Des. Codes Cryptogr.
DOI 10.1007/s10623-015-0164-5

Suzuki-invariant codes from the Suzuki curve

Abdulla Eid[1] · **Hilaf Hasson**[2] · **Amy Ksir**[3] · **Justin Peachey**[4]

Received: 25 November 2014 / Revised: 11 November 2015 / Accepted: 12 November 2015

Abstract In this paper we consider the Suzuki curve $y^q + y = x^{q_0}(x^q + x)$ over the field with $q = 2^{2m+1}$ elements. The automorphism group of this curve is known to be the Suzuki group $\mathrm{Sz}(q)$ with $q^2(q-1)(q^2+1)$ elements. We construct AG codes over $\mathbb{F}_{q^4}$ from an $\mathrm{Sz}(q)$-invariant divisor D, giving an explicit basis for the Riemann–Roch space $L(\ell D)$ for $0 < \ell \leq q^2 - 1$. The full Suzuki group $\mathrm{Sz}(q)$ acts faithfully on each code. These families of codes have very good parameters and information rate close to 1. In addition, they are explicitly constructed. The dual codes of these families are of the same kind if $2g - 1 \leq \ell \leq q^2 - 1$.

Keywords Algebraic geometric codes · Riemann–Roch spaces · Suzuki curve · Error correcting codes · Dual codes

Mathematics Subject Classification MSC 94B27 · MSC 11G20

Communicated by P. Charpin.

✉ Hilaf Hasson
hilaf@stanford.edu

Abdulla Eid
aeid@uob.edu.bh

Amy Ksir
ksir@usna.edu

Justin Peachey
jdpeachey@gmail.com

[1] Department of Mathematics, University of Bahrain, Sakhir Campus, Bahrain

[2] Department of Mathematics, Stanford University, Palo Alto, CA 94305, USA

[3] Department of Mathematics, United States Naval Academy, Annapolis, MD 21402, USA

[4] Arlington, VA, USA

Published online: 07 December 2015

1 Introduction

Codes with large automorphism groups tend to have very good properties. For example, many have large minimum distance compared to their dimension. Furthermore, the symmetries of the code can potentially be exploited when devising encoding and decoding algorithms. In general, constructing error-correcting codes with large automorphism groups compared to their lengths can be difficult. However, one natural way to do this is by constructing algebraic geometry (AG) codes using an algebraic curve with a large automorphism group, and basing the code not at one-point, but on a divisor which is invariant under the automorphism group of the curve [18]. In algebraic geometry in characteristic 0, the Hurwitz bound gives a maximum size of the automorphism group of a curve of genus $g \geq 2$ as $84(g-1)$ [17]. However, to construct an AG code one works over finite fields, and so can look for particular curves whose automorphism groups exceed the Hurwitz bound.

The Suzuki curve is one such curve. It has a very large automorphism group for its genus, namely the Suzuki group $\mathrm{Sz}(q) = {}^2B_2$ of order $q^2(q-1)(q^2+1)$. It has already been a source of very good error-correcting codes. Codes constructed from the Suzuki curve have been studied, for example, in [4,13] (one-point codes), and [6,7,20] (two-point codes) and shown to have very good parameters. However, the one-point and two-point codes previously studied had automorphism groups which were not the full Suzuki group. In this paper, we construct a family of codes on the Suzuki curve with the full Suzuki group as a subgroup of its group of automorphisms. For some of the codes constructed, we can prove that $\mathrm{Sz}(q)$ is exactly the automorphism group; for others the automorphism group contains $\mathrm{Sz}(q)$ as a subgroup but may be larger. We find that our codes also have very good parameters.

The outline of our paper is as follows: In Sect. 2 we start with some preliminaries about the Suzuki curve. In Sect. 3 we give an explicit basis for the Riemann–Roch space $L(\ell D)$ for $0 < \ell \leq q^2 - 1$, where the divisor D is the sum of all $\mathbb{F}_q$-rational points of the Suzuki curve. In Sect. 4 we construct families of AG-codes with good parameters, and with the full Suzuki group as automorphism group. These families are explicitly constructed in polynomial time with rate close to one. In Sect. 5 we describe explicitly the dual codes of the codes constructed in Sect. 4 and we describe the conditions for the dual code to be of the same kind as the original code. We also state the conditions when the code is isodual (equivalent to its dual) and iso-orthogonal (equivalent to a subcode of its dual code).

2 Preliminaries

Let $m \geq 1$ be an integer, $q_0 := 2^m$, $q := 2^{2m+1} = 2q_0^2$, and let X_m denote the smooth projective curve with affine plane equation

$$y^q + y = x^{q_0}(x^q + x) \tag{1}$$

over $\mathbb{F}_q$. Then, X_m has a singular projective plane model Y_m in $\mathbb{P}^2_{\bar{\mathbb{F}}_2}$ with the homogeneous equation

$$y^q t^{q_0} + y t^{q+q_0-1} = x^{q+q_0} + x^{q_0+1} t^{q-1}$$

in homogeneous coordinates $[t : x : y]$. This curve has been studied, for example, in [5,15] and it has been shown in [11] that the curve has a smooth projective embedding in $\mathbb{P}^4$. Moreover, X_m has a very large automorphism group for its genus, namely the Suzuki group

$\mathrm{Sz}(q)$ of order $q^2(q-1)(q^2+1)$. As such, X_m is known as the Suzuki curve. We summarize these properties as well as several others shown in [9,13] in the following proposition:

Proposition 1 *Let $m \geq 1$ be an integer, $q_0 := 2^m$, $q := 2^{2m+1} = 2q_0^2$, and let X_m denote the Suzuki curve. Then,*

1. *The smooth projective curve X_m has a single point P_∞ above the singularity at infinity $[0:0:1]$ of Y_m.*
2. *The genus of X_m is $g := q_0(q-1)$.*
3. *The number of $\mathbb{F}_q$-rational points is q^2+1, which is maximal as shown by the Serre bound.*
4. *The Suzuki curve X_m is the unique curve (up to $\mathbb{F}_q$-isomorphism) with properties (2) and (3) above.*
5. *The automorphism group of X_m, as well as that of $X_m \times_{\mathbb{F}_q} \bar{\mathbb{F}}_2$, is the Suzuki group $\mathrm{Sz}(q)$ $= {}^2B_2$ of order $q^2(q-1)(q^2+1)$.*
6. *The functions x, y, $z := x^{2q_0+1} - y^{2q_0}$, and $w := xy^{2q_0} - z^{2q_0}$ are regular outside P_∞ with pole orders at P_∞ given by $q, q+q_0, q+2q_0$, and $q+2q_0+1$ respectively.*
7. *The functions t, x, y, z and w give a smooth embedding of X_m into $\mathbb{P}^4$.*

The number $N_j(X_m)$ of $\mathbb{F}_{q^j}$-rational points on the curve can be determined using the zeta function of the curve, or more specifically using the L polynomial, which is the numerator of the zeta function, as follows. By [21, Corollary 5.1.16], if the L-polynomial is $L(X_m,t) = \prod_{k=1}^{2g}(1-\alpha_k t)$, then

$$N_j(X_m) = q^j + 1 - \sum_{k=1}^{2g} \alpha_k^j. \tag{2}$$

For the Suzuki curve, it was shown in [12] that

$$L(X_m,t) = (1 + 2q_0 t + qt^2)^g.$$

The roots of the polynomial $L(X_m,t)$ are $\underbrace{\alpha,\alpha,\ldots,\alpha}_{g \text{ times}}$ and $\underbrace{\beta,\beta,\ldots,\beta}_{g \text{ times}}$, where

$$\alpha := q_0(-1+i)$$

and

$$\beta := \bar{\alpha} = q_0(-1-i).$$

$$N_j(X_m) = q^j + 1 - g(q_0(-1+i))^j - g(q_0(-1-i))^j. \tag{3}$$

In particular, for the smallest fields, we see that

$$N_1(X_m) = q + 1 + q(q-1) = q^2 + 1 \tag{4}$$
$$N_2(X_m) = q^2 + 1 \tag{5}$$
$$N_3(X_m) = q^3 + 1 - q^2(q-1) = q^2 + 1 \tag{6}$$
$$N_4(X_m) = q^4 + 1 + 2q_0 q^2(q-1). \tag{7}$$

Thus there are no rational points over $\mathbb{F}_{q^2}$ or $\mathbb{F}_{q^3}$ that are not $\mathbb{F}_q$ points. However, there are more points over $\mathbb{F}_{q^4}$. In fact, the Suzuki curve is a maximal curve over $\mathbb{F}_{q^4}$, meeting the Hasse-Weil bound. We will use the points of $X(\mathbb{F}_q)$ and $X(\mathbb{F}_{q^4})$ to construct our codes.

3 The Riemann–Roch space $\mathcal{L}(\ell D)$

In order to construct an AG code whose automorphism group is the full automorphism group $\mathrm{Sz}(q)$ of X_m, we need to choose a divisor that is invariant under the action of $\mathrm{Sz}(q)$ on X_m. Suzuki originally constructed $\mathrm{Sz}(q)$ as a doubly transitive group acting on the curve [22]. So the only way to choose an invariant divisor is to take the set of *all* $\mathbb{F}_{q^j}$ points for some j. The smallest such set of points is the set of $\mathbb{F}_q$-points.

Consider the divisor $D \in \mathrm{Div}(X_m)$ given by the sum of all $\mathbb{F}_q$-rational points of X_m. These are the points $P_{\alpha,\beta}$ with affine coordinates (α, β) for any α and β in $\mathbb{F}_q$, plus the point at infinity. Thus

$$D = P_\infty + \sum_{\alpha,\beta\in\mathbb{F}_q} P_{\alpha,\beta}.$$

Since there are $q^2 + 1$ many $\mathbb{F}_q$-rational points of X_m, $\deg(D) = q^2 + 1$. Moreover, the divisor D is fixed by $\mathrm{Sz}(q)$, which will allow us in Sect. 4 to construct codes which have the full Suzuki group $\mathrm{Sz}(q)$ as a subgroup of their permutation automorphism group.

In this section, we prove the following theorem, finding an explicit $\mathbb{F}_q$-basis for the space $\mathcal{L}(\ell D)$, where $\ell \le q^2 - 1$.

Theorem 1 *Let $\ell \in \mathbb{N}$, $\ell \le q^2 - 1$, and D be defined to be the sum of all $\mathbb{F}_q$-rational points of X_m. Then,*

$$S := \left\{ \frac{x^a y^b z^c w^d}{(x^q + x)^r} : \begin{array}{l} aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) \le rq^2 + \ell, \\ 0 \le a \le q - 1, 0 \le b \le 1, 0 \le c \le q_0 - 1, \\ 0 \le d \le q_0 - 1, 0 \le r \le \ell \end{array} \right\} \tag{8}$$

is a basis for $\mathcal{L}(\ell D)$.

Note that the function $x^q + x$ vanishes at every affine point of X_m and has a pole of order q^2 at P_∞. Therefore

$$\mathrm{div}(x^q + x) = -q^2 P_\infty + \sum_{\alpha,\beta\in\mathbb{F}_q} P_{\alpha,\beta}.$$

Hence, $\ell D = \ell(q^2 + 1)P_\infty + \mathrm{div}((x^q + x)^\ell)$, i.e., $\ell D \sim \ell(q^2 + 1)P_\infty$. Thus, we have that $\mathcal{L}(\ell D) \simeq \mathcal{L}(\ell(q^2 + 1)P_\infty)$ where the $\mathbb{F}_q$-isomorphism is given by $f \mapsto (x^q + x)^\ell f$ for $f \in \mathcal{L}(\ell D)$. Thus Theorem 1 is equivalent (via $r' = \ell - r$) to the following.

Theorem 2 *Let $\ell \in \mathbb{N}$, $\ell \le q^2 - 1$. Then*

$$S' := \left\{ x^a y^b z^c w^d (x^q + x)^{r'} : \begin{array}{l} aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) + r'q^2 \le \ell(q^2 + 1) \\ 0 \le a \le q - 1, 0 \le b \le 1, 0 \le c \le q_0 - 1, \\ 0 \le d \le q_0 - 1, 0 \le r' \le \ell \end{array} \right\} \tag{9}$$

is a basis for $\mathcal{L}(\ell(q^2 + 1)P_\infty)$.

In order to prove this theorem, we recall a result in [13]. Let $\mathcal{P} \subseteq \mathbb{Z}_{\ge 0}$ be the semigroup generated by the pole orders of the functions x, y, z, and w defined in Proposition 1. That is,

$$\mathcal{P} := \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1 \rangle \subseteq \mathbb{Z}_{\ge 0}. \tag{10}$$

Proposition 1.6 in [13] is equivalent to the following:

Proposition 2 ([13]) *For every integer j,*

$$\dim_{\mathbb{F}_q}(\mathcal{L}(jP_\infty)) = \#\{n \in \mathcal{P} | n \leq j\}.$$

We are now ready for the proof.

Proof (Theorem 2) Let $f = x^a y^b z^c w^d (x^q + x)^{r'}$ be an element of S', and let v_∞ be the discrete valuation corresponding to the point P_∞. Then

$$v_\infty(f) = -\left[aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) + r'q^2\right],$$

and f has no other poles. Thus the first inequality in the definition of S' shows that $S' \subseteq \mathcal{L}(\ell(q^2 + 1)P_\infty)$. Thus, in light of Proposition 2, it suffices to show that for every $n \in \mathcal{P}$ such that $n \leq \ell(q^2 + 1)$, S' contains exactly one function with a pole of order n at P_∞. First we show that the valuations at P_∞ of the functions in S' are distinct. Suppose that F_1 and F_2 in S' had the same valuation at infinity, where $F_1 = x^{a_1} y^{b_1} z^{c_1} w^{d_1} (x^q + x)^{r_1}$ and $F_2 = x^{a_2} y^{b_2} z^{c_2} w^{d_2} (x^q + x)^{r_2}$. Then

$$\begin{aligned} & a_1 q + b_1(q + q_0) + c_1(q + 2q_0) + d_1(q + 2q_0 + 1) + r_1 q^2 \\ & \quad = a_2 q + b_2(q + q_0) + c_2(q + 2q_0) + d_2(q + 2q_0 + 1) + r_2 q^2. \end{aligned} \tag{11}$$

We consider (11) modulo q_0. Then,

$$d_1 \equiv d_2 \pmod{q_0}.$$

Since $1 \leq d_1, d_2 \leq q_0 - 1$, it must be that $d_1 = d_2$. Next, we consider (11) modulo $2q_0$. Then,

$$b_1 q_0 + d_1 \equiv b_2 q_0 + d_1 \pmod{2q_0}.$$

Note that $0 \leq b_1, b_2 \leq 1$. Thus, is must be that $b_1 = b_2$. Next, consider (11) modulo q. Since $d_1 = d_2$ and $b_1 = b_2$, we get

$$2c_1 q_0 \equiv 2c_2 q_0 \pmod{q}$$

and therefore $c_1 \equiv c_2 \pmod{q_0}$. Since $0 \leq c_1, c_2 \leq q_0 - 1$, it must be the case that $c_1 = c_2$.

Finally, consider (11) modulo q^2. Then, since $b_1 = b_2$, $c_1 = c_2$, $d_1 = d_2$, we have

$$a_1 q \equiv a_2 q \pmod{q^2}.$$

Note that $0 \leq a_1, a_2 \leq q - 1$. Thus, it must be that $a_1 = a_2$. This also shows that $r_1 = r_2$. We conclude that if $v_\infty(F_1) = v_\infty(F_2)$, then $F_1 = F_2$.

Now we must show that if $n \leq \ell(q^2 + 1)$ is an element of $\mathcal{P}$, then there is a function in S' with pole order n at P_∞. Let n be such an element. By definition,

$$n = aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) \tag{12}$$

for some non-negative integers a, b, c, d. We need to show that there are a',b',c',d', and r' such that

$$n = a'q + b'(q + q_0) + c'(q + 2q_0) + d'(q + 2q_0 + 1) + r'q^2 \tag{13}$$

and $0 \leq a' \leq q - 1$, $0 \leq b' \leq 1$, $0 \leq c' \leq q_0 - 1$, $0 \leq d' \leq q_0 - 1$, and $0 \leq r' \leq \ell$.

Let d' be the remainder when n is divided by q_0. Then d' will be in the correct range. Let

$$n_d = \frac{n - d'(q + 2q_0 + 1)}{q_0}.$$

Let b' be the remainder when n_d is divided by 2. Again, b' will be in the correct range. Let

$$n_b = \frac{n_d - b'(2q_0 + 1)}{2}.$$

Let c' be the remainder when n_b is divided by q_0. Now $0 \le c' \le q_0 - 1$. Let

$$n_c = \frac{n_b - c'(q_0 + 1)}{q_0}.$$

Finally, let a' be the remainder when n_c is divided by q, so that $0 \le a' \le q - 1$, and let

$$r' = \frac{n_c - a'}{q}.$$

Then we can put these back together as follows:

$$\begin{aligned} n &= n_d q_0 + d'(q + 2q_0 + 1) \\ &= (2n_b + b'(2q_0 + 1))q_0 + d'(q + 2q_0 + 1) \\ &= 2q_0 n_b + b'(q + q_0) + d'(q + 2q_0 + q) \\ &= 2q_0(q_0 n_c + c'(q_0 + 1)) + b'(q + q_0) + d'(q + 2q_0 + q) \\ &= n_c q + c'(q + 2q_0) + b'(q + q_0) + d'(q + 2q_0 + q) \\ &= r'q^2 + a'q + c'(q + 2q_0) + b'(q + q_0) + d'(q + 2q_0 + q). \end{aligned}$$

What remains is to show that r' is in the correct range. Since $n \le \ell(q^2 + 1)$, this means that

$$\begin{aligned} n_d &\le \ell\left(2qq_0 + \frac{1}{q_0}\right) \\ n_b &\le \ell\left(qq_0 + \frac{1}{2q_0}\right) \\ n_c &\le \ell\left(q + \frac{1}{q}\right) \\ r' &\le \ell + \frac{\ell}{q^2}. \end{aligned}$$

Since r' is an integer and $\ell < q^2$, this means that $r' \le \ell$. Finally, to see that $0 \le r'$ we need first to show that n_d, n_b, n_c are non-negative integers. Since $n \equiv d' \pmod{q_0}$, we have that $d \equiv d' \pmod{q_0}$ and so we can write $d - d' = t_d q_0$. Since $0 \le d$ and $0 \le d' \le q_0 - 1$, t_d must be non-negative. Now we have that

$$\begin{aligned} n_d :&= \frac{n - d'(q + 2q_0 + 1)}{q_0} = \frac{aq + b(q + q_0) + c(q + 2q_0) + (d - d')(q + 2q_0 + 1)}{q_0} \\ &= a(2q_0) + b(2q_0 + 1) + c(2q_0 + 2) + t_d(q + 2q_0 + 1) \end{aligned}$$

which is a non-negative integer.

Next we have that $n_d \equiv b' \pmod 2$, so we have $b + t_d \equiv b' \pmod 2$, with $0 \le b + t_d$ and $0 \le b' \le 1$, so again we can write it as $b + t_d - b' = 2t_b$, for some non-negative integer t_b. Now we have that

$$\begin{aligned} n_b :&= \frac{n_d - b'(2q_0 + 1)}{2} = \frac{a(2q_0) + c(2q_0 + 2) + (b + t_d - b')(2q_0 + 1) + t_d(q)}{2} \\ &= a(q_0) + c(q_0 + 1) + t_b(2q_0 + 1) + t_d q_0^2, \end{aligned}$$

which is again a non-negative integer.

Next, we have that $n_b \equiv c' \pmod{q_0}$, so we have $c + t_b \equiv c' \pmod{q_0}$ and we write $c + t_b - c' = t_c q_0$, for some non-negative integer t_c and we have that

$$\begin{aligned} n_c := \frac{n_b - c'(q_0+1)}{q_0} &= \frac{a(q_0) + (c + t_b - c')(q_0+1) + t_b q_0 + t_d q_0^2}{q_0} \\ &= a + t_c(q_0+1) + t_b + t_d q_0 \end{aligned}$$

which is a non-negative integer. Finally, we have $n_c \equiv a' \pmod{q}$, with $0 \leq n_c$ and $0 \leq a' \leq q-1$, so we have that $n_c - a'$ is a non-negative multiple of q and thus r' is a non-negative integer. □

Remark 1 The dimension of $\mathcal{L}(\ell D)$ is given by

$$\dim_{\mathbb{F}_q} \mathcal{L}(\ell D) = \ell(q^2+1) - q_0(q-1) + 1, \tag{14}$$

which we can see in two ways. First, since $q^2 + 1 > 2q_0(q-1)$, we have $\deg D > 2g$ and the result follows from the Riemann–Roch theorem. Second, in [13, Appendix A], it is shown that $\#(\mathbb{N} \setminus \mathcal{P}) = q_0(q-1)$, and an analysis of their proof shows that the largest number in $\mathbb{N} \setminus \mathcal{P}$ is $2q_0(q-1) - 1$. Since $2q_0(q-1) - 1 \leq \ell(q^2+1)$ for any natural number ℓ, it follows that $\#\{n \in \mathcal{P} | n \leq \ell(q^2+1)\}$ (which is equal to $\#S$, by Proposition 2) is equal $1 + \ell(q^2+1) - \#(\mathbb{N} \setminus \mathcal{P}) = \ell(q^2+1) - q_0(q-1) + 1$.

Theorem 1 gives us an explicit basis for $\mathcal{L}(\ell D)$, which we use to construct Suzuki-invariant codes in the next section.

4 Construction and properties of the code $C(E, \ell D)$

As above, let $D \in \mathrm{Div}(X_m)$ be the sum of all $\mathbb{F}_q$-rational points in X_m. By Theorem 1, for $\ell \leq q^2 - 1$ the Riemann–Roch space $\mathcal{L}(\ell D)$ has the $\mathbb{F}_q$-basis (8), and by Remark 1 $\dim_{\mathbb{F}_q} \mathcal{L}(\ell D) = \ell(q^2+1) - g + 1 = \ell(q^2+1) - q_0(q-1) + 1$.

Now to construct a Suzuki-invariant geometry code, we must choose another set of points, disjoint from D, which is also invariant under $\mathrm{Sz}(q)$. Since we have used all of the $\mathbb{F}_q$ points for D, we must look to points over extensions of $\mathbb{F}_q$. We saw at the end of Sect. 2 that there are no new rational points over $\mathbb{F}_{q^2}$ or $\mathbb{F}_{q^3}$. Therefore we let the divisor $E \in \mathrm{Div}(X_m)$ be the sum of all $\mathbb{F}_{q^4}$-points minus the sum of all $\mathbb{F}_q$-points.

Now we have

$$n := \deg(E) = N_4(X_m) - N_1(X_m),$$

where $N_4(X_m)$ is given by the formula (7), i.e.,

$$N_4(X_m) = q^4 + 1 + 2q_0 q^2(q-1).$$

Therefore, $n = \deg(E) = q^4 + 1 + 2q_0q^2(q-1) - (q^2+1) = q^4 + 2q_0q^2(q-1) - q^2$.

Since $\mathrm{Supp}(E) \cap \mathrm{Supp}(D) = \varnothing$ and Theorem 1 provides an explicit basis for $\mathcal{L}(\ell D)$, we construct an algebraic geometry code using the divisors E, D as follows. Let $P_1, \ldots, P_n$ be all the points in support of E. Define

$$C_{m,\ell} := C_{\mathcal{L}}(E, \ell D) = \Big\{ \big(f(P_1), f(P_2), \ldots, f(P_n)\big) \in \mathbb{F}_{q^4}^n \mid f \in \mathcal{L}(\ell D) \Big\}.$$

By construction, $C_{m,\ell}$ is an $[n,k,d]$-linear code, where

$$\begin{aligned} n &= \deg(E) = q^4 + 2q_0q^2(q-1) - q^2, \\ k &:= \dim_{\mathbb{F}_q} \mathcal{L}(\ell D) = \ell(q^2+1) - q_0(q-1) + 1. \end{aligned}$$

Remark 2 Let $S = \{f_1, \dots, f_k\}$ be the $\mathbb{F}_q$-basis for $\mathcal{L}(\ell D)$ as in Theorem 1. Then, the code $C_{m,\ell}$ has generator matrix $G_{m,\ell} := (f_j(P_i))_{1\le j\le k, 1\le i\le n}$.

Theorem 3 *The algebraic geometry code defined above, $C_{m,\ell} = C_{\mathcal{L}}(E, \ell D)$ over $\mathbb{F}_{q^4}$, where $\ell \le q^2 - 1$, has* Sz(q) *as a subgroup of its automorphism group.*

Proof Because we chose D to be an invariant divisor, Sz(q) acts on both $\mathcal{L}(\ell D)$ and on the code $C_{m,\ell}$. We need to show that it acts faithfully. Because $\deg(\ell D) = \ell(q^2+1) > 2g+1$, the divisor ℓD separates points (see [14, Chap. II.7]). This means that if $A \in$ Sz(q), and $P \in X_m$ so that $A(P) = Q$ and $Q \neq P$, then there is a function f in $\mathcal{L}(\ell D)$ so that $f(P) \neq f(Q)$. Therefore A must act nontrivially on $\mathcal{L}(\ell D)$. Similarly, since $\deg E > \deg \ell D$, the kernel of the evaluation map $\mathcal{L}(\ell D) \to C_{m,\ell}$ is zero and so A must also act nontrivially on $C_{m,\ell}$. Thus the automorphism group of the code contains Sz(q) as a subgroup.

In the case where

$$\ell \le \frac{q^2(q^2+2g-1)}{(q^2+1)(g+1)},$$

it was shown in [18] that in fact the permutation group of $C_{m,\ell}$ will be isomorphic to the Suzuki group Sz(q). For larger ℓ, the code may have even more automorphisms. □

Theorem 4 *The minimum distance d of the code $C_{m,\ell} = C_{\mathcal{L}}(E, \ell D)$ is at least*

$$d \ge d^* := n - \deg(\ell D) = n - \ell(q^2+1).$$

Proof The designed minimum distance (Goppa bound) of the code is d^*. The Feng–Rao bound on the minimum distance is also d^*, and several other more recent bounds [7] on the minimum distance also agree (see Remark 4). A closer analysis of the zeroes of the functions x, y, z, w over $\mathbb{F}_{q^4}$ would be necessary to completely determine d. □

We now focus on the family of codes where $\ell = q^2 - 1$. Denote this family by C_m, i.e., $C_m := C_{m,q^2-1} = C_{\mathcal{L}}(E, (q^2-1)D)$. By Theorem 4, C_m is a $[n, k, d \ge d^*]$-linear code, where

$$\begin{aligned} n &= q^4 + 2q_0q^2(q-1) - q^2, \\ k &= (q^2-1)(q^2+1) - q_0(q-1) + 1 = q^4 - q_0(q-1), \\ d^* &= n - q^4 + 1 = 2q_0q^2(q-1) - q^2 + 1. \end{aligned}$$

Using the above, C_m has information rate

$$R_m := \frac{k_m}{n_m} = \frac{q^4 - q_0q + q_0}{q^4 + 2q_0q^2(q-1) - q^2} = \frac{16q_0^8 - 2q_0^3 + q_0}{16q_0^8 + 16q_0^7 - 4q_0^5 - 4q_0^4}.$$

Thus, as $m \to \infty$, we have $R_m \to 1$. This shows that these codes are significant because they have very good parameter, explicitly constructed in polynomial-time, with rate asymptotically approaches one, and in many cases cannot be achieved by Reed-Solomon codes.

Example 1 The rate gets close to one very quickly. In order to show this, let us consider the following examples:

1. Let $m = 1$; thus, $q = 8, q_0 = 2$. Then, the resulting code $C_1 = C_{1,63}$ is a $[5824, 4082, \geq 1729]$-linear code over $\mathbb{F}_{4096}$ and can correct up to 864 errors with information rate $R_1 = 0.7008$.
2. Let $m = 2$; thus, $q = 2^5 = 32, q_0 = 4$. Then, the resulting code $C_2 = C_{2,1023}$ is a $[1051679, 1048452, \geq 3104]$-linear code over $\mathbb{F}_{1048576}$ and can correct at least 1551 errors with information rate $R_2 = 0.996$.

5 Dual code

As before, let D be the sum of all $\mathbb{F}_q$-points and the divisor E is the sum of all $\mathbb{F}_{q^4}$-rational points minus all the $\mathbb{F}_q$-rational points. Next, we study the dual code of the code $C_{m,\ell} := C_{\mathcal{L}}(E, \ell D)$, where $\ell \leq q^2 - 1$.

Recall from [21, Proposition 2.2.10] that the dual of an algebraic geometry code is given by $C_{\mathcal{L}}(E, \ell D)^{\perp} = C_{\mathcal{L}}(E, E - \ell D + (\eta))$, where η is a Weil differential such that $\nu_{P_i}(\eta) = -1$ and $\text{res}_{P_i}(\eta) = 1$, for all $i = 1, 2, \ldots, n$.

In order to find η we first identify the points of $\mathbb{P}^1_{\mathbb{F}_{q^4}}(\mathbb{F}_{q^4})$ whose fiber in $X_m \times_{\mathbb{F}_q} \mathbb{F}_{q^4}$ via the map induced by x has an $\mathbb{F}_{q^4}$-rational point. Note that the degree q map $X_m \times_{\mathbb{F}_q} \mathbb{F}_{q^4} \to \mathbb{P}^1_{\mathbb{F}_{q^4}}$ is Galois. (Indeed, the extension of function fields is the splitting field of the separable polynomial $Y^q + Y - x^{q_0}(x^q + x)$, with roots $\{y + k | k \in \mathbb{F}_q\}$.) Furthermore, note that $P_\infty \times_{\mathbb{F}_q} \mathbb{F}_{q^4}$ (whose residue field is $\mathbb{F}_{q^4}$) is the only point of ramification of this map. Therefore the number of points in $\mathbb{P}^1_{\mathbb{F}_{q^4}}(\mathbb{F}_{q^4})$ with an $\mathbb{F}_{q^4}$-rational point in the fiber is exactly $\frac{N_4(X_m)-1}{q} = q^3 + 2q_0q(q-1) = q^3 + 2gq$.

Let T be the set of α's in $\mathbb{F}_{q^4}$ such that $x = \alpha$ splits, and let $t := \prod_{\alpha \in T}(x - \alpha)$ be viewed as an element of the function field $\kappa(X_m)$ of X_m, and let $\eta := dt/t$.

Proposition 3 *The differential η defined above satisfies the following three conditions:*

1. $v_P(\eta) = v_P(dt/t) = -1$*, for every $\mathbb{F}_{q^4}$-rational point P of X_m except P_∞.*
2. $\text{res}_P(\eta) = \text{res}_{P,t}(1/t) = 1$ *(following the notation in* [21, Chap. IV]), for every $\mathbb{F}_{q^4}$-rational point P of X_m except P_∞.
3. $(\eta) = (dt/t) = (2g - 2 + q^4 + 2gq^2)P_\infty - (E + D - P_\infty)$.

Proof By the above discussion, every $\mathbb{F}_{q^4}$-rational point P of X_m except for P_∞ lies above some affine point $Q_\alpha := (x - \alpha)$ of $\mathbb{P}^1_{\mathbb{F}_{q^4}}$ where $\alpha \in T$. Therefore:

$$v_P(t) = e(P|Q_\alpha)v_{Q_\alpha}(t) = 1 \cdot v_{Q_\alpha}\left(\prod_{\alpha \in T}(x - \alpha)\right) = 1.$$

And so:

$$v_P(\eta) = v_P(dt/t) = -1$$

and

$$\text{res}_P(\eta) = \text{res}_{P,t}(1/t) = 1.$$

Since we have seen that $v_P(\eta) = -1$ for every $\mathbb{F}_{q^4}$-point of X_m other than P_∞, it follows that

$$(\eta) = v_{P_\infty}(\eta)P_\infty - (E + D - P_\infty).$$

It therefore remains only to compute the valuation of η at P_∞. Note that since $\deg(E + D - P_\infty) = N_4(X_m) - 1 = q^4 + 2gq^2$, it follows that

$$\deg((\eta)) = 2g - 2 = v_{P_\infty}(\eta) - (q^4 + 2gq^2),$$

and therefore

$$v_{P_\infty}(\eta) = 2g - 2 + q^4 + 2gq^2.$$

Thus,

$$(\eta) = (2g - 2 + q^4 + 2gq^2)P_\infty - (E + D - P_\infty).$$

□

By Proposition 3 and [21, Proposition 2.2.10], the dual of $C_{m,\ell} = C_{\mathcal{L}}(E, \ell D)$ is given by $C_{\mathcal{L}}(E, G^\perp)$, where

$$\begin{aligned} G^\perp &= E - \ell D + (\eta) \\ &= E - \ell D + (2g - 2 + q^4 + 2gq^2)P_\infty - (E + D - P_\infty) \\ &= (-1 - \ell)D + (2g - 2 + 1 + q^4 + 2gq^2)P_\infty \\ &= (-1 - \ell)D + (q^2 - 1 + 2g)(q^2 + 1)P_\infty. \end{aligned}$$

Since $D \sim (q^2 + 1)P_\infty$,

$$\begin{aligned} G^\perp &\sim (-1 - \ell)D + (q^2 + 2g - 1)D \\ &\sim (q^2 + 2g - 1 - 1 - \ell)D. \end{aligned}$$

Thus, the dual code of $C_{\mathcal{L}}(E, \ell D)$ is equivalent to the code $C_{\mathcal{L}}(E, (q^2 + 2g - 2 - \ell)D)$. Moreover, the dual code $C_{\mathcal{L}}(E, (q^2+2g-2-\ell)D)$ is also of the form $C_{m,\ell'} = C_{\mathcal{L}}(E, \ell' D)$ if $q^2 + 2g - 2 - \ell \leq q^2 - 1$, i.e., whenever $2g - 1 \leq \ell \leq q^2 - 1$. (In which case $\ell' = q^2 + 2g - 2 - \ell$.)

Thus, we obtain the following result.

Theorem 5 *If $\ell \leq q^2 - 1$, then the dual code of $C_{\mathcal{L}}(E, \ell D)$ is equivalent to the code $C_{\mathcal{L}}(E, (q^2 + 2g - 2 - \ell)D)$. Moreover, if $2g - 1 \leq \ell$, $C^\perp_{m,\ell}$ is of the form $C_{m,\ell'}$ for $\ell' = q^2 + 2g - 2 - \ell$.*

Proposition 4
1. *$C_{\mathcal{L}}(E, \ell D)$ is isodual (i.e., equivalent in the sense of* [21, Definition 2.2.13] *to its dual code) if and only if $\ell = q^2/2 + g - 1$.*
2. *$C_{\mathcal{L}}(E, \ell D)$ is iso-orthogonal (i.e., equivalent to a subcode of its dual code) if and only if $\ell \leq q^2/2 + g - 1$.*

Proof In light of Theorem 5, it is easy to see that $\ell \leq q^2/2 + g - 1$ (resp. $\ell = q^2/2 + g - 1$) is equivalent to $\deg(\ell D) \leq \deg(G^\perp)$ (resp. $\deg(\ell D) = \deg(G^\perp)$), and that if $\deg(\ell D) \leq \deg(G^\perp)$ (resp. $\deg(\ell D) = \deg(G^\perp)$) then $C_{\mathcal{L}}(E, \ell D)$ is iso-orthogonal (resp. isodual).

In order to show that the reverse statements hold, we note that the following inequalities are easy to verify:

$$2g - 2 < \deg(\ell D), \deg(G^\perp) < \deg(E) = N_4(X_m) - N_1(X_m).$$

Assume that the code $C_{\mathcal{L}}(E, \ell D)$ is iso-orthogonal (resp. isodual). Then $C_{\mathcal{L}}(E, \ell D)$ is equivalent to a subcode C of $C_{\mathcal{L}}(E, G^\perp)$ (resp. to $C = C_{\mathcal{L}}(E, G^\perp)$). Invoking [21, Proposition 2.2.14], there exists a divisor H such that $C = C_{\mathcal{L}}(E, H)$ with $H \sim \ell D$. Since both $\deg(\ell D) = \deg(H)$ and $\deg(G^{\perp})$ are less than $\deg(E)$, it follows that $l(\ell D) \leq l(G^{\perp})$ (respectively, $l(\ell D) = l(G^{\perp})$). Using Riemann–Roch and the fact that both $\deg(\ell D) = \deg(H)$ and $\deg(G^{\perp})$ are greater than $2g - 2$, this implies that $\deg(\ell D) \leq \deg(G^{\perp})$ (resp. $\deg(\ell D) = \deg(G^{\perp})$), proving the result. □

Example 2 The smallest case of an isodual code in our family is the case $m = 1$ and $\ell = q^2/2 + g - 1 = 8^2/2 + 14 - 1 = 45$. In that case the code $C_{1,45}$ is isodual.

Remark 3 Note that since the codes $C_{\mathcal{L}}(E, \ell D)$ and $C_{\mathcal{L}}(E, \ell(q^2 + 1)P_\infty)$ are equivalent (since $D \sim (q^2 + 1)P_\infty$), the code $C_{m,\ell}$ is equivalent to a one-point algebraic geometry code.

Remark 4 Since our code and its dual are both equivalent to one-point codes for $2g - 1 \leq \ell \leq q^2 - 1$, we can calculate the Feng–Rao bound [8,16] for both codes hoping for a better estimate for the minimum distance of the codes. According to [3, Proposition 4.2 (iii), (iv)], for the bound to be trivial (i.e., the Feng–Rao bound coincides with the Goppa bound) it suffice to show that

$$\deg(G) \geq 2c - 2, \tag{15}$$

where G is the divisor and c is the conductor of the Weierstrass numerical semigroup of the Suzuki curve at P_∞ (i.e., c is the largest element in the Weierstrass semigroup such that $c - 1$ is not).

First, to find the Feng–Rao bound for the dual code of $C_{\mathcal{L}}(E; \ell(q^2 + 1)P_\infty)$, we have $\deg(G) = \ell(q^2 + 1)$, with $1 \leq \ell \leq q^2 - 1$ and $c = 2g$ (because the Weierstrass semigroup is symmetric; i.e., for every $a \in \mathbb{Z}$, we have that a is in the semigroup if and only if $2g - 1 - a$ is.). Recall that $q = 2q_0^2$ and q_0 is a power of 2. We verify Eq. (15)

$$\begin{aligned}
\deg(G) - (2c - 2) &= \deg(G) - 2c + 1 = \ell(q^2 + 1) - 4g + 2 \\
&= 4\ell q_0^4 + \ell - 4q_0(q - 1) + 2 \\
&= 4\ell q_0^4 + \ell - 8q_0^3 + 4q_0 + 2 \\
&= 4q_0^3(\ell q_0 - 2) + 4q_0 + 2
\end{aligned}$$

Since $\ell \geq 1$ and $q_0 \geq 2$, we must have that $\deg(G) - 2c + 2 > 0$, i.e., $\deg(G) > 2c - 2$ and hence we get that the Feng–Rao bound is the same as the Goppa bound for the dual code of $C_{\mathcal{L}}(E; \ell(q^2 + 1)P_\infty)$.

Second, to find the Feng–Rao bound for the actual code $C_{\mathcal{L}}(E; \ell(q^2 + 1)P_\infty)$, we look at its dual, i.e., the code $C_{\mathcal{L}}(E; \ell'(q^2 + 1)P_\infty)$ ($\ell' := q^2 + 2g - 2 - \ell$), which is again a one-point Suzuki code if $2g - 1 \leq \ell \leq q^2 - 1$. Now we verify Eq. (15)

$$\begin{aligned}
\deg(G) - (2c - 2) &= \ell'(q^2 + 1) - 2c + 2 \\
&= (q^2 + 2g - 2 - \ell)(q^2 + 1) - 4g + 2
\end{aligned}$$

We check only the case $\ell = q^2 - 1$ which gives the least value:

$$\begin{aligned}\deg(G) - (2c-2) &= (q^2 + 2g - 2 - q^2 + 1)(q^2+1) - 4g + 2\\ &= (2g-1)(q^2+1) - 4g + 2\\ &= (2g-1)(q^2+1) - (4g-2)\\ &= (2g-1)(q^2+1) - 2(2g-1)\\ &= (2g-1)(q^2+1-2)\\ &= (2g-1)(q^2-1)\\ &> 0.\end{aligned}$$

This again gives the trivial bound, i.e., the Feng–Rao bound coincides with the Goppa bound. Another interesting floor bound is d_{LM} [19, Theorem 3.3]. Again this bound coincides with the Feng–Rao bound if it is applied to one-point codes [19, Remark 3.5].

Next we look at another special order-type bound for general linear codes [1]. This bound was applied by [10] to the case of one-point codes and the authors came up with a bound d^* that can be computed using a set H^* consisting of all non-negative integers h such that $C_{\mathcal{L}}(E; hP_\infty) \neq C_{\mathcal{L}}(E; (h-1)P_\infty)$. Moreover, the authors showed that d^* coincides with the Feng–Rao bound if the code and its dual are both one-point codes [10, Sect. 4] and thus there will be no improvement in our case for the range $2g - 1 \leq \ell \leq q^2 - 1$.

We investigate the order–bounds in the paper of Duursma–Park–Kirov bounds [7]. A lower bound for the parameter $\gamma(G-K; S, \emptyset)$ (see [7, Definition 5.1]) can be found using [7, Theorem 6.1] which will serve as a lower bound for the order-bounds in that paper. This parameter is trivial (i.e., is equal to $\deg(G-K)$) if $\deg(G-K) \geq 2g$. But for our code, we have shown this in Eq. (15). Therefore, there will be no improvement using Theorem 6.1 and thus we get no improvement with all order–bounds in [7] and [2].

Acknowledgments The authors would like to thank Rachel Pries for organizing the workshop on rational points on Suzuki Curves in which this paper was conceived. We also would like to thank the two anonymous reviewers for the very useful comments and suggestions which helped us improve the quality of our paper. This work was conducted at the Mathematics Department, Colorado State University, Summer 2011, funded by NSF grant DMS-11-01712.

References

1. Andersen H., Geil O.: Evaluation codes from order domain theory. Finite Fields Appl. **14**(1), 92–123 (2008).
2. Beelen P.: The order bound for general algebraic geometric codes. Finite Fields Appl. **13**(3), 665–680 (2007).
3. Campillo A., Farrán J.: Computing Weierstrass semigroups and the Feng–Rao distance from singular plane models. Finite Fields Appl. **6**(1), 71–92 (2000).
4. Chen C., Duursma I.: Geometry Reed–Solomon codes of length 64 and 65 over $\mathbb{F}_8$. IEEE Trans. Inf. Theory **49**(5), 1351–1353 (2003).
5. Deligne P., Lusztig G.: Representations of reductive groups over finite fields. Ann. Math. **103**, 103–161 (1976).
6. Duursma I., Park S.: Delta sets for divisors supported in two points. Finite Fields Appl. **18**(5), 865–885 (2012).
7. Duursma I., Park S., Kirov R.: Distance bounds for algebraic geometric codes. J. Pure Appl. Algebra **215**(8), 1863–1878 (2011).
8. Feng G., Rao T.: Decoding algebraic-geometric codes up to the designed minimum distance. IEEE Trans. Inf. Theory **39**(1), 37–45 (1993).

9. Fuhrmann R., Fernando T.: On Weierstrass points and optimal curves. Rend. Circ. Mat. Palermo **2**(51), 25–46 (1998).
10. Geil O., Munuera C., Ruano D., Torres F.: On the order bounds for one-point AG codes. Adv. Math. Commun. **5**(3), 489–504 (2011).
11. Giulietti M., Korchmáros G., Torres F.: Quotient curves of the Suzuki curve. Acta Arith. **122**(3), 245–274 (2006).
12. Hansen J.P.: Deligne–Lusztig varieties and group codes. In: Coding Theory and Algebraic Geometry (Luminy, 1991). Lecture Notes in Mathematics, vol. 1518, pp. 63–81. Springer, Berlin (1992).
13. Hansen J.P., Stichtenoth H.: Group codes on certain algebraic curves with many rational points. Appl. Algebra Eng. Commun. Comput. **1**(1), 67–77 (1990).
14. Hartshorne R.: Algebraic Geometry. Graduate Texts in Mathematics, vol. 52. Springer, New York (1977).
15. Henn H.: Funktionenkörper mit grosser Automorphismengruppe. J. Reine Angew. Math. **302**, 96–115 (1978).
16. Høholdt T., van Lint J., Pellikaan R.: Algebraic geometry codes. In: Handbook of Coding Theory 1, vol. I, pp. 871–961. Elsevier, Amsterdam (1998).
17. Hurwitz A.: Über algebraische Gebilde mit Eindeutigen Transformationen in sich. Math. Ann. **41**(3), 403–442 (1893).
18. Joyner D., Ksir A.: Automorphism groups of some AG codes. IEEE Trans. Inf. Theory **52**(7), 3325–3329 (2006).
19. Lundell B., McCullough J.: A generalized floor bound for the minimum distance of geometric Goppa codes. J. Pure Appl. Algebra **207**(1), 155–164 (2006).
20. Matthews G.L: Codes from the Suzuki function field. IEEE Trans. Inf. Theory **50**(12), 3298–3302 (2004).
21. Stichtenoth H.: Algebraic function field and codes. Springer, Berlin (2009).
22. Suzuki M.: On a class of doubly transitive groups. Ann. Math. **75**, 105–145 (1962).