Two-point coordinate rings for GK-curves

Iwan M. Duursma

April 27 (revised August 16) 2010

Abstract

Giulietti and Korchmáros presented new curves with the maximal number of points over a field of size q^6. Garcia, Güneri, and Stichtenoth extended the construction to curves that are maximal over fields of size q^{2n}, for odd $n \geq 3$. The generalized GK-curves have affine equations $x^q + x = y^{q+1}$ and $y^{q^2} - y = z^r$, for $r = (q^n + 1)/(q + 1)$. We give a new proof for the maximality of the generalized GK-curves and we outline methods to efficiently obtain their two-point coordinate ring.

Introduction

One of the main open problems for curves over finite fields is the classification of maximal curves, curves that have the maximum number of points in the Hasse-Weil upper bound. Additional motivation for the problem comes from coding theory since curves with many points can be used to construct long codes with good parameters. For many years, all new examples of maximal curves could be derived as subcovers of the ubiquitous Hermitian curve. Giulietti and Korchmáros [7] presented an important new family of maximal curves (GK-curves) that can not be obtained in this way. The Natural Embedding Theorem says that a curve is maximal over a field of size q^2 if and only if it is a curve of degree $q + 1$ on a Hermitian hypersurface [11], [8]. GK-curves have a known embedding as a curve on a Hermitian surface [7].

Building on an example of Serre, Abdón, Bezerra and Quoos [1] formulated a new family of plane maximal curves. Garcia, Güneri and Stichtenoth [2] construct generalized GK-curves as suitable covers of those plane curves. For a generalized GK-curve it is not known if it is covered by the Hermitian curve. Nor is it known how the curve is embedded in a Hermitian hypersurface.

In this paper, we provide an elementary proof that generalized GK-curves are maximal. It is well known that maximality can be shown by giving, for an arbitrary point over the algebraic closure, a carefully chosen hypersurface that intersects the curve only in that point and its conjugates, with prescribed multiplicities. For the Hermitian curve, the choice is straightforward. The curve is a plane curve and for the hypersurface one

can choose the tangent at a point. A similar straightforward choice is available for GK-curves, using their known embedding in a Hermitian surface, but not for generalized GK-curves. Generalized GK-curves are defined by two equations in 3−space and our maximality proof consists of explicitly presenting the surface that intersects the curve with the required multiplicities. A different maximality proof appeared in [2]. It would be interesting to have yet another proof, along the lines of Weil's classical paper on curves over finite fields and exponential sums, by expressing the Frobenius eigenvalues as exponential sums and then connecting the exponential sums to Gauss sums.
The surface that we present in our maximality proof plays a role in the second part of the paper, where we describe the ring of functions on generalized GK-curves that are regular outside two given points. That ring contains a subring $k[h, h^{-1}]$ of finite index, where $h = 0$ is the equation of the surface. We describe a method to obtain a basis for the full ring as a free module over the subring $k[h, h^{-1}]$. A possible application, not considered in this paper, is the construction of good codes on generalized GK-curves. From the given description it is straightforward to efficiently construct such codes.
To illustrate our methods we present the two-point non-gaps for GK-curves defined over a field of size q^6, for $q = 2, 3, 4$. This extends earlier results for one-point non-gaps for the cases $q = 2, 3$ that were obtained in [6].

Maximal curves

The Hermitian curve $y^q + y = x^{q+1}$ over the field k of q^2 elements is special in several ways. It has $N = q^3 + 1$ rational points (q^3 solutions $(x, y) \in k^2$ and one point at infinity) and genus $g = q(q-1)/2$. With these parameters it attains the maximum in the Hasse-Weil bound $N \leq q^2 + 1 + 2gq$. Moreover, as was shown by Ihara [9], its genus is maximal among all curves that meet the Hasse-Weil upper bound (the so-called maximal curves). Ihara's result has the following generalization. A curve over the field of q elements with number of points $N > r^m + 1$, for $r = \sqrt{q}$, $m \geq 2$, has at least one Frobenius eigenvalue $\alpha = re^{i\theta}$ with $\theta \in (\pi/m, 3\pi/m)$ [4]. A curve is maximal if and only if $\alpha = -r$ and $\theta = \pi$ for all Frobenius eigenvalues. And in particular, a maximal curve can not have more than $r^3 + 1$ rational points. The maximum $N = r^3 + 1$ is attained only if the curve is Hermitian [13]. The classification of maximal curves remains a major challenge. An important tool in the classification is the Natural Embedding Theorem [11], [8, Theorem 10.22, Remark 10.24] which says that a curve over k is maximal if and only if it is a curve of degree $q + 1$ on a Hermitian hypersurface. Giulietti and Korchmáros [7] presented a curve that lies on a Hermitian surface and that can not be obtained as a subcover of the Hermitian curve. It is defined by the equations (we use the equivalent equations introduced in [2]) $x^q + x = y^{q+1}$ and $y^{q^2} - y = z^{q^2-q+1}$ and is maximal over the field of size q^6. Garcia, Güneri and Stichtenoth [2] extended this to a larger class by proving that more generally the curve is maximal over q^{2n} for odd n if the exponent for z is replaced with $(q^n + 1)/(q + 1)$. The proof in [2] uses results by Abdón, Bezerra and Quoos [1] for

plane curves $y^{q^2} - y = z^{(q^n+1)/(q+1)}$. The genera are

$$g \;=\; \frac{(q-1)(q^n-q)}{2} \quad \text{and} \quad g \;=\; \frac{(q-1)(q^{n+1}+q^n-q^2)}{2},$$

respectively, for the plane curve and for the generalized GK-curve [2, Proposition 2.2]. To prove maximality it is then verified that the number of points N meets the Hasse-Weil bound. In this paper we give a different proof that shows that for a generalized GK-curve all Frobenius eigenvalues are equal to $-q^n$. Whereas the maximality proof in [2] uses the results in [1], our proof implies those results. Our proof is elementary and consists of two steps. We look for a special function h that intersects the curve with high multiplicity in a given point. The two steps are (1) find suitable equations for h and (2) find the function h as a solution to the equations. The main difficulty is to stay away from computing large resultants and to introduce suitable short cuts in the computations. The structure of the curves is nice enough that this is indeed possible and the computations remain perfectly manageable.

Rings of regular functions

A second goal of the paper is to describe the functions on the generalized GK-curve in a way that makes it feasible to use the curve for the construction of good linear codes. The first results in this direction were obtained by Fanali and Giulietti [6], with a description of the functions regular outside a rational point on the GK-curve, for the cases $q = 2$ and $q = 3$. The functions that we are looking for generalize similar functions for the Hermitian curve. For the Hermitian curve with equation $x^q + x = y^{q+1}$ (note that we follow the notation for the GK-curve and not the common notation $y^q + y = x^{q+1}$ for the Hermitian curve), one-point Hermitian codes use as ring of functions

$$k[x,y] \;=\; \text{the free } k[x] \text{ module with basis } \{1, y, \ldots, y^q\}.$$

The functions in the ring have no poles outside the point of infinity. Two-point codes use a larger ring of functions with the possibility of poles at a second point. For the choice of $(0,0)$ as the second point, the ring extends to

$$k[x, x^{-1}, y] = \text{ the free } k[x, x^{-1}] \text{ module with basis } \{1, y, \ldots, y^q\}.$$

More generally, for a choice (α, β) as second point, and for $(a,b) = (\alpha^q, \beta^q)$ we obtain the ring

$$\begin{aligned} &k[x+a-by, (x+a-by)^{-1}, y-b^q] \\ &\qquad = \text{ the free } k[(x+a-by), (x+a-by)^{-1}] \text{ module} \\ &\qquad\qquad \text{with basis } \{1, y-b^q, \ldots, (y-b^q)^q = y^q - b\}. \end{aligned}$$

The surface $h = 0$ that we will determine in the next two sections generalizes the line $x + a = by$. As outlined above, the function h can be used to prove the maximality

of the generalized GK-curves. For the Hermitian curve, the automorphism group acts transitively on ordered pairs of rational points and we can always assume that the first point is the point at infinity and the second point is the origin $(0,0)$. For the generalized GK-curves, this is not the case. For the GK-curve itself, the rational points divide into two orbits [7]. We claim that the ring of functions regular outside the point at infinity and the origin $(0,0,0)$ is the ring

$$k[x,x^{-1},y,z] \;=\; \text{the free } k[x,x^{-1}] \text{ module with basis } \{y^iz^j : 0 \le i < q+1, 0 \le j < r\}.$$

It is known ([7, Proposition 1], see also [6, Section IV]) that the ring of functions regular outside the point at infinity is generated by the three functions x, y and z. To find the full ring it suffices to invert one function that has poles only at infinity and that vanishes only in $(0,0,0)$. The function x qualifies. In Section 3, we give a description when the second point is not in the orbit of the origin $(0,0,0)$.

1 The surface $x + a = by + Z$ in implicit form

The generalized GK-curve $\mathcal{C}_n$ is defined, for an odd integer n, and for $r = (q^n+1)/(q+1)$, by the pair of equations

$$\begin{cases} x^q + x = y^{q+1} \\ y^{q^2} - y = z^r \end{cases}$$

The curves were formulated in [2] and it was shown there that the curve $\mathcal{C}_n$ has genus

$$g(\mathcal{C}_n) = \frac{(q-1)(q^{n+1}+q^n-q^2)}{2}$$

and that it has the maximum number $N = q^{2n} + 1 + 2gq^n$ of $\mathbb{F}_{q^{2n}}$-rational points. A curve is maximal over $\mathbb{F}_{q^{2n}}$ if and only if, for an arbitrary point P on the curve and for a rational point P_0, the following *fundamental linear equivalence* holds,

$$q^nP + \Phi(P) \sim (q^n+1)P_0.$$

Here Φ denotes the q^{2n}-Frobenius morphism that raises the coordinates of a point to the power q^{2n}. The equivalence implies that the q^{2n}-Frobenius action on the Jacobian of $\mathcal{C}_n$ (more precisely on a ℓ-adic Tate module for the Jacobian) has unique eigenvalue $-q^n$, and therefore that the curve has the maximum number of $q^2 + 1 + 2gq^n$ rational points over $\mathbb{F}_{q^{2n}}$. We will present, for any point $P = (\alpha,\beta,\gamma)$ on $\mathcal{C}_n$, possibly with coordinates in an extension field, a polynomial $h_P \in k[x,y,z]$ with divisor

$$(h_P) = q^n(\alpha,\beta,\gamma) + (\alpha^{q^{2n}},\beta^{q^{2n}},\gamma^{q^{2n}}) - (q^n+1)\infty,$$

where ∞ denotes the common pole of x, y and z. This proves the fundamental linear equivalence and hence the maximality of $\mathcal{C}_n$. The function h uses coefficients $a = \alpha^{q^n}$,

$b = \beta^{q^n}$, and $c = \gamma^{q^n}$. Clearly, (a, b, c) is a point on $\mathcal{C}_n$.

$$\begin{cases} a^q + a = b^{q+1} \\ b^{q^2} - b = c^r \end{cases}$$

Ignoring for the moment the second equation and the variable z, we are left with the Hermitian curve $x^q + x = y^{q+1}$ and a point (a, b) on the Hermitian curve, i.e. $a^q + a = b^{q+1}$.

For $a = \alpha^q$ and $b = \beta^q$, the line $x + a = by$ intersects the curve in (α, β) (q times) and $(\alpha^{q^2}, \beta^{q^2})$ (multiplicity one). This is the classical proof that the Hermitian curve of degree $q + 1$ is maximal over the field of q^2 elements. For the computation of the intersection divisor of the line $x + a = by$, we start with the three equations

$$\begin{cases} x^q + x = y^{q+1} \\ a^q + a = b^{q+1} \\ x + a = by \end{cases}$$

After elimination of x and a we find

$$y^{q+1} + b^{q+1} - (by)^q - by = (y^q - b)(y - b^q) = 0.$$

For $b = \beta^q$, the solutions are $y = \beta$ (q times) and $y = \beta^{q^2}$ (multiplicity one).

We want to extend the argument, which is well known for the Hermitian curve, to the curve $\mathcal{C}_n$. For the curve $\mathcal{C}_n$, we bring in the second equation and consider the system of equations

$$\begin{cases} x^q + x = y^{q+1} \\ a^q + a = b^{q+1} \\ y^{q^2} - y = z^r \\ b^{q^2} - b = c^r \\ x + a = by + Z \end{cases}$$

The purpose is to replace Z with a suitable polynomial such that the surface $x + a = by + Z$ vanishes in (α, β, γ) (q^n times) and $(\alpha^{q^{2n}}, \beta^{q^{2n}}, \gamma^{q^{2n}})$ (multiplicity one), for $a = \alpha^{q^n}, b = \beta^{q^n}$, and $c = \gamma^{q^n}$. To this end we eliminate x and a as well as y and b from the equations, which will lead to an expression

$$F(Z, z, c) = 0,$$

for a polynomial F that is symmetric in z and c. The next step will be to choose $Z = Z(z, c)$ such that

$$F(Z(z, c), z, c) = (z^{q^n} - c)(z - c^{q^n}).$$

For such a choice of Z, the hypersurface $x + a = by + Z$ intersects the curve $\mathcal{C}_n$ in points (x, y, z) with z a root of

$$(z^{q^n} - c)(z - c^{q^n}) = (z^{q^n} - \gamma^{q^n})(z - \gamma^{q^{2n}}) = (z - \gamma)^{q^n}(z - \gamma^{q^{2n}}) = 0.$$

After elimination of x and a we find

$$\begin{cases} (y^q - b)(y - b^q) = Z^q + Z \\ y^{q^2} - y = z^r \\ b^{q^2} - b = c^r \end{cases}$$

We express the left hand sides in terms of the new variables $u = y^q - b$ and $v = y - b^q$. And we replace the last two equations with two new equations.

$$\begin{cases} uv = Z^q + Z \\ (u^q - v)(u - v^q) = (cz)^r \\ (u^{q^2} - u)(v^{q^2} - v) = (z^{qr} - c^r)(z^r - c^{qr}) \end{cases}$$

Elimination of u and v is straightforward. Note that all left sides are symmetric polynomials in u and v. The symmetric polynomial $(X^{q-1} - 1)(Y^{q-1} - 1)$ can be written as a polynomial $F(X + Y, XY)$ in $X + Y$ and XY.

$$\begin{aligned} (X^{q-1} - 1)(Y^{q-1} - 1) &= \prod_{\zeta^{q-1}=1} (X - \zeta)(Y - \zeta) \\ &= \prod_{\zeta^{q-1}=1} (XY - \zeta(X + Y) + \zeta^2) =: F(X + Y, XY). \end{aligned}$$

Thus, for $X = u^{q+1}, Y = v^{q+1}$,

$$\begin{aligned} (z^{qr} - c^r)(z^r - c^{qr}) &= (u^{q^2} - u)(v^{q^2} - v) \\ &= (uv)(X^{q-1} - 1)(Y^{q-1} - 1) \\ &= (uv)F(X + Y, XY) \\ &= (uv)F((cz)^r + uv + (uv)^q, (uv)^{q+1}). \end{aligned}$$

With $(q + 1)r = q^n + 1$, we have

$$\begin{aligned} (z^{qr} - c^r)(z^r - c^{qr}) &= (z^{q^n} - c)(z - c^{q^n}) + cz + (cz)^{q^n} - (cz)^r - (cz)^{rq} \\ &= (z^{q^n} - c)(z - c^{q^n}) + ((cz)^r - cz)((cz)^{qr-1} - 1). \end{aligned}$$

Thus we are looking for Z such that, for $uv = Z^q + Z$,

$$(cz)(uv)F((cz)^r + uv + (uv)^q, (uv)^{q+1}) = ((cz)^r - cz)((cz)^{qr} - cz).$$

For $t = cz$, and for $w = uv = Z^q + Z$,

$$twF(t^r + w + w^q, w^{q+1}) = (t^r - t)(t^{qr} - t),$$

where $F(X + Y, XY) = (X^{q-1} - 1)(Y^{q-1} - 1)$.

Theorem 1.1. *For odd $n \geq 1$, let $\mathcal{C}_n$ be the generalized GK-curve over $\mathbb{F}_{q^{2n}}$, defined by the equations*

$$\begin{cases} x^q + x = y^{q+1} \\ y^{q^2} - y = z^r \end{cases}$$

where $r = (q^n+1)/(q+1)$. Let

$$twF(t^r + w + w^q, w^{q+1}) = (t^r - t)(t^{qr} - t)$$

for $w = Z^q + Z, t = cz$ and for $F(X+Y, XY) = (X^{q-1}-1)(Y^{q-1}-1)$. Then, for any point $(\alpha, \beta, \gamma) \in C_n$, and for $(a, b, c) = (\alpha^{q^n}, \beta^{q^n}, \gamma^{q^n})$, the surface $x + a = by + Z$ intersects the curve C_n in

$$(\alpha, \beta, \gamma) \ (q^n \ \textit{times}) \quad \textit{and} \quad (\alpha^{q^{2n}}, \beta^{q^{2n}}, \gamma^{q^{2n}}) \ (\textit{multiplicity one}).$$

Corollary 1.2. *Let $\mathcal{X}_n$ be the plane curve over $\mathbb{F}_{q^{2n}}$, defined by the equation $y^{q^2} - y = z^r$. Then, for any point $(\beta, \gamma) \in \mathcal{X}_n$, and for $(b, c) = (\beta^{q^n}, \gamma^{q^n})$, the curve $(y^q - b)(y - b^q) - w$ intersects the curve $\mathcal{X}_n$ in*

$$(\beta, \gamma) \ (q^n \ \textit{times}) \quad \textit{and} \quad (\beta^{q^{2n}}, \gamma^{q^{2n}}) \ (\textit{multiplicity one}).$$

Proof. The equation of the curve follows by taking the trace of $x + a - (by + Z)$,

$$\begin{aligned}(x^q + x) + (a^q + a) - (yb)^q - (yb) - (Z^q + Z) = \\ y^{q+1} + b^{q+1} - (by)^q - by - (Z^q + Z) = (y^q - b)(y - b^q) - w.\end{aligned}$$

□

2 The surface $x + a = by + Z$ in explicit form

For a prime power $q = p^m$, we define two formal sums $\hat{f}$ and $\hat{g}$ in the variable t with coefficients in a field of characteristic p.

$$\begin{aligned}\hat{f} &= \sum_{n \geq 1} t^{r_n}, \qquad r_n = (q^{2n-1} + 1)/(q+1), \\ \hat{g} &= \sum_{n \geq 0} t^{s_n}, \qquad s_n = (q^{2n} - 1)/(q+1).\end{aligned}$$

So that

$$\begin{aligned}\hat{f} &= t + t^{q^2-q+1} + t^{q^4-q^3+q^2-q+1} + \cdots, \\ \hat{g} &= 1 + t^{q-1} + t^{q^3-q^2+q-1} + \cdots.\end{aligned}$$

As power series in the variable t, $\hat{f}$ and $\hat{g}$ are uniquely determined by their initial terms, $\hat{f} = t + (\text{higher order terms})$ and $\hat{g} = 1 + (\text{higher order terms})$, and by the relations

$$\hat{f} = t\hat{g}^q, \quad t\hat{g} = t + \hat{f}^q.$$

It follows that

$$t^{q-1}(\hat{f} - t) = \hat{f}^{q^2}, \quad (\hat{g} - 1) = t^{q-1}\hat{g}^{q^2}.$$

We will also use

$$\hat{f}\hat{g} = \hat{f} + (\hat{f}\hat{g})^q = \hat{f} + \hat{f}^q + \hat{f}^{q^2} + \cdots.$$

For a given n, let $r = r_n$ and $s = s_n$, so that $s = qr - 1$ and $r + s = q^{2n-1}$. Let f be the sum of monomials in $\hat{f}$ of degree less than r and let g be the sum of monomials in $\hat{g}$ of degree less than s.

Lemma 2.1. *The equation*

$$twF(t^r + w + w^q, w^{q+1}) = (t^r - t)(t^{qr} - t),$$

where $F(X + Y, XY) = (X^{q-1} - 1)(Y^{q-1} - 1)$, *has a polynomial solution* $w = fg$.

Proof. The polynomials f and g satisfy

$$t^{q-1}(f + t^r - t) = f^{q^2},$$
$$(g + t^s - 1) = t^{q-1}g^{q^2}.$$

And therefore,

$$\begin{aligned} t^r - t &= (X^{q-1} - 1)f \quad \text{for } \ tX = f^{q+1}, \\ t^s - 1 &= (Y^{q-1} - 1)g \quad \text{for } \ Y = tg^{q+1}. \end{aligned}$$

Moreover,

$$f + t^r = tg^q, \qquad tg = t + f^q.$$

Let $w = fg$, so that $XY = w^{q+1}$. Then

$$X = f(g - 1), \quad Y = (f + t^r)g,$$
$$w = fg, \quad w^q = XY/w = (g - 1)(f + t^r),$$

and $X + Y = w + w^q + t^r$. Thus $w = fg$ is a solution. □

For the surface $x + a = by + Z$ in Theorem 1.1 we need Z such that $Z^q + Z = w$. With the lemma we may obtain Z as a solution to $Z^q + Z = fg$. For a given n, $f = t^{r_1} + \cdots + t^{r_{n-1}}$ and $g = t^{s_0} + \cdots + t^{s_{n-1}}$. The product fg is the sum of $(n-1)n$ terms of the form $t^{r_i + s_j}$. It is helpful to picture the sums $r_i + s_j$ in an addition table. For $n = 4$,

	s_0	s_1	s_2	s_3
r_1	1	q		
r_2		q^2	q^3	
r_3			q^4	q^5

Only the entries near the diagonal have been filled in. They follow from the relations $r_i + s_{i-1} = q^{2i-2}$ and $r_i + s_i = q^{2i-1}$, for $i \geq 1$. In general, for $0 \leq j < i < n$,

$$r_{j+1} + s_i = q(r_i + s_j).$$

Thus the entries above the diagonal are q-multiples of the entries below the diagonal. And we can choose $Z = \sum_{0 \leq j < i < n} t^{r_i + s_j}$.

Example 2.2. Let $\mathcal{C}$ be the GK-curve defined by $x^q + x = y^{q+1}, y^{q^2} - y = z^r$, $r = q^2 - q + 1$, over $\mathbb{F}_{q^6}$. Then $w = t^q + t$ and $Z = t$. The equation of the hypersurface is $x + a - by - cz = 0$. The equation appears in [6] and in this special case can be obtained directly as the tangent plane to the Hermitian surface $x^{q^3} + x = y^{q^3+1} + z^{q^3+1}$. It follows from the proof of the Natural Embeding Theorem [11], see also [8, Theorem 10.22, Remark 10.24] that the latter approach to find the equation of the hypersurface applies more generally to all maximal curves with a known embedding in a Hermitian hypersurface.

Example 2.3. Let $\mathcal{C}$ be the maximal curve defined by $x^2 + x = y^3, y^4 - y = z^{11}$ over $\mathbb{F}_{2^{10}}$. Let (α, β, γ) be a rational point with $\gamma \neq 0$ and let $(a, b, c) = (\alpha^{32}, \beta^{32}, \gamma^{32})$. For $q = 2$, $\hat{f} = t + t^3 + t^{11} + t^{43} + \cdots$ and $\hat{g} = 1 + t + t^5 + t^{21} + t^{85} + \cdots$. For the given curve we use $r = 11$, $s = 21$, $r + s = 32$, $f = t + t^3$ and $g = 1 + t + t^5$. The rational function

$$(y^2 - b)(y - b^2) - f(cz)g(cz)$$

for the plane curve $\mathcal{X}$ with $y^4 - y = z^{11}$ has a pole of order $2^5 + 1$ at infinity and a zero of order $2^5 + 1$ at (β, γ). With $fg = (t + t^3 + t^4) + (t + t^3 + t^4)^2$ and $Z = t + t^3 + t^4$, the rational function

$$x + a - by - Z(cz)$$

for the curve $\mathcal{C}$ has a pole of order $2^5 + 1$ at infinity and a zero of order $2^5 + 1$ at (α, β, γ).

Remark 2.4. The equations that we used in the previous section are formulated for pairs of points (x, y, z) and (a, b, c) on the same curve, and the equations express a correspondence between two copies of the same curve. For a curve with function field K/k defined over a finite field of size q, let $F : K \longrightarrow K$ be the purely inseparable map $F(x) = x^q$ and let $\psi : K \longrightarrow K$ be the map $\psi(x) = x^{q^2} - x$. Using two copies of this map, we find a map $\psi \times \psi : K \times K \longrightarrow K \times K$ with a factorization $\psi \times \psi = \phi \circ \phi$, for $\phi : K \times K \longrightarrow K \times K$ such that $\phi(x, y) = (x^q - y, x - y^q)$. In matrix form,

$$\begin{pmatrix} F^2 - 1 & 0 \\ 0 & F^2 - 1 \end{pmatrix} = \begin{pmatrix} F & -1 \\ 1 & -F \end{pmatrix} \begin{pmatrix} F & -1 \\ 1 & -F \end{pmatrix}.$$

If we denote by $p : K \times K \longrightarrow K$ the product $p(x, y) = xy$ then we can write the left sides of our equations as

$$\begin{aligned} p \circ \phi(y, b) &= uv \\ p \circ \phi^2(y, b) &= (u^q - v)(u - v^q) \\ p \circ \phi^3(y, b) &= (u^{q^2} - u)(v^{q^2} - v). \end{aligned}$$

3 Two-point coordinate rings

For the Hermitian curve, with equation $x^q + x = y^{q+1}$, the functions that are regular except possibly at infinity are the polynomials in x and y. Using the equation of the curve, each such polynomial can be represented uniquely as a polynomial of degree at most q in y with coefficients in $k[x]$,

$$k[x, y] \;=\; \text{the free } k[x] \text{ module with basis } \{1, y, \ldots, y^q\}.$$

The larger ring of all functions that are regular except possibly at infinity or at the origin $(0, 0)$ is

$$k[x, x^{-1}, y] \;=\; \text{the free } k[x, x^{-1}] \text{ module with basis } \{1, y, \ldots, y^q\}.$$

The function x has divisor $(q+1)((0,0) - \infty)$. It has a zero of order $q+1$ at the origin, a pole of order $q+1$ at infinity, and no other zeros or poles. The function y has poles only at infinity, of order q, and it has q zeros of order one including a zero at the origin. Note that as f runs through $\{1, y, \ldots, y^q\}$, the pole order of f at infinity and the order of vanishing of f at the origin both run through all the residue classes modulo $q+1$. This assures that the functions $1, y, \ldots, y^q$ are independent over $k[x]$.

For the curve with equation $y^{q^2} - y = z^r$, for $r = (q^n + 1)/(q + 1)$, n odd, the functions that are regular outside infinity are again the polynomials in y and z. The ring of functions that are regular except possibly at infinity or at the origin $(0, 0)$ is

$$k[y, y^{-1}, z] = \text{ the free } k[y, y^{-1}] \text{ module with basis } \{1, z, \ldots, z^{r-1}\}.$$

The main properties are the same as before. For a choice of (β, γ) as second point such that $\gamma = 0$, we replace y with $y - \beta$. The function $y - \beta$ has a pole of order r at infinity and a unique zero at $(\beta, 0)$ of order r. However when we choose as second point on the curve a rational point (β, γ) with $\gamma \neq 0$, then we need the function h of the previous section. For $b = \beta^{q^n}$, $c = \gamma^{q^n}$,

$$(h) = (q^n + 1)((\beta, \gamma) - \infty), \qquad \text{for } \; h = (y^q - b)(y - b^q) - f(cz)g(cz).$$

The ring of functions regular outside infinity and (β, γ) becomes

$$k[h, h^{-1}, y, z] = \text{ the free } k[h, h^{-1}] \text{ module with basis } \{y^i z^j : 0 \leq i < q+1, 0 \leq j < r\}.$$

While this gives a correct description of the ring it is not quite in the right form to recognize the k-subspaces that are needed for the construction of two-point codes. For that purpose we order the monomials $y^i z^j$ by increasing pole order at infinity. And we replace each monomial $y^i z^j$ with a polynomial $f_{i,j}$ that has $y^i z^j$ as leading monomial and whose vanishing order at the second point (β, γ) is maximal.

$$\begin{aligned} k[h, h^{-1}, y, z] = \; & \text{the free } k[h, h^{-1}] \text{ module with} \\ & \text{basis } \{f_{i,j} = y^i z^j + \cdots : 0 \leq i < q+1, 0 \leq j < r\}. \end{aligned}$$

The function h with $(h) = (q^n+1)((\beta,\gamma)-\infty)$ provides useful relations between the Weierstrass semigroups at the points (β,γ) and ∞. We make a small digression to describe these relations for general points P and Q and for a function h with divisor $m(P-Q)$. Applying the relations with $P=\infty$ and $Q=(\beta,\gamma)$ we will then be able to determine properties of the Weierstrass semigroup at Q using known properties of the Weierstrass semigroup at P. We will also be able to motivate the choice of the modified free basis $\{f_{i,j}\}$ for the two-point coordinate ring. Properties of pairs of Weierstrass nongaps are considered in [10], [12]. In those papers a pair of nonnegative integers (a,b) is called a nongap for (P,Q) if there exists a rational function f with pole divisor $aP+bQ$. In [3, Definition 1], this definition is relaxed to arbitrary pairs of integers, and a pair of integers (a,b) is a nongap if there exists a function f with no poles outside P and Q such that $-\operatorname{ord}_P(f)=a, -\operatorname{ord}_Q(f)=b$. At least one of a,b is nonnegative. If $a,b\geq 0$ the nongap is a classical pole divisor. If $a\geq 0$ and $b<0$ then f has a pole of order a at P and vanishes to the order $-b$ at Q, with a similar interpretation when $b\geq 0$ and $a<0$.

For two points P and Q, fix an integer m such that $mP\sim mQ$, and let h be a function with divisor $(h)=m(P-Q)$. Clearly m is a common Weierstrass nongap for P and Q. We call a Weierstrass P-nongap a minimal if it is the smallest nongap in the residue class $a+m\mathbb{Z}$. Similarly for a Weierstrass Q-nongap b. The Weierstrass semigroups for P and Q are determined by their m minimal nongaps. The number of minimal Weierstrass nongaps in the interval $(im-m,im]$ is the same for P and for Q, for any integer i. This is easy to see using that $\dim L(imP)=\dim L(imQ)$, for every integer i. We show that moreover there exists a natural bijection between the minimal nongaps in $(im-m,im]$ for P and those for Q. The bijection is the restriction of a bijection defined on all integers in [3, Definition 13, Proposition 14(i)], [5, Theorem 8.5].

Proposition 3.1. *For a Weierstrass P-nongap $a\in(im-m,im]$, let b be maximal such that there exists a function $f\in L(aP)$ with precise pole order a at P and precise vanishing order b at Q. Then a is minimal if and only if $b\in[0,m)$. In that case, $b'=im-b\in(im-m,im]$ is a minimal Weierstrass Q-nongap with maximal vanishing order $a'=im-a\in[0,m)$ at P.*

Proof. Assume that a is minimal. Clearly, $b\geq 0$. On the other hand $b<m$. For otherwise f/h would be a function with poles only at P of order $a-m$, contradicting minimality of a. The function f/h^i has a pole only at Q of order $b'=im-b\in(im-m,im]$. The relation between a and b is characterized by

$$L(aP-bQ)\neq L((a-1)P-bQ)\quad\text{and}\quad L(aP-(b+1)Q)=L((a-1)P-(b+1)Q,$$

which is equivalent to the combination

$$L(aP-bQ)\neq L(aP-(b+1)Q)\quad\text{and}\quad L((a-1)P-bQ)=L((a-1)P-(b+1)Q.$$

For $a'=im-a$ and $b'=im-b$, the latter becomes

$$L(b'Q-a'P)\neq L((b'-1)Q-a'P)\quad\text{and}\quad L(b'Q-(a'+1)P)=L((b'-1)Q-(a'+1)P).$$

This shows that a' is the maximum vanishing order at P for a function with precise pole order b' at Q. Since $a \in (im-m, im]$, $a' \in [0, m)$. But then $b' \in (im-m, im]$ is minimal. □

We return to the special case $P = \infty$ and $Q = (\beta, \gamma)$, with $m = q^n + 1$. The $q^n + 1$ minimal P-nongaps are $\{ir + jq^2 : 0 \leq i < q+1, 0 \leq j < r\}$. With the proposition the minimal Q-nongaps can be determined from the maximal vanishing orders at Q of functions with poles only at P. In the process of finding the maximal vanishing orders we update the free basis of monomials $\{y^i z^j\}$ to the free basis $\{f_{i,j}\}$. The new basis will be useful when we need to find a basis for a given vector space $L(aP+bQ)$. If $L((a-1)P+bQ)$ is properly contained in $L(aP+bQ)$ then we choose $f \in L(aP+bQ) \backslash L((a-1)P+bQ)$ as follows. Let $a - km$ be a minimal nongap and let g be the function in the free basis $\{f_{i,j}\}$ with precise pole order $a - km$ at P. Then g vanishes with maximal order at Q and we can choose $f = gh^k$.

Replacing the monomial $y^i z^j$ with a polynomial $f_{i,j} = y^i z^j + \cdots$ is essentially a process of Gaussian elimination on a square matrix of size $q^n + 1$ over k. Namely for each monomial $y^i z^j$ we consider its development as a power series in a local parameter t at the point (β, γ) as follows. The functions $y - \beta$ and $z - \gamma$ each vanish to the order one in (β, γ). We set $z = \gamma(t+1)$, so that the new variable t vanishes to the order one in (β, γ). After fixing t as a local parameter we express y as a power series in t. Note that $(y-\beta)^{q^2} - (y-\beta) = z^r - \gamma^r = \gamma^r((1+t)^r - 1)$. If we let $T = (1+t)^r - 1$ and $c = \gamma^r$ then

$$y = \beta - cT - (cT)^{q^2} - (cT)^{q^4} - \cdots .$$

For an arbitrary monomial $y^i z^j$ we find its power series in t by substituting the series for y and for z. We associate to each monomial a vector of length $q^n + 1$ whose coordinates are the coefficients of its power series modulo t^{q^n+1}. The Gaussian elimination comes with the restriction that only previous rows can be used to clear entries in the current row. The computations reduce significantly if we fill in the rows one at a time, and each time a row is needed we fill it not with the development of $y^i z^j$ but with the development of either $f_{i-1,j} y$ or $f_{i,j-1} z$. In that case each new row requires at most $q+1$ operations to be updated to a polynomial $f_{i,j}$. This is very similar to the obtained improvements in the Berlekamp-Massey algorithm.

For the curves $y^4 - y = z^3$ over $\mathbb{F}_{2^6}$, $y^9 - y = z^7$ over $\mathbb{F}_{3^6}$, and $y^{16} - y = z^{13}$ over $\mathbb{F}_{4^6}$, the results are summarized in tables that give the positions of the pivots after the Gaussian elimination is completed. The matrices are of size 9×9, 28×28 and 65×65 respectively. Rows in the matrices correspond to monomials $y^i z^j$ and are ordered by increasing pole order at infinity (i.e. $1 < y < z < y^2 < yz < z^2 < y^3 < \cdots$). For each monomial $y^i z^j$, the table lists the maximal vanishing order at a point (β, γ) with $\gamma \neq 0$, for a polynomial $f_{i,j}$ with leading monomial $y^i z^j$. A vanishing order of m corresponds to a power series with leading term t^m and to a row with a pivot in the $m+1$-st column.

The polynomials that result after the Gaussian elimination is completed are independent, with distinct vanishing orders in the range 0 to q^n.

When we extend the plane curves to the GK-curves

$$\begin{array}{lll} x^2+x=y^3, & y^4-y=z^3 & \text{over } \mathbb{F}_{2^6}, \\ x^3+x=y^4, & y^9-y=z^7 & \text{over } \mathbb{F}_{3^6}, \\ x^4+x=y^5, & y^{16}-y=z^{13} & \text{over } \mathbb{F}_{4^6}, \end{array}$$

and choose as second point (α,β,γ) with $\gamma\neq 0$ then we can use the same functions $f_{i,j}$ with the same vanishing orders (since (α,β,γ) is one of q distinct points lying above (β,γ)). The pole orders in the left table on the other hand are all multiplied by q (since the point at infinity is the unique point above the point at infinity on the plane curve, in a covering of degree q). In other words, the plane curve and the GK-curve share the same free basis for their two-point coordinate rings. The generating functions h for the ring $k[h,h^{-1}]$ are different in each case but are related via $h_{GK}^q+h_{GK}=h$, where we can choose $h_{GK}=Z$ and $h=w$ as in Section 1 and Section 2. For the GK-curve, rational points (α,β,γ) with $\gamma\neq 0$ lie in a single orbit under the action of the automorphism group ([7]) and the tables do not depend on the choice of the second point.

The tables contain all the information about two-point Weierstrass nongaps and in particular about one-point Weierstrass nongaps. Of particular interest are the functions with leading monomial

$(q=2)$	Y	$(6,-1)$	Z	$(8,-2)$	Z^2	$(16,-5)$				
$(q=3)$	Y	$(21,-1)$	Z	$(27,-3)$	Z^3	$(81,-10)$	Z^5	$(135,-19)$		
$(q=4)$	Y	$(52,-1)$	Z	$(64,-4)$	Z^4	$(256,-17)$	Z^7	$(448,-33)$	Z^{10}	$(640,-49)$

For each function, the numbers (a,b) in parentheses give the pole order a at infinity and the vanishing order $-b$ at a point (α,β,γ) above (β,γ), $\gamma\neq 0$. After multiplication with a power of the function h_{GK} we find functions with poles only at the second point that vanish with maximal order at infinity. The numbers (a',b') give the pole order b' at the second point and the corresponding maximal order of vanishing $-a'$ at the point at infinty.

$(q=2)$	Y	$(-3,8)$	Z	$(-1,7)$	Z^2	$(-2,13)$				
$(q=3)$	Y	$(-7,27)$	Z	$(-1,25)$	Z^3	$(-3,74)$	Z^5	$(-5,121)$		
$(q=4)$	Y	$(-13,64)$	Z	$(-1,61)$	Z^4	$(-4,243)$	Z^7	$(-7,422)$	Z^{10}	$(-10,601)$

In this way we recover the numerical semigroups $\langle 7,8,9,13\rangle$ $(q=2)$, $\langle 25,27,28,74,121\rangle$ $(q=3)$, and $\langle 61,64,65,243,422,601\rangle$ $(q=4)$. The cases $q=2,3$ were computed in [6]. We do not list the functions themselves, which are in general returned by the algorithm as rather long polynomials.

The pole orders in the left tables are minimal non-gaps within their residue class modulo q^3+1. With Proposition 3.1 this guarantees that the corresponding vanishing orders in the right table lie in the interval $[0, q^3+1)$. Proposition 3.1 applies to general curves. Both the plane curve $y^{q^2}-y=z^r$ and the generalized GK-curve $\mathcal{C}_n$ have the special property that the canonical divisor is a multiple of the point at infinity. We indicate briefly how this can be used to explain in a different way that the vanishing orders in the right table lie in the interval $[0, q^3)$. The largest entry in the left table is the pole order of the monomial $y^q z^{r-1}$. For general n, this pole order is

$$q \cdot r + (r-1) \cdot q^2 = q(q+1)r - q^2 = q^{n+1} + q - q^2,$$

for the plane curve $y^{q^2}-y=z^r$, and $q^{n+2}+q^2-q^3$ for the generalized GK-curve $\mathcal{C}_n$. In both cases the pole order equals $2g-1+q^n+1$. This pole order is minimal within its residue class modulo q^n+1 and thus, for both the plane curve and the curve $\mathcal{C}_n$, $2g-1$ is a nongap for the point at infinity, and the canonical divisor is a multiple of the point at infinity. To the pole order $2g-1+q^n+1$ corresponds the maximal vanishing order q^n. Using $K=(2g-2)\infty$ it can be shown that if (a,b) is any pair of a pole order a and a corresponding maximal vanishing order b then (a',b') is another such pair for $a+a'=2g-1+q^n+1$ and $b+b'=q^n$. The claim corresponds to Lemma 8.2 in [5]. It follows from the characterization

$$L(aP-bQ) \neq L((a-1)P-bQ) \quad \text{and} \quad L(aP-(b+1)Q) = L((a-1)P-(b+1)Q,$$

for pairs (a,b), using the Riemann-Roch theorem together with the assumption $K=(2g-2)\infty$.

A clear pattern emerges from the cases $q=2,3,4$. In terms of a general q the observed patterns are the following. There exist functions with pole order a at ∞ with maximal vanishing order $-b$ at (α,β,γ), for $\gamma\neq 0$, for

$$\begin{cases} (a,b) = (q^3-q^2+q,-1),(q^3,-q),(q^3+1,-q^3-1), & \text{and for} \\ (a,b) = (q^4+i(q^4-q^3),-q^2-1-iq^2), & i=0,1,\ldots,q-2. \end{cases}$$

The corresponding set of pairs (a',b') such that there exist functions with pole order b' at (α,β,γ), for $\gamma\neq 0$, with maximal order of vanishing $-a'$ at ∞ are

$$\begin{cases} (a',b') = (-q^2+q-1,q^3),(-1,q^3+1-q),(-q^3-1,q^3+1), & \text{and for} \\ (a',b') = (-q-i(q-1),q^4+q+i(q^4+q-q^3-1)-q^2-1-iq^2), & i=0,1,\ldots,q-2, \end{cases}$$

In particular, the Weierstrass semigroup at (α,β,γ), for $\gamma\neq 0$, is

$$\langle q^3-q+1, q^3, q^3+1, q^4-q^2+q-1+i(q^4-q^3-q^2+q-1) : i=0,1,\ldots,q-2\rangle.$$

The patterns hold for other values of q as well (we tested up to $q=9$, using Magma) but a proof of the general case seems to require a further analysis of the functions involved.

	1	Y	Y^2
1	0	3	6
Z	4	7	10
Z^2	8	11	14

	1	Y	Y^2
1	0	1	3
Z	2	4	6
Z^2	5	7	8

	1	Y	Y^2	Y^3
1	0	7	14	21
Z	9	16	23	30
Z^2	18	25	32	39
Z^3	27	34	41	48
Z^4	36	43	50	57
Z^5	45	52	59	66
Z^6	54	61	68	75

	1	Y	Y^2	Y^3
1	0	1	2	5
Z	3	4	7	8
Z^2	6	9	11	14
Z^3	10	12	15	17
Z^4	13	16	18	21
Z^5	19	20	23	24
Z^6	22	25	26	27

0	1	Y	Y^2	Y^3	Y^4
1	0	13	26	39	52
Z	16	29	42	55	68
Z^2	32	45	58	71	84
Z^3	48	61	74	87	100
Z^4	64	77	90	103	116
Z^5	80	93	106	119	132
Z^6	96	109	122	135	148
Z^7	112	125	138	151	164
Z^8	128	141	154	167	180
Z^9	144	157	170	183	196
Z^{10}	160	173	186	199	212
Z^{11}	176	189	202	215	228
Z^{12}	192	205	218	231	244

	1	Y	Y^2	Y^3	Y^4
1	0	1	2	3	7
Z	4	5	6	10	11
Z^2	8	9	13	14	15
Z^3	12	16	18	19	23
Z^4	17	20	22	26	27
Z^5	21	24	28	30	31
Z^6	25	29	32	35	39
Z^7	33	34	36	40	43
Z^8	37	38	42	44	47
Z^9	41	45	46	48	52
Z^{10}	49	50	51	55	56
Z^{11}	53	54	58	59	60
Z^{12}	57	61	62	63	64

Pole orders (left) and vanishing orders (right) for the curves
$y^4 - y = z^3$ (top), $y^9 - y = z^7$ (middle), $y^{16} - y = z^{13}$ (bottom).

4 Conclusion

We provided a new self-contained proof for the maximality of a generalized GK-curve. Furthermore, we provided an efficient way to construct functions with prescribed poles or vanishing orders at two given points P and Q on the curve, for P the point at infinity and for Q a rational point (α, β, γ) with $\gamma \neq 0$. For the original GK-curve, we expect to be able to give generating functions in closed form for the ring of functions with poles only at Q. That would make it possible to settle the structure of the Weierstrass semigroup at Q.

References

[1] Miriam Abdón, Juscelino Bezerra, and Luciane Quoos. Further examples of maximal curves. *J. Pure Appl. Algebra*, 213(6):1192–1196, 2009.

[2] Cem Güneri Arnaldo Garcia and Henning Stichtenoth. A generalization of the Giulietti-Korchmáros maximal curve. *Adv. Geom.*, 10(3):427–434, 2010.

[3] Peter Beelen and Nesrin Tutaş. A generalization of the Weierstrass semigroup. *J. Pure Appl. Algebra*, 207(2):243–260, 2006.

[4] Iwan Duursma and Jean-Yves Enjalbert. Bounds for completely decomposable Jacobians. In *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, pages 86–93. Springer, Berlin, 2002.

[5] Iwan Duursma and Seungkook Park. Coset bounds for algebraic geometric codes. *Extended version*, arXiv:0810.2789, 2008.

[6] Stefania Fanali and Massimo Giulietti. One-point AG codes on the GK maximal curves. *IEEE Trans. Inform. Theory*, 56(1):202–210, 2010.

[7] Massimo Giulietti and Gábor Korchmáros. A new family of maximal curves over a finite field. *Math. Ann.*, 343(1):229–245, 2009.

[8] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[9] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.

[10] Seon Jeong Kim. On the index of the Weierstrass semigroup of a pair of points on a curve. *Arch. Math. (Basel)*, 62(1):73–82, 1994.

[11] Gábor Korchmáros and Fernando Torres. Embedding of a maximal curve in a Hermitian variety. *Compositio Math.*, 128(1):95–113, 2001.

[12] Gretchen L. Matthews. Weierstrass pairs and minimum distance of Goppa codes. *Des. Codes Cryptogr.*, 22(2):107–121, 2001.

[13] Hans-Georg Rück and Henning Stichtenoth. A characterization of Hermitian function fields over finite fields. *J. Reine Angew. Math.*, 457:185–188, 1994.