© DISCRETE MATHEMATICS 3 (1972) 153–162. North-Holland Publishing Company

GOOD SELF DUAL CODES EXIST

F.J. MacWILLIAMS and N.J.A. SLOANE
Bell Telephone Laboratories, Inc., Murray Hill, N.J. 07974, U.S.A.

and

J.G. THOMPSON
University of Cambridge, Cambridge, England

Received 6 November 1971

Abstract. It is shown that for any block length n which is a multiple of 8, there exists a binary self dual code in which all weights are divisible by 4, and the minimum weight is asymptotically the same as that given by the Varshamov–Gilbert bound.

§ 1. Preliminaries

Let F^n denote the vector space of all vectors of length n with components from GF(2). The *weight* of a vector $u = (u_1, u_2, ..., u_n)$ in F^n is the number of nonzero u_j, and is denoted by $w(u)$.

For vectors u, v in F^n we define

$$u * v = (u_1 v_1, u_2 v_2, ..., u_n v_n) .$$

Clearly $w(u * v)$ is the number of places in which both u_j and v_j are 1. We frequently use the obvious formula

$$w(u + v) = w(u) + w(v) - 2w(u * v) . \tag{1.1}$$

The scalar product in F^n is defined by

$$(u, v) = \sum_{j=1}^{n} u_j v_j ,$$

where the sum is evaluated in GF(2).

If $(u, v) = 0$ we say that u and v are *orthogonal*. A vector u is orthogonal to itself, or *self orthogonal*, if and only if $w(u) = 0 \pmod 2$; i.e., all even weight vectors are self orthogonal.

A *code* $\mathcal{C}$ is a subspace of F^n, and the vectors in $\mathcal{C}$ are called codewords. If the dimension of $\mathcal{C}$ is k, and the smallest nonzero weight of a vector in $\mathcal{C}$ is d, we write $\mathcal{C}[n, k, d]$ or simply $\mathcal{C}[n, k]$.

The *dual* code of $\mathcal{C}[n, k]$ is

$$\mathcal{C}^{\perp}[n, n-k] = \{v \in F^n : (v, c) = 0 \text{ for all } c \in \mathcal{C}\} ;$$

$\mathcal{C}^{\perp}$ obviously has dimension $n - k$.

If $\mathcal{C} = \mathcal{C}^{\perp}$ we say $\mathcal{C}$ is *strongly self dual*. The symbols $\mathcal{A}$, $\mathcal{B}$ will be reserved for strongly self dual codes. The dimension of a strongly self dual code is $\frac{1}{2}n$, and so n must be even, say $n = 2t$. We frequently write t instead of $\frac{1}{2}n$.

If $\mathcal{A} = \mathcal{A}^{\perp}$, every vector $A \in \mathcal{A}$ is self orthogonal; hence $w(A) \equiv 0 \pmod 2$. Therefore the vector $\mathbf{1}$ of weight n is orthogonal to every $A \in \mathcal{A}$, and $\mathbf{1} \in \mathcal{A}^{\perp} = \mathcal{A}$.

The set of strongly self dual codes will be denoted by α. Let β denote the (possibly empty) subset of α consisting of all self dual codes in which the weight of every codeword is divisible by 4. Let $\alpha - \beta$ be the set of codes which are in α but not in β.

Since $\mathbf{1} \in \mathcal{A}$ for every $\mathcal{A}$, the set β is empty unless n is divisible by 4. In fact we show in Corollary 4.7 that β is nonempty if and only if n is divisible by 8.

If $\mathcal{C}[n, k]$ is such that

$$\mathbf{1} \in \mathcal{C}[n, k] \subset \mathcal{C}^{\perp}[n, n-k] ,$$

we say that $\mathcal{C}$ is *weakly self dual*. Since $\mathbf{1} \in \mathcal{C}$, every vector in $\mathcal{C}^{\perp}$ has even weight.

§ 2. The theorems

We prove the following main theorems and corollaries.

Theorem 2.1. *Let $n = 2t$. Let $\mathcal{C}[n, s]$ be a weakly self dual code. The number of codes in α which contain $\mathcal{C}[n, s]$ is*

$$(2^{t-s} + 1)(2^{t-s-1} + 1) \ldots (2^2 + 1)(2 + 1) .$$

The case $s = 1$ of Theorem 2.1 was given by Pless [3, 4].

Theorem 2.2. *Let n be divisible by 8. Let $\mathcal{C}[n, s]$ be a weakly self dual code in which all codewords have weight divisible by 4. The number of codes in β which contain $\mathcal{C}[n, s]$ is*

$$(2^{t-s-1} + 1)(2^{t-s-2} + 1) \ldots (2 + 1)2 .$$

Corollary 2.3. *The number of codes in β is*

$$(2^{t-2} + 1)(2^{t-3} + 1) \ldots (2 + 1)2 .$$

Recall that they all contain the code $\mathcal{C}[n, 1]$ consisting of the vectors **0**, **1**.

Corollary 2.4. *Let v be a vector other than* **0**, **1** *with $w(v) \equiv 0 \pmod 4$. The number of codes in β which contain v is*

$$(2^{t-3} + 1)(2^{t-4} + 1) \ldots (2 + 1)2 .$$

Theorem 2.5. *Let r be the largest integer such that*

$$\binom{n}{4} + \binom{n}{8} + \binom{n}{12} + \ldots + \binom{n}{4(r-1)} < 2^{\frac{1}{2}n-2} + 1 .$$

Then there exists a self dual code in which all weights are divisible by 4 and with minimum weight at least $4r$.

Theorem 2.5 is an immediate consequence of Corollaries 2.3 and 2.4; the proof is left as an exercise.

§3. Comparison with the Varshamov–Gilbert bound

The Varshamov–Gilbert bound for self dual codes (Peterson [2, p.51]) states that if d is the largest integer such that

$$1 + \binom{n-1}{1} + \binom{n-1}{2} + \ldots + \binom{n-1}{d-2} < 2^{\frac{1}{2}n}, \tag{3.1}$$

then an $[n, \frac{1}{2}n, d]$ code exists.

Asymptotically, Theorem 2.5 and (3.1) are equivalent; they both imply that there exist codes with $\frac{k}{n} = \frac{1}{2}$ and $\frac{d}{n} = H^{-1}(\frac{1}{2}) \approx 0{\cdot}110$, where $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$, and H^{-1} denotes the inverse of H, not the reciprocal (see Peterson [2, p. 52, eq. (4.6)].)

For small values of n, Table 1 gives: d_1, the value of d guaranteed by the Varshamov–Gilbert bound (3.1); d_2, the value of d guaranteed by Theorem 2.5; and d_3, the largest minimum weight of any *known* self dual code in which all weights are divisible by 4. The values of d_3 are

Table 1
Minimum nonzero weights of self dual codes

Length n	Lower bounds d_1	Lower bounds d_2	Known d_3
8	3	4	4
16	4	4	4
24	5	4	8
32	6	4	8
40	7	8	8
48	8	8	12
56	9	8	12
64	9	8	12
72	10	12	12
80	11	12	16
88	12	12	16
96	13	12	12
104	14	12	20
112	15	16	16

either taken from Berlekamp [1, Fig. 15.02 (corrected) and Table 16.1], or are obtained using the $(x, x+y)$ construction given in [5], or were communicated by Maurice Karlin.

§4. The proofs

The rest of the paper is devoted to the proofs of Theorems 2.1 (easy) and 2.2 (hard).

Proof of Theorem 2.1. Let $\sigma_{n,k}$, $s \le k < t$, be the number of weakly self dual codes $\mathcal{C}[n, k]$ which contain the given code $\mathcal{C}[n, s]$. (Clearly $\sigma_{n,s} = 1$.) We establish a recursion formula for $\sigma_{n,k}$.

A particular $\mathcal{C}[n, k]$ can be extended to a suitable $\mathcal{C}[n, k+1]$ by adjoining any vector of $\mathcal{C}^{\perp}[n, n-k]$ which is not already there. Write $\mathcal{C}^{\perp}$ as the union of $2^{n-k}/2^k$ translates of $\mathcal{C}$,

$$\mathcal{C}^{\perp} = \mathcal{C} \cup (h_1 + \mathcal{C}) \cup \ldots \cup (h_l + \mathcal{C}),$$

where $l = 2^{n-2k} - 1$.

We have l different extensions of $\mathcal{C}[n, k]$, namely $\mathcal{C} \cup (h_j + \mathcal{C})$ for $j = 1, 2, \ldots, l$. In any one of these extensions there are $2^{k-s+1} - 1$ subspaces $\mathcal{C}'[n, k]$ which contain the given $\mathcal{C}[n, s]$, since that is the number of nonzero vectors in $\mathcal{C} \cup (h_j + \mathcal{C})$ which are orthogonal to $\mathcal{C}[n, s]$. Thus for $s \le k < t$,

$$\sigma_{n,k+1} = \sigma_{n,k} \cdot \frac{2^{n-2k} - 1}{2^{k-s+1} - 1}.$$

Starting from $\sigma_{n,s} = 1$ we obtain

$$\sigma_{n,t} = \frac{(2^{n-2s} - 1)(2^{n-2s-2} - 1) \ldots (2^2 - 1)}{(2 - 1)(2^2 - 1)(2^3 - 1) \ldots (2^{t-s} - 1)}$$

$$= (2^{t-s} + 1)(2^{t-s-1} + 1) \ldots (2 + 1).$$

For Theorem 2.2 we need several subsidiary lemmas. The first one is well known.

Let G be a commutative group, with group operation $+$. (In our applications G is always a code.) Let G^+ be a subgroup of G and write $G = G^+ \cup G^-$, where G^+ and G^- are disjoint. Suppose for all $b_1, b_2 \in G^-$, it follows that $b_1 + b_2 \in G^+$. Then:

Lemma 4.1. *If G^- is not empty, then $|G^+| = |G^-| = \frac{1}{2}|G|$ (where $|x|$ denotes the order of the set x).*

Proof. If $b \in G^-$ so is $-b$, since the zero of G is in G^+. Let b be a fixed element of G^-. For any other element b' of G^- we have

$$b' = b + (b' - b) = b + a', \quad a' \in G^+ .$$

Thus

$$G^- = b + G^+, \text{ and } |G^-| = |G^+| = \tfrac{1}{2}|G| .$$

We need the following applications of this basic lemma.

Corollary 4.2. *Let n be even, and let $\mathcal{A}[n, t]$ belong to $\alpha - \beta$. Then $\mathcal{A}$ contains 2^{t-1} codewords with weight divisible by 4.*

Proof. Set $\mathcal{A}[n, t] = G$, and $G^+ = \{A \in \mathcal{A}; w(A) \equiv 0 \pmod 4\}$. If A_1, $A_2 \in G^+$, so is $A_1 + A_2$ by (1.1). The other necessary properties are easily verified.

Corollary 4.3. *Let $\Lambda[n, k]$ be a code, and let u be a vector of F^n not in Λ^1. Then u is orthogonal to exactly 2^{k-1} codewords of Λ.*

Proof. Let $G = \Lambda[n, k]$ and $G^+ = \{v \in \Lambda; (u, v) = 0\}$.

Corollary 4.4. *Let n be even. Let $\mathcal{C}[n, k]$ be a weakly self dual code, such that $w(c) \equiv 0 \pmod 4$ for all codewords c. Let f be a vector of F^n such that $f \notin \mathcal{C}^1$, and $w(f) \equiv 0 \pmod 2$. Then $w(f + c) \equiv 0 \pmod 4$ for 2^{k-1} vectors $c \in \mathcal{C}$.*

Proof. The proof uses Lemma 4. . and the observations that

$$w(f+c) \equiv w(f) \pmod 4 \text{ if } (f,c) = 0\,,$$
$$w(f+c) \equiv w(f) + 2 \pmod 4 \text{ if } (f,c) = 1\,.$$

Let n be divisible by 4. Let K_4 be the number of vectors v in F^n such that $w(v) \equiv 0 \pmod 4$. Let K_2 be the number of vectors such that $w(v) \equiv 2 \pmod 4$. (Of course $K_2 + K_4 = 2^{n-1}$.)

Lemma 4.5. (i). *If $\frac{1}{4}n$ is odd,*

$$K_2 = 2^{2t-2} + 2^{t-1}\,,\quad K_4 = 2^{2t-2} - 2^{t-1}\,.$$

(ii). *If $\frac{1}{4}n$ is even,*

$$K_2 = 2^{2t-2} - 2^{t-1}\,,\quad K_4 = 2^{2t-2} + 2^{t-1}\,.$$

Proof. In the identity $(1+x)^n = \sum_{j=0}^{n} \binom{n}{j} x^j$ set $x = 1, -1, \mathrm{i}, -\mathrm{i}$. We readily obtain

$$4K_4 = 4 \sum_{j=0}^{n/4} \binom{n}{4j} = 2^n + (1+\mathrm{i})^n + (1-\mathrm{i})^n\,.$$

Since $1 \pm \mathrm{i} = \sqrt{2}\, e^{\pm \pi \mathrm{i}/4}$, the lemma follows immediately.

We now establish the important result that if n is divisible by 8, any weakly self dual code in which all weights are divisible by 4 can be extended to a strongly self dual code with the same property.

Lemma 4.6. *Let n be divisible by 4, and let $\mathcal{C}[n, k]$ be a weakly self dual code such that $w(c) \equiv 0 \pmod 4$ for $c \in \mathcal{C}$. If $\frac{1}{4}n$ is even, $\mathcal{C}$ is contained in a code of β. If $\frac{1}{4}n$ is odd, there is no code of β which contains $\mathcal{C}$.*

Corollary 4.7. *Strongly self dual codes $\mathcal{C}[n, \frac{1}{2}n]$ in which all weights are divisible by 4 exist if and only if n is divisible by 8.*

Take $\mathcal{C}[n, k] = \{0, 1\}$ in Lemma 4.6.

Proof of Lemma 4.6. By Theorem 2.1 there is a code of α such that $\mathcal{C} \subset \mathcal{A} \subset \mathcal{C}^{\perp}$. By Corollary 4.2, $\mathcal{A}$ contains at least 2^{t-1} vectors A with $w(A) \equiv 0 \pmod 4$. Hence we can augment $\mathcal{C}[n, k]$ to $\mathcal{C}[n, k+1]$ by adjoining a vector A with $w(A) \equiv 0 \pmod 4$ as long as $2^k < 2^{t-1}$. (It is readily checked by (1.1) that all codewords of the extended code have weights divisible by 4.)

It remains to consider the case $k = t - 1$. We have

$$\mathcal{C}[n, t-1] \subset \mathcal{C}^{\perp}[n, t+1] .$$

All codewords in $\mathcal{C}$ have weight divisible by 4; the question is whether there are any more such vectors in $\mathcal{C}^{\perp} - \mathcal{C}$.

Let $\hat{F}[n, n-1]$ be the code consisting of all even weight vectors of F^n, and write $\hat{F}$ as the union of $2^{n-1}/2^{t-1} = 2^t$ translates of $\mathcal{C}$,

$$\hat{F} = \mathcal{C} \cup (g_1 + \mathcal{C}) \cup (g_2 + \mathcal{C}) \cup (g_3 + \mathcal{C}) \cup (f + \mathcal{C}) \cup \ldots$$

$$\cup (f' + \mathcal{C}) ,$$

where the first four translates comprise $\mathcal{C}^{\perp}$, and the remaining $2^t - 4$ make up $\hat{F} - \mathcal{C}^{\perp}$. By Corollary 4.4, each translate $(f + \mathcal{C})$, $f \notin \mathcal{C}^{\perp}$ contains 2^{t-2} vectors v with $w(v) \equiv 0 \pmod 4$. This part of the decomposition of $\hat{F}$ contains $2^{t-2}(2^t - 4) = 2^{n-2} - 2^t$ such vectors.

Since $g_i \in \mathcal{C}^{\perp}$, $w(g_j + \mathcal{C}) \equiv w(g_j) \pmod 4$. Let ϵ $(= 0, 1, 2, 3)$ be the number of g_j with $w(g_j) \equiv 0 \pmod 4$. In the three translates $(g_j + \mathcal{C})$ there are $2^{t-1} \cdot \epsilon$ vectors with weights divisible by 4. In $\mathcal{C}$ itself there are 2^{t-1} such vectors. Hence

$$K_4 = 2^{t-1} + \epsilon \cdot 2^{t-1} + 2^{n-2} - 2^t$$

$$= 2^{n-2} + 2^{t-1} + \epsilon \cdot 2^{t-1} .$$

Consulting Lemma 4.5 we see that $\epsilon = 0$ if $\frac{1}{4}n$ is odd, in which case $\mathcal{C}^{\perp}[n, t+1] - \mathcal{C}[n, t-1]$ contains no vectors with weight divisible by 4, and $\mathcal{C}$ cannot be extended to a code of β.

If $\frac{1}{4}n$ is even, $\epsilon = 2$ and $\mathcal{C}[n, t-1]$ has two extensions in β and one in $\alpha - \beta$. This completes the proof.

Now assume that n is divisible by 8. Let $\mathcal{C}[n, s]$ be a weakly self dual code such that $w(c) \equiv 0 \pmod 4$ for $c \in \mathcal{C}$. We will find the number of codes in $\alpha - \beta$ which contain $\mathcal{C}[n, s]$. For this we need another lemma.

Lemma 4.8. *The number of vectors H in $\mathcal{C}^{\perp}[n, n-s]$ such that $w(H) \equiv 2 \pmod 4$ is $2^{n-s-1} - 2^{t-1}$.*

Proof. By Lemma 4.6 there is a code $\mathcal{B}$ such that

$$\mathcal{C}[n, s] \subset \mathcal{B} \subset \mathcal{C}^{\perp}[n, n-s] .$$

Write $\mathcal{C}^{\perp}$ as the union of $2^{n-s}/2^t$ translates of $\mathcal{B}$,

$$\mathcal{C}^{\perp} = \mathcal{B} \cup (f_1 + \mathcal{B}) \cup \ldots \cup (f_l + \mathcal{B}) ,$$

where $l = 2^{t-s} - 1$. Since $f_j \notin \mathcal{B}^{\perp}$, each translate $(f_j + \mathcal{B})$ contains 2^{t-1} vectors H with $w(H) \equiv 2 \pmod 4$. Hence the total number of such H is $2^{t-1}(2^{t-s} - 1) = 2^{n-s-1} - 2^{t-1}$.

Lemma 4.9. *The number of codes in $\alpha - \beta$ which contain $\mathcal{C}[n, s]$ is*

$$(2^{t-s-1} + 1)(2^{t-s-2} + 1) \ldots (2 + 1)(2^{t-s} - 1) .$$

Proof. To make sure that the code is in $\alpha - \beta$ we immediately adjoin to $\mathcal{C}[n, s]$ one of the vectors H of the preceding lemma; say

$$\mathcal{C}_H[n, s+1] = \mathcal{C} \cup (H + \mathcal{C}) .$$

The number of strongly self dual codes which contain $\mathcal{C}_H[n, s+1]$ for a particular H is given by Theorem 2.1, starting with $\sigma_{n,s+1} = 1$, and is $(2^{t-s-1} + 1) \ldots (2 + 1)$. Each such code contains 2^{t-1} vectors H with $w(H) \equiv 2 \pmod 4$. Hence the number of distinct codes for all suitable H is

$$(2^{t-s-1}+1)\ldots(2+1)(2^{n-s-1}-2^{t-1})/2^{t-1}\,.$$

Proof of Theorem 2.2. We subtract from the total number of strongly self dual codes which contain $\mathcal{C}[n, s]$ (Theorem 2.1) the number which lie in $\alpha - \beta$ (Lemma 4.9), viz.

$$(2^{t-s}+1)(2^{t-s-1}+1)\ldots(2+1)-(2^{t-s-1}+1)\ldots(2+1)(2^{t-s}-1)$$

$$=(2^{t-s-1}+1)(2^{t-s-2}+1)\ldots(2+1)2\,.$$

References

[1] E.R. Berlekamp, Algebraic coding theory (McGraw-Hill, New York, 1968).
[2] W.W. Peterson, Error-correcting codes (MIT Press, Cambridge, Mass., 1961).
[3] V.S. Pless, The number of isotropic subspaces in a finite geometry, Accad. Nazl. Lincei, Rend. Cl. Sci. Fis. Mat. e Natur. VIII, 39 (1965).
[4] V.S. Pless, On the uniqueness of the Golay code, J. Combinatorial Theory 5 (3) (1968) 215–228.
[5] N.J.A. Sloane and D.S. Whitehead, A new family of single-error correcting codes, IEEE Trans. Information Theory IT-16 (6) (1970) 717–719.