mathematics

MDPI

Article

Extremal Binary and Ternary Codes of Length 60 with an Automorphism of Order 29 and a Generalization

Stefka Bouyuklieva [1], Javier de la Cruz [2,*] and Darwin Villar [3]

[1] Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, 5000 Veliko Tarnovo, Bulgaria; stefka@ts.uni-vt.bg
[2] Departamento de Matemáticas, Universidad del Norte, Km. 5 vía Puerto Colombia, Barranquilla 081007, Colombia
[3] Institute of Mathematics, Statistics and Scientific Computation-IMECC, Universidade Estadual de Campinas-UNICAMP, Campinas 13083856, SP, Brazil; d191649@dac.unicamp.br
* Correspondence: jdelacruz@uninorte.edu.co

Abstract: In this paper, all extremal Type I and Type III codes of length 60 with an automorphism of order 29 are classified up to equivalence. In both cases, it has been proven that there are three inequivalent codes. In addition, a new family of self-dual codes over non-binary fields is presented.

Keywords: self-dual codes; extremal codes; automorphisms

MSC: 94B05; 94B60

Citation: Bouyuklieva, S.; de la Cruz, J.; Villar, D. Extremal Binary and Ternary Codes of Length 60 with an Automorphism of Order 29 and a Generalization. *Mathematics* **2022**, *10*, 748. https://doi.org/10.3390/math10050748

Academic Editor: Patrick Solé

Received: 17 January 2022
Accepted: 9 February 2022
Published: 26 February 2022

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. An $[n,k,d]_q$ code C is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. Let $\cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in $\mathbb{F}_q^n$. The *dual code* of C is $C^\perp := \left\{ u \in \mathbb{F}_q^n : u \cdot v = 0, \ \forall v \in C \right\}$. It is well known that $C^\perp$ is a linear $[n, n-k]$ code. If $C \subseteq C^\perp$, then C is called *self-orthogonal*, and if $C = C^\perp$, then C is called *self-dual*.

There are two types of binary self-dual codes: Type I (or singly-even) codes, which contain codewords of weight $\equiv 2 \pmod 4$, and Type II (or doubly-even) codes, which consist only of codewords with weights divisible by 4. Self-dual ternary codes are also called Type III codes. Type I codes of length n exist for all even positive integers n, while Type II codes exist only for n divisible by 8. Type III codes exist only for lengths a multiple of 4 and only have codewords of Hamming weight a multiple of 3 [1].

Let C be a self-dual code of length n with minimum distance d. By results of Mallows-Sloane [2] and Rains [3], if C is binary, then

$$d \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4 & \text{if } n \not\equiv 22 \bmod 24 \\ 4\lfloor \frac{n}{24} \rfloor + 6 & \text{if } n \equiv 22 \bmod 24, \end{cases}$$

and if C is ternary, then $d \leq 3\lfloor \frac{n}{12} \rfloor + 3$. A self-dual code meeting the respective upper bound is called an *extremal* code. It is worth to mention that for some lengths extremal codes do not exist.

The classification of self-dual codes began in the seventies in the work of Vera Pless [4], where she classified the binary self-dual codes of length $n \leq 20$. In the survey [5] Huffman summarized the classification of all binary self-dual codes of length $n \leq 36$ and ternary self-dual codes of length $n \leq 20$. The Type II codes of length 40 were completely classified by Betsumiya, Harada and Munemasa in [6]. The classification of Type I codes of lengths 38 and 40 was completed in [7,8], respectively. Type III codes of length 24 were fully classified by Harada and Munemasa [9].

For larger lengths, a complete classification seems to be very difficult because of the large number of codes, therefore researchers have attempted to classify those of most interest—the extremal codes. Nevertheless, for length $n > 40$ in the binary and $n > 24$ in the ternary case, only extremal Type I codes of length 46, extremal Type II codes of length 48, and extremal Type III codes of length 28 have been classified [5,10].

At the same time, researchers have tried to classify the extremal codes with additional restrictions, such as finding the extremal codes with a given automorphism. Methods to construct and classify self-dual codes under the assumption that they have an automorphism of a given prime order were developed by Huffman and Yorgov [11–15]. Since then, many extremal self-dual codes of different lengths with different automorphisms were classified.

Our idea is to study extremal self-dual codes of the same length invariant under the same permutation, but over different fields, in our case $\mathbb{F}_2$ and $\mathbb{F}_3$. Therefore, we need a length for which both extremal Type I and Type III codes exist, and moreover, some of these codes share the same automorphism. For $n = 60$, extremal binary and ternary codes with automorphisms of order 29 exist, so we focus on this length.

In Section 2, we describe the structure of a self-dual code with an automorphism of prime order $p \neq \mathrm{char}(\mathbb{F}_q)$, and generalize some results established in [14,15]. The classification of extremal binary and ternary self-dual codes of length 60 with an automorphism of order 29 is given in Section 3. Finally, in Section 4, a general construction of self-dual codes invariant under the group $SL_2(p)$, where p is a prime so that $p \equiv 5 \pmod 8$, is presented. This leads to a new family of codes, which includes the new extremal $[60, 30, 18]$ Type III code $\mathcal{V}_3(29)$.

2. Automorphisms of Self-Dual Codes

The most general definition for equivalence of linear codes of length n over the finite field $\mathbb{F}_q$ is based on the action of the semilinear isometries group $\mathcal{M}_n^*(q) = \mathrm{Mon}_n(\mathbb{F}_q^*) \rtimes \mathrm{Aut}(\mathbb{F}_q) \leq \Gamma_n(\mathbb{F}_q)$ on the vector space $\mathbb{F}_q^n$, where $\Gamma_n(\mathbb{F}_q)$ is the set of all semilinear mappings, i.e., the general semilinear group, $\mathrm{Mon}_n(\mathbb{F}_q^*)$ is the group of all monomial $n \times n$ matrices over $\mathbb{F}_q$, and $\mathrm{Aut}(\mathbb{F}_q)$ is the automorphisms group of the field $\mathbb{F}_q$.

Linear q-ary codes C and C' of the same length n are equivalent whenever $C' = CT$ for some $T \in \mathcal{M}_n^*(q)$. If $CT = C$ for an element $T \in \mathcal{M}_n^*(q)$ then T is called an automorphism of the code. The set of all automorphisms of C form a group denoted by $\mathrm{Aut}(C)$.

Any element $T \in \mathcal{M}_n^*(q)$ can be written as $T = PD\tau$ where P is a permutation matrix (permutation part), D is a diagonal matrix (diagonal part), and $\tau \in \mathrm{Aut}(\mathbb{F}_q)$. Note that in the case of prime q, $\mathcal{M}_n^*(q) = \mathrm{Mon}_n(\mathbb{F}_q^*)$, and if $q = 2$ then $\mathcal{M}_n^*(q) \cong \mathrm{Sym}(n)$ where $\mathrm{Sym}(n)$ is the symmetric group of degree n. The following lemma implies that in some cases, when considering automorphisms of prime order, we only need to examine permutation automorphisms.

Lemma 1 ([13]). *Let C be a linear code over $\mathbb{F}_q$ with an automorphism $T = PD\tau$ of prime order p where $p \nmid (q-1)$ and $p \nmid |\mathrm{Aut}(\mathbb{F}_q)|$. Then there exists a code C' equivalent to C where $P \in \mathrm{Aut}(C')$.*

We consider codes over $\mathbb{F}_2$ and $\mathbb{F}_3$ having an automorphism of prime order $p > 3$. For these fields p satisfies the conditions from Lemma 1 and therefore we can use only permutation automorphisms of order p. So instead of the action of the group $\mathcal{M}_n^*(q)$, we use the action of the symmetric group $\mathrm{Sym}(n)$ on $\mathbb{F}_q^n$ defined by $v\sigma := (v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(n)})$, where $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ and $\sigma \in \mathrm{Sym}(n)$.

Let $C \leq \mathbb{F}_q^n$ be a linear code with a permutation automorphism $\sigma \in \mathrm{Sym}(n)$ of order r (not necessarily prime) with c cycles of length r and f fixed points. In this case, we say that σ is of type r-(c, f). Without loss of generality we can assume that

$$\sigma = \Omega_1 \ldots \Omega_c \Omega_{c+1} \ldots \Omega_{c+f} \tag{1}$$

where $\Omega_i = ((i-1)r+1,\ldots,ir), i = 1,\ldots,c$, are the cycles of length r, and $\Omega_{c+i} = (cr+i), i = 1,\ldots,f$, are the fixed points. Obviously, $cr+f = n$.

We put

$$F_\sigma(C) := \{v \in C \mid v\sigma = v\}$$

and

$$E_\sigma(C) := \{v \in C : \sum_{i\in\Omega_j} v_i = 0 \text{ for all } j = 1,\ldots,c+f\}.$$

The Euclidean inner product over the field $\mathbb{F}_q$ is defined by

$$u \cdot v = \sum_{i=1}^{n} u_i v_i, \quad u = (u_1,\ldots,u_n), v = (v_1,\ldots,v_n) \in \mathbb{F}_q^n. \tag{2}$$

The following theorem gives a very important decomposition of the linear code C.

Theorem 1 ([11]). *Let $C \leq \mathbb{F}_q^n$ be a linear code with a permutation automorphism $\sigma \in \mathrm{Sym}(n)$ of order r such that $char(\mathbb{F}_q) \nmid r$. Then the following hold.*

(i) *$C = F_\sigma(C) \oplus E_\sigma(C)$. Both $F_\sigma(C)$ and $E_\sigma(C)$ are σ-invariant.*

(ii) *If C is self-dual under the inner product (2), then*

$$\dim(F_\sigma(C)) = \frac{c+f}{2}, \quad \dim(E_\sigma(C)) = \frac{c(r-1)}{2}.$$

Note that $v \in F_\sigma(C)$ if and only if $v \in C$ and $v\mid_{\Omega_j}$ is constant for $j = 1,\ldots,c+f$. This allows us to define the map $\pi : F_\sigma(C) \to \mathbb{F}_q^{c+f}$ by $(\pi(v))_j = v_i$ for some $i \in \Omega_j$, $j = 1,2,\ldots,c+f, v \in F_\sigma(C)$.

Theorem 2 ([11,16]). *Assume C is a self-dual $[n,n/2,d]_q$ code under the inner product (2). Then $C_\pi = \pi(F_\sigma(C))$ is a $[c+f,(c+f)/2,d_\pi]_q$ self-dual code with respect to the inner product*

$$u \cdot v = \sum_{i=1}^{c} r u_i v_i + \sum_{i=c+1}^{c+f} u_i v_i. \tag{3}$$

If either $r \equiv 1 \pmod{char(\mathbb{F}_q)}$ or $f = 0$, C_π is self-dual under (2).

For the rest of this section, we assume that σ is a permutation automorphism of C of prime order $p \neq \mathrm{char}(\mathbb{F}_q)$. If $\mathrm{ord}_p(q) = p-1$, where $\mathrm{ord}_p(q)$ is the multiplicative order of q modulo p, then the polynomial $1+x+\cdots+x^{p-1}$ is irreducible over the field $\mathbb{F}_q$. Let $\mathcal{P}$ be the principal ideal of $\mathcal{R}_p = \mathbb{F}_q[x]/(x^p-1)$ generated by the polynomial $(1-x)$. Obviously, $\mathcal{P} = \{v(x) \in \mathcal{R}_p : \sum_{i=0}^{p-1} v_i = 0\}$. The following result generalizes Lemma 4 of [12].

Lemma 2 ([11]). *If $1+x+x^2+\cdots+x^{p-1}$ is irreducible over $\mathbb{F}_q$, then $\mathcal{P}$ is a finite field with q^{p-1} elements. The identity is $(-1/p)((1-p)+x+x^2+\cdots+x^{p-1})$. Multiplication by $(-1/p)(1+(1-p)x+x^2+\cdots+x^{p-1})$ in $\mathcal{P}$ corresponds to multiplication by x modulo (x^p-1).*

Let $E_\sigma(C)^*$ denote the code $E_\sigma(C)$ without the last f coordinates. For $v \in E_\sigma(C)^*$ we identify $v\mid_{\Omega_j} = (v_0,v_1,\ldots,v_{p-1})$ with the polynomial $v_0+v_1x+\cdots+v_{p-1}x^{p-1}$ from $\mathcal{P} \subset \mathcal{R}_p$. Thus, we obtain the map $\varphi : E_\sigma(C)^* \longrightarrow P^c$. Results in [12,14] show that if $q = 2$ and p is prime, $C_\varphi = \varphi(E_\sigma(C)^*)$ is self-dual with respect to a given inner product. Huffman generalized this in the following theorem.

Theorem 3 ([11]). *Assume that C is a self-dual $[n, n/2, d]$ code under (2) and that $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbb{F}_q$. Suppose that there is a nonnegative integer t such that $q^t \equiv -1 \pmod{p}$. Then C_φ is a $[c, c/2, d']$ self-dual code over $\mathcal{P}$ under the inner product $\langle \cdot, \cdot \rangle$ given by*

$$\langle u, v \rangle = \sum_{i=1}^{c} u_i v_i^{q^t}, \tag{4}$$

where $u = (u_1, \ldots, u_c)$, $v = (v_1, \ldots, v_c) \in \mathcal{P}^c$.

On $\mathcal{P}^c$, we can use the Hermitian inner product, defined in [17]: for $u = (u_1, \ldots, u_c)$ and $v = (v_1, \ldots, u_c)$

$$u \cdot v = \sum_{i=1}^{c} u_i \overline{v_i}, \tag{5}$$

where $\overline{v_i} = v_i(x^{-1}) = v_i(x^{p-1})$.

Remark 1. *In the last theorem note that $v_i(x^{-1}) = v_i(x^{q^t}) = v_i(x)^{q^t}$. Therefore, the Hermitian product (5) is equivalent to*

$$u \cdot v = \sum_{i=1}^{c} u_i v_i^{q^t}.$$

Moreover, if $\mathrm{ord}_p(q) = p - 1$ and $p \neq 2$, then $q^{\frac{p-1}{2}} \equiv -1 \mod p$. Therefore we can take $t = \frac{p-1}{2}$.

The following theorem is an immediate generalization of (Theorem 3) in [14] .

Theorem 4. *Let $C \leq \mathbb{F}_q^n$ be a linear code with an automorphism σ of prime order $p \neq char(\mathbb{F}_q)$. Suppose that $\mathrm{ord}_p(q) = p - 1$ and there is a nonnegative integer t such that $q^t \equiv -1 \pmod{p}$. Then C is a self-dual code under (2) if and only if the following two conditions hold:*

(i) $\pi(F_\sigma(C))$ is a self-dual code of length $c + f$ under the inner product (3).
(ii) $\varphi(E_\sigma(C)^*)$ is a self-dual code of length c over the field P under the inner product (4).

Proof. Assume that C is self-dual. Conditions (i) and (ii) follow from Lemma 2 and Theorem 3, respectively. Reciprocally, assume (i) and (ii). In this case, $\dim_{\mathbb{F}_q}(\pi(F_\sigma(C))) = \frac{c+f}{2}$ and $\dim_p(\varphi(E_\sigma(C)^*)) = \frac{c}{2}$. Therefore $\dim_{\mathbb{F}_q}(E_\sigma(C)) = \dim_{\mathbb{F}_q}(\varphi(E_\sigma(C)^*)) = (p-1)\frac{c}{2}$. Since $C = F_\sigma(C) \oplus E_\sigma(C)$, then $\dim_{\mathbb{F}_q}(C) = \frac{(c+f)}{2} + \frac{c(p-1)}{2} = \frac{(cp+f)}{2} = \frac{n}{2}$. Now let's prove that $C \leq C^\perp$. Since $F_\sigma(C) \perp E_\sigma(C)$, it is sufficient to prove that $F_\sigma(C)$ and $E_\sigma(C)$ are self-orthogonal. For $F_\sigma(C)$ the statement is trivial.

Let $a(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{p-1}x^{p-1}$, $b(x) = \beta_0 + \beta_1 x + \cdots + \beta_{p-1}x^{p-1} \in \mathcal{P}$. If $a = (\alpha_0, \ldots, \alpha_{p-1})$ and $b = (\beta_0, \ldots, \beta_{p-1})$, then

$$\begin{aligned} a(x)b(x^{-1}) &= (\alpha_0 + \cdots + \alpha_{p-1}x^{p-1})(\beta_0 + \beta_1 x^{p-1} + \cdots + \beta_{p-1}x) \\ &= a \cdot b + (a \cdot (b\sigma))x + \cdots + (a \cdot (b\sigma^{p-1}))x^{p-1}. \end{aligned}$$

For $u = (u_1(x), \ldots, u_c(x))$, $v = (v_1(x), \ldots, v_c(x)) \in \mathcal{P}^c$ we have

$$\begin{aligned} \sum_{i=1}^{c} u_i(x)v_i(x^{-1}) = \sum_{i=1}^{c} u_i \cdot v_i + (\sum_{i=1}^{c} u_i \cdot (v_i\sigma))x + \cdots \\ + (\sum_{i=1}^{c} u_i \cdot (v_i\sigma^{p-1}))x^{p-1}. \end{aligned}$$

Suppose that C_φ is a self-dual code with respect to the Hermitian inner product (4). If $u, v \in C_\varphi$, then

$$0 = \langle u, v \rangle = \sum_{i=1}^{c} u_i(x) v_i(x^{-1}) = \sum_{i=1}^{c} u_i \cdot v_i + (\sum_{i=1}^{c} u_i \cdot (v_i\sigma))x + \cdots + (\sum_{i=1}^{c} u_i \cdot (v_i\sigma^{p-1}))x^{p-1}.$$

It turns out that

$$\sum_{i=1}^{c} u_i \cdot v_i = \sum_{i=1}^{c} u_i \cdot (v_i\sigma) = \cdots = \sum_{i=1}^{c} u_i \cdot (v_i\sigma^{p-1}) = 0.$$

If $u_i(x) = u_{i0} + \cdots + u_{i,p-1}x^{p-1}$, $v_i(x) = v_{i0} + \cdots + v_{i,p-1}x^{p-1}$, $i = 1, \ldots, c$, and $u' = (u_{00}, \ldots, u_{c,p-1}) \in \mathbb{F}_q^{pc}$, $v' = (v_{00}, \ldots, v_{c,p-1}) \in \mathbb{F}_q^{pc}$, then $u', v' \in E_\sigma(C)^*$ and

$$u' \cdot v' = \sum_{i=1}^{c} \sum_{j=0}^{p-1} u_{ij} v_{ij} = \sum_{i=1}^{c} u_i \cdot v_i = 0.$$

Hence the codewords of $E_\sigma(C)^*$ are orthogonal to each other and the code is self-orthogonal. □

The following result is a generalization of (Theorem 3) in [15].

Theorem 5. *Let C and C' be self-dual codes in $\mathbb{F}_q^n$ and let $\sigma \in PAut(C)$ of prime order $p \neq char(\mathbb{F}_q)$. A sufficient condition for equivalence of C and C' with $\sigma \in PAut(C')$ is that C' can be obtained from C by*

(i) a substitution $x \longmapsto x^t$ in $\varphi(E_\sigma(C)^*)$ where t is an integer with $1 \leq t \leq p-1$;
(ii) a multiplication of the j-th coordinate of $\varphi(E_\sigma(C)^*)$ by x^{t_j} where t_j is an integer with $0 \leq t_j \leq p-1$ and $j = 1, \ldots, c$;
(iii) permutation of the first c cycles of C;
(iv) permutation of the last f coordinates of C.

3. Extremal Type I and Type III Codes of Length 60 with an Automorphism of Order 29

In this section we apply the results established in the previous section to give a classification of all extremal Type I and Type III codes of length 60 with an automorphism of order 29.

The weight enumerator $W(y)$ of a code C is given by $W(y) = \sum_{i=0}^{n} A_i y^i$ where A_i is the number of codewords of weight i in C.

The possible weight enumerators of the extremal $[60, 30, 12]$ Type I codes were calculated in [18], namely

$$W_1(y) = 1 + (2555 + 64\beta)y^{12} + (33600 - 384\beta)y^{14} + \cdots$$

for $0 \leq \beta \leq 10$ and

$$W_2(y) = 1 + 3451y^{12} + 24128y^{14} + \cdots$$

Extremal Type I codes with weight enumerator $W_1(y)$ for $\beta = 0, 1, 5, 7$ and 10, were constructed in [18–22], respectively. An extremal Type I with weight enumerator $W_2(y)$ was given in [23]. Recently, Harada presented a classification of four-circulant $[60, 30, 12]$ Type I codes and obtained codes with weight enumerator $W_1(y)$ for $\beta = 2$ and 6 [24].

Regarding the extremal $[60, 30, 18]$ Type III codes, two codes are known so far: the extended quadratic residue code $\mathcal{XQR}(59)$ and the Pless doubly circulant (or symmetry) code $\mathcal{P}(59)$ [25,26]. A construction method of unimodular lattices from extremal Type III codes has been presented in [27]. For instance, an extremal odd unimodular lattice has been constructed from the extended quadratic residue code $\mathcal{XQR}(59)$.

Let C be a binary or ternary self-dual $[60, 30, d > 2]$ code with a permutation automorphism

$$\sigma = (1, 2, \ldots, 29)(30, 31, \ldots, 58). \tag{6}$$

By Lemma 2, $\pi(F_\sigma(C))$ is a self-dual $[4, 2, 2]$ code over $\mathbb{F}_2$ or $\mathbb{F}_3$, respectively, with respect to the inner product (3). Thus,

$$\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \end{array}\right),$$

where $\mathbf{1}$ is the all-ones vector and $\mathbf{0}$ the zero-vector of length 29.

Next we determine $E_\sigma(C)$. Note that $\mathrm{ord}_{29}(q) = 28$ and $q^{14} \equiv -1 \pmod{29}$ for $q = 2$ and $q = 3$. Thus, by Theorem 4, $C_\varphi = \varphi(E_\sigma(C)^*)$ is a self dual $[2, 1]$ code over the field $\mathcal{P} = \mathbb{F}_{q^{28}}$ under the Hermitian product

$$\langle u, v \rangle = u_1(x)v_1(x)^{q^{14}} + u_2(x)v_2(x)^{q^{14}}.$$

According to Lemma 2, the identity element of $\mathcal{P}$ is $e_2(x) = x + x^2 + \cdots + x^{28}$ for $q = 2$, and $e_3(x) = 2 + x + x^2 + \cdots + x^{28}$ for $q = 3$. Because of the orthogonality, the weight of all nonzero codewords in C_φ is equal to 2. Hence, $\mathrm{gen}(C_\varphi) = (e(x), a(x))$, where $0 \neq a(x) \in \mathcal{P}$, and $e(x)$ is the identity of $\mathcal{P}$. If α is a primitive element of the field $\mathcal{P}$, then we have $a(x) = \alpha(x)^t$ for some t with $0 \leq t \leq q^{28} - 2$. Due to the orthogonality we get

$$\langle (e(x), a(x)), (e(x), a(x)) \rangle = e(x) + a(x)^{q^{14}+1} = e(x) + \alpha(x)^{(q^{14}+1)t} = 0.$$

Then $\alpha(x)^{(q^{14}+1)t} = -e(x)$. Since the order of α is $q^{28} - 1$, we have $t = (2^{14} - 1)k$ in the binary case, $0 \leq k \leq 2^{14}$, and $t = \frac{3^{14}-1}{2}k$ in the ternary case, $0 \leq k \leq 2.3^{14} + 1$ with k an odd integer. Let $\delta = \alpha^{2^{14}-1}$ in the binary case, and $\delta = \alpha^{(3^{14}-1)/2}$ in the ternary case, respectively. It follows that $\mathrm{gen}(C_\varphi) = (e(x), \delta^k)$.

Let $c(x) \in \mathcal{P}$, $c(x) = c_0 + c_1 + \cdots + c_{28}x^{28}$. Denote by $[c(x)]$ the 28×29 circulant matrix with first row $(c_0, c_1, \ldots, c_{28})$. From the considered generator matrix of the code C_φ we obtain $\mathrm{gen}(E_\sigma(C)^*) = ([e(x)], [\delta^k])$. So we proved the following lemma.

Lemma 3. *Let C be a self-dual $[60, 30, d > 2]_q$ code, $q = 2$ or 3, with a permutation automorphism of type 29-$(2, 2)$. Let α be a primitive element of the field $\mathcal{P}$, and e be its identity element. Then the code C has a generator matrix in the form*

$$A = \left(\begin{array}{cc|cc} \boldsymbol{1} & \boldsymbol{0} & 1 & 0 \\ \boldsymbol{0} & \boldsymbol{1} & 0 & 1 \\ \hline [e(x)] & [\delta^k] & 0 & 0 \end{array}\right), \tag{7}$$

where $\delta = \alpha^{(q^{14}-1)/(q-1)}$, $0 \leq k \leq (q-1)q^{14} + q - 2$.

We use Lemma 3 to prove the main theorems of this section.

Theorem 6. *There are exactly three nonequivalent extremal $[60, 30, 12]$ Type I codes with an automorphism of order 29.*

Proof. Note that in this case $\mathcal{P}$ is a field with $2^{28} - 1$ elements and $\delta \in \mathcal{P}$ is an element of order $2^{14} + 1 = 5 \times 29 \times 113$. The element $xe(x)$ of order 29 belongs to the cyclic group $\langle \delta \rangle$. Since 29 and $5 \times 113 = 565$ are relatively prime, each element of $\langle \delta \rangle$ can be written in the form $x^s\theta^k$, where $\theta \in \langle \delta \rangle$ has order 565. According to Theorem 5, the vectors $(e(x), a(x))$ and $(e(x), xa(x))$ generate equivalent codes and therefore we can consider only the elements $a(x) = \theta^k$ for $0 \leq k \leq 564$.

It is known that the operation $k \longmapsto 2k$ defines a partition of $\mathbb{Z}_{565}$ into orbits $\mathrm{orb}(k) = \{2^n \cdot k \mod 565 \mid n \in \mathbb{Z}\}$, where $k \in \mathbb{Z}_{565}$. Observe, by Lemma 5 (ii), that for all $j \in \mathrm{orb}(k)$ the corresponding codes C are equivalent. A calculation in MAGMA [28] shows that there are exactly 21 orbits, whose representatives are

$$\{1, 3, 5, 7, 9, 13, 15, 17, 19, 23, 25, 27, 29, 39, 41, 45, 47, 49, 51, 81, 113\}.$$

By Lemma 3 (i) we only have to consider generator matrices

$$\mathrm{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [e(x)] & [\alpha(x)^{(2^{14}-1)k}] & 0 & 0 \end{array}\right),$$

where k runs through the representatives of the 21 orbits. With MAGMA one easily checks that for each

$$k' \in \{1, 7, 9, 13, 17, 19, 23, 25, 27, 29, 39, 41, 45, 47, 49, 51, 81, 113\}$$

there is a codeword of weight smaller than 12. However, for 3, 5 and 15 the codes C are extremal, $|\mathrm{Aut}(C)| = 58$ and the weight enumerator is given by

$$\begin{aligned} W_C(y) =& 1 + 3451y^{12} + 24128^{14} + 336081y^{16} + 1469952y^{18} + 8556856y^{20} + \\ & 24907520y^{22} + 68747400y^{24} + 130023936y^{26} + 190791667y^{28} \\ & + 224019840y^{30} + 190791667y^{32} + 130023936y^{34} + 68747400^{36} \\ & + 24907520y^{38} + 8556856y^{40} + 1469952y^{42} + 336081y^{44} + 24128^{46} \\ & + 3451y^{48} + y^{60}. \end{aligned}$$

In addition we know that

$$\begin{aligned} W_{C_1}(y) =& y^2 + 319^{10} + 39672y^{14} + 1981309y^{18} + \cdots \\ W_{C_3}(y) =& 24128y^{14} + 1469952y^{18} + \cdots, \end{aligned}$$

where $S = C_1 \cup C_3$ is the shadow of C. □

Remark 2. *These three codes were constructed in [29] as bordered double-circulant self-dual codes.*

By [2] it is known that the weight enumerator of an extremal $[60, 30, 18]$ Type III code C is given by

$$W_C(y) = \sum_{j=0}^{60} A_j y^j = \sum_{i=0}^{5} a_i f(y)^{15-3i} g(y)^i,$$

where $f(y) = 1 + 8y^3$, $g(y) = y^3(1 - y^3)^3$ and $a_i \in \mathbb{Z}$. A simple calculation shows that $a_0 = 1$, $a_1 = -120$, $a_2 = 4440$, $a_3 = -53320$, $a_4 = 140760$ and $a_5 = -41184$. Therefore, the weight enumerator is uniquely determined and is given by

$$\begin{aligned}
A_{18} &= 3901080\\
A_{21} &= 241456320\\
A_{24} &= 8824242960\\
A_{27} &= 172074038080\\
A_{30} &= 1850359081824\\
A_{33} &= 11014750094040\\
A_{36} &= 36099369380880\\
A_{39} &= 63958467767040\\
A_{42} &= 59278900150800\\
A_{45} &= 27270640178880\\
A_{48} &= 5739257192760\\
A_{51} &= 485029078560\\
A_{54} &= 13144038880\\
A_{57} &= 71451360\\
A_{60} &= 41184
\end{aligned}$$

Theorem 7. *There are exactly three nonequivalent extremal [60,30,18] Type III codes with an automorphism of order $p = 29$.*

Proof. There are two possible types for a permutation automorphism of order 29, either 29-$(1, 31)$ or 29-$(2, 2)$. For the first case, we have that $E_\sigma(C)^*$ is a $[29, 14, d']$ ternary code with $d' \geq 18$. However, by the Singleton bound (see Theorem 2.4.1 in [1]) such a code does not exist and the type of σ is 29-$(2, 2)$. Similarly as in the binary case, we reduce the number of possibilities for the generating matrix (7). Now $\mathcal{P}$ is a field with $3^{28} - 1$ elements and $\delta \in \mathcal{P}$ is an element of order $2(3^{14} + 1) = 29 \times 329860$. As in the binary case, the element $xe(x)$ of order 29 belongs to the cyclic group $\langle\delta\rangle$, and $\gcd(29, 329860) = 1$, so each element of $\langle\delta\rangle$ can be written in the form $x^s\theta^k$, where $\theta \in \langle\delta\rangle$ has order 329860. According to Theorem 5, we can consider only the elements $a(x) = \theta^k$ for $0 \leq k \leq 329859$. The transformation $k \longmapsto 3k$ divides the set $\mathbb{Z}_{329860}$ in 11786 orbits $\mathrm{orb}(k)$, of which only 5893 correspond to odd integers k. With MAGMA we have checked that only the values 1031, 2261, 82465, 16493 and 181423 lead to an extremal code. More precisely, we found that the values 181423 and 16493 corresponding to a new code, which we denote by $\mathcal{V}_3(29)$. The codes corresponding to 2261 and 1031 are equivalent to $\mathcal{XQR}$ and the code associated to 82465 is $\mathcal{P}(29)$. Using MAGMA one gets the automorphism groups:

- $\mathrm{Aut}(\mathcal{V}_3(29)) = \mathrm{SL}_2(29)$, $|\mathrm{Aut}(\mathcal{V}_3(29))| = 24360 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29$
- $\mathrm{Aut}(\mathcal{XQR}(59)) = \mathrm{SL}_2(59)$, $|\mathrm{Aut}(\mathcal{XQR}(59))| = 205320 = 2^3 \cdot 3 \cdot 5 \cdot 29 \cdot 59$
- $\mathrm{Aut}(\mathcal{P}(29)) = 2.(\mathrm{PSL}_2(59) \times C_4)$, $|\mathrm{Aut}(\mathcal{P}(29))| = 97440 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 29$.

□

Remark 3. *The primitive elements used in Theorems 6 and 7 have the following coefficients*

$$[0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$

and

$$[0, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1],$$

respectively.

4. Generalized Construction from $\mathcal{V}_3(29)$

In this section, we shall show that the new extremal Type III code $\mathcal{V}_3(29)$ obtained in Theorem 7 belongs to a family of invariant codes under $\mathrm{SL}_2(p)$, for $p - 1 \equiv 4 \pmod 8$

and $\mathrm{char}(\mathbb{F}_q) \neq 2$. We give here an extended and more detailed version of the construction presented briefly in [30]. This technique has been applied for permutational representations in (Chapter II.12) in [31] and for monomial representations by Muller in (Section I.1) in [32]. In order to describe the construction, we introduce some definitions.

Since a monomial matrix M can be written in the form $P(\sigma)D$, where D is a diagonal matrix and $P(\sigma)$ is the permutation matrix associated to the permutation σ, then $\mathrm{Mon}_n(\mathbb{F}_q^*) \cong (\mathbb{F}_q^*)^n \rtimes \mathrm{Sym}(n)$, where $(\mathbb{F}_q^*)^n$ denotes the group of all diagonal $n \times n$ matrices. The action of $\mathrm{Mon}_n(\mathbb{F}_q^*)$ on $\mathbb{F}_q^n$ is given in the following way:

$$(\mathbb{F}_q^*)^n \rtimes \mathrm{Sym}(n) \longrightarrow \mathbb{F}_q^n : ((D, P(\sigma)), v) \longmapsto (v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(n)})D.$$

For any subgroup $S \leq \mathbb{F}_q^*$ we define $\mathrm{Mon}_n(S) := S^n \rtimes \mathrm{Sym}(n)$ to be the subgroup of monomial matrices having all non-zero entries in S. Note that there is a natural epimorphism $\pi : \mathrm{Mon}_n(S) \longrightarrow \mathrm{Sym}(n)$ mapping any monomial matrix to the associated permutation.

A linear $\mathbb{F}_q$-representation $\Delta : G \longrightarrow \mathrm{GL}_n(\mathbb{F}_q)$ of a group G is called *monomial*, if its image $\Delta(G)$ is conjugate in $\mathrm{GL}_n(\mathbb{F}_q)$ for some subgroup N of $\mathrm{Mon}_n(\mathbb{F}_q^*)$, or in other words there exists a basis with respect to which $\Delta(g)$ is a monomial matrix for every $g \in G$, i.e., a matrix with exactly one non-zero entry in every row and column. If, in addition, $\pi(\Delta(G))$ is a transitive subgroup of $\mathrm{Sym}(n)$, the monomial representation is *transitive*.

In the following we present a technique to obtain Δ by inducing up a degree 1 representation of H. Let H be a subgroup of G of index $n := [G : H]$. Consider the decomposition of G into H-double cosets with representatives $g_1, \ldots, g_m \in G$ such that

$$G = \dot{\bigcup}_{\ell=1}^{m} Hg_\ell H$$

and also for every $l \in \{1, \ldots, m\}$ put

$$H_\ell := H \cap g_\ell H g_\ell^{-1} \leq H.$$

Choose some right transversal of H_ℓ in H, say $h_{\ell,j}$ of H_ℓ in H, so that $h_{\ell,1} = 1$ and $H = \dot{\bigcup}_{j=1}^{k_\ell} H_\ell h_{\ell,j}$. Hence, we can decompose $Hg_\ell H$ into right H-cosets as

$$Hg_\ell H = \dot{\bigcup}_{j=1}^{k_\ell} Hg_\ell h_{\ell,j}$$

and in consequence also G can be decomposed into right H-cosets as

$$G = \dot{\bigcup}_{\ell=1}^{m} \dot{\bigcup}_{j=1}^{k_\ell} Hg_\ell h_{\ell,j},$$

with a right transversal $\{g_\ell h_{\ell,j} \mid \ell = 1, \ldots, m, k = 1, \ldots, k_\ell\}$, a set of cardinality n which will be used as an index set for the $n \times n$-matrices.

For a group homomorphism $\lambda : H \longrightarrow \mathbb{F}_q^*$ the associated *monomial representation* of G is $\Delta := \lambda_H^G : G \longrightarrow \mathrm{Mon}_n(\lambda(H))$ defined by

$$(\lambda_H^G(g))_{g_\ell h_{\ell j}, g_{\ell'} h_{\ell', j'}} = \begin{cases} 0 & \text{if } g_\ell h_{\ell j} g (g_{\ell'} h_{\ell', j'})^{-1} \notin H \\ \lambda(g_\ell h_{\ell j} g (g_{\ell'} h_{\ell', j'})^{-1}) & \text{if } g_\ell h_{\ell j} g (g_{\ell'} h_{\ell', j'})^{-1} \in H \end{cases}.$$

The representation λ restricts in two obvious ways to a representation of H_ℓ:

$$\lambda_\ell : H_\ell \longrightarrow \mathbb{F}_q^*, h \mapsto \lambda(h)$$

and

$$\lambda_\ell^{g_\ell} : H_\ell \longrightarrow \mathbb{F}_q^*, h \mapsto \lambda(g_\ell h g_\ell^{-1}).$$

Let $\mathcal{I} := \{\ell \in \{1,\ldots,m\} \mid \lambda_\ell = \lambda_\ell^{g_\ell}\}$ be the set of indexes ℓ for which both representations of H_ℓ coincide and reorder the double coset representatives so that $\mathcal{I} = \{1,\ldots,d\}$. Then the *endomorphism ring*

$$\mathrm{End}(\Delta) := \{X \in \mathbb{F}_q^{n\times n} : X\Delta(g) = \Delta(g)X \text{ for all } g \in G\}$$

has dimension d and as in (Theorem 1.8) in [32] the *Schur basis* of $\mathrm{End}(\Delta)$ is $(B_1 = I_n, B_2, \ldots, B_d)$, where $(B_\ell)_{1,g_\ell} = 1$ and $(B_\ell)_{1,g_k h_{k,i}} \neq 0$ if and only if $\ell = k$. As $\Delta(h_{\ell,k})B_\ell = B_\ell\Delta(h_{\ell,k})$ this means

$$\lambda(h_{\ell,k})(B_\ell)_{1,g_\ell h_{\ell,j}} = \Delta(h_{\ell,k})_{g_\ell,g_\ell h_{\ell,j}} = \lambda(h_{\ell,k})\lambda(h_{\ell,j}^{-1}),$$

then $(B_\ell)_{1,g_\ell h_{\ell,j}} = \lambda(h_{\ell,j})^{-1}$ for all j. More generally, one gets

Lemma 4. *If $g_{k'}h_{k',i'}h_{k,i}^{-1}g_k^{-1} \notin Hg_\ell H$, then $(B_\ell)_{g_k h_{k,i},g_{k'}h_{k',i'}} = 0$. Otherwise, write $g_{k'}h_{k',i'}h_{k,i}^{-1}g_k^{-1} = hg_\ell h_{\ell,j}$ for some $h \in H$. Then*

$$(B_\ell)_{g_k h_{k,i},g_{k'}h_{k',j'}} = \lambda(h)^{-1}\lambda(h_{\ell,j}^{-1}).$$

Proof. To see this choose $g = (g_k h_{k,i})^{-1} \in G$. Then $\Delta(g)_{g_k h_{k,i},1} = 1$ and hence

$$(\Delta(g)B_\ell)_{g_k h_{k,i},g_\ell h_{\ell,j}} = \Delta(g)_{g_k h_{k,i},1}(B_\ell)_{1,g_\ell h_{\ell,j}} = \lambda(h_{\ell,j})^{-1}.$$

On the other hand

$$(B_\ell\Delta(g))_{g_k h_{k,i},g_\ell h_{\ell,j}} = (B_\ell)_{g_k h_{k,i},g_{k'}h_{k',i'}}\Delta(g)_{g_{k'}h_{k',i'},g_\ell h_{\ell,j}}$$

for the unique (k',i') such that

$$h := g_{k'}h_{k',i'}(g_k h_{k,i})^{-1}(g_\ell h_{\ell,j})^{-1} \in H$$

and then $\Delta(g)_{g_{k'}h_{k',i'},g_\ell h_{\ell,j}} = \lambda(h)$. As $\Delta(g)B_\ell = B_\ell\Delta(g)$ compute

$$\lambda(h_{\ell,j})^{-1} = (B_\ell)_{g_k h_{k,i},g_{k'}h_{k',i'}}\lambda(h).$$

□

We now construct a monomial representation of $\mathrm{SL}_2(p)$ of degree $2(p+1)$. Suppose now $\mathrm{char}(\mathbb{F}_q) \neq 2$ and p is a prime p so that $p - 1 \equiv 4 \mod 8$. The subgroup

$$B^{(2)} := \left\{ \begin{pmatrix} a^2 & 0 \\ b & a^{-2} \end{pmatrix} : a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\} \leq \mathrm{SL}_2(p)$$

is of index $2(p+1)$ in $\mathrm{SL}_2(p)$ and has a group homomorphism $\gamma : B^{(2)} \longrightarrow \mathbb{F}_q^*$ with $\gamma(B^{(2)}) = \{\pm 1\}$, defined by

$$\gamma\left(\begin{pmatrix} a^2 & 0 \\ b & a^{-2} \end{pmatrix}\right) = \left(\frac{a}{p}\right),$$

the Legendre symbol of a.

Thus $\Delta' := \gamma_{B^{(2)}}^{\mathrm{SL}_2(p)}$ is a faithful monomial representation of degree $2(p+1)$. To obtain explicit matrices, let us choose

$$w := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We know that $\left(\frac{2}{p}\right) = -1$, whenever $p \equiv \pm 3 \mod 8$. Here by assumption $p \equiv 5 \mod 8$, then $2 \in \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$. Let

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(p) \right\} = \left\langle h_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \zeta := \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \right\rangle.$$

Then B is a subgroup of $\mathrm{SL}_2(p)$ of index $p+1$, isomorphic to the semidirect product $C_p : C_{p-1}$, with center

$$Z(B) = Z(\mathrm{SL}_2(p)) = \langle \zeta^{(p-1)/2} \rangle = \{\pm I_2\}.$$

If $\epsilon := \mathrm{diag}(2, 2^{-1})$, then

$$B = B^{(2)} \dot\cup B^{(2)}\epsilon,$$

and by means of the *Gauß-Bruhat* decomposition one gets

$$\mathrm{SL}_2(p) = B \dot\cup BwB = B^{(2)} \dot\cup B^{(2)}wB^{(2)} \dot\cup B^{(2)}\epsilon \dot\cup B^{(2)}\epsilon w B^{(2)}.$$

In consequence a right transversal of $B^{(2)}$ in $\mathrm{SL}_2(p)$ is given by

$$[1, wh_x, \epsilon, \epsilon w h_x : x \in \mathbb{F}_p],$$

where $h_x := \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in B^{(2)}$.

Lemma 5. *$End(\Delta')$ has a Schur basis $(B_1, B_w, B_\epsilon, B_{\epsilon w} = B_\epsilon B_w)$, where $B_\epsilon = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ and $B_w = \begin{pmatrix} X & Y \\ -Y^{tr} & X^{tr} \end{pmatrix}$ with*

$$X = \begin{pmatrix} 0 & 1 & \dots & 1 \\ -1 & & & \\ \vdots & & R_X & \\ -1 & & & \end{pmatrix}, Y = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & R_Y & \\ 0 & & & \end{pmatrix},$$

in which the rows and columns of R_X and R_Y are indexed by the elements $\{0, \dots, p-1\}$ of $\mathbb{F}_p$,

$$(R_X)_{a,b} = \begin{cases} 0, & b - a \notin (\mathbb{F}_p^*)^2 \\ \left(\frac{c}{p}\right), & b - a = c^2 \in (\mathbb{F}_p^*)^2 \end{cases}$$

and

$$(R_Y)_{a,b} = \begin{cases} 0, & 2(b-a) \notin (\mathbb{F}_p^*)^2 \\ \left(\frac{c}{p}\right), & 2(b-a) = c^2 \in (\mathbb{F}_p^*)^2. \end{cases}$$

Proof. It is true that $(B_w)_{wh_x, wh_y} \neq 0$ if and only if

$$wh_{x-y}w^{-1} = \begin{pmatrix} 1 & y-x \\ 0 & 1 \end{pmatrix} \in B^{(2)}wB^{(2)}.$$

This is equivalent to say that $y - x = a^2$, for some $a \in \mathbb{F}_p$ and then

$$wh_{x-y}w^{-1} = \begin{pmatrix} a^2 & 0 \\ 1 & a^{-2} \end{pmatrix} w \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

hence $(B_w)_{wh_x,wh_y} = \left(\frac{a}{p}\right)$. □

Remark 4. *Note that* $(-1) = c^2$ *is a square but not a 4th power, which implies that* $\left(\frac{c}{p}\right) = -1$. *Then X is skew symmetric or* $x_{ij} = -x_{ji}$, *and* $B_w^{tr} = -B_w, B_{\epsilon w}^{tr} = -B_{\epsilon w}$. *Since* $B_w^2 = B_{\epsilon w}^2 = -p$ *and* $B_\epsilon^2 = -1$, *then* $\mathrm{End}(\Delta') \cong \left(\frac{-p,-1}{\mathbb{F}_q}\right)$ *is isomorphic to a quaternion algebra over* $\mathbb{F}_q$. *Furthermore, we obtain that* $(B_w + B_{\epsilon w})^2 = -2p$.

Definition 1. *Let p be a prime,* $p \equiv 4 \pmod 8$, *and let* $a \in \mathbb{F}_q^*$ *such that* $a^2 = -tp$ *for* $t = 1$ *or* $t = 2$. *We define the code* $\mathcal{V}_q(p)$ *as the the linear code spanned by the rows of* $V_t(p)$, *where*

$$V_t(p) := \begin{cases} aI_{2(p+1)} + B_w, & t = 1 \\ aI_{2(p+1)} + B_w + B_{\epsilon w}, & t = 2. \end{cases}$$

Theorem 8. *The code* $\mathcal{V}_q(p) \leq \mathbb{F}_q^{2(p+1)}$ *is self-dual and* $\mathrm{Aut}(\mathcal{V}_q(p))$ *contains the group* $\mathrm{SL}_2(p)$.

Proof. By construction, the code $\mathcal{V}_q(p) \leq \mathbb{F}_q^{2(p+1)}$ is invariant under $\mathrm{SL}_2(p) \cong \Delta'(\mathrm{SL}_2(p))$. To prove that $\mathcal{V}_q(p)$ is self-orthogonal notice that

$$\begin{aligned} V_1(p)V_1(p)^{tr} &= (a + B_w)(a + B_w^{tr}) \\ &= a^2 + a(B_w + B_w^{tr}) + B_w B_w^{tr} \\ &= a^2 - B_w^2 = 0 \end{aligned}$$

and

$$\begin{aligned} V_2(p)V_2(p)^{tr} &= (a + B_w + B_{\epsilon w})(a + B_w^{tr} + B_{\epsilon w}^{tr}) \\ &= a^2 - (B_w + B_{\epsilon w})^2 = 0. \end{aligned}$$

To obtain the rank of the matrix $V_t(p)$ note that

$$\mathrm{End}(\Delta') \cong \left(\frac{-p,-1}{\mathbb{F}_q}\right) \cong \mathbb{F}_q^{2\times 2}.$$

This means the representation Δ' is the sum of two equivalent representations over $\mathbb{F}_q$ which have the same degree, $p+1$, half of the degree of Δ' and therefore $p+1$ divides the rank of any matrix in $\mathrm{End}(\Delta')$. □

Remark 5. *The matrices of rank* $p+1$ *in* $\mathrm{End}(\Delta')$ *yield* $q+1$ *different self-dual codes invariant under* $\Delta'(\mathrm{SL}_2(p))$. *In general, these fall into different equivalence classes. For instance, for* $q = 7$, *where* 2 *is a square mod 7, the codes spanned by the rows of* $V_1(p)$ *and* $V_2(p)$ *are nonequivalent. This is also true for* $p = 5$ *and* $p = 13$, *although they have the same minimum distance. For* $q = 3$, $p = 29$ *all 4 codes are equivalent and are just represented as the code* $\mathcal{V}_3(29)$.

The first few ternary codes $\mathcal{V}_3(p)$ have the following parameters (computed with MAGMA):

p	5	13	29	37	53
$2(p+1)$	12	28	60	76	108
$d(\mathcal{V}_3(p))$	6	9	18	18	24
$\mathrm{Aut}(\mathcal{V}_3(p))$	$2.M_{12}$	$\mathrm{SL}_2(13)$	$\mathrm{SL}_2(29)$	$\geq \mathrm{SL}_2(37)$	$\geq \mathrm{SL}_2(53)$

For $q = 5, 7$, and 11 the size of the field and small lengths it was computed $d(\mathcal{V}_q(p))$ with MAGMA:

(p,q)	$(13,5)$	$(29,5)$	$(5,7)$	$(13,7)$	$(5,11)$	$(13,11)$
$2(p+1)$	28	60	12	28	12	28
$d(\mathcal{V}_q(p))$	10	16	6	9	7	11

Here it can be noticed that even though the family yields extremal Type III codes for small values of primes p, such that $p \equiv 5 \pmod 8$, the minimum distance does not always grow with p, and for $q > 3$ the minimum distance is also not bigger either.

Remark 6. *We recall that a type III code C is said to be admissible if C contains the all-one vector (hence $n \in 12\mathbb{Z}$) and for every codeword $c \in C$ the number of 1's in the components of c is even. In [27], the authors proved that the code $\mathcal{XQR}(59)$ is admissible, whereas $\mathcal{P}(29)$ is not. Therefore, $\mathcal{XQR}(59)$ yields an extremal unimodular lattice, while $\mathcal{P}(29)$ does not. We verified that the code $\mathcal{V}_3(29)$ is not admissible. As a result, $\mathcal{V}_3(29)$ does not yield an unknown extremal unimodular lattice.*

Author Contributions: Conceptualization, S.B., J.d.l.C. and D.V.; methodology, S.B., J.d.l.C. and D.V.; formal analysis, S.B., J.d.l.C. and D.V.; Funding acquisition, S.B. and J.d.l.C.; Investigation, S.B., J.C. and D.V.; Supervision, S.B., J.d.l.C. and D.V.; Writing—original draft, S.B., J.d.l.C. and D.V.; Writing—review and editing, S.B., J.d.l.C. and D.V. All authors have read and agreed to the published version of the manuscript.

Funding: The research of S. Bouyuklieva was supported by Bulgarian National Science Fund grant number KP-06-N32/2-2019.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are very grateful to Gabriele Nebe for valuable discussions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Huffman, W.C.; Pless, V. *Fundamentals of Error-Correcting Codes*; Cambridge University Press: Cambridge, UK, 2003.
2. Mallows, C.L.; Sloane, N.J. An upper bound for self-dual codes. *Inf. Control.* **1973**, *22*, 188–200. [CrossRef]
3. Rains, E.M. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory* **1998**, *44*, 134–139. [CrossRef]
4. Pless, V. A classification of self-orthogonal codes over $GF(2)$. *Discrete Math.* **1972**, *3*, 209–246. [CrossRef]
5. Huffman, W.C. On the classification and enumeration of self-dual codes. *Finite Fields Appl.* **2005**, *11*, 451–490. [CrossRef]
6. Betsumiya, K.; Harada, M.; Munemasa, A. A complete classification of doubly even self-dual codes of length 40. *Electronic J. Combin.* **2012**, *19*, 1–12. [CrossRef]
7. Bouyukliev, I.; Dzhumalieva-Stoeva, M.; Monev, V. Classification of Binary Self-Dual Codes of Length 40. *IEEE Trans. Inform. Theory* **2015**, *61*, 4253–4258. [CrossRef]
8. Bouyuklieva, S.; Bouyukliev, I. An algorithm for classification of binary self-dual codes. *IEEE Trans. Inform. Theory* **2012**, *58*, 3933–3940. [CrossRef]
9. Harada, M.; Munemasa, A. A complete classification of ternary self-dual codes of length 24. *J. Combin. Theory Ser. A* **2009**, *116*, 1063–1072. [CrossRef]
10. Harada, M.; Munemasa, A.; Venkov, B. Classification of ternary extremal self-dual codes of length 28. *Math. Comp.* **2009**, *78*, 1787–1796. [CrossRef]
11. Huffman, W.C. Decomposing and shortening codes using automorphisms. *IEEE Trans. Inform. Theory* **1986**, *32*, 833–836. [CrossRef]
12. Huffman, W.C. Automorphisms of Codes with Applications to Extremal Doubly Even Codes of Length 48. *IEEE Trans. Inform. Theory* **1982**, *28*, 511–521. [CrossRef]
13. Huffman, W.C. On extremal self-dual ternary codes of lengths 28 to 40. *IEEE Trans. Inform. Theory* **1992**, *38*, 1395–1400. [CrossRef]
14. Yorgov, V. Binary self-dual codes with automorphisms of odd order. *Problems Inform. Transm.* **1983**, *19*, 260–270.
15. Yorgov, V. A method for Constructing Inequivalent Self-Dual Codes with Applications to Length 56. *IEEE Trans. Inform. Theory* **1987**, *33*, 77–82. [CrossRef]
16. Nebe, G. On Extremal Self-Dual Ternary Codes of Length 48. *Int. J. Comb.* **2012**, *2012*, 1–9. [CrossRef]

17. Ling S.; Solè, P. On the algebraic structure of quasi-cyclic codes I: Finite fields. *IEEE Trans. Inform. Theory* **2001**, *47*, 2751–2760. [CrossRef]
18. Gulliver, T.A.; Harada, M. Weight enumerators of extremal singly-even [60,30,12] codes. *IEEE Trans. Inform. Theory* **1996**, *42*, 658–659. [CrossRef]
19. Bouyuklieva, S.; Russeva, R.; Yankov, N. On the structure of binary self-dual codes having an automorphism of order a square of an odd prime. *IEEE Trans. Inform. Theory* **2005**, *51*, 3678–3686. [CrossRef]
20. Dontcheva, R.; Harada, M. Some Extremal Self-Dual Codes with an Automorphism of Order 7. *Appl. Algebra Eng. Comm. Computing* **2004**, *50*, 311–318.
21. Tsai, H.P.; Jiang, Y.J. Some new extremal self-dual [58,29,10] codes. *IEEE Trans. Inform. Theory* **1998**, *44*, 813–814. [CrossRef]
22. Yankov, N.; Lee, M.H. New binary self-dual codes of lengths 50–60. *Designs Codes Cryptogr.* **2014**, *73*, 983–996. [CrossRef]
23. Conway, J.H.; Sloane, N.J. A New Upper Bound of the Minimal Distance of Self-Dual Codes. *IEEE Trans. Inform. Theory* **1990**, *36*, 1319–1333. [CrossRef]
24. Harada, M. Binary extremal codes of length 60 and related codes. *Des. Codes Cryptogr.* **2017**, *86*, 1085–1094. [CrossRef]
25. Assmus, E.F., Jr.; Mattson, H.F., Jr. New 5-designs. *J. Combin. Theory* **1969**, *6*, 122–151. [CrossRef]
26. Pless, V. Symmetry codes over $GF(3)$ and new five-designs. *J. Combin. Theory* **1972**, *12*, 119–142. [CrossRef]
27. Harada, M.; Kitazume, M.; Ozeki, M. Ternary Code Construction of Unimodular Lattices and Self-dual Codes over $\mathbb{Z}_6$. *J. Algebr. Comb.* **2002**, *16*, 209–223. [CrossRef]
28. Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system I: The user language. *J. Symbolic Comput.* **1997**, *24*, 235–265. [CrossRef]
29. Harada, M.; Gulliver, T.A.; Kaneta, H. Classification of extremal double-circulant self-dual codes of length up to 62. *Discret. Math.* **1998**, *188*, 127–136. [CrossRef]
30. Nebe, G.; Villar, D. An analogue of the Pless symmetry codes. *Seventh Int. Workshop Optim. Codes Relat. Top.* **2013**, 158–163.
31. Landrock, P. Finite group algebras and their modules. *Lond. Math. Soc. Lect. Notes* **1983**, *84*, 172–186.
32. Müller, J. *On Endomorphism Rings And Character Tables*; Habilitationsschrift, RWHT-Aachen: Aachen, Germany, 2003.