A Prize Problem in Coding Theory

Jon-Lark Kim

Department of Mathematics, University of Louisville, Louisville, KY 40292, USA
jl.kim@louisville.edu

Summary. In this short note, we describe one of the long-standing open problems in algebraic coding theory, i.e., whether there exists a binary self-dual $[72, 36, 16]$ code.

1 Introduction

Binary self-dual codes or self-dual codes over finite fields in general have been of great interest partly because many good linear block codes are either self-orthogonal or self-dual. It turns out that they satisfy a nonconstructive lower bound, analogous to the Gilbert-Varshamov bound in linear codes. Furthermore, they have nice algebraic properties; in particular, the weight enumerator of a self-dual code over a finite field is invariant under a certain finite matrix group, which further restricts the minimum distance of a self-dual code over $GF(2)$, $GF(3)$, or $GF(4)$. We refer to [13], [9] for a full discussion of self-dual codes.

A binary self-dual code C under the usual inner product is called a *Type II (or doubly-even) code* if all codewords have weight $\equiv 0 \pmod 4$, and a *Type I (or singly-even) code* if there is a codeword whose weight $\equiv 2 \pmod 4$. Given a binary Type I code C, one can obtain the doubly-even subcode C_0 of C (consisting of all codewords whose weight $\equiv 0 \pmod 4$). The *shadow* S of C is defined by $S := C_0^{\perp} \backslash C$ [1]. The weight enumerator $S(x, y)$ of the shadow of C is determined by the weight enumerator $C(x, y)$ of C as $S(x, y) = \frac{1}{|C|} C(x + y, i(x - y))$, where $i = \sqrt{-1}$. This additional relation gives a further restriction on a possible weight enumerator of a binary self-dual code, often proving the nonexistence of a putative binary self-dual code [1].

Using $C(x, y)$ and $S(x, y)$ in a sophisticated way, Rains [12] derived a tight upper bound on the minimum distance of a binary self-dual code. More precisely, if C is a binary self-dual code of length n with minimum distance d then $d \leq 4\lfloor n/24 \rfloor + 4$ except when $n \equiv 22 \pmod{24}$, in which case $d \leq 4\lfloor n/24 \rfloor + 6$ (see [12]). Further if C is a Type I code of length $n \equiv 0 \pmod{24}$, then $d \leq 4\lfloor n/24 \rfloor + 2$. A Type I self-dual code whose minimum distance d attains this bound is called *extremal*. A Type II code of length n with minimum distance $d = 4\lfloor n/24 \rfloor + 4$ is called *extremal*.

It has been one of important problems in coding theory to find (binary) extremal self-dual codes (see [6] for recent results on extremal self-dual codes over $GF(2)$, $GF(3)$, $GF(4)$, Z_4, $GF(2)+uGF(2)$, and $GF(2)+vGF(2)$), due to their connection with other mathematical areas including designs, lattices, and modular forms [11], [9].

In particular, one of the most famous open problems is the following.

Problem : Does there exist a Type II $[24k, 12k, 4k+4]$ code $C(k)$ for $k \geq 3$?

We note the following results.

1. If $k = 1$, then $C(1)$ is the Type II $[24, 12, 8]$ code (the binary extended Golay code). In fact, any binary linear code with parameters $[24, 12, 8]$ is equivalent to $C(1)$ (Pless, 1968 [10]).
2. If $k = 2$, then $C(2)$ is the extended quadratic residue code XQ_{47} of length 48. This is unique up to equivalence among self-dual codes with parameters $[48, 24, 12]$ (Houghten, Lam, Thiel, and Parker, 2003 [5]). It is not known whether there is a linear binary $[48, 24, 12]$ code other than XQ_{47}.
3. **The existence of a Type II $[72, 36, 16]$ code $C(3)$ is one of the long-standing open problems in coding theory.** This was officially suggested by Sloane in 1973 [14]. If it exists, then the codewords of weight 16 form a 5 - $(72, 16, 78)$ design whose existence is unknown.
4. If $k \geq 154$, then $C(k)$ does not exist since A_{4k+8} (the number of codewords of weight $4k+8$) is negative ([15]).

2 Related facts about a putative Type II $[72, 36, 16]$ code

The weight enumerator of a putative Type II $[72, 36, 16]$ code $C(3)$ is given as follows.

$W = 1 + 249,849y^{16} + 18,106,704y^{20} + 462,962,955y^{24} + 4,397,342,400y^{28} + +16,602,715,899y^{32} + 25,756,721,120y^{36} + \cdots$.

One possible attack to prove or disprove the existence of $C(3)$ is to investigate the order of the automorphism group of $C(3)$. The only possible *prime orders* of an automorphism of $C(3)$ are $2, 3, 5$, and 7. It is remarked [6] that Yorgov recently proved that the automorphism group has order a divisor of 72 or order $504, 252, 56, 14, 7, 360, 180, 60, 30, 10$, or 5.

Another attack is to construct codes related to $C(3)$. The existence of $C(3)$ is equivalent to that of a Type I $[70, 35, 14]$ code (Rains, 1998 [12]). The weight enumerator of a Type I $[70, 35, 14]$ code is corrected in [6] as follows:

$W = 1 + 11,730y^{14} + 150,535y^{16} + 1,345,960y^{18} + \cdots$.

Gulliver, Harada, and Kim [4] showed that the existence of $C(k)$ implies the existence of a Type I $[24k, 12k, 4k+2]$ code for $k \geq 1$. Hence if there is $C(3)$, then there is a Type I $[72, 36, 14]$ code. Equivalently, if there is no Type I $[72, 36, 14]$ code, there is no $C(3)$. No self-dual codes with parameters $[72, 36, 14]$ are known to exist. There are exactly three possible weight enumerators for a Type I $[72, 36, 14]$ code as follows.

$W_1 = 1 + 7616y^{14} + 134,521y^{16} + 1,151,040y^{18} + \cdots,$
$W_2 = 1 + 8576y^{14} + 124,665y^{16} + 1,206,912y^{18} + \cdots,$
$W_3 = 1 + 8640y^{14} + 124,281y^{16} + 1,207,360y^{18} + \cdots$

3 Future work

There is a hope that $C(3)$ might exist. For example, although it is not known yet whether there exists a binary linear $[72, 36, 16]$ code, there is a $[72, 36, 15]$ code by puncturing a $[73, 36, 16]$ cyclic code and any $[72, 36, d]$ code satisfies $d \leq 17$ from Brouwer's Table.

A recent attempt to construct $C(3)$ was made by Dougherty, Kim, and Solé [2] by considering double circulant codes based on strongly regular graphs and doubly regular tournaments. In particular, SRG (Strongly Regular Graphs) with parameters $(36, 15, 6, 6)$ produce a lot of Type II $[72, 36, 12]$ codes. Similarly DRT (Doubly Regular Tournaments) of order 36 produce Type II $[72, 36, 8$ or $12]$ codes. It is hoped that $d = 16$ is possible if there is enough data for DRT of the above parameters.

Furthermore, recently we [7] have shown that skew Hadamard matrices of order $4m$ where a prime p divides m produce self-dual codes over $GF(p)$. In particular, if $m = 18$, then we have plenty of Type II $[72, 36, 12]$ codes with various weight enumerators from the 990 skew Hadamard matrices of order 72 in [8]. This motivates an active search for more skew Hadamard matrices of order 72.

From the viewpoint of the Groebner basis, it is shown [3] how to construct the input basis of a zero-dimensional polynomial ideal, whose solutions correspond to binary systematic non-linear codes with fixed parameters (length, dimension, and distance). It is obvious how to specialize it to classify binary linear codes. By computing the Groebner basis G of Guerrini-Sala's ideal B for parameters $[72, 36, 16]$, we would immediately have a complete classification for such codes, if they exist. In particular, if G turns out to be trivial ($G = \{1\}$), then there are no such codes. If it is not trivial, its solutions can be tested whether they are self-dual. However, it is well possible that the computation of G is infeasible, since I has $36^2 = 1296$ variables.

4 Monetary Prizes

As far as we know, the existence of $C(3)$ is the only coding problem with monetary prizes. The detail can be found from http://academic.scranton.edu/faculty/doughertys1/

- N.J.A. Sloane offers $10 (1973) - still valid (confirmed in 2006)
- F.J. MacWilliams offered $10 (1977) - invalid now.

The following monetary prizes were announced in the Yamagata conference, October, 2000, and at WCC2001 in Paris.

- S.T. Dougherty offers $100 for the existence of $C(3)$.
- M. Harada offers $200 for the nonexistence of $C(3)$.

The prize is awarded only once and the result must be published in a refereed reputable mathematics journal. All decisions about the prize are decided by those offering the prize.

Acknowledgement: The author would like to thank Dr. Massimiliano Sala for his remark on the Groebner basis in Section 3.

References

1. Conway JH, Sloane NJA (1990) A new upper bound on the minimal distance of self-dual codes. IEEE Trans. Inform. Theory 36:1319–1333.
2. Dougherty ST, Kim J-L, Solé P (2007) Double circulant codes from two class association schemes. Advances in Mathematics of Communications 1:45–64.
3. Guerrini E, Sala M (2007) An algebraic approach to the classification of some non-linear codes. Workshop on Coding and Cryptography 2007, INRIA, 177–185.
4. Gulliver TA, Harada M, Kim J-L (2003) Construction of some extremal self-dual codes. Discrete Math 263:81–91.
5. Houghten SK, Lam CWH, Thiel LH, Parker JA (2003) The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code. IEEE Trans. Inform. Theory 49:53–59.
6. Huffman WC (2005) On the classification and enumeration of self-dual codes. Finite Fields and Their Applications 11:451–490.
7. Kim J-L and Solé P (2008) Skew Hadamard designs and their codes, to appear in Designs, Codes, and Cryptography.
8. Kotsireas I, http://www.medicis.polytechnique.fr/∼kotsirea/
9. Nebe G, Rains EM, Sloane NJA (2006) *Self-Dual Codes and Invariant Theory,* Series: Algorithms and Computation in Mathematics, vol. 17, Berlin, Springer.
10. Pless V(1968) On the uniqueness of the Golay codes. J. Combin. Theory, 5: 215–228.
11. Pless VS, Huffman WC, Eds. *Handbook of Coding Theory*, Amsterdam. The Netherlands: Elsevier, 1998.
12. Rains EM (1998) Shadow bounds for self-dual codes. IEEE Trans. Inform. Theory, 44:134–139.
13. Rains EM, Sloane NJA (1998) Self-dual codes. in *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, pp. 177–294.
14. Sloane NJA (1973) Is there a $(72, 36)$ $d = 16$ self-dual code. IEEE Trans. Inform. Theory 19:251.
15. Zhang S (1999) On the nonexistence of extremal self-dual codes. Discrete Appl. Math. 91:277–286.