Bulletin of the Iranian Mathematical Society Vol. 37 *No. 3 (2011), pp 109-115.*

SOME OPTIMAL CODES FROM DESIGNS

M. EMAMI AND CH. MAYSOORI

Communicated by Samad Hedayat

Abstract. The binary and ternary codes spanned by the rows of the point by block incidence matrices of some 2-designs and their complementary and orthogonal designs are studied. A new method is also introduced to study optimal codes.

1. Introduction

Let t, v, k and λ be positive integers such that $v > k > t$ and let V be a set of size v. The elements of V are called *points* and the k-subsets of V are called *blocks*. A t-(v, k, λ) *design* D (in short a t-design) is a pair $(V, \mathcal{B})$, where $\mathcal{B}$ is a collection of blocks with the property that every t-subset of V occurs in exactly λ blocks of $\mathcal{B}$. A t-design is called *simple* if it contains no repeated blocks. It is well known that any t-design is also a j-design, for $0 < j < t$. The *complementary* design of a t-(v, k, λ) design D, denoted by D^c, is the pair $(V, \mathcal{B}')$, where $\mathcal{B}' = \{V \backslash B;\ B \in \mathcal{B}\}$. Note that D^c is a t-$(v, v-k, \lambda^c)$ design, where $\lambda^c = \lambda\left(\binom{v}{t}/\binom{k}{t} - \sum_{i=1}^{t}(-1)^{i-1}\binom{v-i}{t-i}/\binom{k-i}{t-i}\right)$.

The incidence matrix of a t-(v, k, λ) design $D = (V, \mathcal{B})$ is the matrix $\mathcal{D}$, where the rows are indexed by points, the columns by blocks and $\mathcal{D}(P, B)$=1 if and only if $P \in B$; see [3].

MSC(2000): Primary: 05B05; Secondary: 97K20, 11H71.
Keywords: Optimal code, t-design.
Received: 18 May 2009, Accepted: 23 January 2010.
∗Corresponding author

Let n and k be two positive integers. A *q-ray linear* $[n, k]$ *code* $\mathcal{C}$ of length n is a k-dimensional subspace of an n-dimensional vector space over finite field $GF(q)$. The elements of $\mathcal{C}$ are called *codewords*. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two codewords. The *Hamming distance* $d(x, y)$ of x and y is given by

$$d(x, y) = |\{i : 1 \leq i \leq n, x_i \neq y_i\}|.$$

The *minimum distance* of $\mathcal{C}$ is defined by

$$d = d(\mathcal{C}) = min\{d(x, y) : x, y \in \mathcal{C}, x \neq y\}.$$

The *weight* of a codeword $x \in \mathcal{C}$ is defined by $w(x) = d(x, 0)$. In linear codes, the minimum distance and the minimum weight are equal. A linear $[n, k]$ code with minimum distance d is denoted by $[n, k, d]$. A linear $[n, k, d]$ code is said to be *optimal* if d has the maximum possible value for fixed n and k [1]. In other words, a linear $[n, k, d]$ code is optimal if there is no $[n, k, d']$ linear code for $d' > d$. Let $Lb(n, k)$ and $Ub(n, k)$ denote the lower and upper bounds for the maximum distance d of an $[n, k, d]$ optimal code, respectively. Clearly, a linear $[n, k, d]$ code is optimal if and only if $Lb(n, k) = d = Ub(n, k)$. For a given (n, k), we abbreviate $Lb(n, k)$ and $Ub(n, k)$ to Lb and Ub, respectively. We use the list of known Lb and Ub as they appear in [4, 5].

Let $\mathcal{D}$ be the incidence matrix of a t-design D. The vector space spanned by the rows of $\mathcal{D}$ over $GF(2)$ is a linear code $\mathcal{C}$. The rows of $\mathcal{D}$ have equal weight γ, which is called the *row-weight* of $\mathcal{D}$. The linear code spanned by the row space of $\mathcal{D}^c$ is denoted by $\mathcal{C}^c$. Note that since the repeated blocks in a design do not affect the parameters of the code obtained from its incidence matrix, it is more natural to study only simple designs; see [2].

The *dual* or *orthogonal code* of a linear $[n, k]$ code $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is the set of all vectors which are orthogonal to all codewords of $\mathcal{C}$. In other words,

$$\mathcal{C}^\perp = \{u : u.v = 0 \text{ for all } v \in \mathcal{C}\}.$$

It is known that $\mathcal{C}^\perp$ is a linear $[n, n - k]$ code. Let D be a t-(v, k, λ) design. Then, the row space of $\mathcal{D}$ is a $[b, x]$ linear code $\mathcal{C}$, where b is the number of blocks of D and $x \leq v$. The row-weight γ of $\mathcal{D}$ is r, where r is the number of blocks containing a given fixed point. The dual code $\mathcal{C}^\perp$ is a $[b, b-x]$ linear code. The complementary design D^c with the incidence matrix $\mathcal{D}^c$ also gives two linear codes $\mathcal{C}^c$ and $\mathcal{C}^{c\perp}$ with the parameters

$[b, y]$ and $[b, b-y]$, respectively, where $y \leq v$. The row-weight γ^c of $\mathcal{D}^c$ is $b - r$.

2. A Useful Method

Intuitively a greater minimum distance may be achieved if the row-weight of the incidence matrix of design is as large as possible. The following lemma guides us to start with a design and switch to its complementary design to generate a better code. We will see in tables 1-3 that some optimal codes are obtained by this method.

Lemma 2.1. *Let $\mathcal{D}$ be the incidence matrix of a t-(v, k, λ) design D, and suppose that $k < v/2$. Then, the row-weight of the incidence matrix of design D^c is greater than the row-weight of the incidence matrix of design D.*

Proof. Let b and r be the number of blocks and the number of blocks through a given fixed point of design D, respectively. If γ and γ^c are the row-weights of $\mathcal{D}$ and $\mathcal{D}^c$, respectively, then $k < v/2$ implies that

$$\gamma^c = b - r > b - \frac{bk}{v} = b\ \frac{v-k}{v} > b\ \frac{k}{v} = r = \gamma.$$

□

The method is to apply the above lemma to obtain codes with higher minimum weights. As we shall see in some cases, this process leads us to optimal codes. Note that this method is useful only if the minimum weight of the code is the row-weight of its incidence matrix. These kinds of codes are also studied in [6]. As an example, suppose that D is a 2-$(15, 3, 1)$ design. So, $b = 35$ and $r = 7$. There are 80 non-isomorphic designs with these parameters and the rank$(\mathcal{D})$ over $GF(2)$ is one of the numbers 11, 13, 14 and 15 [10]. In all these 4 cases, $d = 7$, while we have $Lb(35, 11) = Ub(35, 11) = 12$, $Lb(35, 13) = Ub(35, 13) = 11$, $Lb(35, 14) = Ub(35, 14) = 10$ and $Lb(35, 15) = Ub(35, 15) = 9$. Now, if we utilize the above lemma and take the complementary design, then in all these cases the rank$(\mathcal{D}^c)$ over $GF(2)$ is equal to 10 and $d = 12$, while $Lb(35, 10) = 12$ and $Ub(35, 10) = 13$. In other words, we get a linear code spanned by the row space of $\mathcal{D}^c$, that is a candidate to be an optimal code.

3. **The Results**

We applied our algorithm above on a selected number of designs and presented our obtained codes in tables 1-3. All designs in these tables are selected from the CRC handbook or the references therein [9]. In each case, we considered all non-isomorphic designs to build their incidence matrices and then computed their corresponding $[b, x]$ linear code. In the final step, for fixed b and x, we computed and listed all the codes with the highest minimum distance. For example, we considered all the 332 non-isomorphic simple 2-(9,3,3) designs [8]. All generated codes from these designs are [36,8] codes and the best minimum distance (over $GF(2)$) is $d = 8$. These codes and the codes obtained from their complementary design, over $GF(2)$ and $GF(3)$, are listed in row 8 of Table 1 and rows 3 and 4 of Table 2. The codes spanned from all 80 non-isomorphic simple 2-(15,3,1) designs and their complementary designs are listed in row 12 of Table 1 and rows 1 and 2 of Table 2. In Table 2, we studied three designs 2-(15,3,1), 2-(9,3,3) and 2-(9,3,4) with the complementary designs 2-(15,12,22), 2-(9,6,15) and 2-(9,6,20), respectively (see also [7]). They are arranged in successive rows. The column $Type$ in each table shows the type of the computed codes in each row, from the given design. In Table 3, we considered five different designs all of which are optimal codes. In Table 1, the codes and the optimal codes arising from some selected triple systems are listed. As seen, our method generates a good number of optimal codes. Data in column (Lb, Ub) are taken from some on-line database servers [4, 5].

Table 1. Codes and optimal codes arising from some selected triple systems.

Design	Codes over $GF(2)$		(Lb, Ub)	Codes over $GF(3)$		(Lb, Ub)
	Parameters	Type		Parameters	Type	
2-(6,3,2)	[10,6,3]	$\mathcal{C}, \mathcal{C}^c$	optimal	[10,5,5]	$\mathcal{C}, \mathcal{C}^{\perp}$	optimal
	[10,4,4]	$\mathcal{C}^{\perp}, \mathcal{C}^{c\perp}$	optimal	[10,5,5]	$\mathcal{C}^c, \mathcal{C}^{c\perp}$	optimal
2-(7,3,1)	[7,4,3]	$\mathcal{C}, \mathcal{C}^c$	optimal	[7,6,2]	$\mathcal{C}$	optimal
	[7,3,4]	$\mathcal{C}^c, \mathcal{C}^{\perp}$	optimal	[7,7,1]	$\mathcal{C}^c$	optimal
2-(7,3,2)	[14,7,4]	$\mathcal{C}, \mathcal{C}^{\perp}$	optimal	[14,6,6]	$\mathcal{C}$	optimal
				[14,8,5]	$\mathcal{C}$	optimal
2-(7,3,3)	[21,7,8]	$\mathcal{C}$	optimal	[21,15,4]	$\mathcal{C}^{\perp}$	optimal
	[21,14,4]	$\mathcal{C}^{\perp}$	optimal			
2-(7,3,4)	[28,7,11]	$\mathcal{C}$	(12,12)	[28,6,11]	$\mathcal{C}$	(15,15)
	[28,6,11]	$\mathcal{C}^c$	(12,12)	[28,7,11]	$\mathcal{C}^c$	(15,15)
2-(9,3,1)	[12,9,2]	$\mathcal{C}$	optimal	[12,6,4]	$\mathcal{C}$	(6,6)
	[12,3,6]	$\mathcal{C}^{\perp}$	optimal	[12,6,5]	$\mathcal{C}^c$	(6.6)
2-(9.3,2)	[24,16,4]	$\mathcal{C}^{\perp}$	optimal			
	[24,15,4]	$\mathcal{C}^{\perp}$	optimal			
	[24,8,8]	$\mathcal{C}$	optimal			
2-(9,3,3)	[36,8,8]	$\mathcal{C}$	(16,16)	[36,8,12]	$\mathcal{C}$	(18,19)
	[36,8,14]	$\mathcal{C}^c$	(16,16)	[36,8,15]	$\mathcal{C}^c$	(18,19)
2-(9,3,4)	[48,9,16]	$\mathcal{C}$	(22,22)	[48,8,16]	$\mathcal{C}$	(26,27)
	[48,8,20]	$\mathcal{C}^c$	(22,22)	[48,8,23]	$\mathcal{C}^c$	(26,27)
2-(9,3,5)	[60,9,20]	$\mathcal{C}$	(22,26)	[60,8,20]	$\mathcal{C}$	(33,36)
	[60,8,25]	$\mathcal{C}^c$	(27,27)	[60,8,28]	$\mathcal{C}^c$	(33,36)
2-(9,3,6)	[72,9,24]	$\mathcal{C}$	(32,32)	[72,8,24]	$\mathcal{C}$	(42,44)
	[72,8,32]	$\mathcal{C}^c$	optimal	[72,8,36]	$\mathcal{C}^c$	(42,44)
2-(15,3,1)	[35,11,7]	$\mathcal{C}$	(12,12)	[35,14,7]	$\mathcal{C}$	(12,15)
	[35,13,7]	$\mathcal{C}$	(11,11)	[35,14,10]	$\mathcal{C}^c$	(12,15)
	[35,14,7]	$\mathcal{C}$	(10,10)			
	[35,15,7]	$\mathcal{C}$	(9,9)			
	[35,10,12]	$\mathcal{C}^c$	(12,13)			

Table 2. Codes from some selected designs and their complements.

Design	Type	Codes over $GF(2)$	(Lb, Ub)	Codes over $GF(3)$	(Lb, Ub)
2-$(15, 3, 1)$	$\mathcal{C}$	$[35, 11, 7]$	(12,12)	$[35, 14, 7]$	(12,15)
		$[35, 13, 7]$	(11,11)		
		$[35, 14, 7]$	(10,10)		
		$[35, 15, 7]$	(9,9)		
2-$(15, 12, 22)$	$\mathcal{C}^c$	$[35, 10, 12]$	(12,13)	$[35, 14, 10]$	(12,15)
2-$(9, 3, 3)$	$\mathcal{C}$	$[36, 8, 8]$	(16,16)	$[36, 8, 12]$	(18,19)
2-$(9, 6, 15)$	$\mathcal{C}^c$	$[36, 8, 14]$	(16,16)	$[36, 8, 15]$	(18,19)
2-$(9, 3, 4)$	$\mathcal{C}$	$[48, 9, 16]$	(22,22)	$[48, 8, 16]$	(26,27)
2-$(9, 6, 20)$	$\mathcal{C}^c$	$[48, 8, 20]$	(22,22)	$[48, 8, 23]$	(26,27)

Table 3. Optimal codes arising from some other designs

Design	Codes over $GF(2)$		Codes over $GF(3)$	
	Parameters	Type	Parameters	Type
2-$(8, 4, 3)$	$[14, 10, 3]$	$\mathcal{C}^{\perp}$	$[14, 6, 6]$	$\mathcal{C}^{\perp}$
			$[14, 8, 5]$	$\mathcal{C}$
2-$(9, 4, 3)$			$[18, 9, 6]$	$\mathcal{C}^{\perp}$
2-$(15, 7, 3)$	$[15, 8, 4]$	$\mathcal{C}^{\perp}$		
	$[15, 9, 4]$	$\mathcal{C}^{\perp}$		
	$[15, 10, 4]$	$\mathcal{C}^{\perp}$		
	$[15, 5, 7]$	$\mathcal{C}$		
2-$(16, 6, 2)$	$[16, 10, 4]$	$\mathcal{C}^{\perp}$	$[16, 15, 2]$	$\mathcal{C}$
	$[16, 9, 4]$	$\mathcal{C}^{\perp}$		
	$[16, 6, 6]$	$\mathcal{C}$		
2-$(19, 9, 4)$			$[19, 18, 2]$	$\mathcal{C}$

Acknowledgments

The authors give their best gratitude to Professor Khosrovshahi for his guidance in preparing this work. They also thank the editorial board of BIMS and the referees of this manuscript.

References

[1] E.F. Assmus and J.D. Key, *Designs and Their Codes*, Cambridge Tracts in Mathematics, 103, Cambridge University Press, Cambridge, 1992.
[2] A. Baartmans, I. Landjev and V.D. Tonchev, On the binary codes of Steiner triple systems, Special issue dedicated to Hanfried Lenz, *Des. Codes Cryptogr.* **8** (1996) 29-43.
[3] T.H. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1986.
[4] A.E. Brouwer, Linear code bounds, http://www.win.tue.ni/ aeb/voorlincod.html.
[5] Code Table, http://www.codetables.de/.
[6] C.J. Colbourn, Minimum weights of point codes of Steiner triple systems, Special issue on design combinatorics: in honor of S. S. Shrikhande, *J. Statist. Plann. Inference* **95** (2001) 161-166.
[7] M. Emami, G.B. Khosrovshahi and Ch. Maysoori, Some designs of small orders and their codes, *J. Combin. Math. Combin. Comput.* **43** (2002) 101-117.
[8] J.J. Harms, C.J. Colbourn and A.V. Ivanov, A census of (9,3,3) block designs without repeated blocks, Sixteenth Manitoba conference on numerical mathematics and computing (Winnipeg, Man., 1986), *Congr. Numer.* **57** (1987) 147-170.
[9] V.D. Tonchev, *Codes*, in: *The CRC handbook of combinatorial designs* (C.J. Colbourn and J.H. Dinitz, eds), CRC Press, Boca Raton, 1996, pp. 517-543.
[10] V.D. Tonchev and R.S. Weishaar, Steiner triple systems of order 15 and their codes, *J. Statist. Plann. Inference* **58** (1997) 207-216.

M. Emami
Department of Mathematics, University of Zanjan, P.O. Box 45195-313 Zanjan, Iran
Email: emami@znu.ac.ir

Ch. Maysoori
Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran
Email: tiziq@yahoo.com