On binary self-dual extremal codes

Wolfgang Willems

***Abstract*— There is a large gap between Zhang's theoretical bound for the length n of a binary extremal self-dual doubly-even code and what we can construct. The largest n is 136. In order to find examples for larger n a non-trivial automorphism group might be helpful. In the list of known examples extended quadratic residue codes and quadratic double circulant codes have large automorphism groups. But in both classes the extremal ones are all known. They are exactly those which are in the list; hence of small length. The investigations we have done so far give some evidence that for larger n the automorphism group of a putative extremal self-dual doubly-even code may be very small, if not trivial. Thus the code merely seems to be a big combinatorial object and therefore possibly hard to find.**

Due to Mallows-Sloane [7] and Rains [9] a binary self-dual code C of length n and minimum distance d satisfies

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

We call C *extremal* if equality holds. If in addition $24 \mid n$ then C is always doubly-even. Extremal doubly-even codes do not exist for large n as noticed already in [7]. More precisely, by a result of Zhang [11], we have $n \leq 3928$ for such codes. Note that, as far as the autor is aware, the existence of a length-bound for singly-even extremal codes is still open. However, the largest n for which an extremal code has been found is $n = 136$. Thus there is a large gap between the bound of doubly-even extremal codes and what we really can construct.

On the other hand, constructing a 'big combinatorial object' the existence of non-trivial automorphisms may be helpful. Thus in order to prove the existence of an extremal code a non-trival automorphism group might be of interest. Looking at the lengths for which doubly-even extremal codes exist, i.e.,

$$n = 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136$$

(see [8], [6]) there always is a code with non-trivial automorphism group. The groups even act transitely on the coordinate positions and are in many cases relatively large and non-solvable.

However, the investigations we have done so far give some evidence that for large n the automorphism group of an extremal code seems to have only small primes in its order and may be very small if not trivial. For instance, if $p \geq 5$ is a prime dividing $|\mathrm{Aut}(C)|$ and $p \geq \frac{n}{2}$ then $p = n - 1$ (see [1]). Extended doubly-even quadratic residue codes satisfy this condition. But the extremal ones are all known. They exist only in dimensions

$$n = 8, 24, 32, 48, 80, 104$$

(see [1]). One other class of doubly-even codes, the so-called quadratic double circulant codes of length $n = 2q + 2$ where $q \equiv 3 \bmod 8$ is a prime have automorphisms of order q. Thus there is again an automorphism of relative large order relative to n. However, due to a recent result of Malevich they are extremal only if

$$n = 8, 24, 40, 88, 136.$$

In all other known cases the primes in $|\mathrm{Aut}(C)|$ are small.

In the special special case of a putative self-dual $[72, 36, 16]$ code the automorphism group has order $5, 7, 10, 14$, or d where d divides 18 or 24, or $G = \mathrm{A}_4 \times C_3$. In particular, $\mathrm{Aut}(C)$ contains at most the primes $2, 3, 5$ and 7 in its order (see [2], [3], [10]). The order of the automorphism group of a putative self-dual $[96, 48, 20]$ code contains at most the primes $2, 3$ and 5 (see [4]). Here a bound for the order is still unknown. Due to recent investigations of de la Cruz the order of the automorphism group of a putative self-dual $[120, 60, 24]$ code also seems to contain only small primes.

If these observations turn out to be true in general (there are more indications of evidence as mentioned above) then an extremal code of large length carries only the structure of a 'big combinatorial object', without symmetries or only symmetries of a very small order. As a consequence the code is therefore possibly hard to construct if it exists.

In proving the non-existence one may try to improve the bound of Zhang. Surprisingly, Duursma used in [5] completely different methods, more elementary and avoiding invariant theory, but ended up with exactly the same bound as Zhang did. The reason might be caused by the fact that both authors only use the weight distribution which is uniquely determined. If the bound can be improved then further ingredients on the structure of the code, which we do not see how to apply useful in a proof, have to come in.

W. Willems is with the Faculty of Mathematics, Otto-von-Guericke-University, 39106 Magdeburg, Germany willems@ovgu.de

References

[1] S. Bouyuklieva, A. Malevich and W. Willems, Automorphisms of extremal self-dual codes, to appear IEEE Trans. Inform. Theory.

[2] S. Bouyuklieva, E.A. O'Brien and W. Willems, The automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code is solvable, *IEEE Trans. Inform. Theory*, vol. 52, 2006, pp 4244-4248.

[3] E.A. O'Brien and W. Willems, On the automorphism group of a binary self-dual $[72, 36, 16]$ code, to appear.

[4] R. Dontcheva, On the doubly-even self-dual codes of length 96, *IEEE, Trans. Inform. Theory*, vol. 48, 2002, pp 557-561.

[5] I. Duursma, Extremal weight enumerators and ultraspherical polynomials, *Discrete Math.*, vol. 268, 2003, pp 103-127.

[6] M. Harada, An extremal doubly even self-dual code of length 12, *Electr. J. Combin.*, vol. 15, 2008, .

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

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

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

[10] V. Yorgov, On the automorphism group of a putative code, *IEEE Trans. Inform. Theory*, vol. 52, 2006, pp 1724-1726.

[11] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.*, vol. 91, 1999, pp 277-286.