On Subfield Subcodes Obtained from Restricted Evaluation Codes*

Cem Güneri[1], Ferruh Özbudak[2], and Selcen Sayıcı[2]

Faculty of Engineering and Natural Sciences, Sabancı University, 34956, Tuzla, İstanbul, Turkey
cem.guneri@sabanciuniv.edu
Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
ozbudak@metu.edu.tr, ssayici@metu.edu.tr

Abstract. Galindo et al. introduced a class of codes which are obtained by evaluation of polynomials at the roots of a trace map ([4]). Via subfield subcodes, this construction yields new linear codes with good parameters as well as good resulting quantum codes. Here, we extend this construction to allow evaluation at the roots of any polynomial which splits in the field of evaluation. Our proof relies on Galois-closedness of codes in consideration. Moreover, we introduce a lengthening process that preserves Galois-closed property of restricted evaluation codes. Subfield subcodes of such lengthened codes yield further good linear codes.

Keywords: Evaluation code · subfield subcode · good codes.

1 Introduction

In [4], the authors constructed a class of evaluation codes at the roots of the trace polynomial from $\mathbb{F}_{q^{2n}}$ to $\mathbb{F}_q$. Then, they studied the subfield subcodes over $\mathbb{F}_{q^2}$ of the dual of these evaluation codes. The set of polynomials evaluated at the trace roots are generated by monomials, whose exponents come from a union of consecutive q^2-cyclotomic cosets. Polynomials evaluated in the construction and the restricted set of evaluation points play role in the parameters of the dual code and its subfield subcode. Namely, a BCH-type bound is obtained for the dual code and its subfield subcode via the cyclotomic cosets. Due to evaluation at the trace roots, one can possibly have a gain in the dimension of the dual code and its subfield subcode. As a result, they obtained two record-breaking codes over $\mathbb{F}_4$ ($[128, 70, 20]_4$ and $[128, 75, 22]_4$ codes) and further obtained good codes via shortening of these two original codes. Without proof, they also noted that one can have similar results if the evaluation is carried out at the complementary set in $\mathbb{F}_{q^{2n}}$ of the roots of the trace polynomial.

* The authors are supported by a bilateral cooperation program between Korea and Turkey: TÜBİTAK project 120N932.

We call such evaluation codes "restricted evaluation codes" in this manuscript. As noted in [4], these codes are special one variable J-affine variety codes ([2, 3]), with $J = \emptyset$.

We first observe that this construction can be extended to more general restricted evaluation codes. Namely, for any extension field $\mathbb{F}_{q^n}/\mathbb{F}_q$ and any polynomial $\Lambda(X)$ that splits in $\mathbb{F}_{q^n}$ (i.e. having all roots in $\mathbb{F}_{q^n}$), we evaluate polynomials generated by consecutive $\mathbb{F}_q$-cyclotomic cosets at the roots of Λ. A critical fact here is that the choice of such evaluated polynomials guarantees that the resulting evaluation code over $\mathbb{F}_{q^n}$, and hence its dual, is Galois closed with respect to $\mathbb{F}_q$, regardless of the choice of Λ. It is well-known that the subfield subcode over $\mathbb{F}_q$ and the original $\mathbb{F}_q$-Galois closed code have the same dimension and minimum distance [7]. Hence we can determine the dimension and estimate the minimum distance of the subfield subcode of the dual code as in [4] for these more general restricted evaluation codes.

Moreover, we introduce a lengthening process for these restricted evaluation codes in a way that the resulting code is still Galois closed. We state the dimension and the BCH bound for the dual code of the lengthened code, which are valid for the subfield subcode as well due to Galois closedness. Via this new construction, we obtain 6 new codes (with respect to [5]) over $\mathbb{F}_4$. Two of these new codes are of length 193 and four of them are of length 129. Two of the new length 129 new codes yield further record-breaking codes by shortening. The fact that our results allow the use of arbitrary polynomials Λ instead of a particular trace polynomial, and the new lengthening idea, show high potential to lead to further code examples that improve currently known best code parameters.

We introduce evaluation codes in Section 2 and general restricted evaluation codes in Section 3. The new lengthening construction is presented in Section 4. Theorems 1 and 2 state the parameters of subfield subcodes obtained from generalized restricted evaluation codes and their lengthening, respectively. Good codes found by lengthening are presented in Example 1.

2 Evaluation Codes

Let q be a power of a prime number p, $n \geq 2$ be an integer and $R = q^n$. Let $\{Q_1, Q_2, \ldots, Q_R\}$ be the set of elements of $\mathbb{F}_{q^n}$.

For $0 \leq \ell < q^n - 1$, let

$$Orbit(\ell) = \{q^u \ell \bmod (q^n - 1) : 0 \leq u \leq n - 1\}.$$

Note that $Orbit(\ell)$ is also commonly called the q-cyclotomic coset of ℓ modulo $(q^n - 1)$. We define ℓ as the *orbit leader* if $\ell < \ell'$ for all other $\ell' \in Orbit(\ell)$. Let m be the number of distinct orbits, which can be computed explicitly. We list the orbit leaders in increasing order as $0 = \ell_1 < \ell_2 < \ldots < \ell_m$. Let us also note that the orbits as defined above partition the set $\{0, 1, \ldots, q^n - 2\}$ into disjoint sets and the size t of any such orbit divides n ([6, Pages 114-115]).

Consider the quotient ring $\mathbb{F}_{q^n}[X]/\langle X^R - X\rangle$. For $f(X) \in \mathbb{F}_{q^n}[X]$, denote the representative of the coset containing $f(X)$ by $Red(f)$. Hence, $Red(f)$ is

the unique polynomial of degree less than R which satisfies $Red(f) \equiv f \bmod (X^R - X)$. For $f(X) \in \mathbb{F}_{q^n}[X]$ and $\rho \in \mathbb{F}_{q^n}$, let $Ev(f, \rho)$ denote the evaluation of the polynomial $f(X)$ at ρ.

For $1 \leq s \leq m$, let $V(s)$ be the subspace of $\mathbb{F}_{q^n}[X]/\langle X^R - X\rangle$ defined as

$$V(s) = \mathrm{Span}_{\mathbb{F}_{q^n}}\Big\{X^i : i \in \bigcup_{j=1}^{s} Orbit(\ell_j)\Big\}. \tag{1}$$

If t_j denotes the cardinality of $Orbit(\ell_j)$, for each j, then $V(s)$ consists of $t_1 + \cdots + t_s$ distinct monomials whose powers come from the orbits. Hence we have $\dim_{\mathbb{F}_{q^n}} V(s) = t_1 + \cdots + t_s$.

Note that the following map is well-defined and it is an injective $\mathbb{F}_{q^n}$-linear transformation.

$$\begin{array}{rcl} Ev : \mathbb{F}_{q^n}[X]/\langle X^R - X\rangle & \longrightarrow & \mathbb{F}_{q^n}^R \\ Red(f) & \longmapsto & (Ev(Red(f), Q_1), \ldots, Ev(Red(f), Q_R)) \end{array} \tag{2}$$

The image C of this map, when restricted to $V(s)$, is an evaluation code, which is a linear code over $\mathbb{F}_{q^n}$ of length R and dimension $\dim_{\mathbb{F}_{q^n}} V(s)$.

We denote by $C^\perp$ the dual code with respect to the Euclidean inner product throughout the paper. For $C^\perp$, we have the BCH bound $d(C^\perp) \geq \ell_{s+1} + 1$, due to definition of ℓ_j's (orbit leaders). Hence, $C^\perp$ is a $[R, R - \sum_{i=1}^{s} t_i, \geq \ell_{s+1} + 1]_{q^n}$ linear code. The subfield subcode of $C^\perp$ is defined as $C^\perp_{|\mathbb{F}_q} := C^\perp \cap \mathbb{F}_q^R$. By construction of C, it can be shown that the parameters of $C^\perp$ and $C^\perp_{|\mathbb{F}_q}$ are the same. The reason behind this fact will be explained in Section 3.

3 Restricted Evaluation Codes and Subfield Subcodes

Let N be an integer such that $N < R = q^n$ and consider N distinct elements $P_1, P_2, \ldots, P_N$ of $\mathbb{F}_{q^n}$. Consider the polynomial

$$\Lambda(X) = \prod_{i=1}^{N}(X - P_i) \in \mathbb{F}_{q^n}[X],$$

which clearly divides $X^R - X$.

We revise the notions introduced in Section 2 now. Consider the quotient ring $\mathbb{F}_{q^n}[X]/\langle \Lambda(X)\rangle$. For $f(X) \in \mathbb{F}_{q^n}[X]$, denote the representative of the coset containing $f(X)$ by $Red(f)$. Hence, $Red(f)$ is the unique polynomial of degree less than N which satisfies $Red(f) \equiv f \bmod (\Lambda(X))$. It is clear that $Ev(f, \rho) = Ev(Red(f), \rho)$ for $\rho \in \{P_1, \ldots, P_N\}$. We define the space $V(s)$ as in (1), though we note that the reduction of monomials is modulo $\Lambda(X)$ (instead of $X^R - X$ as in Section 2). A crucial point to note here is that some elements in orbits $Orbit(\ell_j)$, which go into the degrees of monomials in $V(s)$, may be greater than or equal to $N = \deg \Lambda(X)$. This brings the possibility over $\mathbb{F}_{q^n}$ of dimension

of $V(s)$, as a subspace of $\mathbb{F}_{q^n}[X]/\langle \Lambda(X)\rangle$, being smaller than $t_1 + \cdots + t_s$ (cf. Remark 2).

Consider the restricted evaluation map:

$$\begin{array}{rcl} Ev : \mathbb{F}_{q^n}[X]/\langle \Lambda(X)\rangle & \longrightarrow & \mathbb{F}_{q^n}^N \\ Red(f) & \longmapsto & (Ev(Red(f), P_1), \ldots, Ev(Red(f), P_N)) \end{array} \tag{3}$$

We denote the image $Ev(V(s))$ of this injective $\mathbb{F}_{q^n}$-linear map by $C_1(s)$, which is the restricted evaluation code we study.

For $1 \leq i \leq s$, the orbit of ℓ_i consists of t_i elements, which we denote by $Orbit(\ell_i) = \{\ell_i = \ell_{i,1}, \ell_{i,2}, \ldots \ell_{i,t_i}\}$. Hence, $\ell_{i,u} = q\ell_{i,u-1} \pmod{q^n - 1}$ for all $u = 2, \ldots, t_i$. For each $u \in \{1, 2, \ldots, t_i\}$, define the following length N vector:

$$R_{i,u} = (Ev(Red(X^{\ell_{i,u}}), P_1),\ Ev(Red(X^{\ell_{i,u}}), P_2),\ \ldots,\ Ev(Red(X^{\ell_{i,u}}), P_N)). \tag{4}$$

Consider the $t_i \times N$ matrix

$$M_i = \begin{bmatrix} R_{i,1} \\ R_{i,2} \\ \vdots \\ R_{i,t_i} \end{bmatrix},$$

and put all of these matrices together (for $1 \leq i \leq s$) to define a $(t_1 + t_2 + \ldots + t_s) \times N$ matrix M over $\mathbb{F}_{q^n}$:

$$M = \begin{bmatrix} M_1 \\ M_2 \\ \vdots \\ M_s \end{bmatrix}$$

It is clear that M generates $C_1(s)$ and its rank is $\dim_{\mathbb{F}_{q^n}} V(s)$. We let $C_2(s) = C_1(s)^{\perp}$, where $\perp$ denotes the dual with respect to the Euclidean inner product on $\mathbb{F}_{q^n}^N$. Define the code $C(s)$ as the subfield subcode of $C_2(s)$ over $\mathbb{F}_q$, which is $C(s) = C_2(s)_{|\mathbb{F}_q} := C_2(s) \cap \mathbb{F}_q^N$.

Remark 1. For any $f(X) \in \mathbb{F}_{q^n}[X]$, it is clear and has already been observed that $Ev(f, P_i) = Ev(Red(f), P_i)$ for all $1 \leq i \leq N$. Therefore for any $1 \leq i \leq s$ and $2 \leq u \leq t_i$, we have $R_{i,u} = R_{i,u-1}^q$, where $R_{i,u-1}^q$ denotes the N-tuple obtained from $R_{i,u-1}$ by raising each coordinate to q power. This shows that $C_1(s)$ is Galois closed (with respect to the subfield $\mathbb{F}_q$), which clearly implies that its dual $C_2(s)$ is also Galois closed.

Theorem 1. *With the notation above, $C(s)$ is an $\mathbb{F}_q$-linear code of length N and dimension $N - \dim_{\mathbb{F}_{q^n}} V(s)$.*

i. If $0 \in \{P_1, P_2, \ldots, P_N\}$, let d^* be the largest positive integer such that $\{0, 1, \ldots, d^* - 1\} \subseteq \bigcup_{i=1}^{s} Orbit(\ell_i)$.

ii. If $0 \notin \{P_1, P_2, \ldots, P_N\}$, let d^* be the largest positive integer such that there exists $j \in \bigcup_{i=1}^{s} Orbit(\ell_i)$ with $\{j, j+1, \ldots, j + d^* - 1\} \subseteq \bigcup_{i=1}^{s} Orbit(\ell_i)$.

Then the minimum distance $d(C(s))$ is at least $d^* + 1$.

Proof. Since the evaluation map (3) is injective, we have $\dim_{\mathbb{F}_{q^n}}(C_2(s)) = N - \dim_{\mathbb{F}_{q^n}} V(s)$. Since $C_2(s)$ is Galois closed, [7, Lemma 1] yields $\dim_{\mathbb{F}_q} C(s) = \dim_{\mathbb{F}_{q^n}}(C_2(s)) = N - \dim_{\mathbb{F}_{q^n}} V(s)$. Moreover, $d(C(s)) = d(C_2(s))$ by [7, Corollary 1].

Assume on the contrary that $d(C_2(s)) \leq d^*$. Then there exist d^* distinct columns of M that are linearly dependent over $\mathbb{F}_{q^n}$. Let $\beta_1, \beta_2, \ldots, \beta_{d^*}$ be distinct points in $\{P_1, P_2, \ldots, P_N\}$ corresponding to these linearly dependent columns of M. If $0 \in \{P_1, P_2, \ldots, P_N\}$, then consider the submatrix of M corresponding to the rows which are indexed by monomials whose powers are $0, 1, \ldots, d^* - 1$. This gives a $d^* \times d^*$ Vandermonde type submatrix

$$M^{(1)} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \beta_1 & \beta_2 & \ldots & \beta_{d^*} \\ \vdots & \vdots & & \vdots \\ \beta_1^{d^*-1} & \beta_2^{d^*-1} & \ldots & \beta_{d^*}^{d^*-1} \end{pmatrix}$$

of M. Since $\beta_1, \beta_2, \ldots, \beta_{d^*}$ are distinct points, even if $\beta_i = 0$ for some i, $M^{(1)}$ is invertible. This is a contradiction to our assumption.

If $0 \notin \{P_1, P_2, \ldots, P_N\}$, then consider the following $d^* \times d^*$ submatrix of M:

$$M^{(2)} = \begin{pmatrix} \beta_1^j & \beta_2^j & \ldots & \beta_{d^*}^j \\ \beta_1^{j+1} & \beta_2^{j+1} & \ldots & \beta_{d^*}^{j+1} \\ \vdots & \vdots & & \vdots \\ \beta_1^{j+d^*-1} & \beta_2^{j+d^*-1} & \ldots & \beta_{d^*}^{j+d^*-1} \end{pmatrix}.$$

Since $0 \notin \{P_1, P_2, \ldots, P_N\}$, all of $\beta_1, \beta_2, \ldots, \beta_{d^*}$ are distinct and nonzero. So we can divide the columns of $M^{(2)}$ by $\beta_1^j, \beta_2^j, \ldots, \beta_{d^*}^j$, respectively, without changing its rank. This is nothing but the matrix $M^{(1)}$, which completes the proof. □

Remark 2. In [4], the authors consider a square finite field $\mathbb{F}_q$ with $q = r^2$ and a special choice for $\Lambda(X)$, namely the trace polynomial from $\mathbb{F}_{q^n} = \mathbb{F}_{r^{2n}}$ to $\mathbb{F}_r$:

$$\Lambda(X) = \mathrm{Tr}(X) = X + X^r + X^{r^2} + \cdots + X^{r^{2n-1}}$$

Hence, the monomials in $V(s)$ are considered modulo $\mathrm{Tr}(X)$. In this case the length of the evaluation code $C_1(s)$ is $N = \deg \mathrm{Tr}(X) = r^{2n-1}$. Moreover, the points $\{P_1, \ldots, P_N\}$ of evaluation are the roots of the trace polynomial. Since $0 \in \{P_1, \ldots, P_N\}$ in this case, part (i) of Theorem 1 applies for $C(s) = C_2(s)_{|_{\mathbb{F}_{r^2}}}$. Since the coset leaders of orbits are minimally chosen, every element from $0 = \ell_1$ up to $\ell_{s+1} - 1$ are contained in $\bigcup_{i=1}^{s} Orbit(\ell_i)$. Hence, $d^* = \ell_{s+1}$.

For the dimension of $C(s)$, which is $N - \dim_{\mathbb{F}_{q^n}}(V(s))$, [4, Theorem 13] implies the following lower bound:

$$\dim(C(s)) \geq N - \sum_{i=1}^{s} t_i. \tag{5}$$

4 Lengthening of Restricted Evaluation Codes: A New Construction

We continue with the notation in Section 3. Let $1 \leq s \leq m$. We consider two cases.

Case 1. Assume that $0 \in \{P_1, P_2, \ldots, P_N\}$ and let d^* be the largest positive integer such that $\{0, 1, \ldots, d^* - 1\} \subseteq \bigcup_{u=1}^{s} Orbit(\ell_u)$. Moreover, assume that $\{0, 1, \ldots, d^* - 2\} \cap Orbit(d^* - 1) = \emptyset$ and let $1 \leq i^* \leq s$ be the integer such that $d^* - 1 \in Orbit(\ell_{i^*})$.

Note that by the minimality of orbit leaders, we have $\ell_{i^*} = d^* - 1$. Let us denote the cardinality of $Orbit(\ell_{i^*})$ by t_{i^*}. Consistent with earlier notation, we have

$$\begin{aligned} \ell_{i^*,1} &= d^* - 1 \\ \ell_{i^*,2} &= q\ell_{i^*,1} \pmod{(q^n - 1)} \\ &\vdots \\ \ell_{i^*,t_{i^*}} &= q\ell_{i^*,t_{i^*}-1} \pmod{(q^n - 1)}. \end{aligned}$$

We lengthen the rows defined in (4) as follows. For $j \in \{1, \ldots, s\} \setminus \{i^*\}$ and $u \in \{1, \ldots, t_j\}$, we set

$$\hat{R}_{j,u} = \left[R_{j,u}\ 0 \right], \tag{6}$$

and define the $t_j \times (N+1)$ matrix $\hat{M}_j$ as

$$\hat{M}_j = \begin{bmatrix} \hat{R}_{j,1} \\ \hat{R}_{j,2} \\ \vdots \\ \hat{R}_{j,t_j} \end{bmatrix}. \tag{7}$$

Let ϵ be a nonzero element in $\mathbb{F}_{q^n}$ and for $1 \leq u \leq t_{i^*}$, let $\hat{R}_{i^*,u}$ be the row of length $N+1$ defined as

$$\hat{R}_{i^*,u} = \left[R_{i^*,u}\ \epsilon^{q^{u-1}} \right].$$

Similarly, define the $t_{i^*} \times (N+1)$ matrix $\hat{M}_{i^*}$ as

$$\hat{M}_{i^*} = \begin{bmatrix} \hat{R}_{i^*,1} \\ \hat{R}_{i^*,2} \\ \vdots \\ \hat{R}_{i^*,t_{i^*}} \end{bmatrix} \tag{8}$$

and set

$$\hat{M} = \begin{bmatrix} \hat{M}_1 \\ \hat{M}_2 \\ \vdots \\ \hat{M}_s \end{bmatrix}, \tag{9}$$

which is a $(t_1 + t_2 + \ldots + t_s) \times (N+1)$ matrix over $\mathbb{F}_{q^n}$.

Let $\hat{C}_1(s)$ be the linear code over $\mathbb{F}_{q^n}$ of length $N+1$ spanned by the rows of $\hat{M}$ (9) and let $\hat{C}_2(s) = \hat{C}_1(s)^{\perp}$ as before. Define the code $\hat{C}(s)$ as the subfield subcode of $\hat{C}_2(s)$ over $\mathbb{F}_q$, which is $\hat{C}(s) = \hat{C}_2(s)_{|_{\mathbb{F}_q}} := \hat{C}_2(s) \cap \mathbb{F}_q^{N+1}$. By construction of $\hat{M}$, $\hat{C}_1(s)$ and hence $\hat{C}_2(s)$ are both Galois closed. Therefore, the dimension and the minimum distances of $\hat{C}(s)$ and $\hat{C}_2(s)$ are equal.

Note that by the following elementary row operations, we can transform $\hat{M}_{i^*}$ to

$$\hat{\mathcal{M}}_{i^*} = \begin{bmatrix} R_{i^*,1} & \epsilon \\ R_{i^*,2} - \epsilon^{q-1} R_{i^*,1} & 0 \\ \vdots & \vdots \\ R_{i^*,t_{i^*}} - \epsilon^{q^{t_{i^*}-1}-1} R_{i^*,1} & 0 \end{bmatrix}.$$

Hence, $\hat{C}_1(s)$ can also be spanned by the rows of the matrix

$$\hat{\mathcal{M}} = \begin{bmatrix} \hat{M}_1 \\ \vdots \\ \hat{\mathcal{M}}_{i^*} \\ \vdots \\ \hat{M}_s \end{bmatrix}, \tag{10}$$

for which all rows, except the one corresponding to $\ell_{i^*,1} = d^* - 1$ have zero in the last entry.

Case 2. Assume that $0 \notin \{P_1, P_2, \ldots, P_N\}$ and let d^* be the largest positive integer such that there exists j with $\{j, j+1, \ldots, j+d^*-1\} \subseteq \bigcup_{u=1}^{s} Orbit(\ell_u)$. Moreover, assume that $\{j, j+1, \ldots, j+d^*-2\} \cap Orbit(j+d^*-1) = \emptyset$ and let $1 \leq i^* \leq s$ be the integer such that $j + d^* - 1 \in Orbit(\ell_{i^*})$. Note that in this case ℓ_{i^*} is not necessarily equal to $j + d^* - 1$. Assume that $j + d^* - 1 = q^{\mu-1}\ell_{i^*} \mod (q^n - 1)$, for some $\mu \geq 1$.

Let

$$\begin{aligned}
\ell_{i^*,1} &= \ell_{i^*} \\
\ell_{i^*,2} &= q\ell_{i^*,1} \ (\mathrm{mod}(q^n-1)) \\
&\vdots \\
\ell_{i^*,\mu} &= q\ell_{i^*,\mu-1} = q^{\mu-1}\ell_{i^*,1} = j + d^* - 1 \ (\mathrm{mod}(q^n-1)) \\
&\vdots \\
\ell_{i^*,t_{i^*}} &= q\ell_{i^*,t_{i^*}-1} \ (\mathrm{mod}(q^n-1)).
\end{aligned}$$

For each $j \in \{1, \ldots, s\} \setminus \{i^*\}$ and all $1 \leq u \leq t_j$, define the rows $\hat{R}_{j,u}$ as in (6) and the matrix $\hat{M}_j$ as in (7) by listing the rows $\hat{R}_{j,u}$ for $1 \leq u \leq t_j$. Since t_{i^*} divides n, $\mathbb{F}_{q^{t_{i^*}}}$ is a subfield of $\mathbb{F}_{q^n}$. Let ϵ be a nonzero element in $\mathbb{F}_{q^{t_{i^*}}}$ this

time, and set $\delta := \epsilon^{q^{\mu-1}}$. Define lengthened rows $\hat{R}_{i^*,u}$, for $1 \le u \le t_{i^*}$, as

$$\hat{R}_{i^*,u} = \left[R_{i^*,u} \; \epsilon^{q^{u-1}} \right],$$

and note that if we set $r := t_{i^*} - \mu$, we can also write

$$\hat{R}_{i^*,u} = \left[R_{i^*,u} \; \delta^{q^{r+u}} \right],$$

for all $1 \le u \le t_{i^*}$. Form the $t_{i^*} \times (N+1)$ matrix $\hat{M}_{i^*}$ as in (8) using the $\hat{R}_{i^*,u}$'s defined as above and form the $(t_1 + \cdots + t_s) \times (N+1)$ matrix $\hat{M}$ using the blocks $\hat{M}_1, \ldots, \hat{M}_s$ as before.

Let $\hat{C}_1(s)$ denote the $\mathbb{F}_{q^n}$-linear code of length $N+1$ generated by the rows of $\hat{M}$. Define $\hat{C}_2(s)$ and $\hat{C}(s)$ similarly to Case 1. Note that $\hat{C}_1(s)$ is $\mathbb{F}_q$-Galois closed.

Via the following elementary row operations, $\hat{M}_{i^*}$ can be transformed to

$$\hat{\mathcal{M}}_{i^*} = \begin{bmatrix} R_{i^*,1} - \delta^{q^{r+1}-1} R_{i^*,\mu} & 0 \\ R_{i^*,2} - \delta^{q^{r+2}-1} R_{i^*,\mu} & 0 \\ \vdots & \vdots \\ R_{i^*,\mu} & \delta \\ \vdots & \vdots \\ R_{i^*,t_{i^*}} - \delta^{q^{r+t_{i^*}}-1} R_{i^*,\mu} & 0 \end{bmatrix}.$$

Hence, as in Case 1, both the matrix $\hat{M}$ and the transformed matrix $\hat{\mathcal{M}}$, which is obtained by replacing the block $\hat{M}_{i^*}$ by $\hat{\mathcal{M}}_{i^*}$, generate the same code $\hat{C}_1(s)$. Observe that this time, the only row with a nonzero last entry (namely, δ) in $\hat{\mathcal{M}}$ is $\hat{R}_{i^*,\mu}$, which corresponds to the evaluation of the monomial with power $j + d^* - 1$.

Theorem 2. *Consider the code $\hat{C}(s)$, which is obtained from the lengthening of a restricted evaluation code and its dual, as described in this Section.*

In the Case 1, define the subspace $\hat{V}(s)$ in $\mathbb{F}_{q^n}[X]/\langle \Lambda(X) \rangle$ as

$$\hat{V}(s) = Span_{\mathbb{F}_{q^n}} \Big\{ \{Red(X^i) : i \in \cup_{j=1, j \neq i^*}^{s} Orbit(\ell_j)\} \bigcup \{Red(X^{\ell_{i^*,u}} - \epsilon^{q^{u-1}-1} X^{\ell_{i^*,1}}) : 2 \le u \le t_{i^*}\} \Big\}.$$

In the Case 2, define $\hat{V}(s)$ as

$$\hat{V}(s) = Span_{\mathbb{F}_{q^n}} \Big\{ \{Red(X^i) : i \in \cup_{j=1, j \neq i^*}^{s} Orbit(\ell_j)\} \bigcup \{Red(X^{\ell_{i^*,u}} - \delta^{q^{r+u}-1} X^{\ell_{i^*,\mu}}) : 1 \le u \le t_{i^*}, u \neq \mu\} \Big\}.$$

Then $\hat{C}(s)$ is an $\mathbb{F}_q$-linear code of length $N+1$ and dimension $N - \dim_{\mathbb{F}_{q^n}} \hat{V}(s)$. Moreover its minimum distance $d(\hat{C}(s))$ is at least $d^* + 1$.

Proof. We only prove the first case. The proof in the second case follows from similar arguments.

Since $\hat{C}_1(s)$ is $\mathbb{F}_q$-Galois closed, we have $\dim_{\mathbb{F}_q} \hat{C}(s) = N+1-dim_{\mathbb{F}_{q^n}} \hat{C}_1(s)$ and $d(\hat{C}(s)) = d(\hat{C}_2(s))$. Revise the evaluation map (3) to $\hat{Ev}$ by appending 0 at the end of the image $Ev(Red(f))$ of every element $Red(f) \in \mathbb{F}_{q^n}[X]/\langle \Lambda(X) \rangle$ so that it takes values in $\mathbb{F}_{q^n}^{N+1}$. It is clear that $\hat{Ev}$ is also $\mathbb{F}_{q^n}$-linear and injective. Moreover, the dimension of $\hat{Ev}(\hat{V}(s))$ is nothing but the rank of the matrix which is obtained from $\hat{\mathcal{M}}$ in (10) by removing the only row (corresponding to $\ell_{i^*,1} = d^* - 1$) that has a nonzero element in its last entry. Therefore the rank of $\hat{M}$ (or $\hat{\mathcal{M}}$) is $1 + \dim_{\mathbb{F}_{q^n}} \hat{V}(s)$. Hence the dimension of $\hat{C}(s)$ over $\mathbb{F}_q$ is $(N+1) - (1 + \dim_{\mathbb{F}_{q^n}} \hat{V}(s)) = N - \dim_{\mathbb{F}_{q^n}} \hat{V}(s)$.

Assume on the contrary that $d(\hat{C}_2(s)) \leq d^*$. So there exist d^* columns of $\hat{M}$ which are linearly dependent over $\mathbb{F}_{q^n}$. Assume first that these columns are among the first N columns. Then using the same argument as in the proof of Theorem 1, we reach a contradiction. Assume next that these columns include the last, $(N+1)^{st}$, column. Then we have $d^* - 1$ distinct elements $\beta_1, \beta_2, \ldots, \beta_{d^*-1}$ in the set $\{P_1, \ldots, P_N\}$ corresponding to the dependent columns aside from the last one. Consider the following $d^* \times d^*$ submatrix of $\hat{M}$

$$\hat{M}^{(1)} = \begin{pmatrix} 1 & 1 & \ldots 1 & 0 \\ \beta_1 & \beta_2 & \ldots \beta_{d^*-1} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \beta_1^{d^*-2} & \beta_2^{d^*-2} & \ldots \beta_{d^*-1}^{d^*-2} & 0 \\ \beta_1^{d^*-1} & \beta_2^{d^*-1} & \ldots \beta_{d^*-1}^{d^*-1} & \epsilon \end{pmatrix},$$

whose rows correspond to the monomials with powers $0, 1, \ldots, d^* - 1$. As $\epsilon \neq 0$, $\hat{M}^{(1)}$ is invertible if and only if the Vandermonde $(d^* - 1) \times (d^* - 1)$ submatrix

$$\hat{M}^{(2)} = \begin{pmatrix} 1 & 1 & \ldots 1 \\ \beta_1 & \beta_2 & \ldots \beta_{d^*-1} \\ \vdots & \vdots & \vdots \\ \beta_1^{d^*-2} & \beta_2^{d^*-2} & \ldots \beta_{d^*-1}^{d^*-2} \end{pmatrix}$$

is invertible, which is the case. So we reach a contradiction and the proof is completed. □

Example 1. We let $\Lambda(X)$ be the trace map from $\mathbb{F}_{2^8}$ to $\mathbb{F}_2$ and consider $\mathbb{F}_4$-orbits (cyclotomic cosets) of elements for construction of $\hat{V}(s)$. Hence, we study length 129 linear codes $\hat{C}(s)$ over $\mathbb{F}_4$ (cf. Theorem 2) for various s values. With the help of Magma ([1]), we obtain four new quaternary codes of length 129 for the code tables [5]. Moreover, shortening of the new $[129, 42, 43]_4$ and $[129, 41, 44]_4$ codes yield further codes that improve the entries in [5]. These linear codes are presented in Table 1.

We give brief detail for the first entry in the table. Here, $s = 11$ and the dimension of the code $\hat{C}(11)$ is 90. Corresponding orbit leaders are

$$\ell_1 = 0, \ell_2 = 1, \ell_3 = 2, \ell_4 = 3, \ell_5 = 5, \ell_6 = 6, \ell_7 = 7,$$

$$\ell_8 = 9, \ell_9 = 10, \ell_{10} = 11, \ell_{11} = 13 = d^* - 1.$$

Hence the BCH bound (Theorem 2) yields $d(\hat{C}(11)) \geq 15$.

Example 2. Let $\mathrm{Tr}_{8/2}$ denote the trace map from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^2}$ and consider

$$\Lambda(X) = \frac{X^{256} - X}{\mathrm{Tr}_{8/2}(X)}.$$

In other words, the evaluation points for our codes are the nonzeros of $\mathrm{Tr}_{8/2}(X)$. We consider $\mathbb{F}_4$-orbits (cyclotomic cosets) of elements for construction of $\hat{V}(s)$ in Theorem 2. Hence, we study length 193 linear codes $\hat{C}(s)$ over $\mathbb{F}_4$ for various s values and obtain two new entries for the code tables [5]. Parameters of these two codes are also are presented in Table 1.

Remark 3. We note that the actual minimum distances of the codes presented in Table 1 may be larger than what is guaranteed by the BCH-type bound, which is already good enough to lead to improvements in [5]. We point this out by denoting the minimum distances with $\geq$ sign.

Table 1. Record-breaking Linear Codes over $\mathbb{F}_4$

s	ℓ_s	Lengthened Codes	Shortened Codes
11	13	$[129, 90, \geq 15]$	
15	18	$[129, 80, \geq 20]$	
31	41	$[129, 42, \geq 43]$	$[128, 41, \geq 43], [127, 40, \geq 43], [126, 39, \geq 43], [125, 38, \geq 43], [124, 37, \geq 43]$
32	42	$[129, 41, \geq 44]$	$[128, 40, \geq 44], [127, 39, \geq 44], [126, 38, \geq 44], [125, 37, \geq 44]$
15	18	$[193, 139, \geq 20]$	
17	21	$[193, 131, \geq 23]$	

Remark 4. As noted throughout the paper and shown by examples, our approach brings flexibility in choosing the polynomial $\Lambda(X)$ compared to [4]. Moreover, the new lengthening idea for restricted evaluation codes also makes finding further good codes possible. Hence, a future research can be carried out to find further record-breaking linear codes with these techniques. Moreover, one can study applications of the resulting codes for construction of good quantum error correcting codes.

References

1. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265 (1997).
2. Galindo, C., Geil, O., Hernando, F., Ruano, D.: On the distance of stabilizer quantum codes from J -affine variety codes. Quantum Inf. Process. **16**, 111 (2017).

3. Galindo, C., Hernando, F., Ruano, D.: Stabilizer quantum codes from J -affine variety codes and a new Steane-like enlargement. Quantum Inf. Process. **14**, 3211-3231 (2015).
4. Galindo, C., Hernando, F., Ruano, D.: Classical and quantum evaluation codes at the trace roots. IEEE Trans. Inform. Theory **65**, 2593-2602 (2019).
5. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de. Last accessed 18 November 2021.
6. Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, (2003).
7. Stichtenoth, H.: On the dimension of subfield subcodes. IEEE Trans. Inform. Theory **36**, 90-93 (1990).