

A New Upper Bound on the Minimal Distance of Self-Dual Codes*

J. H. Conway

Mathematics Department
Princeton University
Princeton, New Jersey 08540

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

1. Introduction

The problem of classifying binary self-dual codes has been studied by a number of authors [1]-[5], [9]-[11], [13], [18], [20], [21], [24]-[27], [30], [32]-[34], [38]-[54], [57]-[64], [66]-[73], [14, Chap. 7], [31, Chap. 19]. The main results of the present paper are contained in the following theorems.

Theorem 1. *The minimal distance d of a binary self-dual code \mathbf{C} of length n ($n \neq 2, 8, 12, 22, 24, 32, 48, 72$) satisfies*

$$d \leq 2 \left\lceil \frac{n+6}{10} \right\rceil. \quad (1)$$

If \mathbf{C} is of Type I (i.e. the weights are not all multiples of 4) then the bound fails just when n (necessarily even) is 2, 12, 22 and 32, and if \mathbf{C} is of Type II (i.e. the weights are multiples of 4) the bound fails just when n (necessarily a multiple of 8) is 8, 24, 32, 48 and possibly 72. The greatest minimal distance for these exceptional lengths is $2[(n+6)/10] + 2$.

In [34] it was shown that $d \leq 2\lceil n/8 \rceil + 2$ for all n , and in [33] that $d \leq n/4 - c$, for any constant c , provided n is sufficiently large. The bound (1) is stronger than these, although asymptotically weaker than the McEliece-Rodemich-Rumsey-Welch bound, which for rate one-

* This paper appeared in *IEEE Trans. Inform. Theory*, vol. 36 (Nov. 1990), pp. 1319-1333.

half code implies $d \leq 0.182490n + o(n)$ ([37], [36], [31, Chap. 17]).⁽¹⁾ For Type II codes it is known that

$$d \leq 4 \left\lceil \frac{n}{24} \right\rceil + 4, \quad \text{for all } n, \quad (2)$$

and $d \leq n/6 - c$ for any constant c provided n is sufficiently large ([34], [33], [31, Chap. 19]).

Theorem 1 is a consequence of some new restrictions on the weight enumerator of a Type I self-dual code, obtained by studying a particular translate of the code called its “shadow” (see Theorem 5 and Section 2). For small values of n we can often obtain additional information about the weight enumerator from its shadow, leading to the following result.

Theorem 2. *The highest minimal distance of any self-dual code of length $n \leq 60$ is known. The actual values are as given in Table I.*

Before this, the highest minimal distance was known only for $n \leq 32$ ([11], [45]). Table I also shows our present state of knowledge about codes of lengths 62 to 72. In the table d_I (resp. d_{II}) denotes the highest minimal distance of any Type I (resp. Type II) self-dual code.

(1) On p. 629 of [31] this is incorrectly stated as $d \leq 0.178n + o(n)$.

Table I

The highest minimal distance of a self-dual code

n	d_I	d_{II}	Codes	n	d_I	d_{II}	Codes
2	2		i_2 .	38	8		≥ 2
4	2		i_4 .	40	8	8	≥ 2 ; ≥ 100 [60], [73]
6	2		i_6 .	42	8		≥ 9
8	2	4	$i_8; e_8$.	44	8		≥ 14
10	2		$i_{10}; e_8 i_2$.	46	10		≥ 1
12	4		d_{12}^+ .	48	10	12	≥ 1 ; ≥ 1
14	4		e_7^{2+} .	50	10		≥ 1
16	4	4	$d_8^{2+}; d_{16}^+, e_8^2$.	52	10		≥ 1
18	4		$d_6^{3+}, (d_{10} e_7 f_1)^+$.	54	10		≥ 1
20	4		7 codes [44].	56	10 or 12	12	?; ≥ 20 [9], [70]
22	6		g_{22} [48].	58	10		≥ 2
24	6	8	$f_{24}; g_{24}$ [48].	60	12		≥ 1
26	6		f_{13}^2 [45].	62	10 or 12		
28	6		$f_7^4(a), f_7^4(b), D1$.	64	12	12	≥ 1 ; ≥ 38 [71]
30	6		13 codes.	66	12		≥ 1
32	8	8	3 codes; 5 codes.	68	12		≥ 1
34	6		≥ 200	70	10 or 12		
36	8		≥ 2	72	12 or 14	12 or 16	

The fourth column of the table gives the known codes having the indicated minimal distance. A period indicates that the lists of codes is complete. These enumerations (for $n \leq 30$ and for Type II codes of length 32) are due to Pless [43]-[45], Pless and Sloane [48], and Conway and Pless [11] (but see however [13]). When n is a multiple of 8 a semicolon separates the Type I and Type II codes. The codes in the fourth column are described in greater detail in Sect. 3; several of them are new. In the past, codes of length 32 have received a great deal of attention [11], [24], [25], [45], [72]. In particular, it is known that there are precisely five [32,16,8] Type II self-dual codes [11] (see Section 4 below).

Theorem 3. *There are precisely three $[32, 16, 8]$ Type I self-dual codes.*

We also determine all lengths for which there exist 2-, 3- and 4-error-correcting self-dual codes.

Theorem 4. *Self-dual codes with minimal distance*

$$\begin{aligned} d \geq 6 & \quad \text{exist precisely for } n \geq 22, \\ d \geq 8 & \quad \text{exist precisely for } n = 24, 32 \text{ and } n \geq 36, \\ d \geq 10 & \quad \text{exist precisely for } n \geq 46. \end{aligned}$$

For larger values of d we have less complete information. For example, self-dual codes with:

- (a) $d = 12$ exist for $n = 48, 56, 60, 64-68, n \geq 72$, perhaps $n = 62, 70$, and no other values of n ;
- (b) $d = 14$ exist for $n = 78, 80, 86, 88, n \geq 98$ (and possibly other values);
- (c) $d = 16$ exist for $n = 80, 88, 100-104, n \geq 122$ (and possible other values).

The key idea in proving these results is to study the ‘‘shadow’’ of a code. The shadow of a self-dual code \mathbf{C} is defined as follows. (A more general definition is given in Sect. 2.) Let $\mathbf{C}^{(0)}$ be the subcode of \mathbf{C} consisting of all words whose weights are multiples of 4, and let $\mathbf{C}^{(2)} = \mathbf{C} \setminus \mathbf{C}^{(0)}$. The *shadow code* $\mathbf{S} = \mathbf{S}(\mathbf{C})$ consists of all ‘‘parity vectors’’ for \mathbf{C} : those vectors u with the property that

$$\begin{aligned} u \cdot v &= 0 & \text{for all } v \in \mathbf{C}^{(0)}, \\ u \cdot v &= 1 & \text{for all } v \in \mathbf{C}^{(2)}. \end{aligned}$$

If \mathbf{C} is a Type II code then $\mathbf{C}^{(2)} = \emptyset$ and $\mathbf{S}(\mathbf{C}) = \mathbf{C}$.

The next theorem summarizes a number of properties of the shadow of a Type I code.

Theorem 5. *Let $\mathbf{S} = \mathbf{S}(\mathbf{C})$ be the shadow code corresponding to an $[n, n/2, d]$ Type I self-dual code \mathbf{C} . The dual $\mathbf{C}^{(0)*}$ consists of the union of four cosets of $\mathbf{C}^{(0)}$, say*

$\mathbf{C}^{(0)} \cup \mathbf{C}^{(1)} \cup \mathbf{C}^{(2)} \cup \mathbf{C}^{(3)}$, with $\mathbf{C} = \mathbf{C}^{(0)} \cup \mathbf{C}^{(2)}$.

- (i) $\mathbf{S} = \mathbf{C}^{(0)*} \setminus \mathbf{C} = \mathbf{C}^{(1)} \cup \mathbf{C}^{(3)}$.
- (ii) *The sum of any two vectors in \mathbf{S} is in \mathbf{C} . More precisely, if $u, v \in \mathbf{C}^{(1)}$ then $u+v \in \mathbf{C}^{(0)}$; if $u \in \mathbf{C}^{(1)}, v \in \mathbf{C}^{(3)}$ then $u+v \in \mathbf{C}^{(2)}$; and if $u, v \in \mathbf{C}^{(3)}$ then $u+v \in \mathbf{C}^{(0)}$.*
- (iii) *Let $S(x, y) = \sum B_r x^{n-r} y^r$ be the weight enumerator of \mathbf{S} . Then*

$$S(x, y) = W \left[\frac{x+y}{\sqrt{2}}, i \frac{x-y}{\sqrt{2}} \right], \quad (3)$$

where $W(x, y)$ is the weight enumerator of \mathbf{C} . Also $B_r = B_{n-r}$ for all r ,

$$B_r = 0 \text{ unless } r \equiv n/2 \pmod{4}, \quad (4)$$

$$B_0 = 0, \quad (5)$$

$$B_r \leq 1 \text{ for } r < d/2, \quad (6)$$

$$B_{d/2} \leq 2n/d, \quad (7)$$

$$B_r \leq A(n, d, r)^{(2)}, \text{ for all } r, \text{ and} \quad (8)$$

$$\text{at most one } B_r \text{ is nonzero for } r < (d+4)/2. \quad (9)$$

- (iv) *If we write*

$$W(x, y) = \sum_{j=0}^{\lfloor n/8 \rfloor} a_j (x^2 + y^2)^{n/2-4j} \{x^2 y^2 (x^2 - y^2)^2\}^j \quad (10)$$

using Gleason's theorem ([2], [14, p. 186], [18], [30], [31, p. 602], [51]-[54]), for suitable integers a_j , then

$$S(x, y) = \sum_{j=0}^{\lfloor n/8 \rfloor} (-1)^j a_j 2^{n/2-6j} (xy)^{n/2-4j} (x^4 - y^4)^{2j}. \quad (11)$$

(2) $A(n, d, w)$ denotes the maximal possible number of binary vectors of length n , weight w and Hamming distance at least d apart [7], [31].

In particular, a_j is divisible by $2^{n/2-6j}$ for all j .

(v) Let $W^{(j)}(x, y)$ be the weight enumerator of $\mathbf{C}^{(j)}$ ($0 \leq j \leq 3$), so that $W = W^{(0)} + W^{(2)}$, $S = W^{(1)} + W^{(3)}$. Then $W^{(1)} - W^{(3)}$ is:

(a) a polynomial in $f_8 = x^8 + 14x^4y^4 + y^8$ and $f_{24} = x^4y^4(x^4 - y^4)^4$, if $n \equiv 0 \pmod{8}$,

(b) f_{18} times a polynomial in f_8 and f_{24} , if $n \equiv 2 \pmod{8}$, where

$$\begin{aligned} f_{18} &= x^{17}y - 34x^{13}y^5 + 34x^5y^{13} - xy^{17} \\ &= xy(x^8 - y^8)(x^8 - 34x^4y^4 + y^8) \\ &= xy(x^8 - y^8)(x^2 - 2xy - y^2)(x^2 + 2xy - y^2)(x^4 + 6x^2y^2 + y^4), \end{aligned} \quad (12)$$

(c) f_{12} times a polynomial in f_8 and f_{24} , if $n \equiv 4 \pmod{8}$, where

$$\begin{aligned} f_{12} &= x^{10}y^2 - 2x^6y^6 + x^2y^{10} \\ &= x^2y^2(x^4 - y^4)^2 = f_{24}^{1/2}, \end{aligned} \quad (13)$$

(d) $f_{30} = f_{12} f_{18}$ times a polynomial in f_8 and f_{24} , if $n \equiv 6 \pmod{8}$.

Remarks. (a) Part (iv) is due to Ward [64], who investigated the weight enumerator of \mathbf{S} (without however considering \mathbf{S} as a code in its own right).

(b) One of the differences between Type I and Type II codes is that the weight enumerator $W(x, y)$ of a Type I code is invariant under a group of order 16, whereas for a Type II code $W(x, y)$ is invariant under a group of order 192 ([31, Chap. 19], [51]-[54]). Thus $W(x, y)$ is more strongly constrained for Type II codes. As we shall see in Sect. 2, part (v) of the theorem restores the balance to a certain extent by requiring $W^{(1)} - W^{(3)}$ to be a relative invariant (with respect to a certain character) for the group of order 192.

In Sect. 2 we give a more general definition of the shadow code and establish some of its properties, including those stated in Theorem 5.

In Section 3 we study self-dual codes of length $n \leq 72$, where considerable information about the best codes can be obtained by considering their shadows, and in particular establish Theorem 2. Often we can restrict the weight enumerator of the code and its shadow to one of small number of possibilities.

This approach enables us to give analytical proofs of various results that were previously known only from the complete enumerations mentioned above. Typical results are that there are only two possible weight enumerators for a $[18,9,4]$ Type I code and only one for a $[24,12,6]$ Type I code. (Gleason's theorem alone does not imply these results.) It also follows immediately that there do not exist linear codes with the same weight enumerators as the "formally self-dual" nonlinear codes of lengths 8 ([31, p. 140, Fig. 5.1), and 16 (the Nordstrom-Robinson code), etc.

Consideration of the shadow code has also revealed some errors in the literature. At length 28, minimal distance 6, there are two possible weight enumerators (see Sect. 3). Reference [45] does give two codes, but only one of them ($2f_{14}(\text{I})$) corresponds to one of our weight enumerators. The other code ($2f_{14}(\text{II})$) in [45] has nonintegral coefficients in the weight enumerator of its shadow, and in fact is not a self-dual code. The coefficients in the second of our weight enumerators suggest that a code might exist which it is invariant under a permutation of order 13, and indeed such a code exists. It is a child (omitted from [45]) of the length 32 code $d_6 f_{13}^2$. There are in fact three $[28,15,6]$ Type I codes – see Sect. 3. Reference [13] contains the corrections to [45].

At length 58 our results show that the highest possible minimal distance is 10. On the other hand, [3] claims to present a $[58,29,12]$ self-dual code. However, the weight enumerator of the shadow of that code (found for example from Eq. (3)) begins

$$\frac{29}{8192} y + \frac{19285}{4096} y^5 + \dots,$$

which is impossible.⁽³⁾ A code (D12) with $d = 10$ does exist – see Table II below.

Theorems 3 and 4 are proved (using the results of Sect. 3) in Sect. 4. The final section contains the proof of Theorem 1.

Codes with trivial group. There has been interest recently in self-dual codes with trivial automorphism group [37b], [60]. We have found numerous [34,17,6] self-dual codes with trivial group, for example the code R0 in Table III. (The 22 words of weight 6 generate R0, and the program Nauty [37a] was used to show that this 22-word constant weight code has trivial group.) All the [34,17,6] codes with trivial group that we found have weight enumerators of the form $W = 1 + (34 - \beta)y^6 + (255 + 4\beta)y^8 + \dots$ (see Sect. 3) with $\beta=2$ (at least three distinct codes), $\beta=3$ (at least six distinct codes) or $\beta=4$ (at least six distinct codes).

It is very likely that these length 34 Type I codes are the shortest possible self-dual codes with trivial group. For we know ([11],[13]) that the trivial group does not occur for a Type I code with $n \leq 30$, nor for a Type II code with $n \leq 32$, and an extensive computer search has failed to produce a Type I example of length 32.

Length 40 is the smallest possible length where a Type II code with no group can exist, and Tonchev [60] gives an example of such a code. Our computer search suggests that in fact [40,20,8] Type II codes with no group are very common (out of 50 codes chosen at random, 44 had trivial group and were all distinct). This is not surprising, since the total mass $\sum |\text{Aut}(C)|^{-1}$ for all Type II codes of length 40 is 17492.86...

The results of this paper were announced in [15]. Similar theorems can be proved for unimodular lattices [16], [17].

(3) Indeed, the code described in [3] has generator matrix of the form given in Eq. (41) below, where the first row of R is 19E89179 in hexadecimal, and is not self-dual.

Open questions. (1) Since there are many more Type I than Type II codes ([48], [31, Chap. 19]), and the best bound known for Type I codes (Eq. (1)) is larger than that for Type II codes (Eq. (2)), it is natural to ask for the smallest length at which a Type I code has a higher minimal distance than any Type II code. Table I suggests this could be $n=72$ – see the weight enumerators in Sect. 3.

(2) The bound of Theorem 1 can be tightened slightly (at the cost of allowing more exceptions) by using (8) to bound B_r for $r > d/2$. This suggests that by following the methods of [33] it may be possible to prove that $d \leq n/5 - c$ holds for any constant c , provided n is sufficiently large.

(3) Determine precisely when self-dual codes with $d = 12, 14$ and 16 exist (see the remarks following Theorem 4).

(4) Remove some gaps in Table I and Section 3 by constructing or proving nonexistence of the following codes (see Sect. 3, where the corresponding weight enumerators are indicated by the symbol \mathbb{C}): $[42,21,8]$, second case; $[48,24,10]$, Type I, first case; $[50,25,10]$, first case; $[52,26,10]$, second case; $[54,26,10]$, second case; $[56,28,12]$, Type I, two cases; $[60,30,12]$, two of the three cases; $[64,32,12]$, Type I, first case; $[72,36,14]$, Type I, three cases; etc.

Notation. An $[n, k, d]$ code \mathbf{C} is a binary linear code of length n , dimension k and minimal distance d . $W(x, y) = \sum A_r x^{n-r} y^r$ is its weight enumerator, where A_r is the number of words of weight r . $S(x, y) = \sum B_r x^{n-r} y^r$ is the weight enumerator of the shadow code $\mathbf{S}(\mathbf{C})$. The dual to \mathbf{C} is denoted by \mathbf{C}^* . A self-dual code (with $\mathbf{C} = \mathbf{C}^*$) is of Type II (or doubly even) if the weight of every word is a multiple of 4; otherwise is of Type I (or singly even). If \mathbf{C} is of Type I, $\mathbf{C}^{(0)}$ denotes the doubly even subcode, $\mathbf{C}^{(0)*} = \mathbf{C}^{(0)} \cup \mathbf{C}^{(1)} \cup \mathbf{C}^{(2)} \cup \mathbf{C}^{(3)}$, $\mathbf{C} = \mathbf{C}^{(0)} \cup \mathbf{C}^{(2)}$, $\mathbf{S}(\mathbf{C}) = \mathbf{C}^{(1)} \cup \mathbf{C}^{(3)}$, and $W^{(j)}(x, y)$ denotes the weight enumerator of $\mathbf{C}^{(j)}$. We often set $x = 1$ in weight enumerators and write $W(y)$ for $W(1, y)$, etc. $\overset{\leftarrow}{f}(y) = y^n f(1/y)$ denotes a reciprocal

polynomial.

For codes of length up to 32 we sometimes use the d_n, e_n, f_n, g_n notation of [11], [45], [48].

To save space some vectors have been written in *hexadecimal*, using $0 = 0000, \dots, 9 = 1001, A = 1010, \dots, F = 1111$, usually omitting leading zeros (so the vectors are right-justified).

2. Shadow codes

We give a general definition of the shadow of a code, which reduces to that of Sect. 1 when the code is self-dual. Let \mathbf{C} be a binary linear $[n, k, d]$ code which contains its dual $\mathbf{C}^* = \mathbf{B}$ (say). Let $\mathbf{B}^{(0)}$ be the subcode of \mathbf{B} consisting of all words with weights divisible by 4 (the weights in \mathbf{B} are necessarily even). The shadow code $\mathbf{S} = \mathbf{S}(\mathbf{C})$ consists of all ‘parity vectors’ for \mathbf{C}^* : all vectors u such that $u \cdot v = 0$ for all $v \in \mathbf{B}^{(0)}$, $u \cdot v = 1$ for all $v \in \mathbf{B} \setminus \mathbf{B}^{(0)}$.

We give four examples; others will be found in Sect. 3. (i) If \mathbf{C} consists of all even weight vectors of even length n , then $\mathbf{S} = \mathbf{C}$ if n is a multiple of 4, and otherwise \mathbf{S} consists of all odd weight vectors. (ii) If \mathbf{C} is the self-dual code

$$i_{2m} = i_2 \text{ 6 } i_2 \text{ 6 } \cdots \text{ 6 } i_2, \quad i_2 = \{00, 11\}, \quad (14)$$

consisting of all vectors $u = u_1 u_2 \cdots u_{2m}$ with $u_1 = u_2, u_3 = u_4, \dots$, then \mathbf{S} is the translate of \mathbf{C} by the vector 101010..., and consists of all vectors u with $u_1 \neq u_2, u_3 \neq u_4, \dots$. (iii) If \mathbf{C} is the self-dual code $(d_{10} e_7 f_1)^+$ of [44], [48], with generator matrix

$ \begin{array}{cccc} 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ & & 1 & 1 \\ & & & 1 \end{array} $		
	$ \begin{array}{cccc} 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ 1 & & 1 & 1 \end{array} $	(15)
$1 \quad 1 \quad 1 \quad 1 \quad 1$		1
$1 \quad 1$	$1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1$	1

then \mathbf{S} is the translate of \mathbf{C} by the vector $0^{17}1$. (iv) Let $\mathbf{C} = g_{22}$, the $[22,11,6]$ ‘‘shorter Golay code’’ [4], formed by subtracting (see [12]) i_2 from the $[24,12,8]$ Golay code g_{24} . Thus g_{22} consists of all words of g_{24} that begin 00 or 11, with these two coordinates deleted. Then \mathbf{S} consists of the remaining words of g_{24} with the same two coordinates deleted.

Theorem 6. *Let \mathbf{C} be an $[n, k, d]$ code such that $\mathbf{C} \supseteq \mathbf{C}^*$, and let $\mathbf{S} = \mathbf{S}(\mathbf{C})$ be its shadow. If all weights in \mathbf{C}^* are multiples of 4 then $\mathbf{S} = \mathbf{C}$. If not then:*

(a) \mathbf{S} is a nonlinear code, a translate of \mathbf{C} , given by

$$\mathbf{S} = \mathbf{B}^{(0)*} \setminus \mathbf{C} . \tag{16}$$

(b) If $u, v \in \mathbf{S}$ then $u + v \in \mathbf{C}$.

(c) Let $S(x, y) = \sum B_r x^{n-r} y^r$ be the weight enumerator of \mathbf{S} . Then the B_r are nonnegative integers satisfying $B_r = B_{n-r}$ for all r ,

$$B_0 = 0 , \tag{17}$$

$$B_r \leq 1 \quad \text{for } r < d/2 , \tag{18}$$

$$B_{d/2} \leq 2n/d , \tag{19}$$

$$B_r \leq A(n, d, r), \quad \text{for all } r , \quad \text{and} \tag{20}$$

$$\text{at most one } B_r \text{ is nonzero for } r < (d+1)/2 . \tag{21}$$

(d) If $W(x, y)$ and $W^*(x, y)$ are the weight enumerators of \mathbf{C} and \mathbf{C}^* respectively then

$$S(x, y) = W \left[\frac{(1+i)x + (1-i)y}{2}, \frac{(1-i)x + (1+i)y}{2} \right] \quad (22)$$

and

$$S(x, y) = \frac{1}{2^{n-k}} W^*(x+y, i(x-y)). \quad (23)$$

Remark. For comparison, note that the MacWilliams identity [31, Chap. 5] states that

$$W(x, y) = \frac{1}{2^{n-k}} W^*(x+y, x-y). \quad (24)$$

Proof. If all weights in \mathbf{C}^* are multiples of 4 then $\mathbf{B}^{(0)} = \mathbf{B}$ and $\mathbf{S} = \mathbf{C}$. Otherwise $\mathbf{B}^{(0)}$ is a subcode of \mathbf{B} of index 2, and $\mathbf{B}^{(0)*} = \mathbf{C} \cup (a + \mathbf{C})$ for some $a \notin \mathbf{C}$. We will show that $\mathbf{S} = a + \mathbf{C}$. It follows immediately from the definition that $\mathbf{S} \subseteq \mathbf{B}^{(0)*} \setminus \mathbf{C}$. On the other hand if $u \in \mathbf{B}^{(0)*} \setminus \mathbf{C}$ then for some $v \in \mathbf{B} \setminus \mathbf{B}^{(0)}$ we have $u \cdot v = 1$. Any $v' \in \mathbf{B} \setminus \mathbf{B}^{(0)}$ can be written as $v' = v + w$, $w \in \mathbf{B}^{(0)}$, and $u \cdot v' = u \cdot v + u \cdot w = 1$. Thus $\mathbf{S} = \mathbf{B}^{(0)*} \setminus \mathbf{C}$, which proves (a). Part (b) follows immediately from (a). (c) \mathbf{C} must contain the all-ones vector, so $W(y, x) = W(x, y)$. This implies $S(y, x) = S(x, y)$ from (22) (proved below), hence $B_r = B_{n-r}$ for all r . Equation (17) holds because 0 is not a parity vector, and (18), (20), (21) all follow from (b). Equation (19) is a special case of (20). To prove (d) we compute the following weight enumerators, using the MacWilliams identity [31, Chap. 5].

$$\mathbf{B} = \mathbf{C}^* : \frac{1}{2^k} W(x+y, x-y),$$

$$\mathbf{B}^{(0)} : \frac{1}{2^{k+1}} \{ W(x+y, x-y) + W(x+iy, x-iy) \},$$

$$\mathbf{B}^{(0)*} : \frac{1}{2^n} \{ W(2x, 2y) + W((1+i)x + (1-i)y, (1-i)x + (1-i)y) \},$$

$$\mathbf{S} = \mathbf{B}^{(0)*} \setminus \mathbf{C} : W \left[\frac{(1+i)x + (1-i)y}{2}, \frac{(1-i)x + (1+i)y}{2} \right].$$

(To obtain the final expression we use the fact that $W(x, y)$ is homogeneous of degree n .)

Equation (23) follows similarly.

Proof of Theorem 5. Suppose \mathbf{C} is an $[n, n/2, d]$ Type I code. (i) Then $\mathbf{B} = \mathbf{C}$, $\mathbf{B}^{(0)} = \mathbf{C}^{(0)}$, $\mathbf{B}^{(0)*} = \mathbf{C}^{(0)} \cup \mathbf{C}^{(1)} \cup \mathbf{C}^{(2)} \cup \mathbf{C}^{(3)}$ where $\mathbf{C} = \mathbf{C}^{(0)} \cup \mathbf{C}^{(2)}$. Then $\mathbf{S} = \mathbf{C}^{(1)} \cup \mathbf{C}^{(3)}$ from (16). (ii) follows because $\mathbf{C}^{(0)*}/\mathbf{C}^{(0)}$ is a 4-group. (It is a group of order 4 and is not cyclic since it is the quotient of a vector space over $GF(2)$.)

(iii), (iv) Equation (3) follows from (23) (since now $W^* = W$), and (5)-(9) from (17)-(21). Equation (11) follows from (3) and (10), and (4) from (11).

(v) We begin by showing that $\mathbf{C}^{(0)} \cup \mathbf{C}^{(1)}$ and $\mathbf{C}^{(0)} \cup \mathbf{C}^{(3)}$ are both self-dual if $n \equiv 0 \pmod{4}$, while $\mathbf{C}^{(0)} \cup \mathbf{C}^{(1)}$ and $\mathbf{C}^{(0)} \cup \mathbf{C}^{(3)}$ are dual to each other if $n \equiv 2 \pmod{4}$. Proof. The dual of $\mathbf{C}^{(0)} \cup \mathbf{C}^{(1)}$ contains $\mathbf{C}^{(0)}$ and is contained in $\mathbf{C}^{(0)} \cup \mathbf{C}^{(1)} \cup \mathbf{C}^{(2)} \cup \mathbf{C}^{(3)}$. If $n \equiv 0 \pmod{4}$ and $u, v \in \mathbf{C}^{(1)}$ we read $wt(u+v) = wt(u) + wt(v) - 2wt(u \cap v)$ modulo 4 and (using Eq. (4)) deduce that $wt(u \cap v)$ is even. Hence $\mathbf{C}^{(0)} \cup \mathbf{C}^{(1)}$ is self-dual. A similar argument applies if $n \equiv 2 \pmod{4}$.

For a matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ we write $A \circ f(x, y) = f(ax+b, cx+d)$. From the previous paragraph (and the MacWilliams identity), if $n \equiv 0 \pmod{4}$ we have

$$\begin{aligned} M \circ (W^{(0)} + W^{(1)}) &= W^{(0)} + W^{(1)}, \\ M \circ (W^{(0)} + W^{(3)}) &= W^{(0)} + W^{(3)}, \\ M \circ (W^{(1)} - W^{(3)}) &= W^{(1)} - W^{(3)}, \end{aligned}$$

where

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Therefore $W^{(1)} - W^{(3)}$ satisfies

$$\begin{aligned} M \circ (W^{(1)} - W^{(3)}) &= (-1)^{n/2} (W^{(1)} - W^{(3)}) , \\ J \circ (W^{(1)} - W^{(3)}) &= i^{n/2} (W^{(1)} - W^{(3)}) , \end{aligned} \quad (25)$$

where $J = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$, using (4).

The matrices M, J generate a unitary reflection group \mathbf{G} of order 192 [31, Chap. 19], [51]-[54], and (25) implies that $W^{(1)} - W^{(3)}$ is a relative invariant for \mathbf{G} with respect to the character defined by $\chi(M) = (-1)^{n/2}$, $\chi(J) = i^{n/2}$. If $n \equiv 0 \pmod{8}$ then χ is identically 1 and $W^{(1)} - W^{(3)}$ is an absolute invariant for \mathbf{G} , hence a polynomial in f_8 and f_{24} [31, p. 602].

If $n \not\equiv 0 \pmod{8}$ then $W^{(1)} - W^{(3)}$ is a relative but not absolute invariant for \mathbf{G} . In this situation there is a particular polynomial f (depending on χ) such that $W^{(1)} - W^{(3)}$ can be written uniquely as f times an absolute invariant for \mathbf{G} (see for example [55], [56]). To find the degree of f we compute the Molien series

$$\Phi_{\chi}(\lambda) = \frac{1}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \frac{\overline{\chi(A)}}{\det(I - \lambda A)} \quad (26)$$

where the bar denotes complex conjugation. This is easily computed if we observe that \mathbf{G} has a subgroup \mathbf{H} of order 24 generated by

$$U = RMJMJ^2M = \frac{1}{\sqrt{2}} \begin{bmatrix} -i & 1 \\ i & 1 \end{bmatrix} ,$$

where

$$R = MJ^2M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} .$$

Then

$$\mathbf{G} = \bigcup_{j=0}^7 C_j \mathbf{H} ,$$

where $C_j = T^j$, $C_{j+4} = RT^4$ ($0 \leq j \leq 3$), and $T = MR$. Using this in (26) we find that $\Phi_\chi(\lambda)$ is

$$\begin{aligned} & \frac{\lambda^{18}}{(1-\lambda^8)(1-\lambda^{24})}, & \text{if } n \equiv 2 \pmod{8}, \\ & \frac{\lambda^{12}}{(1-\lambda^8)(1-\lambda^{24})}, & \text{if } n \equiv 4 \pmod{8}, \\ & \frac{\lambda^{30}}{(1-\lambda^8)(1-\lambda^{24})}, & \text{if } n \equiv 6 \pmod{8}. \end{aligned}$$

On the other hand it is easy to verify that the polynomials $f_{18}, f_{12}, f_{18}, f_{12}$ (see (12),(13)), of degrees 18, 12, 30 respectively, are indeed relative invariants with respect to the appropriate χ . This completes the proof of Theorem 5.

3. Self-dual codes of length up to 72 and their weight enumerators

In this section we attempt to determine the weight enumerators of self-dual codes of length $n \leq 72$ having the highest minimal distance d .

Calculation of weight enumerators. It is convenient to write the weight enumerator of \mathbf{C} as

$$W(y) = \sum A_r y^r$$

(setting $x = 1$ in $W(x, y)$), where A_r is the number of words of weight r , so that

$$W(y) = 1 + A_d y^d + \cdots . \tag{27}$$

From Gleason's theorem (see (10)) we can write

$$W(y) = \sum_{j=0}^{\lfloor n/8 \rfloor} a_j (1+y^2)^{n/2-4j} \{y^2(1-y^2)^2\}^j, \tag{28}$$

where $a_0 = 1$, and determine $a_1, \dots, a_{d/2-1}$ from (27). There are $\lfloor n/8 \rfloor$ coefficients a_j available, and if they are chosen to make $A_2 = A_4 = \cdots = A_{2\lfloor n/8 \rfloor} = 0$ then it is known that $A_{2\lfloor n/8 \rfloor+2} \neq 0$, and so any self-dual code satisfies

$$d \leq 2 \left\lceil \frac{n}{8} \right\rceil + 2 \quad (29)$$

([34], [31, Chap. 19]). The corresponding $W(y)$ is called an extremal weight enumerator. As we shall see, usually we cannot achieve equality in (29).

The weight enumerator of the shadow code (for any choice of the a_j 's) is given by

$$S(y) = \sum_{j=0}^{\lfloor n/8 \rfloor} (-1)^j a_j 2^{n/2-6j} y^{n/2-4j} (1-y^4)^{2j}, \quad (30)$$

(see (11)). From Theorem 5 we know that if \mathbf{C} is of Type II then

$$S(y) = 1 + A_d y^d + \cdots = W(y), \quad (31)$$

and if \mathbf{C} is of Type I then either

$$S(y) = y^{i_0} + a B_{d'} y^{d'} + \cdots \quad (32)$$

or

$$S(y) = B_{d'} y^{d'} + \cdots, \quad (33)$$

where $0 < i_0 < d/2$ and $d' \geq (d+4)/2$. This restriction on S constrains the final a_r 's, namely $a_{\lfloor n/8 \rfloor}, a_{\lfloor n/8 \rfloor - 1}, \dots$, often determining them uniquely.

We may then use Theorem 5(v) to determine the weight enumerators $W^{(1)}, W^{(3)}$ of cosets $\mathbf{C}^{(1)}, \mathbf{C}^{(3)}$. These satisfy

$$S(y) = W^{(1)}(y) + W^{(3)}(y).$$

The weight enumerators $W^{(0)}, W^{(2)}$ of cosets $\mathbf{C}^{(0)}, \mathbf{C}^{(2)}$ consist of the terms of $W(y)$ of the form y^{4m}, y^{4m+2} respectively. Thus

$$W(y) = W^{(0)}(y) + W^{(2)}(y).$$

An example. To illustrate we consider self-dual codes of length $n = 18$. From (29), $d \leq 6$. If $d = 6$ then from (27) we have $a_1 = a_2 = -9$; and

$$S(y) = -\frac{9}{8}y + \frac{153}{2}y^5 + \frac{1445}{4}y^9 + \frac{153}{2}y^{13} - \frac{9}{8}y^{17}$$

is determined by (11). Since the coefficients are not integers, this is impossible. Now suppose $d=4$. From (27) we have

$$\begin{aligned} W(y) &= 1 + (9+a_2)y^4 + (75-3a_2)y^6 + \cdots, \\ S(y) &= \frac{a_2}{8}y + \frac{144-a_2}{2}y^5 + \cdots. \end{aligned} \quad (34)$$

Therefore, from Theorem 5(iii), a_2 is 0 or 8, and so there are just two possibilities: either

$$\begin{aligned} W(y) &= 1 + 9y^4 + 75y^6 + 171y^8 + \cdots, \\ S(y) &= 72y^5 + 368y^9 + 72y^{13}, \end{aligned} \quad (35)$$

or

$$\begin{aligned} W(y) &= 1 + 17y^4 + 51y^6 + 187y^8 + \cdots, \\ S(y) &= y + 68y^5 + 374y^9 + 68y^{13} + y^{17}. \end{aligned} \quad (36)$$

We see the advantage of considering the shadow code. From Gleason's theorem alone we could conclude (if $d=4$) only that $W(y)$ has the form (34) for some undetermined a_2 .

In fact each possibility is realized by a unique code, (35) by the code d_6^{3+} and (36) by $(d_{10}e_7f_1)^+$ (see Eq. (15)) [44], [48].

We now determine the weight enumerators $W^{(j)}$ of the individual cosets $\mathbf{C}^{(j)}$ ($0 \leq j \leq 3$). In the case (35),

$$W^{(1)}(y) + W^{(3)}(y) = S(y) = 72y^5 + 368y^9 + \cdots, \quad (37)$$

while from Theorem 5 (since $n \equiv 2 \pmod{8}$) $W^{(1)}(y) - W^{(3)}(y)$ is a multiple of $f_{18} = y - 34y^5 + 34y^{13} - y^{17}$, say cf_{18} . From (12), (37), $c=0$, and $W^{(1)}(y) = W^{(3)}(y)$. We conclude that

$$\begin{aligned}
 W^{(0)}(y) &= 1 + 9y^4 + 171y^8 + \cdots , \\
 W^{(2)}(y) &= 75y^6 + \cdots , \\
 W^{(1)}(y) &= W^{(3)}(y) = 36y^5 + 184y^9 + \cdots .
 \end{aligned} \tag{38}$$

In the case (36),

$$\begin{aligned}
 W^{(1)}(y) + W^{(3)}(y) &= y + 68y^5 + 374y^9 + \cdots , \\
 W^{(1)}(y) - W^{(3)}(y) &= cf^{18} ,
 \end{aligned}$$

and so $c = \pm 1$, say $+1$. Then

$$\begin{aligned}
 W^{(0)}(y) &= 1 + 17y^4 + 187y^8 + \cdots , \\
 W^{(2)}(y) &= 51y^6 + \cdots , \\
 W^{(1)}(y) &= y + 17y^5 + 187y^9 + 51y^{13} , \\
 W^{(3)}(y) &= 51y^5 + 187y^9 + 17y^{13} + y^{17} .
 \end{aligned} \tag{39}$$

Weight enumerators of code (or putative codes) with the highest possible minimal distance. In the following paragraphs we record the results of applying the above method to codes of length up to 72.

When it is possible to use Theorem 5(v) to decompose S uniquely into $W^{(1)}$ and $W^{(3)}$ we do so, otherwise we just give S . The coefficients of $W(y)$, $S(y)$ (and sometimes $W^{(1)}(y)$, $W^{(3)}(y)$) are palindromic, and we give them only up to the midpoint. For codes of length $n \geq 34$ the expansions have been further truncated. We use β and γ for undetermined parameters, and $\overleftarrow{f}(y) = y^n f(1/y)$ to denote a reciprocal polynomial. The symbol \mathcal{E} indicates a family of weight enumerators for which no corresponding codes are known.

$n=2,4,6$, $d=2$. $W = (1+y^2)^{n/2}$, $S = (2y)^{n/2}$, $W^{(1)} = W^{(3)}$, a unique code (i_n – see (14),

[44]).

$n=8, d=4$, Type II. $W = S = f_g = 1 + 14y^4 + y^8$, a unique code (the Hamming code e_8 – see [44]).

$n=8, d=2$, Type I. $W = (1+y^2)^4, S = (2y)^4, W^{(1)} = W^{(3)}$, a unique code (i_{10} – see (14), [44]). (So there is no self-dual code with the weight enumerator $1 + 7y^2 + 7y^6 + y^8$ of the nonlinear formally self-dual code given in [31, p. 141, Fig. 5.1].)

$n=10, d=4$. $S = 5y/2 + 27y^5 + \dots$, impossible.

$n=10, d=2$. $W = 1 + (5-2\beta)y^2 + \dots, S = \beta y + (32-2\beta)y^5 + \dots, W^{(1)} = W^{(3)}$, so β is even and ≤ 2 , hence two possibilities: $W = 1 + y^2 + 14y^4 + \dots, S = 2y + 28y^5 + \dots$; or $W = 1 + 5y^2 + 10y^4 + \dots, S = 32y^5$. Each is realized by a unique code ($e_8 i_2; i_{10}$ – see [44]).

$n=12, d=4$. $W = 1 + 15y^4 + 32y^6 + \dots, S = 6y^2 + 52y^6 + \dots, W^{(1)} = 6y^2 + 20y^6 + \dots, W^{(3)} = 32y^6$, a unique code (d_{12}^+ – see [44]).

$n=14, d=4$. $W = 1 + 14y^4 + 49y^6 + \dots, S = 14y^3 + 100y^7 + \dots, W^{(1)} = W^{(3)}$, a unique code (e_7^2 – see [44]).

$n=16, d=6$. $W = 1 + 112y^6 + 30y^8 + \dots, S = -3/4 + 35y^4 + \dots$, impossible. (So there is no self-dual code with the weight enumerator of the Nordstrom-Robinson code.)

$n=16, d=4$. Either $W = S = f_8^2$, Type II, precisely two codes (e_8^2, d_{16}^+ – see [44]); or $W = 1 + 12y^4 + 64y^6 + 102y^8 + \dots, S = 32y^4 + 192y^8 + \dots, W^{(1)} = W^{(3)}$, a unique code (d_8^2 – see [44]).

$n=18$: discussed earlier in this section.

From now on we usually do not mention weight enumerators that can be eliminated.

$n=20, d=4$. $W = 1 + (5+4\beta)y^4 + (80-8\beta)y^6 + (250-4\beta)y^8 + (352+16\beta)y^{10} + \dots, S = \beta y^2 + (160-4\beta)y^6 + (704+6\beta)y^{10} + \dots$, precisely 7 codes, corresponding to

$\beta = 0, \dots, 4, 6, 10$ – see [44].

$n=22, \quad d=6. \quad W = 1+77y^6+330y^8+616y^{10} + \dots, \quad S = 352y^7+1344y^{11} + \dots,$
 $W^{(1)} = W^{(3)},$ a unique code (the “shorter Golay code” g_{22} defined in Sect. 2 – see [48]).

$n=24, d=8,$ Type II. $W = S = 1+759y^8+2576y^{12} + \dots,$ a unique code (the Golay code g_{24} – see [43], [48], [31], [14]).

$n=24, \quad d=6,$ Type I. $W = 1+64y^6+375y^8+960y^{10}+1296y^{12} + \dots, \quad S = 6y^4+744y^8$
 $+2596y^{12} + \dots, \quad W^{(1)} = 6y^4+360y^8+1316y^{12} + \dots, \quad W^{(3)} = 384y^8+1280y^{12} + \dots,$
a unique code (the “odd Golay code” f_{24} – see [48]).

$n=26, \quad d=6. \quad 2 \quad$ cases: either $W = 1+52y^6+390y^8+1313y^{10}+2340y^{12} + \dots,$
 $S = 26y^5+1560y^9+5020y^{13} + \dots, \quad W^{(1)} = W^{(3)},$ a unique code ($A_{26}=f_{13}^{2+}$ – see Table II,
[13], [45]); or $W = 1+20y^6+550y^8+1025y^{10}+2500y^{12} + \dots, \quad S = y+20y^5$
 $+1575y^9+5000y^{13} + \dots, \quad W^{(1)} = y+550y^9+2500y^{13}+1025y^{17}+20y^{21}, \quad W^{(3)} = \overset{\leftarrow}{W}^{(1)}$
(no code exists – see [13], [45]).

$n=28, \quad d=6. \quad$ Either $W = 1+26y^6+442y^8+1560y^{10}+3653y^{12}+5020y^{14} + \dots,$
 $W^{(1)} = y^2+52y^6+1703y^{10}+4680y^{14} + \dots, \quad W^{(3)} = 26y^6+1560y^{10}+5020y^{14} + \dots,$ a
unique code ($A_{28}=D1,$ omitted from [45] – see Table II, [13]); or
 $W = 1+42y^6+378y^8+1624y^{10}+3717y^{12} + 4680y^{14} + \dots, \quad S = 84y^6+3248y^{10} +$
 $9720y^{14} + \dots,$ precisely 2 codes ($B_{28}=f_7^{4+}(a), C_{28}=f_7^{4+}(b)$ – see [13], [45]).

$n=30, \quad d=6. \quad$ Three cases: $W = 1+19y^6+393y^8+1848y^{10}+5192y^{12}+8931y^{14} + \dots,$
 $W^{(1)} = W^{(3)} = y^3+114y^7+3375y^{11}+9404y^{15} + \dots,$ precisely 3 codes ($A_{30}, B_{30}, C_{30},$
omitted from [45] – see [13]); $W = 1+27y^6+369y^8+1848y^{10}+5256y^{12}+8883y^{14} + \dots,$
 $W^{(1)} = y^3+234y^7+6735y^{11}+18828y^{15} + \dots, \quad W^{(3)} = y^3 + 99y^7+3402y^{11}$
 $+9414y^{15} + \dots,$ a unique code ($D_{30},$ omitted from [45] – see [13]); or
 $W = 1+35y^6+345y^8+1848y^{10}+5320y^{12}+8835y^{14} + \dots, \quad W^{(1)} = W^{(3)} = 120y^7$

+3360y¹¹+9424y¹⁵+... , precisely 9 codes (E_{30}, \dots, M_{30} , only 8 of which are given in [45] – see [13]).

$n=32, d=8$. Either $W = S = 1+620y^8+13888y^{12}+36518y^{16}+\dots$, Type II, precisely 5 codes (see Sect. 4, [11]) or $W = 1+364y^8+2048y^{10}+6720y^{12}+14336y^{14}+18598y^{16}+\dots$, $S = 8y^4+592y^8+13944y^{12}+36448y^{16}+\dots$, $W^{(1)} = 8y^4+336y^8+6776y^{12}+18528y^{16}+\dots$, $W^{(3)} = 256y^8+7168y^{12}+17920y^{16}+\dots$, Type I; precisely 3 codes (see Sect. 4).

$n=34, d=6$. Either $W = 1+(34-4\beta)y^6+(255+4\beta)y^8+(1921+20\beta)y^{10}+(8466-20\beta)y^{12}+\dots$, $W^{(1)} = W^{(3)} = \beta y^5+(816-6\beta)y^9+(14144+15\beta)y^{13}+\dots$, codes exist corresponding to $\beta = 0$ (D2), 3 (R0), 1, 2, 4, 5, 6, 7 (not shown); or $W = 1+6y^6+411y^8+1165y^{10}+10886y^{12}+\dots$, $W^{(1)} = y+411y^9+10886y^{13}+\dots$, $W^{(3)} = 6y^5+1165y^9+17556y^{13}+\dots$, a code exists (R1).

$n=36, d=8$. Either $W = 1+225y^8+2016y^{10}+9555y^{12}+28800y^{14}+\dots$, $S = 42y^6+3780y^{10}+58230y^{14}+\dots$; or $W = 1+289y^8+1632y^{10}+10387y^{12}+28288y^{14}+\dots$, $W^{(1)} = y^2+34y^6+2176y^{10}+29886y^{14}+\dots$, $W^{(3)} = 1632y^{10}+28288y^{14}+\dots$; codes exist in both cases (R2, D3).

$n=38, d=8$. Either $W = 1+171y^8+1862y^{10}+10374y^{12}+36765y^{14}+\dots$, $S = 114y^7+9044y^{11}+118446y^{15}+\dots$; or $W = 1+203y^8+1702y^{10}+10598y^{12}+36925y^{14}+\dots$, $S = y^3+106y^7+9072y^{11}+118390y^{15}+\dots$, codes exist in both cases (D4, R3).

$n=40, d=8$. Either $W = S = 1+285y^8+21280y^{12}+239970y^{16}+525504y^{20}+\dots$, Type II, at least 100 codes – see [60], [73] (e.g. D5); or $W = 1+(125+16\beta)y^8+(1664-64\beta)y^{10}+(10720+32\beta)y^{12}+(44160+192\beta)y^{14}+\dots$, $S = \beta y^{14}+(320-8\beta)y^8+(21120+28\beta)y^{12}+\dots$, Type I, codes exist corresponding to $\beta=0$ and 10 (D6, D7) and possibly

other values.

$n=42, \quad d=8.$ Either $W = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + (10640 - 16\beta)y^{12} + (50256 + 112\beta)y^{16} + \dots$, $S = \beta y^5 + (896 - 8\beta)y^9 + (48384 + 28\beta)y^{13} + \dots$, codes exist corresponding to at least $\beta = 0$ (R4), $1, \dots, 7$ (not shown), and 42 (a cyclic self-dual code with generator polynomial $(x+1)(x^2+x+1)(x^3+x+1)^2(x^6+x^5+x^4+x^2+1)^2$ [17a], [54a]); or $\mathcal{C} \quad W = 1 + 164y^8 + 697y^{10} + 15088y^{12} + 33456y^{14} + \dots$, $W^{(1)} = \overleftarrow{W}^{(3)} = y + 164y^9 + 15088y^{13} + 196718y^{17} + 512992y^{21} + 289460y^{25} + 33456y^{29} + 697y^{33}$, no known codes.

$n=44, \quad d=8.$ Either $W = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + (12289 - 20\beta)y^{12} + (47904 + 48\beta)y^{14} + \dots$, $W^{(1)} = y^2 + (\beta - 10)y^6 + 1533y^{10} + (61096 - 20\beta)y^{14} + \dots$, $W^{(3)} = (976 - 8\beta)y^{10} + (47904 + 48\beta)y^{14} + \dots$, codes exist corresponding to at least $\beta=14$ (not shown) and 17 (D8); or $W = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} + (54560 + 48\beta)y^{14} + \dots$, $S = \beta y^6 + (2464 - 8\beta)y^{10} + (109120 + 28\beta)y^{14} + \dots$, codes exist corresponding to at least $\beta=4$ (R5), $5, \dots, 15$ (not shown).

$n=46, \quad d=10.$ $W = 1 + 1012y^{10} + 9660y^{12} + 56925y^{14} + 235290y^{16} + \dots$, $W^{(1)} = W^{(3)} = 3312y^{11} + 121440y^{15} + \dots$, a code exists (subtract i_2 from q_{48}).

$n=48, \quad d=12,$ Type II. $W = S = 1 + 17296y^{12} + 535095y^{16} + 3995376y^{20} + 7681680y^{24} + \dots$, a code exists (q_{48} – see also [20]).

$n=48, \quad d=10,$ Type I. Either $\mathcal{C} \quad W = 1 + 704y^{10} + 8976y^{12} + 56896y^{14} + 267575y^{16} + \dots$, $S = y^4 + 44y^8 + 17021y^{12} + 535920y^{16}$, no known codes; or $W = 1 + 768y^{10} + 8592y^{12} + 57600y^{14} + 267831y^{16} + \dots$, $S = 54y^8 + 16976y^{12} + 536040y^{16}$, ... a code exists (N1).

$n=50, \quad d=10.$ Either $\mathcal{C} \quad W = 1 + 196y^{10} + 11368y^{12} + 31752y^{14} + 397782y^{16} + \dots$,

$W^{(1)} = \overleftarrow{W}^{(3)} = y + 11368y^{13} + 397782y^{17} + \dots + 31752y^{37} + 196y^{41}$, no known codes;
 or $W = 1 + (580 - 32\beta)y^{10} + (7400 + 160\beta)y^{12} + (56200 - 160\beta)y^{14} + (292950 - 480\beta)y^{16}$
 $+ \dots$, $S = \beta y^5 + (250 - 10\beta)y^9 + (42800 + 45\beta)y^{13} + \dots$, a code exists corresponding to
 $\beta=0$ (D9). *Remark.* Suppose a $[50,25,10]$ code exists corresponding to the first weight
 enumerator, and let C be the $[49,25,9]$ code obtained by deleting the coordinate corresponding
 to the y term in $W^{(1)}$. Then it can be shown [6] that the codewords of any fixed weight in C
 form a 2-design. In particular, the codewords of minimal weight form a 2-design with
 parameters $v=49, b=196, r=36, k=9, \lambda=6$, in which any two distinct blocks meet in either
 1 or 3 points. Conversely, if such a design exists then so does the code.

$n=52, d=10$. Either $W = 1 + 250y^{10} + 7980y^{12} + 42800y^{14} + 349150y^{16} + \dots$, $W^{(1)} = y^2 +$
 $580y^{10} + 63600y^{14} + \dots$, $W^{(3)} = 250y^{10} + 42800y^{14} + \dots$, a code exists (D10); or \overleftarrow{W}
 $W = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + 53040y^{14} + (308958 - 320\beta)y^{16} + \dots$, $S =$
 $\beta y^6 + (884 - 10\beta)y^{10} + (106080 + 45\beta)y^{14} + \dots$, no known codes.

$n=54, d=10$. Either $W = 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + (48492 + 32\beta)y^{14}$
 $+ (315198 - 160\beta)y^{16} + \dots$, $S = \beta y^7 + (2808 - 10\beta)y^{11} + (258624 + 45\beta)y^{15} + \dots$, a
 code exists (subtract i_2 from D11); or \overleftarrow{W} $W = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12}$
 $+ (43884 + 32\beta)y^{14} + (332094 - 160\beta)y^{16} + \dots$, $S = y^3 + (\beta - 12)y^7 + (2874 - 10\beta)y^{11}$
 $+ (258404 + 45\beta)y^{15} + \dots$, no known codes.

$n=56, d=12$, Type II. $W = S = 1 + 8190y^{12} + 622314y^{16} + 11699688y^{20} + 64909845y^{24}$
 $+ \dots$, at least 20 codes exist – see [9], [70] (for example D11).

$n=56, d=12$, Type I. Either \overleftarrow{W} $W = 1 + 4606y^{12} + 45056y^{14} + 306922y^{16}$
 $+ 1576960y^{18} + \dots$, $S = 77y^8 + 7630y^{12} + 624393y^{16} + \dots$; or \overleftarrow{W} $W = 1 + 4862y^{12}$
 $+ 43008y^{14} + 313066y^{16} + 1570816y^{18} + \dots$, $W^{(1)} = y^4 + 65y^8 + 4368y^{12} + 314926y^{16}$
 $+ \dots$, $W^{(3)} = 3328y^{12} + 309248y^{16} + \dots$; no known codes in either case. A code exists

with $d = 10$ (N2).

$n = 58, d = 10$. Either \mathcal{C} $W = 1 + (165 - 2\gamma)y^{10} + (5078 + 2\gamma)y^{12} + (17190 + 188)y^{14} + (433323 - 18\gamma)y^{16} + \dots$, $S = y + \gamma y^9 + (23918 - 10\gamma)y^{13} + (1471338 + 458)y^{17} + \dots$, no known codes; or $W = 1 + (319 - 24\beta - 2\gamma)y^{10} + (3132 + 152\beta + 2\gamma)y^{12} + (36540 - 680\beta + 18\gamma)y^{14} + (299541 + 1832\beta - 18\gamma)y^{16} + \dots$, $S = \beta y^5 + \gamma y^9 + (24128 - 54\beta - 10\gamma)y^{13} + (1469952 + 320\beta + 45\gamma)y^{17} + \dots$, codes exist corresponding to $\beta = \gamma = 0$ (D12) and $\beta = 0, \gamma = 58$ (D12a).

$n = 60, d = 12$. Three cases: \mathcal{C} $W = 1 + 2555y^{12} + 33600y^{14} + 278865y^{16} + 1717760y^{18} + \dots$, $S = 396y^{10} + 63240y^{14} + 3453340y^{18} + \dots$, no known codes; \mathcal{C} $W = 1 + 2619y^{12} + 33216y^{14} + 279441y^{16} + 1718784y^{18} + \dots$, $S = y^6 + 384y^{10} + 63306y^{14} + 3453120y^{18} + \dots$, no known codes; or $W = 1 + 3451y^{12} + 24128y^{14} + 336081y^{16} + 1469952y^{18} + \dots$, $W^{(1)} = y^2 + 319y^{10} + 39672y^{14} + 1981309y^{18} + \dots$, $W^{(3)} = 24128y^{14} + 1469952y^{18} + \dots$, a code exists (D13).

(This completes the proof of Theorem 2.)

$n = 62, d = 12$. Either \mathcal{C} $W = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + (255533 + 96\beta)y^{16} + (1718020 + 800\beta)y^{18} + \dots$, $S = \beta y^7 + (1116 - 12\beta)y^{11} + (171368 + 66\beta)y^{15} + \dots$, or \mathcal{C} $W = 1 + 2308y^{12} + 23767y^{14} + 279405y^{16} + 1622724y^{18} + \dots$, $S = y^3 + 1039y^{11} + 171928y^{15} + \dots$; no known codes in either case.

$n = 64, d = 12$, Type II. $W = S = 1 + 2976y^{12} + 454956y^{16} + 18275616y^{20} + 233419584y^{24} + \dots$; at least 38 codes exist – see [71] (for example D14).

$n = 64, d = 12$, Type I. Either \mathcal{C} $W = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + (239148 - 32\beta)y^{16} + \dots$, $S = y^4 + (\beta - 14)y^8 + (3419 - 12\beta)y^{12} + (451732 + 66\beta)y^{16} + \dots$, no known codes; or $W = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + (228908 - 32\beta)y^{16} + \dots$, $S = \beta y^8 + (3328 - 12\beta)y^{12} + (452096 + 66\beta)y^{16} + \dots$, a

code exists corresponding to $\beta = 32$ (D15).

$n = 72$, $d = 14$, Type I. Three cases: ☞ $W = 1 + 7616y^{14} + 134521y^{16} + 1151040y^{18} + \dots$,
 $S = y^4 + 442y^{12} + 245480y^{16} + \dots$; ☞ $W = 1 + 8576y^{14} + 124665y^{16} + 1206912y^{18}$
 $+ \dots$, $S = y^8 + 532y^{12} + 244675y^{16} + \dots$; or ☞ $W = 1 + 8640y^{14} + 124281y^{16}$
 $+ 1207360y^{18} + \dots$, $S = 546y^{12} + 244584y^{16} + \dots$; no known codes in any case.

Examples of self-dual codes. The following codes, referred to in the preceding paragraphs, have the highest possible minimal distance d of any self-dual code of the given length and type. (The codes N1, N2, D1-D4, D6-D10, D12-D13, D15-D20, R1-R5 appear to be new.)

The neighbor construction. If C is a self-dual code and $u \notin C$ has even weight then the *neighbor* $N(u)$ of C corresponding to u is generated by u and the vectors $\{v \in C : u \cdot v = 0\}$. It is easy to show that $N(u)$ is self-dual and that any self-dual code of length n can be reached from any other by taking successive neighbors. The analogous construction for lattices was used by Kneser [23].

(q_{48}). The $[48,24,12]$ Type II quadratic residue code q_{48} is generated by the vectors 11...1 and

$$1(01111011110010101110010011011000101011000010000)$$

(with 1's at the nonzero squares modulo 47). The parentheses indicate as usual that all cyclic shifts are to be used – compare [7], [11].

(N1) If $u = 08050410CD00$, the corresponding neighbor $N(u)$ of q_{48} is a $[48,24,10]$ Type I code.

(N2) If $u = B12FC10D44D47C$ the corresponding neighbor $N(u)$ of D11 (see Table II) is a $[56,28,10]$ Type I code.⁽⁴⁾

(4) Unlike other codes in this section, this does not necessarily have the highest possible d (cf. Table I).

The double circulant construction. Table II lists self-dual codes having generator matrices of the form

I	0	1	1	1	1
	1	R			
	1				
	1				
	1				
	1				

(40)

or

I	R
---	---

(41)

where R is a circulant matrix with first row r . (40) is used only when $n \equiv 0 \pmod{4}$. These constructions have been investigated by several authors [1], [3], [21], [22], [29], [31, Chap. 16], [49], [62], [63], [68]-[71].

Table II

Double circulant codes

Name	n	k	d	Type	Form	r (hexadecimal)
g_{22}	22	11	6	I	(41)	97
g_{24}	24	12	8	II	(40)	B7
$A_{26} = f_{13}^{2+}$	26	13	6	I	(41)	5F7
$A_{28} = D1$	28	14	6	I	(40)	8D
D2	34	17	6	I	(41)	1ECE
D3	36	18	8	I	(40)	2C6B
D4	38	19	8	I	(41)	5793
D5	40	20	8	II	(41)	57EB
D6	40	20	8	I	(41)	11E35
D7	40	20	8	I	(41)	B393
D8	44	22	8	I	(40)	5E6B5
D9	50	25	10	I	(41)	31C4D
D10	52	26	10	I	(40)	57F69D
D11	56	28	12	II	(40)	ADF1FF
D12	58	29	10	I	(41)	D5A89B
D12a	58	29	10	I	(41)	2DD1D3
D13	60	30	12	I	(40)	3EF6B77
D14	64	32	12	II	(40)	427BD0B
D15	64	32	12	I	(41)	2EF3DD75
D16	66	33	12	I	(41)	B2D97D9
D17	68	34	12	I	(41)	1F5C885F
D18 ⁽⁴⁾	72	36	12	I	(41)	2B8795E5
D19 ⁽⁴⁾	74	37	12	I	(41)	1439372C7
D20 ⁽⁴⁾	82	41	12	I	(41)	A464B919B

Codes with no known structure. The codes in Table III were found by constructing self-dual codes at random until a sufficiently high minimal distance occurred. The algorithm used was a binary version of that given in the appendix to [28], modified as follows. After $n/2 - 1$ generators are found, instead of searching randomly for the final generator, the program searches for an even weight vector in $B^* \setminus B$, where B is the code generated by the first $n/2 - 1$ generators.

We describe these codes by giving the rows of A in hexadecimal, where $[IA]$ is a generator matrix.

Table III

Codes with no known structure

(R0) [34,17,6]: 033E3, 037D8, 03D05, 0710E, 07C0F, 08548, 08A2B, 0AC94, 0B8AB, 0D09C, 107C8, 11CAE, 150A6, 186FB, 1C018, 1C693, 1CBB0

(R1) [34,17,6]: 04B8A, 04D43, 05A07, 083A9, 0C84E, 0CBFC, 0CD28, 0D5BD, 0D834, 0EF5A, 0F5D3, 0F902, 12331, 188D4, 197B3, 1DCEC, 1E0BA

(R2) [36,18,8]: 03BB4, 05FEA, 07113, 0C7F6, 123BA, 133C6, 13770, 19B64, 1A86D, 1CAE1, 1F3A0, 260FA, 2A751, 2EAEF, 31666, 32179, 36502, 37F59

(R3) [38,19,8]: 078F4, 1499B, 15B0D, 18338, 18744, 19194, 1E2FA, 2B40A, 2DF8A, 31457, 35F67, 3C23F, 4C3A6, 4C535, 530FB, 566C1, 5B226, 6EA18, 70897

(R4) [42,21,8]: 020D3D, 02854A, 039F91, 061D23, 06295C, 06DA9F, 076544, 086B07, 0A7377, 0DD96D, 0DF2FE, 0F505E, 125583, 139C17, 14AA29, 198EAA, 19D343, 1B6414, 1C7EB2, 1D3619, 1F12EB

(R5) [44,22,8]: 01597D, 03E68E, 0684E0, 06D614, 09E19E, 0A6385, 141CDB, 178090, 1D71EC, 1F2F97, 1F52D3, 22F5FB, 260267, 268334, 277D38, 282BD9, 293F8E, 2A8D24, 33AE9F, 350159, 3528E5, 3D17C0

4. The proof of Theorems 3 and 4

It was shown in [11] that there are precisely five [32,16,8] codes. Koch [24], [25] has given an alternative proof of this result. These codes are

- CP1 (or q_{32}), a quadratic residue code,
- CP2 (or r_{32}), a second-order Reed-Muller code,
- CP3 (or $2g_{16}$), a twisted Reed-Muller code,
- CP4 (or $8f_4$),
- CP5 (or $16f_2$).

CP1 is generated by the vectors

$$1(0001001000011101010001111011011)$$

(having 1's at the nonresidues modulo 31), CP2 is well-known (see for example [31]), and a generator matrix for CP5 is given at the foot of p. 41 of [11]. Koch [24] and Yorgov [72] have given alternative constructions for CP3 and CP4. Let e_8 be the particular version of the [8,4,4] Hamming code generated by the vectors $1(1101000)$, let e'_8 be the version generated by $1(1011000)$, and let G_1, G_2 be corresponding generator matrices. Let τ be the permutation $(0)(1, 2, \dots, 7)$. Then CP3 and CP4 have generator matrices

$$\text{CP3 : } \begin{bmatrix} G_1 & 0 & G_1 & 0 \\ 0 & G_1 & G_1 & G_1 \\ G_2 & G_2 & G_2 & 0 \\ 0 & G_2 & 0 & G_2 \end{bmatrix}, \quad (42)$$

$$\text{CP4 : } \begin{bmatrix} G_1 & 0 & G_1 & G_1 \\ 0 & G_1 & G_1 & \tau G_1 \\ G_2 & G_2 & G_2 & 0 \\ G_2 & \tau^{-1} G_2 & 0 & G_2 \end{bmatrix}. \quad (43)$$

An *octet* in one of these codes is a set eight mutually disjoint sets of four coordinates (called *tetrads*) with the property that the union of any two is the support of a word of weight eight in the code. It is not difficult to verify with the assistance of a computer that the number of octets is as follows:

$$\text{CP1} : 0, \text{CP2} : 155, \text{CP3} : 35, \text{CP4} : 1, \text{CP5} : 0.$$

Also all octets in any CP_i are equivalent under the group of the code. Furthermore, if t_1, \dots, t_8 are the tetrads of an octet in CP_i , then for all $u \in \text{CP}_i$, either $|u \cap t_1|, \dots, |u \cap t_8|$ are even or $|u \cap t_1|, \dots, |u \cap t_8|$ are odd.

Proof of Theorem 3. We show that any $[32,16,8]$ Type I code \mathbf{C} can be constructed in a certain way from a unique $[32,16,8]$ Type II code \mathbf{B} . From Theorem 5 it follows (see the previous section) that $W = 1 + 364y^8 + 2048y^{10} + \dots$, $S = 8y^4 + 592y^8 + \dots$. If $\mathbf{C}^{(1)}$ and $\mathbf{C}^{(3)}$ both contain vectors of weight 4 then their sum is in $\mathbf{C}^{(2)}$ and so has weight 6, a contradiction. Therefore we may assume $\mathbf{C}^{(1)}$ contains all 8 vectors of weight 4. These must be disjoint, and the sum of any two is a word of weight 8 in $\mathbf{C}^{(0)}$.

The code $\mathbf{B} = \mathbf{C}^{(0)} \cup \mathbf{C}^{(3)}$ is self-dual (see the proof of Theorem 5), has minimal weight 8, and so must be one of the CP_i . By the previous paragraph \mathbf{B} contains an octet. Also $\mathbf{C}^{(2)}$ is a translate of $\mathbf{C}^{(3)}$ by any of the eight tetrads in the octet. Thus \mathbf{C} is obtained from \mathbf{B} by the following construction.

Let \mathbf{B} be a CP_i that contains an octet, and let t be any tetrad of the octet. We form \mathbf{C} by taking all words $u \in \mathbf{B}$ that meet t in an even number of coordinates, together with all words $u + t$ where $u \in \mathbf{B}$ meets t in an odd number of coordinates. It is easy to check that \mathbf{C} is linear and self-dual, and is independent of the choice of t . Also the minimal weight in \mathbf{C} is 8, since if u intersects t oddly then u intersects all eight tetrads oddly and so has weight at least 8. By adding t we change the weight of u from $4m$ to $4m \pm 2$. We conclude that \mathbf{C} is a $[32,16,8]$ Type I code. Precisely three such codes arise in this way, from CP_2 , CP_3 and CP_4 , since each of these contains just one type of octet. This completes the proof.

Proof of Theorem 4. Let Ω_n be the set of all distinct (but not necessarily inequivalent) self-dual codes of length n (of both types if n is a multiple of 8), and let

$$\Psi(y) = \frac{1}{|\Omega_n|} \sum_{C \in \Omega_n} W(y) = \sum_0^n \psi_j y^j \quad (44)$$

be their average weight enumerator. If $\psi_2 + \psi_4 + \dots + \psi_{d-2} < 1$, there must exist an $[n, n/2, d]$ self-dual code. We know from [48] that, if $n = 2m$,

$$\Psi(y) = \left[2^{m-1} + 1 \right]^{-1} \left\{ 2^{m-1} (1 + y^{2m}) + \sum_{j=0}^m \binom{2m}{2j} y^{2j} \right\}. \quad (45)$$

There are similar expressions for codes of Type I and Type II alone. Equation (45) implies that self-dual codes with

$d \geq 4$	exist	if	$n \geq 16$
$d \geq 6$	exist	if	$n \geq 34$
$d \geq 8$	exist	if	$n \geq 50$
$d \geq 10$	exist	if	$n \geq 68$
$d \geq 12$	exist	if	$n \geq 86$
$d \geq 14$	exist	if	$n \geq 104$
$d \geq 16$	exist	if	$n \geq 122$
$d \geq 18$	exist	if	$n \geq 140$
$d \geq 20$	exist	if	$n \geq 158$.

This, coupled with codes from [31] and Section III, completes the proof of Theorem 4.

The same method can be used to obtain lower bounds on the number of inequivalent codes. Consider Type I codes of length 34, for example. Let N be the total number of distinct codes, and let N_r be the number that contain precisely r words of weights 2 and 4. Then

$$N = \prod_{j=1}^{16} (2^j + 1) = 2.0769 \dots \cdot 10^{41},$$

(from [48]), and from (44), (45) the average number of vectors of weights 2 and 4 is

$$\psi_2 + \psi_4 = \frac{46937}{65537} = \lambda \quad (\text{say}).$$

The total number of words of weight 2 and 4 is

$$\begin{aligned}\lambda N &= 1 \cdot N_1 + 2 \cdot N_2 + 3 \cdot N_3 + \dots \\ &\geq N_1 + N_2 + N_3 + \dots = N - N_0.\end{aligned}$$

Therefore the number of codes with no vectors of weight 6 is

$$N_0 \geq N(1-\lambda) = 5.8945\dots \cdot 10^{40}.$$

Since each code has a symmetry group of order at most $34!$, we conclude that there are at least $5.8945\dots \cdot 10^{40}/34! = 199.65\dots$ (hence 200) inequivalent [34,17,8] Type I codes (see Table I).

5. The proof of Theorem 1.

Type II codes. If \mathbf{C} is of Type II then the highest minimal distance is known for $n \leq 88$, $n \neq 72$ [14, p. 194], [31, p. 626]. For $n \geq 80$, $2[(n+6)/10]$ is greater than or equal to the Mallows-Sloane bound (2). This establishes the result for Type II codes.

Type I codes. Let \mathbf{C} be a Type I code of length $n = 8k + 2t$, $0 \leq t \leq 3$. The weight enumerators of \mathbf{C} and its shadow \mathbf{S} can be written as in (28), (30), for certain integers $a_0 = 1$, a_1, \dots, a_k . For $n \leq 72$ the theorem follows from the results in Section 4, so we now assume $n > 72$. We write $n = 10l + 2\delta$, $-3 \leq \delta \leq 1$, and suppose, contrary to the theorem, that $d \geq 2[(n+6)/10] + 2$. We actually assume $d = 2[(n+6)/10] + 2 = 2l + 2$, for the same contradictions apply if d is greater than this value. Then

$$W(y) = 1 + A_d y^{2l+2} + \dots \tag{46}$$

We apply the method used in [34]. Equating (28) and (46) and dividing by $(1+y^2)^{n/2}$ yields

$$(1+Y)^{-n/2} = \sum_{j=0}^l a_j \left\{ \frac{Y(1-Y)}{(1+Y)^4} \right\}^j + \text{terms of order } Y^{l+1},$$

where $Y = y^2$. The a_j for $j \leq l$ can be determined by expanding $(1+Y)^{-n/2}$ in powers of

$$\phi = \frac{Y(1-Y)}{(1+Y)^4}$$

via the Bürmann-Lagrange theorem ([19], [31, p. 627], [33], [34], [65]):

$$\begin{aligned} a_j &= \frac{1}{j!} \left[\frac{d^{j-1}}{dY^{j-1}} \left\{ \frac{d}{dY} (1+Y)^{-n/2} \left[\frac{Y}{\phi} \right]^j \right\} \right]_{Y=0} \\ &= - \frac{n}{2 \cdot j!} \left[\frac{d^{j-1}}{dY^{j-1}} \left\{ (1+Y)^{-n/2-1-4j} (1-Y)^{-2j} \right\} \right]_{Y=0}, \end{aligned} \quad (47)$$

and in particular

$$a_l = - \frac{n}{2l} \cdot \text{coefficient of } Y^{l-1} \text{ in } (1+Y)^{-l-\delta-1} (1-Y)^{-2l} \quad (48)$$

$$\begin{aligned} &= - \frac{n}{2l} \sum_{j=0}^{l-1} (-1)^j \begin{bmatrix} -2l \\ j \end{bmatrix} \begin{bmatrix} -l-\delta-1 \\ l-j-1 \end{bmatrix} \\ &= \frac{n}{2l} \sum_{j=0}^{l-1} (-1)^{l+j} \begin{bmatrix} 2l+j-1 \\ j \end{bmatrix} \begin{bmatrix} 2l+\delta-j-1 \\ l-j-1 \end{bmatrix}. \end{aligned} \quad (49)$$

On the other hand an upper bound for $|a_l|$ can be obtained by considering S . Let

$$S = \sum B_r y^r. \quad (50)$$

From Theorem 5 we know that there is at most one nonzero B_r for $r < (d+4)/2$. Let $B_{i_0} y^{i_0}$ be the lowest degree nonzero term in S . Then $B_{i_0} = 1$ if $i_0 < d/2$, $B_{i_0} \leq 2n/d$ if $i_0 = d/2$ (from Eqs. (6),(7)). Furthermore $B_0 = 0$ (Eq. (5)), and (from (4)) $B_r = 0$ unless $r \equiv t \pmod{4}$.

Therefore we can rewrite (30) as

$$\frac{S}{y^t} = \sum_{j=j_0}^k (-1)^{k-j} a_{k-j} 2^{n/2-6k+6j} Z^j (1-Z)^{2k-2j},$$

where $i_0 = 4j_0 + t$, $Z = y^4$,

$$= B_{i_0} Z^{j_0} + \text{terms of order } Z^J, \quad (51)$$

where $J = \lceil (d/2 + 1 - t)/4 \rceil$. We divide this by $(1-Z)^{2k}$ and use the Bürmann-Lagrange theorem

to expand $Z^{j_0}(1-Z)^{-2k}$ in powers of $\phi = Z(1-Z)^{-2}$. Let

$$Z^{j_0}(1-Z)^{-2k} = \sum \alpha_j \phi^j . \quad (52)$$

Then α_j is determined for $j \leq J-1$. We have

$$\alpha_j = \frac{1}{j!} \left[\frac{d^{j-1}}{dZ^{j-1}} \left\{ \frac{d}{dZ} (Z^{j_0}(1-Z)^{-2k}) \left[\frac{Z}{\phi} \right]^j \right\} \right]_{Z=0} , \quad (53)$$

and (comparing (51), (52)),

$$a_{k-j} = (-1)^{k-j} 2^{-n/2+6k-6j} B_{i_0} \alpha_j , \quad (54)$$

for $j \leq J-1$. To obtain a bound for a_l we set $j=j'$, where $k-j' = l$. The value of j' depends on the residue class of n modulo 40, as shown in Table IV. The table also gives d and $J-1$.

Table IV

Values of d , $J-1$ and j' as functions of n

$n=40a +$	0	2	4	6	8	10	12	14	16	18
k	$5a$	$5a$	$5a$	$5a$	$5a+1$	$5a+1$	$5a+1$	$5a+1$	$5a+2$	$5a+2$
t	0	1	2	3	0	1	2	3	0	1
l	$4a$	$4a$	$4a+1$	$4a+1$	$4a+1$	$4a+1$	$4a+1$	$4a+2$	$4a+2$	$4a+2$
δ	0	1	-3	-2	-1	0	1	-3	-2	-1
d	$8a+2$	$8a+2$	$8a+4$	$8a+4$	$8a+4$	$8a+4$	$8a+4$	$8a+6$	$8a+6$	$8a+6$
$J-1$	a	a	a	$a-1$	a	a	a	a	a	a
j'	a	a	$a-1$	$a-1$	a	a	a	$a-1$	a	a
$n=40a +$	20	22	24	26	28	30	32	34	36	38
k	$5a+2$	$5a+2$	$5a+3$	$5a+3$	$5a+3$	$5a+3$	$5a+4$	$5a+4$	$5a+4$	$5a+4$
t	2	3	0	1	2	3	0	1	2	3
l	$4a+2$	$4a+2$	$4a+3$	$4a+3$	$4a+3$	$4a+3$	$4a+3$	$4a+4$	$4a+4$	$4a+4$
δ	0	1	-3	-2	-1	0	1	-3	-2	-1
d	$8a+6$	$8a+6$	$8a+8$	$8a+8$	$8a+8$	$8a+8$	$8a+8$	$8a+10$	$8a+10$	$8a+10$
$J-1$	a	a	$a+1$	a	a	a	$a+1$	$a+1$	a	a
j'	a	a	a	a	a	a	$a+1$	a	a	a

From (23),

$$\begin{aligned} \alpha_{j'} &= \frac{j_0}{j'} \cdot \text{coefficient of } Z^{j'-j_0} \text{ in } (1-Z)^{2j'-2k} \\ &\quad - \frac{2k}{j'} \cdot \text{coefficient of } Z^{j'-j_0-1} \text{ in } (1-Z)^{2j'-2k-1} \end{aligned} \quad (55)$$

$$= - \frac{2(kj' - 2kj_0 + j'j_0)}{j'(j'-j_0)} \left[\frac{2k-j'-j_0-1}{j'-j_0-1} \right]. \quad (56)$$

The magnitude of this expression is maximized by taking $j_0=0$. Setting $j_0=0$ in (54), (56) we obtain

$$|a_l| \leq \frac{2kc}{j'} 2^{6l-n/2} \left[\frac{2k-j'-1}{j'-1} \right], \quad (57)$$

where c is 1 unless $4j'+t = d/2$, in which case $c = 2n/d$. This is the desired bound for a_l .

For n in the range $74 \leq n \leq 500$, (49) exceeds this bound (thus proving the result), for all except the 12 values $n=82, 92, 102, 112, 122, 132, 152, 162, 172, 192, 202$ and 232 . This may be established by direct calculation of (49) and (57). Even though there is massive cancellation in (49), double precision arithmetic on a Cray X-MP computer is accurate enough to evaluate the sum in (49) to at least 14 significant digits. For example, when $n=500, l=50$, from (49) we find that $a_{50} = -3.347020 \cdots \cdot 10^{33}$ (although the largest terms in the sum are around $\pm 10^{46}$), while (57) gives $|a_{50}| \leq 1.059833 \cdots \cdot 10^{31}$, a contradiction.

For the 12 values $82, \dots, 232$ we establish a contradiction as follows. The coefficients a_0, \dots, a_l are calculated from (28) and (46), and substituted in S (in Eq.(30)). Then a_{l+1}, a_{l+2}, \dots are determined by requiring that the leading coefficients $\{B_i : i < d/2\}$ in S shall either all be zero or exactly one of them be 1 and the rest zero. In every case it turns out that one of the next two coefficients in S (B_{4J+t} or B_{4J+4+t}) is negative. This is impossible, and establishes the result. For example, when $n=82$ (so that $k=8, t=1, l=8, d=18$), we have $a_0=1, a_1=-41, a_2=615, a_3=-4182, a_4=13161, a_5=-18040, a_6=9512, a_7=-3280$ and

$a_8 = -39524$. If we require that S/y begins $0 \cdot Z + 0 \cdot Z^2 + \dots$, then $a_9 = a_{10} = 0$ and

$$S/y = -308.78\dots Z^3 + 6580.5 Z^4 + \dots$$

The negative coefficient yields the desired contradiction. (We could also deduce the contradiction from the fact that the coefficients are not integers.) Similar contradictions arise in the cases $S/y = 1 \cdot Z + 0 \cdot Z^2 + \dots$ and $0 \cdot Z + 1 \cdot Z^2 + \dots$.

For $n \geq 500$ we apply the saddle-point method [8]. For simplicity we assume that n is a multiple of 40, $n = 40a$ say, so that $k = 4a$, $t = 0$, $l = 4a$, $\delta = 0$, $d = 8a + 2$ and $j' = a$. The other 19 residue classes modulo 40 can be handled in the same way.

To further simplify the analysis⁽⁵⁾ we begin by verifying that (49) exceeds (57) for all $n = 40a$ in the range $500 < n \leq 3000$. This calculation can be carried out exactly (in multiple-precision integers) using the Macsyma program [35]. For example when $n = 3000$ we find from (49) that $a_{300} = -8.890\dots \cdot 10^{207}$, whereas from (57) $|a_{300}| < 2.002\dots \cdot 10^{193}$, a contradiction. Therefore, when applying the saddle-point method, we may assume $n > 3000$, $l > 300$.

We first estimate $b_l = -2n^{-1}l a_l$, which from (48) is equal to the coefficient of Y^{l-1} in $(1+Y)^{-l-1}(1-Y)^{-2l}$. From Cauchy's formula,

$$b_l = \frac{1}{2\pi i} \int \frac{(1+Y)^{-l-1}(1-Y)^{-2l}}{Y^{l+1}} dY,$$

integrated along a small circle around 0. Let $Y = e^{2\pi iz}$, $z = \theta + iy$, so that

$$\begin{aligned} b_l &= \int_P \frac{1}{1+e^{2\pi iz}} \left\{ \frac{1}{e^{2\pi iz}(1-e^{2\pi iz})(1-e^{4\pi iz})} \right\}^l dz \\ &= \int_P g(z) e^{lh(z)} dz, \end{aligned} \tag{58}$$

(5) In retrospect it is clear that a much smaller value than 3000 would suffice.

where P is any path $\{ z = \theta + iy : -\frac{1}{2} < \theta \leq \frac{1}{2} \}$, $y > 0$, $g(z) = (1 + e^{2\pi iz})^{-1}$ and

$$h(z) = -\log \{ e^{2\pi iz}(1 - e^{2\pi iz})(1 - e^{4\pi iz}) \}.$$

Then

$$h'(z) = 2\pi i \cdot \frac{4q^2 + q - 1}{1 - q^2}, \quad q = e^{2\pi iz},$$

$$h''(z) = 4\pi^2 \cdot \frac{4q^5 - 3q^4 - 7q^3 - 2q^2 + q - 1}{q(1 - q^2)^2}.$$

We see that $h'(z) = 0$ when $q = q_0 = (\sqrt{17} - 1)/8 = 0.390\dots$ and $z = z_0 = iy_0$, $y_0 = 0.14970331\dots$. Then

$$e^{h(z_0)} = \frac{1}{q_0(1 - q_0)(1 - q_0^2)} = \frac{512}{51\sqrt{17} - 107}$$

$$= 4.95747480\dots = c_1 \quad (\text{say}), \quad (59)$$

$$h''(z_0) = -192.04135\dots = -\alpha \quad (\text{say}). \quad (60)$$

In fact $h(z)$ has a saddle point at z_0 , and we choose $P = \{ \theta + iy_0 : -\frac{1}{2} < \theta \leq \frac{1}{2} \}$. We divide P into three sections: $-\frac{1}{2} < \theta \leq -\sqrt{\log l/\sqrt{l}}$, $-\sqrt{\log l/\sqrt{l}} < \theta \leq \sqrt{\log l/\sqrt{l}}$, $\sqrt{\log l/\sqrt{l}} < \theta \leq \frac{1}{2}$, and denote the corresponding integrals in (58) by I_L, I_M, I_R respectively.

Then, for $l \geq 300$,

$$I_M \geq 2g(z_0) \int_0^{\sqrt{\log l/\sqrt{l}}} \exp \left\{ l \left[h(z_0) - \frac{\alpha}{2} \theta^2 - \frac{\beta}{6} \theta^3 \right] \right\} d\theta,$$

where

$$\beta = \max \left\{ |h'''(z)| : z = \theta + iy_0, \quad |\theta| \leq \sqrt{\frac{\log 300}{300}} \right\}.$$

By computer we find that $\beta = 1503.9\dots$. Therefore

$$I_M \geq 0.7192\dots c_1^l I_M',$$

where

$$I'_M = 2 \int_0^{\sqrt{\log l}/\sqrt{l}} e^{-l \left[\frac{\alpha}{2} \theta^2 + \frac{\beta}{6} \theta^3 \right]} d\theta .$$

We set $\theta = t/\sqrt{\alpha l}$, obtaining

$$I'_M \geq \frac{2}{\sqrt{\alpha l}} \int_0^{\sqrt{\alpha \log l}} e^{-\frac{t^2}{2} - \frac{\gamma}{\sqrt{l}} t^3} dt$$

where $\gamma = \beta/(6\alpha^{3/2}) = 0.09418\dots$

$$= \frac{2}{\sqrt{\alpha l}} \left[\int_0^{\infty} - \int_{\sqrt{\alpha \log l}}^{\infty} \right] e^{-\frac{t^2}{2} - \frac{\gamma}{\sqrt{l}} t^3} dt . \quad (61)$$

The first term in (61) is

$$\geq \frac{2}{\sqrt{\alpha l}} \int_0^1 e^{-\frac{t^2}{2} - c_2 t^3} dt ,$$

where $c_2 = \gamma/\sqrt{300} = 0.0054\dots$,

$$\geq \frac{2}{\sqrt{\alpha l}} \int_0^1 e^{-c_3 t^2} dt , \quad c_3 = \frac{1}{2} + c_2 = 0.5054\dots$$

$$= \sqrt{\frac{\pi}{c_3 \alpha l}} \operatorname{erf}(\sqrt{c_3}) = \frac{0.123\dots}{\sqrt{l}} .$$

The second term in (61) is easily shown to be negligible (less than 10^{-470} in fact) for $l \geq 300$.

Thus

$$I_M \geq \frac{0.0885\dots c_1^l}{\sqrt{l}} , \quad \text{for } l \geq 300 .$$

In evaluating the next integral we make use of the inequality

$$\cos x < 1 - \frac{c}{2} x^2, \quad \text{for } 0 < x < a, \quad (62)$$

where

$$c = \left[\frac{\sin \frac{a}{2}}{\frac{a}{2}} \right]^2.$$

We omit the easy proof.

The contribution to b_l from the right-hand section of the path is

$$I_R \geq \frac{1}{1-q_0} \int_{\sqrt{\log l}/\sqrt{l}}^{\frac{1}{2}} \left\{ \frac{e^{-2\pi i\theta}}{q_0(1-q_0 e^{2\pi i\theta})(1-q_0 e^{4\pi i\theta})} \right\}^l d\theta.$$

Let

$$\begin{aligned} D &= \left| (1-q_0 e^{2\pi i\theta})(1-q_0 e^{4\pi i\theta}) \right|^2 \\ &\geq \left| (1-q_0 e^{2\pi i\varepsilon})(1-q_0 e^{4\pi i\varepsilon}) \right|^2 \end{aligned}$$

in the range of the integral, where $\varepsilon = \sqrt{\log l}/\sqrt{l}$, and so

$$D \geq (1+q_0^2 - 2q_0 \cos 2\pi\varepsilon)((1+q_0)^2 - 4q_0 \cos^2 2\pi\varepsilon).$$

Regarded as a cubic polynomial in $\cos 2\pi\varepsilon$, this expression has negative slope near 1, and so we obtain a lower bound to it (from (62)) by replacing $\cos 2\pi\varepsilon$ by

$$1 - \frac{c_4}{2} \frac{\log l}{l}$$

where

$$c_4 = \left[\frac{\sin \frac{\pi \sqrt{\log 300}}{\sqrt{300}}}{\frac{\pi \sqrt{\log 300}}{\sqrt{300}}} \right]^2 = 0.9390\dots$$

After some further simplifications we obtain

$$D \geq 0.2670\dots \left[1 + \frac{70 \log l}{l} \right].$$

Therefore, for $l \geq 300$,

$$I_r \geq \frac{1}{1-q_0} \left[1 + \frac{70 \log l}{l} \right]^{-1/2} (4.95747480\dots)^l \int_{\frac{\sqrt{\log l}}{\sqrt{l}}}^{\frac{1}{2}} e^{-2\pi i \theta} d\theta \geq \frac{c_1^l}{l^{34}}.$$

The same bound applies to I_L . These terms are negligible compared with I_M , and we conclude that

$$b_l \geq \frac{0.0885\dots c_1^l}{\sqrt{l}}, \quad l \geq 300, \quad (63)$$

where c_1 is given by (59).

On the other hand (57) implies

$$|b_l| < \frac{20}{9} 2^{4a} \left[\frac{9a}{a} \right] \leq \frac{5}{3 \sqrt{\pi a}} 2^{4a+9aH_2(1/9)},$$

from [28, p. 309], where $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$, and so

$$|b_l| < \frac{1.8806\dots c_5^l}{\sqrt{l}}, \quad (64)$$

where

$$c_5 = 2^{1+(9/4)H_2(1/9)} = 4.38425361\dots$$

It is easy to verify that the two bounds (63) and (64) are incompatible for $l \geq 300$. This

completes the proof of Theorem 1.

Acknowledgements. We thank A. M. Odlyzko for helpful suggestions concerning the proof of Theorem 1, A. R. Calderbank, W. C. Huffman and H. Janwa for useful discussions, and V. Pless for comments on an earlier draft of this paper.

References

- [1] G. F. M. Beenker, "On double circulant codes", Report 80-WSK-04, Mathematics Dept., Technological Univ. Eindhoven, Eindhoven, Netherlands, July 1980.
- [2] E. R. Berlekamp, F. J. MacWilliams and N. J. A. Sloane, "Gleason's theorem on self-dual codes", IEEE Trans. Info. Theory, vol. 18 (1972), pp. 409-414.
- [3] V. K. Bhargava and C. Nguyen, "Circulant codes based on the prime 29", IEEE Trans. Info. Theory, vol. 26 (1980), pp. 363-364.
- [4] V. K. Bhargava and J. M. Stein, " (v, k, d) configurations and self dual codes", Inform. Control, vol. 28 (1975), pp. 352-355.
- [5] V. K. Bhargava, G. Young and A. K. Bhargava, "A characterization of a $(56, 28)$ extremal self-dual code", IEEE Trans. Info. Theory, vol. 27 (1981), pp. 258-260.
- [6] A. Blokhuis and A. R. Calderbank, personal communication.
- [7] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, "A new table of constant weight codes", IEEE Trans. Info. Theory, to appear.
- [8] N. G. de Bruijn, "Asymptotic Methods in Analysis", North-Holland, Amsterdam, 3rd edition, 1970.
- [9] F. C. Bussemaker and V. D. Tonchev, "New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28", Discrete Math., vol. 76 (1989), pp. 45-49.
- [10]
- [11] J. H. Conway and V. Pless, "On the enumeration of self-dual codes", J. Combinatorial Theory, vol. A **28** (1980), pp. 26-53.

- [12] J. H. Conway, V. Pless and N. J. A. Sloane, "Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16", IEEE Trans. Info. Theory, vol. 25 (1979), pp. 312-322.
- [13] J. H. Conway, V. Pless and N. J. A. Sloane, "The binary self-dual code of length up to 32: a revised enumeration", J. Combin Theory, Series A, vol. 60 (1992), 183-195.
- [14] J. H. Conway and N. J. A. Sloane, "Sphere Packings, Lattices and Groups", Springer-Verlag, NY, 2nd edition, 1993.
- [15] J. H. Conway and N. J. A. Sloane, "A new upper bound for the minimum of an integral lattice of determinant one", Bull. Amer. Math. Soc., vol. 23 (1990), 383-387.
- [16] J. H. Conway and N. J. A. Sloane, "On the minimum of unimodular lattices I: Upper bounds", in preparation.
- [17] J. H. Conway and N. J. A. Sloane, "On the minimum of unimodular lattices II: Lower bounds", in preparation.
- [17a] R. Dougherty and H. Janwa, "Covering radius computations for binary cyclic codes", Math. Comp., submitted.
- [18] A. M. Gleason, "Weight polynomials of codes and the MacWilliams identities", Actes Congrès Intern. de Math., Gauthier-Villars, Paris, 1971, vol. 3, pp. 211-215.
- [19] P. Henrici, "Applied and Computational Complex Analysis", Wiley, NY 1974, vol. 1.
- [20] W. C. Huffman, "Automorphisms of codes with applications to extremal doubly-even codes of length 48", IEEE Trans. Info. Theory, vol. 28 (1982), pp. 511-521.
- [21] W. C. Huffman and V. I. Yorgov, "A $[72,36,16]$ doubly even code does not have an automorphism of order 11", IEEE Trans. Info. Theory, vol. 33 (1987), pp. 749-752.
- [22] M. Karlin, "New binary coding results by circulants", IEEE Trans. Info. Theory, vol. 15

(1969), pp. 81-92.

- [23] M. Kneser, "Klassenzahlen definiter quadratischer Formen", *Archiv Math.*, vol. 8 (1957), pp. 241-250.
- [24] H. V. Koch, "On self-dual, doubly-even codes of length 32", Report P-Math-32/84, Institut für Mathematik, Akademie der Wissenschaften der DDR, Berlin, 1984.
- [25] H. Koch, "Unimodular lattices and self-dual codes", in "Proc. Intern. Congress Math., Berkeley 1986", Amer. Math. Soc., Providence RI, 1987, vol. 1, pp. 457-465.
- [26] H. Koch and B. B. Venkov, "Ueber ganzzahlige unimodulare euklidische Gitter", *J. Reine Angew. Math.*, vol. 398 (1989), pp. 144-168.
- [27] J. S. Leon, J. M. Masley and V. Pless, "Duadic codes", *IEEE Trans. Info. Theory*, vol. 30 (1984), pp. 709-714.
- [28] J. S. Leon, V. Pless and N. J. A. Sloane, "On ternary self-dual codes of length 24", *IEEE Trans. Info. Theory*, vol. 27 (1981), pp. 176-180.
- [29] F. J. MacWilliams, "Orthogonal circulant matrices over finite fields, and how to find them", *J. Comb. Theory*, vol. 10 (1971), pp. 1-17.
- [30] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane, "Generalizations of Gleason's theorem on weight enumerators of self-dual codes", *IEEE Trans. Info. Theory*, vol. 18 (1972), pp. 794-805.
- [31] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, Amsterdam, 1977.
- [32] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson, "Good self-dual codes exist", *Discrete Math.*, vol. 3 (1972), pp. 153-162.

- [33] C. L. Mallows, A. M. Odlyzko and N. J. A. Sloane, “Upper bounds for modular forms, lattices, and codes”, *J. Alg.*, vol. 36 (1975), pp. 68-76.
- [34] C. L. Mallows and N. J. A. Sloane, “An upper bound for self-dual codes”, *Information and Control*, vol. 22 (1973), pp. 188-200.
- [35] Mathlab Group, “MACSYMA Reference Manual”, Laboratory for Computer Science, M.I.T., Cambridge, MA, version 10, 1983.
- [36] R. J. McEliece, personal communication.
- [37] R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr. and L. R. Welch, “New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities”, *IEEE Trans. Info. Theory*, vol. 23 (1977), pp. 157-166.
- [37a] B. D. McKay, “NAUTY User’s Guide (Version 1.2)”, Dept. Computer Science Technical Report TR-CS-87-03, Australian National University, Canberra, Australia, 1987.
- [37b] H. Oral and K. T. Phelps, “Almost all self-dual codes are rigid”, preprint.
- [38] M. Ozeki, “Hadamard matrices and doubly-even self-dual error-correcting codes”, *J. Comb. Theory*, vol. A 44 (1987), pp. 274-287.
- [39] M. Ozeki, “Examples of even unimodular extremal lattices of rank 40 and their Siegel theta series of degree 2”, *J. Number Theory*, vol. 28 (1988), pp. 119-131.
- [40] G. Pasquier, “A binary extremal doubly even self-dual code (64,32,12) obtained from an extended Reed-Solomon code over F_{16} ”, *IEEE Trans. Info. Theory*, vol. 27 (1981), pp. 807-808.
- [41] G. Pasquier, “Projections et images binaires de codes sur F_{2^m} ”, *Rev. CETHEDDEC Cahier*, (no. 2, 1981), pp. 45-56.

- [42] G. Pasquier, "Binary images of some self-dual codes over $GF(2^m)$ with respect to trace-orthogonal basis", *Discrete Math.*, vol. 37 (1981), pp. 127-129.
- [43] V. Pless, "On the uniqueness of the Golay codes", *J. Comb. Theory*, vol. 5 (1968), pp. 215-228.
- [44] V. Pless, "A classification of self-orthogonal codes over $GF(2)$ ", *Discrete Math.*, vol. 3 (1972), pp. 209-246.
- [45] V. Pless, "The children of the (32, 16) doubly even codes", *IEEE Trans. Info. Theory*, vol. 24 (1982), pp. 738-746.
- [46] V. Pless, "Extremal codes are homogeneous", preprint.
- [47] V. Pless, J. M. Masley and J. S. Leon, "On weights in duadic codes", *J. Comb. Theory*, vol. A 44 (1987), pp. 6-21.
- [48] V. Pless and N. J. A. Sloane, "On the classification and enumeration of self-dual codes", *J. Comb. Theory*, vol. A 18 (1975), pp. 313-335.
- [49] A. Poli and C. Rigoni, "Enumeration of self-dual $2k$ circulant codes", *Lect. Notes. Comp. Sci.*, vol. 228 (1986), pp. 61-70.
- [50] N. J. A. Sloane, "Is there a (72, 36) $d=16$ self-dual code?", *IEEE Trans. Info. Theory*, vol. 19 (1973), p. 251.
- [51] N. J. A. Sloane, "Weight enumerators of codes", in "Combinatorics", ed. M. Hall, Jr. and J. H. van Lint, Reidel, Dordrecht, Holland, 1975, pp. 115-142.
- [52] N. J. A. Sloane, "Binary codes, lattices and sphere packings", in "Combinatorial Surveys", edited P. J. Cameron, Academic Press, NY, 1977, pp. 117-164.
- [53] N. J. A. Sloane, "Error-correcting codes and invariant theory: new applications of a

- nineteenth-century technique'', Amer. Math. Monthly, vol. **84** (1977), pp. 82-107.
- [54] N. J. A. Sloane, "Self-dual codes and lattices'', Proc. Symp. Pure Math., vol. 34 (1979), pp. 273-308.
- [54a] N. J. A. Sloane and J. G. Thompson, "Cyclic self-dual codes'', IEEE Trans. Info. Theory, vol. 29 (1983), pp. 364-366.
- [55] T. A. Springer, "Regular elements of finite reflection groups'', Invent. Math., vol. 25 (1974), pp. 159-198.
- [56] R. P. Stanley, "Relative invariants of finite groups generated by pseudoreflections'', J. Algebra, vol. 49 (1977), pp. 134-148.
- [57] V. D. Tonchev, "Inequivalence of certain extremal self-dual codes'', Compt. Rend. Acad. Bulg. Sci., vol. 36 (1983), pp. 181-184.
- [58] V. D. Tonchev, "Hadamard-type block designs and self-dual codes'' (in Russian), Problemy Peredachi Inform., vol. 19 (no. 4, 1983), pp. 25-30. English translation in Problems of Information Transmission, vol. 19 (1983), pp. 270-274.
- [59] V. D. Tonchev, "Symmetric designs without ovals and extremal self-dual codes'', in "Combinatorics '86'', North-Holland, Amsterdam, 1988, pp. 451-457.
- [60] V. D. Tonchev, "Self-orthogonal designs and extremal doubly even codes'', J. Comb. Theory, vol. A 52 (1989), pp. 197-205.
- [61] V. D. Tonchev, "Self-orthogonal designs'', Contemp. Math., to appear.
- [62] V. D. Tonchev and R. V. Raev, "Cyclic 2-(17,8,7) designs and related doubly even codes'', Compt. Rend. Acad. Bulg. Sci., vol. 35 (no. 10, 1982).
- [63] M. Ventou and C. Rigoni, "Self-dual doubly circulant codes'', Discrete Math., vol. 56

- (1985), pp. 291-298.
- [64] H. N. Ward, "A restriction on the weight enumerator of a self-dual code", *J. Comb. Theory*, vol. A **21** (1976), pp. 253-255.
- [65] E. T. Whittaker and G. N. Watson, "A Course of Modern Analysis", 4th ed., Cambridge Univ. Press, 1963.
- [66] J. Wolfmann, "A class of doubly even self dual binary codes", *Discrete Math.*, vol. 56 (1985), pp. 299-303.
- [67] J. Wolfmann, "A group algebra construction of binary even self dual codes", *Discrete Math.*, vol. 65 (1987), pp. 81-89.
- [68] V. Y. Yorgov, "Binary self-dual codes with automorphisms of odd order" (in Russian), *Prob. Pered. Inform.*, vol. 19 (no. 4, 1983), pp. 11-24. English translation in *Problems Info. Transmission*, vol. 19 (1983), pp. 260-270.
- [69] V. Y. Yorgov, "Extremality of self-dual doubly even codes of length 56" (in Bulgarian), in "Mathematics and Education", *Bulgarian Acad. Sci.*, 1987, pp. 435-439.
- [70] V. Y. Yorgov, "A method for constructing inequivalent self-dual codes with applications to length 56", *IEEE Trans. Info. Theory*, vol. 33 (1987), pp. 77-82.
- [71] V. Y. Yorgov, "Doubly-even extremal codes of length 64" (in Russian), *Prob. Pered. Inform.*, vol. 22 (no. 4, 1986), pp. 35-42. English translation in *Problems Info. Transmission*, vol. 22 (1986), pp. 277-284.
- [72] V. Y. Yorgov, "On the extremal doubly-even codes of length 32", *Proceedings Fourth Joint Swedish-Soviet International Workshop on Information Theory*, Gotland, Sweden, 1989, pp. 275-279.

- [73] V. Y. Yorgov and N. P. Ziapkov, “Extremal codes of length 40 and automorphism of order 5”, preprint.

List of Footnotes

- (1) On p. 629 of [31] this is incorrectly stated as $d \leq 0.178n + o(n)$.
- (2) $A(n, d, w)$ denotes the maximal possible number of binary vectors of length n , weight w and Hamming distance at least d apart [7], [31].
- (3) Indeed, the code described in [3] has generator matrix of the form given in Eq. (41) below, where the first row of R is 19E89179 in hexadecimal, and is not self-dual.
- (4) Unlike other codes in this section, this does not necessarily have the highest possible d (cf. Table I).
- (5) In retrospect it is clear that a much smaller value than 3000 would suffice.

A New Upper Bound on the Minimal Distance of Self-Dual Codes*

J. H. Conway

Mathematics Department
Princeton University
Princeton, New Jersey 08540

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

It is shown that the minimal distance d of a binary self-dual code of length $n \geq 74$ is at most $2\lfloor(n+6)/10\rfloor$. This bound is a consequence of some new conditions on the weight enumerator of a self-dual code obtained by considering a particular translate of the code called its ‘‘shadow’’. These conditions also enable us to find the highest possible minimal distance of a self-dual code for all $n \leq 60$; to show that self-dual codes with $d \geq 6$ exist precisely for $n \geq 22$, with $d \geq 8$ exist precisely for $n = 24, 32$ and $n \geq 36$, and with $d \geq 10$ exist precisely for $n \geq 46$; and to show that there are exactly eight self-dual codes of length 32 with $d = 8$. Several of the self-dual codes of length 34 have a trivial group (this appears to be the smallest length where this can happen).

* This paper appeared in *IEEE Trans. Inform. Theory*, vol. **36** (Nov. 1990), pp. 1319-1333.