Restrictions on the weight distribution of quaternary linear codes

Sugi Guritman and Juriaan Simonis
Department of Mediamatics, Faculty of Information Technology and Systems, Delft University of Technology, P.O. Box 5031, 2600 GA Delft, the Netherlands

Abstract - This paper describes some nonexistence results for quaternary linear codes. The standard linear program is strengthened with constraints from the weight distribution of binary Reed-Muller codes.

Keyword - Linear code, Reed-Muller code, Polynomial degree

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of ordered n-tuples over field $\mathbb{F}_q$. A linear code of length n over $\mathbb{F}_q$ is just a subspace $\mathcal{C} \subset \mathbb{F}_q^n$. If $\mathcal{C}$ has dimension k and minimum distance d, it is called an $[n,k,d]_q$-code. A central problem in algebraic coding theory is to optimize one of the parameters n, k, and d for given values of the other two. Although it is unlikely that this optimization problem will ever be solved in its full generality, many specific results have been obtained so far. The state of the art is listed in Brouwer's tables [2]. It is immediately clear from these tables that the amount of available information quickly diminishes with growing field size q. The present paper is devoted to the quaternary case, which is less well studied than the binary and ternary ones. Some of the significant results can be found in the papers [3] by Daskalov and [5] by Greenough and Hill.

Any set of parameters for which no code exists gives bounds for optimal codes. The most successful method so far of proving the nonexistence of codes has been linear programming. Let us describe in short this fundamental idea of Delsarte [4]. The *dual* $\mathcal{C}^\perp$ of an $[n,k,d]_q$-code $\mathcal{C}$ is its orthogonal with respect to the standard inner product in $\mathbb{F}_q^n$. Let $A_i(\mathcal{C})$ and $B_i(\mathcal{C})$ be the number of words of weight i in $\mathcal{C}$ and in $\mathcal{C}^\perp$, respectively. (These numbers are said to constitute the *weight distributions* of $\mathcal{C}$ and $\mathcal{C}^\perp$ respectively.) Obviously, $A_0(\mathcal{C}) = B_0(\mathcal{C}) = 1$. The remaining numbers satisfy the following set of linear constraints:

$$\begin{cases} A_i \geq 0 & (1 \leq i \leq n), \\ B_i \geq 0 & (1 \leq i \leq n), \\ A_i = 0 & (1 \leq i \leq d-1), \\ q^k B_i = \sum_{j=1}^{n} K_i(j) A_j + \binom{n}{i} & (1 \leq i \leq n). \end{cases} \tag{1}$$

The last equations are the celebrated MacWilliams identities, cf [8]. Now the basic idea is that the code $\mathcal{C}$ cannot exist if the linear program (1) is infeasible. Of course, adding new constraints makes for sharper bounds.

The second section describes the standard ways to strengthen (1). Section three shows that certain weight sums in $\mathcal{C}$ are weights in Reed-Muller codes of low order. Theorems of Hill and Lizak and of the second author are exploited in Section four. The next section sharpens the Reed-Muller tool for even weight quaternary codes. The paper ends with a list of all new nonexistence results.

2 Standard tools

In this section we present the standard ways to add constraints to the linear program (1). A good reference is Greenough and Hill [5].

ISSN: 1571-0653

Definition 1 *Let $\mathcal{C}$ be an $[n,k,d]_4$-code with generator matrix G, and let $\mathbf{c} \in \mathcal{C}$ be a word of weight w. Then the* residual code $\mathrm{Res}(\mathcal{C};\mathbf{c})$ *of $\mathcal{C}$ with respect to $\mathbf{c}$, is the code generated by the restriction of G to the columns where $\mathbf{c}$ has a zero entry. We will denote it by $\mathrm{Res}(\mathcal{C};w)$ if only the weight w of $\mathbf{c}$ matters.*

Proposition 2 *Let $\mathcal{C}$ be an $[n,k,d]_4$-code and let $d > \frac{3w}{4}$. Then $Res(\mathcal{C};w)$ has the parameters $[n-w, k-1, \geq (d - \lfloor \frac{3w}{4} \rfloor)]_4$.*

Hence if we know – for instance from Brouwer's tables [2] – that no code with parameters $[n-w, k-1, \geq (d - \lfloor \frac{3w}{4} \rfloor)]_4$ exists, we infer that $A_w(\mathcal{C}) = 0$.

Proposition 3 *The existence of an $[n,k,d]_4$-code with dual distance $d^\perp$ implies the existence of an $[n-d^\perp, k-d^\perp+1, d]_4$-code.*

So if no codes exist with parameters $[n-i, k-i+1, d]_4$, $i = 1, 2, \ldots, \alpha$, then the dual distance of any $[n,k,d]_4$-code $\mathcal{C}$ is at least $\alpha+1$, i.e. $B_1(\mathcal{C}) = B_2(\mathcal{C}) = \cdots = B_\alpha(\mathcal{C}) = 0$.

The next proposition tells us that there cannot be too many words of high weight.

Proposition 4 *Let $\mathcal{C}$ be an $[n,k,d]_4$-code. Then $\mathcal{C}$ satisfies the following conditions:*

1. *$A_i(\mathcal{C}) = 0$ or 3 for $i > (4n-3d)/2$,*
2. *If $A_i(\mathcal{C}) > 0$, then $A_j(\mathcal{C}) = 0$ for $j > 4n-3d-i$ and $i \neq j$.*

Example 5 *There is no $[94,6,68]_4$-code.*

Proof. Suppose $\mathcal{C}$ is a code with parameters $[94,6,68]_4$. The residual code argument and Brouwer's table [2] imply that the non-zero weights of $\mathcal{C}$ are in the set

$$\{0, 68, 70, 71, 72, 80, 83, 84, 88, 91, 92, 93, 94\}.$$

Table [2] tells us also that no linear codes with parameters $[93,6,68]_4$, $[92,5,68]_4$, or $[91,4,68]_4$ exist. By Proposition 3, we conclude that the dual distance of $\mathcal{C}$ is at least 4. With these additional constraints and those from Proposition 4, the linear program (1) turns out to be infeasible. ∎

In each of the examples in the sequel we shall use the linear program (1) together with the constraints from Proposition 2, Proposition 3 and Proposition 4. We shall call the complete set of constraints the *enhanced linear program*.

3 Constraints from gaps in the weight distribution of Reed-Muller codes

The ideas that underlie this section have been described in [10] and [6]. They find their origin in Brouwer's paper [1].

Consider the functions $\varphi_1, \varphi_2 : \mathbb{F}_4^n \to \mathbb{F}_4$ defined by

$$\varphi_1(\mathbf{x}) := \sum_{i=1}^{n} x_i^3, \ \varphi_2(\mathbf{x}) := \sum_{1 \leq i < j \leq n} x_i^3 x_j^3.$$

ISSN: 1571-0653

First of all we note that these functions only take the value 0 or 1 and that this value only depends on the weight. In fact, if $\mathrm{wt}(x) = w$, then

$$\varphi_1(\mathbf{x}) = w \bmod 2 \text{ and } \varphi_2(\mathbf{x}) = \binom{w}{2} \bmod 2.$$

In the sequel we view $\mathbb{F}_4^n$ as a binary $2n$-dimensional vector space. The binary degree of φ_1, φ_2 is the degree of their polynomial representation with respect to any binary coordinate system. We claim that $\deg \varphi_1 = 2$ and $\deg \varphi_2 = 4$. Indeed, the function

$$\mathbb{F}_4 \to \mathbb{F}_4,\ x \mapsto x^2,$$

is $\mathbb{F}_2$-linear, and $x^3 = x \cdot x^2$ is the product of two $\mathbb{F}_2$-linear functions.

Now let $\mathcal{C}$ be a quaternary linear code of length n and (quaternary) dimension k. So $\mathcal{C}$ is a $2k$-dimensional binary subspace of $\mathbb{F}_4^n$. Consider the restrictions

$$\psi_1 := \varphi_1|_{\mathcal{C}},\ \psi_2 := \varphi_2|_{\mathcal{C}}.$$

Since

$$\deg \psi_1 \le \deg \varphi_1 = 2,\ \ \deg \psi_2 \le \deg \varphi_2 = 4,$$

the support of ψ_1 is a word in the binary Reed-Muller code $\mathcal{R}(2, \mathcal{C}) = \mathcal{R}(2, 2k)$ of order 2 and the support of ψ_2 is a word in the binary Reed-Muller code $\mathcal{R}(4, \mathcal{C}) = \mathcal{R}(4, 2k)$ of order 4.

The weight distribution of Reed-Muller codes contains gaps, and these gaps are bigger if the order is smaller. We summarize some known facts in the following proposition. Proofs can be found in the standard reference [9].

Proposition 6 *Let $\mathcal{R}_2(r, m)$ be the rth order binary Reed-Muller code of length 2^m, where $r \ge 1$, and let w be a non-zero weight in $\mathcal{R}_2(r, m)$. Then*

1. *w is divisible by $2^{\lfloor \frac{m-1}{r} \rfloor}$,*
2. *$w \ge 2^{m-r}$,*
3. *if $2^{m-r} \le w < 2^{m-r+1}$, then, for appropriate t,*
$$w = 2^{m-r+1} - 2^{m-r+1-t},$$
4. *if $r = 2$, then*
$$w = 2^{m-1} \text{ or } w = 2^{m-1} \pm 2^{m-1-j}\ (0 \le j \le \frac{m}{2}).$$

Now we look at the sizes of the supports of ψ_1, ψ_2 and $\psi_1 + \psi_2$. These are expressions in the weight distribution of $\mathcal{C}$. In fact, we have

$$\begin{aligned} |\operatorname{supp} \psi_1| &= A^{(1,3)}, \\ |\operatorname{supp} \psi_2| &= A^{(2,3)}, \\ |\operatorname{supp}(\psi_2 + \psi_1)| &= A^{(1,2)}, \end{aligned}$$

where $A^{(a,b)}$ is short for $\sum_{i \equiv a \text{ or } b(4)} A_i$. So Proposition 6 yields constraints for the weight distribution of $\mathcal{C}$.

These can be improved by the trivial observation that $A^{(1,3)}$, $A^{(2,3)}$ and $A^{(1,2)}$ are divisible by 3. The complementary sums $A^{(0,2)}$, $A^{(0,1)}$ and $A^{(0,3)}$ are congruent to 1 modulo 3. We summarize the results of this section in Theorem 7 and Theorem 9.

ISSN: 1571-0653

Theorem 7 *If $\mathcal{C}$ is a quaternary linear code of dimension k, then the integer $A^{(1,3)} = \sum_{i \ odd} A_i(\mathcal{C})$ is a weight in the Reed-Muller code $\mathcal{R}_2(2, 2k)$ which is divisible by 3. Hence*

$$\sum_{i \equiv 1 \ or \ 3(4)} A_i(\mathcal{C}) \quad \in$$

$$\{2^{2k-1} + 2^{2k-2j} \ (1 \quad \leq \quad j \leq \lceil \frac{k}{2} \rceil), \ 2^{2k-1} - 2^{2k-1-2j} \ (0 \leq j \leq \lfloor \frac{k}{2} \rfloor)\}$$

Example 8 *There is no $[57, 8, 38]_4$-code.*

Proof. Suppose $\mathcal{C}$ is a code with parameters $[57, 8, 38]_4$. The dual distance of $\mathcal{C}$ is at least 6. Optimize $A^{(1,3)}$ with respect to the enhanced constraints (cf. p. 735). We find that $6651 \leq A^{(1,3)} \leq 20231$, which contradicts the preceding theorem. ∎

Theorem 9 *Let ω denote weight sum $A^{(1,2)}$, $A^{(2,3)}$, $A^{(0,3)}$ or $A^{(0,1)}$. Then in the first two cases ω is divisible by 3 and in the last two cases it is congruent to 1 modulo 2. Furthermore, ω is divisible by $2^{\lfloor \frac{2k-1}{4} \rfloor}$. Finally,*

1. *if $\omega < 2^{2k-3}$, then $\omega = 2^{2k-3} - 2^{2k-3-t}$, and*
2. *if $\omega > 2^{2k} - 2^{2k-3}$, then $\omega = 2^{2k} - 2^{2k-3} + 2^{2k-3-t}$*

for suitable t.

Example 10 *There is no $[78, 9, 53]_4$-code.*

Proof. Suppose $\mathcal{C}$ is a code of parameters $[78, 9, 53]_4$. Optimizing $A^{(1,3)}$ with respect to the enhanced constraints yields $77263 \leq A^{(1,3)} \leq 129839$, which is improved by Theorem 7 to $98304 \leq A^{(1,3)} \leq 129024$. Add this constraint and then optimize $A^{(2,3)}$. We obtain $6331 \leq A^{(2,3)} \leq 22598$. which contradicts Theorem 9. ∎

4 Adding a parity check bit

In 1995, Hill and Lizak found an amusing and useful result.

Theorem 11 *([7]) Let $\mathcal{C}$ be a linear $[n, k, d]$-code over $\mathbb{F}_q$ with $\gcd(d, q) = 1$ and with all weights congruent to 0 or d (modulo q). Then $\mathcal{C}$ can be extended to an $[n+1, k, d+1]$-code whose weights are congruent to 0 or $d + 1$ (modulo q).*

Their proof was based on the following lemma.

Lemma 12 *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$-code, and let s be an integer which is relatively prime to q and such that all weights in $\mathcal{C}$ are congruent to 0 or s modulo q. Then $\{\mathbf{c} \in \mathcal{C} \mid \mathrm{wt}(\mathbf{c}) \equiv 0(q)\}$ is a linear subcode of $\mathcal{C}$ of dimension $\geq k - 1$.*

Here is an example of how this lemma can be used.

Example 13 *No code of parameters $[54, 8, 36]_4$ exists.*

ISSN: 1571-0653

Proof. Suppose $\mathcal{C}$ is a code of parameters $[54, 8, 36]_4$. Optimizing $A^{(1,3)}$ with respect to the usual enhanced constraints yields $18672 \leq A^{(1,3)} \leq 47882$. Theorem 7 then implies that

$$A^{(1,3)} \in \{24576, 30720, 32256, 32640, 33024, 33792, 36864\}. \tag{2}$$

Use this to optimize $A^{(2,3)}$. The result is $23982 \leq A^{(2,3)} \leq 42255$. Now Theorem 9 improves this to $24000 \leq A^{(2,3)} \leq 42240$. Next we switch to $A^{(1,2)}$. Enhanced linear programming with the additional constraints and Theorem 9 imply that $A^{(1,2)} = 0$ or 6144. If $A^{(1,2)} = 6144$, the optimization of $A^{(1,3)}$ would give $34110 \leq A^{(1,3)} \leq 35615$, in conflict with Theorem 7. Hence $A^{(1,2)} = 0$. That means that all weights in $\mathcal{C}$ are congruent to 0 or 3 modulo 4. Now apply Lemma 12. The size of $\{\mathbf{c} \in \mathcal{C} \mid \mathrm{wt}(\mathbf{c}) \equiv 0(4)\}$ is equal to 4^7 or 4^8. Hence $A^{(1,3)} = 4^8 - 4^7 = 49152$ or $A^{(1,3)} = 0$. This contradicts (2). ■

Recently, an improvement of Theorem 11 was found.

Theorem 14 *[11]Let $\mathcal{C}$ be a linear $[n, k, d]$-code over a field $\mathbb{F}_q$ of characteristic p. If $d \not\equiv 0 \bmod p$ and*

$$\sum_{i \not\equiv u(p)} A_i(\mathcal{C}) = q^{k-1},$$

for some $u \in \{1, 2, \ldots, p-1\}$, then $\mathcal{C}$ can be extended to an $[n+1, k, d+1]$-code.

The next example demonstrates how this result can be used in nonexistence proofs.

Example 15 *There is no $[86, 5, 63]_4$-code.*

Proof. Suppose $\mathcal{C}$ is a code of parameters $[86, 5, 63]_4$. The enhanced linear program and Theorem 7 imply that

$$A^{(1,3)} \in \{480, 528, 576, 768\}.$$

Suppose $480 \leq A^{(1,3)} \leq 576$. Then these extra constraints would yield $0 \leq A^{(1,2)} \leq 68$, and Theorem 9 would reduce this to $A^{(1,2)} = 0$. Then $\mathcal{C}$ would satisfy the conditions of Theorem 11. But Brouwer's table [2] tells us that there is no $[87, 5, 64]_4$-code. We infer that $A^{(1,3)} = 768 = 4^5 - 4^{5-1}$. Now Theorem 14 applies. Again, a code of parameters $[87, 5, 64]_4$ must exist, a contradiction. ■

5 Even weight quaternary linear codes

In Section 3, we have seen that the restriction of the function

$$\varphi_2(\mathbf{x}) := \sum_{1 \leq i < j \leq n} x_i^3 x_j^3$$

to a quaternary linear code $\mathcal{C}$ has degree ≤ 4. We claim that we can do better if all weights in $\mathcal{C}$ are even.

Theorem 16 *If all weights in a quaternary linear code $\mathcal{C}$ are even, then the restriction ψ of φ_2 to $\mathcal{C}$ has degree ≤ 3. Hence $\sum_{i \equiv 0(4)} A_i(\mathcal{C})$ is a weight in a Reed-Muller code of order* three.

Proof. Let $\mathcal{C}$ be a quaternary linear code without any words of odd length. Then the words of weight divisible by 4 in $\mathcal{C}$ are the support of the restriction of $\varphi_2 + 1$ to $\mathcal{C}$. So the last statement follows if we can prove that we have to prove that $\deg \psi = \deg(\varphi_2|_{\mathcal{C}}) \leq 3$. It is sufficient to prove that $\deg(\varphi_2|_{\mathcal{D}}) \leq 3$ for all 4-dimensional binary linear subcodes $\mathcal{D}$ of $\mathcal{C}$. Hence, it is sufficient to prove that the theorem is true for all quaternary linear codes of dimension ≤ 4. We shall do this in the following three lemmas. Let α be a primitive element of $\mathbb{F}_4$. So $\mathbb{F}_4 = \{0, 1, \alpha, \overline{\alpha} = \alpha^2\}$. Note that φ_2 is invariant under multiplication by α, i.e. $\varphi_2(\alpha \mathbf{x}) = \varphi_2(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_4^n$. ■

ISSN: 1571-0653

Lemma 17 *16 is true for* $\dim \mathcal{C} = 2$.

Proof. Since $\mathcal{C}$ is a binary vector space of dimension 4, we have to show that the support of ψ is a word in the Reed-Muller code $R_2(4,3)$, i.e. that the size of $\{\mathbf{c} \in \mathcal{C} \mid \psi(\mathbf{c}) = 1\}$ is even. We may assume that $\mathcal{C}$ has a generator matrix of the form

row $\mathbf{c}_1$	1...1	1...1	1...1	1...1	0...0	0...0
row $\mathbf{c}_2$	1...1	α...α	$\overline{\alpha}$...$\overline{\alpha}$	0...0	1...1	0...0
# columns	a	b	c	d	e	

The five codewords $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3 := \mathbf{c}_1 + \mathbf{c}_2$, $\mathbf{c}_4 := \mathbf{c}_1 + \alpha\mathbf{c}_2$, and $\mathbf{c}_5 := \mathbf{c}_1 + \overline{\alpha}\mathbf{c}_2$ have even weight. So

$$\begin{aligned} a+b+c+d &\equiv 0 \bmod 2, \\ a+b+c+e &\equiv 0 \bmod 2, \\ b+c+d+e &\equiv 0 \bmod 2, \\ a+c+d+e &\equiv 0 \bmod 2, \\ a+b+d+e &\equiv 0 \bmod 2, \end{aligned}$$

whence a, b, c, d and e have the same parity. The value of ψ in $\mathbf{c}_1$ is equal to

$$ab + ac + ad + bc + bd + cd + \binom{a}{2} + \binom{b}{2} + \binom{c}{2} + \binom{d}{2},$$

but the fist six terms add up to an even number. So we find

$$\psi(\mathbf{c}_1) \equiv \binom{a}{2} + \binom{b}{2} + \binom{c}{2} + \binom{d}{2} \bmod 2,$$

and, analogously,

$$\begin{aligned} \psi(\mathbf{c}_2) &\equiv \binom{a}{2} + \binom{b}{2} + \binom{c}{2} + \binom{e}{2} \bmod 2, \\ \psi(\mathbf{c}_3) &\equiv \binom{b}{2} + \binom{c}{2} + \binom{d}{2} + \binom{e}{2} \bmod 2, \\ \psi(\mathbf{c}_4) &\equiv \binom{a}{2} + \binom{c}{2} + \binom{d}{2} + \binom{e}{2} \bmod 2, \\ \psi(\mathbf{c}_5) &\equiv \binom{a}{2} + \binom{b}{2} + \binom{d}{2} + \binom{e}{2} \bmod 2. \end{aligned}$$

Now it is straightforward to check that for all values of $\binom{a}{2}$, $\binom{b}{2}$, ..., $\binom{e}{2}$ an even number of the $\psi(\mathbf{c}_i)$ takes the value 1. The size of the support of ψ is three times this number. So it is even as well. ∎

Lemma 18 *Theorem 16 is true for* $\dim \mathcal{C} = 3$.

Proof. We know that $\deg(\psi|_{\mathcal{D}}) \leq 3$ for all 2-dimensional quaternary subcodes of $\mathcal{C}$ and that $\psi(\alpha\mathbf{x}) = \psi(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{C}$. Choose three independent quaternary coordinates x, y, and z on $\mathcal{C}$. We can write them as $x = x_0 + \alpha x_1$, $y = y_0 + \alpha y_1$, and $z = z_0 + \alpha z_1$, where x_0, x_1, y_0, y_1, z_0, z_1 are 6 binary coordinates. Let ψ_4 be the part of degree 4 of $\psi(x_0, x_1, y_0, y_1, z_0, z_1)$. All nonzero

ISSN: 1571-0653

monomials of ψ_4 must have coordinates from x, y and z. If, for instance, ψ_4 would contain the monomial $x_0x_1y_0y_1$, then the restriction of ψ to $\{z=0\}$ would have degree 4, a contradiction to the preceding lemma. Hence ψ_4 is a linear combination of the twelve monomials

$$\begin{array}{llllll} x_0x_1y_0z_0, & x_0x_1y_0z_1, & x_0x_1y_1z_0, & x_0x_1y_1z_1, & y_0y_1x_0z_0, & y_0y_1x_0z_1 \\ y_0y_1x_1z_0, & y_0y_1x_1z_1, & z_0z_1x_0y_0, & z_0z_1x_0y_1, & z_0z_1x_1y_0, & z_0z_1x_1y_1. \end{array}$$

Since the restriction of ψ_4 to $\{y=x\}$, i.e. to $\{y_0=x_0, y_1=x_1\}$, has degree 3, the coefficients of $z_0z_1x_1y_0$ and $z_0z_1x_0y_1$ must be equal. We get analogous results with respect to the subcodes $\{y=z\}$ and $\{x=z\}$. Multiplication by α changes the list of polynomials

$$\begin{bmatrix} x_0x_1y_0z_0 \\ x_0x_1y_0z_1+x_0x_1y_1z_0 \\ x_0x_1y_1z_1 \\ y_0y_1x_0z_0 \\ y_0y_1x_0z_1+y_0y_1x_1z_0 \\ y_0y_1x_1z_1 \\ z_0z_1x_0y_0 \\ z_0z_1x_0y_1+z_0z_1x_1y_0 \\ z_0z_1x_1y_1 \end{bmatrix} \text{ to } \begin{bmatrix} x_0x_1y_1z_1 \\ x_0x_1y_0z_1+x_0x_1y_1z_0 \\ x_0x_1y_0z_0+x_0x_1y_0z_1+x_0x_1y_1z_0+x_0x_1y_1z_1 \\ y_0y_1x_1z_1 \\ y_0y_1x_0z_1+y_0y_1x_1z_0 \\ y_0y_1x_0z_0+y_0y_1x_0z_1+y_0y_1x_1z_0+y_0y_1x_1z_1 \\ z_0z_1x_1y_1 \\ z_0z_1x_0y_1+z_0z_1x_1y_0 \\ z_0z_1x_0y_0+z_0z_1x_0y_1+z_0z_1x_1y_0+z_0z_1x_1y_1 \end{bmatrix}.$$

Since ψ is invariant under multiplication by α, we infer that the coefficients of

$$x_0x_1y_0z_0,\ x_0x_1y_1z_1,\ y_0y_1x_0z_0,\ y_0y_1x_1z_1,\ z_0z_1x_0y_0 \text{ and } z_0z_1x_1y_1$$

must be zero. Finally by restricting ψ_4 to $\{y=\alpha x\}$, $\{z=\alpha y\}$ and $\{x=\alpha z\}$ we see that the coefficients of the remaining monomials must be zero as well. ∎

Lemma 19 *Theorem 16 is true for* $\dim \mathcal{C}=4$.

Proof. We proceed in the same way as in the preceding lemma. We choose four independent quaternary coordinates x, y, z, and u. We can write them as $x=x_0+\alpha x_1$, $y=y_0+\alpha y_1$, $z=z_0+\alpha z_1$, and $u=u_0+\alpha u_1$, where x_0, x_1, y_0, y_1, z_0, z_1, u_0, u_1 are 8 binary coordinates. Let ψ_4 be the part of degree 4 of $\psi(x_0,x_1,y_0,y_1,z_0,z_1,u_0,u_1)$. Since the restrictions of ψ to the 3-dimensional subcodes like $\{x=0\}$ must have degree ≤ 3, we infer that only the sixteen monomials

$$\begin{array}{llll} x_0y_0z_0u_0, & x_1y_0z_0u_0, & x_0y_1z_0u_0, & x_1y_1z_0u_0, \\ x_0y_0z_1u_0, & x_1y_0z_1u_0, & x_0y_1z_1u_0, & x_1y_1z_1u_0, \\ x_0y_0z_0u_1, & x_1y_0z_0u_1, & x_0y_1z_0u_1, & x_1y_1z_0u_1, \\ x_0y_0z_1u_1, & x_1y_0z_1u_1, & x_0y_1z_1u_1, & x_1y_1z_1u_1 \end{array}$$

are involved in ψ_4. From the restrictions to the other 3-dimensional subcodes we learn that ψ_4 must be a linear combination of the three polynomials

$$\begin{gathered} x_0y_0z_0u_0+x_0y_1z_1u_1+x_1y_0z_1u_1+x_1y_1z_0u_1+x_1y_1z_1u_0, \\ x_1y_1z_1u_1+x_1y_0z_0u_0+x_0y_1z_0u_0+x_0y_0z_1u_0+x_0y_0z_0u_1, \\ x_1y_1z_0u_0+x_1y_0z_1u_0+x_1y_0z_0u_1+x_0y_1z_1u_0+x_0y_1z_0u_1+x_0y_0z_1u_1. \end{gathered}$$

The invariance of ψ under multiplication by α then implies that $\psi_4=0$. ∎

If we combine the preceding theorem with Proposition 6, we obtain the following constraints for the weight distribution of even quaternary codes.

ISSN: 1571-0653

Theorem 20 *Let $\mathcal{C}$ be a k-dimensional quaternary linear code in which all codewords have even weight. Then the weight sum $\omega := \sum_{i \equiv 2(4)} A_i(\mathcal{C})$ is divisible by 3 and by $2^{\lfloor \frac{2k-1}{3} \rfloor}$. Moreover,*

1. *if $\omega < 2^{2k-2}$, then $\omega = 2^{2k-2} - 2^{2k-2-t}$, and*
2. *if $\omega > 2^{2k} - 2^{2k-2}$, then $\varpi = 2^{2k} - 2^{2k-2} + 2^{2k-2-t}$*

for suitable t.

Example 21 *There is no $[77, 7, 54]_4$-code.*

Proof. Suppose $\mathcal{C}$ is a code of parameters $[77, 7, 54]_4$. We optimize $A^{(1,3)}$ with respect to the usual enhanced constraints and then apply Theorem 7. As a result, we find that $A^{(1,3)} = 0$, i.e. that $\mathcal{C}$ is an even weight code. Now we optimize $\omega := \sum_{i \equiv 2(4)} A_i$ to find that $13402 \leq \omega \leq 14056$. This contradicts Theorem 20. ∎

References

[1] A. E. Brouwer, "The linear programming bound for binary linear codes," *IEEE Trans. Inform. Theory,* vol. **39**, no. 2, pp. 677–680, 1993.

[2] A. E. Brouwer, "Bounds on the size of linear codes," in *Handbook of Coding theory*, ed.: V.Pless and W. C. Huffman. Elsevier, 1998. ISBN: 0-444-50088-X. Online version: http://www.win.tue.nl/math/dw/voorlincod.html.

[3] R. N. Daskalov and E. Metodieva, "The nonexistence of some five-dimensional Quaternary linear codes," *IEEE Trans. Inform. Theory,* vol. **41**, no. 2, pp. 581–583, 1995.

[4] P. Delsarte, "An Algebraic Approach to the Association Schemes of Coding Theory," *Philips Res. Rep. Suppl. 10*, 1973.

[5] P. Greenough and R. Hill, "Optimal linear codes over $GF(4)$," 13th British Combinatorial Conference (Guildford, 1991), *Discrete Math,* vol. **125**, no. 1-3, pp. 187-199, 1994.

[6] S. Guritman, F. Hoogweg and J. Simonis, "The degree of functions and weights in linear codes," To appear in *Discrete Applied Mathematics.*

[7] R. Hill, and P. Lizak, "Extensions of linear codes," *Proc. International Symposium on Inform. Theory,* pp. 345, (Whistler, Canada, 1995).

[8] F.J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell System Tech. J.* **42** (1963), 79-94.

[9] F. J. MacWilliams and N. J. A. Sloane, "The theory of error-correcting codes," 2nd reprint, North-Holland Mathematical Library, vol. 16, *North-Holland Publishing Co., Amsterdam - New York - Oxford,* 1983, xx+762 pp. ISBN: 0-444-85009-0 and 0-444-85010–4.

[10] J. Simonis, "Restrictions on the weight distribution of binary linear codes imposed by the structure of Reed-Muller codes," *IEEE Trans. Inform. Theory,* vol. **40**, no. 1, pp. 194–196, 1994.

[11] J. Simonis, "Adding a parity check bit," to appear in *IEEE Trans. Inform. Theory.*

ISSN: 1571-0653