J. Algebra Comb. Discrete Appl.
5(1) • 1–4

Received: 27 December 2016
Accepted: 6 April 2017

Journal of Algebra Combinatorics Discrete Structures and Applications

Ternary maximal self-orthogonal codes of lengths $21, 22$ and 23

Research Article

Makoto Araya, Masaaki Harada, Yuichi Suzuki *

Abstract: We give a classification of ternary maximal self-orthogonal codes of lengths $21, 22$ and 23. This completes a classification of ternary maximal self-orthogonal codes of lengths up to 24.

2010 MSC: 94B05

Keywords: Ternary code, Self-dual code, Self-orthogonal code

1. Introduction

A ternary $[n, k]$ *code* C is a k-dimensional vector subspace of $\mathbb{F}_3^n$, where $\mathbb{F}_3$ denotes the finite field of order 3. All codes in this note are ternary. The parameters n and k are called the *length* and the *dimension* of C, respectively. The *weight* of a vector $x \in \mathbb{F}_3^n$ is the number of non-zero components of x. A vector of C is a *codeword* of C. The minimum non-zero weight of all codewords in C is called the *minimum weight* of C. Two codes C and C' are *equivalent* if there is a $(0, 1, -1)$-monomial matrix P with $C' = C \cdot P = \{xP \mid x \in C\}$, and *inequivalent* otherwise. The *automorphism group* $\mathrm{Aut}(C)$ of C is the group of all $(0, 1, -1)$-monomial matrices P with $C = C \cdot P$.

The *dual* code $C^\perp$ of a code C of length n is defined as $C^\perp = \{x \in \mathbb{F}_3^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y$ is the standard inner product. A code C is *self-dual* if $C = C^\perp$, and C is *self-orthogonal* if $C \subset C^\perp$. A self-dual code of length n exists if and only if $n \equiv 0 \pmod 4$. A self-orthogonal code C is *maximal* if C is the only self-orthogonal code containing C. A self-dual code is automatically maximal. The dimension of a maximal self-orthogonal code of length n is a constant depending only on n. More precisely, a maximal self-orthogonal code of length n has dimension $(n-1)/2$ if n is odd, $n/2-1$ if $n \equiv 2 \pmod 4$ (see [8]).

Makoto Araya (Corresponding Author); Department of Computer Science, Shizuoka University, Hamamatsu 432–8011, Japan (email: araya@inf.shizuoka.ac.jp).
Masaaki Harada; Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan (email: mharada@m.tohoku.ac.jp).
Yuichi Suzuki; Hitachi Systems, Ltd., 1–2–1, Osaki, Shinagawa-ku, Tokyo, 141–0032, Japan.
** This author carried out his work at Yamagata University.*

http://dx.doi.org/10.13069/jacodesmath.327391 ISSN 2148-838X

A classification of maximal self-orthogonal codes of lengths up to 12, lengths $13, 14, 15, 16$ and lengths $17, 18, 19, 20$ was done in [8], [2] and [9], respectively (see [4] for lengths 18 and 19). In this note, we give a classification of maximal self-orthogonal codes of lengths $21, 22$ and 23. The mass formula is used to verify that our classification is complete. Since a classification of self-dual codes of length 24 was done in [3], our result completes a classification of maximal self-orthogonal codes of lengths up to 24.

2. Classification results

Let C be a code of length n and let $S = \{i_1, i_2, \dots, i_j\}$ be a subset of $\{1, 2, \dots, n\}$. A *shortened code* of C is the set by selecting only the codewords of C having zeros in each of the coordinate positions $i_1, i_2, \dots, i_j$ and deleting these components. Throughout this note, we denote the code by $C(S)$. All maximal self-orthogonal codes of lengths $4m+1, 4m+2, 4m+3$ can be obtained from self-dual codes of length $4m+4$ as shortened codes (see [2]).

For length 24, there are 338 inequivalent self-dual codes, two of which have minimum weight 9, 166 of which have minimum weight 6 and 170 of which have minimum weight 3 [3] and [7]. From the 338 self-dual codes C of length 24, we found maximal self-orthogonal codes of lengths 23 and 22, which must be checked further for equivalences, as shortened codes $C(S)$ by considering all sets S with $|S| = 1$ and 2, respectively. This computer calculation was done by using the Magma [1] function `ShortenCode`. Then we determined the equivalence or inequivalence of two codes among the maximal self-orthogonal codes. This calculation was done by the Magma function `IsIsomorphic`. Then we have 13625 and 2005 inequivalent maximal self-orthogonal codes of lengths 22 and 23, respectively. Note that the dimensions of maximal self-orthogonal codes of lengths 21 and 22 are 10. The 126 codes among the 13625 maximal self-orthogonal codes of length 22 have a zero coordinate. Hence, 216 inequivalent maximal self-orthogonal codes of length 21 are obtained, as shortened codes. We denote by $\mathcal{C}(n, d)$ the set of the inequivalent maximal self-orthogonal codes of length n and minimum weight d for $(n, d) = (21, 3)$, $(21, 6)$, $(22, 3)$, $(22, 6)$, $(22, 9)$, $(23, 3)$, $(23, 6)$ and $(23, 9)$. In addition, we define subsets of $\mathcal{C}(n, d)$:

$$\mathcal{C}(n, d, d') = \{C \in \mathcal{C}(n, d) \mid d(C^\perp) = d'\},$$

where $d(C)$ denotes the minimum weight of C. The numbers $|\mathcal{C}(n, d, d')|$ are listed in Table 1.

As a check, in order to verify that $\mathcal{C}(n, d)$ contains no pair of equivalent codes for the above (n, d), we employed the following method obtained by applying the method given in [6, Section 2]. Let C be a code of length n. Suppose that t is a positive integer such that the codewords of weight t generate C. Let A_t denote the number of codewords of weight t in C. We expand each codeword of C into a binary vector of length $2n$ by mapping the elements $0, 1$ and 2 of $\mathbb{F}_3$ to the binary vectors $(0, 0), (0, 1)$ and $(1, 0)$, respectively. In this way, we have an $A_t \times 2n$ binary matrix $M(C, t)$ composed of the binary vectors obtained from the A_t codewords of weight t in C. Then, from $M(C, t)$, we have an incidence structure $\mathcal{D}(C, t)$ having $2n$ points. This calculation was done by using the Magma function `IncidenceStructure`. If C and C' are equivalent, then $\mathcal{D}(C, t)$ and $\mathcal{D}(C', t)$ are isomorphic. By the Magma function `IsIsomorphic`, we verified that the incidence structures $\mathcal{D}(C, t)$ are non-isomorphic for the above (n, d). This shows that $\mathcal{C}(n, d)$ contains no pair of equivalent codes for the above (n, d).

The number of distinct maximal self-orthogonal codes of length n is known [8] as:

$$N(n) = \begin{cases} \prod_{i=1}^{(n-1)/2}(3^i+1) & \text{if } n \text{ is odd}, \\ \prod_{i=2}^{n/2}(3^i+1) & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

We calculated the following values:

$$T(n, d, d') = \sum_{C \in \mathcal{C}(n,d,d')} \frac{2^n \cdot n!}{|\operatorname{Aut}(C)|}.$$

The results are listed in Table 1. The automorphism groups of the codes were calculated by the Magma function `AutomorphismGroup`. We remark that the automorphism group of a code C is isomorphic to the

Table 1. $|\mathcal{C}(n, d, d')|$ **and** $T(n, d, d')$**.**

(n, d, d')	$\lvert\mathcal{C}(n, d, d')\rvert$	$T(n, d, d')$
(21, 3, 1)	18	3726123366661269504000 0
(21, 3, 3)	129	22666803510606607679488000
(21, 6, 1)	6	1569126209257255993344 00
(21, 6, 4)	59	221566090068991210527129600
(21, 6, 6)	4	28572125748609278803968000
(22, 3, 1)	147	499079550803678108594176000
(22, 3, 2)	671	8999173098190687835078656000
(22, 3, 3)	3606	39745065815646420244417740800 0
(22, 6, 1)	69	5504766786817393746876825600
(22, 6, 2)	458	116255553756749319466332979200
(22, 6, 4)	6528	8198363298466655101459523174400
(22, 6, 5)	2142	3362889158614819168464981196800
(22, 9, 7)	4	353580056139039825199104000
(23, 3, 2)	153	23004306466349702422944153600
(23, 3, 3)	728	1838692744522339728778225254400
(23, 6, 2)	63	25313987440741169520307077120 0
(23, 6, 5)	1059	46245009828325897079698017484800
(23, 9, 8)	2	1414320224556159300796416000

stabilizer of $\{\{1,2\},\{3,4\},\ldots,\{2n-1,2n\}\}$ inside of the automorphism group of the incidence structure $\mathcal{D}(C,t)$. In order to verify the correctness of the above calculations of the automorphism groups, we also calculated the stabilizers for $\mathcal{D}(C,t)$. This was done by the MAGMA function `Stabilizer`. Finally, as a check, we verified the mass formula:

$$\begin{aligned}
N(21) =& T(21,3,1) + T(21,3,3) + T(21,6,1) + T(21,6,4) + T(21,6,6), \\
N(22) =& T(22,3,1) + T(22,3,2) + T(22,3,3) + T(22,6,1) \\
&+ T(22,6,2) + T(22,6,4) + T(22,6,5) + T(22,9,7), \\
N(23) =& T(23,3,2) + T(23,3,3) + T(23,6,2) + T(23,6,5) + T(23,9,8).
\end{aligned}$$

The mass formula shows that there is no other maximal self-orthogonal code of lengths $21, 22$ and 23. We summarize a classification of maximal self-orthogonal codes of lengths 21, 22 and 23.

Proposition 2.1. (1) *Up to equivalence, there are* 216 *maximal self-orthogonal codes of length* 21*,* 147 *of which have minimum weight* 3 *and* 69 *of which have minimum weight* 6*.*

(2) *Up to equivalence, there are* 13625 *maximal self-orthogonal codes of length* 22*,* 4424 *of which have minimum weight* 3*,* 9197 *of which have minimum weight* 6 *and* 4 *of which have minimum weight* 9*.*

(3) *Up to equivalence, there are* 2005 *maximal self-orthogonal codes of length* 23*,* 881 *of which have minimum weight* 3*,* 1122 *of which have minimum weight* 6 *and* 2 *of which have minimum weight* 9*.*

Remark 2.2. *Generator matrices of all the maximal self-orthogonal codes of lengths* $21, 22$ *and* 23 *can be obtained electronically from [5].*

Acknowledgment: The first and second authors would like to thank Ken Saito for helpful discussions on the classification method given in [6]. The first author would also like to thank the Graduate School of Information Sciences, Tohoku University for the hospitality during his visit in August and December 2016. This work is supported by JSPS KAKENHI Grant Numbers 15H03633 and 15K04976.

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symb. Comput. 24(3–4) (1997) 235–265.
[2] J. Conway, V. Pless, N. J. A. Sloane, Self–dual codes over GF(3) and GF(4) of length not exceeding 16, IEEE Trans. Inform. Theory 25(3) (1979) 312–322.
[3] M. Harada, A. Munemasa, A complete classification of ternary self–dual codes of length 24, J. Combin. Theory Ser. A 116(5) (2009) 1063–1072.
[4] M. Harada, A. Munemasa, On the classification of weighing matrices and self–orthogonal codes, J. Combin. Des. 20(1) (2012) 40–57.
[5] M. Harada, A. Munemasa, Database of Ternary Maximal Self–Orthogonal Codes, http://www.math.is.tohoku.ac.jp/~munemasa/research/codes/mso3.htm.
[6] C. W. H. Lam, L. Thiel, A. Pautasso, On ternary codes generated by Hadamard matrices of order 24, Congr. Numer. 89 (1992) 7–14.
[7] J. Leon, V. Pless, N. J. A. Sloane, On ternary self–dual codes of length 24, IEEE Trans. Inform. Theory 27(2) (1981) 176–180.
[8] C. L. Mallows, V. Pless, N. J. A. Sloane, Self–dual codes over GF(3), SIAM J. Appl. Math. 31(4) (1976) 649–666.
[9] V. Pless, N. J. A. Sloane, H. N. Ward, Ternary codes of minimum weight 6 and the classification of the self–dual codes of length 20, IEEE Trans. Inform. Theory 26(3) (1980) 305–316.