Nonexistence Proofs for Five Ternary Linear Codes

Sugi Guritman*
Department of Mathematics, Bogor Agricultural University
Jl. Raya Pajajaran Bogor, 16144 Indonesia

Abstract

An $[n, k, d]_3$-code is a ternary linear code with length n, dimension k and minimum distance d. We prove that codes with parameters $[110, 6, 72]_3$, $[109, 6, 71]_3$, $[237, 6, 157]_3$, $[69, 7, 43]_3$, and $[120, 9, 75]_3$ do not exist.

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of ordered n-tuples over the finite field $\mathbb{F}_q$. A linear code of length n over $\mathbb{F}_q$ is a subspace $C \subseteq \mathbb{F}_q^n$. If 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 [1]. It is immediately clear from these tables that the amount of available information quickly diminishes with growing field size q.

The current paper presents nonexistence proofs of ternary linear codes ($q = 3$) with certain parameters. Of course, any set of parameters for which no code exists gives bounds for optimal codes. The main tools for nonexistence proofs use the linear programming method. We classify the tools into standard tools and an additional tool. The standard tools are the standard residual code argument, the MacWilliams equations and the existence of "minimal" generator matrices which will be described in Section 2. The additional tool is based on the weight distribution of Reed-Muller codes which will be described in Section 3. Finally Section 3 presents the main results. Below is a short description of the linear programming method.

Let us describe briefly this fundamental idea of Delsarte [3]. The *dual* $C^\perp$ of an $[n, k, d]_q$-code C is its orthogonal with respect to the standard inner product in $\mathbb{F}_q^n$. Let $A_i(C)$ and $B_i(C)$ be the number of words of weight i in C and in $C^\perp$, respectively. Obviously, $A_0(C) = B_0(C) = 1$. The remaining numbers satisfy the following set of

*e-mail: guritman@indo.net.id

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 [9]. Now the basic idea is that the code C cannot exist if the linear program (1) is infeasible. Of course, adding new constraints makes for sharper bounds. The standard tools is the classical ways to strengthen (1).

1.1 Standard tools

These standard references are [2], [7] and [4].

Definition 1 *Let C be an $[n, k, d]_3$-code with generator matrix G, and let $\mathbf{c} \in C$ be a word of weight w. Then the residual code $\mathrm{Res}(C; \mathbf{c})$ of 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 $\mathrm{Res}(C; w)$ if only the weight w of $\mathbf{c}$ matters.*

Proposition 2 *Let C be an $[n, k, d]_3$-code such that $d > \frac{2w}{3}$: Then $Res(C; w)$ has the parameters $[n - w, k - 1, d - \lfloor \frac{2w}{3} \rfloor]_3$.*

Proposition 3 (The MacWilliams Equations) *Let C be an $[n, k, d]_3$-code and let $C^\perp$ be the dual of C. Let $A_i(C)$ and $B_i(C)$ be the number of words of weight i in C and in $C^\perp$, respectively. Then*

$$\sum_{j=0}^{n} K_i(j) A_j(C) = 3^k B_i(C), 0 \leq i \leq n,$$

where the coefficients $K_i(j)$ are defined by

$$K_i(j) := \sum_{s=0}^{i} (-1)^s \binom{n-j}{i-s} \binom{j}{s} 2^{i-s}, \quad 0 \leq i \leq n.$$

Proposition 4 *The existence of an $[n, k, d]_3$-code with dual distance $d^\perp$ implies the existence of an $[n - d^\perp, k - d^\perp + 1, d]_3$-code.*

Proposition 5 *Suppose $\mathbf{x}$ and $\mathbf{y}$ are two ternary vectors of length n. Then*

$$\mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) + \mathrm{wt}(\mathbf{x} + \mathbf{y}) + \mathrm{wt}(\mathbf{x} + 2\mathbf{y}) = 3(n - z), \tag{2}$$

where z is the number of coordinates places in which both $\mathbf{x}$ and $\mathbf{y}$ are zero.

Proposition 6 *If C is an $[n, k, d]_3$-code, then*

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

1.2 Additional tools

The following proposition is the ternary version of a result by Hill and Lizak.

Proposition 7 [8] *Let C be an $[n,k,d]_3$-code with $\gcd(d,3)=1$. If all weights in C are congruent to 0 or d modulo 3, then C can be extended to an $[n+1,k,d+1]_3$-code whose weights are congruent to 0 or $d+1$ modulo 3.*

The proof is actually based on the following lemma.

Lemma 8 *Let C be an $[n,k,d]_3$-code, and let $s \in \{1,2\}$ be such that all weights in C are congruent to 0 or s modulo 3. Then $\mathcal{D} = \{c \in C \mid \mathrm{wt}(c) \equiv 0(3)\}$ is a linear subcode of C of dimension $\geq k-1$.*

Gaps in the weight distribution of ternary Reed-Muller codes imply restrictions on the weight distribution of ternary linear codes (cf. [5]). Here are two results of this type:

Proposition 9 *If C is a ternary linear code of dimension k, then*

$$\sum_{i\equiv 0(3)} A_i(C) \in \{3^{k-1}, 3^{k-1} \pm 2\cdot 3^{k-1-j} \ (0 \leq j \leq \tfrac{k}{2})\},$$
$$\sum_{i\equiv u(3)} A_i(C) \in \{3^{k-1} \pm 3^{k-1-j} \ (0 \leq j \leq \tfrac{k}{2})\}, \quad u = 1,2.$$

Proposition 10 *Let C be ternary linear code of dimension k. If $\sum_{i\not\equiv u(3)} A_i(C) = 3^{k-1}$ for some $u \in \{1,2\}$, then $\{c \in C \mid \mathrm{wt}(c) \not\equiv u(3)\}$ is a linear subcode of C of dimension $k-1$.*

2 Some nonexistence proofs

In this section we prove the nonexistence of a few ternary linear codes. The computerized calculations were done by MAPLE. We use the notation $A^{(u)} := \sum_{i\not\equiv u(3)} A_i(C)$ for $u \in \{0,1,2\}$.

Theorem 11 *There is no $[110,6,72]_3$-code.*

Proof. Suppose C is a code of parameters $[110,6,72]_3$. From the residual code technique and known nonexistence results in dimension 5 (cf. the table in [1]) we find that the weight set of C is contained in

$$\{0,72,81,90,99,108,109,110\}.$$

Proposition 4 and the table in [1] imply that the dual distance is at least 2. Apply the linear programming with respect to the MacWilliams equations, the above constraints and those from Proposition 6. We respectively find that C has no words of weight 110, 109, 108 and 99. Moreover, we find that $0 \leq A_{81}(C) \leq 60$.

Let $\mathbf{x} \in \mathcal{C}$ with $\mathrm{wt}(\mathbf{x}) = 90$, and let $\mathbf{y}$ be a word in $\mathcal{C}$ which is linearly independent of $\mathbf{x}$. If z is the number of coordinates places in which both $\mathbf{x}$ and $\mathbf{y}$ are zero, then Equation 2 becomes

$$\mathrm{wt}(\mathbf{y}) + \mathrm{wt}(\mathbf{x}+\mathbf{y}) + \mathrm{wt}(\mathbf{x}+2\mathbf{y}) = 3(110 - z) - 90. \tag{3}$$

The residual code $\mathcal{D} := \mathrm{Res}(\mathcal{C}; \mathbf{x})$ has parameters $[20, 5, 12]_3$, and $\mathbf{y}$ corresponds to a word in $\mathcal{D}$ of weight $20 - z$. Suppose that this word has weight 15, i.e. that $z = 5$. Then Equation 3 becomes

$$\mathrm{wt}(\mathbf{y}) + \mathrm{wt}(\mathbf{y}+\mathbf{x}) + \mathrm{wt}(\mathbf{y}+2\mathbf{x}) = 225.$$

Since the nonzero weight set of $\mathcal{C}$ is $\{72, 81, 90\}$, exactly one of $\mathbf{y}$, $\mathbf{y}+\mathbf{x}$ and $\mathbf{y}+2\mathbf{x}$ have weight 81 and the other two have weight 72. That means that $A_{81}(\mathcal{C}) \geq A_{15}(\mathcal{D})$. Hamada, Helleseth and Ytrehus, however, have shown in [10] that the $[20, 5, 12]_3$-codes must have the weight distribution $A_{12}(\mathcal{D}) = 150$, $A_{15}(\mathcal{D}) = 72$, and $A_{20}(\mathcal{D}) = 20$. ∎

Theorem 12 *There is no* $[109, 6, 71]_3$*-code.*

Proof. Suppose $\mathcal{C}$ is a code of parameters $[109, 6, 71]_3$. We reduce the number of possible weights by means of the residual code technique and note that the dual distance is at least 2. The optimizing the weight sum $A^{(0)}$ with respect to the MacWilliams equations gives $73 \leq A^{(0)} \leq 728$. From Proposition 9 we infer that actually $324 \leq A^{(0)} \leq 648$. Add these new constraints constraint to optimize $A^{(1)}$. The result is $727 \leq A^{(1)} \leq 729$, and then Proposition 9 implies that $A^{(1)} = 729 = 3^6$. So all weights in $\mathcal{C}$ are congruent to 0 or 2 modulo 3, and Proposition 7 applies. This leads to a contradiction, because we have shown in the preceding theorem that no $[110, 6, 72]_3$-code exists. ∎

Theorem 13 *There is no* $[237, 6, 157]_3$*-code.*

Proof. Suppose $\mathcal{C}$ is a code of parameters $[237, 6, 157]_3$. Its dual distance is at least 3. Using the standard techniques, we reduce the weight set to

$$\{0, 157, 158, 159, 168, 182, 183\}.$$

Optimizing $A^{(0)}$ with respect to the MacWilliams equations then gives $530 \leq A^{(0)} \leq 728$, and Proposition 9 improves this to $A^{(0)} = 540$ or 648. Use these new constraints to optimize $A^{(1)}$. The result is $85 \leq A^{(1)} \leq 307$, and Proposition 9 implies that $A^{(1)} = 243 = 3^{6-1}$. According to Proposition 10, the words of weight congruent to 0 or 2 modulo 3 in $\mathcal{C}$ constitute a 1-codimensional subcode $\mathcal{D}$. Let $\mathbf{x} \in \mathcal{C}$ with $\mathrm{wt}(\mathbf{x}) \equiv 2 \bmod 3$ and $\mathbf{y} \in \mathcal{C}$ with $\mathrm{wt}(\mathbf{y}) \equiv 1 \bmod 3$. Since $\mathbf{x} \in \mathcal{D}$ and $\mathbf{y} \notin \mathcal{D}$, both $\mathbf{x}+\mathbf{y}$ and $\mathbf{x}+2\mathbf{y}$ are in the complement of $\mathcal{D}$. Hence $\mathrm{wt}(\mathbf{x}+\mathbf{y}) \equiv 1 \bmod 3$ and $\mathrm{wt}(\mathbf{x}+2\mathbf{y}) \equiv 1 \bmod 3$. Then Equation 2 becomes $2 \equiv 0 (\mathrm{mod}\ 3)$, a contradiction. ∎

Theorem 14 *There is no* $[69, 7, 43]_3$*-code.*

Proof. Suppose C is a code of parameters $[69,7,43]_3$. Its dual distance is at least 4 and its weight set is contained in

$$\{0,43,44,45,47,48,51,54,56,57,58,59,60,62,63,65,66,67,68,69\}.$$

Optimization of $A^{(0)}$ with respect to the MacWilliams equations yields $1149 \leq A^{(0)} \leq 1556$, and by Proposition 9 this can be strengthened to $1296 \leq A^{(0)} \leq 1512$. Add these new constraints, and optimize $A^{(1)}$. The result is $882 \leq A^{(1)} \leq 1233$, and now Proposition 9 implies that $A^{(1)} = 1215$. With this new information we optimize $A^{(2)}$. We find that $1708 \leq A^{(2)} \leq 1742$, which contradicts Proposition 9. ∎

Theorem 15 *There is no* $[120,9,75]_3$*-code.*

Proof. Suppose C is a code of parameters $[120,9,75]_3$. We proceed as in the theorems above, and optimize $A^{(0)}$ with respect to the MacWilliams equations, taking into account that some weights do not occur and that the dual distance is at least 3. We find that $933 \leq A^{(0)} \leq 10140$. and from Proposition 9 we infer that $A^{(0)} = 8748$. Add this constraint to the program, and optimize $A^{(1)}$. The result is $17832 \leq A^{(1)} \leq 19638$, and Proposition 9 now implies that $A^{(1)} = 19683 = 3^9$. So C contains no words of weight 1 modulo 3. Then, optimizing $A^{(2)}$, we find that $A^{(2)} = 10935$, i.e. the number of words of weight 0 modulo 3 in C is $10935 \neq 3^{9-1}$. This contradicts Lemma 8. ∎

Let $D_3(n,k)$ be the largest integer d for which an $[n,k,d]_3$ code exists. The state of the art for bounds on $D_3(n,k)$ can be found in Brouwer's on-line table [1]. On April 7, 2000, we checked that the results above improve this table as follows:

$$\begin{aligned} D_3(110,6) &= 71,\ D_3(109,6) = 70,\ D_3(237,6) = 156, \\ 41 &\leq D_3(69,7) \leq 42 \text{ and } 72 \leq D_3(120,9) \leq 74. \end{aligned}$$

We have investigated other cases in Brouwer's table using the tools and methods in this paper. There are more than 200 improvements for the upper bound of $D_3(n,k)$, $k \leq 17$. These have been reported in [6].

References

[1] 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.

[2] R. N. Daskalov, "On the nonexistence of some 7-dimensional ternary linear codes," *In Proc. OCRT,* Sozopol, Bulgaria, May 26-June 1, pp. 49-53, 1998.

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

[4] P. 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.

[5] S. Guritman, F. Hoogweg and J. Simonis, "The degree of functions and weights in linear codes," *Discrete Applied Mathematics,* vol. **111**, pp. 87–102, 2001.

[6] S. Guritman, *Restrictions on the weights distribution of linear codes.* Delft University of Technology, the Netherlands: PhD Thesis, 2000.

[7] R. Hill and D. E. Newton, "Optimal ternary linear codes," *Des. Codes Cryptogr,* vol. **2**, no. 2, pp. 137–157, 1992.

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

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

[10] N. Hamada, T. Helleseth and Ø. Ytrehus, "There are exactly two nonequivalent $[20, 5, 12; 3]$-codes," *Ars Comb.,* vol **35**, pp. 3–14, 1993.