МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2005
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2005
Proceedings of the Thirty Fourth Spring Conference of the Union of Bulgarian Mathematicians
Borovets, April 6–9, 2005

A NEW PROOF FOR THE NONEXISTENCE OF A $[15, 6; (\mathrm{r} =)3]$ CODE*

Veselin Vl. Vavrek

It is proved that a linear code of length 15, dimension 6 and covering radius 3 cannot exist. This proof differs considerably from a geometry based proof by Simonis.

1. Introduction. In [1] a special improved back-tracking algorithm is used to prove the nonexistence of $[17, 6; (\mathrm{r} =)4]$, $[17, 8; (\mathrm{r} =)5]$, $[18, 7; (\mathrm{r} =)4]$, $[18, 7; (\mathrm{r} =)4]$, $[19, 7; (\mathrm{r} =)4]$, $[20, 8; (\mathrm{r} =)4]$ and $[21, 7; (\mathrm{r} =)5]$ codes. Here, $[n, k; (\mathrm{r} =)f]$ denotes a linear code with length n, dimension k and covering radius f (we enclose the "r" in brackets, to distinguish it from a variable r). However, the proofs presented in [1] were accomplished by making use of computer computations. In [4] the nonexistence of a $[15, 6; (\mathrm{r} =)3]$ code is proved, by applying "geometrically inspired arguments", like using hyperplanes, and also by applying the Mac Williams identities.

In this paper we shall give a proof based on the algorithm presented in [5, Chapter 3.2]. We remark that our result is also a corollary of [2]. By $C^\perp$ we denote the dual of a linear code C. This is the set of all binary vectors which are orthogonal to all codewords of C. It is well-known, that if C is an $[n, k]$ code, then $C^\perp$ is an $[n, n-k]$ code.

2. Preliminaries. Let C_0 be the set (linear code), consisting of all even codewords of length Δ. We shall denote by $q_\Delta(r)$ the minimal number of spheres – with center in C_0 and radius r – which cover all odd vectors, i.e all vectors in $GF(2)^\Delta$ which have an odd weight.

The following proposition holds.

Proposition 1. *Let C be an $[n, k; (\mathrm{r} =)r]$ code, and let $\mathbf{c} \in C^\perp$ be a codeword of weight Δ. Let H be the restriction of the generator matrix of C to the columns j, for which $c_j = 0$. Let $H^\perp$ be the generator matrix of the code dual to the code generated by the rows of H, and let $\mathbf{v} \in GF(2)^{n-\Delta-k}$ be any vector of length $n - \Delta - k$. If $\mathbf{v}$ cannot be presented as a sum of i columns (and if it can be presented as a sum of $i + 1$ columns) of $H^\perp$, then we can present $\mathbf{v}$ as a sum of at most $r - 1$ columns of $H^\perp$ in at least $q_\Delta(r - 1 - i)$ ways, $r \geq i + 1$, with $i \geq -1$, and where we define the empty sum as $\mathbf{0}$.*

The proof can be found in [5]. To apply this proposition we also need $q_\Delta(4) \geq 1; q_\Delta(3) \geq 1; q_\Delta(2) \geq 2; q_\Delta(1) \geq 2$.

*Partially supported by the Bulgarian NSF under Contract MM 1405/2004

Proposition 1 is a generalization of the following well-known property.(cf. [3, Theorem 2.1.9])

Proposition 2. *The $[n,k]$ code C has covering radius r, if and only if every vector from $GF(2)^{n-k}$ can be presented as a sum of at most r columns of a generating matrix of $C^{\perp}$.*

3. Proof of the nonexistence. We call the code generated by the matrix H in Proposition 1 a "residue" code, although strictly speaking a residue code is defined with respect to a codeword of C itself, whereas here $\mathbf{c}$ is taken from $C^{\perp}$.

Let us suppose that we have a $[15,6;(\mathrm{r}=)3]$ linear code C. First, we must find a minimal weight Δ of the code $C^{\perp}$. If $\Delta > 4$, $C^{\perp}$ is a $[15,9;(\mathrm{d}) \geq 5]$ linear code (which means, a linear code with minimal distance ≥ 5). Such a code does not exist. Let $\Delta < 4$. Then a (15×9)-generator matrix of the dual code can be presented in the form

$$T^{\perp} = \left(\begin{array}{c|c} \overbrace{11\ldots1}^{\Delta} & 00 \quad \ldots \quad 0 \\ \hline & \\ & \end{array} \right),$$

and from Proposition 2 we have that any vector $\mathbf{v} = (1\ \mathbf{v}_1\ \mathbf{v}_2 \ldots \mathbf{v}_8)^t$ can be presented as a sum of at most 3 columns of $T^{\perp}$. The total number of such vectors $\mathbf{v}$ is 256, while the number of all combinations of $t \leq 3$ vectors such that the first component equals 1 is:

$$\binom{\Delta}{3} + \Delta\left(\binom{15-\Delta}{2} + \binom{15-\Delta}{1} + \binom{15-\Delta}{0}\right).$$

But in case when $\Delta = 1, 2$ or 3, the above sum is less than 256, and we have contradiction.

It remains to consider the case $\Delta = 4$ (the most difficult case).

The following matrix appears to be a suitable generator matrix of C_{res} satisfying all conditions of Proposition 1

$$G(C_{\mathrm{res}}) = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

This matrix was found by computer search. However we are not going to use it. Instead, we start from a (9×15)-generator matrix of $C^{\perp}$ in the form

$$T^{\perp} = \left(\begin{array}{c|c} 0000 & \\ \vdots & H^{\perp} \\ 0000 & \\ \hline 1111 & 00\ldots0 \\ 0100 & \\ 0010 & G \\ 0001 & \end{array} \right), \tag{1}$$

Let us consider the (5×11)-matrix $H^{\perp}$. It is a generator matrix of the dual "residue" code of C. Let $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{11}$ be the columns of the matrix $H^{\perp}$ and let us (for convenience) define $\mathbf{h}_0 := \mathbf{0}$. For every vector $\mathbf{v} \in GF(2)^5$, we define

$$H_{\mathbf{v}} := \{(i,j) \mid 0 \le i < j \le 11,\ \mathbf{h}_i + \mathbf{h}_j = \mathbf{v}\}.$$

Let $\mathbf{0}_5$ be a column vector of height 5, which contains only zeros. Let us define the functions:

$$\mathcal{A}_2(\mathbf{v}) := \begin{cases} |H_{\mathbf{v}}|, & \mathbf{v} \neq \mathbf{0}_5, \\ 1 + |H_{\mathbf{v}}|, & \mathbf{v} = \mathbf{0}_5, \end{cases}$$

$$\mathcal{R}_2(\mathbf{v}) := \begin{cases} 2, & \mathbf{v} \neq \mathbf{0}_5, \\ 1, & \mathbf{v} = \mathbf{0}_5, \end{cases}$$

$$\mathcal{E}_2(\mathbf{v}) := \mathcal{A}_2(\mathbf{v}) - \mathcal{R}_2(\mathbf{v}).$$

We call these functions *all presentations* (giving the number of ways $\mathbf{v}$ can be presented as sum of 0, 1 or 2 columns of $H^\perp$), *required presentations* and *extra presentations* of vector $\mathbf{v}$. The last name is due to the inequality

$$\mathcal{E}_2(\mathbf{v}) \ge 0, \forall \mathbf{v} \in GF(2)^5, \tag{2}$$

which follows from Proposition 1 with $r = 3$ and $i = 1$ respectively $i = 0$ and from $q_4(2) \ge 2$, $q_4(1) \ge 2$.

Let us consider the sum

$$S(H) := \sum_{\mathbf{v} \in GF(2)^5} \mathcal{E}_2(\mathbf{v}).$$

This is the total number of extra presentations. For a putative $[15, 6; (\mathrm{r}) = 3]$ code C we can calculate this number $S = S(H)$ without knowing the specific structure of such a code (cf. Lemma 1). If we next can prove that such a C has more than S extra presentations, we can conclude that this C does not exists.

The first step is to calculate the exact value of $S(H)$.

Lemma 1.

$$S(H) = 4$$

Proof. We have

$$S(H) = \sum_{\mathbf{v} \in GF(2)^5} \mathcal{E}_2(\mathbf{v}) = \sum_{\mathbf{v} \in GF(2)^5} (\mathcal{A}_2(\mathbf{v}) - \mathcal{R}_2(\mathbf{v}))$$

$$= 1 + |\{(i,j) \mid 0 \le i, j \le 11,\ i \neq j\}| - \sum_{\mathbf{v} \in GF(2)^5} \mathcal{R}_2(\mathbf{v})$$

$$= 1 + \binom{12}{2} - (2.2^5 - 1) = 4 \qquad \square$$

To prove the nonexistence, we consider the generator matrix $T^\perp$ (cf. (1)). We label the columns of $H^\perp$ as $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{11}$, as before, and the columns of G as $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_{11}$. We assume that $\mathbf{h}_0 := \mathbf{0}_5$ and $\mathbf{g}_0 = \mathbf{0}_3$.

Furthermore, we define the property

$$P_{i,j,k,l} \Leftrightarrow \mathbf{h}_i + \mathbf{h}_j + \mathbf{h}_k + \mathbf{h}_l = \mathbf{0}_5 \ \wedge\ \mathbf{g}_i + \mathbf{g}_j + \mathbf{g}_k + \mathbf{g}_l \neq \mathbf{1}_3$$

for $i, j, k, l \in \{0, 1, \ldots, 11\}$.

Lemma 2. *If for* $\mathbf{v} \in GF(2)^5 \backslash \{\mathbf{0}\}$ *we have* $\mathcal{E}_2(\mathbf{v}) = 0$*, which implies*

$$\mathbf{v} = \mathbf{h}_i + \mathbf{h}_j \text{ and } \mathbf{v} = \mathbf{h}_k + \mathbf{h}_l,\ \{i,j\} \neq \{k,l\},$$

then $\mathbf{g}_i + \mathbf{g}_j + \mathbf{g}_k + \mathbf{g}_l = \mathbf{1}_3$.

Proof. From Proposition 2 we have that each vector of length 9 can be presented as a sum of at most three column vectors of $T^\perp$. Let us consider the vector $(\mathbf{v}\ 1\ 0\ 0\ 0)^t$. This vector can be presented as a sum of two columns $\alpha = (\mathbf{h}_i\ 0\ \mathbf{g}_i)$ and $\beta = (\mathbf{h}_j\ 0\ \mathbf{g}_j)$ and one column γ from the first four columns of $T^\perp$.

Let $\alpha + \beta = (\mathbf{v}\ 0\ \mathbf{u})^t$. Choosing various γ, we can cover a subset S' of $S = \{(\mathbf{v}1\boldsymbol{a}) \mid \boldsymbol{a} \in GF(2)^3\}$, and thus the corresponding $\boldsymbol{a}$ are contained in a sphere with center $\mathbf{u}$ and radius 1. As it can be easily seen, the remaining vectors of $GF(2)^3$, which correspond to $S \backslash S'$, can be covered by a sphere of radius 1 if and only if the center of this sphere is $\mathbf{1}_3 + \mathbf{u}$.

Thus, from the second representation of $\mathbf{v} = \mathbf{h}_k + \mathbf{h}_l$ it follows $\mathbf{g}_k + \mathbf{g}_l = \mathbf{g}_i + \mathbf{g}_j + \mathbf{1}_3$. $\square$

Lemma 3. *If for some vector* $\mathbf{v}$ *we have* $\mathcal{E}_2(\mathbf{v}) > 0$*, i.e.*

$$\mathbf{v} = \mathbf{h}_i + \mathbf{h}_j = \mathbf{h}_k + \mathbf{h}_l = \mathbf{h}_m + \mathbf{h}_n, \{i,j\} \neq \{h,l\} \neq \{m,n\},$$

then $P_{i,j,k,l}$ *or* $P_{i,j,m,n}$ *or* $P_{k,l,m,n}$.

Proof. If we suppose that all P. are false, then from Lemma 2 we have

$$\mathbf{g}_i + \mathbf{g}_j + \mathbf{g}_k + \mathbf{g}_l = \mathbf{1}_3,\ \mathbf{g}_i + \mathbf{g}_j + \mathbf{g}_m + \mathbf{g}_n = \mathbf{1}_3,\ \mathbf{g}_k + \mathbf{g}_l + \mathbf{g}_m + \mathbf{g}_n = \mathbf{1}_3,$$

but this is impossible, since the sum of all left-hand sides is zero. $\square$

Lemma 4. $P_{i,j,k,l}$ *implies* $\mathcal{E}_2(\mathbf{h}_i + \mathbf{h}_j) > 0$, $\mathcal{E}_2(\mathbf{h}_i + \mathbf{h}_k) > 0$ *and* $\mathcal{E}_2(\mathbf{h}_i + \mathbf{h}_l) > 0$.

Proof. From the definition of the P., we have that $\mathbf{h}_i + \mathbf{h}_j = \mathbf{h}_k + \mathbf{h}_l$. If for example $\mathcal{E}_2(\mathbf{h}_i + \mathbf{h}_j) = 0$, then from Lemma 2 it follows that $\mathbf{g}_i + \mathbf{g}_j + \mathbf{g}_k + \mathbf{g}_l = \mathbf{1}_3$. This contradicts the definition of the property P. . $\square$

Lemma 5. *If* $H^\perp$ *is in standard form, then a submatrix which contains exactly* 2 *lines, must be of the form, up to permutations of the columns,*

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \mathbf{d}_1\ \mathbf{d}_1\ \mathbf{d}_1\ \mathbf{d}_2\ \mathbf{d}_2\ \mathbf{d}_3\ \mathbf{d}_3 \\ 0 & 0 & 0 & 0 & \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \mathbf{d}_1\ \mathbf{d}_1\ \mathbf{d}_2\ \mathbf{d}_2\ \mathbf{d}_3\ \mathbf{d}_3 \\ 0 & 0 & 0 & 0 & 0 & \end{pmatrix},$$

where $\mathbf{d}_1, \mathbf{d}_2, \mathbf{d}_3$ *are the nonzero vectors of the vector space* $GF(2)^2$.

Proof. Let us assume, that the submatrix consists of the last two rows of $H^\perp$. The first step is to calculate the number of all sums of 0, 1 or 2 column vectors, ending at two zeros, or at some $\mathbf{d}_i$. Suppose we have a_0 vectors ending at $\mathbf{0}_2$, and a_i vectors ending at $\mathbf{d}_i$, $i = 1, 2, 3$, in matrix $T^\perp$ (cf. (1)). Then we have

$$n_0 := 1 + a_0 + \sum_{i=0}^{3} \frac{a_i(a_i - 1)}{2} \text{ combinations yielding } \mathbf{0}_2,$$

and

$$n_i := a_i + a_i a_0 + a_j a_k \text{ combinations yielding } \mathbf{d}_i,$$

where $\{i, j, k\} \equiv \{1, 2, 3\}$ in the last relation.

From Proposition 1 and Lemma 1 it follows that $15 \le n_0 \le 19$ and $16 \le n_i \le 20$, for $i \in \{1, 2, 3\}$. In the next table we consider all possibilities for the combinations a_0, a_i, a_j, a_k, and we indicate when some value of n gives a contradiction (remember that $a_0 \ge 3$, since $H^\perp$ is in standard form).

a_0	a_i	a_j	a_k		a_0	a_i	a_j	a_k		a_0	a_i	a_j	a_k	
3	3	3	2	$n_0 = 14$	4	3	2	2		5	3	2	1	$n_k = 12$
3	4	3	1		4	3	3	1	$n_k = 14$	5	4	$*$	$*$	$n_i = 24$
3	4	2	2	$(n_i = 20)$	4	4	2	1	$n_k = 13$	6	$*$	$*$	$*$	$n_0 = 21$
3	5	$*$	$*$	$n_i > 20$	5	2	2	2						

The case $(3,4,3,1)$ must be considered separately. It can be treated similarly as filling the matrices, at the end of this proof (cf. [5]). The case $(3,4,2,2)$ is impossible, since from Lemmas 1,3 and 4 it follows that there exist three column vectors with extra presentations the sun of which must be equal to $\mathbf{0}_5$. $\square$

Proposition 3. *A linear* $[15, 6; (\mathrm{r}=)3]$ *code does not exist.*

Proof. First, we consider the case when we have an extra presentation ($\mathcal{E}_2(\mathbf{v}) > 0$) only for the zero vector $\mathbf{v} = \mathbf{0}$. Then we choose four vectors $\mathbf{h}_i$, $\mathbf{h}_j$, $\mathbf{h}_k$, $\mathbf{h}_l$ such that $\mathbf{h}_i = \mathbf{h}_j$, $\mathbf{h}_k = \mathbf{h}_l$, and $\mathbf{h}_i + \mathbf{h}_k \neq 0$, $\mathcal{E}_2(\mathbf{v}_1 + \mathbf{v}_2) \geq 2$. Contradiction.

From Lemma 3, the condition $P_{i,j,k,l}$ is satisfied for some i, j, k, l. We assume w.l.g. that $i = 1$, $j = 2$, $k = 3$, $l = 4$. From the definition of $P_{\cdot,\cdot,\cdot,\cdot}$, we have $\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 + \mathbf{h}_4 = 0$. The generator matrix $H^{\perp}$ can be converted by changing the basis, such that if in the last equation we have 4, 3 or 2 different nonzero vectors $\mathbf{h}_i$, then the left part of $H^{\perp}$ is equal to

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \text{ respectively.}$$

We treat the first two cases simultaneously. It is easy to show, that if in the first submatrix we replace 1 in position $(1,4)$ by 0, then we obtain the submatrix corresponding to the second case, applying again basis changings.

From Lemmas 3 and 4, we have that any of the vectors $\mathbf{v}_1 = (110\,00)^t$, $\mathbf{v}_2 = (011\,00)^t$ and $\mathbf{v}_3 = (101\,00)^t$ can be presented as a sum of at most 2 columns, one of which is not from $\{\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \mathbf{h}_4\}$. Let these presentations be

$$\mathbf{v}_1 = \mathbf{h}_{w_1} + \mathbf{h}_{u_1} \ \mathbf{v}_2 = \mathbf{h}_{w_2} + \mathbf{h}_{u_2} \ \mathbf{v}_3 = \mathbf{h}_{w_3} + \mathbf{h}_{u_3},$$

where $w_i \geq 5$, and $u_i \geq 0$.

The only posibilities are: 1. $w_1 = w_2$, and $\mathbf{h}_{w_1}$ ends at $(00)^t$, 2. $w_1 = w_2$ and $\mathbf{h}_{w_1}$ does not end at $(00)^t$ and 3. $w_1 \neq w_2 \neq w_3 \neq w_1$.

It is not possible that all w_i be different, since two of the corresponding $\mathbf{h}_{w_i}$ must end at $(00)^t$, and, hence, we would have 6 columns ending at $(00)^t$ (a contradiction to Lemma 5). With similar arguments we prove, that the situation when all vectors $\mathbf{h}_{w_1}, \mathbf{h}_{u_1}, \mathbf{h}_{w_2}, \mathbf{h}_{u_2}$ are different, and two of them end at $(00)^t$, is impossible.

If some $\mathbf{h}_{w_i}$ does not end at $(00)^t$, then we can apply a suitable operation (a changing of the basis) to convert it to the vector $(00010)^t$. We can also apply similar operations, to convert the matrix in standard form, but preserving the vectors $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3$. Finally, we can fill in the last 2 rows, according to Lemma 5 (it determines how many vectors can end at 00, 01, 10 or 11). We consider four cases (without any subcases), to complete the proof. The arguments are simple, but they will not be presented here. For more details we refer to [5, Section 3.2/5]. □

REFERENCES

[1] T. Baicheva, V. Vavrek. On the least covering radius of binary linear codes with small lengths. *IEEE Trans. Info. Theory*, **49**, *3* (2003), 738–740.
[2] S. Bouyuklieva. The minimal covering radius of [16, 7] codes. *Annuaire de l'Univ. Sofia*, 1988.
[3] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein. Covering Codes. Amsterdam, The Netherlands: Elsevier Science B.V, North-Holland, 1997.
[4] J. Simonis. The minimal covering radius $t[15, 6]$ of a six-dimensional binary linear code of length 15 is equal to 4. *IEEE Trans. Info. Theory*, **34**, *5* (1988), 1344-1345.
[5] V. V. Vavrek. Ph.D. thesis, in preparation.

Department of Mathematics
Faculty of Information Theory and Systems
Delft University of Technology
P.O. BOX 5031, 2600 GA Delft, The Netherlands
e-mail: V.Vavrek@ewi.tudelft.nl

НОВО ДОКАЗАТЕЛСТВО НА НЕСЪЩЕСТВУВАНЕТО НА [15, 6; (r =)3] КОД

Веселин Вл. Ваврек

Доказанео е несъществеването на линеен код с дължина 15,, размерност 6 и радиус на покритие 3. Това доказателство се различава съществено от това на Симонис използващо геометрични аргументи.