Five New Optimal [34,15,9] Codes

P. Farkaš,

Dept. of Telecommunications, Faculty of Electrical Eng. and Information Technology, Slovak University of Technology, Ilkovicova 3, 812 19 Bratislava, SLOVAKIA,
and
SWH s. r. o. , Stromova 9, P. O. Box 93, 837 93 Bratislava, SLOVAKIA
p.farkas@ieee.org

Abstract: This paper presents five new [34,15,9] binary linear block code which reach the upper bound in [1] for best known codes with different spectra as the known [34,15,9] codes constructed by Hashim and Constantinides [2] and Farkas [5-8] and [10-11].

Keywords: Block codes, Hamming distance, weight spectrum, generator matrix**.**

1. Introduction

The question concerning the existence of good error control codes belongs to the most important in communication theory. A short introduction into the theory of error control code could be found in [9]. We now give only an extract from that theory. The linear block code is a *k*-dimensional subspace of an *n*-dimensional vector space over finite field. Therefore all codewords of the code are linear combinations of *k* linearly independent vectors - the so-called basis vectors. One compact description of a linear block code is by the generator matrix **G**. The rows of generator matrix are the basis vectors that span the space of all codewords. Therefore it is obvious, that the generator matrix has *k* rows and *n* columns and also that the same code could have many different generator matrices. All codewords ***c*** could be obtained by multiplication of the so called information vector ***i*** and the **G** matrix:

$$\boldsymbol{c} = \boldsymbol{i}\mathbf{G}$$

Equivalent codes in strict sense are codes obtained by elementary row operations in **G**. Elementary row operations are:

1. Exchange of two rows,
2. addition of one row to another row,
3. multiplication of a row by a scalar.

Hamming distance between two vectors is defined as the number of different coordinates of the two vectors. For example the Hamming distance between ***u*** = (110110) and ***v*** = (011100) is $d(\boldsymbol{u},\boldsymbol{v}) = 3$. The Hamming distance of codewords is closely related to the error control capability of the code. We could suppose that the two vectors ***u*** and ***v*** in our example are two codewords of some code with only two codewords. Than we can observe that at least 3 errors must occur in ***u*** to change it into ***v***. If only one error in ***u*** will occur the corrupted vector will be closer to ***u*** than to ***v*** in therms of Hamming distance in all cases. Therefore the decoder will be able (after receiving the corrupted vector) to select the closest codeword vector ***u*** in other words the decoder will be able to correct all single errors in any of the codewords. Such a strategy is often using for decoding. In more general case the error control capability of a code is dependent of the minimal Hamming distance between any two codewords of the code- the *code distance*. Let us denote *n* the code-word length, k the number of information symbols and *d* the code-distance of a code. If two codes have the same value *n* and identical value *k* the code with greater value *d* is classified as better, because these code has greater error control capability by the same redundancy which is defined as $r = n - k$. The lower and upper bounds on $d(n,k)$, the maximum possible Hamming-distance of some linear binary block codes can be found in table in [1]. An interactive interface to the lower and upper bounds on $d(n,k)$ of some linear binary, ternary and quadruple block codes can be found on: http://www.win.tue.nl/win/math/dw/voorlicod.html

To show, that codes with the same parameters *n, k, and d* aren't equivalent, it is necessary to find they weight spectra. The code weight spectrum can be given by a set of constants a_i, which represent the number of code words with the Hamming-weight *i*. The Hamming weight of a code word from a linear binary code is equal to the number of ones in this code word. The [*n,k,d*] codes with different weight spectra are not equivalent. The generator matrix of any linear block code could be brought to a systematic form by elementary row operations. The systematic form is such a form that the encoded information is explicitly visible in all codewords. The **G** matrix in systematic form has at least *k* columns with single one in each of those columns at different position (in different rows). One possible systematic form could be described by expressing the generator matrix **G** using two submatrices:

G = [**I P**],

where **I** is an identity matrix and **P** is the so-called parity matrix of the code. In the following section we present generator matrices and weight spectra of the known and five new [34,15,9] codes, which reach the upper bound for *d(n,k)* in [1]. In conclusion we give some remarks.

2. New Codes

Hashim and Constantinides had constructed the first [34,15,9] Code [2], Farkaš in [5-8] found other [34,15,9]. In this paper five different new codes are presented, which where found using computerized search. The searching method was based on one variation of the known algorithm [3], described in [4]. The search was realized on the super computer Fujitsu VP 2600/20.

The [34,15,9] Hashim, Constantinides code [2] has the following parity matrix:

$$\mathbf{P} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&0&0&1&0&0&1&0&1&1&0&0&1&1&0&1&0&1&0\\
0&0&1&0&0&0&1&0&1&1&1&1&0&0&1&1&0&0&0\\
1&0&0&0&0&1&0&0&1&1&0&1&1&0&0&0&1&0&1\\
1&1&0&0&1&0&0&0&0&1&1&0&1&0&0&1&1&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0&0&1\\
0&1&0&1&0&1&0&0&0&1&0&0&0&1&0&1&1&0&1\\
0&1&1&1&0&1&0&1&0&0&1&1&0&0&0&1&1&1&0\\
1&0&0&1&0&1&0&1&1&0&0&0&1&0&0&0&1&0&1\\
1&1&0&0&1&1&1&0&1&0&1&1&1&1&0&1&0&0&1\\
1&1&1&1&1&0&1&0&1&0&0&1&0&0&0&0&0&1&0
\end{bmatrix}$$

and the weight spectrum:
$a_0 = 1$, $a_9 = 140$, $a_{10} = 340$, $a_9 = 530$, $a_{12} = 1018$, $a_{13} = 1705$, $a_{14} = 2562$, $a15 = 3552$, $a_{16} = 4271$, $a_{17} = 4588$, $a_{18} = 4226$, $a_{19} = 3412$, $a_{20} = 2642$, $a_{21} = 1790$, $a_{22} = 1030$, $a_{23} = 560$, $a_{24} = 256$, $a_{25} = 96$, $a_{26} = 34$, $a_{27} = 10$, $a_{28} = 4$, $a_{29} = 1$.

Now the five new codes and their weight spectra are presented

1.

$a_0 = 1$, $a_9 = 141$, $a_{10} = 346$, $a_9 = 522$, $a_{12} = 999$, $a_{13} = 1712$, $a_{14} = 2579$, $a_{15} = 3591$, $a_{16} = 4264$, $a_{17} = 4497$, $a_{18} = 4251$, $a_{19} = 3471$, $a_{20} = 2601$, $a_{21} = 1803$, $a_{22} = 1049$, $a_{23} = 533$, $a_{24} = 259$, $a_{25} = 102$, $a_{26} = 31$, $a_{27} = 11$, $a_{28} = 4$, $a_{29} = 1$.

$$\mathbf{P} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&0&0&1&0&0&1&0&1&1&0&0&1&1&0&1&0&1&0\\
0&0&1&0&0&0&1&0&1&1&1&1&0&0&1&1&0&0&0\\
1&0&0&0&0&1&0&0&1&1&0&1&1&0&0&0&1&0&1\\
1&1&0&0&1&0&0&0&0&1&1&0&1&0&0&1&1&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0&0&1\\
0&1&0&1&0&1&0&0&0&1&0&0&0&1&0&1&1&0&1\\
0&1&1&1&0&1&0&1&0&0&1&1&0&0&0&1&1&1&0\\
1&0&0&1&0&1&1&0&0&0&1&1&0&1&0&1&1&1&1\\
1&1&1&0&1&1&0&0&1&0&1&1&0&1&0&0&0&1&0\\
1&1&1&1&1&0&1&1&1&0&0&0&0&0&1&0&0&1&0
\end{bmatrix}$$

2.

$a_0 = 1$, $a_9 = 143$, $a_{10} = 347$, $a_9 = 523$, $a_{12} = 988$, $a_{13} = 1690$, $a_{14} = 2618$, $a_{15} = 3624$, $a_{16} = 4203$, $a_{17} = 4486$, $a_{18} = 4288$, $a_{19} = 3478$, $a_{20} = 2610$, $a_{21} = 1772$, $a_{22} = 1030$, $a_{23} = 560$, $a_{24} = 260$, $a_{25} = 99$, $a_{26} = 37$, $a_{27} = 7$, $a_{28} = 2$, $a_{29} = 2$.

$$\mathbf{P} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&0&0&1&0&0&1&0&1&1&0&0&1&1&0&1&0&1&0\\
0&0&1&0&0&0&1&0&1&1&1&1&0&0&1&1&0&0&0\\
1&0&0&0&0&1&0&0&1&1&0&1&1&0&0&0&1&0&1\\
1&1&0&0&1&0&0&0&0&1&1&0&1&0&0&1&1&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0&0&1\\
0&1&0&1&0&1&0&0&0&1&0&0&0&1&0&1&1&0&1\\
0&1&1&1&0&1&0&1&0&0&1&1&0&0&0&1&1&1&0\\
1&0&0&1&0&1&1&0&1&0&0&1&0&1&1&0&0&1&0\\
1&1&0&0&1&1&0&0&1&0&0&0&1&1&0&0&0&0&1\\
1&1&1&1&1&1&0&1&1&1&1&0&0&0&0&1&0&0&1
\end{bmatrix}$$

3.

a_0= 1, a_9= 145, a_{10}= 339, a_9= 513, a_{12}= 1024, a_{13}= 1719, a_{14}= 2554, a_{15}= 3562, a_{16}= 4263, a_{17}= 4572, a_{18}= 4248, a_{19}= 3412, a_{20}= 2638, a_{21}= 1792, a_{22}= 1014, a_{23}= 566, a_{24}= 264, a_{25}= 91, a_{26}= 37, a_{27}= 11, a_{28}= 2, a_{29}= 1.

$$\mathbf{P} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&0&0&1&0&0&1&0&1&1&0&0&1&1&0&1&0&1&0\\
0&0&1&0&0&0&1&0&1&1&1&1&0&0&1&1&0&0&0\\
1&0&0&0&0&1&0&0&1&1&0&1&1&0&0&0&1&0&1\\
1&1&0&0&1&0&0&0&0&1&1&0&1&0&0&1&1&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0&0&1\\
0&1&0&1&0&1&0&0&0&1&0&0&0&1&0&1&1&0&1\\
0&1&1&1&0&1&0&1&0&0&1&1&0&0&0&1&1&1&0\\
1&0&0&1&0&1&1&0&1&0&0&1&0&1&1&0&0&1&0\\
1&1&0&0&1&1&0&0&1&0&0&0&1&1&0&0&0&0&1\\
1&1&1&1&1&1&0&1&1&1&1&0&0&0&0&1&0&0&1
\end{bmatrix}$$

4.

a_0= 1, a_9= 141, a_{10}= 355, a_9= 517, a_{12}= 984, a_{13}= 1709, a_{14}= 2571, a_{15}= 3632, a_{16}= 4271, a_{17}= 4450, a_{18}= 4292, a_{19}= 3482, a_{20}= 2550, a_{21}= 1794, a_{22}= 1068, a_{23}= 552, a_{24}= 256, a_{25}= 97, a_{26}= 33, a_{27}= 9, a_{28}= 2, a_{29}= 1.

$$\mathbf{P} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&0&0&1&0&0&1&0&1&1&0&0&1&1&0&1&0&1&0\\
0&0&1&0&0&0&1&0&1&1&1&1&0&0&1&1&0&0&0\\
1&0&0&0&0&1&0&0&1&1&0&1&1&0&0&0&1&0&1\\
1&1&0&0&1&0&0&0&0&1&1&0&1&0&0&1&1&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0&0&1\\
0&1&0&1&0&1&0&0&0&1&0&0&0&1&0&1&1&0&1\\
0&1&1&1&0&1&0&1&0&0&1&1&0&0&0&1&1&1&0\\
1&0&0&1&0&1&1&0&1&0&1&1&1&1&0&0&0&1&1\\
1&0&1&0&1&1&1&1&1&1&0&0&1&0&1&1&1&1&1\\
1&1&0&1&1&1&0&1&0&1&0&0&1&1&0&0&0&0&0
\end{bmatrix}$$

5.

a_0= 1, a_9= 141, a_{10}= 337, a_9= 534, a_{12}= 1036, a_{13}= 1668, a_{14}= 2526, a_{15}= 3644, a_{16}= 4291, a_{17}= 4478, a_{18}= 4248, a_{19}= 3472, a_{20}= 2610, a_{21}= 1796, a_{22}= 1042, a_{23}= 532, a_{24}= 252, a_{25}= 109, a_{26}= 39, a_{27}= 10, a_{28}= 2.

$$\mathbf{P} = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0
\end{bmatrix}$$

3. Conclusion

It is known that from the codes, which we found other new [34,15,10] codes could be constructed by adding overall parity check to each code word. This paper shows, that more linear binary codes exists, which reach the lower bound d (34,15) = 9. We can not guaranty, that we found all linear binary [34,15,9] codes and therefore the question how much such codes exist remains open.

4. Acknowledgement

The work was supported by Scientific Grant Agency of Ministry of Education of Slovak Republic and Slovak Academy of Sciences, Commission VEGA, no. 1/7615/20. The author wants to express thanks also to SWH s. r. o. for additional support of the work.

References

[1] Brouwer, A. E., Verhoeff, T.: An Updated Table of Minimum - Distance Bounds for Binary Linear Code. In: IEEE Trans. Inform. Theory, IT-39, 1993, no. 2, pp. 662-677.

[2] Hashim, A., A., Constantinides, A. G.: Some new results on binary linear block codes. Electronic Letters, vol. 10, no. 3, 1974, pp. 31-33.

[3] Farkaš, P., Smirnov, A. S., Sotskov, J. V.: Lineárne kódy opravujúce mnohonásobné chyby. In: Informacné systémy, vol. 14, 1986, no. 5, pp. 533-542.

[4] Farkaš, P., Bruehl, K.: Three Best Binary Linear Block Codes of Minimum Distance Fifteen. In: IEEE Trans. on Inform. Theory, IT-40, 1994, no. 3, pp. 949-951.

[5] Farkaš, P.: Weight spectra of some new best error control codes. In: Proc. of Radioelectronics'94, FEI TU Košice, 27. 9. - 28. 9. 1994, Kosice, pp. 135-140.

[6] Farkaš P.: Four new best [34,15,9] codes. JEE, vol. 46, no. 2, 1995, pp. 73-74.

[7] Farkaš, P.: Another two new best [34,15,9] codes. In: Proc. of the conference ELEKTRO'95, EF VSD Žilina, 7. 2. - 8. 2. 1995, pp. 244-247.

[8] Farkaš, P.: Six new [34,15,9] codes and their spectra. In: Proc. of ISCTA'95, Ambleside, UK, 10. 7. -14. 7. 1995, pp. 37- 40.

[9] Clark, G. C., Jr., Cain, J. B.: Error-correction coding for digital communications, Plenum, New York, 1981.

[10] Farkas, P.: Seven New Optimal [34,15,9] Codes. Accepted for publication in JEE-Journal of Electrical Eng., vol. 52, no. 7-8, 2001, pp.234-236.

[11] Farkas, P.: Three New Optimal [34,15,9] Codes.In Proc. of: RTT'2001-International Conference - Research in Telecommunication Technology, September 24-26, 2001 Brno, Lednice, Czech Republic, pp. 10-13.