Appl. Math. Inf. Sci. **9**, No. 6, 2899-2903 (2015)

Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090616

A Study on Minimality of the Codewords in the Dual Code of the Code of a Symmetric (v,k,λ) -Design

Selda ÇALKAVUR[*]

Department of Mathematics, Kocaeli University, Kocaeli, Turkey

Received: 16 Feb. 2015, Revised: 16 Apr. 2015, Accepted: 17 Apr. 2015
Published online: 1 Nov. 2015

Abstract: The F_q - code of a symmetric (v,k,λ)- design is a subspace generated by the incidence matrix of the symmetric design. In this paper, we examine the minimality of the codewords in the dual code $C^{\perp}$ of the binary code C of a symmetric $(v,k,\lambda)-$ design. So, we use the relationship between the minimum and maximum nonzero weights in the dual code $C^{\perp}$ with the number of F_q.

Keywords: Linear code, the code of a symmetric design, secret sharing scheme, minimal codeword.
2000 *Mathematics Subject Classification:* 14G50, 94A60, 94C30

1 Introduction

It is important that a secret key, passwords, informations of the plan of a secret place or an important formula of a product or i.e. must be kept secret. One of the ways of solving this problem is to give secret sharing schemes.

In fact, for a secret sharing the main problem is to divide the secret into pieces instead of storing the whole.

The secret sharing schemes were introduced by Blakley [3] and Shamir [15] in 1979. Since then, many constructions have been proposed. In this section, it is given some basic definitions on the subject. (In this paper, the finite field $GF(q)$ will be denoted by the symbol F_q.)

Definition 11*(The Code of a Symmetric Design) The F_q-code of a symmetric (v,k,λ)- design is a subspace generated by the incidence matrix of the symmetric design [9].*

Before giving the definition of minimal access set we have to remind some basic notions of the system of secret sharing:

Let $G=(g_0,g_1,...,g_{n-1})$ be a generator matrix of $[n,k,d]$ - code C , where $g_0,g_1,...,g_{n-1}$ are column vectors of G. To obtain a secret sharing scheme the first step is to considered a secret space. A secret space consists of the set of participants and a dealer. (For example ”director”.)

If we use the way of constructing the secret sharing scheme described by Massey [10], there are three parts of secret sharing scheme based on C, these are
1) the secret which is element of F_q,
2) $(n-1)$ participants and
3) a dealer.

The dealer has a secret. So, the main question is ”How is the secret shared between the participants?” and one of the important problems is ”If the dealer (”director”) lose the secret, how is it recovered? In this context, we remind some definitions about the subject.

Definition 12*(Minimal Access Set) A subset of participants is called a minimal access set, if the participants in the subsets can recover the secret by combining their shares but any subset at the participants can not do so [12].*

Definition 13*(Support of a Vector) The set $S=\{0\le i\le n-1|c_i\neq 0\}$ is called support of a vector $c=c_1c_2...c_n\in(F_q)^n$. A codeword c_2 covers a codeword c_1 if the support of c_2 contains that of c_1 [12].*

Definition 14*(Minimal Codeword) A minimal codeword c is a codeword which covers just only its scalar multiples [12].*

[*] Corresponding author e-mail: selda.calkavur@kocaeli.edu.tr

2 Characterizations of Minimal Codewords

In a secret sharing scheme, to know whether of codewords are minimal is an important problem. We need minimal codewords to determine the access structure of secret sharing scheme. Before giving our two theorems on this subject, we will remind some definitions and two lemmas given in [16] and [9].

Definition 21(*$2-(v,k,\lambda)$ Design) A $2-(v,k,\lambda)$ design is an incidence structure satisfying the following requirements:*
i) There are v points.
ii) Any block is incident with k points.
iii) Any 2 points are incident with λ blocks [9].

Definition 22(*Maximum and Minimum Weight of the Code) Let C be an $[n,k,d]$ code over F_q. The elements of C are called codewords. The weight of a codeword is the number of nonzero coordinates in it. The minimum weight of a code is the smallest nonzero weight of any codeword. The maximum weight of a code is the biggest weight of any codeword [9].*

Lemma 23*A code C has minimum weight $\geq d$, if and only if every $d-1$ columns in a parity-check matrix are linearly independent [16].*

Lemma 24*If A is the $b \times v$ incidence matrix of a $2-(v,k,\lambda)$ design, then the dual of the binary code with generator matrix A has minimum weight*

$$w_{min} \geq \frac{(r+\lambda)}{\lambda}, \tag{2.1}$$

where r is the number of blocks on a point [16].

*Proof.*Let S be a minimum set of linearly dependent columns of A, where A is a matrix over F_2 and suppose $|S| = m$. Then every set of $m-1$ columns is linearly dependent and Lemma 2.3 shows that $dim(C^{\perp}) \geq m$. Suppose n_j is the number of rows that have j ones in the columns of S add to a zero column vector. $n_j = 0$ for odd j and we have the incidence equations:

$$\sum 2in_{2i} = rm$$

and

$$\sum 2i(2i-1)n_{2i} = m(m-1)\lambda$$

So

$$\sum 2i(2i-2)n_{2i} = m[(m-1)\lambda - r]$$

and every summand is non-negative. Therefore

$$m-1 \geq \frac{r}{\lambda}$$

$$m \geq \frac{r+\lambda}{\lambda}$$

[16].

Lemma 25*If A is the $b \times v$ incidence matrix of a $2-(v,k,\lambda)$ design, then the dual of the binary code with generator matrix*

$$D = \begin{pmatrix} 1 & \vdots & \\ \vdots & \vdots & A \\ 1 & \vdots & \end{pmatrix}$$

has minimum weight

$$w_{min} \geq min\left\{\frac{b+r}{r}, \frac{r+\lambda}{\lambda}\right\}[16].$$

*Proof.*Let S be a minimum set of linearly independent columns of D and suppose $|S| = m$. If the left-most column vector j of all ones does not belong to S, then

$$|S| = m \geq \frac{r+\lambda}{\lambda}$$

and we are done by Lemma 2.3. Suppose j belongs to S. Then the columns of S' add to j, where S' is the set of all the columns of S except j. Hence if n_i is the number of A that have i ones in common with the columns of S', then $n_i = 0$, for even i and

$$\sum n_{2i+1} = b$$

and

$$\sum (2i+1)n_{2i+1} = r(m-1)$$

that is

$$\sum 2in_{2i+1} = r(m-1) - b \geq 0.$$

So,

$$m \geq \frac{b+r}{r}$$

and we are done.

Theorem 26*(Ashikmin-Barg) In an $[n,k]$- code C over F_q, let w_{min} and w_{max} be the minimum and maximum nonzero weights, respectively. If*

$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q}, \tag{2.2}$$

then all of the nonzero codewords of C are minimal [18].

*Proof.*Suppose $c_1 = (u_0, u_1, ..., u_{n-1})$ covers $c_2 = (v_0, v_1, ..., v_{n-1})$ and c_1 is not a multiple of c_2. Then

$$w_{min} \leq w(c_2) \leq w(c_1) \leq w_{max}.$$

For any $t \in F_q^*$ let $m_t = |\{i : v_i \neq 0, u_i = tv_i\}|$. By definition

$$\sum_{t \in F_q^*} m_t = w_2.$$

Hence there exists some t such that $m_t \geq \frac{w_2}{q-1}$. For the codeword $c_1 - tc_2$.

$$w(c_1 - tc_2) \leq w_1 - \frac{w_2}{q-1} \leq w_{max} - \frac{w_{min}}{q-1} < \frac{q}{q-1} w_{min} - \frac{w_{min}}{q-1} = w_{min}$$

This means the nonzero codeword $c_1 - tc_2$ has weight less than w_{min}, which is impossible [6].

Using the definitions, lemmas and theorem given above, we give two theorems as follows:

Theorem 27 *Let C be the binary code of a symmetric (v,k,λ)- design. If*

$$w_{max} < \frac{2(k+\lambda)}{\lambda} \tag{2.3}$$

for the dual code $C^{\perp}$ of the binary code C, then all of the nonzero codewords in the dual code $C^{\perp}$ are minimal [4].

Proof. For a linear code C, the dual code $C^{\perp}$ of the code C is also a linear code. From the Theorem 2.6 if

$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q}$$

for the dual code $C^{\perp}$ of the binary code C, then all of the nonzero codewords in the dual code $C^{\perp}$ are minimal. For the binary code $q=2$, then

$$\frac{q-1}{q} = \frac{1}{2}.$$

So, if

$$\frac{w_{min}}{w_{max}} > \frac{1}{2},$$

then all of the nonzero codewords in the dual code $C^{\perp}$ are minimal.

Now we have to prove that

$$\frac{w_{min}}{w_{max}} > \frac{1}{2},$$

if

$$w_{max} < \frac{2(k+\lambda)}{\lambda}.$$

Let $A_{b\times v}$ be the incidence matrix of a $2-(v,k,\lambda)$ design. From
Lemma 2.4 the dual code of the binary code with generator matrix A has minimum weight

$$w_{min} \geq \frac{r+\lambda}{\lambda},$$

where r is the number of blocks that are incident with a point. Particularly, in a symmetric $(v,k,\lambda)-$ design $k=r$ and the minimum weight of the dual code $C^{\perp}$ of the code C which is generated by the rows of the matrix A is

$$w_{min} \geq \frac{k+\lambda}{\lambda}.$$

Now, suppose that

$$w_{max} < \frac{2(k+\lambda)}{\lambda}.$$

Then,

$$\frac{1}{w_{max}} > \frac{\lambda}{2(k+\lambda)}. \tag{2.4}$$

If we multiply both sides of inequality (2.4) by $(\frac{k+\lambda}{\lambda})$, it is obtained that

$$\frac{\frac{k+\lambda}{\lambda}}{w_{max}} > \frac{1}{2}. \tag{2.5}$$

Since $w_{min} \geq \frac{k+\lambda}{\lambda}$, it is obtained that $\frac{w_{min}}{w_{max}} > \frac{1}{2}$, if it is written w_{min} instead of $(\frac{k+\lambda}{\lambda})$ in (2.5). This means all of the nonzero codewords in the dual code $C^{\perp}$ are minimal.

Theorem 28 *Let A be the incidence matrix of the symmetric $(v,k,\lambda)-$ design. All of the nonzero codewords in the dual code $C^{\perp}$ of the binary code C which is generated by the rows of the matrix*

$$D = \begin{pmatrix} 1 & \vdots & \\ \vdots & \vdots & A \\ 1 & \vdots & \end{pmatrix}$$

are minimal if $w_{max} < \frac{2(v+k)}{k}$ [4].

Proof. Let $A_{b\times v}$ be the incidence matrix of a $2-(v,k,\lambda)$ design. Then, from Lemma 2.5 the minimum weight of the dual code of the binary code generated by the rows of the matrix D satisfy the boundary

$$w_{min} \geq min\left\{\frac{b+r}{r}, \frac{r+\lambda}{\lambda}\right\}. \tag{2.6}$$

For the symmetric $(v,k,\lambda)-$ design since $k=r$, $b=v$; inequality (2.6) is transformed to

$$w_{min} \geq min\left\{\frac{v+k}{k}, \frac{k+\lambda}{\lambda}\right\}.$$

Since $k > \lambda$, we have

$$\frac{v+k}{k} < \frac{k+\lambda}{\lambda}. \tag{2.7}$$

From (2.7) we obtain

$$min\left\{\frac{v+k}{k}, \frac{k+\lambda}{\lambda}\right\} = \frac{v+k}{k}.$$

So

$$w_{min} \geq \frac{v+k}{k}.$$

Therefore we find

$$\frac{w_{min}}{w_{max}} \geq \frac{\frac{v+k}{k}}{w_{max}}. \tag{2.8}$$

Now we suppose that

$$w_{max} < \frac{2(v+k)}{k}.$$

Then,

$$\frac{1}{w_{max}} > \frac{k}{2(v+k)}. \tag{2.9}$$

If it is multiplied both sides of inequality (2.9) by $(\frac{v+k}{k})$, we find

$$\frac{\frac{v+k}{k}}{w_{max}} > \frac{1}{2}. \tag{2.10}$$

From (2.8) and (2.10) we obtained that,

$$\frac{w_{min}}{w_{max}} > \frac{1}{2}. \tag{2.11}$$

3 Conclusion

In this work, we investigated the minimality of the codewords in the dual code $C^{\perp}$ of the binary code C of a symmetric $(v,k,\lambda)-$ design and obtained the following results:

– Let C be the binary code of a symmetric $(v,k,\lambda)-$ design. If

$$w_{max} < \frac{2(k+\lambda)}{\lambda} \tag{3.1}$$

for the dual code $C^{\perp}$ of the binary code C, then all of the nonzero codewords in the dual code $C^{\perp}$ are minimal.

– Let A be the incidence matrix of the symmetric $(v,k,\lambda)-$ design. All of the nonzero codewords in the dual code $C^{\perp}$ of the binary code C which is generated by the rows of the matrix

$$D = \begin{pmatrix} 1 \vdots & \\ \vdots \vdots & A \\ 1 \vdots & \end{pmatrix}$$

are minimal if $w_{max} < \frac{2(v+k)}{k}$.

References

[1] Ashikmin, A., Barg, A., Cohen, G. "Variations on Minimal Codewords in Linear Codes", in Proc. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC 1995) (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1995, vol. 948, pp. 96-105.

[2] Ashikmin, A. and Barg, A. "Minimal Vectors in Linear Codes", IEEE Trans. Inf. Theory, vol. 44, no 5, pp. 2010-2017, Sep. 1998.

[3] Blakley, G. R. "Safeguarding Cryptographic Keys", in Proc. 1979 National Computer Conf., New York, Jun. 1979, pp. 313-317.

[4] Çalkavur, S. "Symmetric Designs, Codes and a Study on Secret Sharing Schemes" , PhDThesis pp. 59-63. İstanbul:İstanbul Kültür University, July 2010.

[5] Ding, C., Kohel, D. and Ling, S. "Secret Sharing with a Class of Ternary Codes", Theor. Comp. Sci., vol. 246, pp. 285-298, 2000.

[6] Ding, C., and Yuan, J. "Covering and Secret Sharing with Linear Codes" in Discrete Mathematics and Theoretical Computer Science (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2731, pp. 11-25.

[7] Hill, R. " A First Course in Coding Theory", Oxford: Oxford University, 1986.

[8] Karnin, E. D., Greene, J. W. and Hellman, M. E. "On Secret Sharing Systems", IEEE Trans. Inf. Theory, vol. IT-29, no:1, pp. 35-41, Jan. 1983.

[9] Lander, E. S. "Symmetric Designs an Algebraic Approach", Cambridge: Cambridge University, 1983.

[10] Massey, J. L. "Minimal Codewords and Secret Sharing", in Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden, pp. 276-279, Aug. 1993.

[11] Okada, K. and Kurosawa, K. "MDS Secret Sharing Scheme Secure Against Cheaters", IEEE Trans. Inf. Theory, vol. 46, no. 3, pp. 1078-1081.

[12] Özadam, H., Özbudak, F., Saygı, Z., "Secret Sharing Schemes and Linear Codes", Information Security Cryptology Conference with International Participation, Proceedings, pp.101-106, December 2007.

[13] Pieprzyk, J. and Zhang, X. M. "Ideal Threshold Schemes from MDS Codes" , in Information Security and Cryptology-Proc. of ICISC 2002 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2587, pp. 269-279.

[14] Renvall, A. and Ding, C."The Access Structure of Some Secret Sharing Schemes", in Information Security and Privacy (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1996, vol. 1172, pp. 67-78.

[15] Shamir, A. "How to Share a Secret", Commun. Assoc. Comp. Mach., vol. 22, pp. 612-613, 1979.

[16] Shrikhande, M. S., Sane, S., "Quasi-Symmetric Designs", London Mathematical Society Lecture Note Series 164, Cambridge University Press, Melbourne, Sydney, pp. 194-195, 1991.

[17] Yuan, J. and Ding, C., Secret Sharing Schemes from Two Weight Codes", in Proc. R. C. Bose Centenary Symp. Discrete Mathematics and Applications, Kolkata, India, Dec. 2002.

[18] Yuan, J., Ding, C., Senior Member, IEEE, "Secret Sharing Schemes from Three Classes of Linear Codes," IEEE Trans. on Inf. Theory, vol. 52, no. 1, pp. 206-212, Jan. 2006.

[19] - "Some Applications of Coding Theory", Cryptography, Codes and Ciphers: Cryptography and Coding IV, pp. 33-47, 1995.

Selda Çalkavur received Doctor degree from Istanbul Kultur University, Istanbul, Turkey in 2010. She has been working as an assistant professor at Kocaeli University, Kocaeli, Turkey since 2011. She has became a board member in 2011, head of department in 2012 and a vice director in 2013 at Kocaeli University. Her research interests include coding theory, cryptography, design theory and algebra.