Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 26-31*

On extremal codes with automorphisms

Stefka Bouyuklieva stefka@uni-vt.bg
Veliko Tarnovo University, 5000 Veliko Tarnovo, BULGARIA,

Anton Malevich anton.malevich@st.ovgu.de
Wolfgang Willems willems@ovgu.de
Both: Otto-von-Guericke Universität, 39016 Magdeburg, GERMANY

Abstract. Let C be a binary extremal self-dual doubly-even code of length $n \geq 48$. If such a code has an automorphism σ of prime order $p \geq 5$ then the number of fixed points in the permutation action on the coordinates is bounded by the number of p-cycles. It turns out that large primes p, i.e. $n-p$ small, occur extremely rarely in $\mathrm{Aut}(C)$. Examples are the extended quadratic residue codes. We prove that doubly-even extended quadratic residue codes of length $n = p+1$ are extremal if and only if $n = 8, 24, 32, 48, 80$ or 104. Moreover, we reduce the list of putative extremal doubly-even codes with an automorphism of prime order $p = n-1$ to merely 12 cases. We conjecture that in fact such an extremal code, if it is not an extended quadratic residue code of one of the lengths given above, does not exist.

1 Introduction

Let $C = C^{\perp}$ be a binary self-dual doubly-even code of length n and minimum distance d. By Gleason [2], we have $n = 24m + 8i$, $i = 0, 1, 2$. Due to Mallows-Sloane [6] and Rains [8] there is the following bound on the minimum distance

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

and C is called extremal if equality holds. Extremal codes do not exist for large n. If C is doubly-even then $n \leq 3823$, by a result of S. Zhang [10]. However, we know extremal codes only for small lengths, the largest being 136. Thus there is a big gap between the bound we have for extremal doubly-even codes and what we can construct. In order to find extremal codes of larger lengths automorphisms may be helpful.

Let $G = \mathrm{Aut}(C)$ and let $\sigma \in G$ be a permutation of order p where p is an odd prime. The action of σ on the positions produces, say c cycles of length p and f fixed points, and in this case we call σ of type $p-(c,f)$. In Sections 2 and 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 only if $n = 8, 24, 32, 48, 80$ and 104.

2 Extremal doubly-even extended QR-codes

Let $C = C^{\perp}$ be extremal and doubly-even of length $n \geq 48$. Furthermore, we assume that C has an automorphism, say σ, of prime order $p > \frac{n}{2}$. The following result which extends the main theorem of [1] turns out to be crucial in our investigations.

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

Thus we have that 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. Finally, let $s(p)$ denote the smallest number $s \in \mathbb{N}$ such that $p \mid 2^s - 1$.

In [1] the following has been shown

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

The condition $s(p) = \frac{p-1}{2}$ is very often satisfied. If $n = 24m = p + 1$ then $m \leq 153$ and $s(p) = \frac{p-1}{2}$ except the cases

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

If $n = 24m + 8 = p + 1$ then $m \leq 158$ and $s(p) = \frac{p-1}{2}$ in about half of the cases. Thus, by Theorem 2, we see that many of the codes in question are extended quadratic residue codes. For this class of codes we can give a complete answer.

Theorem. 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 [9]). In all other cases we have to find a code word of weight strictly smaller than $4\lfloor \frac{n}{24} \rfloor + 4$.

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 we choose H to 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 the 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 $4\lfloor \frac{n}{24} \rfloor + 4$ and the proof is complete. $\square$

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

3 The general case, i.e. $s(p)$ arbitrary

If $s(p)$ is arbitrary we have the following decomposition

$$\mathbb{F}_2\langle\sigma\rangle = V_0 \oplus V_1 \oplus \ldots \oplus V_k$$

with irreducible modules V_i, each of dimension $s(p)$ for $i = 1, \ldots, k$, and V_0 the trivial module. Furthermore, all modules are pairwise non-isomorphic and $V_1, \ldots, V_k$ may be considered as the minimal ideals in the group algebra $\mathbb{F}_2\langle\sigma\rangle$. Moreover, they are generated as ideals or $\mathbb{F}_2\langle\sigma\rangle$-modules by primitive idempotents, say $e_{i_1}, \ldots, e_{i_k}$. They are unique and can be constructed as follows.

Let α be a p-th root of unity in $\mathbb{F}_{2^{s(p)}}$ and let $C_{i_1}, \ldots, C_{i_k}$ denote the 2-cyclotomic cosets modulo p and C_0 the trivial coset containing only 0. Then

$$e_t = \sum_{i=0}^{p-1} \varepsilon_i \sigma^i \quad \text{with} \quad \varepsilon_i = \sum_{j \in C_t} \alpha^{ij}$$

where $t = i_1, \ldots, i_k$ is a representative of the coset C_t. Furthermore, any ideal in $\mathbb{F}_2\langle\sigma\rangle$ is generated by the sum of suitable e_t's.

Clearly, such an ideal is a cyclic code since of $\mathbb{F}_2\langle\sigma\rangle \cong \mathbb{F}_2[x]/_{(x^p-1)}$ as algebras. Since we are interested in self-dual $[p+1, \frac{p+1}{2}]$-codes we have to look at all possible ideals of type $V = V_{i_1} \oplus \ldots \oplus V_{i_{k/2}}$ with the property that V does not contain ${V_j}^*$ if it contains V_j. There are precisely $2^{k/2}$ possibilities for V, and V is generated by a suitable sum of primitive idempotents. In our case (a binary field and p an odd prime) these are duadic codes in the sense of [4] (see [5] for properties of such codes). There is an easy way to compute the classes of inequivalent codes.

Proposition. (Pálfy, see [3]) Let C_1 and C_2 be cyclic $[n,k]$-codes over $\mathbb{F}_q$. Assume that $\gcd(n, \varphi(n)) = 1$ where φ is the Euler φ-function. Then C_1 and

C_2 are equivalent if and only if there is a multiplier that maps the idempotent of C_1 to the idempotent of C_2.

The multipliers are group automorphisms of the form $\mu_a \colon \sigma \mapsto \sigma^a$. There are in fact exactly k multipliers, having different actions on the cyclotomic cosets and thus on the idempotents. They are of the form μ_t where t runs through a set of representatives of the cyclotomic cosets.

For each prime p with $s(p) \neq \frac{p-1}{2}$ we have to consider $2^{k/2}$ different codes. Each equivalence class consists of at most k codes. Thus the number of inequivalent codes is at least $\left\lfloor \frac{2^{k/2}}{k} \right\rfloor$, including the extended QR code.

In the table below we list all primes $p = 24m + 8i - 1 > 48$ for $i = 0, 1$ with $s(p) \neq \frac{p-1}{2}$. The boldfaced entries are the exceptions from [1] where $p = 24m - 1$. The column "Num of Codes" gives the minimum number of inequivalent codes, i.e. $\left\lfloor \frac{2^{k/2}}{k} \right\rfloor$. In the second last column d stands for the extremal minimum distance. There are three types of entries in the column "w found". For the case $k = 6$ the number stands for the weight $w < d$ we found in a code not equivalent to the QR code. The "not extremal" for $k > 6$ means that for all possible codes a weight smaller than d was found. In case we were unable to find a weight smaller than d the field is left with a blank.

The weights have been computed using the computer algebra-system MAGMA. The cases with p small we ruled out by a direct enumeration of codewords. For p large, the algorithm described in the Theorem was used. The problem which turned out is that little can be said about the automorphism group of duadic codes different from QR codes. But since they are extended cyclic codes they possess at least two automorphisms, namely σ of order p and μ_2 of order $s(p)$. Furthermore if $s(p)$ is not prime then $\langle {\mu_2}^i \rangle$ for some i can be used instead of H in the Theorem. Therefore we have included the prime factorization of $s(p)$ in the second column.

Based on the information from the table below there is some evidence for the

Conjecture. There are no extremal self-dual doubly-even codes having an automorphism of prime order $p > n/2 \geq 24$ apart from the cases listed in Theorem.

p	$s(p)$	k	Num of Codes	d	w found
127	$7= 7^1$	18	29	24	not extremal
151	$15= 3^1 \cdot 5^1$	10	4	28	not extremal
223	$37= 37^1$	6	2	40	36
431	$43= 43^1$	10	4	76	not extremal
439	$73= 73^1$	6	2	76	72
631	$45= 3^2 \cdot 5^1$	14	10	108	not extremal
727	$121= 11^2$	6	2	124	112
911	$91= 7^1 \cdot 13^1$	10	4	156	not extremal
919	$153= 3^2 \cdot 17^1$	6	2	156	144
1103	$29= 29^1$	38	13798	188	
1327	$221= 13^1 \cdot 17^1$	6	2	224	208
1399	$233= 233^1$	6	2	236	
1423	$237= 3^1 \cdot 79^1$	6	2	240	232
1471	$245= 5^1 \cdot 7^2$	6	2	248	236
1831	$305= 5^1 \cdot 61^1$	6	2	308	300
1999	$333= 3^2 \cdot 37^1$	6	2	236	308
2143	$51= 3^1 \cdot 17^1$	42	49933	360	
2287	$381= 3^1 \cdot 127^1$	6	2	384	380
2351	$47= 47^1$	50	671089	396	
2383	$397= 397^1$	6	2	400	
2671	$445= 5^1 \cdot 89^1$	6	2	448	416
2687	$79= 79^1$	34	3856	452	
2767	$461= 461^1$	6	2	464	
2791	$465= 3^1 \cdot 5^1 \cdot 31^1$	6	2	468	436
3191	$55= 5^1 \cdot 11^1$	58	9256396	536	
3271	$545= 5^1 \cdot 109^1$	6	2	548	540
3343	$557= 557^1$	6	2	560	
3391	$113= 113^1$	30	1093	568	
3463	$577= 577^1$	6	2	580	
3601	$601= 601^1$	6	2	604	
3631	$605= 5^1 \cdot 11^2$	6	2	608	596
3823	$637= 7^2 \cdot 13^1$	6	2	640	612

References

[1] S. Bouyuklieva, W. Willems, Notes on automorphism groups of extremal codes. *Proc. ACCT,* Pamporovo 2008, 16-22.

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

[3] W. C. Huffman, V. Job, V. Pless, Multipliers and generalized multipliers of cyclic codes and cyclic objects. *J. Comb. Theory* A-62, 1993, 183-215.

[4] J. S. Leon, J. M. Masley, V. Pless, Duadic codes, *IEEE Trans. Inform. Theory* 30, 1984, 709-714.

[5] J. S. Leon, J. M. Masley, V. Pless, On weights in duadic codes. *J. Comb. Theory* A-44, 1987, 6-21.

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

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

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

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

[10] S. Zhang, On the nonexistence of extremal self-dual codes, *Discr. Appl. Math.* 91, 1999, 277-286.