Codes with locality from a cyclic extension of the Suzuki curve*

Gretchen L. Matthews[1][0000−0002−8977−8171]

Department of Mathematics, Virginia Tech, Blacksburg, VA 24061 gmatthews@vt.edu
http://www.math.vt.edu/people/gmatthews

Abstract. Recently, Skabelund defined a new maximal curve which is a cyclic extension of the Suzuki curve. In this paper, we consider locally recoverable codes constructed from this new curve. Locally recoverable codes allow for the recovery of single symbol by accessing only a few others which form what is known as a recovery set. If every symbol has at least two disjoint recovery sets, the code is said to have availability. Two constructions are described, as each best fits a particular situation. The first employs the original construction of locally recoverable codes from curves by Tamo and Barg. The second yields codes with availability by appealing to the use of fiber products as described by Haymaker, Malmskog, and Matthews. In both instances, we see that the cyclic extension of the Suzuki code provides codes with smaller locality than those typically found in the literature.

Keywords: locality · Suzuki curve · locally recoverable code.

1 Introduction

Maximal curves have played a role in a number of applications in coding theory. For instance, they allow for the construction of long algebraic geometry codes and yield explicit families of codes with parameters exceeding the Gilbert-Varshamov bound [16]. More recently, they have proven useful in the construction of codes with locality. In some applications, it is desirable to recover a single (or small number of) codeword symbol(s) by accessing only a few, say r, particular symbols of the received word. This leads to the notion of locally recoverable codes, or LRCs. In principle, the locality r should be small so as to limit network traffic though this can adversely impact other code parameters. While an $[n, k, d]$ code C, meaning a code of length n, dimension k, and minimum distance d, can recover any $d-1$ erasures or correct any $\lfloor \frac{d-1}{2} \rfloor$ errors, this assumes access to all other symbols of the entire received word. More precisely, the code C is locally recoverable with locality r if and only if for all $j \in [n] := \{1, \ldots, n\}$ there exists

$$A_j \subseteq [n] \setminus \{j\} \text{ with } |A_j| = r$$

and

$$c_j = \phi_j(c|_{A_j})$$

* Supported by NSF DMS-1403062 and DMS-1855136.

for some function $\phi_j : A_j \to \mathbb{F}$ for all $c \in C$. The set A_j is called a recovery set for coordinate j. Tamo and Barg [15] introduced a construction for codes with locality that is similar to that of algebraic geometry codes. This motivated much work on locally recoverable codes, including [1], [2], [5], [8], [10]. In [7], we employ maximal curves to construct LRCs with availability $t \geq 2$, meaning each coordinate j has t disjoint recovery sets. Implementing codes with availability makes information more available to more users, since recovery of an erasure is not entirely dependent on a single set of coordinates (which may itself contain erasures).

In this paper, we define codes with locality from a new maximal curve constructed by Skabelund [13] using a cyclic cover of the Suzuki curve. The Suzuki curve S_q over $\mathbb{F}_q$ gets its name from its automorphism group which is the Suzuki group $Suz(q)$ of order $q^2(q^2+1)(q-1)$. In [6], Hansen and Stichtenoth considered this curve and applications to algebraic geometry codes leading to other works such as [9], [11]. Recently, Eid, Hammond, Ksir, and Peachey [3] constructed an AG code over $\mathbb{F}_{q^4}$ whose automorphism group is $Suz(q)$. Skabelund considers a cyclic extension of S_q and proves it is maximal over $\mathbb{F}_q$ and $\mathbb{F}_{q^4}$. The construction is similar to that of the Giulietti-Korchmáros, or GK, curve, which has already proven useful in constructing codes with locality. This cyclic extension of the Suzuki curve has been utilized for algebraic geometry codes and for quantum codes [12].

This extended abstract is organized as follows. In Section 2, we obtain codes with locality from the cyclic extension $\tilde{S}_q$ of the Suzuki curve S_q. The locality is much smaller relative to the alphabet size and code length than comparable constructions. In Section 3, we build upon this to construct codes with availability from $\tilde{S}_q$. Our constructions build on tools found in [15] and [7], and some useful background may be found there. As we demonstrate, the cyclic extension of the Suzuki curve introduced by Skabelund offers great flexility in the construction of codes with locality.

2 Locally recoverable codes

The Suzuki curve S_q may be described by the equation

$$S_q : y^q + y = x^{q_0}\left(x^q + x\right)$$

where $q_0 = 2^s$, $q = 2q_0^2$, and $s \in \mathbb{N}$. It is optimal over $\mathbb{F}_q$, having q^2+1 $\mathbb{F}_q$-rational points. Indeed, if $a, b \in \mathbb{F}_q$, $a^q = a$ and $b^q = b$; since char $\mathbb{F}_q = 2$, $b^q + b = 0 = a^{q_0}\left(a^q + a\right)$. In addition, there is a unique point at infinity corresponding to $x = z = 0$ and $y = 1$. The genus of S_q is $q_0\left(q-1\right)$ [6]. It is maximal over $\mathbb{F}_{q^4}$, having $q^4 + 1 + 2q_0q^2(q-1)$ $\mathbb{F}_{q^4}$-rational points [3]. Define

$$\tilde{S}_q : \begin{cases} y^q + y = x^{q_0}\left(x^q + x\right) \\ t^m = x^q + x. \end{cases}$$

where $m = q - 2q_0 + 1$. The curve $\tilde{S}_q$ has a unique point at infinity, and affine points will be denoted $P_{abc} := (a : b : c : 1)$ to mean the unique zero of $x - a$,

$y-b$, and $t-c$, just as those of S_q will be denoted by P_{ab}. The genus of $\tilde{S}_q$ is $\frac{q^3-2q^2+q}{2}$ [13]. According to [12], the number of $\mathbb{F}_{q^4}$-rational points on $\tilde{S}_q$ that are not $\mathbb{F}_q$-rational is

$$q^5-q^4+q^3-q^2;$$

see also [13] for a discussion of the points on this curve. Define

$$\begin{array}{rcl} g: \tilde{S}_q & \to & S_q \\ P_{abc} & \mapsto & P_{ab} \end{array}$$

Let

$$S := S_q\left(\mathbb{F}_{q^4}\right) \setminus S_q\left(\mathbb{F}_q\right). \tag{1}$$

Then $|S| = q^4 + 2q_0q^2(q-1) - q^2$ [3]. Set $D := \sum_{P\in\mathcal{D}} P$ where

$$\mathcal{D} := g^{-1}(S) = \left\{ P_{abc} \in \tilde{S}_q\left(\mathbb{F}_{q^4}\right) : c \neq 0 \right\}. \tag{2}$$

For each $P_{ab} \in S$, $g^{-1}(P_{ab}) = \{P_{abc} : c^m = a^q + a\}$, so

$$|g^{-1}(P_{ab})| = q - 2q_0 + 1. \tag{3}$$

Recall that given a divisor G on a curve X over a field $\mathbb{F}$, the space of functions determined by G is

$$\mathcal{L}(G) := \{f \in \mathbb{F}(X) : (f) \geq -G\} \cup \{0\}$$

where $\mathbb{F}(X)$ denotes the set of rational functions on X, and (f) denotes the divisor of the function f; to say that $(f) = \sum_{Q\in\mathcal{Z}} a_Q Q - \sum_{P\in\mathcal{P}} b_P P$ with $a_Q, b_P \in \mathbb{Z}^+$ means f has a zero of order a_Q at Q and a pole of order b_P at P. Let $\alpha \in \mathbb{Z}^+$, and consider the divisor

$$G := \alpha\left(P_\infty + \sum_{a,b\in\mathbb{F}_q} P_{ab}\right)$$

on S_q. According to [3], a basis for $\mathcal{L}(G)$ is given by

$$\mathcal{B} := \left\{ \frac{x^a y^b u^c v^d}{(x^q+x)^e} : \begin{array}{c} aq + b(q+q_0) + c(q+2q_0) \\ +d(q+2q_0+1) \leq \alpha + eq^2 \\ a \in \{0,\ldots,q-1\}, b \in \{0,1\}, \\ c,d \in \{0,\ldots,q_0-1\}, e \in \{0,\ldots,\alpha\} \end{array} \right\} \subseteq \mathbb{F}_{q^4}(S_q)$$

where $u = x^{2q_0+1} - y^{2q_0}$ and $v = xy^{2q_0} - u^{2q_0}$. Set

$$V := \left\langle ft^i : i = 0,\ldots,m-2; f \in \mathcal{B} \right\rangle.$$

Now define

$$\begin{array}{rcl} ev: V & \to & \mathbb{F}_{q^4}^{(q-2q_0+1)\left(q^4+2q_0q^2(q-1)-q^2\right)} \\ f & \mapsto & \left(f(P_{abc})\right)_{P_{abc}\in\tilde{S}_q\left(\mathbb{F}_{q^4}\right)\setminus\tilde{S}_q\left(\mathbb{F}_q\right)}, \end{array}$$

and set $C(D,G,g) := ev(V)$.

Theorem 1. *Suppose $C(D,G,g)$ is constructed as above where $\deg G < |S|$. Then $C(D,G,g)$ is an $[n,k,d]$ code over $\mathbb{F}_{q^4}$ with locality $q-2q_0$,*

$$n = (q-2q_0+1)\left(q^4+2q_0q^2(q-1)-q^2\right),$$

$$k = (q-2q_0)\left(\alpha\left(q^2+1\right)-q_0(q-1)+1\right),$$

and

$$d \geq n-(q-2q_0+1)(\alpha-q-2q_0-1).$$

Proof. The length and bound on the minimum distance can be verified directly (or using [15]). Indeed, we take the evaluation points for $C(D,G,g)$ to be the points in the support of D. According to (2) and (3), $|suppD| = (q-2q_0+1)\left(q^4+2q_0q^2(q-1)-q^2\right)$. The dimension is given by $|V|$ which follows from [3, Remark 1]. We claim that $R := g^{-1}(P_{ab}) \setminus \{P_{abc}\}$ is a recovery set for the position corresponding to P_{abc}. Suppose $f \in V$. Then $f(x,y,t) = \sum_{i=0}^{m-2}\sum_{j=1}^{M} a_{ij}f_j^*t^i$. Notice that $f(a,b,t) \in \mathbb{F}_q[t]$ and $\deg f(a,b,t) \leq m-2$. Hence, $f(a,b,t)$ can be recovered using the $m-1$ interpolation points: $P_{abc'} \in R$. As a result, $f(P_{abc})$ may be recovered using only elements of R.

Example 1. Let $q=8$ and $q_0=2$, so $q^4=4096$. Notice that $S_8 : y^8+y = x^2\left(x^8+x\right)$ has 64 $\mathbb{F}_8$-rational points and 29120 $\mathbb{F}_{4096}$-rational points. Here, $|S| = 5824$ and $n=29120$. Then $C(D,G,g)$ has locality is 4. We can compare this with an LRC C' from the Hermitian curve $y^{64}+y=x^{65}$ over the same field, $\mathbb{F}_{4096}$. Using a projection onto the x-coordinate gives a code of length 262144 with locality 63 whereas projection onto the y-coordinate yields locality 64. Hence, the construction using $\tilde{S}_8$ has a smaller ratios of locality to code length and to alphabet size.

Alternatively, an LRC may be constructed using the projection

$$\begin{aligned} g : \ \tilde{S}_q &\to C_m \\ P_{abc} &\mapsto Q_{ac} \end{aligned}$$

where Q_{ac} denotes the common zero of $x-a$ and $t-c$. Let S be as in (1), D as in (2), and $G' := \alpha Q_\infty$ where Q_∞ is the point at infinity on C_m. Then a basis for $\mathcal{L}(\alpha Q_\infty)$ is given by $\mathcal{B}' := \left\{t^ix^j : i \geq 0, j \in \{0,\ldots,q-1\}, qi+mj \leq \alpha\right\}$. Use this to define

$$V = \left\langle fy^i : i \in \{0,\ldots,q-2\}, f \in \mathcal{B}'\right\rangle.$$

The code $C(D,G',g)$ has locality $q-1$ and dimension $(q-1)|\mathcal{B}|$. It is worth noting that $\mathcal{L}\left(.\alpha\left(P_\infty+\sum_{a,b\in\mathbb{F}_q}P_{ab}\right)\right) \cong \mathcal{L}\left(\alpha\left(q^2+1\right)P_\infty\right)$.

In the next section, we will see how these two approaches can be combined to give LRCs with availability.

3 Locally recoverable codes with availability

If every coordinate j has t disjoint recovery sets, then C is said to have availability t to reflect that information is more available to more users in the presence of erasure. In [7], fiber products of curves are used to construct locally recoverable codes with availability. We review the construction in the case $t = 2$ below.

Suppose $X = Y_1 \times_Y Y_2$ where Y_1, Y_2, and Y are curves over a finite field $\mathbb{F}$ with rational, separable maps $h_i : Y_i \to Y$. The $\mathbb{F}_q$-rational points of X are $\{(P_1, P_2) : P_i \text{is } \mathbb{F}_q - \text{rational point on } Y_i, h_1(P_1) = h_2(P_2)\}$. Thus, there are projection maps $g_i : X \to Y_i$ defined by $g_i(P_1, P_2) = P_i$; a rational, separable map $g : X \to Y$ given by $g = h_1 \circ g_1 = h_2 \circ g_2$; maps of function fields $h_i^* : \mathbb{F}(Y) \to \mathbb{F}(Y_1)$ given by $h_i^*(f) := f \circ h_i$; and primitive elements x_i of the extensions $\mathbb{F}(Y_i)/h_i^*(\mathbb{F}(Y))$. Let S be a set of rational points on Y, and take $D := \sum_{P \in g^{-1}(S)} P$. Choose an effective divisor G on Y of degree $\ell < |S|$, and take a basis $\{f_1, \ldots, f_t\}$ for $\mathcal{L}(G)$. Set

$$V := Span\left\{(f_i \circ g)\, x_1^{*e_1} x_2^{*e_2} : 1 \le i \le t, 0 \le e_i \le \deg h_i - 2\right\}.$$

Then the code $C(D, G, g)$ has length $|D| = \deg g|S|$, dimension

$$t\left(\deg h_1 - 1\right)\left(h_2 - 1\right),$$

and minimum distance bounded below according to [7]. For $i = 1, 2$, $g_i^{-1}\left(g_i\left(Q\right)\right) \backslash \{Q\}$ serves as a recovery set for $Q \in S$. Hence, $C(D, G, g)$ has locality 2. Next we apply this construction to $\tilde{S}_q$.

Because $\tilde{S}_q$ is the fiber product of covers $S_q \to \mathbb{P}_x^1$ and $C_m \to \mathbb{P}_x^1$ where $C_m : t^m = x^q + x$, we may apply this construction to obtain a code with availability 2 and localities m and q; that is, every coordinate has 2 disjoint recovery sets, one of cardinality $q - 2q_0$ and one of cardinality $q - 1$. To do this, consider the projection maps $g_1 : \tilde{S}_q \to C_m$, $g_2 : \tilde{S}_q \to S_q$, and $g : \tilde{S}_q \to \mathbb{P}_x^1$. We take S as in (1), D as in (2), and $G := \alpha P_\infty$ where P_∞ is the unique point at infinity on $\mathbb{P}_x^1$. Fix a basis $\mathcal{B}$ of $\mathcal{L}(G)$, and

$$V := \left\langle f y^i t^j : f \in \mathcal{B} \right\rangle.$$

Theorem 2. *Suppose $C(D, G, g)$ is constructed as above. Then $C(D, G, g)$ is an $[n, k, d]$ code over $\mathbb{F}_{q^4}$ with availability 2 and recovery sets for each coordinate of sizes $q - 2q_0$ and $q - 1$, where*

$$n = \left(q - 2q_0 + 1\right)\left(q^4 + 2q_0 q^2\left(q - 1\right) - q^2\right),$$

$$k = \left(q - 2q_0\right)\left(\alpha\left(q^2 + 1\right) - q_0\left(q - 1\right) + 1\right),$$

and

$$d \ge n - \left(q - 2q_0 + 1\right)\left(\alpha - q - 2q_0 - 1\right).$$

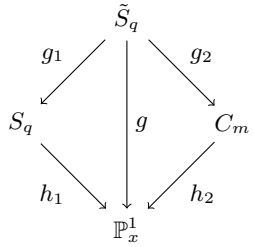

Fig. 1. Cyclic extension of Suzuki curve viewed as a fiber product

Proof. The parameters can be verified directly. We claim that

$$R^{(1)} := g_2^{-1}\left(g_2\left(P_{abc}\right)\right) \setminus \{P_{abc}\} = \left\{P_{ab'c} : b' \in \mathbb{F}_{q^4} \setminus \{b\}\right\}$$

and

$$R^{(2)} := g_1^{-1}\left(g_1\left(P_{abc}\right)\right) \setminus \{P_{abc}\} = \left\{P_{abc'} : c' \in \mathbb{F}_{q^4} \setminus \{c\}\right\}$$

are recovery sets for the position corresponding to P_{abc}. Suppose $f \in V$. Then $f(x,y,t) = \sum_{i=0}^{m-2}\sum_{j=1}^{M} a_{ij} f_j^* t^i$. Notice that $f(a,b,t) \in \mathbb{F}_q[t]$ and $\deg f(a,b,t) \leq m-2$. Hence, $f(a,b,t)$ can be recovered using the $m-1$ interpolation points: $P_{abc'} \in R$. As a result, $f\left(P_{abc}\right)$ may be recovered using only elements of R.

Observe the functions in the set V are modified from the construction in Section 2 in order to obtain multiple recovery sets for each position, thus impacting the dimension of the code.

One might compare this with the code found in [7, Theorem 6.1], which has availability 2 with recovery sets of size $q-1$, length $n = q(q-1)(q^2+2qq_0+q+1)$ and dimension $k = (q-1)(q-2)(q^2+2qq_0+q+1)$. Notice that the new codes defined using $\tilde{S}_q$ give the option of using a smaller recovery set (cardinality $q-2q_0$ compared with $q-1$).

References

1. Barg, A., Haymaker, K., Howe, E., Matthews, G. L., Varilly-Alvarado A.: Locally recoverable codes from algebraic curves and surfaces, in Algebraic Geometry for Coding Theory and Cryptography, E.W. Howe, K.E. Lauter, and J.L. Walker, Editors, Springer, 2017, pp. 95126.
2. Ballentine, S., Barg, A., Vlăduţ, S.: Codes with hierarchical locality from covering maps of curves. arXiv:1807.05473.
3. Eid, A., Hasson, H., Ksir, A. , Peachey, J.: Suzuki-invariant codes from the Suzuki curve. Des. Codes Cryptogr. (2016) 81: 413. https://doi.org/10.1007/s10623-015-0164-5.
4. Giulietti, M., Korchmros, G.: A new family of maximal curves over a finite field. Math. Ann. (2009) 343: 229. https://doi.org/10.1007/s00208-008-0270-z.
5. Guruswami, V., Jin, L., Xing, C.: Constructions of maximally recoverable local reconstruction codes via function fields. arXiv:1808.04539.

6. Hansen, J.P., Stichtenoth, H.: Group codes on certain algebraic curves with many rational points. Appl. Algebra Eng. Comm. Comput. 1, 6777 (1990).
7. Haymaker, K., Malmskog, B., Matthews, G. L.: Locally recoverable codes with availability $t \geq 2$ from fiber products of curves. Advances in Mathematics of Communications, 2018, 12 (2) : 317-336. doi: 10.3934/amc.2018020.
8. Jin, L., Ma, L., Xing, C.: Construction of optimal locally repairable codes via automorphism groups of rational function fields. 2017, arXiv:1710.09638
9. Kirfel, C., Pellikaan, R.: The minimum distance of codes in an array coming from telescopic semigroups. IEEE Transactions on Information Theory, vol. 41, no. 6, pp. 1720-1732, Nov. 1995. doi: 10.1109/18.476245
10. Li, X., Ma, L., and Xing, C.: Optimal locally repairable codes via elliptic curves. IEEE Transactions on Information Theory. doi: 10.1109/TIT.2018.2844216.
11. Matthews, G. L.: Codes from the Suzuki function field. IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 3298-3302, Dec. 2004. doi: 10.1109/TIT.2004.838102.
12. Montanucci, M., Timpanella, M., Zini, G.: AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves. J. Geom. (2018) 109: 23. https://doi.org/10.1007/s00022-018-0428-0.
13. Skabelund, D. C.: New maximal curves as ray class fields over Deligne-Lusztig curves. Proc. Amer. Math. Soc. 146 (2018), no. 2, 525–540.
14. Tamo, I., Barg, A.: Bounds on locally recoverable codes with multiple recovering sets, 2014 IEEE International Symposium on Information Theory, Honolulu, HI, 2014, pp. 691-695. doi: 10.1109/ISIT.2014.6874921.
15. Tamo, I., Barg, A.: A Family of Optimal Locally Recoverable Codes," in IEEE Transactions on Information Theory, vol. 60, no. 8, pp. 4661-4676, Aug. 2014. doi: 10.1109/TIT.2014.2321280.
16. Tsfasman, M., Vlăduţ, S., Zink, T.: Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound, Mathematische Nachrichten 109 (1982), pp. 2128.