Automorphisms of extremal codes

Stefka Bouyuklieva
Department of Mathematics and Informatics,
Veliko Tarnovo University, 5000 Veliko Tarnovo, Bulgaria,

Anton Malevich and Wolfgang Willems
Institut für Algebra und Geometrie, Fakultät für Mathematik,
Otto-von-Guericke Universität, 39016 Magdeburg, Germany

Abstract

Let C be a binary extremal self-dual code of length $n \geq 48$. We prove that for each $\sigma \in \mathrm{Aut}(C)$ of prime order $p \geq 5$ the number of fixed points in the permutation action on the coordinate positions is bounded by the number of p-cycles. It turns out that large primes p, i.e. $n - p$ small, seem to occur in $|\mathrm{Aut}(C)|$ very rarely. Examples are the extended quadratic residue codes. We further prove that doubly-even extended quadratic residue codes of length $n = p + 1$ are extremal only in the cases $n = 8, 24, 32, 48, 80$ and 104.

1 Introduction

Throughout this paper all codes are assumed to be binary. Let $C = C^{\perp}$ be a self-dual code of length n and minimum distance d. By results of Mallows-Sloane [14] and Rains [19], we have

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

and C is called extremal if equality holds. Extremal codes do not exist for large n. If C is doubly-even then $n \leq 3928$, by a result of Zhang [25]. However, we know extremal doubly-even codes only for small n; the largest n is 136. Thus there is a big gap between the bound which has been proved so far and what we are really able to construct.

In this paper we investigate primes p which may occur in the order of the automorphism group $G = \mathrm{Aut}(C)$ and determine the cycle structure of permutations in G. Let $\sigma \in G$ be of order p where p is an odd prime. The action of σ on the coordinate positions produces, say c cycles of length p and f fixed points. In this case we call σ of type p-(c, f). In Section 2 we prove as the main result that $c \geq f$ for any automorphism of C of prime order $p \geq 5$ and $n \geq 48$. In Section 3 we investigate the case $c = f = 1$. In particular, we prove that extended doubly-even quadratic residue codes of length $n = p + 1$ are extremal exactly in the cases $n = 8, 24, 32, 48, 80$ and 104.

2 The cycle structure of automorphisms

All binary self-dual codes of length $n \leq 20$ are classified by Vera Pless [17]. Extremal among them are the codes A_8 (the extended Hamming code), B_{12} (length 12), D_{14}, $A_8 \oplus A_8$, E_{16}, F_{16}, H_{18}, I_{18}, J_{20}, $A_8 \oplus B_{12}$, K_{20}, L_{20}, S_{20}, R_{20} and M_{20} (see Appendix, Table 1). Looking at their automorphism groups we can conclude:

- Neither of them has an automorphism of prime order $p > 7$.
- The codes A_8, D_{14}, $A_8 \oplus A_8$, E_{16}, I_{18}, J_{20}, $A_8 \oplus B_{12}$, and L_{20} have automorphisms of order 7. Appart from E_{16} and J_{20} all codes have an automorphism of order 7 with only one cycle. So the types for elements of order 7 are (1,1) (for A_8), (1,7) (for D_{14}), (1,9) (for $A_8 \oplus A_8$), (1,11) (for I_{18}), and (1,13) (for $A_8 \oplus B_{12}$ and L_{20}). The code J_{20} has automorphisms of type 7-(2,6).
- The codes B_{12}, E_{16}, I_{18}, J_{20}, $A_8 \oplus B_{12}$, K_{20}, and M_{20} have automorphisms of order 5. The types of these automorphisms are (2,2), (2,6), (2,8), (2,10), (2,10), and (4,0), respectively.
- All codes have automorphisms of orders 2 and 3.

More information on the structure of extremal [22,11,6] and [24,12,8] codes and their automorphism groups can be found in [18]. The only extremal [22,11,6] code is the shortened Golay code G_{22}. Its automorphisms of odd prime order are of type 11-(2,0), 7-(3,1), 5-(4,2) and 3-(6,4). The automorphism group of the extended Golay code is M_{24} and the automorphisms of odd prime order are of type 23-(1,1), 11-(2,2), 7-(3,3), 5-(4,4), 3-(6,6) and 3-(8,0).

Extremal self-dual codes of lengths 26, 28, 30 and 34 do not exist. There are five extremal doubly-even [32,16,8] codes (see [6]). According to Theorem 3 below the possible types of the automorphisms of odd prime order are 31-(1,1), 7-(4,4), 5-(6,2), 3-(8,8) and 3-(10,2). The code C82 in [6] has automorphisms of any of all these types. All extremal self-dual codes of length 36 are classified (see [9]). We calculated their automorphism groups using the program Q-Extension [2]. These groups contain permutations of types 17-(2,2), 7-(5,1), 5-(6,6), 3-(12,0), 3-(10,6), 3-(6,18), but no 3-(8,12). In Table 2 (see Appendix) we state the possible automorphisms of the extremal self-dual codes of lengths $36 \leq n \leq 68$. In the second column we list the automorphisms for which a corresponding self-dual code has been constructed. Column 3 consists of all types of automorphisms for which the existence of a corresponding code is not known. This table is based on Tables 2 and 3 in [13]. For the parameters in the second column, which are mentioned in [13] as open cases but have been answered meanwhile, we cite the corresponding papers.

Lemma 1 ([16, Theorem 2]) *Let C be a self-dual $[n, n/2]$ code with generator matrix*

$$G = \begin{pmatrix} G_{11} & O \\ O & G_{22} \\ G_{31} & G_{32} \end{pmatrix} \tag{1}$$

where $\begin{pmatrix} G_{11} & O \end{pmatrix}$ *resp.* $\begin{pmatrix} O & G_{22} \end{pmatrix}$ *is a generator matrix of the largest subcode of* C *whose support is contained entirely in the left* n_1 *resp. right* n_2 *coordinates and* $n = n_1 + n_2$. *Then*

$$\operatorname{rank} G_{22} = \frac{n}{2} + \operatorname{rank} G_{11} - n_1.$$

Let C be a code of length n with an automorphism σ of odd order p with exactly c independent p-cycles and $f = n - pc$ fixed points in its permutation action on the coordinate positions. We put

$$C^\sigma = \{v \in C \mid v\sigma = v\}.$$

Clearly, $v = (v_1, \dots, v_n) \in C^\sigma$ if and only if $v \in C$ takes constant entries in the positions which form an orbit of σ. Next we consider the projection map

$$\pi : C^\sigma \to \mathbb{F}_2^{c+f}$$

defined by $(v\pi)_i = v_j$ for some (hence all) j in the orbit of i and put C_π the image of C^σ under π. With this notation we have the following result which is part of Lemma 1 in [12].

Lemma 2 *If* C *is self-dual then* C_π *is a self-dual code of length* $c + f$.

Proof: We may suppose that the first c positions belong to the c different non-trivial orbits and the next f positions are the fixed points of σ. Thus, for $v, w \in C^\sigma$ we have $v\pi = (v_1, \dots, v_{c+f}), w\pi = (w_1, \dots, w_{c+f})$. It follows

$$0 = (v, w) = p\sum_{i=1}^{c} v_i w_i + \sum_{i=c+1}^{c+f} v_i w_i = \sum_{i=1}^{c} v_i w_i + \sum_{i=c+1}^{c+f} v_i w_i = (v\pi, w\pi)$$

since p is odd. Thus C_π is self-orthogonal in $\mathbb{F}_2^{c+f}$. Let $V = \mathbb{F}_2^n$ and $V^\sigma = \{v \in V \mid v\sigma = v\}$. By Maschke (see [1], Section 2, Corollary 8), we get $V = V^\sigma \oplus X$ with a KG-module X and $C = C^\sigma \oplus Y$ with a KG-module $Y \leq X$. Moreover $V = V^\sigma \perp X$ since X does not contain the trivial module. Thus C^σ is self-dual in V^σ, hence C_π is self-dual in $\mathbb{F}_2^{c+f}$. $\square$

To restrict the possible automorphisms for particular codes we need

Theorem 3 [24] *Let* C *be a binary self-dual* $[n, k, d]$ *code and let* $\sigma \in \operatorname{Aut}(C)$ *be of type* $p - (c, f)$, *where* p *is an odd prime. If* $g(s) = \sum_{i=0}^{s-1} \lceil \frac{d}{2^i} \rceil$ *then*
(i) $pc \geq g(\frac{p-1}{2}c)$ *and*
(ii) $f \geq g(\frac{f-c}{2})$ *for* $f > c$.

For an odd prime p let $s(p)$ denote the smallest number $s \in \mathbb{N}$ such that $p \mid 2^s - 1$.

Lemma 4 *Let* C *be a binary self-dual code of length* n *and let* $\sigma \in \operatorname{Aut}(C)$ *be of type* p-(c, f), *where* p *is an odd prime. If* $s(p)$ *is even then* c *is even. In particular, if* 2 *is a primitive root modulo* p *then* c *must be even.*

Proof: Since $2 \mid s(p)$ the group algebra $\mathbb{F}_2\langle\sigma\rangle$ has a non-trivial self-dual irreducible module, say V, by Theorem 2.7 of [15]. Clearly, the multiplicity of V as a composition factor of $\mathbb{F}_2^n$ is c. On the other hand, by Proposition 2.3 of [23], this multiplicity must be even. Finally note that $s(p)$ is even if 2 is a primitive root modulo p. □

We should mention here that the assertion of Lemma 4 in case that 2 is a primitive root of p was already proved in [12].

Lemma 5 *Let C be an extremal self-dual $[24m+2r, 12m+r, 4m+4]$, $0 \leq r \leq 10$ or $[24m+22, 12m+11, 4m+6]$ code with $m \geq 0$. If σ is an automorphism of C of type p-(c,f) where $p \geq 5$ is a prime then $f \neq c+2$.*

Proof: Suppose $f = c+2$. First we consider the case $n = 24m+22$ and $d = 4m+6$. According to Theorem 3, $f \geq g(1) = 4m+6$ and so $c \geq 4m+4$. Then

$$24m+22 = cp+c+2 \geq (4m+4)(p+1)+2 = 4(p+1)m+4p+6.$$

Hence $4(5-p)m \geq 4p-16$ and therefore $0 \geq (5-p)m \geq p-4 > 0$, a contradiction.

Now let $n = 24m+2r$ with $0 \leq r \leq 10$ and $d = 4m+4$. By Theorem 3 we have $f \geq g(1) = 4m+4$, hence $c \geq 4m+2$. Since

$$24m+2r \geq (4m+2)p+4m+4 = 4(p+1)m+2p+4$$

we obtain $4(5-p)m \geq 2(p+2-r) \geq 2(p-8)$. Obviously, if $p > 8$ then $4(5-p)m < 0$, but $2(p-8) > 0$ and therefore the above inequality is not possible. If $p = 7$ then $-8m \geq 2(9-r)$ which is possible only if $m = 0$, $r = 9$ or 10, and $c = (r-1)/4$. As c is integer, $r = 9$, $n = 18$, $c = 2$. Two extremal self-dual [18,9,4]-codes exist, namely H_{18} and I_{18}. Only I_{18} has an automorphism of order 7, but by [17], the type of this automorphism is 7-(1,11). If $p = 5$ then $24m+2r \geq 24m+14$. Thus $r = 7$, 8, 9, or 10, and $c = 4m+(r-1)/3$. Since c is an integer, moreover c even by Lemma 4, only the case $r = 7$ remains to consider.

To finish the proof we consider a generator matrix G_π of the binary self-dual $[c+f = 2c+2, c+1]$ code C_π in the form (1) where $n_1 = c$ and $n_2 = f = c+2$. Then

$$\operatorname{rank} G_{22} = \operatorname{rank} G_{11} + 1 \geq 1.$$

But G_{22} generates a self-orthogonal code of length $c+2 = 4m+4$ and minimum distance at least $4m+4$. Thus G_{22} generates the repetition code and the rank-equation above yields $G_{11} = 0$. Therefore we may assume that G_π has the form

$$G_\pi = \left(\begin{array}{c|c} O & x \\ \hline & y_1 \\ I_c & \cdots \\ & y_c \end{array}\right), \tag{2}$$

Now observe that the vectors $(00\ldots000000, x)$ and $(00\ldots011111, *)$ generate a subcode of C of effective length $c+7 = 4m+9$ and dimension 2 whose minimum distance is at least $4m+4$. Therefore $4m+9 \geq 6m+6$ which is possible only when $m=0$ or 1. The automorphism group of the unique self-dual [14,7,4] code, which is denoted by D_{14}, is $\mathrm{PSL}(2,7)^2.S_2$ and 5 does not divide its order (see Appendix, Table 1). As well no self-dual [38,19,8] code has an automorphism of order 5 (see Appendix, Table 2). $\square$

Remark 1 The above lemma proves that the extremal [62,31,12] codes cannot have automorphisms of type 5-(10,12). This possibility is mentioned in Table 2 in Huffman's survey on self-dual codes [13].

Lemma 6 *If there exists an extremal self-dual* $[24m+22, 12m+11, 4m+6]$ *code having an automorphism of type* p-(c,f)*, where* $f \geq 2$ *and* p *is an odd prime, then there exists an extremal self-dual* $[24m+20, 12m+10, 4m+4]$ *code having an automorphism of type* p-$(c, f-2)$.

Proof: Let C be a self-dual $[24m+22, 12m+11, 4m+6]$ code and let σ be an automorphism of C of type p-(c,f). We may assume that the last two positions of the underlying ambient space are fixed points of σ. Thus C has a generator matrix of the form

$$G = \begin{pmatrix} & x & & 0 & 1 \\ 1 & \dots & 1 & 1 & 1 \\ & & & 0 & 0 \\ & G' & & \vdots & \vdots \\ & & & 0 & 0 \end{pmatrix}.$$

Obviously, the code C' generated by

$$G = \begin{pmatrix} 1 & \dots & 1 \\ & G' & \end{pmatrix}.$$

is a self-orthogonal $[24m+20, 12m+10, d]$ code with $d \geq 4m+4$. By the results of Mallows-Sloane and Rains it follows that $d = 4m+4$. Thus C' is an extremal code. $\square$

Now let $n = 24m+2r$ with $0 \leq r \leq 10$, and $d = 4m+4$. Then we have $g(1) = 4m+4$, $g(2) = 6m+6$, $g(3) = 7m+7$, and for $s \geq 4$

$$g(s) = \sum_{i=0}^{s-1} \left\lceil \frac{4m+4}{2^i} \right\rceil = 7m+7+\sum_{i=3}^{s-1} \left\lceil \frac{4m+4}{2^i} \right\rceil = 7m+7+\sum_{i=1}^{s-3} \left\lceil \frac{m+1}{2^i} \right\rceil.$$

If $2^l < m+1 \leq 2^{l+1}$ for $l \in \mathbb{N}_0$ then

$$g(s) \geq 7m+7+\sum_{i=1}^{s-3} \frac{m+1}{2^i} = 7m+7+(m+1)\frac{2^{s-3}-1}{2^{s-3}} = (m+1)\frac{2^s-1}{2^{s-3}}.$$

For $i > l$ we have $\frac{m+1}{2^i} < 2^{l+1-i} \leq 1$ and therefore $\lceil \frac{m+1}{2^i} \rceil = 1$. Hence for $s - 3 > l$ the following inequality holds

$$g(s) = g(l+3) + s - 3 - l \geq \Big(8 - \frac{1}{2^l}\Big)(m+1) - l - 3 + s = A + s.$$

Using the above inequalities and Theorem 3 we prove the

Main Theorem 7 *If C is an extremal self-dual code of length $24m + 2r$, $0 \leq r \leq 11$, $m \geq 2$, and σ is an automorphism of C of type p-(c, f), where $p \geq 5$ is a prime, then $c \geq f$.*

Proof: As we see in (Appendix, Table 2) we have $c \geq f$ for all extremal codes of length $48 + 2r$ with $r = 0, 1, \ldots, 11$. Thus we may assume $m \geq 3$. Furthermore we choose $l \in \mathbb{N}_0$ such that $2^l < m + 1 \leq 2^{l+1}$.

Let C be an extremal self-dual $[24m + 2r, 12m + r, 4m + 4]$ code with $0 \leq r \leq 10$ and $m \geq 3$. Suppose that $f > c$. By Theorem 3, we have

$$pc \geq g\Big(\frac{p-1}{2}c\Big) \text{ and } f \geq g\Big(\frac{f-c}{2}\Big)$$

(a) We claim $\frac{p-1}{2}c > l + 3$.
If $\frac{p-1}{2}c \leq l + 3$ then $c \leq \frac{2(l+3)}{p-1}$. Since $p \geq 5$ we have $\frac{p-1}{2}c \geq 2c \geq 3$ (for $p = 5$ use Lemma 4). Therefore $pc \geq g(\frac{p-1}{2}c) \geq g(3) = 7m + 7$. Thus

$$\frac{7m+7}{p} \leq c \leq \frac{2l+6}{p-1}$$

implies

$$(7m + 7 - 2l - 6)p \leq 7m + 7,$$

hence

$$p \leq \frac{7m+7}{7m+1-2l} < 2,$$

a contradiction.

(b) Next we claim $\frac{f-c}{2} > l + 3$.
If $\frac{f-c}{2} \leq l + 3$ then $f \leq 2l + 6 + c$. Moreover, $f \geq g(\frac{f-c}{2}) \geq g(2) = 6m + 6$. Hence $6m + 6 \leq 2l + 6 + c$ and $c \geq 6m - 2l$. Therefore $n = 24m + 2r = pc + f > (p + 1)c \geq (p + 1)(6m - 2l)$ and

$$p < \frac{18m + 2r + 2l}{6m - 2l} = 3 + \frac{8l + 2r}{6m - 2l} = 3 + \frac{4l + r}{3m - l}.$$

If $m = 3$ then $l = 1$ and $p < 3 + \frac{r+4}{8} < 5$.
If $m \geq 4$ then $l \geq 2$. Since

$$4l + r - 2(3m - l) = 6l - 6m + r = 6(l - m) + r \leq 6(l - 2^l) + 10 < 0$$

we get $\frac{4l+r}{3m-l} \leq 2$ and therefore $p < 5$, a contradiction.

As $f = n - pc$ we obtain, by (a) and (b), that

$$pc \geq A + \frac{p-1}{2}c \quad \text{and} \quad n - pc \geq A + \frac{n-(p+1)c}{2}, \tag{3}$$

hence $\frac{2A}{p+1} \leq c \leq \frac{n-2A}{p-1}$ and therefore $2A(p-1) \leq (n-2A)(p+1)$ or $(4A-n)p \leq n$. Since

$$\begin{array}{rcll} 4A - n & = & 4(8 - \frac{1}{2^l})(m+1) - 4l - 12 - 24m - 2r & \\ & = & (8 - \frac{4}{2^l})m - \frac{4}{2^l} - 4l + 20 - 2r & \\ & \geq & (8 - \frac{4}{2^l})m - \frac{4}{2^l} - 4l & (*) \\ & \geq & (8 - \frac{4}{2^l})2^l - \frac{4}{2^l} - 4l & \\ & = & 8 \cdot 2^l - 4 - \frac{4}{2^l} - 4l & \\ & \geq & 8 \cdot 2^l - 6 - 4l = 4(2^{l+1} - l - 1) - 2 > 0 & \end{array}$$

we get $p \leq \dfrac{n}{4A-n}$. If $l \geq 2$ we have $4A - n \geq 7m - 1 - 4l$ by $(*)$ and therefore

$$p \leq \frac{n}{7m-1-4l} \leq \frac{24m+20}{7m-1-4l}.$$

Since $p \geq 5$ this contradicts to

$$\frac{24m+20}{7m-1-4l} - 5 = \frac{24m+20-35m+5+20l}{7m-1-4l} = \frac{25+20l-11m}{7m-1-4l} \leq \frac{25+20l-11 \cdot 2^l}{7 \cdot 2^l - 1 - 4l} < 0.$$

So we proved that $f > c$ is not possible if $p \geq 5$ and $l \geq 2$.

Now let $l = 1$, hence $m = 3$. Then $A = \frac{15}{2}(m+1) - 4 = 26$ and

$$p \leq \frac{n}{4A-n} = \frac{72+2r}{104-72-2r} = \frac{72+2r}{32-2r} < 8.$$

If $p = 7$ then $7c \geq g(3c) = 3c + 26$ by (3), hence $c \geq 7$, and $f \geq \frac{f-c}{2} + 26$ also by (3). This implies

$$72 + 2r - 7c = f \geq 52 - c,$$

hence $20 + 2r \geq 6c \geq 42$ or $r \geq 11$, a contradiction.

If $p = 5$ then c is even, by Lemma 4. Now $5c \geq g(2c) = 2c + 26$ yields $c \geq 10$. Furthermore $f \geq \frac{f-c}{2} + 26$ implies

$$72 + 2r - 5c = f \geq 52 - c.$$

Thus $20 + 2r \geq 4c \geq 40$ which forces $r \geq 10$. It follows that $n = 92$, $c = 10$ and $f = 42$.

To get a contradiction we consider the code C_π with parameters $[52, 26, d_\pi]$ (see Lemma 2) and take a generator matrix in the form (1). The matrix G_{22} generates a self-orthogonal code with parameters $[42, k_2, \geq 16]$. By Lemma 1, we have $k_2 = 26 + k_1 - 10 \geq 16$. But a $[42, \geq 16, \geq 16]$ code does not exist.

This proves that $c \geq f$ for the extremal codes of lengths $24m + 2r$ if $r \leq 10$. Finally, let C be an extremal $[24m+22, 12m+11, 4m+6]$ code with $m \geq 2$. If C has an automorphism of type p-(c, f) where $c < f$ and $p \geq 5$ is a prime, then there is an extremal self-dual $[24m+20, 12m+10, 4m+4]$ code having an automorphism of type $p-(c, f-2)$, by Lemma 6. Hence $f > c \geq f - 2$, by what we have proved above. The condition $n = pc + f$ yields that $f - c$ is even. Thus we get $c = f - 2$, a contradiction to Lemma 5, and the proof is complete. □

For the prime 3 the statement of the main theorem holds no longer true. Examples are given in the boldface entries in Table 2 of the Appendix.

3 Automorphisms of prime order $p > \frac{n}{2}$

Let $C = C^{\perp}$ be extremal and doubly-even of length $n \geq 48$. By Gleason [10], we have

$$n = 24m + 8i \qquad (i = 0, 1, 2).$$

Furthermore, we assume that C has an automorphism, say σ, of prime order $p > \frac{n}{2}$. Thus, by Theorem 7, σ is of type $p - (1, 1)$ and $n = 24m + 8i = p + 1$. In particular,

$$p \equiv -1 \bmod 8.$$

Moreover, $i \neq 2$ since otherwise $3 \mid 24m + 16 - 1 = p > 3$, a contradiction.

Lemma 8 *For $p > \frac{n}{2}$ we have $s(p)$ odd.*

Proof: Since $p \equiv -1 \bmod 8$ the prime 2 is a square mod p. This yields the congruence $2^{\frac{p-1}{2}} \equiv 1 \bmod p$. As $s(p) \mid \frac{p-1}{2}$ and $\frac{p-1}{2}$ is odd the proof is complete. □

Lemma 9 *The trivial module is the only irreducible self-dual $\mathbb{F}_2\langle\sigma\rangle$-module.*

Proof: By Lemma 8, we know that $s(p)$ is odd. The assertion now follows directly by Theorem 2.7 of [15]. □

Theorem 10 *If $s(p) = \frac{p-1}{2}$ then C is an extended quadratic residue code.*

Proof: The ambient space $\mathbb{F}_2^n$ of C can be written as

$$\mathbb{F}_2^n = \mathbb{F}_2\langle\sigma\rangle \oplus \mathbb{F}_2.$$

Since $s(p) = \frac{p-1}{2}$ the non-trivial irreducible $\mathbb{F}_2\langle\sigma\rangle$-modules are of dimension $\frac{p-1}{2}$. Thus by Maschke (see [1], Section 2, Corollary 8), we have the decomposition

$$(*) \qquad \mathbb{F}_2\langle\sigma\rangle = \mathbb{F}_2 \oplus V \oplus W$$

with irreducible modules V and W both of dimension $s(p) = \frac{p-1}{2}$. By Lemma 9, we have $V \ncong V^*$ and $W \ncong W^*$. Since a group algebra is always self-dual as a module we obtain $W \cong V^*$. Furthermore, the decomposition in $(*)$ is unique since the three modules are non-isomorphic. On the other hand, we know that

$$\mathbb{F}_2\langle\sigma\rangle = \mathbb{F}_2 \oplus Q \oplus N$$

where Q is the code associated to the squares mod p and N to the non-squares. Since Q is equivalent to N we may assume that $V = Q$. Finally, if C_0 is the subspace of C with 0 in the last position then $C = \langle C_0, c\rangle$ where c is the all one word. This shows that C is an extended quadratic residue code. $\square$

Remark 2 a) If $n = 24m = p + 1$ then $m \leq 153$ and $s(p) = \frac{p-1}{2}$ except the cases

$$m = 18, 38, 46, 98, 112, 133.$$

b) If $n = 24m + 8 = p + 1$ then $m \leq 158$ and $s(p) = \frac{p-1}{2}$ in about half of the cases.

The remark above and Theorem 10 show that many of the codes in question are extended quadratic residue codes. For this class of codes we can give a complete answer.

Theorem 11 *Let $C = C^\perp$ be a doubly-even extended quadratic residue code of length n. Then C is extremal exactly for*

$$n = 8, 24, 32, 48, 80 \text{ and } 104.$$

Proof: Let $n = p + 1$ be the length of C. It is well-known that $\mathrm{PSL}(2, p)$ is contained in the automorphism group of C. We may assume that n is different from $8, 24, 32, 48, 80, 104$ since extended quadratic residue codes of these lengths are extremal (see [20]). In all other cases we have to find a codeword of weight strictly smaller than $4\lfloor\frac{n}{24}\rfloor + 4 = 4m + 4$.

This can be done along the following lines using the computer algebra system MAGMA. For each $n = p + 1$ we choose a suitable subgroup, say H of $\mathrm{PSL}(2, p)$. In most cases H will be a cyclic group of order 4 or 6 or a Sylow 2-subgroup of $\mathrm{PSL}(2, p)$.

Next we find the subcode C^H of C which consists of those vectors of C which are fixed by all elements of H. This subcode is in general much smaller than C.

Finally by direct enumeration we find in C^H codewords of weight strictly less than $4m + 4$ which completes the proof. $\square$

Remark 3 In the proof of the previous theorem H is chosen so that on the one hand the subcode C^H is small enough for enumeration and on the other hand it contains codewords of small weight.

By what we have proved so far the following question may have an affirmative answer.

Question 12 Is a doubly-even extremal code of length n which carries an automorphism of prime order $p > \frac{n}{2}$ an extended quadratic residue code?

References

[1] J.L. Alperin and R.B. Bell, Groups and representations, Springer GTM, New York/Heidelberg 1995.

[2] I. Bouyukliev, About the code equivalence, in *Advances in Coding Theory and Cryptology*, T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko: Series on Coding Theory and Cryptology, 2. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007.

[3] S. Bouyuklieva, R. Russeva, and N. Yankov, On the structure of binary self-dual codes having an automorphism of order a square of an odd prime, *IEEE Transactions on Information Theory* **51** (2005), 3678–3686.

[4] S. Bouyuklieva, R. Russeva and N. Yankov, The binary self-dual $[44, 22, 8]$ codes with automorphisms of order 3, preprint.

[5] S. Bouyuklieva, N. Yankov and R. Russeva, Classification of the binary self-dual $[42, 21, 8]$ codes having an automorphism of order 3, *Finite Fields Appl.* **13** (2007), 605-615.

[6] J.H.Conway, V.Pless and N.J.A.Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *J. Comb. Theory*, Ser. A, **60** (1992), 183-195.

[7] R. Dontcheva and M. Harada, Some extremal self-dual codes with an automorphism of order 7, *Appl. Algebra in Eng. Comm. and Computing* **14** (2003), 75–79.

[8] R. Dontcheva and M. Harada, New extremal self-dual codes of length 62 and related extremal self-dual codes, *IEEE Trans. Inform. Theory* **48** (2002), 2060–2064.

[9] P. Gaborit, `www.unilim.fr/pages_perso/philippe.gaborit/SD/index.html`.

[10] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes Congrès Internat. Math.* **3** (1970), 211-215.

[11] M. Harada, T. Nishimura and R. Yorgova, New extremal self-dual codes of length 66, *Mathematica Balkanica* **21** (2007), 113-121.

[12] W.C.Huffman, Automorphisms of codes with application to extremal doubly-even codes of lenght 48, *IEEE Trans. Inform. Theory* **28** (1982) 511-521.

[13] W.C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields *Appl.* **11** (2005), 451–490.

[14] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. and Control* **22** (1973), 188-200.

[15] C. Martínez-Pérez and W. Willems, Self-dual extended cyclic codes, *Appl. Algebra in Eng. Comm. and Computing* **17** (2006), 1-16.

[16] V. Pless, Coding constructions, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 141-176.

[17] V. Pless, A classification of self-orthogonal codes over GF(2), *Discrete Math.* **3** (1972), 209-246.

[18] V.Pless and N.J.A.Sloane, On the classification and enumeration of self-dual codes, *J. Comb. Theory*, Ser. A, **18** (1975), 313-335.

[19] E.M. Rains, Shadow bounds for self-dual-codes, *IEEE Trans. Inform. Theory* **44** (1998), 134-139.

[20] E.M. Rains and N.J.A. Sloane Self-dual codes, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177-294.

[21] R. Russeva and N. Yankov, On binary self-dual codes of lengths 60, 62, 64 and 66 having an automorphism of order 9, *Designs, Codes and Cryptography* 45 (2007), 335 - 346.

[22] R. Russeva and N. Yankov, Classification of the binary self-dual [44,22,8] codes with automorphisms of order 7, Mathematics and Math. Education (2008), 239-244.

[23] W. Willems, A note on self-dual group codes, *IEEE Trans. Inform. Theory* **48** (2002), 3107-3109.

[24] V.Y.Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory* **33** (1987), 77-82.

[25] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277-286.

Appendix

Table 1: Extremal self-dual codes of lengths $n \leq 20$

code C	$Aut(C)$	order	types of σ
A_8	G_8	$7.3.2^6$	7-(1,1), 3-(2,2)
B_{12}	$Z_2^5.S_6$	$2^5.6! = 5.3^2.2^9$	5-(2,2), 3-(2,6), 3-(4,0)
D_{14}	$PSL_2(7)^2.S_2$	$7^2.3^2.2^7$	7-(1,7), 7-(2,0), 3-(2,8), 3-(4,2)
$A_8 \oplus A_8$	$G_8^2.S_2$	$7^2.3^2.2^{13}$	7-(1,9), 7-(2,2), 3-(2,10), 3-(4,4)
E_{16}	$Z_2^7.S_8$	$2^7.8! = 7.5.3^2.2^{14}$	7-(2,2), 5-(2,6), 3-(2,10), 3-(4,4)
F_{16}	$[Z_2^3.S_4]^2.S_2$	$(8.4!)^2.2 = 3^2.2^{13}$	3-(2,10), 3-(4,4)
H_{18}	$[Z_2^2.S_3]^3.S_3$	$(4.6)^3.6 = 3^4.2^{10}$	3-(2,12), 3-(4,6), 3-(6,0)
I_{18}	$PSL_2(7) \times [Z_2^4.S_5]$	$7.3.2^3.2^4.5! = 7.5.3^2.2^{10}$	7-(1,11), 5-(2,8), 3-(2,12), 3-(4,6)
J_{20}	$Z_2^9.S_{10}$	$2^9.10! = 7.5^2.3^4.2^{17}$	7-(2,6), 5-(2,10), 5-(4,0), 3-(2,14), 3-(4,8), 3-(6,2)
$A_8 \oplus B_{12}$	$G_8 \times [Z_2^5.S_6]$	$7.3.2^6.2^5.6! = 7.5.3^3.2^{15}$	7-(1,13), 5-(2,10), 3-(2,14), 3-(4,8), 3-(6,2)
K_{20}	$[Z_2^3.S_4] \times [Z_2^5.S_6]$	$2^3.4!.2^5.6! = 5.3^3.2^{15}$	5-(2,10), 3-(2,14), 3-(4,8), 3-(6,2)
L_{20}	$[PSL_2(7)^2.Z_2] \times [Z_2^2.S_3]$	$(7.3.2^3)^2.2.2^2.6 = 7^2.3^3.2^{10}$	7-(1,13), 7-(2,6), 3-(2,14), 3-(4,8), 3-(6,2)
S_{20}	$[Z_2.S_2] \times [[Z_2^3.S_4]^2.S_2]$	$4.(2^3.4!)^2.2 = 3^2.2^{15}$	3-(2,14), 3-(4,8)
R_{20}	$[Z_2^2.S_3]^3.S_3$	$(2^2.6)^3.6 = 3^4.2^{10}$	3-(2,14), 3-(4,8), 3-(6,2)
M_{20}	$K_4^5.S_5$	$4^5.5! = 5.3.2^{13}$	5-(4,0), 3-(4,8)

Table 2: Extremal self-dual codes of lengths $36 \leq n \leq 68$ with automorphisms of type p-(c,f) for an odd prime p

n	p-(c,f) in constructed codes [Reference]	Open cases
36	17-(2,2), 7-(5,1), 5-(6,6), 3-(12,0), 3-(10,6), **3-(6,18)**[9], **3-(8,12)**/0[9]	-
38	19-(2,0), 7-(5,3), 3-(12,2)[3]	**3-(6,20), 3-(8,14)**, 3-(10,8)
40	19-(2,2), 7-(5,5), **5-(4,20)**, 5-(8,0), **3-(6,22)**, 3-(12,4)[3]	**3-(8,16)**, 3-(10,10)
42	7-(3,21), 7-(6,0), **5-(4,22)**, 5-(8,2), **3-(6,24)**[5], **3-(8,18)**[5], **3-(10,12)**[5], 3-(12,6)[5], 3-(14,0)[5]	-
44	**11-(2,22)**, 11-(4,0), **7-(3,23)**/3[22], 7-(6,2)[22], **5-(4,24)**, 5-(8,4), **3-(6,26)**, 3-(12,8)[3], **3-(10,14)**[4], 3-(14,2)[4], **3-(8,20)**[4]	-
46	23-(2,0)	-
48	47-(1,1), 23-(2,2), 3-(16,0)	-
56	13-(4,4), 3-(18,2)[BDC]	7-(7,7), 7-(8,0), 5-(10,6), 3-(14,14), 3-(16,8)
60	29-(2,2), 7-(8,4)[7], 5-(12,0)[DC], 3-(20,0)[DC], 3-(18,6)[21]	5-(10,10), **3-(14,18)**, 3-(16,12)
62	5-(12,2)[8], 5-(10,12)/0[Remark 1], 3-(20,2)[8], 3-(18,8)[21]	31-(2,0), 7-(8,6), 3-(16,14)
64	31-(2,2), 7-(9,1)[7], 7-(8,8)/0[7], 3-(18,10)[21]	5-(12,4), 3-(16,16), 3-(20,4)
66	11-(6,0)[DC], 7-(9,3)[11], 5-(12,6)[11], 3-(22,0)[DC], 3-(18,12)[21]	**3-(14,24), 3-(16,18)**, 3-(20,6)
68	17-(4,0)[DC], 11-(6,2)[BDC], 3-(22,2)[BDC]	7-(9,5), 5-(12,8), **3-(14,26)**, **3-(16,20)**, 3-(18,14), 3-(20,8)

DC	double circulant construction
BDC	bordered double circulant construction
p-$(c,f)/0$	cycle structure does not occur