CODES FROM THE SUZUKI FUNCTION FIELD

GRETCHEN L. MATTHEWS
DEPARTMENT OF MATHEMATICAL SCIENCES
CLEMSON UNIVERSITY
CLEMSON, SC 29634-0975
U.S.A.
E-MAIL: GMATTHE@CLEMSON.EDU

ABSTRACT. We construct algebraic geometry codes from the function field $\mathbb{F}_{2^{2n+1}}(x,y)/\mathbb{F}_{2^{2n+1}}$ defined by $y^{2^{2n+1}} - y = x^{2^n}(x^{2^{2n+1}} - x)$ where n is a positive integer. These codes are supported by two places, and many have parameters that are better than those of any comparable code supported by one place of the same function field. To define such codes, we determine and exploit the structure of the Weierstrass gap set of an arbitrary pair of rational places of $\mathbb{F}_{2^{2n+1}}(x,y)/\mathbb{F}_{2^{2n+1}}$. Moreover, we find some codes over $\mathbb{F}_8$ with parameters that are better than any known code.

1. INTRODUCTION

In [3], the function field $\mathbb{F}_8(x,y)/\mathbb{F}_8$ defined by

$$y^8 - y = x^2(x^8 - x)$$

is used to construct codes supported by a single place that have better parameters than any known code. Such codes are sometimes referred to as one-point codes. In [14], it is shown that there are m-point codes with $m \geq 2$, that is algebraic geometry codes supported by m places where $m \geq 2$, that have better parameters than any comparable one-point code constructed from the same curve. In this correspondence, we combine these ideas to find such two-point codes over $\mathbb{F}_{2^{2n+1}}$ where n is a positive integer. Of those we find, some have better parameters than any comparable one-point code and some have better parameters than any known code.

We consider the function field $F := \mathbb{F}_q(x,y)/\mathbb{F}_q$ defined by

$$y^q - y = x^{q_0}(x^q - x)$$

where $q_0 = 2^n$, $q = 2^{2n+1}$, and n is a positive integer. The projective curve X defined by the above equation was considered in [8] as an example of a curve with an automorphism group that is large with respect to its genus. The curve X (resp. function field F) is sometimes called the Suzuki curve (resp. Suzuki function field) as the automorphism group of X (resp. F) is the Suzuki group of order $q^2(q^2+1)(q-1)$. In [10], Hansen and Stichtenoth considered this curve and applications to algebraic geometry codes. More recently, Kirfel and Pellikaan determined the Feng-Rao bound on the minimum distances of some of these algebraic geometry codes [12]. The case where $n = 1$ has been examined by Chen and Duursma as mentioned above. Here, we use the structure of Weierstrass gap sets to construct

This project was supported by NSF DMS-0201286.

codes and estimate their parameters. This method was first suggested by Goppa ([6], [7]) and later made more explicit in [5], [14], [9], [4], and [13]. We see that these new codes compare quite favorably with those studied in [10], [12], and [3].

This work is organized as follows. Section 2 contains the necessary background information on the Suzuki function field. In Section 3, we determine the Weierstrass gap set of any pair of rational places. In Section 4, this gap set is used to define two-point algebraic geometry codes. These codes are compared with one-point codes constructed from the Suzuki function field. In addition, we find codes over $\mathbb{F}_8$ other than those in [3] with better parameters than any known code.

2. Suzuki function fields

Let $F := \mathbb{F}_q(x,y)/\mathbb{F}_q$ denote the algebraic function field defined by

$$y^q - y = x^{q_0}(x^q - x)$$

where $q_0 = 2^n$ and $q = 2^{2n+1}$ for some positive integer n. Let us review some facts about $F/\mathbb{F}_q$ found in [10]. The notation we use is as in [16]. A place of $F/\mathbb{F}_q$ of degree one will be called a rational place. The set of all rational places of $F/\mathbb{F}_q$ is denoted by $\mathbb{P}_F$, and the divisor (resp. pole divisor) of a function $f \in F$ is denoted by (f) (resp. $(f)_\infty$). The function field $F/\mathbb{F}_q$ has exactly q^2+1 rational places. In fact, for each $a, b \in \mathbb{F}_q$ there exists a unique rational place $P_{ab} \in \mathbb{P}_F$ that is a common zero of $x-a$ and $y-b$. In addition, F has a single place at infinity, P_∞. The genus of F is $g := q_0(q-1)$. Moreover, the explicit formulas of Weil can be used to show that F is an optimal function field.

It will be convenient at times to view F as an extension of the rational function field $\mathbb{F}_q(x)$. Then $[F : \mathbb{F}_q(x)] = q$ (see [10, Lemma 1.8]). Let $Q_a \in \mathbb{P}_{\mathbb{F}_q(x)}$ denote the zero of $x-a$ and $Q_\infty \in \mathbb{P}_{\mathbb{F}_q(x)}$ denote the place at infinity. It will also be useful to consider the functions

$$x, y, v := y^{\frac{q}{q_0}} - x^{\frac{q}{q_0}+1}, w := y^{\frac{q}{q_0}} x^{\frac{q}{q_0^2}-1} + v^{\frac{q}{q_0}} \in F$$

along with their pole divisors as given in [10, Proposition 1.3]:

$$\begin{array}{lcl} (x)_\infty & = & qP_\infty \\ (y)_\infty & = & (q+q_0)P_\infty \\ (v)_\infty & = & (q+\frac{q}{q_0})P_\infty \\ (w)_\infty & = & (q+\frac{q}{q_0}+1)P_\infty. \end{array}$$

Since P_{0b} lies over Q_0 for all $b \in \mathbb{F}_q$ and $F/\mathbb{F}_q(x)$ is an extension of degree q, the place Q_0 splits completely in F. This implies

$$(x) = \sum_{b \in \mathbb{F}_q} P_{0b} - qP_\infty$$

as the pole divisor of x is of degree q. Thus, $v_{P_{00}}(y) = v_{Q_0}(y)$ as $e(P_{00} \mid Q_0) = 1$. Notice that $v_{Q_0}(y) = (q_0+1)v_{Q_0}(x) + \sum_{a \in \mathbb{F}_q^*} v_{Q_0}(x-a) - v_{Q_0}(y^{q-1}-1) = q_0+1$ as $y(y^{q-1}-1) = x^{q_0+1}\prod_{a \in \mathbb{F}_q^*}(x-a)$. Hence, $v_{P_{00}}(y) = q_0+1$. It follows immediately that $v_{P_{00}}(v) = \frac{q}{q_0}+1$ and $v_{P_{00}}(w) = (q+\frac{q}{q_0}+1)$. Moreover, since the degree of the pole divisor of w is $q+\frac{q}{q_0}+1$, we have that

$$(w) = (q+\frac{q}{q_0}+1)P_{00} - (q+\frac{q}{q_0}+1)P_\infty.$$

Now fix $a, b \in \mathbb{F}_q$. According to [10, Proposition 3.2], there is an automorphism $\sigma \in Aut(F/\mathbb{F}_q)$ such that

$$\begin{array}{rccl} \sigma: & x & \mapsto & x-a \\ & y & \mapsto & y-b+a^{q_0}(x-a). \end{array}$$

As a result, we have the following principal divisors:

$$\begin{array}{lcll} (x-a) & = & \sum_{c\in\mathbb{F}_q} P_{ac} & - \quad qP_\infty \\ (y-b) & = & (q_0+1)P_{0b} + \sum_{c\in\mathbb{F}_q^*} P_{cb} & - \quad (q+q_0)P_\infty \\ (u_{ab}) & = & (q_0+1)P_{ab} + A & - \quad (q+q_0)P_\infty \\ (v_{ab}) & = & (\frac{q}{q_0}+1)P_{ab} + A' & - \quad (q+\frac{q}{q_0})P_\infty \\ (w_{ab}) & = & (q+\frac{q}{q_0}+1)P_{ab} & - \quad (q+\frac{q}{q_0}+1)P_\infty, \end{array}$$

where

$$\begin{array}{lcl} u_{ab} & := & y-b+a^{q_0}(x-a) \\ v_{ab} & := & (y-b)^{\frac{q}{q_0}} - (x-a)^{\frac{q}{q_0}+1} \\ w_{ab} & := & (y-b)^{\frac{q}{q_0}}(x-a)^{\frac{q}{q_0^2}-1} + v_{ab}^{\frac{q}{q_0}} \end{array}$$

and A and A' are effective divisors whose supports contain neither P_{ab} nor P_∞. Thus, we conclude that for all $a, b \in \mathbb{F}_q$,

$$\begin{array}{lcl} \left(v_{ab}w_{ab}^{-1}\right)_\infty & = & qP_{ab} \\ \left(u_{ab}w_{ab}^{-1}\right)_\infty & = & (q+q_0)P_{ab} \\ \left((x-a)w_{ab}^{-1}\right)_\infty & = & (q+\frac{q}{q_0})P_{ab} \\ \left(w_{ab}^{-1}\right)_\infty & = & (q+\frac{q}{q_0}+1)P_{ab} \end{array}$$

As we will see in Section 3, these functions will be enough to determine the Weierstrass semigroup of any pair of rational places of the Suzuki function field.

3. The Weierstrass gap set of pairs of places

Let $\mathbb{N}_0$ (resp. $\mathbb{N}$) denote the set of nonnegative integers (resp. positive integers). Let P_1 and P_2 be distinct rational places of F. The Weierstrass semigroup of the place P_1 is

$$H(P_1) = \{\alpha \in \mathbb{N}_0 : \exists f \in \mathbb{F}_q(X) \text{ with } (f)_\infty = \alpha P_1\}$$

and the Weierstrass semigroup of the pair (P_1, P_2) is

$$H(P_1, P_2) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0^2 : \exists f \in \mathbb{F}_q(X) \text{ with } (f)_\infty = \alpha_1 P_1 + \alpha_2 P_2\}.$$

We will write $\langle a_1, \ldots, a_k\rangle := \{\sum_{i=1}^k c_i a_i : c_i \in \mathbb{N}_0\}$ to denote the subsemigroup of nonnegative integers generated by $a_1, \ldots, a_k \in \mathbb{N}$. The Weierstrass gap sets $G(P_1)$ and $G(P_1, P_2)$ are defined by

$$G(P_1) = \mathbb{N}_0 \setminus H(P_1)$$

and

$$G(P_1, P_2) = \mathbb{N}_0^2 \setminus H(P_1, P_2).$$

These two sets differ in that for any rational place P_1, $|G(P_1)| = g$, but $|G(P_1, P_2)|$ depends on the choice of rational places P_1 and P_2 [1]. Using the fact that $|G(P_1)| = g$ and the functions described in the previous section one can prove the following.

Lemma 3.1. *Let P be any rational place of the Suzuki function field $F/\mathbb{F}_q$. Then the Weierstrass semigroup of P is $H(P) = \left\langle q, q+q_0, q+\frac{q}{q_0}, q+\frac{q}{q_0}+1\right\rangle$.*

Next, we consider Weierstrass gap sets of pairs of rational places of F. Let $(P_1, P_2) \in \mathbb{P}_F$ be a pair of distinct rational places of F. According to [11], to determine $H(P_1, P_2)$, we need only find

$$\Gamma(P_1, P_2) := \{(\alpha, \beta_\alpha) : \alpha \in G(P_1)\},$$

where

$$\beta_\alpha := \min\{\beta \in \mathbb{N}_0 : (\alpha, \beta) \in H(P_1, P_2)\}.$$

Given $\mathbf{u} = (u_1, u_2), \mathbf{v} = (v_1, v_2) \in \mathbb{N}_0^2$, define the least upper bound of $\mathbf{u}$ and $\mathbf{v}$ by

$$\text{lub}\{\mathbf{u}, \mathbf{v}\} = (\max\{u_1, v_1\}, \max\{u_2, v_2\}) \in \mathbb{N}_0^2.$$

The following lemma, found in [11] and generalized in [15], describes how the sets $\Gamma(P_1, P_2)$, $H(P_1)$, and $H(P_2)$ generate the entire Weierstrass semigroup $H(P_1, P_2)$.

Lemma 3.2. *Let P_1 and P_2 be distinct rational places of a function field F. The Weierstrass semigroup of the pair $(P_1, P_2) \in \mathbb{P}_F^2$ is*

$$H(P_1, P_2) = \{\text{lub}\{\boldsymbol{\gamma_1}, \boldsymbol{\gamma_2}\} : \boldsymbol{\gamma_1}, \boldsymbol{\gamma_2} \in S\}$$

where $S := \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))$.

Since $Aut(F/\mathbb{F}_q)$ is doubly transitive, there exists an automorphism $\sigma \in Aut(F/\mathbb{F}_q)$ such that $\sigma(P_{00}) = P_1$ and $\sigma(P_\infty) = P_2$. It follows that

$$G(P_1, P_2) = G(P_{00}, P_\infty).$$

Hence, we may assume that $P_1 = P_{00}$ and $P_2 = P_\infty$. To determine $G(P_1, P_2)$, we only need to determine β_α for all $\alpha \in G(P_1)$. It will be convenient to partition the elements of the Weierstrass gap set $G(P_1)$ into blocks

$$B_b := \{\alpha \in G(P_1) : (q + \frac{q}{q_0} + 1)b + 1 \leq \alpha \leq (q + \frac{q}{q_0} + 1)(b+1) - 1\}$$

where $0 \leq b \leq 2q_0 - 2$. For each $0 \leq b \leq 2q_0 - 2$, we organize the elements of the block B_b into rows and columns. If $\alpha \in B_b$, then

$$\alpha = \lfloor \frac{\alpha}{q + \frac{q}{q_0} + 1} \rfloor (q + \frac{q}{q_0} + 1) + mq_0 + s$$

for some $0 \leq s \leq q_0 - 1$. Place α in row

$$r := \begin{cases} m & \text{if } 0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor + 1 \\ m+1 & \text{if } \lfloor \frac{m-1}{2} \rfloor + 2 \leq s \leq q_0 - 1 \end{cases}$$

and in column $j := \alpha - \lfloor \frac{\alpha}{q + \frac{q}{q_0} + 1} \rfloor (q + \frac{q}{q_0} + 1) - (r-1)q_0$. For an illustration of this, see Example 3.4.

Theorem 3.3. *Let P_1 and P_2 be distinct rational places of the Suzuki function field $F/\mathbb{F}_q$. If $\alpha \in G(P_1)$, then*

$$\beta_\alpha = 2g - 1 + q - (q-1)j - \alpha$$

where j denotes the column of α. Therefore, the Weierstrass semigroup of any pair of rational places of F is generated by

$$\{(\alpha, 2g - 1 + q - (q-1)j - \alpha) : \alpha \in G(P_1)\} \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2)).$$

Proof. Without loss of generality, we may assume that $P_1 = P_{00}$ and $P_2 = P_\infty$. Suppose $\alpha \in G(P_{00})$ is in block B_b, row r, and column j. Let

$$f_\alpha = \begin{cases} \dfrac{v^{j-r} y^{\frac{q}{q_0}+1+r-2j}}{w^{\lfloor \frac{\alpha}{q+q_0+1} \rfloor + 1}} & \text{if } r \leq j. \\ \dfrac{x^{r-j} y^{\frac{q}{q_0}+1-r}}{w^{\lfloor \frac{\alpha}{q+q_0+1} \rfloor + 1}} & \text{if } r > j. \end{cases}$$

Notice that

$$\alpha = \lfloor \frac{\alpha}{q + \frac{q}{q_0} + 1} \rfloor (q + \frac{q}{q_0} + 1) + (r-1)q_0 + j.$$

If $r \leq j$, then

$$\left(\frac{v^{j-r} y^{\frac{q}{q_0}+1+r-2j}}{w^{\lfloor \frac{\alpha}{q+q_0+1} \rfloor + 1}} \right)_\infty = \alpha P_{00} + (2g - 1 + q - (q-1)j - \alpha) P_\infty.$$

If $r > j$, then

$$\left(\frac{x^{r-j} y^{\frac{q}{q_0}+1-r}}{w^{\lfloor \frac{\alpha}{q+q_0+1} \rfloor + 1}} \right)_\infty = \alpha P_{00} + (2g - 1 + q - (q-1)j - \alpha) P_\infty.$$

This yields

$$(f_\alpha)_\infty = \alpha P_{00} + (2g - 1 + q - (q-1)j - \alpha) P_\infty.$$

Hence, $(\alpha, 2g - 1 + q - (q-1)j - \alpha) \in H(P_{00}, P_\infty)$ for all $\alpha \in G(P_{00})$. Using the fact that

$$\begin{array}{ccc} G(P_{00}) & \to & G(P_\infty) \\ \alpha & \mapsto & \beta_\alpha \end{array}$$

is a one-to-one correspondence [11, Lemma 2.6], we conclude that $\beta_\alpha = 2g - 1 + q - (q-1)j - \alpha$ as desired. □

Example 3.4. Consider the function field $F := \mathbb{F}_8(x, y)/\mathbb{F}_8$ defined by the equation $y^8 - y = x^2(x^8 - x)$. Note that the genus of F is 14. According to Lemma 3.1, the Weierstrass semigroup of each rational place $P \in \mathbb{P}_F$ is

$$H(P) = \langle 8, 10, 12, 13 \rangle$$

and the elements of the gap set $G(P)$ are as follows:

$$\begin{array}{ccc} 1 & 2 & 3 \\ & 4 & 5 \\ & 6 & 7 \\ & & 9 \\ & & 11 \\ 14 & 15 & \\ & 17 & \\ & 19 & \\ 27. & & \end{array}$$

The divisors of the functions f_α, $\alpha \in G(P_{00})$, given in the proof of Theorem 3.3 are listed here:

$$\begin{array}{llllll}
\left(\frac{y^4}{w}\right)_\infty = & P_{00}+27P_\infty & \left(\frac{vy^2}{w}\right)_\infty = & 2P_{00}+19P_\infty & \left(\frac{v^2}{w}\right)_\infty = & 3P_{00}+11P_\infty \\
 & & \left(\frac{y^3}{w}\right)_\infty = & 4P_{00}+17P_\infty & \left(\frac{vy}{w}\right)_\infty = & 5P_{00}+9P_\infty \\
 & & \left(\frac{xy^2}{w}\right)_\infty = & 6P_{00}+15P_\infty & \left(\frac{y^2}{w}\right)_\infty = & 7P_{00}+7P_\infty \\
 & & & & \left(\frac{xy}{w}\right)_\infty = & 9P_{00}+5P_\infty \\
 & & & & \left(\frac{x^2}{w}\right)_\infty = & 11P_{00}+3P_\infty \\
\left(\frac{y^4}{w^2}\right)_\infty = & 14P_{00}+14P_\infty & \left(\frac{vy^2}{w^2}\right)_\infty = & 15P_{00}+6P_\infty & & \\
 & & \left(\frac{y^3}{w^2}\right)_\infty = & 17P_{00}+4P_\infty & & \\
 & & \left(\frac{xy^2}{w^2}\right)_\infty = & 19P_{00}+2P_\infty & & \\
\left(\frac{y^4}{w^3}\right)_\infty = & 27P_{00}+P_\infty. & & & &
\end{array}$$

This gives

$$\left\{ \begin{array}{l} (1,27),(2,19),(3,11),(4,17),(5,9),(6,15),(7,7), \\ (27,1),(19,2),(11,3),(17,4),(9,5),(15,6),(14,14) \end{array} \right\} \subseteq H(P_{00},P_\infty).$$

Now, since $(27,1) \in H(P_{00},P_\infty)$, $\beta_{27}=1$. This implies $\beta_{19} \geq 2$. Since $(19,2) \in H(P_{00},P_\infty)$, $\beta_{19}=2$. Then $\beta_{11} \geq 3$ implies that $\beta_{11}=3$ as $(11,3) \in H(P_{00},P_\infty)$. Continuing in this manner, we see that

$$\Gamma(P_{00},P_\infty) = \left\{ \begin{array}{l} (1,27),(2,19),(3,11),(4,17),(5,9),(6,15),(7,7), \\ (27,1),(19,2),(11,3),(17,4),(9,5),(15,6),(14,14) \end{array} \right\}.$$

Therefore, the Weierstrass semigroup $H(P_{00},P_\infty)$ is generated by

$$\Gamma(P_{00},P_\infty) \cup (\langle 8,10,12,13\rangle \times \{0\}) \cup (\{0\} \times \langle 8,10,12,13\rangle).$$

In fact, this set is a minimal generating set for the Weierstrass semigroup of any pair of rational places of F.

Since we now know the functions that generate the Weierstrass semigroup of a pair (P_1,P_2) of rational places, we can construct spanning sets for the vector spaces $\mathcal{L}(\alpha P_1+\gamma P_2)$. Recall that if A is a divisor of $F/\mathbb{F}_q$, $\mathcal{L}(A)$ is the $\mathbb{F}_q$-vector space of rational functions $f \in F$ with divisor $(f) \geq -A$ together with the zero function. Let $\ell(A)$ denote the dimension of $\mathcal{L}(A)$.

Let

$$S := \Gamma(P_1,P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))$$

as in Lemma 3.2. Since $S \subseteq H(P_1,P_2)$, $(a,b) \in S$ implies that there exists $f_a \in F$ such that

$$(f_a)_\infty = aP_1 + bP_2.$$

Now suppose $(a,b) \in H(P_1,P_2)$. According to Lemma 3.2,

$$(a,b) = \operatorname{lub}\{(a',b'),(a'',b'')\}$$

for some $(a',b'),(a'',b'') \in S$. Then there are constants $c',c'' \in \mathbb{F}_q$ such that the function $f_{a,b} := c'f_{a'} + c''f_{a''}$ has pole divisor

$$(f_{a,b})_\infty = aP_1 + bP_2. \tag{1}$$

Define a partial order $\preceq$ on $\mathbb{N}_0^2$ by $(n_1, n_2) \preceq (p_1, p_2)$ if and only if $n_1 \leq p_1$ and $n_2 \leq p_2$. Then we obtain the following result.

Proposition 3.5. *Let P_1 and P_2 be distinct rational places of the Suzuki function field $F/\mathbb{F}_q$ and let $\alpha, \gamma \in \mathbb{N}$. The vector space $\mathcal{L}(\alpha P_1 + \gamma P_2)$ is spanned by*

$$\{f_{a,b} : (a,b) \in H(P_1, P_2), (a,b) \preceq (\alpha, \gamma)\}$$

where $f_{a,b}$ is as defined in (1).

In the next section, we will see how this proposition enables one to construct spanning sets for certain algebraic geometry codes.

4. Codes from the Suzuki function field

In this section, we will use information about the Weierstrass gap set obtained in Section 3 to study algebraic geometry codes from the Suzuki function field. Let G be a divisor of $F/\mathbb{F}_q$ and let $D = Q_1 + \cdots + Q_l$ be another divisor of F where $Q_1, \ldots, Q_l$ are distinct rational places, each not belonging to the support of G. The algebraic geometry codes $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ are constructed as follows:

$$\begin{aligned} C_{\mathcal{L}}(D,G) &:= \{(f(Q_1), f(Q_2), \ldots, f(Q_l)) : f \in \mathcal{L}(G)\} \\ C_{\Omega}(D,G) &:= \{(res_{Q_1}(\eta), res_{Q_2}(\eta), \ldots, res_{Q_l}(\eta)) : \eta \in \Omega(G-D)\}, \end{aligned}$$

where $\Omega(G-D)$ denotes the set of rational differentials η of $F/\mathbb{F}_q$ with divisor $(\eta) \geq G - D$ together with the zero differential. If $\deg G < l$, then the code $C_{\mathcal{L}}(D, G)$ has dimension $\ell(G) \geq \deg G + 1 - g$ and minimum distance at least $l - \deg G$. If $2g-2 < \deg G$, then the code $C_{\Omega}(D, G)$ has dimension $\ell(K+D-G) \geq l - \deg G + g - 1$, where K is a canonical divisor of F, and minimum distance at least $\deg G - (2g-2)$. The codes $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ are sometimes referred to as m-point codes where m is the number of rational places in the support of G.

One-point codes defined using the Suzuki function field were first studied in [10]. Bases for one-point codes $C_{\mathcal{L}}(D, \alpha P_\infty)$ are given. By using the automorphism group of $F/\mathbb{F}_q$, or, more explicitly, using the functions $x - a$, u_{ab}, v_{ab}, and w_{ab}, one can obtain a basis for any one-point code $C_{\mathcal{L}}(D, \alpha P_{ab})$ constructed from the Suzuki function field.

We will now describe spanning sets for two-point codes of the form $C_{\mathcal{L}}(D, G)$. Since the automorphism group of $F/\mathbb{F}_q$ is doubly transitive, we may restrict our attention to codes of the form $C_{\mathcal{L}}(D, \alpha P_1 + \gamma P_2)$ where $P_1 = P_{00}$ and $P_2 = P_\infty$. Then it only remains to describe a spanning set for the vector space $\mathcal{L}(\alpha P_1 + \gamma P_2)$. Recall that this was established in Proposition 3.5.

Proposition 4.1. *Let $F/\mathbb{F}_q$ denote the Suzuki function field, P_1 and P_2 be distinct rational places of F, and $\alpha, \gamma \in \mathbb{N}$. Set $D := Q_1 + \cdots + Q_l$ to be the sum of all rational places of F other than P_1 and P_2. Then the algebraic geometry code $C_{\mathcal{L}}(D, \alpha P_1 + \gamma P_2)$ is generated by*

$$\{(f_{a,b}(Q_1), \ldots, f_{a,b}(Q_l)) : (a,b) \in H(P_1, P_2), (a,b) \preceq (\alpha, \gamma)\} \subseteq C_{\mathcal{L}}(D, \alpha P_1 + \gamma P_2)$$

where $f_{a,b}$ is as defined in (1).

Next, we turn our attention to codes of the form $C_{\Omega}(D, \alpha P_1 + \gamma P_2)$. In estimating the parameters of these codes, we will use the following result.

Proposition 4.2. [14, Theorem 2.1] *Let $\alpha_1, \alpha_2 \in \mathbb{N}$. Assume that*

$$(\alpha_1, \alpha), (\gamma_1, \gamma_2 - t - 1) \in G(P_1, P_2)$$

for $0 \leq \alpha \leq \alpha_2$ and $0 \leq t \leq \min\{\gamma_2 - 1, 2g - 1 - \alpha_1 - \alpha_2\}$. Set

$$G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2$$

and $D = Q_1 + \cdots + Q_l$, where each Q_i is a rational place not in the support of G. If the dimension of $C_\Omega(D, G)$ is positive, then $C_\Omega(D, G)$ has minimum distance at least $\deg G - 2g + 3$.

Proposition 4.3. *For each positive integer n, there are two-point codes constructed from the Suzuki function field $F/\mathbb{F}_{2^{2n+1}}$ that have better parameters than any comparable one-point code constructed from F.*

Proof. Set $P_1 = P_{00}$ and $P_2 = P_\infty$. Let m be an integer such that $q - \frac{q-1}{q_0} \leq m < q$. Set $(\alpha_1, \alpha_2) = (1, 2g-2)$ and $(\gamma_1, \gamma_2) = (1, q^2 - mq - 1)$. According to Theorem 3.3, $\beta_1 = 2g - 1$. Hence, $(1, \gamma) \in G(P_1, P_2)$ for all $\gamma \leq 2g - 2$. Let

$$G := P_1 + (q^2 + 2g - mq - 4)P_2$$

and D be the sum of all rational places of F other than P_1 and P_2. Applying Proposition 4.2 we see that $C_\Omega(D, G)$ is a $[q^2 - 1, mq + 1 - g, \geq q(q - m)]$ code. The one-point code $C_\mathcal{L}(D + P_1, mqP_2)$ is a $[q^2, mq + 1 - g, \geq q(q - m)]$ code. To see that the minimum distance of $C_\mathcal{L}(D + P_1, mqP_2)$ is exactly $q(q - m)$, consider

$$f := \prod_{i=1}^{m} (x - \omega^i)$$

where ω is a primitive element of $\mathbb{F}_{2^{2n+1}}$. Clearly, f gives rise to a codeword of weight $q(q - m)$ and so $C_\mathcal{L}(D + P_1, mqP_2)$ is a $[q^2 - 1, mq + 1 - g, q(q - m)]$ code. □

Example 4.4. Consider the function field $F/\mathbb{F}_8$ defined by

$$y^8 - y = x^2(x^8 - x).$$

Take $(\alpha_1, \alpha_2) = (14, 9)$ and $(\beta_1, \beta_2) = (14, 14)$. Then Proposition 4.2 applies with $G = 27P_{00} + 22P_\infty$ and D the sum of the remaining rational places of $F/\mathbb{F}_8$. As a result, $C_\Omega(D, G)$ is a $[63, 27, \geq 24]$ code. According to the Brouwer tables [2], the best known code over $\mathbb{F}_8$ of length 63 and dimension 27 has minimum distance 23.

Now take $(\alpha_1, \alpha_2) = (14, 13)$ and $(\beta_1, \beta_2) = (14, 11)$ in Proposition 4.2. Then $C_\Omega(D, 27P_{00} + 23P_\infty)$ is a $[63, 26, \geq 25]$ code over $\mathbb{F}_8$. According to the Brouwer tables [2], the best known code over $\mathbb{F}_8$ of length 63 and dimension 26 has minimum distance 24.

Remark 4.5. We note that there are a number of two-point codes constructed using the Suzuki function field over $\mathbb{F}_8$ with the same parameters as those of the best known comparable code found in [2]. There are several two-point codes constructed from the Suzuki function field over $\mathbb{F}_8$ that have parameters $[63, 27, \geq 24]$ and $[63, 26, \geq 25]$. In addition, there are a number of two-point codes (in addition to those mentioned in the proof of Proposition 4.3) with minimum distance at least that of the one-point code of the same dimension.

References

[1] E. Arbarello, M. Cornalba, P. Griffiths, and J. Harris, *Geometry of Algebraic Curves*, Springer-Verlag, 1985.

[2] A. E. Brouwer, Linear code bounds, available online at: http://www.win.tue.nl/aeb/voorlincod.html.

[3] Chien-Yu Chen and I. M. Duursma, *Geometric Reed-Solomon codes of length* 64 *and* 65 *over* $\mathbb{F}_8$, IEEE Trans. Inform. Theory **49** no. 5 (2003), 1351–1353.

[4] C. Carvalho and F. Torres, *On Goppa codes and Weierstrass gaps at several points*, preprint.

[5] A. Garcia, S. J. Kim, and R. F. Lax, *Consecutive Weierstrass gaps and minimum distance of Goppa codes*, J. Pure Appl. Algebra **84** (1993), 199–207.

[6] V. D. Goppa, *Algebraico-geometric codes*, Math. USSR-Izv. **21** (1983), 75–91.

[7] V. D. Goppa, *Geometry and Codes*, Kluwer, 1988.

[8] H. W. Henn, *Funktionenkörper mit grosser automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115.

[9] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra **162** (2001), 273–290.

[10] J. P. Hansen and H. Stichtenoth, *Group codes on certain algebraic curves with many rational points*, Appl. Algebra Engrg. Comm. Comput. **1** no. 1 (1990), 67–77.

[11] S. J. Kim, *On the index of the Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **62** (1994), 73–82. .

[12] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41** no. 6 (1995), 1720–1732.

[13] H. Maharaj, G. L. Matthews, and G. Pirsic, *Riemann-Roch spaces for the Hermitian function field with applications to low-discrepency sequences and algebraic geometry codes*, preprint.

[14] G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Des. Codes and Cryptog. **22** (2001), 107–221.

[15] G. L. Matthews, *The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve*, in press.

[16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.