Title	Special Self-Dual Codes over $ \mathbb{F}_4$(Theory and Applications of Combinatorial Designs with Related Field)
Author(s)	Betsumiya, Koichi
Citation	数理解析研究所講究録 (2006), 1465: 119-125
Issue Date	2006-01
URL	http://hdl.handle.net/2433/48021
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1465 巻 2006 年 119-125

Special Self-Dual Codes over $\mathbb{F}_4$*

上武大学・ビジネス情報学部　別宮 耕一 (Koichi Betsumiya)
Department of Business Information Sciences
Jobu University

1 Statement of the result

The notion "special self-dual codes" in the title of this proceeding is just defined for this conference temporarily not common terminology. In this proceeding we call a self-dual code of length 16 over $\mathbb{F}_4$ *special* if the Frobenius automorphism does not preserve the complete weight enumerator of the code.

Our purpose of this proceeding is to enumerate the special codes. In order to do this, we give a classification of Type I codes of length 16 over $\mathbb{F}_4$ by means of Munemasa's method [3]. Consequently we find that there exist precisely 9858 codes up to permutation-equivalence. 2948 codes of them are the special codes.

In order to obtain this result, we calculated by means of the software package MAGMA on an AMD Opteron 242 (64bits 1.6MHz) machine Linux-operated. We needed about 2 hours for the total calculation.

We organize this proceeding as following. First, we give necessary terminology in Section 2. In Section 3 we introduce a background of this work. In Section 6 we give the main result of this proceeding — an enumeration of special codes. In Section 4 and Section 5, we give a classification $[16, 7]$-self-orthogonal codes and Type I code of length 16 respectively to show the main result.

2 Notation and Definitions

Let $\mathbb{F}_4$ be the finite field constructed by 4 elements $\{0, 1, \omega, \omega^2\}$ where $\omega^2 + \omega + 1 = 0$. A *linear code* of length n is a subspace of the vector space $\mathbb{F}_4^n$. A $[n, k]$-code is a code of

*This work was partially supported by the MEXT, Japan, Grant-in-Aid for Young Scientists (B) (16740023).

length n of dimension k. With respect to a inner product $(\ ,\ )$, we define the *dual code* of a code C to be

$$C^{\perp} = \{u \in \mathbb{F}_4^n \mid (u, v) = 0 \text{ for all } v \in C\}.$$

If $C = C^{\perp}$, C is said to be *self-dual*. If $C \subset C^{\perp}$, C is said to be *self-orthogonal*. Through this proceeding we fix the inner product to be the *Euclidean* inner product

$$(u, v) = \sum_{i=1}^{n} u_i v_i.$$

A vector $(c_1, c_2, \ldots, c_n)$ satisfies $\sum_{i=1}^{n} c_i = 0$ and $\sum_{i<j} c_i c_j = 0$ is called *doubly-even*. For a self-dual code C, if every codeword $c \in C$ is doubly-even, C is called *Type II* or *doubly-even*, otherwise C is called *Type I* or *singly-even*.

When a code D is obtained by permutating coordinates of a code C, we call D is permutation-equivalent to C. When a code D is obtained by permutating coordinates and by the Frobenius automorphism operating entrywise of a code C, we call D is equivalent to C where the Frobenius automorphism is a map defined by $x \mapsto x^2$. Let C be a code, S_n be the symmetric group of degree n and $\mathrm{Gal}_{\mathbb{F}_4/\mathbb{F}_2}$ be the Galois group of $\mathbb{F}_4$ over $\mathbb{F}_2$ generated by the Frobenius automorphism. The groups

$$\mathrm{PAut}(C) := \{\sigma \in S_n \mid C = C^{\sigma}\}$$

and

$$\mathrm{Aut}(C) := \{\sigma \in S_n \times \mathrm{Gal}_{\mathbb{F}_4/\mathbb{F}_2} \mid C = C^{\sigma}\}$$

are called the *permutation-automorphism group* and the *automorphism group* of C respectively.

The *complete weight enumerator* of a code C is a polynomial in $\mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]$ defined by

$$\mathrm{cwe}_C(y_0, y_1, y_\omega, y_{\omega^2}) = \sum_{c \in C} \prod_{i=1}^{n} y_{c_i}.$$

Now we define that a *special* code is a self-dual code of length 16 over $\mathbb{F}_4$ of which complete weight enumerator is not preserved by the Frobenius automorphism.

3 Background of this Work

Let M, g_1, g_2 and f be ring homomorphisms on the polynomial ring $\mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]$ defined by $M(y_\alpha) := (1/2)\sum_{\beta \in \mathbb{F}_4} (-1)^{\mathrm{Tr}(\alpha\beta)} y_\beta$, $g_1(y_\alpha) := y_{\alpha+1}$, $g_2(y_\alpha) := y_{\alpha\omega}$ and $f(y_\alpha) := y_{\alpha^2}$.

These homomorphisms are described by matrices indexed by $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ as

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

respectively. Let G and H be groups generated by $\{M, g_1, g_2, f\}$ and $\{M, g_1, g_2\}$ respectively.

It is known that the invariant ring $\mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]^H$ coincides with the ring generated by the complete weight enumerators of self-dual codes (c.f. [2, 4]). The Molien series of H is

$$\sum_{i=0}^{\infty} \dim_i(\mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]^H)t^i = \frac{1 + t^{16}}{(1-t^2)(1-t^4)(1-t^6)(1-t^8)}.$$

The other hand, the Molien series G is

$$\sum_{i=0}^{\infty} \dim_i(\mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]^G)t^i = \frac{1}{(1-t^2)(1-t^4)(1-t^6)(1-t^8)}.$$

These Molien series indicate that $\mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]^G$ is a polynomial ring and

$$\mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]^H = \mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]^G \oplus \mathbb{C}[y_\alpha \mid \alpha \in \mathbb{F}_4]^G \phi_{16}$$

where ϕ_{16} is a complete weight enumerator of special code. An example of such code was constructed in [2] as a double circulant code C_{16}.

From the facts above, it is natural to appear some questions:

- there exists the other example or not,
- there exists a certain standard code like other generators or not.

In order to answer these questions, we will give a classification of such codes in the following sections.

4 Enumeration of $[16, 7]$-Self-Orthogonal Codes Containing 1

In this section we will give a classification of $[16, 7]$-self-orthogonal codes which contain all-one vector by means of the classification of Type II codes of length 16 in [1].

Theorem 4.1 *There exist* 3611 $[16, 7]$*-self-orthogonal codes containing* **1** *up to permutation-equivalence. For* 1469 *of them, the Frobenius map image of the code are permutation-equivalent of itself. Hence, there exist* 2540 $[16, 7]$*-self-orthogonal codes containing* **1** *up to equivalence.*

We will explain how to obtain the theorem. Before doing this, we recall the facts as following.

Proposition 4.2 ([1]) *There precisely exist* 48 *Type II codes of length* 16 *up to permutation-equivalence.*

Proposition 4.3 *Any* $[2k, k-1]$*-self-orthogonal code containing* **1** *is contained in precisely two Type II codes of length* $2k$*.*

Let `C` be a Type II code of length 16. By means of the method in [3], we construct all hyperplanes of `C` up to equivalence with respect to Aut(`C`) action. Repeating the calculation for each Type II code, we obtain distinct 10719 $[16, 7]$-self-orthogonal codes. To classify these codes up to equivalence, we compute the following invariants of each $[16, 7]$-self-orthogonal code `H`:

- The two Type II codes containing `H`,
- The complete weight enumerator of `H`,
- The invariant `twoptdegreeSorted` for weight 8 defined in [3].

For the first invariant, one of the Type II codes is `C` which is the initial Type II code constracting `H`. We obtain the other Type II code `D` containing `H` by means of the following MAGMA script.

```
K<a>:=GF(4);
V:=VectorSpace(K,16);
U:=UniverseCode(K,16);
H0:=VectorSpace(H);
Hd:=VectorSpace(Dual(H));
for v in Transversal(Hd, H0) do
        if v ne 0 and not U!v in C and
           LW(a*v) mod 4 eq 0 and LW(a^2*v) mod 4 eq 0 then
                D:=LinearCode(sub<V | H, v>);
                break v;
        end if;
end for;
```

Here we give an algorithm to obtain `twoptdegreeSorted`. It is clear that this is invariant of equivalence class as well as permutation-equivalence class.

```
supportdesign:=function(C,t)
   return IncidenceStructure< Length(C) |
      { Support(u) : u in C | Weight(u) eq t } >;
end function;
twoptdegreeSorted:=function(C,t)
    des:=supportdesign(C,t);
    return Sort([
       #{b : b in BlockSet(des) | {Point(des,j): j in x } subset b }
          : x in Subsets({1..16},2) ] );
end function;
```

Eventually we obtain 2540 different invariants. Moreover we can verify that the invariant characterizes inequivalence class of codes by means of mass formula as following.

Theorem 4.4 *If n is a positive integer divisible by 4, then the number of the $[n, n/2-1]$-self-orthogonal codes containing 1 is equal to*

$$\begin{aligned}\frac{1}{3}\left(\prod_{i=1}^{n/2-1}(4^i+1)-\prod_{i=0}^{n/2-2}(4^i+1)\right) &= 32563225114005625\\ &= \sum_{C\in\mathcal{C}}\frac{n!\cdot 2}{|\operatorname{Aut}(C)|}\\ &= \sum_{C\in\mathcal{C}'}\frac{n!}{|\operatorname{PAut}(C)|},\end{aligned}$$

where $\mathcal{C}$ and $\mathcal{C}'$ are a complete sets of representatives of equivalence classes of $[n, n/2-1]$-self-orthogonal codes and permutation-equivalence classes of $[n, n/2-1]$-self-orthogonal codes respectively.

There is no build-in command in MAGMA to calculate our automorphism groups. So we calculate the order of automorpshim groups by means of the following MAGMA script which is modified the script in [3]. The function `auto` returns $|\operatorname{PAut}(C)|$ and $|\operatorname{Aut}(C) : \operatorname{PAut}(C)|$.

```
GoodDist:=function(C,cwe);
    U:=Generic(C);
    m1:=U![K!1:i in [1..Length(U)]];
    CF:=sub<U|[U![g^2 : g in Eltseq(C.j)] : j in [1..Dimension(C)]]>;
    mono:=Monomials(cwe);
    for j in [2..#mono-1] do
         if Degree(mono[j],y2) eq Degree(mono[j],y3) and
             MonomialCoefficient(cwe,mono[j]) gt 72 then
                 pow:=<Degree(mono[j],v) : v in [y0,y1,y2]>;
                 break j;
         end if;
    end for;
end function;
```

```
auto:=function(C,cwe);
    pow := GoodDist(C,cwe);
    SP := { Support(u) : u in C |
      <Length(C)-Distance(u,x) : x in [U!0,m1,a*m1]> eq pow};
   D:=IncidenceStructure< Length(C) | SP>;
   A:=PointGroup(D);
   orbit:=C^A;
   if CF in orbit then
       frob:=2;
   else
       frob:=1;
   end if;
   return <#A/#orbit, frob>;
end function;
```

5 Enumeration of Type I Self-Dual Codes

In this section we will give a classification of Type I codes of length 16 by means of the result above.

Theorem 5.1 *There exist* 9858 *Type I codes up to permutation-equivalence. For* 2200 *of them, the Frobenius map image of the code is permutation-equivalent to itself. Hence, there exist* 6029 *Type I codes up to equivalence.*

We will explain how to obtain the theorem. Before doing this, we recall the facts as following.

Proposition 5.2 *Any Type I codes of length* $2k$ *contains a unique* $[2k, k-1]$*-self-orthogonal code.*

Proposition 5.3 *Any* $[2k, k-1]$*-self-orthogonal code is contained in precisely three Type I codes of length* $2k$*.*

Let H be a [16, 7]-self-orthogonal code. As same way to obtain a Type II code containing H in the previous section, we obtain three Type I code containing H. The orbit of Aut(H) on the Type I codes shows us whether the three of them are equivalent or not. Therefore we obtain the classification of Type I codes of length 16. The mass formula [4] also guarantees the classification is complete.

Theorem 5.4 (c.f. [4]) *If* n *is a positive integer divisible by* 4*, then the number of the*

Type I codes of length n is equal to

$$\begin{aligned}\prod_{i=1}^{n/2-1}(4^i+1)-\prod_{i=0}^{n/2-2}(4^i+1) &= 97689675342016875\\ &= \sum_{C\in\mathcal{C}}\frac{n!\cdot 2}{|\operatorname{Aut}(C)|}\\ &= \sum_{C\in\mathcal{C}'}\frac{n!}{|\operatorname{PAut}(C)|},\end{aligned}$$

where $\mathcal{C}$ and $\mathcal{C}'$ are a complete sets of representatives of equivalence classes of Type I codes of length n and permutation-equivalence classes of Type I codes of length n respectively.

6 Enumeration of Special Self-Dual Codes

It is easy to distinguish special self-dual codes among Type I codes.

Theorem 6.1 *There precisely exist* 2948 *special self-dual codes up to permutation-equivalence. In particular there precisely exist* 1474 *special self-dual codes up to equivalence.*

Unfortunately we could not succeed to find some standard one among them like other generators.

References

[1] K. Betsumiya. On the classification of Type II codes over $\mathbb{F}_{2^r}$ with binary length 32. preprint, 2001.

[2] K. Betsumiya and Y. Choie. Codes over $\mathbb{F}_4$, Jacobi forms and Hilbert-Siegel modular forms over $\mathbb{Q}(\sqrt{5})$. *European J. Combin.*, 26:629–650, 2005.

[3] A. Munemasa. On the enumeration of self-dual codes. In *Proceedings of the Fourth Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography, University of Tokyo, 2000*, pages 69–77, 2000.

[4] G. Nebe, E. M. Rains, and N. J. A. Sloane. *Self-Dual Code and Invariant Theory.* 2005. working draft.