Norm-trace-lifted codes over binary fields

Gretchen L. Matthews
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061 USA
Email: gmatthews@vt.edu

Aidan W. Murphy
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061 USA
Email: awmurphy@vt.edu

***Abstract*—In this paper, we introduce norm-trace-lifted codes over binary fields, which are codes with locality and high availability based on the norm-trace curve over the field $\mathbb{F}_{2^r}$. While they are inspired by Hermitian-lifted codes, norm-trace-lifted codes are easier to define and provide some potential advantages in terms of locality, meaning the number of symbols required to recover another, or alphabet size.**

I. Introduction

Codes with locality allow for the recovery of any codeword symbol utilizing only a few other symbols. They have been studied extensively in the literature [5], [12], [13], [14], [15] including utilizing Reed-Solomon and other codes from curves [2], [9]. The availability of such a code is the number of disjoint sets of coordinates that support this recovery. Hence, codes with high availability can recover a missing symbol in many different ways which means the stored information is more resilient against erasures.

Hermitian-lifted codes [10] were defined to yield high-availability codes for local recovery using the Hermitian curve. In this paper, we introduce the norm-trace-lifted codes, adapting the construction to the family of norm-trace curves given by

$$\mathcal{X}_{2,r} : x^{2^r-1} = y^{2^{r-1}} + y^{2^{r-2}} + \cdots + y^4 + y^2 + y$$

over $\mathbb{F}_{2^r}$, i.e., $N_{\mathbb{F}_{2^r}/\mathbb{F}_2}(x) = Tr_{\mathbb{F}_{2^r}/\mathbb{F}_2}(y)$, meaning the norm of x is the trace of y where both the norm and the trace are taken relative to the extension $\mathbb{F}_{2^r}/\mathbb{F}_2$. Codes from norm-trace curves were first studied by Geil [6]. The norm-trace-lifted code construction yields evaluation codes defined by functions which are easier to determine than for the Hermitian-lifted codes, due to number of intersection points of the norm-trace curve with non-horizontal lines in the projective space $\mathbb{P}^2$.

Recall that a code $C \subseteq \mathbb{F}_q^n$ has locality r if for each codeword coordinate i, there exists a set R_i of other coordinates such that for all $c \in C$, $c_i = \varphi(c\mid_{R_i})$ for some function $\varphi : \mathbb{F}_q^r \to \mathbb{F}_q$ and $\mid R_i \mid= r$. The set R_i (resp., $R_i \cup \{i\}$) is called a recovery set (resp., repair group) for i. If each coordinate i has t disjoint recovery sets, then the code is said to have availability t.

For the norm-trace-lifted codes, the repair groups are the sets of points of intersection between the curve and non-horizontal lines. The functions employed are those that restrict to low degree polynomials on the non-horizontal lines. Monomials which satisfy this property are called good monomials. For the Hermitian-lifted codes, characterizing the good monomials is a challenging problem which remains open. With the norm-trace-lifted codes considered here, the larger numbers of points of intersection alleviates this difficulty. In all, employing the norm-trace curve yields rates that are asymptotically better than those of the Hermitian-lifted codes, and one may choose whether to focus on smaller locality or maintaining availability. Alternate constructions for locally recoverable codes from norm-trace curves exist in [1] and [3], but each have distinct parameters from the codes constructed here. Lastly, the codes considered in this paper are not an extension of lifted Reed-Solomon codes [4], [7], [8] which utilize multivariate polynomials in such a way that restricting them to lines produces Reed-Solomon codewords. Rather, they are a new construction entirely in which one seeks to identify all functions on a curve that restrict to low degree polynomials on a lines. The difference between "lifted curve codes" and "curve-lifted codes" is expanded on in [10].

This paper is organized as follows. Intersection numbers are determined in Section II. They are applied to define the norm-trace-lifted codes in Section III. Examples and comparisons with other codes are given in Section IV, followed by a conclusion in Section V.

II. Intersection numbers

In this section, we consider how lines of the form $L_{\alpha,\beta}(t) := \left\{(t, \alpha t + \beta) : t \in \mathbb{F}_{2^r}^2\right\}$ intersect the curve

The work of the first author is supported in part by NSF under Grant DMS-1855136 and in part by the Commonwealth Cyber Initiative.

$\mathcal{X}_{2,r}$. Throughout, we will assume that $\alpha \neq 0$, meaning we do not consider horizontal lines. The set of lines of interest is

$$\mathbb{L} := \{L_{\alpha,\beta} : \alpha \in \mathbb{F}_{2^r}\backslash\{0\}, \beta \in \mathbb{F}_{2^r}\}.$$

Note that $\mathcal{X}_{2,r}$ has $2^{2r-1}+1$ $\mathbb{F}_{2^r}$-rational points, a single point at infinity denoted P_∞, and genus $(2^{r-1}-1)^2$ [11].

For $f \in \mathbb{F}_{2^r}[x,y]$ and $g \in \mathbb{F}_{2^r}[t]$ and a line $L_{\alpha,\beta} : \mathbb{F}_{2^r}[t] \to \mathbb{F}_{2^r}^2$, we say that $f \circ L_{\alpha,\beta}$ *agrees with* g *on* $\mathcal{X}_{2,r}$, and write

$$f \circ L_{\alpha,\beta} \equiv g,$$

if $f(L_{\alpha,\beta}(t)) = g(t)$ for all $t \in \mathbb{F}_{2^r}$ with $L_{\alpha,\beta}(t) \in \mathcal{X}_{2,r}$.

Given $\alpha, \beta \in \mathbb{F}_{2^r}$, it will be useful to consider the polynomial

$$p_{\alpha,\beta}(t) := t^{2^r-1} + \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha t + \mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta).$$

Lemma 1. *Consider the norm-trace curve $\mathcal{X}_{2,r}$ over $\mathbb{F}_{2^r}$ with $r \geq 2$. The intersection between a line $L_{\alpha,\beta} \in \mathbb{L}$ and $\mathcal{X}_{2,r}$ has cardinality of $2^{r-1}-1$ or $2^{r-1}+1$; that is,*

$$\mid L_{\alpha,\beta} \cap \mathcal{X}_{2,r} \mid = 2^{r-1} \pm 1.$$

Proof. Notice that points in the intersection $L_{\alpha,\beta} \cap \mathcal{X}_{2,r}$ correspond to values t that satisfy the equation

$$t^{2^r-1} = (\alpha t + \beta)^{2^{r-1}} + \cdots + (\alpha t + \beta)^2 + (\alpha t + \beta).$$

Expanding the terms on the right with Freshman's Dream gives

$$p_{\alpha,\beta}(t) = 0. \tag{1}$$

To determine $|L_{\alpha,\beta} \cap \mathcal{X}_{2,r}|$, we wish to find the degree of $d(t) = \gcd(p_{\alpha,\beta}(t), t^{2^r} - t)$, as the number of points of intersection is exactly the degree of $d(t)$, since $t^{2^r} - t$ is separable over $\mathbb{F}_{q^r}$. Because $\mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) \in \{0,1\}$, we consider two cases as follows.

Case 1: Suppose $\mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) = 0$. Applying the Euclidean algorithm yields

$$\gcd(p_{\alpha,\beta}(t), t^{2^r} - t) = \alpha^{2^{r-1}} t^{2^{r-1}+1} + \cdots + \alpha t^2 + t.$$

See that the degree of this polynomial is $2^{r-1}+1$.

Case 2: Suppose $\mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) = 1$. We again apply the Euclidean algorithm to obtain

$$\gcd(p_{\alpha,\beta}(t), t^{2^r} - t) = \alpha^{2^{r-1}} t^{2^{r-1}-1} + \cdots + \alpha.$$

See that the degree of this polynomial is $2^{r-1}-1$. We conclude that the number of points in the intersection $L_{\alpha,\beta} \cap \mathcal{X}_{2,r}$ is $2^{r-1} \pm 1$. ■

In the next section, we will define codes for which certain points on the lines $L_{\alpha,\beta} \in \mathbb{L}$ will act as repair groups for a coordinate. Lemma 1 guarantees at least $2^{r-1}-1$ available points, giving rise to codes with locality $2^{r-1}-2$.

III. Codes with locality from the norm-trace curve

In this section, we introduce the norm-trace-lifted codes. Polynomials of bounded degree are crucial to the code construction; the set of polynomials in an indeterminate t of degree at most k with coefficients in $\mathbb{F}_{2^r}$ is denoted $\mathbb{F}_{2^r}[t]_{\leq k}$. We will use standard notation from coding theory. An $[n,k]$ code C over a finite field $\mathbb{F}$ is an $\mathbb{F}$-subspace of $\mathbb{F}^n$ with $\dim_{\mathbb{F}} C = k$. The rate of C is $\frac{k}{n}$.

Definition 1. The *norm-trace-lifted code* $\mathcal{C}$ is the evaluation code

$$\mathcal{C} := \{(f(x,y))_{(x,y)\in\mathcal{X}_{2,r}} : f \in \mathcal{F}\} \subseteq \mathbb{F}_{2^r}^{2^{2r-1}}$$

where

$$\mathcal{F} := \left\{ f \in \mathbb{F}_{2^r}[x,y] : \begin{array}{l} \exists g \in \mathbb{F}_{2^r}[t]_{\leq 2^{r-1}-3} \text{ with} \\ f \circ L_{\alpha,\beta} \equiv g \ \forall L_{\alpha,\beta} \in \mathbb{L}, \end{array} \right\}.$$

Hence, the norm-trace-lifted code is the image of $\mathcal{F}$ under the evaluation map

$$\begin{array}{rccl} ev: & \mathbb{F}_{2^r}^{2^{2r-1}}[x,y] & \longrightarrow & \mathbb{F}_{2^r}^n \\ & f & \longmapsto & (f(x,y))_{(x,y)\in\mathcal{X}_{2,r}}. \end{array}$$

It is immediate that $\mathcal{C}$ has length $n = 2^{2r-1}$.

For $\mathcal{C}$, the intersection of a line and the curve is essentially a Reed-Solomon code, because on that set, we are considering low-degree univariate polynomials. In this way, the repair of information would be Reed-Solomon in nature. Also, as each point lies on many lines, recovery may use any of a number of Reed-Solomon codes, one for each line the point lies on.

Next, we consider the rate of $\mathcal{C}$. We will show the rate of these norm-trace-lifted codes is asymptotically nonzero. To do so, we only need to count the number of monomials $M_{ab} := x^a y^b$ which have $a+b$ less than the desired locality of $2^{r-1}-2$.

Lemma 2. *The set of vectors*

$$\left\{ (M_{a,b}(x,y))_{(x,y)\in\mathcal{X}_{q,r}} : \begin{array}{l} 0 \leq a \leq q^{r-1}-1, \\ 0 \leq b \leq q^r - 1 \end{array} \right\}$$

in $\mathbb{F}_{q^r}^{q^{2r-1}}$ is linearly independent.

Proof. Let $\mathcal{L}(mP_\infty)$ denote the Riemann-Roch space associated with the divisor mP_∞, where P_∞ is the point at infinity on the norm-trace curve. We draw inspiration from [10]. The kernel of the evaluation map

$$\begin{array}{rccc} ev: & \mathcal{L}(mP_\infty) & \to & \mathbb{F}_{q^r}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_{q^r})). \end{array}$$

of the q^r affine points of the norm-trace curve $\mathcal{X}_{q,r}$ is generated by

$$x^{\frac{q^r-1}{q-1}} - y^{q^{r-1}} - \cdots - y^q - y,$$
$$x^{q^r} - x, \text{ and } y^{q^r} - y.$$

Under monomial orderings with $x^{\frac{q^r-1}{q-1}} < y^{q^{r-1}}$, $\left\{x^{\frac{q^r-1}{q-1}} - y^{q^{r-1}} - \cdots - y^q - y, x^{q^r} - x\right\}$ is a Gröbner basis for the kernel of the evaluation map, and so the evaluations of $M_{a,b}$ cannot contain any element from the kernel of the evaluation map. Thus, the evaluations of $M_{a,b}$ are linearly independent. ∎

A key difference between this work and that of Hermitian-lifted codes [10] centers on the rate of the codes. There, monomials $x^a y^b$ with $a + b < q$ are among those evaluated to produce codewords. However, the number of such monomials alone is $\frac{q(q+1)}{2}$, giving lower bounds on code rates that are asymptotically zero. Hence, some monomials with $a + b > q$ needed to be counted to guarantee that the rate was asymptotically bounded away from zero. However, as we will see, for binary norm-trace-lifted codes, this is not necessary: more monomials fall naturally within the specifications to produce codewords.

For a polynomial $g(t) \in \mathbb{F}_{2^r}[t]$, define $\hat{g}_{\alpha,\beta}(t)$ to be the remainder resulting from dividing $g(t)$ by $p_{\alpha,\beta}(t)$, and define

$$\deg_{\alpha,\beta}(g) := \deg(\hat{g}_{\alpha,\beta}).$$

Notice that $\deg_{\alpha,\beta}(g) \leq 2^{r-1}-2$ for all $g \in \mathbb{F}_{2^r}[t]$. With the above definition, we note that $M_{a,b} \in \mathcal{F}$ provided

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{\alpha,\beta}) < 2^{r-1} - 2,$$

motivating the next definition.

Definition 2. A monomial $M_{a,b}(x, y)$ is said to be *good* if for all lines $L_{\alpha,\beta} \in \mathbb{L}$,

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{\alpha,\beta}) < 2^{r-1} - 2.$$

Note that if $M_{a,b}$ is good, then $M_{a,b} \in \mathcal{F}$. Hence, we wish to find a large set of good monomials due to Lemma 2. The definitions above provide the exact rate in the following lemma.

Theorem 3. *The norm-trace-lifted code $\mathcal{C}$ over $\mathbb{F}_{2^r}$ is an $[2^{2r-1}, (0.25 - \varepsilon_r) \cdot 2^{2r-1}, \geq 2^r]$ code with locality $2^{r-1} - 2$ and availability $2^r - 1$. Moreover, the rate of the associated norm-trace-lifted code is asymptotically* 0.25

Proof. First, note that the locality of $\mathcal{C}$ follows from Lemma 1. Since each line in $\mathbb{L}$ intersects the curve $\mathcal{X}_{2,r}$ in exactly $2^{r-1}-1$ or $2^{r-1}+1$ distinct affine points, the locality is $(2^{r-1}-1)-1 = 2^{r-1}-2$. Indeed, fix an $\mathbb{F}_{2^r}$-rational point P on $\mathcal{X}_{2,r}$ and a line $L_{\alpha,\beta} \in \mathbb{L}$ through P. Then for $f \in \mathcal{F}$, $f(x, y)|_{L_{\alpha,\beta}} = g(t) \in \mathbb{F}_{2^r}[t]_{\leq 2^{r-1}-3}$. Since $|(L_{\alpha,\beta} \cap \mathcal{X}_{2,r}) \setminus \{P\}| \geq 2^{r-1} - 2$, $f(P)$ may be determined by these $2^{r-1} - 2$ interpolation points.

The availability may be found by determining the number of lines that pass through a given point which intersect the curve in at least $2^{r-1} - 1$ points; since this describes all lines in the space, we simply count the number of lines through any given point. If we fix a particular point, and a particular slope α, then the other parameter of the line β is determined. Similarly, if β is fixed for a point, then α is determined. So, we only consider the number of possible α for a point; this is then simply $2^r - 1$.

To determine the dimension of $\mathcal{C}$, note that the number of monomials M_{ab} with $a + b < 2^{r-1} - 2$ is

$$\frac{(2^{r-1} - 2)(2^{r-1} - 1)}{2} = 2^{2r-3} - 2^{r-1} - 2^{r-2} + 1.$$

Since the number of points on $\mathcal{X}_{2,r}$ is 2^{2r-1}, the norm-trace-lifted code has rate at least

$$\frac{2^{2r-3} - 2^{r-1} - 2^{r-2} + 1}{2^{2r-1}} = \frac{1}{4} - \varepsilon_r$$

where $\varepsilon_r := \frac{1}{2^r} + \frac{1}{2^{r+1}} - \frac{1}{2^{2r-1}}$. Since $\varepsilon_r \to 0$ as $r \to \infty$, the rate approaches $\frac{1}{4}$ as $r \to \infty$.

Next, we show that there are no good monomials $M_{a,b}$ with $a + b \geq 2^{r-1} - 2$. Recall that $0 \leq a \leq 2^r$ and $0 \leq b \leq 2^{r-1}$. To show that such a monomial $M_{a,b}$ is not good, we must find some line L_{α^*,β^*} such that $\deg_{\alpha^*,\beta^*}(M_{a,b} \circ L_{\alpha^*,\beta^*}) \geq 2^{r-1} - 2$.

We consider the following cases to show this fact. In each case, we consider the specific line $L_{1,0}(t) = (t, t)$; because of the particular line considered, $(M_{a,b} \circ L_{1,0})(t) = t^{a+b}$.

Case 1: Let $2^{r-1} - 2 < a+b < 2^r - 1$. Then, because the degree of $p_{1,0}(t)$ is $2^r - 1$, we have

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{1,0}) = \deg_{\alpha,\beta}(t^{a+b}) = a+b > 2^{r-1}-2.$$

Thus, the monomial $M_{a,b}$ is not good.

Case 2: Let $2^r - 1 \leq a + b \leq 2^r + 2^{r-1}$. Then, extending the previous case,

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{1,0}) = \deg_{\alpha,\beta}(t^{a+b}) \geq 2^{r-1} > 2^{r-1}-2.$$

This is because $t^{2^r-1} = t^{2^{r-1}} + \cdots + t$, so again $M_{a,b}$ is not good.

Since in each of the cases above, $\deg_{\alpha,\beta}(M_{a,b} \circ L_{1,0}) > 2^{r-1} - 2$, there are no good monomials with $a + b \geq 2^{r-1} - 2$, so the rate of the code is $0.25 - \varepsilon_r$.

Now we show a lower bound on the minimum distance. We utilize the same counting argument given in [10]. If $c \in \mathcal{C}$ is a codeword with a nonzero symbol in the i^{th} position, then this symbol corresponds to a function f_c which is nonzero on that point. The position i has $2^r - 1$ disjoint recovery sets as we showed above, each of which has at least one corresponding nonzero symbol in c. So, any nonzero codeword must have nonzero entries in at least 2^r positions. ■

Next, we compare the norm-trace-lifted codes with close relatives, including one-point norm-trace codes and Hermitian-lifted codes. In addition, examples of norm-trace-lifted codes are provided.

First, we consider one-point norm-trace codes. Recall that

$$\mathcal{L}(mP_\infty) = \left\langle x^a y^b : \begin{array}{l} a, b \in \mathbb{Z}^+, \\ a2^{r-1} + b\left(2^r - 1\right) \le m \end{array} \right\rangle$$

and the one-point norm-trace code is

$$C(D, mP_\infty) = \left\{ (f(P_1), \dots, f(P_n)) : f \in \mathcal{L}\left(mP_\infty\right) \right\}.$$

We claim that

$$\mathcal{L}(\left(2^{2r-2} - 3 \cdot 2^{r-1}\right) P_\infty) \subseteq \mathcal{F}$$

so that

$$C(D, mP_\infty) \subseteq \mathcal{C}.$$

Let $\hat{m} = 2^{2r-2} - 3 \cdot 2^{r-1}$; we wish to show that this gives $a + b \le 2^{r-1} - 3$, so $x^a y^b \in \mathcal{F}$. If $a2^{r-1} + b(2^r - 1) \le 2^{2r-2} - 3 \cdot 2^{r-1}$, then

$$\begin{aligned} a + b &\le a + 2b - \frac{b}{2^{r-1}} = \frac{a2^{r-1} + b2^r - b}{2^{r-1}} \\ &\le \left\lfloor \frac{2^{2r-2} - 3 \cdot 2^{r-1}}{2^{r-1}} \right\rfloor = \left\lfloor 2^{r-1} - 3 \right\rfloor = 2^{r-1} - 3. \end{aligned}$$

Therefore, since $\hat{m} \le 2^{2r-2} - 3 \cdot 2^{r-1}$, all monomials $x^a y^b \in \mathcal{L}(\hat{m}P_\infty)$ are in the set $\mathcal{F}$.

Next, we confirm that $C(D, \hat{m}P_\infty) \subsetneq \mathcal{C}$. The monomial $y^{2^{r-1}-3} \in \mathcal{F}$, since $a + b < 2^{r-1} - 2$. However, $M_{a,b} \in \mathcal{L}(\hat{m}P_\infty)$ would need to satisfy $a2^{r-1} + b(2^r - 1) \le \hat{m}$. Then, if we consider $a = 0$, the largest that b could be for a monomial y^b would be $\left\lfloor \frac{2^{2r-2} - 3 \cdot 2^{r-1}}{2^r - 1} \right\rfloor \le 2^{r-2} - 2$, because $\hat{m} \le 2^{2r-2} - 3 \cdot 2^{r-1}$. With this, it is clear that the monomial $y^{2^{r-1}-3}$ could not be in $\mathcal{L}(\hat{m}P_\infty)$, because for $y^b \in \mathcal{L}(\hat{m}P_\infty)$ we have shown $b \le 2^{r-2} - 2 < 2^{r-1} - 3$ for $r > 2$. Thus, the sets of evaluation polynomials for the two codes are different. This difference is highlighted in Figure 2.

We also claim that the rate of one-point norm-trace codes with $\hat{m} \le 2^{2r-2} - 3 \cdot 2^{r-1}$ defined over $\mathbb{F}_{2^r}$ is asymptotically 0.125. To find the dimension of $C(D, \hat{m}P_\infty)$, we must count all pairs (a, b) with a and b nonnegative, and $a2^{r-1} + b(2^r - 1) \le 2^{2r-2} - 3 \cdot 2^{r-1}$. So, we wish to find integer solutions within the triangle formed by $(0, 0)$, $(2^{r-1} - 2, 0)$, and $(0, 2^{r-2} - 1)$ (this will yield an overestimate of the dimension). By Pick's theorem, we have that for a plane polygon with integer vertices,

$$A = i + \frac{b}{2} - 1$$

where A is the area of the figure, i the number of interior integer points, b the number of boundary integer points. We will use this to determine $i + b$.

First, by counting, the number of boundary points is

$$(2^{r-1} - 2) + (2^{r-2} - 1) + 2^{r-2} - 3 = 2^r - 6.$$

The area of the figure is just the area of a triangle, so

$$A = \frac{1}{2}\left(2^{r-2} - 1\right)\left(2^{r-1} - 2\right) = 2^{2r-4} - 2^{r-1} + 1.$$

With these two above calculations of A and b, we find the number of interior points to be $i = 2^{2r-4} - 2^r + 5$, so the dimension is upper bounded by $i + b = 2^{2r-4} - 1$. Finally, the rate of the code is asymptotically

$$\frac{2^{2r-4} - 1}{2^{2r-1}} = \frac{1}{2^3} - \frac{1}{2^{2r-1}} \to \frac{1}{8} \text{ as } r \to \infty.$$

In the Hermitian case, the good monomials with $a + b$ less than the locality q were exactly those which formed the basis for the one-point Hermitian codes. It was then those good monomials with $a + b \ge q$ which caused the rate of the lifted codes to be nonzero asymptotically.

This is in contrast with the binary norm-trace-lifted codes, where the good monomials with $a + b < 2^{r-1} - 2$ are the only monomials present. This can be seen in Figure 2. This triangular shape is slightly different from what is observed in the Hermitian-lifted case in two key ways. For Hermitian-lifted codes, the monomials with $a + b$ greater than the locality are necessary to achieve the given rate results.

The figures in this section represent monomials $x^a y^b$, where a is on the horizontal axis and b is on the vertical axis.

IV. Examples and Code Comparisons

In this section, we consider examples and comparisons with Hermitian-lifted codes and one-point codes from norm-trace curves.

Example 1. Figures 1 and 2 reveal the differences in the functions that define codewords when compared with

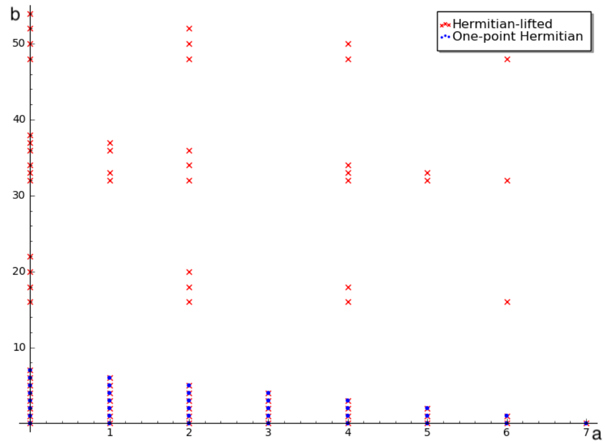

Fig. 1. Monomials $x^a y^b$ evaluated for one-point Hermitian code compared with HLC when $q = 8$ (over $\mathbb{F}_{64}$).

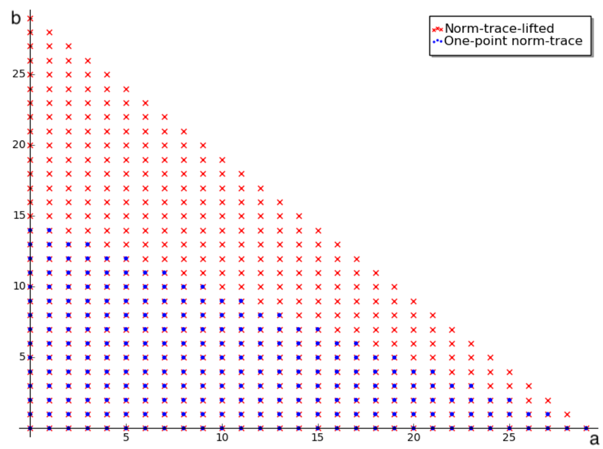

Fig. 2. Monomials $x^a y^b$ evaluated for one-point norm-trace code compared with NTLC when $r = 6$ (over $\mathbb{F}_{64}$).

their one-point code counterparts. Additional monomials may define codewords in the Hermitian-lifted codes.

Example 2. Figure 3 shows why the rates for the norm-trace-lifted codes are better than for Hermitian-lifted codes. Table I compares the Hermitian-lifted codes with the norm-trace-lifted codes based on their localities.

Example 3. Consider the case when $r = 6$ shown in Table II. Values for the dimensions and rates of the Hermitian-lifted codes may be found in [10].

V. Conclusion

In this paper, we introduce norm-trace-lifted codes over binary fields, which are codes with locality and

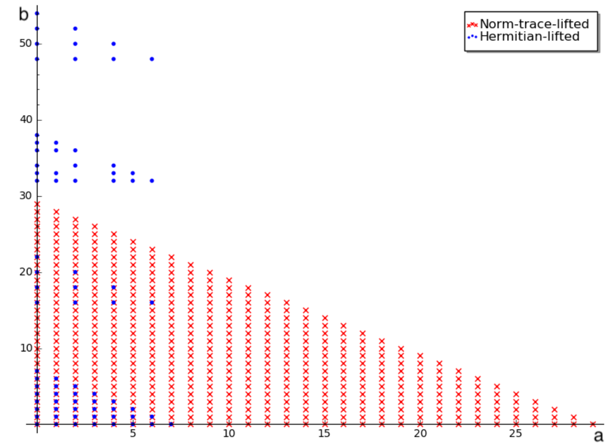

Fig. 3. Monomials $x^a y^b$ evaluated for HLC compared with NTLC when $q = 8$ and $r = 6$ respectively (over $\mathbb{F}_{64}$).

TABLE I

Lifted code comparisons, general

	HLC	NTLC
Locality	2^{r-1}	$2^{r-1} - 2$
Alphabet Size	2^{2r-2}	2^r
Availability	$2^{2r-2} - 1$	$2^r - 1$
Length	2^{3r-3}	2^{2r-1}
Dimension	$\geq 0.007 \cdot 2^{3r-3}$	$(0.25 - \varepsilon_r) \cdot 2^{2r-1}$
Rate	≥ 0.007	$0.25 - \varepsilon_r$
Min. Dist.	$d \geq 2^{2r-2}$	$d \geq 2^r$

TABLE II

One-point codes versus lifted codes over $\mathbb{F}_{64}$

$(r = 6)$	Norm-trace code	HLC	NTLC
Field size	64	64	64
Locality	30	8	30
Availability	63	63	63
Length	2048	512	2048
Dimension	240	75	465
Rate	~ 0.117	~ 0.146	~ 0.227

high availability based on the norm-trace curve over the field $\mathbb{F}_{2^r}$. They are easier to construct than the Hermitian-lifted codes; indeed the functions that define the codewords are explicit and simple to describe. Moreover, the norm-trace-lifted codes compare favorably with Hermitian-lifted codes in that they are higher rate and smaller locality over a smaller alphabet, though this comes with less availability. In addition, they provide higher rate with identical locality and availability when compared with one-point codes on the norm-trace curve.

References

[1] Edoardo Ballico and Chiara Marcolla. Higher Hamming weights for locally recoverable codes on algebraic curves. *Finite Fields*

Appl., 40(C):61–72, July 2016.

[2] Alexander Barg, Itzhak Tamo, and Serge Vlăduţ. Locally recoverable codes on algebraic curves. *IEEE Transactions on Information Theory*, 63(8):4928–4939, 2017.

[3] Daniele Bartoli, Maria Montanucci, and Luciane Quoos. Locally recoverable codes from automorphism groups of function fields of genus $g \geq 1$. *IEEE Transactions on Information Theory*, 66(11):6799–6808, 2020.

[4] Eli Ben-Sasson, Ariel Gabizon, Yohay Kaplan, Swastik Kopparty, and Shubangi Saraf. A new family of locally correctable codes based on degree-lifted algebraic geometry codes. In *Proceedings of the forty-fifth annual ACM symposium on Theory of Computing*, pages 833–842, 2013.

[5] S. Luna Frank-Fischer, Venkatesan Guruswami, and Mary Wootters. Locality via partially lifted codes. *CoRR*, abs/1704.08627, 2017.

[6] Olav Geil. On codes from norm-trace curves. *Finite Fields and their Applications*, 9(3):351 – 371, 2003.

[7] Alan Guo. High-rate locally correctable codes via lifting. *IEEE Transactions on Information Theory*, 62(12):6672–6682, 2015.

[8] Alan Guo, Swastik Kopparty, and Madhu Sudan. New affine-invariant codes from lifting. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 529–540, 2013.

[9] Kathryn Haymaker, Beth Malmskog, and Gretchen L. Matthews. Locally recoverable codes with availability t$\geq$2 from fiber products of curves. *Advances in Mathematics of Communications*, 12(2):317, 2018.

[10] Hiram H López, Beth Malmskog, Gretchen L Matthews, Fernando Piñero-González, and Mary Wootters. Hermitian-lifted codes. *Designs, Codes and Cryptography*, 89(3):497–515, 2021.

[11] Carlos Munuera, Guilherme C Tizziotti, and Fernando Torres. Two-point codes on norm-trace curves. In *Coding Theory and Applications*, pages 128–136. Springer, 2008.

[12] Ankit Singh Rawat, Dimitris S Papailiopoulos, Alexandros G Dimakis, and Sriram Vishwanath. Locality and availability in distributed storage. In *2014 IEEE International Symposium on Information Theory*, pages 681–685. IEEE, 2014.

[13] Itzhak Tamo and Alexander Barg. Bounds on locally recoverable codes with multiple recovering sets. In *2014 IEEE International Symposium on Information Theory*, pages 691–695. IEEE, 2014.

[14] Itzhak Tamo, Alexander Barg, and Alexey Frolov. Bounds on the parameters of locally recoverable codes. *IEEE Transactions on Information Theory*, 62(6):3070–3083, 2016.

[15] Anyu Wang and Zhifang Zhang. Repair locality with multiple erasure tolerance. *IEEE Transactions on Information Theory*, 60(11):6979–6987, 2014.