Two New Four-Error-Correcting Binary Codes

Patric R. J. Östergård*

Department of Electrical and Communications Engineering

Helsinki University of Technology

P.O. Box 3000, 02015 HUT, Finland

E-mail: patric.ostergard@hut.fi

Abstract

Two four-error-correcting binary codes of length 21 and 22 and of cardinality 64 and 80, respectively, are constructed. The codes consist of a union of cosets of linear codes with dimension 3 and were found by a maximum clique algorithm.

*The research was supported in part by the Academy of Finland under Grants No. 100500 and No. 202315.

Keywords: error-correcting code, maximum clique problem

1 Introduction

The maximum cardinality of a binary code of length n and minimum distance d is denoted by $A(n, d)$. For a recent table of exact values and bounds on this function for small n, see [1]. In this note, we present codes proving the lower bounds $A(21, 9) = A(22, 10) \geq 64$ and $A(22, 9) = A(23, 10) \geq 80$; previously it has been known that $50 \leq A(21, 9) \leq 87$ and $76 \leq A(22, 9) \leq 150$, where the lower bounds are from [4] and the upper bounds are from [9] and [2], respectively.

Recent results by Elssel and Zimmermann [3] include a proof of the bound $A(25, 9) \geq 384$, which is attained by a code consisting of six cosets of a binary linear $[25, 6, 11]$ code. This inspired the current work: an extensive search for error-correcting codes consisting of a union of cosets of a linear code. The framework of [8] is convenient when considering codes of this type.

In particular for linear codes with large minimum distance, one may consider *all* inequivalent linear codes with prescribed parameters (whenever the number of these is reasonably small). Linear codes can be classified using the approach in [6]. For each such code, we confront the problem of finding a maximum clique in a graph where each coset corresponds to a vertex and two vertices are connected by an edge iff (the words of) the cosets are at distance at least d from each other. Instances of the maximum clique problem were solved using the program Cliquer [5, 7].

2 The Codes

There are seven binary $[21, 3, d \geq 11]$ codes. (Recall that we consider codes that consist of a union of cosets of a linear code.) The code obtained that proves $A(21, 9) \geq 64$ can be described by the generator matrix

$$
\boldsymbol{G} = \begin{bmatrix} 111111111100000000100 \\ 111110000011111000010 \\ 111001100011000111001 \end{bmatrix}
$$

and the coset leaders

$$
\begin{gathered}
000000000000000000000, \\
000101101101010110000, \\
001010111000001111000, \\
010101101010101001000, \\
011000011111100100000, \\
100001000110111100001, \\
101001010101001010010, \\
110100110000011010001.
\end{gathered}
$$

Since the number of codewords in the new code is $64 = 2^6$, it might be tempting to guess that a $\mathbb{Z}_4$-linear code attaining $A(22, 10) \geq 64$ could exist. However, an exhaustive search revealed that there is no such code.

There are thirty-one binary $[22, 3, d \geq 11]$ codes. Since, in studying $A(22, 9)$, these lead to instances of the maximum clique problem that are far too large to solve directly, isomorph rejection had to be carried out for unions of up to three cosets, after which the rest of the cosets were found by the maximum clique algorithm.

The code obtained that proves $A(22, 9) \geq 80$ can be described by the generator matrix

$$
\boldsymbol{G} = \begin{bmatrix} 1111111111100000000100 \\ 1111100000011111000010 \\ 1100011100111001100001 \end{bmatrix}
$$

and the coset leaders

0000000000000000000000,

0001010001111010001001,

0011011010110101000000,

0011100101100100010001,

0110100100010000011110,

0110101001010011000001,

1000111100010110001000,

1010000010101011010001,

1101110000100001011000,

1110001000001101001100.

References

[1] E. Agrell, A. Vardy and K. Zeger, A table of upper bounds for binary codes, *IEEE Trans. Inform. Theory*, Vol. 47 (2001) pp. 3004–3006.

[2] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko and N. J. A. Sloane, Bounds for binary codes of length less than 25, *IEEE Trans. Inform. Theory*, Vol. 24 (1978) pp. 81–93.

[3] K. Elssel and K.-H. Zimmermann, Two new nonlinear binary codes, preprint.

[4] M. Kaikkonen, Codes from affine permutation groups, *Des. Codes Cryptogr.*, Vol. 15 (1998) pp. 183–186.

[5] S. Niskanen and P. R. J. Östergård, Cliquer user's guide, version 1.0, Tech. Rep. T48, Communications Laboratory, Helsinki University of Technology, Espoo, Finland (2003).

[6] P. R. J. Östergård, Classifying subspaces of Hamming spaces, *Des. Codes Cryptogr.*, Vol. 27 (2002) pp. 297–305.

[7] P. R. J. Östergård, A fast algorithm for the maximum clique problem, *Discrete Appl. Math.*, Vol. 120 (2002) pp. 195–205.

[8] P. R. J. Östergård and M. K. Kaikkonen, New single-error-correcting codes, *IEEE Trans. Inform. Theory*, Vol. 42 (1996) pp. 1261–1262.

[9] A. Schrijver, New code upper bounds from the Terwilliger algebra, preprint.

Preferred mailing address: Patric Östergård

Dept. of Electrical and Communications Eng.

Helsinki University of Technology

Otakaari 5

02150 Espoo

FINLAND

Tel: +358-9-451 2341

Fax: +358-9-451 2359

E-mail: `patric.ostergard@hut.fi`