Shadow Bounds for Self-Dual Codes

Eric M. Rains

***Abstract*—Conway and Sloane have previously given an upper bound on the minimum distance of a singly-even self-dual binary code, using the concept of the shadow of a self-dual code. We improve their bound, finding that the minimum distance of a self-dual binary code of length n is at most $4\lfloor n/24 \rfloor + 4$, except when $n \bmod 24 = 22$, when the bound is $4\lfloor n/24 \rfloor + 6$. We also show that a code of length a multiple of 24 meeting the bound cannot be singly-even. The same technique gives similar results for additive codes over GF (4) (relevant to quantum coding theory).**

***Index Terms*—Bound, self-dual code, shadow, singly-even.**

I. Introduction

In [5], the following was shown:

Theorem: If a doubly-even self-dual $[n, n/2, d]$ exists, then $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$.

The objective of the present work is to remove the restriction that the code be doubly-even. For singly-even codes, much less has hitherto been known; a direct extension of the proof in [5] gives a bound $d \leq 2\lfloor \frac{n}{8} \rfloor + 2$, but this bound is almost never met. The situation was improved greatly by [2], which gives a bound $d \leq 2\lfloor \frac{n+6}{10} \rfloor$, except when n is $2, 12, 22$, or 32; a further improvement appears in [7], which gives the bound $d \leq (n/6) + 2 + (2/3)\log_2(n)$. This is still higher than the bound for doubly-even codes, however. In the sequel, a new bound is proved, of the form

$$d \leq 4\lfloor \frac{n}{24} \rfloor + 4$$

except when $n \bmod 24 = 22$, when

$$d \leq 4\lfloor \frac{n}{24} \rfloor + 6.$$

In particular, whenever n is a multiple of 8, so both singly-even and doubly-even codes exist, we now have the same bound for singly-even and doubly-even codes. In fact, when n is a multiple of 24, it can be shown that any code meeting the bound must be doubly-even.

As the present bound is shown using linear programming, it is natural to inquire how much weaker it is than the full LP bound. Using a high-precision LP package (the author used `maple`), one can readily verify that for all n in the range $8 \leq n \leq 200$, there exists a feasible weight enumerator (including the constraints from the shadow enumerator (see below)) meeting the bound. In some cases, the present bound can be improved upon using *integer* programming, however.

The key idea in the proof is the use of additional constraints coming from the "shadow" of the code [2]. It turns out that this concept has a natural analog in the case of additive codes over GF (4); that is, GF (2)-linear subsets of GF $(4)^n$, self-orthogonal (i.e., contained in its dual) under the inner product

$$\langle v, w \rangle = \sum_i \mathrm{Tr}\,(v_i^2 w_i).$$

These codes appear, for instance, in the theory of quantum error-correcting codes [1]. For these codes, we give a bound $2\lfloor \frac{n}{6} \rfloor + 2$, or $2\lfloor \frac{n}{6} \rfloor + 3$ when $n \bmod 6 = 5$. We also give a result bounding the minimum weight of $C^\perp - C$ when C is a self-orthogonal additive code.

A quick note on notation: We will use the notation $[n, k, d]_4$ to refer to an additive code over GF (4); k will be its dimension as a vector space over GF (2). In particular, a self-dual code will have $k = n$.

Manuscript received January 21, 1997; revised June 20, 1997.

The author is with AT&T Labs–Research, Florham Park, NJ 07932-0971 USA.

Publisher Item Identifier S 0018-9448(98)00087-X.

II. Shadows

Let C be a self-orthogonal binary code. From the congruence

$$\mathrm{wt}\,(v+w) - \mathrm{wt}\,(v) - \mathrm{wt}\,(w) \equiv 2\langle v, w \rangle \equiv 0 \pmod 4$$

it follows that the subset of C consisting of elements of weight a multiple of 4 forms a subspace C_0 of C. If C is doubly-even, then $C_0 = C$, and we define the shadow $S(C) = C^\perp$. Otherwise, we define $S(C) = C_0^\perp - C^\perp$. Equivalently, $S(C)$ is the set of vectors w such that

$$2\langle w, v \rangle \equiv \mathrm{wt}(v) \pmod 4$$

for all $v \in C$.

Theorem 1: Let $A(x, y)$ be the weight enumerator of C, and let $S(x, y)$ be the weight enumerator of $S(C)$. Then

$$S(x, y) = \frac{1}{|C|} A(x+y, i(x-y)).$$

Proof: See [2, Theorem 6, in particular, eq. (23)]. Note that [2] considers codes containing their duals, rather than codes contained in their duals; thus one should exchange C and $C^\perp$ throughout. □

Similarly, let C be an additive code over GF (4), self-orthogonal under the above inner product. One can readily verify that

$$\mathrm{wt}\,(v+w) - \mathrm{wt}\,(v) - \mathrm{wt}\,(w) \equiv \langle v, w \rangle \equiv 0 \bmod 2$$

so as above, the subset C_0 of even codewords in C is a subgroup; defining $S(C)$ as above, or equivalently, as the set of vectors w such that

$$\langle v, w \rangle \equiv \mathrm{wt}\,(v) \bmod 2$$

for all $v \in C$, we have

Theorem 2: Let $A(x,y)$ be the weight enumerator of C, and let $S(x,y)$ be the weight enumerator of $S(C)$. Then

$$S(x,y) = \frac{1}{|C|}A(x+3y, y-x).$$

Proof: Completely analogous. $\square$

For self-dual codes, the weight enumerators have a special form, which carries over to the shadow enumerator

Theorem 3: Let $A(x,y)$ and $S(x,y)$ be, respectively, the enumerator of a self-dual binary code of length n and that of its shadow. Then there exist coefficients $c_i, 0 \le i \le \lfloor \frac{n}{8} \rfloor$, such that

$$A(x,y) = \sum_{0\le i\le \lfloor n/8\rfloor} c_i (x^2+y^2)^{n/2-4i}\{x^2y^2(x^2-y^2)^2\}^i$$
$$S(x,y) = \sum_{0\le i\le \lfloor n/8\rfloor} (-1)^i c_i 2^{n/2-6i}(xy)^{n/2-4i}(x^4-y^4)^{2i}.$$

Proof: This is part 4 of [2, Theorem 5]. $\square$

Analogously, we have

Theorem 4: Let $A(x,y)$ and $S(x,y)$ be, respectively, the enumerator of a self-dual additive code over GF(4) of length n and that of its shadow. Then there exist coefficients $c_i, 0 \le i \le \lfloor \frac{n}{2} \rfloor$, such that

$$A(x,y) = \sum_{0\le i\le \lfloor n/2\rfloor} c_i (x+y)^{n-2i}(y(x-y))^i$$
$$S(x,y) = \sum_{0\le i\le \lfloor n/2\rfloor} (-1)^i 2^{n-3i} c_i y^{n-2i}(x^2-y^2)^i.$$

Proof: Analogous. $\square$

In each case, we prove our bound by expressing an appropriately chosen c_i both as a linear combination of the initial coefficients of the weight enumerator and as a linear combination of the initial coefficients of the shadow enumerator. All but one of the terms in the first linear combination will be 0, based on the putative minimum distance; consequently, the first linear combination reduces to an explicit constant. All coefficients in the second linear combination will turn out to have the same sign, a sign inconsistent with the sign of c_i.

III. Binary Codes

Let C be a self-dual binary code, with shadow S; let $A(x,y)$ and $S(x,y)$ be the respective weight enumerators. Write, as in Theorem 3,

$$\begin{aligned} A(1,y) &= \sum_{0\le j\le \lfloor n/2\rfloor} a_j y^{2j} \\ &= \sum_{0\le i\le \lfloor n/8\rfloor} c_i (1+y^2)^{n/2-4i}(y^2(1-y^2)^2)^i \\ S(1,y) &= \sum_{0\le j\le 2\lfloor n/8\rfloor} b_j y^{4j+t} \\ &= \sum_{0\le i\le \lfloor n/8\rfloor} (-1)^i c_i 2^{n/2-6i} y^{n/2-4i}(1-y^4)^{2i} \end{aligned}$$

where $t = (n/2 \bmod 4)$. Note that $a_0 = 1$, and all a_j and b_j must be nonnegative integers. Also, one can write c_i as a linear combination of the a_j for $0 \le j \le i$, and as a linear combination of the b_j for $0 \le j \le \lfloor n/8 \rfloor - i$.

Define $\alpha_i(n)$ to be the coefficient of a_0 in the expansion of c_i in terms of a_j for $0 \le j \le i$, and define $\beta_{ij}(n)$ to be the coefficient of b_j in the expansion of c_i in terms of b_j for $0 \le j \le \lfloor n/8 \rfloor - i$. Then, except in extreme cases, we will see that $\alpha_i(n) < 0$ for suitably chosen i, while $\beta_{ij}(n) > 0$ for the same i and $0 \le j \le \lfloor n/8 \rfloor - i$. Thus we need to compute $\alpha_i(n)$ and $\beta_{ij}(n)$ at strategically chosen points.

First, $\alpha_i(n)$. For $i > 0$

$$\alpha_i(n) = -\frac{n}{2i}[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-(n/2)-1+4i}(1-y)^{-2i}].$$

This is [2, eq. (48)], and follows from the Bürmann–Lagrange theorem:

Theorem (Bürmann–Lagrange): Let $f(x)$ and $g(x)$ be formal power series, with $g(0)=0$, and $g'(0) \ne 0$. If coefficients κ_{ij} are defined by

$$x^j f(x) = \sum_{0\le i} \kappa_{ij} g(x)^i$$

then

$$\kappa_{ij} = \frac{1}{i}\left[\text{coeff. of } x^{i-1} \text{ in } [jx^{j-1}f(x) + x^j f'(x)]\left(\frac{x}{g(x)}\right)^i\right].$$

Proof: See [8, ch. 7]. $\square$

In particular, for $l \ge 1$, we have

$$\begin{aligned} \alpha_{2m}(24m-2l) &= -\frac{12m-l}{2m}[\text{coeff. of } y^{2m-1} \text{ in } \\ &\qquad (1+y)^{-4m+l-1}(1-y)^{-4m}] \\ &= -\frac{12m-l}{2m}[\text{coeff. of } y^{2m-1} \text{ in } \\ &\qquad (1+y)^{l-1}(1-y^2)^{-4m}] \\ &= -\frac{12m-l}{2m}\sum_{\substack{1\le k\le l-1\\ k \bmod 2=1}} \\ &\qquad \binom{l-1}{k}\binom{(10m-k-3)/2}{4m-1}. \end{aligned}$$

For $1 \le l \le 13$ and $m \ge 2$, each term in the sum is nonnegative, so we can conclude that $\alpha_{2m}(24m-2l) \le 0$, with equality only when $l=1$. Similarly, $\alpha_{2m+1}(24m-2) < 0$ (we need this to handle $n \bmod 24 \equiv 22$).

We will need two more values of α to handle the case $n \bmod 24 = 0$ (i.e., to show that a self-dual $[24m, 12m, 4m+4]$ must be doubly-even):

$$\begin{aligned} \alpha_{2m}(24m) &= -6[\text{coeff. of } y^{2m-1} \text{ in } \\ &\qquad (1+y)^{-4m-1}(1-y)^{-4m}] \\ &= -6[\text{coeff. of } y^{2m-1} \text{ in } (1-y)(1-y^2)^{-4m-1}] \\ &= 6[\text{coeff. of } z^{m-1} \text{ in } (1-z)^{-4m-1}] \\ &= 6(-1)^{m-1}\binom{-4m-1}{m-1} \\ &= \frac{6}{5}\binom{5m}{m} \end{aligned}$$

and

$$\begin{aligned}\alpha_{2m+1}(24m) &= -\frac{12m}{2m+1}[\text{coeff. of } y^{2m} \text{ in} \\ &\qquad (1+y)^{-4m+3}(1-y)^{-4m-2}] \\ &= -\frac{12m}{2m+1}[\text{coeff of } y^{2m} \text{ in} \\ &\qquad (1+y)^5(1-y^2)^{-4m-2}] \\ &= -\frac{12m}{2m+1}\sum_{0\le k\le 2}\binom{5}{2k}(-1)^{m-k} \\ &\qquad \cdot \binom{-4m-2}{m-k} \\ &= -192\frac{m^2}{(2m+1)(4m+1)}\binom{5m}{m}.\end{aligned}$$

It will turn out that

$$\alpha_{2m}(24m) = \beta_{(2m)0}(24m)$$

and

$$\alpha_{2m+1}(24m) = \beta_{(2m+1)0}(24m).$$

A similar Bürmann–Lagrange calculation gives a formula for $\beta_{ij}(n)$

$$\beta_{ij} = (-1)^i 2^{-n/2+6i}\frac{k-j}{i}\binom{k+i-j-1}{k-i-j}$$

valid for $i > 0$, where $k = \lfloor n/8 \rfloor$. Note, in particular, that $(-1)^i\beta_{ij} > 0$ for $0 \le j \le k-i$. The details are omitted for conciseness; the calculation is essentially that in [2], except for an error in [2, eq. (55)] (the second term should be added, not subtracted).

We can now prove

Theorem 5: If a self-dual $[24m+2l, 12m+l, d]$ exists, with $0 \le l \le 11$, then

$$d \le \begin{cases} 4m+4, & l < 11 \\ 4m+6, & l = 11. \end{cases}$$

If a self-dual $[24m+22, 12m+11, 4m+6]$ exists, then so does a doubly-even self-dual $[24m+24, 12m+12, 4m+8]$. Finally, any self-dual $[24m, 12m, 4m+4]$ must be doubly-even.

Proof: We first show that $d \le 4m+4$ for $0 \le l < 11$. Suppose, on the contrary, that $d > 4m+4$. Consider c_{2m+2}. On the one hand, c_{2m+2} is $\alpha_{2m+2}(n)$ plus a linear combination of the a_i for $1 \le i \le 2m+2$; since these are all 0, we have

$$c_{2m+2} = \alpha_{2(m+1)}(24(m+1) - 2(12-l)) < 0.$$

On the other hand,

$$c_{2m+2} = \sum_j \beta_{(2m+2)j} b_j.$$

But $\beta_{(2m+2)j} b_j$ is nonnegative for all j. So $c_{2m+2} \ge 0$, a contradiction.

Now, consider a self-dual $[24m+22, 12m+11, 4m+6]$. In this case, we have

$$\sum_{0\le j\le m} \beta_{(2m+2)j} b_j = c_{2m+2} = \alpha_{2(m+1)}(24(m+1)-2) = 0.$$

But then $b_j = 0$ for $0 \le j \le m$. In other words, the shadow code must have minimum weight $4m+6$ as well. Letting $C^{(i)}$ for $0 \le i \le 3$ be the four cosets of the even subcode $C^{(0)}$ in its dual, we can construct an even self-dual $[24m+24, 12m+12, 4m+8]$ as the set of all vectors of one of the following four forms: $(0,0)|v$, for $v \in C^{(0)}$, $(0,1)|v$, for $v \in C^{(1)}$, $(1,0)|v$, for $v \in C^{(3)}$, or $(1,1)|v$, for $v \in C^{(2)}$. (This construction is given in [4].)

The possibility of a self-dual $[24m+22, 12m+11, 4m+8]$ can be eliminated by remarking that c_{2m+3} is a linear combination of b_j for $0 \le j < m$, so must be 0, but

$$c_{2m+3} = \alpha_{2(m+1)+1}(24(m+1)-2) < 0.$$

Finally, consider a putative $[24m, 12m, 4m+4]$. Consider

$$F = \alpha_{2m+1}(24m)c_{2m} - \alpha_{2m}(24m)c_{2m+1}.$$

Since

$$\alpha_{2m+1}(24m) = \beta_{(2m+1)0}(24m)$$

and

$$\alpha_{2m}(24m) = \beta_{(2m)0}(24m)$$

F is a linear combination of a_1 through a_{2m+1}, so must be 0. On the other hand, we have

$$\begin{aligned}F &= \alpha_{2m+1}(24m)c_{2m} - \alpha_{2m}(24m)c_{2m+1} \\ &= \sum_{0\le j\le m} \beta_{(2m+1)0}\beta_{(2m)j}b_j - \beta_{(2m)0}\beta_{(2m+1)j}b_j \\ &= -\sum_{0\le j\le m} b_j\left(\frac{384}{5}\,\frac{j(3m-j)(6m-j)}{(2m+1)(4m+1)(5m-j)}\right. \\ &\qquad \left.\cdot\binom{5m}{m}\binom{5m-j}{m-j}\right).\end{aligned}$$

This is a negative linear combination of b_1 through b_m. In other words, b_1 through b_m must all be 0. But then

$$\beta_{(2m+1)0} = \alpha_{2m+1}(24m) = c_{2m+1} = \beta_{(2m+1)0}b_0$$

so $b_0 = 1$. But this can only happen if the code is doubly even. □

IV. Additive Codes Over GF(4)

Let C be a self-dual additive code over GF(4), with shadow S; let $A(x,y)$ and $S(x,y)$ be the respective weight enumerators. Write, as in Theorem 4,

$$\begin{aligned}A(1,y) &= \sum_{0\le j\le n} a_j y^j \\ &= \sum_{0\le i\le \lfloor n/2\rfloor} c_i(1+y)^{n-2i}(y(1-y))^i \\ S(1,y) &= \sum_{0\le j\le \lfloor n/2\rfloor} b_j y^{2j+t} \\ &= \sum_{0\le i\le \lfloor n/2\rfloor} (-1)^i 2^{n-3i} c_i y^{n-2i}(1-y^2)^i\end{aligned}$$

where $t = (n \bmod 2)$. As before, $a_0 = 1$, $0 \le a_j, b_j$, and c_i can be written either as a linear combination of the a_j

for $0 \le j \le i$, or as a linear combination of the b_j for $0 \le j \le \lfloor n/2 \rfloor - i$.

Define $\alpha_i(n)$ to be the coefficient of a_0 in c_i; define β_{ij} to be the coefficient of b_j in c_i. As above, we calculate

$$\alpha_{2m}(6m-l) = -\frac{6m-l}{2m} \sum_{\substack{1\le k\le l-1,2m-1 \\ k \bmod 2=1}} \binom{l-1}{k} \cdot \binom{(6m-k-3)/2}{2m-1}.$$

For $1 \le l \le 7$ and $m \ge 2$, or $1 \le l \le 5$ and $m \ge 1$, each term in the sum is nonnegative, so we can conclude that $\alpha_{2m}(6m-l) \le 0$, with equality only when $l = 1$. Similarly, $\alpha_{2m+1}(6m-1) < 0$.

Also

$$\alpha_{2m}(6m) = \binom{3m}{2m}$$

and

$$\alpha_{2m+1}(6m) = -8\binom{3m}{2m+1}.$$

Finally,

$$\beta_{ij}(n) = (-1)^i 2^{3i-n}\binom{k-j}{i}.$$

In particular,

$$\beta_{(2m+1)0}(6m) = \alpha_{2m+1}(6m), \beta_{(2m)0}(6m) = \alpha_{2m}(6m)$$

and

$$\alpha_{2m+1}\beta_{(2m)j} - \alpha_{2m}\beta_{(2m+1)j} = \frac{8mj}{(2m+1)(2m-j+1)}\binom{3m-j}{m}\binom{3m}{m} \ge 0$$

with equality only when $j = 0$.

We can now prove the following

Theorem 6: If a self-dual $[6m+l, 6m+l, d]_4$ exists, with $0 \le l \le 5$, then

$$d \le \begin{cases} 2m+2, & l < 5 \\ 2m+3, & l = 5. \end{cases}$$

If a self-dual $[6m+5, 6m+5, d]_4$ exists, then so does an even self-dual $[6m+6, 6m+6, d]_4$. Finally, any self-dual $[6m+6, 6m+6, d]_4$ must be even.

Proof: Proof as before. We need only give a construction of a $[6m+6, 6m+6, 2m+4]_4$ from a $[6m+5, 6m+5, 2m+3]_4$. Letting $C^{(i)}$ for $0 \le i \le 3$ be the four cosets of the even subcode $C^{(0)}$ in its dual, we can construct an even self-dual $[6m+6, 6m+6, 2m+4]_4$ as the set of all vectors of one of the following forms: $0|v$, for $v \in C^{(0)}$, $1|v$, for $v \in C^{(1)}$, $\omega|v$, for $v \in C^{(2)}$, and $\omega^2|v$, for $v \in C^{(3)}$. □

V. Self-Orthogonal Additive Codes

For applications to quantum error-correcting codes, the objects of interest are additive codes C over GF(4), self-orthogonal under the trace-Hermitian inner product. In particular, we would like a bound on the minimum weight of $C^\perp - C$, given that C has length n and dimension $n - r < n$. (If $r = 0$, then $C^\perp - C$ is empty.) If we merely wanted a bound on the minimum distance of $C^\perp$, we could simply apply Theorem 6, since $C^\perp$ would contain some self-dual code; however, the problem as stated is not quite so simple.

Let $A(x,y), B(x,y)$, and $S(x,y)$ be the enumerators of $C, C^\perp$, and the shadow of C, respectively; then $B(x,y) - A(x,y)$ is the weight enumerator of $C^\perp - C$. Thus we need to find a nonnegative linear combination of the coefficients of $B(x,y) - A(x,y), A(x,y)$, and $S(x,y)$ that equals 0, producing a contradiction.

Note, first, that

$$B(x,y) = 2^r A((x+3y)/2, (x-y)/2)$$

so

$$\Delta(x,y) \triangleq A(x,y) - A\left(\frac{x+3y}{2}, \frac{x-y}{2}\right) = (1-2^{-r})A(x,y) - 2^{-r}(B(x,y) - A(x,y)).$$

In particular, since the first d coefficients of $B(x,y) - A(x,y)$ are 0 (by assumption), we have

$$\Delta(1,y) = (1-2^{-r})A(1,y) + O(y^d).$$

Note that

$$\Sigma(x,y) \triangleq 2^{r-1}\Delta\left(\frac{x+3y}{2}, \frac{y-x}{2}\right) = \frac{1}{2}(S(x,y) - S(-x,y))$$

so $\Sigma(x,y)$ must have nonnegative coefficients.

What we will do, then, is produce a linear combination of the first d coefficients of $\Delta(1,y)$ that is also a linear combination of certain coefficients of $\Sigma(1,y)$; again, the signs will give a contradiction. The main reason we can do this is the following theorem (analogous to Theorems 3 and 4 above).

Theorem 7: Let $\Delta(x,y)$ and $\Sigma(x,y)$ be as above. Then there exist coefficients $e_i, 0 \le i \le \lfloor (n-1)/2 \rfloor$, such that

$$\Delta(x,y) = \sum_{0\le i\le\lfloor(n-1)/2\rfloor} e_i(x-3y)(x+y)^{n-1-2i}(y(x-y))^i$$

$$\Sigma(x,y) = \sum_{0\le i\le\lfloor(n-1)/2\rfloor} (-1)^i 2^{n-1+r-3i} e_i x y^{n-1-2i}(x^2-y^2)^i$$

Proof: Simply note that $\Delta(x,y)$ is taken to its negative by the MacWilliams transform

$$\Delta\left(\frac{x+3y}{2}, \frac{x-y}{2}\right) = -\Delta(x,y).$$

This follows from the fact that the substitution

$$(x,y) \mapsto \left(\frac{x+3y}{2}, \frac{x-y}{2}\right)$$

is self-inverse.

This forces $\Delta(x,y)$ to be in the ring

$$(x-3y)\mathbb{C}[x+y, y(x-y)].$$

One readily verifies that every element of this ring is anti-invariant under the MacWilliams transform; on the other hand, the Molien series of the ring of anti-invariants is $\frac{\lambda}{(1-\lambda)(1-\lambda^2)}$. Thus we have exhausted the space of anti-invariants.

The theorem follows immediately. □

As one might expect, the linear combination we use will be a suitably chosen e_i. Let us therefore write $n = 2k + t + 1$, with $t \in \{0,1\}$, and

$$\Delta(1,y) = \sum_{0\le i\le n} f_i y^i$$
$$\Sigma(1,y) = \sum_{0\le i\le k} g_i y^{2i+t}.$$

Let ϕ_{ij} be the coefficient of f_j in the expansion of e_i in terms of the f_j; similarly, let γ_{ij} be the coefficient of g_j in the expansion of e_i. Then we can compute ϕ_{ij} and γ_{ij} by applying the Bürmann–Lagrange theorem to the identities

$$y^j(1-3y)^{-1}(1+y)^{-n+1} = \sum_{0\le i\le k} \phi_{ij}\left(\frac{y(1-y)}{(1+y)^2}\right)^i + O(y^{k+1})$$

and

$$(-1)^k 2^{r+k-2-t} Y^j (1-Y)^{-k} = \sum_{0\le i\le k} \gamma_{(k-i)j}\left(\frac{-8Y}{(1-Y)}\right)^i + O(Y^{k+1})$$

where $Y = y^2$.

Before applying the Bürmann–Lagrange theorem, it will be helpful to restate the theorem slightly.

Lemma 8: Let $f(x)$ and $g(x)$ be formal power series, with $g(0) = 0$, and $g'(0) \neq 0$. If coefficients κ_{ij} are defined by

$$x^j f(x) = \sum_{0\le i} \kappa_{ij} g(x)^i$$

then

$$\kappa_{ij} = \left[\text{coeff. of } x^{i-j} \text{ in } \frac{xg'(x)}{g(x)} f(x)\left(\frac{x}{g(x)}\right)^i\right].$$

Proof: The Bürmann–Lagrange theorem, as stated above, tells us that

$$\kappa_{ij} = \frac{1}{i}\left[\text{coeff. of } x^{i-1} \text{ in } (jx^{j-1}f(x) + x^j f'(x))\left(\frac{x}{g(x)}\right)^i\right]$$
$$= \frac{1}{i}\left[\text{coeff. of } x^{i-j} \text{ in } \left(j + \frac{xf'(x)}{f(x)}\right) f(x)\left(\frac{x}{g(x)}\right)^i\right].$$

Now, for any function $h(x)$

$$[\text{coeff. of } x^{i-j} \text{ in } (i-j)h(x) - xh'(x)] = 0.$$

Applying this when $h(x) = f(x)(x/g(x))^i$, and adding into κ_{ij}, we get the desired result. □

In particular

$$\phi_{ij} = [\text{coeff. of } y^{i-j} \text{ in } (1+y)^{2i-n}(1-y)^{-i-1}].$$

Thus taking $n = 6m - l$ as before

$$\phi_{(2m-1)j} = [\text{coeff. of } y^{2m-1-j} \text{ in } (1+y)^{l-2}(1-y^2)^{-2m}].$$

This is positive whenever $l > 2$; for $l = 2$, it is nonnegative, and 0 only when j is even. We also have, for $l = 2$,

$$\phi_{(2m)j} = [\text{coeff. of } y^{2m-j} \text{ in } (1+y)^3(1-y^2)^{-2m-1}] > 0.$$

For $l = 1$

$$\phi_{(2m-1)j} = [\text{coeff. of } y^{2m-1-j} \text{ in } (1-y)(1-y^2)^{-2m-1}] = (-1)^{j+1}\binom{3m-1-\lfloor \frac{j}{2}\rfloor}{2m}$$

and

$$\phi_{(2m)j} = [\text{coeff. of } y^{2m-j} \text{ in } (1+y)^2(1-y^2)^{-2m-1}] = \begin{cases} \frac{2m-\lfloor \frac{j}{2}\rfloor}{m}\binom{3m-\lfloor \frac{j}{2}\rfloor-1}{2m-1}, & j \text{ even} \\ 2\binom{3m-\lfloor \frac{j}{2}\rfloor-1}{2m}, & j \text{ odd.}\end{cases}$$

In particular

$$\phi_{(2m)j} + 4\phi_{(2m-1)j} = \begin{cases} \frac{2\lfloor \frac{j}{2}\rfloor}{3m-\lfloor \frac{j}{2}\rfloor}\binom{3m-\lfloor \frac{j}{2}\rfloor}{2m}, & j \text{ even} \\ 6\binom{3m-1-\lfloor \frac{j}{2}\rfloor}{2m}, & j \text{ odd.}\end{cases}$$

This is nonnegative, and 0 only when $j = 0$.

Similarly, we can compute γ_{ij}

$$\gamma_{(k-i)j} = 2^{-r+1}[\text{coeff. of } Y^{i-j} \text{ in } (-1)^{k-i}2^{k-t-1-3i}(1-Y)^{-1-k+i}].$$

So

$$\gamma_{ij} = (-1)^i 2^{3i-n-r+1}[\text{coeff. of } Y^{k-i-j} \text{ in } (1-Y)^{-1-i}] = (-1)^i 2^{3i-n-r+1}\binom{k-j}{i}.$$

In particular, this is negative for i odd; furthermore, for $l = 1$

$$\gamma_{(2m)j} + 4\gamma_{(2m-1)j} = -2^{-r+1}\frac{j}{m}\binom{k-j}{k-m} < 0$$

except when $j = 0$. Also, for $l = 1$

$$\gamma_{(2m)0} = 2^{-r+1}\binom{3m-1}{2m-1} = 2^{-r}\phi_{(2m)0}.$$

We now have the inequalities necessary to prove

Theorem 9: Let C be an additive code over GF(4), of length $n = 6m - 1 + l$ with $0 \le l \le 5$, and dimension $n - r < n$, such that $C^\perp - C$ has minimum weight d. Then $d \le 2m+1$, except when $l = 5$, when $d \le 2m+2$. Any code meeting the bound for $l = 0$ must be the even subcode of a $[6m-1, 6m-1, 2m+1]_4$.

Proof: For $1 \le l \le 4$, we have $\phi_{(2m+1)j} > 0$ and $\gamma_{(2m+1)j} < 0$, giving a contradiction. For $l = 5$, we have $\phi_{(2m+1)j} = 0$ when j is even; consequently, we can conclude only that $f_j = 0$ for odd $j < (2m+1)$, and that $g_j = 0$ for all $j < m$. Now, consider e_{2m+2}. This is a linear combination of the g_j for $j < m-1$, so must equal 0. On the other hand, it is also a positive linear combination of f_j for $0 \le j \le 2m+2$; this is impossible unless $d < 2m+2$.

Finally, for $l = 0$, we consider $e_{2m} + 4e_{2m-1}$. This is a positive linear combination of f_j for $1 \le j \le 2m$, and a negative linear combination of g_j for $1 \le j \le m$. Consequently, all of these f_j and g_j must be 0. Then, considering e_{2m}, we have

$$e_{2m} = \gamma_{(2m)0} g_0 = \phi_{(2m)0} f_0$$

so

$$g_0 = 2^r f_0 = 2^r - 1.$$

If $r > 1$, then $g_0 > 1$, which is impossible (since $g_0 = S(1, 0)$); thus we must have $r = 1$, so $g_0 = 1$ and the code is even. Clearly, then, if we take D to be any self-dual code lying between C and $C^\perp$, then D must be a $[6m{-}1, 6m{-}1, 2m{+}1]_4$, and C is its even subcode. The theorem follows. $\square$

VI. Further Directions

There is still some room for improvements in the above bounds. For instance, integer programming readily shows that no self-dual binary code of length 26 can meet the bound. It should be possible to systematize such effects by considering certain congruences modulo small powers of 2 in the coefficients of the weight and shadow enumerators. Also, it should be possible to show that only a finite number of codes can meet the bound, by considering a_{4m+8}; in general, one would like a result saying that any bound of the form $n/6 - c$ can be exceeded only a finite number of times (this is known for doubly-even codes).

For self-orthogonal additive codes, the bound we give makes no use of the dimension of the code; for smaller codes, one ought to be able to produce much stronger bounds. It should be noted that one could prove a similar result for self-orthogonal binary codes that contain a vector of full weight; however, the object $C^\perp - C$ is much less natural in that case.

The theory of shadows also has an analogue for integral lattices [3]; as one might expect, therefore, the above bounds have analogues for lattices as well. For more details, consult [6].

Acknowledgment

The author wishes to thank N. Sloane for many productive conversations; in particular, for introducing the author to shadow theory.

References

[1] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over GF (4),” LANL e-print quant-ph/9608006.

[2] J. H. Conway and N. J. A. Sloane, “A new upper bound on the minimal distance of self-dual codes,” *IEEE Trans. Inform. Theory*, vol. 36, no. 6, 1990.

[3] ——, “A new upper bound for the minimum of an integral lattice of determinant 1,” *Bull. Amer. Math. Soc.*, vol. 23, no. 2, 1990.

[4] S. T. Dougherty and M. Harada, “Extremal and shadow extremal binary self-dual codes,” preprint.

[5] C. L. Mallows and N. J. A. Sloane, “An upper bound for self-dual codes,” *Inform. Contr.*, vol. 22, pp. 188–200, 1973.

[6] E. M. Rains and N. J. A. Sloane, “The shadow theory of modular and unimodular lattices,” in preparation.

[7] H. N. Ward, “A bound for divisible codes,” *IEEE Trans. Inform. Theory*, vol. 38, no. 1, pp. 191–195, 1992.

[8] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, 4th ed. New York: Cambridge Univ. Press, 1963.