Twisted Tensor Product Codes

Anton Betten

August 5, 2007

Abstract

We present two families of constacyclic linear codes with large automorphism groups. The codes are obtained from the twisted tensor product construction.

AMS subject classification: 05E20, 05B25, 11T71, 94B25, 94B27, 51E22, 51E20, 20G40, 14L35

1 Introduction and Statement of Results

Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$. Let $\mathrm{PG}(n, q) = \mathbf{P}(\mathbb{F}_q^{n+1})$ be the n-dimensional projective space over the field $\mathbb{F}_q$. The elements of $\mathrm{PG}(n, q)$ are written as $\mathbf{P}(x_0, \ldots, x_n)$ where $(x_0, \ldots, x_n)$ is a non-zero element of $\mathbb{F}_q^{n+1}$. We have that $\mathbf{P}(x_0, \ldots, x_n) = \mathbf{P}(y_0, \ldots, y_n)$ whenever there exists $\lambda \in \mathbb{F}_q^\times$ such that $y_i = \lambda x_i$ for $i = 0, 1, \ldots, n$. The number of points of $\mathrm{PG}(n, q)$ is $\theta_n(q) = (q^{n+1} - 1)/(q - 1)$. The automorphisms (or collineations) of $\mathrm{PG}(n, q)$ are the bijective mappings from $\mathbb{F}_q^{n+1}$ to itself that take points to points in such a way that inclusions between subspaces are preserved.

If $q = r^h$, the field $\mathbb{F}_r$ is a subfield of $\mathbb{F}_q$ (of index h). Denote by $\phi_h : x \mapsto x^r$ the Frobenius automorphism of $\mathbb{F}_q$ which fixes $\mathbb{F}_r$. Let T_h and N_h be the trace and norm maps from $\mathbb{F}_q$ to $\mathbb{F}_r$, respectively. The trace map is $\mathbb{F}_r$-linear and additive, the norm map is e-to-1 from $\mathbb{F}_q^\times$ onto $\mathbb{F}_r^\times$, where $e = (q-1)/(r-1)$. A primitive element for $\mathbb{F}_q$ is a generator of the multiplicative group $\mathbb{F}_q^\times$. It always exists. If β is a primitive element for $\mathbb{F}_q$ then β^e is a primitive element for the subfield $\mathbb{F}_r$.

Any invertible linear map of $\mathbb{F}_q^{n+1}$ induces a collineation of the projective space $\mathbf{P}(\mathbb{F}_q^{n+1}) = \mathrm{PG}(n,q)$. The group of all such maps is denoted as $\mathrm{PGL}(n+1,q)$. The order of $\mathrm{PGL}(n,q)$ is

$$q^{\frac{n(n-1)}{2}}\prod_{i=2}^{n}(q^i-1).$$

If bases have been chosen, a linear map can be represented by an $(n+1)\times(n+1)$ matrix. Non-zero scalar multiples of the same linear map induce the same map of projective space. We often ignore this ambiguity and simply speak of the matrix associated to the collineation. The identity collineation is represented by I_{n+1}, the $(n+1)\times(n+1)$ identity matrix. If $m(x) = x^{n+1}+c_nx^n+\ldots+c_1x+c_0 \in \mathbb{F}_q[x]$ and if $c=(c_1,\ldots,c_n)$, then

$$T_m := \left(\begin{array}{c|c} \mathbf{0}_n & -c_0 \\ \hline I_n & -c^\top \end{array}\right) \tag{1}$$

is a matrix whose characteristic polynomial is $m(x)$ (here, $\mathbf{0}_n$ is the all-zero vector of length n). This matrix describes a collineation of $\mathrm{PG}(n,q)$ if and only if $c_0 \neq 0$. The Frobenius automorphism ϕ_h induces the collineation

$$\mathbf{P}(x_0,\ldots,x_n) \;\mapsto\; \mathbf{P}(\phi_h(x_0),\ldots,\phi_h(x_n)).$$

Let $\Gamma_h = \langle\phi_h\rangle$ and $\mathrm{P}\Gamma_h\mathrm{L}(n+1,q) = \mathrm{PGL}(n+1,q)\ltimes\Gamma_h$. The order of $\mathrm{P}\Gamma_h\mathrm{L}(n,q)$ is

$$hq^{\frac{n(n-1)}{2}}\prod_{i=2}^{n}(q^i-1).$$

If $q=p^e$ for some prime p, the group $\mathrm{P}\Gamma\mathrm{L}(n+1,q) = \mathrm{P}\Gamma_e\mathrm{L}(n+1,q)$ is known as the projective semilinear group. $\mathrm{P}\Gamma_h\mathrm{L}(n+1,q)$ is a subgroup of $\mathrm{P}\Gamma\mathrm{L}(n+1,q)$ of index e/h. It is well-known that for $n \geq 2$, the group of automorphisms of $\mathrm{PG}(n,q)$ is $\mathrm{P}\Gamma\mathrm{L}(n+1,q)$. The automorphism group of the projective line $\mathrm{PG}(1,q)$ is defined to be $\mathrm{P}\Gamma\mathrm{L}(2,q)$. Often, the points of $\mathrm{PG}(1,q)$ are identified with the elements of $\mathbb{F}_q$ together with the element ∞, in such a way that $t \leftrightarrow \mathbf{P}(t,1)$ and $\infty \leftrightarrow \mathbf{P}(1,0)$. Under the usual rules for computing with ∞, the element

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{PGL}(2,q)$$

induces the transformation

$$\varphi_{a,b,c,d}:\ t \mapsto \frac{at+c}{bt+d}$$

of $\mathrm{PG}(1,q)$. Also, the Frobenius automorphism ϕ_e of $\mathbb{F}_q$ induces the map (which we have agreed to call automorphism) $t \mapsto \phi_e(t)$ of the projective line $\mathrm{PG}(1,q)$ under the identification $t \leftrightarrow \mathbf{P}(t,1)$. This map fixes ∞. The group $\mathrm{PGL}(2,q)$ acts sharply 3-transitive on the points of $\mathrm{PG}(1,q)$. That is, for any three (distinct) points t_1, t_2, t_3, there is a unique group element which takes $0, 1, \infty$ to t_1, t_2, t_3, respectively.

A *linear code* over $\mathbb{F}_q$ of length n, dimension k and minimum distance $\geq d$ is denoted as $[n, k, \geq d]_q$. A linear code $\mathcal{C}$ is given by means of a *generator matrix.* This is a matrix over $\mathbb{F}_q$ whose k rows (of length n) contain a basis of the code. A *check matrix* is a matrix over $\mathbb{F}_q$ whose $n-k$ rows (also of length n) contain a basis of the dual code $\mathcal{C}^\perp$, which is the subspace of $\mathbb{F}_q^n$ of all vectors which are orthogonal to all vectors of $\mathcal{C}$ (using the standard bilinear form $\sum_{i=1}^n x_i y_i$). It is a well known fact (see, for instance [4] 1.3.10) that a linear code has minimum distance at least d if any $d-1$ columns of the check matrix are independent (as vectors in $\mathbb{F}_q^{n-k}$). The parity extension of a code $\mathcal{C}$ is the code $\mathcal{C}^+$ whose codewords are $(c_1, \ldots, c_n, c_{n+1})$ where $(c_1, \ldots, c_n) \in \mathcal{C}$ and $c_{n+1} = -\sum_{i=1}^n c_i$. If $\mathcal{C}$ is an $[n, k, d]$ code then $\mathcal{C}^+$ is an $[n+1, k, d']$ code where $d' = d+1$ if d is odd and $d' = d$ otherwise. Another construction is as follows. Let $\mathcal{C}^\perp$ be the dual of an $[n, k, d]$ code $\mathcal{C}$. The code $\mathcal{D}$ which is dual to $(\mathcal{C}^\perp)^+$ is said to be obtained from $\mathcal{C}$ by parity extending the dual code. It has length $n+1$, dimension $k+1$ and minimum distance at least $d-1$.

Let $H(n,q)$ be the space $\mathbb{F}_q^n$ equipped with the Hamming metric. Write $q = p^e$ for some prime p. The monomial group $M_n(q)$ is the group of all regular $n \times n$ matrices with exactly one nonzero entry in each row and each column. Let $P_n(q)$ be the subgroup of $M_n(q)$ consisting of all permutation matrices. Then $M_n(q) = \mathbb{F}_q^\times \wr \mathrm{Sym}_n$, with Sym_n the symmetric group of degree n. An element of $M_n(q)$ can be described as a pair (f, π) where $f : \{1, \ldots, n\} \to \mathbb{F}_q^\times$ is a mapping and π is an element of Sym_n. The semilinear monomial group $\Gamma M_n(q)$ is the group generated by $M_n(q)$ and Γ_e. The isometry group of $H(n,q)$ is $\Gamma M_n(q)$. The semilinear automorphism group of a code $\mathcal{C}$, denoted $\Gamma\mathrm{Aut}(C)$, is the stabilizer of $\mathcal{C}$ in $\Gamma M_n(q)$. The monomial automorphism group of $\mathcal{C}$ is $\mathrm{MAut}(\mathcal{C}) = \Gamma\mathrm{Aut}(\mathcal{C}) \cap M_n(q)$ and the permutation automorphism group of $\mathcal{C}$ is $\mathrm{PAut}(\mathcal{C}) = \Gamma\mathrm{Aut}(\mathcal{C}) \cap P_n(q)$. This is the notation of [15, p. 26]. Clearly,

$$\mathrm{PAut}(\mathcal{C}) \le \mathrm{MAut}(\mathcal{C}) \le \Gamma\mathrm{Aut}(\mathcal{C}).$$

We say that a code $\mathcal{C}$ is invariant under a group A if $A \le \Gamma\mathrm{Aut}(C)$.

Let $\sigma_n = (0, 1, \ldots, n-1)$ be an n-cycle in Sym_n. Let f_γ be the map from $\{0, \ldots, n-1\}$ to $\mathbb{F}_q^\times$ with

$$f_\gamma(i) = \begin{cases} \gamma & \text{if } i = n-1, \\ 1 & \text{otherwise.} \end{cases}$$

For $\gamma \neq 0$, let σ_γ be the element $(f_\gamma, \sigma_n) \in M_n(q)$. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called constacyclic (in the sense of [3]) if it is monomially equivalent to a code $\mathcal{D}$ with $\langle \sigma_\gamma \rangle \le \mathrm{MAut}(\mathcal{D})$. That is, the code $\mathcal{D}$ has the property that whenever $(c_0, c_1, \ldots, c_{n-1})$ is in $\mathcal{D}$ then $(\gamma c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is in $\mathcal{D}$ as well. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called cyclic if it is permutation equivalent to a code $\mathcal{D}$ with $\langle \sigma_n \rangle \le \mathrm{PAut}(\mathcal{D})$. That is, a constacyclic code is cyclic if the constant γ can be taken to be the unit element 1.

The purpose of this note is to prove the following two results:

Theorem 1 *For any prime power $q \ge 3$, there exist constacyclic $[q^2+1, q^2-8, \ge 6]_q$ codes. For any even prime power $q \ge 4$, there exist $[q^2+2, q^2-7, \ge 6]_q$ codes. In both case, the semilinear automorphism group of the codes is $\mathrm{P\Gamma L}(2, q^2)$, and $\mathrm{P\Gamma_2 L}(2, q^2)$ is a monomial automorphism group. Among these codes, only those of length q^2+1 for q even are cyclic. The codes of length q^2+2 are not the parity extensions in the dual of the corresponding codes of length q^2+1.*

Theorem 2 *For any prime power $q \ge 3$, there exist constacyclic $[q^3+1, q^3-7, \ge 5]_q$ codes. The semilinear automorphism group of the codes is $\mathrm{P\Gamma L}(2, q^3)$, and $\mathrm{P\Gamma_3 L}(2, q^3)$ is a monomial automorphism group. The codes are cyclic if and only if q is even.*

The following remarks are in order. For undefined terms like cyclotomic sets, see Section 2.

Remark 3 *There exist* $[q^2+1, q^2-8, \geq 6]_q$ *BCH-codes for* $q \geq 4$. *Since* $q^4-1 = (q^2+1)(q^2-1)$, *the field* $\mathbb{F}_{q^4}$ *contains all* $(q^2+1)^{\mathrm{th}}$ *roots of unity. Modulo* q^2+1, *the q-cyclotomic sets of* $0, 1$ *and* 2, *respectively, are*

$$\{0\}, \{1, q, -1, -q\}, \{2, 2q, -2, -2q\}.$$

Their union contains the consecutive set $-2, -1, 0, 1, 2$. *Therefore, the BCH-code generated by the corresponding roots has length* q^2+1, *dimension* q^2-8 *and minimum distance at least* 6. *Since BCH-codes are cyclic, the only possible equivalences between the codes of Theorem 1 and BCH-codes is when q is even and* $n = q^2+1$. *The examples in Section 6 will demonstrate, however, that the codes of length* 17 *and* 65 *of Theorem 1 are not BCH-codes.*

Remark 4 *There exist* $[q^3+1, 8, q(q^2-q-1)]_q$ *codes* $\mathcal{C}(q)$ *for any prime power q. The experimental data in Section 7 indicates that the duals of the codes of Theorem 2 may have exactly these parameters. The statement is true for* $q \leq 7$. *The* $[q^3+1, 8, q(q^2-q-1)]_q$ *codes arise from the X-construction of [22, 19] applied to a class of BCH-codes. In this particular case, the X-construction takes two codes* C_1 *and* C_2 *where* C_2 *is a subcode of* C_1. *The parameters of* C_1 *and* C_2 *are* $[n, k, d]$ *and* $[n, k-1, D]$ *for* $D > d$. *Using an auxiliary* $[1, 1, 1]_q$ *(trivial) code, a* $[n+1, k, d+1]$ *code is produced. Here, with* $n = q^3-1$, $k = 8$, *and* $s = q^3-q^2-q$, *we construct* $\mathcal{C}(q)$ *from* $\mathcal{C}_1(q)$ *and* $\mathcal{C}_2(q)$ *which are* $[n+1, k, s-1]$ *and* $[n+1, k-1, s]$ *codes (respectively). The codes* $\mathcal{C}_1(q)$ *and* $\mathcal{C}_2(q)$ *are constructed in turn using the X-construction applied to BCH-codes* $\mathcal{C}_3(q), \mathcal{C}_4(q), \mathcal{C}_5(q), \mathcal{C}_6(q)$, *with parameters* $[n, k, s-2]$, $[n, k-1, s-1]$, $[n, k-1, s-1]$, $[n, k-2, s]$ *(respectively). If* $A = \{0\}, B = \{1, q, q^2\}, C = \{q+1, q^2+q, q^2+1\}$ *and* $D = \{q^2+q+1\}$ *are q-cyclotomic sets modulo* q^3-1, *then the last four BCH-codes are constructed by using the sets*

$$A \cup B \cup C \cup D, \quad A \cup B \cup C, \quad B \cup C \cup D, \quad B \cup C$$

(resp.) as exponents of non-roots. The bound on the minimum distance in each of the four cases follows by considering the consecutive sets of roots whose exponents are

$$[0, q^2+q+1]', [0, q^2+q]', [1, q^2+q+1]', [1, q^2+q]',$$

where we use the convention that $[i, j]$ *denotes the interval* $\{i, i+1, \ldots, j\}$ *and where* $[i, j]'$ *denote the complement of* $[i, j]$ *in the set* $[0, n-1]$. *For more* *details on these codes, see [5, page 191]. The relationship between the codes $\mathcal{C}(q)$ and the duals of those of Theorem 2 has yet to be examined.*

Remark 5 *Danev and Olsson [8] have constructed $[q^2-q+1, q^2-q-6, 6]_q$ BCH-codes for $q \geq 4$.*

2 Some More Notions From Algebra And Geometry

Let $\mathcal{C}$ be a cyclic code. We can identify the elements of a cyclic code of length n over $\mathbb{F}_q$ with polynomials in the factor space $R_{n,q} := \mathbb{F}_q[x]/(x^n-1)$. Under this identification, the codeword $(c_0, \ldots, c_{n-1}) \in \mathcal{C}$ gets mapped to the polynomial $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ modulo $x^n - 1$. It is well-known that the cyclic codes of length n over $\mathbb{F}_q$ correspond one-to-one to the ideals in $R_{n,q}$. A cyclic code is uniquely described by its generator polynomial, which is the monic polynomial of least degree which generates $\mathcal{C}$ as ideal in $R_{n,q}$. If $g(x)$ is the generator polynomial of $\mathcal{C}$ then $g(x)$ divides x^n-1 and $\dim(\mathcal{C}) = k = n - \deg g(x)$. The zeros of $g(x)$ are n-th roots of unity over $\mathbb{F}_q$. The variety of the code, denoted $V(\mathcal{C})$, is the set of all zeros of $g(x)$ in some extension field.

A q-cyclotomic set modulo n is a set of integers modulo n of the form $\{q^i a \mid i \in \mathbb{Z}\}$. Let ξ be a primitive n-th root of unity over $\mathbb{F}_q$. If $\{a_1, \ldots, a_r\}$ is a q-cyclotomic set modulo n then

$$m_{a_1}(= m_{a_2} = \cdots = m_{a_r}) = \prod_{i=1}^{r}(x - \xi^{a_i})$$

is the minimum polynomial of ξ^{a_1} over $\mathbb{F}_q$. In particular, it is a polynomial in $\mathbb{F}_q[x]$, and no nonconstant polynomial in $\mathbb{F}_q[x]$ of smaller degree divides m_{a_1}.

If $\mathcal{C}$ is a cyclic code over $\mathbb{F}_q$ of length n with generator polynomial $g(x)$, the factorization of $g(x)$ over $\mathbb{F}_q$ corresponds to the unique way in which the variety of $\mathcal{C}$ can be written as disjoint subsets. Each irreducible factor of $g(x)$ contributes one set of n-th roots of unity, the exponents of which form one q-cyclotomic set.

The dual code of a cyclic code is cyclic with generator polynomial $\overleftarrow{h}(x)$, where $h(x) = (x^n - 1)/g(x)$ and $\overleftarrow{h}(x) = x^{\deg h(x)}h(x^{-1})$ is the reverse polynomial of $h(x)$.

Let $m(x)$ be a monic irreducible polynomial in $\mathbb{F}_q[x]$ of degree $d > 1$. The subexponent of $m(x)$ is the smallest positive integer $s = \mathrm{Subexp}(m)$ for which there exists an element $c \in \mathbb{F}_q$ such that $m(x)$ divides $x^s - c$ in $\mathbb{F}_q[x]$. The element c is known as the integral element of $m(x)$ (cf. [13, 14, 4]). The exponent of $m(x)$ is the smallest positive integer $e = \mathrm{Exp}(m)$ for which $m(x)$ divides $x^e - 1$ in $\mathbb{F}_q[x]$. If β is a root of $m(x)$ in some extension field $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$, the subexponent s is the order of $\beta\mathbb{F}_q^\times$ in the factor group $\mathbb{F}_{q^d}^\times/\mathbb{F}_q^\times$ and $\beta^s = c$, the integral element. In particular, we have that

$$\mathrm{Subexp}(m) = \frac{\mathrm{Exp}(m)}{\gcd(q-1, \mathrm{Exp}(m))}. \tag{2}$$

The polynomial $m(x)$ is primitive if $\mathrm{Exp}(m) = q^d - 1$. If β is a root of $m(x)$ in some extension field $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$, then $m(x)$ is primitive precisely if β is a primitive element of $\mathbb{F}_q$, i.e. a generator for the multiplicative group $\mathbb{F}_q^\times$. The polynomial $m(x)$ is subprimitive if $\mathrm{Subexp}(m) = \theta_{d-1}(q)$. Let $\mathcal{R}(d,q)$ be the set of monic subprimitive polynomials in $\mathbb{F}_q[x]$ and let $R(d,q) = |\mathcal{R}(d,q)|$ be their number. Subprimitive polynomials are important because of the following result due to Hirschfeld [13].

Lemma 6 *A linear collineation of* $\mathrm{PG}(n,q)$ *is cyclic (i.e., permutes the* $\theta_n(q)$ *points of* $\mathrm{PG}(n,q)$ *in one cycle) if and only if the characteristic polynomial of an associated matrix is subprimitive. The number* $R(d,q)$ *of subprimitive polynomials of degree* d *over* $\mathbb{F}_q$ *is*

$$R(d,q) = (q-1)\frac{\Phi(\theta_{d-1}(q))}{d},$$

where Φ *is Euler's totient function.*

Let $\mathcal{R}_c(d,q)$ be the set of subprimitive polynomials of degree d over $\mathbb{F}_q$ with integral element $c \in \mathbb{F}_q$. Let $R_c(d,q) = |\mathcal{R}_c(d,q)|$ be the number of those polynomials. The class of polynomials $\mathcal{R}_1(2,q)$ is of particular interest when analyzing whether or not a code is cyclic. Therefore we determine the values of the counting function $R_c(d,q)$.

Lemma 7 *Let α be a primitive element for the finite field $\mathbb{F}_q$. Let*

$$\theta_{d-1}(q) = \prod_{i=1}^{r} p_i^{e_i}$$

be the factorization of $\theta_{d-1}(q)$ into powers of distinct primes. Then

$$R_{\alpha^i}(d,q) = \begin{cases} \frac{1}{d}\Big(\prod_{\substack{j=1 \\ p_j \mid q-1}}^{r} p_j^{e_j} \Big) \cdot \Phi\Big(\prod_{\substack{j=1 \\ p_j \nmid q-1}}^{r} p_j^{e_j} \Big) & \textit{if } \gcd(i, q-1, \theta_{d-1}(q)) = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

The function $R_{\alpha^i}(d,q)$ is periodic in i with period $\gcd(q-1, \theta_{d-1}(q))$. *The non-zero function values depend only on d and q, but not on i. If $d = 2$, we have*

$$R_c(2,q) = \begin{cases} \frac{1}{2}\Phi(q+1) & \textit{for all } c \textit{ if } q \textit{ is even,} \\ \Phi(q+1) & \textit{if } q \textit{ is odd and } c \textit{ is a nonsquare in } \mathbb{F}_q, \\ 0 & \textit{if } q \textit{ is odd and } c \textit{ is a nonzero square in } \mathbb{F}_q. \end{cases}$$

In particular,

$$R_1(2,q) = \begin{cases} \frac{1}{2}\Phi(q+1) & \text{if } q \text{ is even,} \\ 0 & \text{if } q \text{ is odd.} \end{cases}$$

Proof. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and

$$\mathbb{Z}_n^\times = \{i \in \mathbb{Z}_n \mid \gcd(i,n) = 1\}.$$

Let β be a primitive element in $\mathbb{F}_{q^d}$. We may assume that $\alpha = \beta^{\theta_{d-1}(q)}$ is the primitive element of $\mathbb{F}_q$ mentioned in the statement. Define $g := \gcd(q-1, \theta_{d-1}(q))$. Let

$$S_{d,q} = \{i \in \mathbb{Z}_{q^d-1} \mid \gcd(i, \theta_{d-1}(q)) = 1\} \subseteq \mathbb{Z}_{q^d-1}$$

be the set of exponents of subprimitive elements in $\mathbb{F}_{q^d}$. From the properties of the gcd, it follows that $S_{d,q}$ is the union of all cosets

$$\mathbb{Z}_{\theta_{d-1}(q)}^\times + j\theta_{d-1}(q) = \{x + j\theta_{d-1}(q) \mid x \in \mathbb{Z}_{\theta_{d-1}(q)}^\times\}, \tag{3}$$

where the coset representatives j are chosen from $\mathbb{Z}_{q-1}$. Let

$$R_{i,n} = \{x \in \mathbb{Z} \mid x \equiv i \mod n\}$$

be the set of integers which are congruent to i mod n. The equation

$$\left(\beta^{k(q-1)+i}\right)^{\theta_{d-1}(q)} = \beta^{k(q-1)\theta_{d-1}(q)+i\theta_{d-1}(q)} = \left(\beta^{\theta_{d-1}(q)}\right)^i = \alpha^i,$$

shows that the power map

$$x \mapsto x^{\theta_{d-1}(q)}$$

is $\theta_{d-1}(q)$ to 1 from $\mathbb{F}_{q^d}^\times$ to $\mathbb{F}_q^\times$. The set of exponents of all preimages of α^i is

$$\{k(q-1)+i \mid k \in \mathbb{Z}_{\theta_{d-1}(q)}\} = R_{i,q-1} \cap \mathbb{Z}_{q^d-1},$$

which is a set of size $(q^d-1)/(q-1) = \theta_{d-1}(q)$.

Next, we determine the number of subprimitive elements in $\mathbb{F}_{q^d}$ with integral element α^i, which is the size of the set $S_{d,q} \cap R_{i,q-1}$. Let

$$O_i = \{i + k(q-1) \mid k \in \mathbb{Z}_{\theta_{d-1}(q)}\}$$

denote the orbit of i under the additive action of $(q-1)\mathbb{Z}$ on the set $\mathbb{Z}_{\theta_{d-1}(q)}$. Then

$$|O_i| = \frac{\theta_{d-1}(q)}{\gcd(q-1, \theta_{d-1}(q))} = \frac{\theta_{d-1}(q)}{g}. \tag{4}$$

Two orbits O_i and O_j coincide if and only if $i \equiv j \mod (q-1)/g$.

We claim that

$$|S_{d,q} \cap R_{i,q-1}| = g|\mathbb{Z}_{\theta_{d-1}(q)}^\times \cap O_i|, \quad i \in \mathbb{Z}_{q-1} \tag{5}$$

To see this, consider the mapping

$$\varphi : S_{d,q} \longrightarrow \mathbb{Z}_{\theta_{d-1}(q)}^\times,\ x \mapsto x \mod \theta_{d-1}(q).$$

Let $x \in S_{d,q} \cap R_{i,q-1}$, i.e. $x = k(q-1) + i$ for some integer k. Since $x \in S_{d,q}$, it follows from (3) that there is an element $h \in \mathbb{Z}_{\theta_{d-1}(q)}$ and some coset representative $j \in \mathbb{Z}_{q-1}$ such that $x = h + j\theta_{d-1}(q)$. That is,

$$k(q-1) + i = x = h + j\theta_{d-1}(q). \tag{6}$$

The first equation shows that $\varphi(x) \in O_i$, the second equation shows that $\varphi(x) \in \mathbb{Z}^\times_{\theta_{d-1}(q)}$. That is, φ is well-defined. It follows from (6) that $h - i \equiv 0 \mod g$. That is, $h - i = gm$ for some integer m. Also,

$$\begin{aligned} k(q-1)+i &\equiv h \mod \theta_{d-1}(q) \\ \iff k(q-1) &\equiv h-i \mod \theta_{d-1}(q) \\ \iff ka &\equiv m \mod b \end{aligned}$$

where a and b are integers such that $(q-1) = ga$ and $\theta_{d-1}(q) = gb$. Since $\gcd(a,b) = 1$, the last equation has a unique solution. Therefore, the equation $k(q-1) \equiv h - i \mod \theta_{d-1}(q)$ has exactly g solutions. This shows that φ is a g to 1 map from $S_{d,q} \cap R_{i,q-1}$ onto $\mathbb{Z}^\times_{\theta_{d-1}(q)} \cap O_i$. In particular, the size of the former set is g times the size of the latter set, which proves (5).

It remains to compute the size of the set $\mathbb{Z}^\times_{\theta_{d-1}(q)} \cap O_i$. For this, recall that $\theta_{d-1}(q) = \prod_{i=1}^r p_i^{e_i}$ and hence

$$x \in \mathbb{Z}^\times_{\theta_{d-1}(q)} \iff x_i \not\equiv 0 \mod p_i \quad \text{for } i = 1, \ldots, r.$$

Let us introduce some notation. For $x \in \mathbb{Z}$, let

$$Z_x = \{p_j \mid 1 \le j \le r,\ x \equiv 0 \mod p_j\},$$

and

$$N_x = \{p_j \mid 1 \le j \le r,\ x \not\equiv 0 \mod p_j\},$$

so that $N_x \cup Z_x = \{p_1, \ldots, p_r\}$. Observe that $\mathbb{Z}^\times_{\theta_{d-1}(q)} \cap O_i = \emptyset$ if $Z_i \cap Z_{q-1} \neq \emptyset$. Namely, if $p_j \in Z_i \cap Z_{q-1}$ then an arbitrary element $i + k(q-1) \in O_i$ satisfies $i + k(q-1) \equiv 0 \mod p_j$. The condition $Z_i \cap Z_{q-1} \neq \emptyset$ is equivalent to the condition $\gcd(i, q-1, \theta_{d-1}(q)) \neq 1$. Otherwise, the number of elements $x = i + k(q-1)$ for which $x \not\equiv 0 \mod p_j$ for all j can be computed as follows. First note that $p_j \in Z_{q-1}$ implies $p_j \notin Z_i$, i.e. $i + k(q-1) \equiv i \not\equiv 0 \mod p_j$ for all k. That is, the condition $x \in \mathbb{Z}^\times_{\theta_{d-1}(q)} \cap O_i$ reduces to $x \not\equiv 0 \mod p_j$ for all $p_j \in N_{q-1}$. Let A_j be the set of $x \in O_i$ with $x \equiv 0 \mod p_j$. For any subset I of N_{q-1}, let

$$A_I = \bigcap_{p_j \in N_{q-1}} A_j$$

with the convention that $A_\emptyset = O_i$. Notice that

$$|A_I| = \frac{|O_i|}{\prod_{p_j \in I} p_j} = \frac{\theta_{d-1}(q)}{g \prod_{p_j \in I} p_j},$$

using (4). Then

$$x \in \mathbb{Z}^{\times}_{\theta_{d-1}(q)} \cap O_i \iff x \notin A_j \text{ for all } p_j \in N_{q-1}.$$

The Principle of Inclusion and Exclusion implies that the number of elements in O_i which are in none of the A_i (but in $A_\emptyset$) equals

$$\begin{aligned}
& |\mathbb{Z}^{\times}_{\theta_{d-1}(q)} \cap O_i| \\
= & \sum_{I \subseteq N_{q-1}} (-1)^{|I|} |A_I| \\
= & \sum_{I \subseteq N_{q-1}} (-1)^{|I|} \frac{\theta_{d-1}(q)}{g \prod_{p_j \in I} p_j} \\
= & \frac{1}{g} \prod_{p_j \in Z_{q-1}} p_j^{e_j} \sum_{I \subseteq N_{q-1}} (-1)^{|I|} \frac{\prod_{p_j \in N_{q-1}} p_j^{e_j}}{\prod_{p_j \in I} p_j} \\
= & \frac{1}{g} \Big(\prod_{p_j \in Z_{q-1}} p_j^{e_j} \Big) \sum_{I \subseteq N_{q-1}} (-1)^{|I|} \Big(\prod_{p_j \in N_{q-1}} p_j^{e_j} \Big) \Big(\prod_{p_j \in N_{q-1}} \Big(1 - \frac{1}{p_j}\Big)\Big) \\
= & \frac{1}{g} \Big(\prod_{p_j \in Z_{q-1}} p_j^{e_j} \Big) \Phi \Big(\prod_{p_j \in N_{q-1}} p_j^{e_j} \Big).
\end{aligned}$$

In the last step we made use of the well-known formula

$$\Phi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big),$$

for any integer $n = \prod_{j=1}^{r} p_j^{e_j}$. From (5) it follows that

$$|S_{d,q} \cap R_{i,q-1}| = \begin{cases} 0 & \text{if} \gcd(i, q-1, \theta_{d-1}(q)) \neq 1 \\ \Big(\prod_{p_j \in Z_{q-1}} p_j^{e_j} \Big) \Phi \Big(\prod_{p_j \in N_{q-1}} p_j^{e_j} \Big) & \text{otherwise} \end{cases}$$

Since any polynomial in $\mathcal{R}_{\alpha^i}(d,q)$ corresponds to exactly d subprimitive elements we have proved that

$$|R_{\alpha^i}(d,q)| = \begin{cases} 0 & \text{if} \gcd(i, q-1, \theta_{d-1}(q)) \neq 1 \\ \frac{1}{d} \Big(\prod_{\substack{j=1 \\ p_j \mid q-1}}^{r} p_j^{e_j} \Big) \Phi \Big(\prod_{\substack{j=1 \\ p_j \nmid q-1}}^{r} p_j^{e_j} \Big) & \text{otherwise} \end{cases}$$

Consider now the case $d = 2$. Then $\theta_{d-1}(q) = q + 1$. We distinguish cases according to the parity of q. If q is even, then $\gcd(q-1, q+1) = 1$, which implies that the second clause always happens. Also, the first product is empty for the same reason. Thus $R_{\alpha^i}(2,q) = \frac{1}{2}\Phi(q+1)$. If q is odd, then $\gcd(q-1, q+1) = 2$. In particular, 2 is one of the prime factors of $q+1$ and we may assume than $p_1 = 2$. For i odd (i.e., for α^i a nonsquare in $\mathbb{F}_q$) we have

$$R_{\alpha^i}(2,q) = \frac{1}{2}2^{e_1}\Phi\big(\prod_{j=2}^{r} p_j^{e_j}\big) = \Phi\big(2^{e_1}\big)\Phi\big(\prod_{j=2}^{r} p_j^{e_j}\big) = \Phi(q+1).$$

For i even (i.e., for α^i a nonzero square in $\mathbb{F}_q$), we have $R_{\alpha^i}(2,q) = 0$. □

Example 8 *Tab. 1 displays the values of the counting function $R_c(d,q)$ for small d and q. The entry in the table shows the value of $R_c(d,q)$ for some c for which $R_c(d,q) \neq 0$. The period $\gcd(q-1, \theta_{d-1}(q))$ is indicated in the subscript.*

Remark 9 *The fact that each subprimitive polynomial in $\mathcal{R}(d,q)$ has exactly one integral element in $\mathbb{F}_q^\times$ allows for an independent check of Lemma 7 using Lemma 6. Namely, we can check whether $\sum_{c \in \mathbb{F}_q^\times} R_c(d,q) = R(d,q)$. Since $R_c(d,q)$ is periodic in the exponent i of $c = \alpha^i$ with period $g = \gcd(q-1, \theta_{d-1}(q))$ and since all nonzero values of $R_c(d,q)$ for fixed d and q are the same, we get the condition that*

$$\Phi(g)\frac{q-1}{g} \cdot \frac{1}{d}\Big(\prod_{p_j \mid q-1} p_j^{e_j}\Big)\Phi\Big(\prod_{p_j \nmid q-1} p_j^{e_j}\Big) = (q-1)\frac{\Phi\big(\prod_{p_j} p_j^{e_j}\big)}{d},$$

where as before we have $\theta_{d-1}(q) = \prod_{j=1}^{r} p_j^{e_j}$. This last condition is easily seen to hold true.

In $\mathrm{PG}(2,q)$, a regular oval is a nondegenerate conic, i.e. the zero set of a homogeneous polynomial in three variables, which cannot be transformed into a polynomial with fewer variables. It is a set of $q+1$ points, no three collinear. By a theorem of Qvist [21], if q is even, an oval determines a unique point called nucleus. When added to the oval, a set of $q+2$ points results which still has no three points collinear. Such a set is called a regular

$R_c(d,q)$	$d=2$	3	4	5	6	7
$q=2$	1_1	2_1	2_1	6_1	6_1	18_1
3	2_2	4_1	8_2	22_1	48_2	156_1
4	2_1	6_3	16_1	60_1	144_3	756_1
5	2_2	10_1	24_4	140_1	360_2	2790_1
7	4_2	18_3	80_2	560_1	3024_6	18928_1
8	3_1	24_1	72_1	900_1	3888_1	42336_7
9	4_2	24_1	160_4	1320_1	6912_2	85176_1
11	4_2	36_1	240_2	3220_5	15552_2	271908_1
13	6_2	60_3	384_4	6188_1	56160_6	747006_1
16	8_1	72_3	1024_1	12000_5	138240_3	2370816_1
17	6_2	102_1	672_4	17748_1	132192_2	3663738_1
19	8_2	126_3	1440_2	27300_1	296352_6	7084000_1
23	8_2	156_1	1664_2	58512_1	584064_2	21346864_1
25	12_2	180_3	3744_4	72800_1	1296000_6	34997760_1
27	12_2	252_1	3456_2	100320_1	1959552_2	57421728_1
29	8_2	264_1	3360_4	146508_1	1710720_2	88009572_7
31	16_2	330_3	6912_2	173500_5	3991680_6	131012448_1

Table 1: The function $R_c(d,q)$

hyperoval. It is known (see [14], Corollary 7.14, for example) that the automorphism group of the regular oval and the regular hyperoval is $\mathrm{P\Gamma L}(2,q)$. If $q > 4$, this group fixes the nucleus. The only cyclic automorphisms of the regular oval are the Singer-cycles. These arise from cyclic collineations of $\mathrm{PG}(1,q)$ as described by Lemma 6. Their associated matrix has a subprimitive characteristic polynomial. Conversely, any polynomial in $\mathcal{R}(2,q)$ gives rise to a collineation acting transitively on the regular oval in $\mathrm{PG}(2,q)$.

For elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ in a field, we denote the $k \times k$ Vandermonde matrix by

$$V_k(\alpha_1,\alpha_2,\ldots,\alpha_k) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_k^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_k^{k-1} \end{pmatrix}. \qquad (7)$$

3 The Twisted Tensor Product

Let $V = V_n$ be the n-dimensional vector space over a field F, with basis $a_1, a_2, \ldots, a_n$. The h-fold tensor product $\otimes_h V = V \otimes V \otimes \cdots \otimes V$ has a basis consisting of the elements

$$b_{i_1,i_2,\ldots,i_h} = a_{i_1} \otimes a_{i_2} \otimes \cdots \otimes a_{i_h} \tag{8}$$

for $i_1, i_2, \ldots, i_n \in \{1, \ldots, n\}$. From now on, let $F = \mathbb{F}_{q^h}$ be a finite field and let $V_n = \mathbb{F}_q^n$ be the n-dimensional vector space over F. Define a map

$$\iota_h : V_n \to \otimes_h V_n,\ x \mapsto x \otimes \phi_h(x) \otimes \phi_h^2(x) \otimes \cdots \otimes \phi_h^{h-1}(x). \tag{9}$$

The induced mapping between the corresponding projective spaces is denoted by the same symbol:

$$\iota_h : \mathbf{P}(V_n) \to \mathbf{P}(\otimes_h V_n) :\ \mathbf{P}(x) \mapsto \mathbf{P}(\iota_h(x)). \tag{10}$$

Example 10 *Let $V = V_3 = \mathbb{F}_{q^2}^3$, with basis a_1, a_2, a_3, and $x = (a, b, c) \in V$. We may choose bases*

$$\begin{aligned} &c_1 = b_{1,1},\ c_2 = b_{2,2},\ c_3 = b_{3,3}, \\ &c_4 = b_{1,2},\ c_5 = b_{2,1}, \\ &c_6 = b_{1,3},\ c_7 = b_{3,1}, \\ &c_8 = b_{2,3},\ c_9 = b_{3,2} \end{aligned}$$

for $\otimes_2 V$. Then ι_2 is the following mapping from $\mathrm{PG}(2, q^2)$ *to* $\mathrm{PG}(8, q^2)$:

$$\iota_2(\mathbf{P}(a, b, c)) = \mathbf{P}(a^{q+1}, b^{q+1}, c^{q+1}, ab^q, a^q b, ac^q, a^q c, bc^q, b^q c). \tag{11}$$

Example 11 *Consider the projective line* $\mathrm{PG}(1, q^3) = \mathcal{P}(V)$ *over the field $\mathbb{F}_{q^3}$. Let $V = V_2 = \mathbb{F}_{q^3}^2$, with basis a_1, a_2, and $x = (a, b) \in V$. We may choose bases*

$$\begin{aligned} &c_1 = b_{1,1,1},\ c_2 = b_{2,2,2}, \\ &c_3 = b_{1,1,2},\ c_4 = b_{1,2,1},\ c_5 = b_{2,1,1}, \\ &c_6 = b_{1,2,2},\ c_7 = b_{2,2,1},\ c_8 = b_{2,1,2} \end{aligned}$$

for $\otimes_3 V$. Then ι_3 is the following mapping from $\mathrm{PG}(1, q^3)$ *to* $\mathrm{PG}(7, q^3)$:

$$\begin{aligned} \iota_3(\mathbf{P}(a, b)) &= \mathbf{P}(a^{q^2+q+1}, b^{q^2+q+1}, a^{q^2+q} b, a^{q^2+1} b^q, & (12) \\ &\qquad a^{q+1} b^{q^2}, a^{q^2} b^{q+1}, ab^{q^2+q}, a^q b^{q^2+1}). & (13) \end{aligned}$$

As a general reference for twisted tensor products, see [23] or [2]. More recently, the twisted tensor product has been considered in [7] and in connection with the study of large arcs [10].

4 Proof of Theorem 1

Proof. (of Theorem 1) Let $V = V_3 = \mathbb{F}_{q^2}^3$ with basis a_1, a_2, a_3. Let $\mathcal{O}$ be a regular oval in $\mathrm{PG}(2, q^2) = \mathbf{P}(V_3)$, i.e. a nondegenerate conic. Up to projective equivalence, we may assume that $\mathcal{O}$ consists of the points

$$\mathcal{O} = \{\mathbf{P}(1, t, t^2) \mid t \in \mathbb{F}_{q^2}\} \cup \{\mathbf{P}(0, 0, 1)\}.$$

Consider the image of the regular oval $\mathcal{O}$ as defined above under the mapping ι_2 as defined in Example 10. Put

$$m_t := \iota_2(1, t, t^2) = (1, t^{q+1}, t^{2q+2}, t^q, t, t^{2q}, t^2, t^{2q+1}, t^{q+2})$$

for $t \in \mathbb{F}_{q^2}$ and

$$m_\infty = \iota_2(0, 0, 1) = (0, 0, 1, 0, 0, 0, 0, 0, 0).$$

Let $n = q^2 + 1$. Let M be the $9 \times n$ matrix whose columns are the $m_t, t \in \mathbb{F}_{q^2}$ together with m_∞. The matrix M is unique up to right-multiplication by an invertible diagonal matrix over $\mathbb{F}_{q^2}$ (we assume that we have placed an ordering on the elements of $\mathbb{F}_{q^2}$ and that the columns of M are arranged in the corresponding order).

Let β be an element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and consider the invertible matrix

$$C_\beta = \mathrm{diag}(1, 1, 1, V_2(\beta^q, \beta), V_2(\beta^q, \beta), V_2(\beta^q, \beta)). \tag{14}$$

Notice that for $t \in \mathbb{F}_{q^2}$,

$$\begin{aligned} V_2(\beta^q, \beta) \begin{pmatrix} t^q \\ t \end{pmatrix} &= \begin{pmatrix} T_2(t) \\ T_2(\beta t) \end{pmatrix}, \\ V_2(\beta^q, \beta) \begin{pmatrix} t^{2q} \\ t^2 \end{pmatrix} &= \begin{pmatrix} T_2(t^2) \\ T_2(\beta t^2) \end{pmatrix}, \\ V_2(\beta^q, \beta) \begin{pmatrix} t^{2q+1} \\ t^{q+2} \end{pmatrix} &= \begin{pmatrix} T_2(t^{q+2}) \\ T_2(\beta t^{q+2}) \end{pmatrix} \end{aligned}$$

are all in $\mathbb{F}_q^2$ (recall that T_2 is the relative trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$). Therefore,

$$\begin{aligned} h_t^\top &:= C_\beta m_t^\top \\ &= \left(1, t^{q+1}, t^{2q+2}, T_2(t), T_2(\beta t), T_2(t^2), T_2(\beta t^2), T_2(t^{q+2}), T_2(\beta t^{q+2})\right)^\top \end{aligned}$$

is in $\mathbb{F}_q^9$ for all $t \in \mathbb{F}_{q^2}$. Notice that $h_0^\top = m_0^\top$. Also

$$h_\infty^\top := C_\beta m_\infty^\top = m_\infty^\top$$

Let $H = C_\beta \cdot M$ be the $9 \times n$ matrix over $\mathbb{F}_q$ whose columns are the $h_t^\top, t \in \mathbb{F}_{q^2}$, together with $h_\infty^\top$. Then H is a parity check matrix of an $[n, n-9] = [q^2+1, q^2-8]$ code $\mathcal{C}$ over $\mathbb{F}_q$.

Furthermore, we claim that any 5 columns of H are linearly independent. Since C is invertible, we may prove this by showing that any 5 columns of M are linearly independent. Since $\mathrm{PGL}(2, q^2)$ acts triply transitively on the points of $\mathcal{O}$, we may assume that the chosen columns are $m_\infty, m_0, m_1, m_s, m_t$, i.e., the rows of the matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & s^{q+1} & s^{2q+2} & s^q & s & s^{2q} & s^2 & s^{2q+1} & s^{q+2} \\ 1 & t^{q+1} & t^{2q+2} & t^q & t & t^{2q} & t^2 & t^{2q+1} & t^{q+2} \end{pmatrix},$$

where s and t are distinct elements of $\mathbb{F}_{q^2} \setminus \{0, 1\}$. Restricting to columns $1, 2, 3, 4, 9$ yields the submatrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & s^{q+1} & s^{2q+2} & s^q & s^{q+2} \\ 1 & t^{q+1} & t^{2q+2} & t^q & t^{q+2} \end{pmatrix}.$$

Expanding the determinant of this matrix along the first two rows leads to

$$-\begin{vmatrix} 1 & 1 & 1 \\ s^{q+1} & s^q & s^{q+2} \\ t^{q+1} & t^q & t^{q+2} \end{vmatrix} = -s^q t^q \begin{vmatrix} 1 & 1 & 1 \\ s & 1 & s^2 \\ t & 1 & t^2 \end{vmatrix} = |V_3(1, s, t)| \neq 0.$$

This shows that the 5 vectors are independent. Hence H is the parity check matrix of a linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length q^2+1, dimension q^2-8 and minimum distance at least 6.

In order to prove the statement on the automorphism group of these codes, we let $\mathcal{D}$ be the $[q^2+1, q^2-8]$ code over $\mathbb{F}_{q^2}$ generated by M. Recall that $\mathrm{P\Gamma L}(2,q)$ is the full automorphism group of the regular oval in $\mathrm{PG}(2,q)$. We consider an element $\varphi_{a,b,c,d} : t \mapsto \frac{at+c}{bt+d}$ in $\mathrm{PGL}(2,q^2)$ where $ad-bc \neq 0$. Let $x = \iota_2(t)$ and $y = \iota_2(\varphi_{a,b,c,d}(t))$. For sake of simplicity, write A for $at+c$ and B for $bt+d$. Then

$$\begin{aligned}
\mathbf{P}(y) &= \mathbf{P}\Big(1, \Big(\frac{A}{B}\Big)^{q+1}, \Big(\frac{A}{B}\Big)^{2q+2}, \Big(\frac{A}{B}\Big)^{q}, \Big(\frac{A}{B}\Big), \\
&\qquad \Big(\frac{A}{B}\Big)^{2q}, \Big(\frac{A}{B}\Big)^{2}, \Big(\frac{A}{B}\Big)^{2q+1}, \Big(\frac{A}{B}\Big)^{q+2}\Big) \\
&= \mathbf{P}\Big(B^{2q+2}, A^{q+1}B^{q+1}, A^{2q+2}, A^{q}B^{q+2}, AB^{2q+1}, \\
&\qquad A^{2q}B^{2}, A^{2}B^{2q}, A^{2q+1}B, A^{q+2}B^{q}\Big) \\
&= \mathbf{P}(x \cdot R(a,b,c,d)),
\end{aligned}$$

with $R(a,b,c,d)$ as in Table 2. The matrix $R(a,b,c,d)$ corresponding to $\varphi_{a,b,c,d}$ in $\mathrm{PGL}(2,q^2)$ acts as automorphism of the code $\mathcal{D}$. Namely, we have

$$R(a,b,c,d)^{\top} \cdot M \cdot X_{a,b,c,d} = M$$

for some monomial matrix $X_{a,b,c,d} \in M_n(q^2)$. Conjugating the matrix $R(a,b,c,d)$ by the matrix C_β yields

$$U(a,b,c,d,\beta) = C_\beta \cdot R(a,b,c,d)^{\top} \cdot C_\beta^{-1}$$

It follows from the theory of twisted tensor products that the matrix U is over $\mathbb{F}_q$. For this, we refer to [2, 26.3], or to [7, 2.2]. Furthermore,

$$\begin{aligned}
U(a,b,c,d,\beta) \cdot H \cdot X_{a,b,c,d} &= C_\beta \cdot R(a,b,c,d) \cdot C_\beta^{-1} \cdot C_\beta \cdot M \cdot X_{a,b,c,d} \\
&= C_\beta \cdot M = H,
\end{aligned}$$

i.e. $X_{a,b,c,d}$ is an automorphism of the code $\mathcal{C}$. If $q = p^e$, the Frobenius automorphism ϕ_e is a semilinear code automorphism. The automorphism group cannot be larger since it is known that $\mathrm{P\Gamma L}(2,q^2)$ is the automorphism group of the regular oval. This shows that $\mathrm{P\Gamma L}(2,q^2) = \Gamma\mathrm{Aut}(\mathcal{C})$ and that $\mathcal{C}$ is constacyclic.

Let us now investigate which automorphisms are monomial automorphisms. Consider the block diagonal matrix

$$S = \mathrm{diag}(1,1,1,J,J,J),$$

$$R(a,b,c,d) = (R_1 \mid R_2)$$

$$R_1 = \left(\begin{array}{c|c|c|c|c}
d^{2q+2} & c^{q+1}d^{q+1} & c^{2q+2} & c^q d^{q+2} & cd^{2q+1} \\ \hline
4b^{q+1}d^{q+1} & \begin{array}{c} a^{q+1}d^{q+1} \\ +a^q bcd^q \\ +ab^q c^q d \\ +b^{q+1}c^{q+1} \end{array} & 4a^{q+1}c^{q+1} & \begin{array}{c} 2a^q bd^{q+1} \\ +2b^{q+1}c^q d \end{array} & \begin{array}{c} 2ab^q d^{q+1} \\ +2b^{q+1}cd^q \end{array} \\ \hline
b^{2q+2} & a^{q+1}b^{q+1} & a^{2q+2} & a^q b^{q+2} & ab^{2q+1} \\ \hline
2b^q d^{q+2} & \begin{array}{c} a^q cd^{q+1} \\ +b^q c^{q+1}d \end{array} & 2a^q c^{q+2} & \begin{array}{c} a^q d^{q+2} \\ +b^q c^q d^2 \end{array} & 2b^q cd^{q+1} \\ \hline
2bd^{2q+1} & \begin{array}{c} ac^q d^{q+1} \\ +bc^{q+1}d^q \end{array} & 2ac^{2q+1} & 2bc^q d^{q+1} & \begin{array}{c} ad^{2q+1} \\ +bcd^{2q} \end{array} \\ \hline
b^{2q}d^2 & a^q b^q cd & a^{2q}c^2 & a^q b^q d^2 & b^{2q}cd \\ \hline
b^2 d^{2q} & abc^q d^q & a^2 c^{2q} & b^2 c^q d^q & abd^{2q} \\ \hline
2b^{2q+1}d & \begin{array}{c} a^{q+1}b^q d \\ +a^q b^{q+1}c \end{array} & 2a^{2q+1}c & 2a^q b^{q+1}d & \begin{array}{c} ab^{2q}d \\ +b^{2q+1}c \end{array} \\ \hline
2b^{q+2}d^q & \begin{array}{c} a^{q+1}bd^q \\ +ab^{q+1}c^q \end{array} & 2a^{q+2}c^q & \begin{array}{c} a^q b^2 d^q \\ +b^{q+2}c^q \end{array} & 2ab^{q+1}d^q
\end{array}\right)$$

$$R_2 = \left(\begin{array}{c|c|c|c}
c^{2q}d^2 & c^2 d^{2q} & c^{2q+1}d & c^{q+2}d^q \\ \hline
4a^q bc^q d & 4ab^q cd^q & \begin{array}{c} 2a^q bc^{q+1} \\ +2a^{q+1}c^q d \end{array} & \begin{array}{c} 2a^{q+1}cd^q \\ +2ab^q c^{q+1} \end{array} \\ \hline
a^{2q}b^2 & a^2 b^{2q} & a^{2q+1}b & a^{q+2}b^q \\ \hline
2a^q c^q d^2 & 2b^q c^2 d^q & 2a^q c^{q+1}d & \begin{array}{c} a^q c^2 d^q \\ +b^q c^{q+2} \end{array} \\ \hline
2bc^{2q}d & 2acd^{2q} & \begin{array}{c} ac^{2q}d \\ +bc^{2q+1} \end{array} & 2ac^{q+1}d^q \\ \hline
a^{2q}d^2 & b^{2q}c^2 & a^{2q}cd & a^q b^q c^2 \\ \hline
b^2 c^{2q} & a^2 d^{2q} & abc^{2q} & a^2 c^q d^q \\ \hline
2a^{2q}bd & 2ab^{2q}c & \begin{array}{c} a^{2q+1}d \\ +a^{2q}bc \end{array} & 2a^{q+1}b^q c \\ \hline
2a^q b^2 c^q & 2a^2 b^q d^q & 2a^{q+1}bc^q & \begin{array}{c} a^{q+2}d^q \\ +a^2 b^q c^q \end{array}
\end{array}\right)$$

Table 2: The matrix $R(a,b,c,d)$

where

$$J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Left multiplying S (or $S^\top$) is the same as applying ϕ_2 to the matrix M, i.e.

$$S^\top \cdot M \cdot P = \phi_2(M) \cdot P = M,$$

for some permutation matrix P. Conjugating $S^\top$ by the matrix C_β yields

$$V = C_\beta \cdot S^\top \cdot C_\beta^{-1} = \mathrm{diag}(1, 1, 1, K, K, K),$$

where K is the 2×2 matrix

$$K = V_2(\beta^q, \beta) \cdot J \cdot V_2(\beta^q, \beta)^{-1} = \begin{pmatrix} 1 & 0 \\ T_2(\beta) & -1 \end{pmatrix}.$$

over $\mathbb{F}_q$ (since all entries are norm values in the subfield). Furthermore,

$$\begin{aligned} V \cdot H \cdot P &= C_\beta \cdot S^\top \cdot C_\beta^{-1} \cdot C_\beta \cdot M \cdot P \\ &= C_\beta \cdot M = H, \end{aligned}$$

where P is the permutation matrix defined previously. Since $\mathrm{PGL}(2, q^2)$ and ϕ_2 generate $\mathrm{P\Gamma_2L}(2, q^2)$, this is a monomial automorphism group of the code $\mathcal{C}$.

Next we prove that the codes of length $q^2 + 1$ are cyclic if and only if q is even. By Lemma 6, the only automorphisms which permute the elements of $\mathrm{PG}(1, q^2)$ cyclically (i.e., in one orbit of size q^2+1) are those whose associated matrix has a subprimitive characteristic polynomial. Namely, if $m(x) := x^2 + c_1x + c_0$ is subprimitive of degree 2 over $\mathbb{F}_{q^2}$, the associated cyclic collineation is $\mathcal{S} := \varphi_{0,1,-c_0,-c_1}$ in $\mathrm{PGL}(2, q^2)$. Since $m(x)$ is subprimitive, $\mathcal{S}^i = cI_2$, $c \in \mathbb{F}_{q^2}$ forces $i = \mathrm{Subexp}(m)$. In order to induce a cyclic permutation automorphism of the code, we must have $m(x) \in \mathcal{R}_1(2, q^2)$. It follows from Lemma 7 that $\mathcal{R}_1(2, q^2) \neq \emptyset$ precisely if q is even. This finishes the proof for the family of codes of length $q^2 + 1$.

If q is even, we may consider the regular hyperoval $\mathcal{O}^*$ which is obtained by adding to $\mathcal{O}$ the nucleus $\mathbf{P}(0, 1, 0)$, i.e. $\mathcal{O}^* = \mathcal{O} \cup \{\mathbf{P}(0, 1, 0)\}$. Let $n = q^2 + 2$. Consider the $9 \times n$ matrix M whose columns are the $m_t, t \in \mathbb{F}_{q^2}$ together with m_∞ and m_*, where

$$m_* = \iota_2(0, 1, 0) = (0, 1, 0, 0, 0, 0, 0, 0, 0).$$

Let

$$h_*^\top := C_\beta m_*^\top = m_*^\top,$$

and form the $9\times n$ matrix $H = C_\beta \cdot M$ which is over $\mathbb{F}_q$, and whose columns are $h_t^\top, t \in \mathbb{F}_{q^2}$, together with $h_\infty^\top$ and $h_*^\top$. We need to show that any 5 columns of H are linearly independent over $\mathbb{F}_q$. Consider any 5-set of columns. Since the columns not containing $h_*^\top$ have already been shown to satisfy the property, we may assume that h_* is among the 5 chosen columns. Since the stabilizer of the nucleus in $\mathrm{PGL}(2, q^2)$ is still doubly transitive on $\mathcal{O}$, we may assume that the 5 vectors are $m_*, m_\infty, m_0, m_s, m_t$, i.e., the rows of the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & s^{q+1} & s^{2q+2} & s^q & s & s^{2q} & s^2 & s^{2q+1} & s^{q+2} \\ 1 & t^{q+1} & t^{2q+2} & t^q & t & t^{2q} & t^2 & t^{2q+1} & t^{q+2} \end{pmatrix},$$

where s and t are distinct elements of $\mathbb{F}_{q^2}^\times$. Restricting to columns $1, 2, 3, 5, 7$ yields the submatrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & s^{q+1} & s^{2q+2} & s & s^2 \\ 1 & t^{q+1} & t^{2q+2} & t & t^2 \end{pmatrix}.$$

Expanding the determinant of this matrix gives

$$\begin{vmatrix} s & s^2 \\ t & t^2 \end{vmatrix} \neq 0.$$

This shows that H is the check matrix of a $[q^2+2, q^2-7, \geq 6]_q$ code. The automorphism group of this code contains the automorphism of the corresponding code of length q^2+1 examined previously. The group is embedded as the stabilizer of the coordinate corresponding to the nucleus. Since $q^2 > 4$, the nucleus is fixed and hence the code is not cyclic.

It remains to show that the codes of length q^2+2 are not the parity extensions in the dual of the corresponding codes of length q^2+1. To do this, we show that $\sum_{t\in\mathbb{F}_{q^2}} m_t = 0$. Since $m_* \neq m_\infty$, this implies the statement. Note that

$$\sum_{t\in\mathbb{F}_q} t = 0 \text{ (if } q > 2\text{)}, \qquad \sum_{\substack{t,s\in\mathbb{F}_q^\times \\ t\neq s}} ts = 0 \text{ (if } q > 3\text{)},$$

and

$$\sum_{t\in\mathbb{F}_{q^2}} N_2(t) = \sum_{t\in\mathbb{F}_{q^2}} t^{q+1} = (q+1)\sum_{t\in\mathbb{F}_q^\times} t = 0 \text{ (if } q > 2\text{)},$$

the last equation because $N_2(0) = 0$ and because the N_2 map is $(q+1)$ to 1 from $\mathbb{F}_{q^2}^\times$ to $\mathbb{F}_q^\times$. Since $q = 2^e$ is even, the mapping $\phi_e : t \mapsto t^2$ is a permutation of $\mathbb{F}_{q^2}^\times$, which implies that

$$\begin{aligned} \sum_{t\in\mathbb{F}_{q^2}} N_2(t^2) &= \sum_{t\in\mathbb{F}_{q^2}} N_2(t) = 0, \\ \sum_{t\in\mathbb{F}_{q^2}} t^2 &= \sum_{t\in\mathbb{F}_{q^2}} t = 0. \end{aligned}$$

Furthermore,

$$\begin{aligned} \sum_{t\in\mathbb{F}_{q^2}} t^q &= \big(\sum_{t\in\mathbb{F}_{q^2}} t\big)^q = 0, \\ \sum_{t\in\mathbb{F}_{q^2}} t^{2q} &= \big(\sum_{t\in\mathbb{F}_{q^2}} t^2\big)^q = 0. \end{aligned}$$

Lastly, with β a primitive element of $\mathbb{F}_{q^2}$, and β^{q+1} a primitive element of the subfield $\mathbb{F}_q$,

$$\sum_{t\in\mathbb{F}_{q^2}^\times} t^{q+2} = \sum_{t\in\mathbb{F}_{q^2}^\times} N_2(t)t = \sum_{s\in\mathbb{F}_q^\times} s\big(\sum_{\substack{t\in\mathbb{F}_{q^2}^\times \\ N_2(t)=s}} t\big)$$

If $s = \beta^{(q+1)j} \in \mathbb{F}_q^\times$ and $t = \beta^i$, the condition

$$\beta^{(q+1)j} = s = N_2(t) = t^{q+1} = \beta^{(q+1)i}$$

translates into the following condition for the exponents

$$(q+1)j \equiv (q+1)i \mod q^2 - 1$$

which holds if and only if $j \equiv i \mod q-1$. Therefore, we continue

$$\begin{aligned}
&= \sum_{j=1}^{q-1} \beta^{(q+1)j} \sum_{\substack{i \mod q^2-1 \\ i \equiv j \mod q-1}} \beta^{i} \\
&= \sum_{j=1}^{q-1} \beta^{(q+1)j} \sum_{k=0}^{q} \beta^{j+k(q-1)} \\
&= \sum_{j=1}^{q-1} \beta^{(q+1)j} \beta^{j} \sum_{k=0}^{q} (\beta^{q-1})^{k} \\
&= \sum_{j=1}^{q-1} \beta^{(q+1)j} \beta^{j} \frac{(\beta^{q-1})^{q+1}-1}{\beta^{q-1}-1} = 0.
\end{aligned}$$

Thus also

$$\sum_{t \in \mathbb{F}_{q^2}^{\times}} t^{2q+1} = \big(\sum_{t \in \mathbb{F}_{q^2}^{\times}} t^{q+2} \big)^{q} = 0.$$

Using the shorthand notation $\nu_i = \sum_{t \in \mathbb{F}_{q^2}} \nu_{t,i}$ with $\nu_{t,i}$ the coefficient of c_i in $m_t = \iota_2(1, t, t^2)$, we find that

$$\begin{aligned}
\nu_1 &= \sum_{t \in \mathbb{F}_{q^2}} 1 = 0, \\
\nu_2 &= \sum_{t \in \mathbb{F}_{q^2}} t^{q+1} = \sum_{t \in \mathbb{F}_{q^2}} N_2(t) = 0, \\
\nu_3 &= \sum_{t \in \mathbb{F}_{q^2}} t^{2q+2} = \sum_{t \in \mathbb{F}_{q^2}} N_2(t^2) = 0.
\end{aligned}$$

Also,

$$\begin{aligned}
\nu_4 &= \sum_{t \in \mathbb{F}_{q^2}} t^{q} = 0, \quad \nu_5 = \sum_{t \in \mathbb{F}_{q^2}} t = 0, \quad \nu_6 = \sum_{t \in \mathbb{F}_{q^2}} t^{2q} = 0, \\
\nu_7 &= \sum_{t \in \mathbb{F}_{q^2}} t^{2} = 0, \quad \nu_8 = \sum_{t \in \mathbb{F}_{q^2}} t^{2q+1} = 0, \quad \nu_9 = \sum_{t \in \mathbb{F}_{q^2}} t^{q+2} = 0.
\end{aligned}$$

This completes the proof of Theorem 1. □

5 Proof of Theorem 2

Proof. (of Theorem 2) Let $V = V_2 = \mathbb{F}_{q^3}^2$ with basis a_1, a_2. Consider the projective line $\mathrm{PG}(1, q^3) = \mathbf{P}(V_2)$. Let $n = \theta_1(q^3) = q^3 + 1$. Using the map ι_3 and the ordering of basis vectors as in Example 1, we obtain

$$m_t := \iota_3(1, t) = (1, t^{q^2+q+1}, t, t^q, t^{q^2}, t^{q+1}, t^{q^2+q}, t^{q^2+1})$$

for $t \in \mathbb{F}_{q^3}$ and

$$m_\infty = \iota_3(0, 1) = (0, 1, 0, 0, 0, 0, 0, 0).$$

Let M be the $8 \times n$ matrix whose columns are the $m_t, t \in \mathbb{F}_{q^3}$ together with m_∞. The matrix M is unique up to right-multiplication by an invertible diagonal matrix over $\mathbb{F}_{q^3}$ (we assume that we have placed an ordering on the elements of $\mathbb{F}_{q^3}$ and that the columns of M are arranged in the corresponding order).

Let β be an element in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$, and consider the invertible matrix

$$C_\beta = \mathrm{diag}(1, 1, L_1, L_2), \tag{15}$$

where

$$\begin{aligned} L_1 &= V_3(\beta, \beta^q, \beta^{q^2}), \\ L_2 &= V_3(\beta^{q+1}, \beta^{q^2+q}, \beta^{q^2+1})). \end{aligned}$$

Notice that for $t \in \mathbb{F}_{q^3}$,

$$\begin{aligned} L_1 \begin{pmatrix} t \\ t^q \\ t^{q^2} \end{pmatrix} &= \begin{pmatrix} T_3(t) \\ T_3(\beta t) \\ T_3(\beta^2 t) \end{pmatrix}, \\ L_2 \begin{pmatrix} t^{q+1} \\ t^{q^2+q} \\ t^{q^2+1} \end{pmatrix} &= \begin{pmatrix} T_3(t^{q+1}) \\ T_3((\beta t)^{q+1}) \\ T_3((\beta^2 t)^{q+1}) \end{pmatrix} \end{aligned}$$

are all in $\mathbb{F}_q^3$ (recall that T_3 is the relative trace from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$). Therefore,

$$\begin{aligned} h_t^\top &:= C_\beta m_t^\top \\ &= \Big(1, t^{q^2+q+1}, T_3(t), T_3(\beta t), T_3(\beta^2 t), \\ &\qquad T_3(t^{q+1}), T_3((\beta t)^{q+1}, T_3((\beta^2 t)^{q+1})\Big)^\top \end{aligned}$$

is in $\mathbb{F}_q^8$ for all $t \in \mathbb{F}_{q^2}$. Notice that $h_0^\top = m_0^\top$ and $h_\infty^\top := C_\beta m_\infty^\top = m_\infty^\top$. Let $H = C_\beta \cdot M$ be the $8 \times n$ matrix over $\mathbb{F}_q$ whose columns are the $h_t^\top, t \in \mathbb{F}_{q^2}$, together with $h_\infty^\top$. Then H is a parity check matrix of an $[n, n-8]$ code $\mathcal{C}$ over $\mathbb{F}_q$.

Furthermore, we claim that any 4 columns of H are linearly independent. Since C is invertible, we may prove this by showing that any 4 columns of M are linearly independent. Since $\mathrm{PGL}(2, q^3)$ acts triply transitively on the points of $\mathrm{PG}(1, q^3)$, we may assume that the chosen columns are m_∞, m_0, m_1, m_t, $(0 \neq t \neq 1)$ i.e., the rows of the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & t^{q^2+q+1} & t & t^q & t^{q^2} & t^{q+1} & t^{q^2+q} & t^{q^2+1} \end{pmatrix}.$$

Restricting to columns $1, 2, 3, 4$ yields the submatrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & t^{q^2+q+1} & t & t^q \end{pmatrix}.$$

Expanding the determinant of this matrix along the first two rows leads to

$$-\begin{vmatrix} 1 & 1 \\ t & t^q \end{vmatrix} = t(1 - t^{q-1})$$

which is nonzero since $t \notin \mathbb{F}_q$ and $t \neq 0, 1$. This shows that the 4 vectors are independent. Therefore, H is the parity check matrix of a linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, dimension $n - 8$ and minimum distance at least 5.

In order to prove the statement on the automorphism group of these codes, we let $\mathcal{D}$ be the $[q^3 + 1, q^3 - 7]$ code over $\mathbb{F}_{q^3}$ generated by M. The collineation group of the projective line is $\mathrm{P\Gamma L}(2, q^3)$ and is triply transitive on the points of $\mathrm{PG}(1, q^3)$. We consider a linear element $\varphi_{a,b,c,d} : t \mapsto \frac{at+c}{bt+d}$ in $\mathrm{PGL}(2, q^2)$ where $ad - bc \neq 0$. Let $x = \iota_3(t)$ and $y = \iota_3(\varphi_{a,b,c,d}(t))$. For sake

$$\begin{pmatrix} m_{ddd} & m_{ccc} & m_{ddc} & m_{dcd} & m_{cdd} & m_{dcc} & m_{ccd} & m_{cdc} \\ m_{bbb} & m_{aaa} & m_{bba} & m_{bab} & m_{abb} & m_{baa} & m_{aab} & m_{aba} \\ m_{ddb} & m_{cca} & m_{dda} & m_{dcb} & m_{cdb} & m_{dca} & m_{ccb} & m_{cda} \\ m_{dbd} & m_{cac} & m_{dbc} & m_{dad} & m_{cbd} & m_{dac} & m_{cad} & m_{cbc} \\ m_{bdd} & m_{acc} & m_{bdc} & m_{bcd} & m_{add} & m_{bcc} & m_{acd} & m_{adc} \\ m_{dbb} & m_{caa} & m_{dba} & m_{dab} & m_{cbb} & m_{daa} & m_{cab} & m_{cba} \\ m_{bbd} & m_{aac} & m_{bbc} & m_{bad} & m_{abd} & m_{bac} & m_{aad} & m_{abc} \\ m_{bdb} & m_{aca} & m_{bda} & m_{bcb} & m_{adb} & m_{bca} & m_{acb} & m_{ada} \end{pmatrix}$$

Table 3: The matrix $R(a,b,c,d)$ (with $m_{xyz} = x^{q^2} y^q z$)

of simplicity, write A for $at + c$ and B for $bt + d$. Then

$$\begin{aligned} \mathbf{P}(y) &= \mathbf{P}\Big(1, \Big(\frac{A}{B}\Big)^{q^2+q+1}, \frac{A}{B}, \Big(\frac{A}{B}\Big)^{q}, \Big(\frac{A}{B}\Big)^{q^2}, \\ &\qquad \Big(\frac{A}{B}\Big)^{q+1}, \Big(\frac{A}{B}\Big)^{q^2+q}, \Big(\frac{A}{B}\Big)^{q^2+1}\Big) \\ &= \mathbf{P}\Big(B^{2q+q+1}, A^{q^2+q+1}, AB^{q^2+q}, A^q B^{q^2+1}, A^{q^2} B^{q+1}, \\ &\qquad A^{q+1} B^{q^2}, A^{q^2+q} B, A^{q^2+1} B^q\Big) \\ &= \mathbf{P}(x \cdot R(a,b,c,d)), \end{aligned}$$

with $R(a,b,c,d)$ as in Table 3. The matrix $R(a,b,c,d)$ corresponding to $\varphi_{a,b,c,d}$ in $\mathrm{PGL}(2,q^3)$ acts as automorphism of the code $\mathcal{D}$. Namely, we have

$$R(a,b,c,d)^\top \cdot M \cdot X_{a,b,c,d} = M$$

for some monomial matrix $X_{a,b,c,d} \in M_n(q^3)$. Conjugating the matrix $R(a,b,c,d)$ by the matrix C_β yields

$$U(a,b,c,d,\beta) = C_\beta \cdot R(a,b,c,d)^\top \cdot C_\beta^{-1}$$

It follows from the theory of twisted tensor products that the matrix U is over $\mathbb{F}_q$. For this, we refer to [2, 26.3], or to [7, 2.2]. Furthermore,

$$\begin{aligned} U(a,b,c,d,\beta) \cdot H \cdot X_{a,b,c,d} &= C_\beta \cdot R(a,b,c,d) \cdot C_\beta^{-1} \cdot C_\beta \cdot M \cdot X_{a,b,c,d} \\ &= C_\beta \cdot M = H, \end{aligned}$$

i.e. $X_{a,b,c,d}$ is an automorphism of the code $\mathcal{C}$. If $q = p^e$, the Frobenius automorphism ϕ_e is a semilinear code automorphism. This shows that $\mathrm{P\Gamma L}(2, q^3) = \Gamma\mathrm{Aut}(\mathcal{C})$ and that $\mathcal{C}$ is constacyclic.

Let us now investigate which automorphisms are monomial automorphisms. Consider the block diagonal matrix

$$S = \mathrm{diag}(1, 1, J, J),$$

where

$$J = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Left multiplying S is the same as applying ϕ_3 to the matrix M, i.e.

$$S^\top \cdot M \cdot P = \phi_3(M) \cdot P = M,$$

for some permutation matrix P. Conjugating $S^\top$ by the matrix C_β yields

$$V(\beta) = C_\beta \cdot S^\top \cdot C_\beta^{-1} = \mathrm{diag}(1, 1, V_1, V_2),$$

where

$$V_1 = L_1 \cdot J^\top \cdot L_1^{-1}, \quad V_2 = L_2 \cdot J^\top \cdot L_2^{-1}.$$

We find that

$$V_1 = \delta_1 \begin{pmatrix} T_3(\beta_{21} - \beta_{12}) & T_3(\beta_2 - \beta_{20}) & T_3(\beta_{10} - \beta_1) \\ T_3(\beta_{31} - \beta_{22}) & T_3(\beta_{12} - \beta_{30}) & T_3(\beta_{20} - \beta_{11}) \\ T_3(\beta_{41} - \beta_{32}) & T_3(\beta_{22} - \beta_{40}) & T_3(\beta_{30} - \beta_{21}) \end{pmatrix},$$

$$V_2 = \delta_2 \begin{pmatrix} T_3(\beta_{231} - \beta_{132}) & T_3(\beta_{22} - \beta_{220}) & T_3(\beta_{110} - \beta_{11}) \\ T_3(\beta_{341} - \beta_{242}) & T_3(\beta_{132} - \beta_{330}) & T_3(\beta_{220} - \beta_{121}) \\ T_3(\beta_{451} - \beta_{352}) & T_3(\beta_{242} - \beta_{440}) & T_3(\beta_{330} - \beta_{231}) \end{pmatrix},$$

where $\beta_{ijk} = \beta^{iq^2+jq+k}$ and $\beta_{jk} = \beta_{0jk}$ and $\beta_k = \beta_{00k}$. Since all matrix entries are trace or norm values, these matrices are over the subfield $\mathbb{F}_q$. Furthermore,

$$\begin{aligned} V \cdot H \cdot P &= C_\beta \cdot S \cdot C_\beta^{-1} \cdot C_\beta \cdot M \cdot P \\ &= C_\beta \cdot M = H, \end{aligned}$$

where P is the permutation matrix defined previously. Since $\mathrm{PGL}(2, q^3)$ and ϕ_3 generate $\mathrm{P\Gamma_3 L}(2, q^3)$, this is a monomial automorphism group of the code $\mathcal{C}$.

q		Parameters	Comments
4	$\mathcal{C}$	$[17,8,8]_4$	[18], optimal, cyclic
4	$\mathcal{C}^\perp$	$[17,9,7]_4$	optimal, cyclic
5	$\mathcal{C}$	$[26,17,6]_5$	not optimal ($\exists$ $[26,17,7]_5$), constacyclic
5	$\mathcal{C}^\perp$	$[26,9,14]_5$	best known
7	$\mathcal{C}$	$[50,41,6]_7$	best known, constacyclic
7	$\mathcal{C}^\perp$	$[50,9,34]_7$	best known
9	$\mathcal{C}$	$[82,73,6]_9$	best known, constacyclic

Table 4: The codes of length q^2+1 of Theorem 1 for small q

q		Parameter	Comments
4	$\mathcal{C}$	$[18,9,8]_4$	[18], optimal, formally self-dual, not self-dual, not cyclic
4	$\mathcal{C}^\perp$	$[18,9,8]_4$	$\mathcal{C}^\perp=\phi_2(\mathcal{C})$
8	$\mathcal{C}$	$[66,57,6]_8$	best known, not cyclic
8	$\mathcal{C}^\perp$	$[66,9,48]_8$	best known, see also: [20], or X-construction [11]

Table 5: The codes of length q^2+2 of Theorem 1 for small q

Next we prove that the codes are cyclic if and only if q is even. By Lemma 6, the only automorphisms which permute the elements of $\mathrm{PG}(1,q^3)$ cyclically (i.e., in one orbit of size q^3+1) are those whose associated matrix has a subprimitive characteristic polynomial. Namely, if $m(x) := x^2+c_1x+c_0$ is subprimitive of degree 2 over $\mathbb{F}_{q^3}$, the associated cyclic collineation is $\mathcal{S} := \varphi_{0,1,-c_0,-c_1}$ in $\mathrm{PGL}(2,q^3)$. Since $m(x)$ is subprimitive, $\mathcal{S}^i = cI_2$, $c \in \mathbb{F}_{q^3}$ forces $i = \mathrm{Subexp}(m)$. In order to induce a cyclic permutation automorphism of the code, we must have $m(x) \in \mathcal{R}_1(2,q^2)$. It follows from Lemma 7 that $\mathcal{R}_1(2,q^3) \neq \emptyset$ precisely if q is even. This finishes the proof. □

6 Examples: Theorem 1

Tables 4 and 5 summarize the codes constructed by Theorem 1 for small q. Note that Theorem 1 only gives a lower bound for the minimum distance, and the true minimum distance may turn out to be better than predicted by Theorem 1. In the following, we will discuss a few of the codes in more detail.

We let the elements of the finite fields be represented by integers. If the order $q = p$ is a prime, these numbers are the usual representatives of the residue classes of $\mathbb{Z}$ modulo p. Otherwise, if $q = p^e$ with $e > 1$, then we fix a root α of an irreducible polynomial of degree e over $\mathbb{F}_p$. Using this root, we can represent field elements as integers using the correspondence

$$\sum_{i=0}^{e-1} a_i \alpha^i \; \leftrightarrow \; \sum_{i=0}^{e-1} a_i p^i, \tag{16}$$

where we take the coefficients a_i to be integers between 0 and $p - 1$.

To create $\mathbb{F}_{256}$, we may use the primitive polynomial $X^8+X^4+X^3+X^2+1$ over $\mathbb{F}_2$. Let ζ be a root of this polynomial, so that $\zeta^8 = \zeta^4 + \zeta^3 + \zeta^2 + 1$. Then $\mathbb{F}_{256} = \mathbb{F}_2(\zeta)$. Since $\mathbb{F}_{16}^\times$ is a subgroup of index 17 in $\mathbb{F}_{256}^\times$, we have that

$$\mathbb{F}_{16} = \mathbb{F}_2(\zeta^{17}) = \{0, 1, \zeta^{17}, \zeta^{34}, \ldots\} = \mathbb{F}_2(\alpha),$$

where $\alpha = \zeta^{17}$. From

$$\begin{array}{rcl} \alpha^4 & = & \zeta^{68} = \zeta^7 + \zeta^4 + \zeta^3 + 1 \hat{=} 153, \\ \alpha^3 & = & \zeta^{51} = \zeta^3 + \zeta \hat{=} 10, \\ \alpha^2 & = & \zeta^{34} = \zeta^6 + \zeta^3 + \zeta^2 + \zeta \hat{=} 78, \\ \alpha & = & \zeta^{17} = \zeta^7 + \zeta^4 + \zeta^3 \hat{=} 152, \end{array}$$

it follows that $\alpha^4 = \alpha + 1$, i.e. α is a root of the (primitive, irreducible) polynomial $X^4 + X + 1$. Since $\mathbb{F}_4^\times$ is a subgroup of index 5 in $\mathbb{F}_{16}^\times$, we have that

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha^5) = \{0, 1, \alpha^5, \alpha^{10}\} = \mathbb{F}_2(\eta),$$

where $\eta = \alpha^5$. From

$$\begin{array}{rcl} \eta^2 & = & \alpha^{10} = \alpha^2 + \alpha + 1 \hat{=} 7, \\ \eta & = & \alpha^5 = \alpha^2 + \alpha \hat{=} 6, \end{array}$$

it follows that $\eta^2 = \eta + 1$, i.e. η is a root of the (primitive, irreducible) polynomial $X^2 + X + 1$.

For $q = 4$, length 18, the matrix M over $\mathbb{F}_{16}$ is

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 6 & 6 & 7 & 7 & 7 & 6 & 1 & 7 & 1 & 6 & 1 & 6 & 7 & 1 & 0 & 1 \\
0 & 1 & 7 & 7 & 6 & 6 & 6 & 7 & 1 & 6 & 1 & 7 & 1 & 7 & 6 & 1 & 1 & 0 \\
0 & 1 & 3 & 2 & 5 & 4 & 6 & 7 & 15 & 14 & 12 & 13 & 10 & 11 & 9 & 8 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 0 & 0 \\
0 & 1 & 5 & 4 & 2 & 3 & 7 & 6 & 10 & 11 & 15 & 14 & 8 & 9 & 13 & 12 & 0 & 0 \\
0 & 1 & 4 & 5 & 3 & 2 & 7 & 6 & 12 & 13 & 8 & 9 & 15 & 14 & 11 & 10 & 0 & 0 \\
0 & 1 & 10 & 12 & 8 & 15 & 1 & 1 & 15 & 12 & 12 & 8 & 10 & 15 & 10 & 8 & 0 & 0 \\
0 & 1 & 12 & 10 & 15 & 8 & 1 & 1 & 8 & 10 & 10 & 15 & 12 & 8 & 12 & 15 & 0 & 0
\end{pmatrix}.$$

Left multiplying by

$$C_\beta = C_4 = \operatorname{diag}\left(1, 1, 1, \begin{pmatrix} 1 & 1 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 5 & 4 \end{pmatrix}\right)$$

yields the check matrix

$$H = C_4 \cdot M = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 6 & 6 & 7 & 7 & 7 & 6 & 1 & 7 & 1 & 6 & 1 & 6 & 7 & 1 & 0 & 1 \\
0 & 1 & 7 & 7 & 6 & 6 & 6 & 7 & 1 & 6 & 1 & 7 & 1 & 7 & 6 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 7 & 7 & 6 & 6 & 6 & 6 & 7 & 7 & 0 & 0 \\
0 & 1 & 7 & 6 & 1 & 0 & 6 & 7 & 0 & 1 & 7 & 6 & 1 & 0 & 6 & 7 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 6 & 6 & 7 & 7 & 7 & 7 & 6 & 6 & 0 & 0 \\
0 & 1 & 1 & 0 & 6 & 7 & 7 & 6 & 1 & 0 & 0 & 1 & 7 & 6 & 6 & 7 & 0 & 0 \\
0 & 0 & 6 & 6 & 7 & 7 & 0 & 0 & 7 & 6 & 6 & 7 & 6 & 7 & 6 & 7 & 0 & 0 \\
0 & 1 & 1 & 7 & 7 & 0 & 1 & 1 & 0 & 7 & 7 & 7 & 1 & 0 & 1 & 7 & 0 & 0
\end{pmatrix}.$$

This matrix can be rewritten over $\mathbb{F}_4$ as

$$H = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 2 & 2 & 3 & 3 & 3 & 2 & 1 & 3 & 1 & 2 & 1 & 2 & 3 & 1 & 0 & 1 \\
0 & 1 & 3 & 3 & 2 & 2 & 2 & 3 & 1 & 2 & 1 & 3 & 1 & 3 & 2 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 3 & 3 & 2 & 2 & 2 & 2 & 3 & 3 & 0 & 0 \\
0 & 1 & 3 & 2 & 1 & 0 & 2 & 3 & 0 & 1 & 3 & 2 & 1 & 0 & 2 & 3 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 2 & 3 & 3 & 3 & 3 & 2 & 2 & 0 & 0 \\
0 & 1 & 1 & 0 & 2 & 3 & 3 & 2 & 1 & 0 & 0 & 1 & 3 & 2 & 2 & 3 & 0 & 0 \\
0 & 0 & 2 & 2 & 3 & 3 & 0 & 0 & 3 & 2 & 2 & 3 & 2 & 3 & 2 & 3 & 0 & 0 \\
0 & 1 & 1 & 3 & 3 & 0 & 1 & 1 & 0 & 3 & 3 & 3 & 1 & 0 & 1 & 3 & 0 & 0
\end{pmatrix},$$

where $2 \hat{=} \eta$ and $3 \hat{=} \eta^2 = \eta + 1$. A generator matrix is

$$G = \begin{pmatrix} 1&0&0&0&0&0&0&1&0&1&0&0&1&1&0&1&2&3 \\ 0&1&0&0&0&0&0&1&0&0&0&1&1&0&1&1&3&2 \\ 0&0&1&0&0&0&0&1&0&3&0&2&0&3&1&3&3&0 \\ 0&0&0&1&0&0&0&1&0&2&0&3&1&3&1&2&2&1 \\ 0&0&0&0&1&0&0&1&0&2&0&2&3&0&2&1&2&0 \\ 0&0&0&0&0&1&0&1&0&3&0&3&0&2&0&2&1&3 \\ 0&0&0&0&0&0&1&1&0&1&0&1&2&3&3&2&3&3 \\ 0&0&0&0&0&0&0&0&1&1&0&0&2&2&3&3&2&2 \\ 0&0&0&0&0&0&0&0&0&0&1&1&3&3&2&2&2&2 \end{pmatrix},$$

This defines a $[18, 9, 8]_4$ optimal code $\mathcal{C}_{18}$, which seems to have been studied first in [18]. It is uniquely determined by its parameters. The minimum distance is larger than predicted by Theorem 1. As described in [18], the code $\mathcal{C}_{18}$ is formally self-dual but not self-dual. This means that the weight enumerator of the code equals the weight enumerator of its dual code but the two codes are not equal. The weight enumerator of $\mathcal{C}_{18}$ and of the dual code $\mathcal{C}_{18}^{\perp}$ is

$$1 + 2754z^8 + 18360z^{10} + 77112z^{12} + 110160z^{14} + 50949z^{16} + 2808z^{18}.$$

The dual code $\mathcal{C}_{18}^{\perp}$ is again an $[18, 9, 8]_4$ code, and we have that $\mathcal{C}_{18}^{\perp} = \phi_2(\mathcal{C}_{18}) \neq \mathcal{C}_{18}$, as pointed out in [18].

The code of length 17 turns out to be a $[17, 8, 8]_4$ code $\mathcal{C}_{17}$ with generator matrix

$$G = \begin{pmatrix} 1&0&0&0&0&0&0&1&0&1&2&2&0&0&3&2&1 \\ 0&1&0&0&0&0&0&1&0&0&1&0&2&3&3&3&1 \\ 0&0&1&0&0&0&0&1&0&3&0&2&0&3&1&3&3 \\ 0&0&0&1&0&0&0&1&0&2&3&0&3&1&0&3&3 \\ 0&0&0&0&1&0&0&1&0&2&0&2&3&0&2&1&2 \\ 0&0&0&0&0&1&0&1&0&3&2&1&1&3&3&1&2 \\ 0&0&0&0&0&0&1&1&0&1&2&3&3&2&0&1&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0 \end{pmatrix}.$$

The weight enumerator of this code is

$$1 + 1530z^8 + 8160z^{10} + 25704z^{12} + 24480z^{14} + 5661z^{16}.$$

line i	a, b, c	j	$\gamma_j \in \mathbb{F}_{64}$
1	$0, 1, 3$	$2, 8$	$12, 10$
2	$0, 1, 6$	$3, 5$	$2, 3$
3	$0, 2, 3$	$6, 7$	$4, 5$
4	$0, 2, 6$	$1, 4$	$8, 3$

Table 6: The $[17, 8, 8]_4$ code $\mathcal{C}_{17}$ as cyclic code

The generator polynomial for the $[17, 8, 6]_4$ BCH-code from Remark 1 is $1 + x^3 + x^4 + x^5 + x^6 + x^9$. The weight enumerator of the BCH-code is

$$1 + 204z^6 + 255z^8 + 1632z^9 + 5508z^{10} + 8568z^{11} + 11526z^{12} + 14280z^{13} \\ +12648z^{14} + 7752z^{15} + 2754z^{16} + 408z^{17}.$$

Since isometric codes have the same weight enumerator, this data shows that the code of Theorem 1 of length 17 is different from the BCH-code of Remark 1. In this case, the code of Theorem 1 is better, since it has minimum distance 8, whereas the BCH-code only has minimum distance 6.

The code $\mathcal{C}_{17}$ is cyclic in 4 different ways. The field $\mathbb{F}_{256} = \mathbb{F}_2(\zeta)$ with $\zeta^8 = \zeta^4 + \zeta^3 + \zeta^2 + 1$ contains the primitive 17-th root of unity $\xi = \zeta^{15}$. The 16-cyclotomic sets modulo 17 are $\{0\}$ and $\{j, 17 - j\}$ for $j = 1, \ldots, 8$. By Lemma 7, $R_1(2, 16) = \Phi(17)/2 = 8$. The 8 irreducible polynomials in $\mathcal{R}_1(2, 16)$ are w_j, $j = 1, \ldots, 8$ with $w_j = (x - \xi^j)(x - \xi^{17-j}) = x^2 + \gamma_j x + 1$. The values of $\gamma_j \in \mathbb{F}_{16}$ are in order: $8, 12, 2, 15, 3, 4, 5, 10$. Let

$$\mathcal{S}_j = \varphi_{0,1,1,\gamma_j} : \; t \mapsto \frac{1}{t + \gamma_j}$$

be the collineation whose associated matrix has characteristic polynomial $w_j(x)$. In Tab. 6, each line $i = 1, \ldots, 4$ corresponds to one way in which $\mathcal{C}_{17}$ is cyclic. More precisely, each line i corresponds to one permutation equivalence π_i which turns $\mathcal{C}_{17}$ into a code $\mathcal{C}_{17}^{\pi_i}$ which is invariant under σ_{17}. The variety of the code $\mathcal{C}_{17}^{\pi_i}$ consists of exactly three 4-cyclotomic sets modulo 17, with representatives a, b, c of lengths $1, 4, 4$, respectively. The table lists all j for which $\mathcal{S}_j$ induces a conjugate of σ_n as cyclic automorphism. In the last column, the middle coefficient $\gamma_j \in \mathbb{F}_{16}$ in $w_j(x)$ is listed.

We wish to work out one case in more detail. Consider the case of $w_1(x) = x^2 + 8x + 1$ (i.e., with $\gamma := \gamma_1 = 9$). In order to create the code $\mathcal{C}_{17}^{\pi_1}$ invariant under σ_{17}, we may take the point $t = 0$ in $\mathrm{PG}(1, 16)$ and apply $\mathcal{S}_1$ successively to the column $h_0^\top$ in the check matrix H. Let H_γ be the 9×17 matrix over $\mathbb{F}_4$ whose columns are $\mathcal{S}_1^j \cdot h_0^\top$ for $j = 0, \ldots, 16$. Since $\mathcal{S}_j = R(0, 1, 1, \gamma, \beta)$, computing the matrix H_γ involves n matrix vector multiplications. In the case of $\gamma = 8$ and $\beta = 4$, we have (with $2 = \eta$ and $3 = \eta^2 \in \mathbb{F}_4$)

$$U(0,1,1,8,4) = \begin{pmatrix} 1&0&1&0&0&1&2&0&0 \\ 1&1&0&0&3&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0 \\ 3&0&0&1&2&0&3&1&0 \\ 3&0&0&1&3&2&0&1&1 \\ 2&0&0&0&0&1&0&0&0 \\ 3&0&0&0&0&1&1&0&0 \\ 3&0&0&1&0&0&0&0&0 \\ 3&0&0&1&1&0&0&0&0 \end{pmatrix}.$$

We obtain

$$H_\gamma = H_8 = \begin{pmatrix} 1&1&3&1&3&2&2&1&1&2&2&3&1&3&1&1&0 \\ 0&1&2&2&2&1&2&3&1&3&2&1&2&2&2&1&0 \\ 0&1&1&3&1&3&2&2&1&1&2&2&3&1&3&1&1 \\ 0&3&0&1&3&2&3&3&0&2&3&1&2&2&0&3&0 \\ 0&3&1&2&0&2&1&1&1&1&2&0&2&1&3&0&0 \\ 0&2&0&1&3&2&1&2&0&2&1&2&3&1&0&2&0 \\ 0&3&2&0&2&3&0&0&1&2&1&1&1&1&2&1&0 \\ 0&3&0&2&2&1&3&2&0&3&3&2&3&1&0&3&0 \\ 0&3&3&3&0&1&1&3&1&2&2&0&3&3&1&0&0 \end{pmatrix},$$

which can be row-reduced to

$$H_8' = \begin{pmatrix} 1&\eta&0&\eta&\eta&\eta&0&\eta&1&0&0&0&0&0&0&0&0 \\ 0&1&\eta&0&\eta&\eta&\eta&0&\eta&1&0&0&0&0&0&0&0 \\ 0&0&1&\eta&0&\eta&\eta&\eta&0&\eta&1&0&0&0&0&0&0 \\ 0&0&0&1&\eta&0&\eta&\eta&\eta&0&\eta&1&0&0&0&0&0 \\ 0&0&0&0&1&\eta&0&\eta&\eta&\eta&0&\eta&1&0&0&0&0 \\ 0&0&0&0&0&1&\eta&0&\eta&\eta&\eta&0&\eta&1&0&0&0 \\ 0&0&0&0&0&0&1&\eta&0&\eta&\eta&\eta&0&\eta&1&0&0 \\ 0&0&0&0&0&0&0&1&\eta&0&\eta&\eta&\eta&0&\eta&1&0 \\ 0&0&0&0&0&0&0&0&1&\eta&0&\eta&\eta&\eta&0&\eta&1 \end{pmatrix},$$

from which we read off

$$h(x) = 1 + \eta x + \eta x^3 + \eta x^4 + \eta x^5 + \eta x^7 + x^8.$$

Computing the reverse of $(x^{17} - 1)/h(x)$ yields the generator polynomial $g(x)$. The roots of $g(x)$ determine the cyclotomic sets from which the cyclic code is composed. The 4-cyclotomic sets modulo 17 are

$$\{0\}, \{1, 4, 16, 13\}, \{2, 8, 15, 9\}, \{3, 12, 14, 5\}, \{6, 7, 11, 10\},$$

which give rise to the following irreducible polynomials over $\mathbb{F}_4$

$$\begin{aligned} m_0 &= x + 1, \\ m_1 &= 1 + \eta^2 x + x^2 + \eta^2 x^3 + x^4, \\ m_2 &= 1 + \eta x + x^2 + \eta x^3 + x^4, \\ m_3 &= 1 + x + \eta x^2 + x^3 + x^4, \\ m_6 &= 1 + x + \eta^2 x^2 + x^3 + x^4. \end{aligned}$$

We find that

$$g(x) = m_0 m_2 m_6 = x^9 + \eta x^8 + \eta^2 x^7 + \eta^2 x^6 + \eta^2 x^3 + \eta^2 x^2 + \eta x + 1.$$

For $q = 8$, we obtain a (non-cyclic) $[66, 57, 6]_8$ code. It is not known if this code is optimal (but at present no better code is known). The best known upper bound for the minimum distance in this case is $d \leq 8$. The dual is a $[66, 9, 48]_8$. We are aware of two other constructions of codes with these parameters. One is due to Maruta [20], the other is by means of the X-construction [22, 19], as described in [11]. We have reason to believe (but no proof!) that the three codes are all isometric. Let us explain in more detail how we come to this conjecture.

Maruta constructs his code from an orbit of length 65 of a certain projective transformation, extended by a single vector. More precisely, he considers the vectors

$$v_i = T_m^i e_0^\top, \; i = 0, \ldots, 64$$

where $e_0 = (1, 0, 0, 0, 0, 0, 0, 0, 0)$ and $v_{65} = (1, 0, 2, 7, 3, 7, 2, 0, 1)$ and T_m is the matrix from (1) for $m(x) = x^9 + x^8 + 2x^7 + 5x^6 + 4x^5 + 4x^4 + 5x^3 + 2x^2 +$

Code	Parameters	8-cyclotomic sets mod 65
$\mathcal{C}_1$	$[1,1,1]_8$	
$\mathcal{C}_2$	$[65,57,5]_8$	$\{3,24,62,41\},\{21,38,44,27\}$
$\mathcal{C}_4$	$[65,56,6]_8$	$\{0\},\{3,24,62,41\},\{21,38,44,27\}$
$\mathcal{C}_3=\mathcal{C}_2^\perp$	$[65,8,48]_8$	negatives of the complement of those of $\mathcal{C}_2$
$\mathcal{C}_5=\mathcal{C}_4^\perp$	$[65,9,47]_8$	negatives of the complement of those of $\mathcal{C}_4$

Table 7: The codes for construction X

$x+1\in\mathbb{F}_8[x]$. Here, the coefficient $i\alpha^2+j\alpha+k\in\mathbb{F}_8$ is represented by the integer $4i+2j+k$ and $\alpha^3=\alpha+1$. Maruta defines his code by means of the matrix whose columns are the $v_i^\top$, $i=0,\dots,65$.

The X-construction is applied to cyclic codes $\mathcal{C}_5$ and $\mathcal{C}_3$, which are duals of (cyclic) codes $\mathcal{C}_4$ and $\mathcal{C}_2$, respectively. Recall that $V(\mathcal{C})$ denotes the variety of a code, which is the set of roots. Since $V(\mathcal{C}_2)\subseteq V(\mathcal{C}_4)$, the code $\mathcal{C}_4$ is a subcode of $\mathcal{C}_2$. Therefore, $\mathcal{C}_3=\mathcal{C}_2^\perp$ is a subcode of $\mathcal{C}_5=\mathcal{C}_4^\perp$ and construction X applies. Using an auxiliary $[1,1,1]_8$ code $\mathcal{C}_1$, a $[66,9,48]_8$ code is constructed (cf. Tab. 7). The generator polynomial $g_i(x)$ for $\mathcal{C}_i$ $i=2,4$ is $g_2(x)=x^8+6x^6+5x^5+7x^4+5x^3+6x^2+1$ and $g_4(x)=x^9+x^8+6x^7+3x^6+2x^5+2x^4+3x^3+6x^2+x+1$. The 8-cyclotomic sets are expressed with respect to the 65-th root of unity β^{63} where β is a root of the primitive polynomial $x^{12}+x^6+x^4+x+1$ and $\alpha=\beta^{585}$.

It turns out that all three codes have the same weight enumerator, the coefficients of which are listed in Tab. 8. This is why we conjecture that all three codes are in fact the same (up to isometry, of course).

Theorem 1 also yields a cyclic $[65,56,6]_8$ code $\mathcal{C}$. The code $\mathcal{C}$ is cyclic in 12 different ways. Let ζ be a primitive element of $\mathbb{F}_{4096}=\mathbb{F}_2(\zeta)$, with $\zeta^{12}=\zeta^6+\zeta^4+\zeta+1$. Then $\mathbb{F}_{64}=\mathbb{F}_2(\alpha)$ where $\alpha=\zeta^{65}$ satisfies $\alpha^6=\alpha^5+1$. By Lemma 7, $R_1(2,64)=\Phi(65)/2=\Phi(5)\Phi(13)/2=4\cdot 12/2=24$. Let $\xi=\zeta^{63}$ be a primitive 65-th root of unity. Let $r_1,\dots,r_{24}$ be the integers between 1 and 65/2 that are prime to 65 as displayed Tab. 9. The pair $\{r_j,65-r_j\}$ forms a 64-cyclotomic set modulo 65 and hence $w_j(x)=(x-\xi^{r_j})(x-\xi^{65-r_j})=x^2+\gamma_jx+1$ is an irreducible polynomial of degree 2 over $\mathbb{F}_{64}$. In fact, $\mathcal{R}_1(2,64)=\{w_1,\dots,w_{24}\}$. Let $\mathcal{S}_j=\varphi_{0,1,1,\gamma_j}$ be the collineation whose associated matrix has characteristic polynomial $w_j(x)$. In Tab. 10,

i	w_i
0	1
48	420420
50	524160
52	4586400
54	13759200
56	34179600
58	32104800
60	35773920
62	11924640
64	522795
66	421792

Table 8: The non-zero coefficients w_i of the weight enumerator of the $[66, 9, 48]_8$ code constructed by Theorem 1

j	r_j	γ_j	j	r_j	γ_j	j	r_j	γ_j	j	r_j	γ_j
1	1	6	7	8	5	13	17	60	19	24	59
2	2	20	8	9	13	14	18	27	20	27	21
3	3	31	9	11	54	15	19	7	21	28	38
4	4	55	10	12	34	16	21	49	22	29	3
5	6	19	11	14	17	17	22	12	23	31	41
6	7	5	12	16	48	18	23	25	24	32	24

Table 9: The polynomials $w_j(x) = x^2 + \gamma_j x + 1$ in $\mathcal{R}_1(2, 64)$

line i	a, b, c	j	$\gamma_j \in \mathbb{F}_{64}$
1	$0, 1, 7$	$4, 24$	$55, 24$
2	$0, 1, 28$	$11, 14$	$17, 27$
3	$0, 2, 7$	$21, 22$	$38, 3$
4	$0, 2, 14$	$1, 7$	$6, 13$
5	$0, 3, 19$	$9, 18$	$54, 25$
6	$0, 3, 21$	$10, 23$	$34, 41$
7	$0, 4, 14$	$6, 8$	$5, 43$
8	$0, 4, 28$	$2, 12$	$20, 48$
9	$0, 6, 11$	$3, 19$	$31, 21$
10	$0, 6, 21$	$15, 17$	$7, 12$
11	$0, 11, 12$	$16, 20$	$49, 21$
12	$0, 12, 19$	$5, 13$	$19, 60$

Table 10: The $[65, 56, 6]_8$ code as cyclic code

each line i corresponds to one way in which $\mathcal{C}$ is cyclic. More precisely, each line i corresponds to one permutation equivalence π_i which turns $\mathcal{C}$ into a code $\mathcal{C}^{\pi_i}$ which is invariant under σ_n. The variety of the code $\mathcal{C}^{\pi_i}$ consists of exactly three 4-cyclotomic sets modulo 65, with representatives a, b, c of lengths $1, 4, 4$, respectively. The table lists all j for which $\mathcal{S}_j$ induces a conjugate of σ_n as cyclic automorphism. In the last column, the middle coefficient $\gamma_j \in \mathbb{F}_{64}$ in $w_j(x)$ is listed.

7 Examples: Theorem 2

A few small examples of codes constructed by Theorem 2 are listed in Tab. 11. The references given in the comments refer to previous constructions of codes with the same parameter set. It does not imply that the codes are isometric.

At the time this paper was first submitted, the $[126, 118, 5]_5$ code seemed to be new. Brouwer's table [6] indicated that only a $[126, 118, 4]_5$ code was known. At the time of editing the paper according to the reviewers remarks, Brouwer's tables were dysfunctional and a new table [11] was put in place. During the final revisions of this paper, the new table indicated that a $[126, 118, 5]_5$ code can be obtained by means of the XX-construction of [1]. Let us present this construction, which is likely due to Grassl. A special

q		parameter	comments
3	code	$[28, 20, 6]_3$	[17], optimal, constacyclic
3	dual code	$[28, 8, 15]_3$	optimal
4	code	$[65, 57, 5]_4$	[9], optimal, cyclic
4	dual code	$[65, 8, 44]_4$	[12], optimal, cyclic
5	code	$[126, 118, 5]_5$	optimal, new, constacyclic
5	dual code	$[126, 8, 95]_5$	optimal
7	code	$[344, 336, 5]_7$	constacyclic
7	dual code	$[344, 8, 287]_7$	

Table 11: The codes of Theorem 2 for small q

code	parameters	5-cyclotomic sets mod 124
$\mathcal{C}_0$	$[124, 118, 4]_5$	$\{38, 66, 82\}, \{89, 73, 117\}$
$\mathcal{C}_1$	$[124, 117, 4]_5$	$\{0\}, \{38, 66, 82\}, \{89, 73, 117\}$
$\mathcal{C}_2$	$[124, 117, 4]_5$	$\{31\}, \{38, 66, 82\}, \{89, 73, 117\}$
$\mathcal{C}_1 \cap \mathcal{C}_2$	$[124, 116, 5]_5$	$\{0\}, \{31\}, \{38, 66, 82\}, \{89, 73, 117\}$

Table 12: The codes for Alltop's construction XX

case of Alltop's construction applies to an $[n, k, d]_q$ code $\mathcal{C}_0$ with subcodes $\mathcal{C}_i$ $[n, k-1, d_i]_q$ $(i = 1, 2)$ such that $\mathcal{C}_1 \cap \mathcal{C}_2$ has minimum distance at least D. It produces a code $\mathcal{C}$ with parameters

$$[n + 2, k, \min\{D, d_1 + 1, d_2 + 1, d + 2\}]_q.$$

We choose $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ cyclic as in Tab. 12 and obtain an $[126, 118, 5]_5$ code $\mathcal{C}$. To verify the statements about the minimum distance, we apply the bounding technique of van Lint / Wilson [24]. This technique applies to a set $S \subseteq \mathbb{F}_{q^m}$, and defines a collection U_S of subsets of $\mathbb{F}_{q^m}$ (that is, U_S is a subset of the power set of $\mathbb{F}_{q^m}$). The collection U_S is defined as follows:

(i) $\emptyset \in U_S$,

(ii) $A \in U_S,\ A \subseteq S$, and $b \in \mathbb{F}_{q^m} \setminus S$ implies $A \cup \{b\} \in U_S$,

(iii) $A \in U_S,\ c \in \mathbb{F}_{q^m}^{\times}$ implies $cA = \{ca \mid a \in A\} \in U_S$.

If $S = V(\mathcal{C})$ is chosen to be the variety of a cyclic code $\mathcal{C}$ and m the order of q modulo n, then van Lint and Wilson prove that the minimum distance

line i	a	b	j	$\gamma_j \in \mathbb{F}_{64}$
1	13	1	$5, 19, 23$	$19, 59, 41$
2	13	6	$8, 11, 22$	$43, 17, 3$
3	13	9	$9, 15, 16$	$54, 7, 49$
4	13	11	$1, 4, 12$	$6, 55, 48$
5	26	2	$3, 10, 13$	$31, 34, 60$
6	26	3	$6, 14, 21$	$5, 27, 38$
7	26	7	$17, 18, 20$	$12, 25, 21$
8	26	22	$2, 7, 24$	$20, 13, 24$

Table 13: The $[65, 57, 5]_4$ code as cyclic code

of $\mathcal{C}$ is bounded from below by the size of the largest member of U_S (those who read German might consult [16] for a nice discussion of the technique with examples). Let us represent 124-th roots of unity by their exponent with respect to a primitive 124-th root of unity $\alpha \in \mathbb{F}_{125}$. Let us write a_i for the mapping $A \mapsto A \cup \{\alpha^i\}$ (a for add) and let us write s_i for the mapping $A \mapsto \alpha^i \cdot A$ (s for shift). Note further that $\mathcal{C}_1 \cap \mathcal{C}_2$ is another cyclic code. If $g_i(x)$ denotes the generator polynomial of $\mathcal{C}_i$, then $\mathcal{C}_1 \cap \mathcal{C}_2$ has generator polynomial $\operatorname{lcm}(g_1(x), g_2(x))$ and its variety is the union of the varieties of $\mathcal{C}_1$ and $\mathcal{C}_2$. Then

$$\begin{aligned} \{1, 38, 66, 89\} &= a_1 s_{-51} a_{16} s_{-28} a_{21} s_{-1} a_{118}(\emptyset) \in U_{V(\mathcal{C}_i)}, \quad i = 0, 1, 2, \\ \{1, 66, 82, 89, 117\} &= a_1 s_{51} a_{15} s_{38} a_{28} s_{-7} a_7 s_{-1} a_1(\emptyset) \in U_{V(\mathcal{C}_1 \cap \mathcal{C}_2)} \end{aligned}$$

show that $\mathcal{C}_0, \mathcal{C}_1$ and $\mathcal{C}_2$ have distance at least 4 and that $\mathcal{C}_1 \cap \mathcal{C}_2$ has distance $D \geq 5$. Thus, a $[126, 118, 5]_5$ code is constructed.

The $[65, 57, 5]_4$ code $\mathcal{C}$ is cyclic in 8 different ways. Let $\mathcal{R}_1(2, 64) = \{w_1, \ldots, w_{24}\}$ as in Tab. 9. In Tab. 13, each line i corresponds to one way in which $\mathcal{C}$ is cyclic. More precisely, each line i corresponds to one permutation equivalence π_i which turns $\mathcal{C}$ into a code $\mathcal{C}^{\pi_i}$ which is invariant under σ_n. The variety of the code $\mathcal{C}^{\pi_i}$ consists of exactly two 4-cyclotomic sets modulo 65, with representatives a and b of lengths 2 and 6, respectively. The table lists all j for which $\mathcal{S}_j$ induces a conjugate of σ_n as cyclic automorphism. In the last column, the middle coefficient $\gamma_j \in \mathbb{F}_{64}$ in $w_j(x)$ is listed.

8 Acknowledgments

The author thanks Tim Penttila for his hospitality during a visit in the southern hemisphere winter of 2006. He also thanks the referee for pointing out connections outlined in Remarks 3-5 and for posing interesting questions, some of which could be answered. The referee also provided many references to places where code constructions could be found. The author also thanks the Editor for encouragement during the revision process. Last but not least, he thanks Andries Brouwer and Markus Grassl for maintaining Internet databases of best known codes which proved to be tremendously helpful.

References

[1] W. O. Alltop. A method of extending binary linear codes. *IEEE Trans. Inform. Theory*, 30:871–872, 1984.

[2] Michael Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[3] Elwyn R. Berlekamp. *Algebraic coding theory*. McGraw-Hill Book Co., New York, 1968.

[4] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann. *Error-Correcting Linear Codes*, volume 18 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006.

[5] Juergen Bierbrauer. *Introduction to coding theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[6] A.E. Brouwer. Linear code bounds. *http://www.win.tue.nl/˜aeb/voorlincod.html* (dysfunctional as of 2007).

[7] Antonio Cossidente and Oliver H. King. Embeddings of finite classical groups over field extensions and their geometry. *Adv. Geom.*, 2(1):13–27, 2002.

[8] Danyo Danev and Jonas Olsson. On a sequence of cyclic codes with minimum distance six. *IEEE Trans. Inform. Theory*, 46(2):673–674, 2000.

[9] Y. Edel. Eine verallgemeinerung von BCH-codes. Ph.D. Thesis, Univ. Heidelberg, 1996.

[10] Yves Edel and Jürgen Bierbrauer. The largest cap in AG$(4,4)$ and its uniqueness. *Des. Codes Cryptogr.*, 29(1-3):99–104, 2003.

[11] Markus Grassl. Code tables: Bounds on the parameters of various types of codes. *http://www.codetables.de/* accessed June 2007.

[12] B. Groneick and S. Grosse. New binary codes. *IEEE Trans. Inform. Theory*, 45:510–512, 1994.

[13] J. W. P. Hirschfeld. Cyclic projectivities in PG(n, q). In *Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo I*, pages 201–211. Atti dei Convegni Lincei, No. 17. Accad. Naz. Lincei, Rome, 1976.

[14] J. W. P. Hirschfeld. *Projective geometries over finite fields.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[15] W. Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes.* Cambridge University Press, Cambridge, 2003.

[16] Dieter Jungnickel. *Codierungstheorie.* Spektrum Akademischer Verlag GmbH, Heidelberg, 1995.

[17] Frank R. Kschischang and Subbarayan Pasupathy. Some ternary and quaternary codes and associated sphere packings. *IEEE Trans. Inform. Theory*, 38(2, part 1):227–246, 1992.

[18] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward. Self-dual codes over GF(4). *J. Combin. Theory Ser. A*, 25(3):288–318, 1978.

[19] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[20] T. Maruta, M. Shinohara, and M. Takenaka. Constructing linear codes from some orbits of projectivities. to appear in Discrete Math.

[21] B. Qvist. Some remarks concerning curves of the second degree in a finite plane. *Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys.*, 1952(134):1–27, 1952.

[22] N. J. A. Sloane, S. M. Reddy, and C. L. Chen. New binary codes. *IEEE Trans. Inform. Theory*, 18:503–510, 1972.

[23] Robert Steinberg. Representations of algebraic groups. *Nagoya Math. J.*, 22:33–56, 1963.

[24] Jacobus H. van Lint and Richard M. Wilson. On the minimum distance of cyclic codes. *IEEE Trans. Inform. Theory*, 32(1):23–40, 1986.