to calculate. In Section 3, we explain why these bases consist of only monomials and then proceed to calculate an upper bound for the genus by counting the number of Weierstrass gap numbers. These results are summarized in Theorem 6. Examples of families of towers that achieve the bound are also given in Theorem 7.

2. Equations and valuations

Let C be a C_{ab} curve given by equation $f = 0$, for $f \in K[x, y]$. For each $n \geq 0$, let

$$C_n = \left\{(p_0, p_1, \dots, p_n) \in \mathbb{P}^1 \times \cdots \times \mathbb{P}^1 : (p_{j-1}, p_j) \in C \text{ for } j = 1, \dots, n\right\}.$$

Consider the associated tower of function fields $\mathcal{F} = (F_0, F_1, \dots)$, where $F_0 = K(x_0)$ and $F_n = F_{n-1}(x_n)$ for $n \geq 1$. The x_k are related by the equation

$$f(x_{k-1}, x_k) = 0$$

for $k = 1, \dots, n$.

F_0 is a rational function field. The divisor associated to the function x_0 is $P_0 - P_\infty$, where

$$P_0 = \left\{\frac{x_0 \cdot f(x_0)}{g(x_0)} : f(x_0), g(x_0) \in K[x_0], x_0 \nmid g(x_0)\right\}$$

and

$$P_\infty = \left\{\frac{f(x_0)}{g(x_0)} : \deg g > \deg f\right\}.$$

To each place, we have an associated valuation. For the purposes of this paper, we are only interested in the valuation associated to P_∞, which is defined as

$$v_\infty\left(\frac{f(x)}{g(x)}\right) = \deg g - \deg f.$$

Proposition 1. *Let P_∞^n denote a place in $\mathbb{P}_{F_n}$ lying above P_∞, and let v_∞^n be the valuation associated to that place. Then P_∞^n is the only place in $\mathbb{P}_{F_n}$ above P_∞ and $v_\infty^n(x_n) = -a^n$.*

Proof For induction, suppose $n = 0$. The statement holds because we have $F_0 = K(x_0)$, so P_∞^0 is the unique place at infinity in the rational function field and $v_\infty^0(x_0) = -1$.

Now, suppose the statement is true for $n = k$. Since x_k and x_{k+1} satisfy the equation

$$\alpha_{a,0}x_k^a + \alpha_{0,b}x_{k+1}^b + \sum_{aj+bi<ab} \alpha_{i,j}x_k^i x_{k+1}^j = 0,$$

we have

$$\begin{aligned} av_\infty^{k+1}(x_k) &= v_\infty^{k+1}\left(\alpha_{a,0}x_k^a\right) \\ &= v_\infty^{k+1}\left(\alpha_{0,b}x_{k+1}^b + \sum_{aj+ib<ab} \alpha_{i,j}x_k^i x_{k+1}^j\right) \\ &\geq \min\left(\{bv_\infty^{k+1}(x_{k+1})\} \cup \{iv_\infty^{k+1}(x_k) + jv_\infty^{k+1}(x_{k+1}) : aj + ib < ab\}\right), \end{aligned}$$

by the triangle inequality. For the sake of contradiction, suppose

$$iv_\infty^{k+1}(x_k) + jv_\infty^{k+1}(x_{k+1}) \leq bv_\infty^{k+1}(x_{k+1})$$

for some non-negative i, j with $aj + bi < ab$ such that the left-hand side of the inequality is minimal. Then

$$\frac{v_\infty^{k+1}(x_k)}{v_\infty^{k+1}(x_{k+1})} \geq \frac{b-j}{i},$$

and since $aj + bi < ab$, we have $\frac{b-j}{i} > \frac{b}{a}$, so

$$\frac{v_\infty^{k+1}(x_k)}{v_\infty^{k+1}(x_{k+1})} > \frac{b}{a},$$

which means

$$\frac{a}{b} > \frac{v_\infty^{k+1}(x_{k+1})}{v_\infty^{k+1}(x_k)}.$$

On the other hand, if

$$iv_\infty^{k+1}(x_k) + jv_\infty^{k+1}(x_{k+1}) \leq bv_\infty^{k+1}(x_{k+1})$$

for i and j with $aj + bi < ab$ such that the left-hand side is minimal, then by the triangle inequality above,

$$av_\infty^{k+1}(x_k) \geq iv_\infty^{k+1}(x_k) + jv_\infty^{k+1}(x_{k+1}).$$

This implies

$$\frac{a-i}{j} \leq \frac{v_\infty^{k+1}(x_{k+1})}{v_\infty^{k+1}(x_k)}.$$

Since $aj + bi < ab$, we have $\frac{a}{b} < \frac{a-i}{j}$. So

$$\frac{a}{b} < \frac{v_\infty^{k+1}(x_{k+1})}{v_\infty^{k+1}(x_k)}.$$

We have a contradiction to our initial assumption. Therefore, we must have

$$bv_\infty^{k+1}(x_{k+1}) < iv_\infty^{k+1}(x_k) + jv_\infty^{k+1}(x_{k+1})$$

for all i, j with $aj + bi < ab$. Using the strict triangle inequality, we see that

$$av_\infty^{k+1}(x_k) = bv_\infty^{k+1}(x_{k+1}).$$

Since $\gcd(a, b) = 1$, b must divide $v_\infty^{k+1}(x_k)$. Let e denote the ramification degree of P_∞^{k+1} over P_∞^k, so

$$e = \frac{v_\infty^{k+1}(f)}{v_\infty^k(f)}$$

for any $f \in P_\infty^k$. Taking $f = x_k$, we have $ev_\infty^k(x_k) = v_\infty^{k+1}(x_k)$. By the inductive hypothesis, $v_\infty^k(x_k) = -a^k$, so b must divide e. However, since F_{k+1}/F_k is an extension of degree b, the ramification degree is at most b. Therefore, $e = b$, so P_∞^{k+1} is totally ramified over P_∞^k. Since ramification behaves well in towers, P_∞^{k+1} is totally ramified over P_∞^0, and thus unique.

From the formula for the ramification index,

$$\begin{aligned} v_\infty^{k+1}(x_k) &= ev_\infty^k(x_k) \\ &= b(-a^k). \end{aligned}$$

Then, since $av_\infty^{k+1}(x_k) = bv_\infty^{k+1}(x_{k+1})$, we have

$$v_\infty^{k+1}(x_{k+1}) = -a^{k+1},$$

as desired.

By induction, the statement is true for all non-negative integers n. □

Corollary 2. *For $n \geq k$,*

$$v_\infty^n(x_k) = -a^k b^{n-k}.$$

Proof By the formula for the ramification index, we have

$$e(P_\infty^n | P_\infty^k) = \frac{v_\infty^n(x_k)}{v_\infty^k(x_k)},$$

so

$$v_\infty^n(x_k) = -a^k b^{n-k}.$$

From the previous proposition, we know P_∞^n is totally ramified over P_∞^k for all $k < n$ because ramification works transitively in towers. Thus, $e(P_\infty^n | P_\infty^k) = [F_n : F_k] = b^{n-k}$. We also know $v_\infty^k(x_k) = -a^k$. The result follows immediately. □

3. Calculating the genera

In order to calculate the genera, we will count the number of Weierstrass gap numbers of P_∞^n in F_n/K. We do so by considering the pole orders of monomials. In the first subsection, which is motivated by Proposition 14 in [6], we show that the set of pole orders of polynomials is the same as the set of pole orders of monomials. In the second subsection, we show that under certain conditions, one obtains no new pole orders with rational functions. In the third subsection, assuming certain conditions, we calculate the number of Weierstrass gap numbers resulting from monomials, which gives us the genus of the function field. In the fourth subsection, we give examples of towers which satisfy the conditions and hence for which the genus formula applies.

3.1. Valuations of polynomials.

Let

$$I_n = (f(x_0, x_1), \ldots, f(x_{n-1}, x_n)) \subset F_n$$

be the ideal of the curve C_n, and let

$$\Gamma = K[x_0, \ldots, x_n]/I_n$$

be the coordinate ring of C_n. For notation, let $R_b = \{0, 1, \ldots, b-1\}$ be the set of residues mod b.

Claim 1. *Any polynomial $g(x_0, \ldots, x_n) \in \Gamma$ can be written as*

$$g(x_0, \ldots, x_n) = \sum_{\mathbf{e} \in \mathbb{Z}^{\geq 0} \times (R_b)^n} \lambda_{\mathbf{e}} x_0^{e_0} \ldots x_n^{e_n},$$

for $\mathbf{e} = (e_0, e_1, \ldots, e_n)$ and $\lambda_{\mathbf{e}} \in k$. In particular, for $i = 1, \ldots, n$, one has $0 \leq e_i < b$.

Proof Given the polynomial g, one can first reduce all powers of x_n to be less than b using the relation $f(x_{n-1}, x_n) = 0$. One can then reduce all powers of x_{n-1} to be less than b using the relation $f(x_{n-2}, x_{n-1}) = 0$. As this does not affect powers of x_n, one can continue on to reduce all powers of x_{n-2}, …, x_1, giving the resulting form. □

We will call a polynomial written in this form *b-reduced*.

Claim 2. *Let $g(x_0,\dots,x_n)=x_0^{e_0}\dots x_n^{e_n}$ and $h(x_0,\dots,x_n)=x_0^{d_0}\dots x_n^{d_n}$ be two monomials in Γ with $0\le e_i,d_i<b$ for $i=1,\dots,n$. Then $v_\infty^n(g)=v_\infty^n(h)\iff g=h$.*

Proof Since the pole order of x_i is a^ib^{n-i}, this means that

$$\sum_{i=0}^{n} e_i a^i b^{n-i}=\sum_{j=0}^{n} d_j a^j b^{n-j}.$$

Reducing modulo b,

$$e_n a^n \equiv d_n a^n \mod b.$$

Since $\gcd(a^n,b)=1$ and $0\le e_n,d_n<b$, we have $e_n=d_n$. So

$$\sum_{i=0}^{n-1} e_i a^i b^{n-i}=\sum_{j=0}^{n-1} d_j a^j b^{n-j}.$$

Dividing through by b, we similarly obtain $e_{n-1}=d_{n-1}$, and so on to $e_1=d_1$. Thus, $e_0=d_0$, and so $g=h$. □

Claim 3. *Let $g(x_0,\dots,x_n)\in\Gamma$ be a polynomial. Then there exist constants $\lambda_{\mathbf{e}}\in k$ such that*

$$g(x_0,\dots,x_n)=\sum_{\mathbf{e}\in\mathbb{Z}^{\ge 0}\times(R_b)^n}\lambda_{\mathbf{e}}x_0^{e_0}\dots x_n^{e_n},$$

and

$$v_\infty^n(g)=\min\left\{v_\infty^n(x_0^{e_0}\dots x_n^{e_n}):\lambda_{\mathbf{e}}\neq 0\right\}.$$

Proof Since the pole orders at P_∞^n of any different b-reduced monomials are different, by the strong triangle inequality, the valuation at P_∞^n of a sum of b-reduced monomials is the minimum of the valuations of the monomials (i.e. there is no pole cancellation). □

Therefore, to calculate the possible pole orders of all polynomials in Γ, it is enough to calculate the possible pole orders of monomials in Γ.

3.2. **Valuations of rational functions.** Before we can consider the possible pole orders of rational functions, we need the following proposition.

Proposition 3 (From [1], Chapter 2, Proposition 6)**.** *For $\bar{K}$ algebraically closed, let I be an ideal in $\bar{K}[x_1,\dots,x_n]$. Suppose $V(I)=\{P_1,\dots,P_m\}$ is a finite set of points in $\bar{K}^n$. For $\mathcal{O}_i=\mathcal{O}_{P_i}$, there is a natural isomorphism*

$$\bar{K}[x_1,\dots,x_n]/I\longrightarrow\prod_{i=1}^{m}\mathcal{O}_i/I\mathcal{O}_i.$$

Theorem 4. *Let N be the semi-group of pole orders at P_∞^n in F_n generated by elements of Γ. Suppose, for some $r>0$ and $r\notin N$, that there exists $\psi\in F_n$ with $(\psi)_\infty=rP_\infty^n$. Then, for $\psi=g/h$ with $g,h\in\Gamma$, there is a place in the support of $(h)_0$ corresponding to a singular point Q on C_n.*

Proof Fix some algebraic closure $\bar{K}$ of K. Let

$$I_n=(f(x_0,x_1),\dots,f(x_{n-1},x_n))\subset\bar{K}[x_0,\dots,x_n]$$

be an ideal. Let $\Gamma=\bar{K}[x_0,\dots,x_n]/I_n$ be the polynomial ring of C_n.

Suppose there is an element $\psi\in F_n$ with pole only at Q_n. Then $\psi=g/h$ for polynomials $g,h\in\Gamma$. To prove the contrapositive, assume each zero P of h

corresponds to a non-singular point of C_n. Let the local ring of P be $\mathcal{O}_P \subset F_n$ with valuation v_P. Since g/h does not have a pole at P,

$$v_P(g) \geq v_P(h) > 0.$$

Since P is non-singular, $\mathcal{O}_P$ is a valuation ring, so there is a parameter $t_P \in \mathcal{O}_P$ such that $v_P(t_P) = 1$. Since each element $z \in \mathcal{O}_P$ can be written uniquely as $z = t^l u$ for $u \in \mathcal{O}_P^\times$ and $l = v_P(z)$, and since $v_P(g) \geq v_P(h)$, we have

$$g \in (h) \subset \mathcal{O}_P.$$

Thus, for the ideal $I = (h, I_n)$, we have

$$g = 0 \in \mathcal{O}_P / I\mathcal{O}_P$$

for each zero P of h. Since there are finitely many zeroes of h in C_n, $V(I)$ contains a finite number of points. By the isomorphism from the above proposition,

$$g = 0 \in \bar{K}[x_0, \ldots, x_n]/I = \Gamma/(h).$$

Hence, $g = \phi \cdot h \in \Gamma$ for some $\phi \in \Gamma$, so $\psi = g/h = \phi$, a polynomial. While ϕ may have coefficients in an extension of K, the valuation of ϕ is that of a polynomial, and thus in N. □

Thus, if C_n is non-singular, the set of pole orders of rational functions is the set of pole orders of monomials.

3.2.1. *A non-example.* We give an example of a singular C_{ab} curve with a rational function in the Riemann-Roch space.

Consider the curve $C \subset \overline{\mathbb{F}_q}^2$, for q odd, given by

$$C : y^2 - x^2(x-1) = 0.$$

In the associated function field $F/\mathbb{F}_q$, the functions x and y have poles of orders 2 and 3 at P_∞ and nowhere else. Let $P_{i,j}$ be the place corresponding to the point $(i,j) \in C$. Then the divisors associated to x and y are

$$\begin{aligned} (x) &= 2P_{0,0} - 2P_\infty \\ (y) &= 2P_{0,0} + P_{1,0} - 3P_\infty. \end{aligned}$$

Thus,

$$(y/x) = P_{1,0} - P_\infty,$$

so y/x has a pole that is not the pole of a monomial in x and y. There is one place in the support of $(x)_0$, which corresponds to the singular point $(0,0) \in C$, as is expected by the theorem. Note that $\mathcal{O}_{P_{0,0}}$ is not a valuation ring because there is no parameter. In particular, y is not in the ideal generated by x.

3.3. **Gap numbers of monomials.** We now calculate the number of Weierstrass gap numbers at P_∞^n by looking at the pole orders of monomials. We will assume that the curve C_n is non-singular. (If C_n is singular, we only obtain an upper bound for the genus by counting pole orders of monomials.)

For the function field F_n, the elements

$$1, x_0, x_1, \ldots, x_n$$

have poles at P_∞^n of orders

$$0, b^n, b^{n-1}a, \ldots, a^n,$$

respectively. The monomial $x_0^{e_0}x_1^{e_1}\ldots x_n^{e_n}$ has a pole of order $e_0b^n+e_1b^{n-1}a+\cdots+e_na^n$. Thus, to calculate the genus, we need to calculate the number of positive integers α that do not have a solution in non-negative integers e_i to the equation

$$\alpha = e_0b^n + e_1b^{n-1}a + \cdots + e_na^n. \tag{1}$$

As we saw in Section 3.1, we can restrict to the case where $0 \le e_i < b$.

Proposition 5. *Let $g(F_n)$ denote the genus of the function field F_n. For $n \geq 0$,*

$$g(F_{n+1}) = bg(F_n) + \frac{(a^{n+1}-1)(b-1)}{2}.$$

Proof To prove this, we will use two methods of counting, show that the methods do not overlap, and then show that we have not missed anything.

Method 1: Let $A = \{\alpha_i : i = 1, 2, \ldots, g(F_n)\}$ be the set of gap numbers of P_∞^n in F_n. We want to show that for any $\alpha \in A$, there is no monomial with a pole of order $b\alpha + la^{n+1}$ in F_{n+1} for $l \in R_b = \{0, \ldots, b-1\}$.

Since α is a gap number of P_∞^n in F_n, this means that there is no solution in e_i to equation (1).

Suppose we have a monomial with pole order equal to $b\alpha + la^{n+1}$ in F_{n+1}. The variables in F_{n+1} are $1, x_0, \ldots, x_{n+1}$, so this would mean we could find a solution to

$$e_0b^{n+1} + e_1ab^n + \cdots + e_na^nb + e_{n+1}a^{n+1} = b\alpha + la^{n+1}$$

with non-negative integers e_i. Then $e_{n+1} \equiv l \mod b$. Since e_{n+1} and l are in R_b, $e_{n+1} = l$, so

$$b\alpha = e_0b^{n+1} + e_1ab^n + \cdots + e_na^nb.$$

Dividing through by b, one has

$$\alpha = e_0b^n + e_1ab^{n-1} + \cdots + e_na^n.$$

Since $e_0, e_1, \ldots, e_{n-1}$, and e_n are all non-negative integers, this contradicts the fact that α is a gap number of P_∞^n.

The result is that we have gap numbers $b\alpha + la^{n+1}$ of P_∞^{n+1} in F_{n+1} for $l = 0, \ldots, b-1$ and for all $\alpha \in A$. This gives us the $bg(F_n)$ term in the genus formula.

Method 2: Since the only pole orders below a^{n+1} that are achievable with monomials in F_{n+1} are multiples of b, there is no monomial with pole order that is congruent to any of $1, 2, \ldots, b-1 \mod b$ and less than a^{n+1}. Then, between a^{n+1} and $2a^{n+1}$, the only pole orders that are achievable are congruent to 0 or a^{n+1} mod b. Going on in this manner, for $l = 1, 2, \ldots, b-1$, between la^{n+1} and $(l+1)a^{n+1}$, the only pole orders that are achievable are congruent to $0, a^{n+1}, 2a^{n+1}, \ldots, la^{n+1}$ mod b. (Note that these are all distinct congruence classes because a^{n+1} is a unit mod b.)

Counting in this way gives that the number of gap numbers from 0 to la^{n+1} that are congruent to $la^{n+1} \mod b$ is $\lfloor \frac{la^n}{b} \rfloor$. Let p_{n+1} be the total number of these gap numbers in F_{n+1}. For the $b-1$ non-zero congruent classes modulo b, we get

$$p_{n+1} = \left\lfloor \frac{a^{n+1}}{b} \right\rfloor + \left\lfloor \frac{2a^{n+1}}{b} \right\rfloor + \cdots + \left\lfloor \frac{(b-1)a^{n+1}}{b} \right\rfloor$$

missing pole orders.

For any integer m, let $\overline{m} \in R_b$ be the residue of m modulo b. Since

$$\left\lfloor \frac{m}{b} \right\rfloor = \frac{m}{b} - \frac{\overline{m}}{b},$$

and since $\left\{\overline{a^{n+1}}, \overline{2a^{n+1}}, \ldots, \overline{(b-1)a^{n+1}}\right\} = \{1, 2, \ldots, b-1\}$, we get that

$$\begin{aligned} p_{n+1} &= \left(\frac{a^{n+1} + 2a^{n+1} + \cdots + (b-1)a^{n+1}}{b} - \frac{1 + 2 + \cdots + (b-1)}{b}\right) \\ &= \frac{(a^{n+1}-1)(b-1)}{2}. \end{aligned}$$

Overlap? Suppose there exists an element in F_{n+1} with pole order β that is counted by both methods. By the first method, $\beta = b\alpha + la^{n+1}$ for some $\alpha \in A$ and l such that $0 \leq l \leq b-1$. So $\beta \equiv la^{n+1} \mod b$. If β is counted by the second method, then since $\beta \equiv la^{n+1}$, β must be less than la^{n+1}. But $\beta = b\alpha + la^{n+1}$, so this is a contradiction. So

$$g(F_{n+1}) \geq bg(F_n) + \frac{(a^{n+1}-1)(b-1)}{2}.$$

Everything? Suppose there exists a gap number γ for which there is no monomial in F_{n+1} with pole order equal to γ. Then $\gamma \equiv la^{n+1} \mod b$ for some $l \in \{0, 1, \ldots, b-1\}$. Since $v_\infty^{n+1}(x_{n+1}^l) = -la^{n+1}$, we have $\gamma \neq la^{n+1}$. Thus, either $\gamma > la^{n+1}$ or $\gamma < la^{n+1}$.

If $\gamma > la^{n+1}$, then since $\gamma \equiv la^{n+1} \mod b$,

$$\gamma = mb + la^{n+1}$$

for some positive integer m. It follows that mb is a gap number of P_∞^{n+1}, because if it were the pole order of a function f, then the pole order of $f \cdot x_{n+1}^l$ is γ. Thus, m is a gap number of P_∞^n, and we counted all of these gap numbers in the first method.

Suppose $\gamma < la^{n+1}$. In the second method, we counted all integers that are congruent to la^{n+1} modulo b that are less than la^{n+1}, so γ must have been among them. ☐

We have our result.

Theorem 6. *Let q be a power of a prime. For $f(x,y) \in K[x,y]$, let $f = 0$ be the equation of a C_{ab} curve such that* $\gcd(a,b) = 1$*. For $n \geq 0$, let*

$$C_n = \left\{(p_0, \ldots, p_n) \in K^{n+1} : f(p_{i-1}, p_i) = 0 \textit{ for } i = 1, \ldots, n\right\}.$$

Consider the tower of function fields $\mathcal{F} = (F_0, F_1, \ldots)$ where F_n is the function field associated to C_n. If C_n is non-singular, the genus of F_n is given by

$$g(F_n) = \frac{(b-1)a^{n+1} - (a-1)b^{n+1} + a - b}{2(a-b)},$$

and, for any positive integer m and P_∞ the place at infinity in F_n, a basis for $\mathcal{L}(mP_\infty)$ is given by

$$\left\{x_0^{e_0} x_1^{e_1} \ldots x_n^{e_n} : e_0 \geq 0, 0 \leq e_i < b \textit{ for } i = 1, \ldots, n, \textit{ and } \sum_{i=0}^{n} a^i b^{n-i} e_i \leq m\right\}.$$

Note that the above result is an upper bound. If C_n contains singular points, there will be fewer gap numbers, and so a lower genus.

3.4. **Examples.** Working in $\mathbb{F}_7$, let $f(x,y) = x^3 + y^2 - 3$, and let the curves C_n be defined as in Theorem 6. Note that 3 is neither a quadratic nor cubic residue in $\mathbb{F}_7$.

The Jacobian matrix of C_n is the $n \times (n+1)$ matrix J_n defined by

$$J_n = \begin{pmatrix} 3x_0^2 & 2x_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 3x_1^2 & 2x_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & 3x_2^2 & 2x_3 & \dots & 0 & 0 \\ \vdots & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \dots & 2x_{n-1} & 0 \\ 0 & 0 & 0 & 0 & \dots & 3x_{n-1}^2 & 2x_n \end{pmatrix}.$$

The affine curve C_n is nonsingular if the rank of J_n is n for all points on C_n. The rank drops precisely when we have a point that has two coordinates equal to zero. We aim to show that this can never happen by showing there can be no affine point of the form $(0, a_1, a_2, \dots, a_{n-1}, 0)$ on C_n.

From the equation

$$f(a_0, a_1) = a_0^3 + a_1^2 - 3 = 0,$$

if $a_0 = 0$, we have $a_1^2 = 3$. Since 3 is not a quadratic residue in $\mathbb{F}_7$, a_1 is not in $\mathbb{F}_7$, so $a_1 \in \mathbb{F}_{7^2} \setminus \mathbb{F}_7$. Then, from

$$f(a_1, a_2) = a_1^3 + a_2^2 - 3 = 0,$$

we get $a_2^2 = 3 - a_1^3$. Since $a_1 \in \mathbb{F}_{7^2} \setminus \mathbb{F}_7$, it follows that $3 - a_1^3$ is also in $\mathbb{F}_{7^2} \setminus \mathbb{F}_7$, and so $a_2 \in \mathbb{F}_{7^4} \setminus \mathbb{F}_7$. Similarly, it follows that each of $a_3, a_4, \dots, a_{n-1}$ is in $\mathbb{F}_{7^{2^i}} \setminus \mathbb{F}_7$ for some non-negative integer i.

From the equation

$$f(a_{n-1}, a_n) = a_{n-1}^3 + a_n^2 - 3 = 0,$$

if $a_n = 0$, then $a_{n-1}^3 = 3$. Since 3 is not a cubic residue in modulo 7, it follows that $a_{n-1} \in \mathbb{F}_{7^3}$. However, this contradicts our work above, which said that $a_{n-1} \in \mathbb{F}_{7^{2^i}}$. Hence, there can be no point on this curve with first and last coordinates equal to zero. As a result, there can be no point with two zero coordinates at all, which means that the Jacobian matrix has rank n, which means that the curve C_n is nonsingular. By Theorem 6, the genus of C_n and the corresponding function field F_n is

$$g(C_n) = \frac{3^{n+1} - 2^{n+2} + 1}{2}.$$

Working along these lines, we have the following result.

Theorem 7. *Let q be a prime power. Let $a, b \in \mathbb{N}$ with $\gcd(a,b) = 1$. If there exists $\alpha \in \mathbb{F}_q$ such that α is neither an ath or bth power in $\mathbb{F}_q$, then the function $f(x,y) = x^a + y^b - \alpha$ can be used to recursively define a nonsingular tower of curves.*

For the case where q is prime, we are guaranteed to have examples of this type when a and b both share factors with $q-1$, since the maps $x \mapsto x^a$ and $x \mapsto x^b$ are not one-to-one in this case. Since both maps are at least 2 to 1 and the element 1 is in the image of both maps, there must exist some $\alpha \in \mathbb{F}_q$ that is neither an ath or bth power.

In the case of $a = 2, b = 3$ and $q = 7$, the set of non-zero squares is $\{1, 2, 4\}$ and the non-zero cubes is $\{1, 6\}$. Hence, we can let α equal 3 or 5 and obtain a nonsingular tower.

It would be interesting to see if one can create examples for all combinations of a, b, and q.

4. Comments

For more flexibility, note that it is not required that one uses the same polynomial equation $f = 0$ for each level of the tower. Fixing a and b, if one has a sequence of polynomials $f_1, f_2, \dots$ for which $f_i = 0$ is the equation of a C_{ab} curve, then the genus formula given in Theorem 6 still holds.

In fact, consider a sequence $f_1, f_2, \dots,$ where $f_i = 0$ is the equation of a $C_{a_i b_i}$ curve, for $\gcd(a_i, b_i) = 1$ and $a_i > b_i$. As above, let $F_0 = K(x_0)$ and $F_{n+1} = F_n(x_{n+1})$ where $f_n(x_n, x_{n+1}) = 0$. Then, provided that $(a_i, b_j) = 1$ for all i, j, and that there are no singular points on the corresponding curve (except possibly at infinity), one has the following formula:

$$g(F_{n+1}) = b_{n+1} g(F_n) + \frac{(a_1 \cdots a_{n+1} - 1)(b_{n+1} - 1)}{2}.$$

A basis for $\mathcal{L}(mP_\infty)$ is given by

$$\left\{ x_0^{e_0} \dots x_n^{e_n} : \begin{array}{c} e_0 \geq 0, 0 \leq e_i < b_i \text{ for } i = 1, \dots, n, \\ \text{and } \sum_{i=0}^{n} a_1 \cdots a_i b_{i+1} \cdots b_n e_i \leq m \end{array} \right\}.$$

4.1. **Asymptotics.** We have seen that for the towers defined recursively by C_{ab} equations, the genus grows exponentially in a. The number of places of degree one will grow at most exponentially in b, which is strictly smaller than a. Thus, the ratio of number of places of degree one of F_n divided by the genus of F_n will tend to zero as $n \to \infty$. Therefore, these towers are not *asymptotically good*. (This also follows directly from [2], which states that for a recursively defined tower to be asymptotically good, the recursive equation must have balanced degrees.)

Acknowledgments I would like to thank Emma Previato for encouragement and many useful conversations. This work was supported by NSF grant DMS-0205643.

References

[1] W. Fulton, *Algebraic curves*, Benjamin, New York, 1969.

[2] A. Garcia and H. Stichtenoth, *Skew pyramids of function fields are asymptotically bad*, Coding Theory, Cryptography and Related Areas, J. Buchmann, T. Høholdt, H. Stichtenoth, H. Tapia-Recillas (eds.), Springer Verlag, 2000.

[3] Matsumoto, R., *The C_{ab} curve*, available online at `http://www.rmatsumoto.org/cab.html`, 1998.

[4] R. Matsumoto and S. Miura, *On construction and generalization of algebraic geometry codes*, Proceedings of Algebraic Geometry, Number Theory, Coding Theory and Cryptography, (ed. T. Katsura et al.), University of Tokyo, pp. 3-15, 2000.

[5] R. Pellikaan, *On the existence of order functions*, Journal of Statistical Planning and Inference, vol. 94, pp. 287-301, 2001.

[6] K. Saints and C. Heegard, *Algebraic-Geometric Codes and Multidimensional Cyclic Codes: A Unified Theory and Algorithms for Decoding Using Gröbner Bases*, IEEE Transactions on Information Theory, vol. 41, no. 6, November, 1995.

[7] S. Sakata, J. Justesen, Y. Madelung, H.E. Jensen and T. Høholdt, *A Fast Decoding Method of AG Codes from Miura-Kamiya Curves C_{ab} up to Half the Feng-Rao Bound*, Finite Fields and Their Applications, vol. 1, pp. 83-101, 1995.

[8] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin/Heidelberg/New York, 1993.