Peter Farkaš - Sergio Herrera-Garcia *

DVA NOVÉ NAJLEPŠIE KÓDY [27,10,9]

TWO NEW BEST [27,10,9] CODES

V tomto príspevku sú zverejnené dva nové lineárne binárne blokové kódy [27,10,9], ktoré dosahujú hornú hranicu pre kódovú vzdialenosť najlepších kódov [1]. Nové kódy sa vyznačujú rozdielnymi váhovými spektrami v porovnaní s doteraz zverejnenými kódmi [27,10,9] skonštruovanými Piretom [2], Farkašom a Julingom [5].

Kľúčové slová: *Blokový kód, Hammingova vzdialenosť, váhové spektrum, generujúca matica.*

This paper presents two new [27,10,9] binary linear block codes which reach the upper bound in [1] for best known codes. They have different spectra as the known [27,10,9] codes constructed by Piret [2], Farkaš and Juling [5].

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

1. Úvod

Otázka existencie dobrých samoopravných kódov patrí k najdôležitejším otázkam *Teórie komunikácie.* Označme n dĺžku kódového slova, k počet informačných symbolov v kódovom slove a d minimálnu Hammingovu vzdialenosť medzi dvoma kódovými slovami v kóde - *kódovú vzdialenosť.* Uvedené základné hodnoty sa štandardne zapisujú vo forme [n, k, d]. Ak majú dva kódy rovnaké hodnoty n a k, tak za lepší kód sa považuje ten, ktorý má väčšiu hodnotu d. Je to preto, že takýto kód dokáže pri tej istej nadbytočnosti a dĺžke kódového slova ochrániť lepšie prenášanú alebo uchovávanú informáciu. Dolná a horná hranica pre kódovú vzdialenosť ako v závislosti od n a k - $d(n,k)$, sa dá nájsť pre niektoré hodnoty v [1].

Interaktívny prístup k dolným a horným hraniciam $d(n,k)$ pre binárne a nebinárne kódy je možný prostredníctvom: *http://www.win.tue.nl/win/math/dw/voorlicod.html*

V nasledujúcej časti uvedieme generujúce matice a váhové spektrá známeho Piretovho kódu a dvoch nových [27,10,9] kódov, ktoré dosahujú hornú hranicu pre d(n,k) v [1]. V závere sú uvedené niektoré poznámky.

2. Nové kódy

P. Piret v [2] skonštruoval prvý [27,10,9] kód. Nám sa podarilo nájsť iné [27,10,9] kódy. Naša metóda hľadania bola založená na jednej modifikácii známeho postupu z [3], ktorá je opísaná v [4]. Pre vyhľadávanie bol využitý superpočítač Fujitsu VP 2600/20.

Na dôkaz, že kódy, ktoré sa vyznačujú totožnými parametrami n, k, d nie sú zhodné je potrebné určiť ich váhové spektrá. Váhové spektrum je možné opísať ako množinu konštánt a_i, ktoré udávajú počet slov s Hammingovou váhou i. Hammingova váha

1. Introduction

The question concerning the existence of good error control codes belongs to the most important in Communication theory. Let us denote n the codeword length, k the number of information symbols and d the Hamming-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 this code has greater error control capability by the same redundancy.

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*

In the following section we present generator matrices and weight spectra of the known and two new [27,10,9] codes, which reach the upper bound for d(n,k) in [1]. In conclusion we give some remarks.

2. New Codes

Piret [2] has constructed the first [27,10,9] Code [2]. We found other [27,10,9] codes. Our 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.

To show that codes with the same parameters n, k, d aren't equivalent, it is necessary to find their 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-

* **Peter Farkaš[1], Sergio Herrera-Garcia[2]**
[1]Department of Telecommunications, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, SK-812 19 Bratislava, Slovak Republic, E-mail: p.farkas@ieee.org
[2]CITEDI-IPN Research Center and CONACyT 2498 Roll Dr. # 757 Otay Mesa, San Diego, CA 92154

kódového slova je definovaná ako počet nenulových súradníc v tomto kódovom slove. Kódy [n,k,d] s rôznymi váhovými spektrami sú rozdielne.

Piretov kód [27,10,9] z [2] má nasledujúcu generujúcu maticu a ako váhové spektrum:

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 [27,10,9] Piret code [2] has the following generator matrix and weight spectrum:

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

Váhové spektrum kódu:

$a_0 = 1$ $a_9 = 56$ $a_{10} = 99$ $a_{11} = 90$ $a_{12} = 129$
$a_{13} = 144$ $a_{14} = 126$ $a_{15} = 132$ $a_{16} = 117$ $a_{17} = 72$
$a_{18} = 31$ $a_{19} = 18$ $a_{20} = 9$

Weight spectrum of the code:

$a_0 = 1$ $a_9 = 56$ $a_{10} = 99$ $a_{11} = 90$ $a_{12} = 129$
$a_{13} = 144$ $a_{14} = 126$ $a_{15} = 132$ $a_{16} = 117$ $a_{17} = 72$
$a_{18} = 31$ $a_{19} = 18$ $a_{20} = 9$

Nové kódy [27,10,9] majú nasledujúce generujúce matice a spektrá:

1.

The new [27,10,9] codes have the following generator matrices

1.

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

váhové spektrum kódu:

$a_0 = 1$ $a_9 = 54$ $a_{10} = 99$ $a_{11} = 99$ $a_{12} = 128$
$a_{13} = 129$ $a_{14} = 131$ $a_{15} = 142$ $a_{16} = 107$ $a_{17} = 72$
$a_{18} = 41$ $a_{19} = 15$ $a_{20} = 4$ $a_{21} = 1$ $a_{22} = 1$

and weight spectra:

$a_0 = 1$ $a_9 = 54$ $a_{10} = 99$ $a_{11} = 99$ $a_{12} = 128$
$a_{13} = 129$ $a_{14} = 131$ $a_{15} = 142$ $a_{16} = 107$ $a_{17} = 72$
$a_{18} = 41$ $a_{19} = 15$ $a_{20} = 4$ $a_{21} = 1$ $a_{22} = 1$

2.

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

váhové spektru kódu:

$a_0 = 1$ $a_9 = 53$ $a_{10} = 100$ $a_{11} = 104$ $a_{12} = 124$
$a_{13} = 119$ $a_{14} = 136$ $a_{15} = 152$ $a_{16} = 107$ $a_{17} = 67$
$a_{18} = 36$ $a_{19} = 16$ $a_{20} = 8$ $a_{21} = 1$

3. Záver

Je známe, že z kódov, ktoré sme našli a zverejnili v tomto článku, je možné skonštruovať dva ďalšie optimálne kódy [27,10,10] pridaním jedného paritného bitu ku každému kódovému slovu. Doteraz bolo publikovaných deväť kódov, ktoré dosahujú hranicu d (27,10) = 9. Otázka, či existujú ďalšie optimálne kódy s rovnkými parametrami, ostáva otvorená.

Poďakovanie
Autori chcú vyjadriť vďaku CITEDI-IPN Research Center and CONACyT Mexico, ďalej prof. Dieterovi Hauptovi z RWTH Aachen a DAAD za podporu tejto práce a Dr. Klausovi Bruehlovi z Výpočtového strediska RWTH Aachen za napísanie programov potrebných k vyhľadávaniu kódov.

Recenzenti: P. Krajčí, M. Brezňan

2.

and weight spectra:

$a_0 = 1$ $a_9 = 53$ $a_{10} = 100$ $a_{11} = 104$ $a_{12} = 124$
$a_{13} = 119$ $a_{14} = 136$ $a_{15} = 152$ $a_{16} = 107$ $a_{17} = 67$
$a_{18} = 36$ $a_{19} = 16$ $a_{20} = 8$ $a_{21} = 1$

3. Conclusion

It is known that from the codes we found two other new [27,10,10] codes could be constructed by adding overall parity check to each code word. This paper shows, that minimum nine linear binary codes exist, which reach the lower bound d (27,10) = 9. We cannot guarantee, that we found all linear binary [27,10,9] codes and therefore the question how many such codes exist remains open.

Acknowledgement
The authors want to express their thanks to CITEDI-IPN Research Center and CONACyT Mexico and as well to Prof. Dieter Haupt RWTH Aachen and the DAAD for supporting this work and Dr. Klaus Bruehl from the computing center of RWTH Aachen for writing the software needed for the search.

Reviewed by: P. Krajčí, M. Brezňan

Literatúra - 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] PIRET, P.: Good linear codes of lengths 27 and 28. In: IEEE Trans. on Inform. Theory, IT-26, 1980, pp. 227.
[3] FARKAŠ, P., SMIRNOV, A. S., SOTSKOV, J. V.: Lineárne kódy opravujúce mnohonásobné chyby. In: Informačné 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, JULING W.: Five New Best [27,10,9] Codes. In: International Journal of Electronics and Communications, (AEU), vol. 48, 1994, no. 2, pp. 115-116.