Self-dual codes of length 56 with an automorphism of order 5 and self-orthogonal 3-(56, 12, 65) designs

NIKOLAY YANKOV jankov_niki@yahoo.com
Faculty of Mathematics and Informatics, Shumen University, Shumen, BULGARIA

Abstract. We apply a method for constructing binary self-dual codes possessing an automorphism of odd prime order p from [1] and [2]. Using this method we give full classification of optimal binary self-dual $[56, 28, 12]$ codes having an automorphism of order 5 with 10 cycles and 6 fixed points.

The main idea of the method is to decompose the binary self-dual code C into a direct sum of two subcodes. The first subcode $F_\sigma(C)$ is the so called "fixed subcode" consisting of all codewords invariant under the action of the automorphism. The second $E_\sigma(C)$ (the "even subcode") contains all vectors from the code that have even weight on all cycles and zeroes on the fixed points.

In order to construct binary self-dual codes with an automorphism of order 5 having 10 cycles we construct all possible generator matrices for E_σ. It turns out that there are exactly 56 generator matrices, named H_i, $i = 1 \ldots, 56$. Using H_i we prove that there does not exist singly-even self-dual $[56, 28, 12]$ code possessing an automorphism of order 5. Thus by [3, Corollary 1] and [4, Table 3] we prove that there does not exist a singly-even self-dual $[56, 28, 12]$ code with an automorphism of odd prime order $p > 3$.

Next we examine the case of the doubly-even self-dual $[56, 28, 12]$ codes. After finding all possibilities for the subcode F_σ we need to attach the two subcodes. To easily do that assume that E_σ is fixed and we use the right transversal of the symmetric group S_{10} with respect to the automorphism group of F_σ. Also since we looking for optimal codes we need to find only codes with minimum distance $d = 12$. Finally, we need to sort the codes for equivalence. It turns out that there are exactly 3763 inequivalent doubly-even self-dual $[56, 28, 12]$ codes having an automorphism of order 5. In [5] exactly 1151 inequivalent such codes are described. One of these codes have an automorphism of order 7 and none of order 5. Thus all 1151 constructed codes are new. Since every code have an automorphism of order 5 it is easy to describe such a code using just a permutation for F_σ and H_i, $i = 1, \ldots, 56$ for the generators of E_σ.

There are also 4202 inequivalent binary doubly-even $[56, 28, 12]$ self-dual

codes having an automorphism of type $7-(8,0)$ (see [3]). None of these codes have an automorphism of order 5 and thus we have that there exist at least 9115 inequivalent doubly-even self-dual $[56,28,12]$ codes.

In [5] it was proved that any binary doubly-even $[56,28,12]$ self-dual codes generates a self-orthogonal $3-(56,12,65)$ design with block intersection numbers $0,2,4,6$. Two inequivalent extremal doubly-even self-dual codes of length 56 give two non-isomorphic self-orthogonal $3-(56,12,65)$ designs. So we prove that there are at least 9115 inequivalent self-orthogonal $3-(56,12,65)$ designs with block intersection numbers $0,2,4,6$.

For computing the automorphism groups of the codes and for checking code isomorphism we use the computer algebra system Q-extension by Iliya Bouyukliev [6]. For finding right cosets and right transversals we use the system for computational discrete algebra GAP v.4.4 [7]. All assembling of the codes F_σ and E_σ as well as the optimality check was done by the author using the programming language Delphi.

References

[1] W. C. Huffman, "Automorphisms of codes with application to extremal doubly-even codes of length 48," vol. 28, pp. 511–521, 1982.

[2] V. Yorgov, "A method for constructing inequivalent self-dual codes with applications to length 56," vol. 33, pp. 77–82, 1987.

[3] N. Yankov and R. Russeva, "Binary self-dual codes of lengths 52 to 60 with an automorphism of order 7 or 13," vol. 56, pp. 7498–7506, 2011.

[4] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Appl.*, vol. 11, pp. 451–490, 2005.

[5] M. Harada, "Self-orthogonal $3-(56,12,65)$ designs and extremal doubly-even self-dual codes of length 56," *Designs, Codes and Cryptography*, vol. 38, pp. 5–16, 2006.

[6] I. Bouyukliev, *About the code equivalence, Advances in Coding Theory and Cryptography*, ser. Series on coding theory and cryptology, vol. 3. World Scientific Publishing, 2007.

[7] *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, The GAP Group, 2008. [Online]. Available: (http://www.gap-system.org)