Journal of Engineering Technology and Applied Sciences, 2022
Received 3 December 2021, Accepted 17 March 2022
Published online 21 March 2022, Research Article

e-ISSN: 2548-0391
Vol. 7, No. 1, 45-49
doi: 10.30931/jetas.1032180

Citation: Oztas, E. S., "Lifted MDS Codes over Finite Fields". Journal of Engineering Technology and Applied Sciences 7 (1) 2022 : 45-49.

LIFTED MDS CODES OVER FINITE FIELDS

Elif Segah Oztas

Department of Mathematics, Karamanoglu Mehmetbey University, Turkey
esoztas@kmu.edu.tr

Abstract

MDS codes are elegant constructions in coding theory and have mode important applications in network coding, distributed data storage, communication systems etc. In this study, a method is given which MDS codes are lifted to a higher finite field. The presented method satisfies the protection of the distance and creating the MDS code over the F_q by using MDS code over F_p.

Keywords: Lifted MDS codes, distance preserving

1. Introduction

Maximum Distance Separable (MDS) codes [1] are used across a wide area of modern information technology, network coding, data storage, data distribution etc. In [5–18], MDS codes are studied with network coding.

The main generation method for MDS code is Reed Solomon (RS) codes, especially Generalized Reed Solomon (GRS) codes. In GRS, the code $[n, k, n - k + 1]_q$ can be obtained where $n \leq q$. There are some approaches for constructing MDS matrices such that Vandermonde matrix, circulant matrix, Cauchy matrix, Toeplitz matrices etc. [2–4, 19–22]. All of them compute and improve their method over the defined field in the papers. However, calculation complexity increase over the field which has high cardinality for any construction methods for MDS codes, especially in the recursive generating method.

A linear code C with parameters $[n, k, d]_q$ of length n over the finite field F_q where p is a prime and q is a prime power and any two vectors in C differ in at least d places. Singleton bound is $d \leq n - k + 1$ and a code satisfying the equality of this bound is called a maximum distance separable (MDS) code. In this paper, the extension of existed codes are studied on over Fp. Background on coding theory and related material made be found in [1]. In this paper, a method is introduced to construct MDS codes over F_q $(q = p^t)$ by using lift the MDS codes over F_q.

Moreover, computational complexity is less than other recursive algorithms, and a diversity of the codes is satisfied. These situations give advantages for applications of MDS codes, especially in data transfer by using data distributing systems because the given method satisfies the variety of codes.

2. Construction of MDS code over F_{p^t}

In this section, MDS code over F_p (p is a prime) are used to generate MDS codes over F_{p^t} by using distance holder matrix.

Definition 2.1 Let M is a $n \times n$ diagonal matrix.The entry in the i-th row and j-th column of a matrix M denoted as m_{ij}. l is maximum number of same entries among diagonal entries as follow;

$l(M) = \max |\{a : a \in m_{ii}|\}|$.

For example; $A = \begin{pmatrix} w & 0 & 0 \\ 0 & w^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} w & 0 & 0 \\ 0 & w & 0 \\ 0 & 0 & 1 \end{pmatrix}$ over F_4. $l(A) = 1$ and $l(B) = 2$. In matrix A all diagonal entry has a unique element. In matrix B, there are two w and one 1. Then maximum number of repeated entry in diagonal entries is 2.

Definition 2.2 Let M be $n \times n$ diagonal matrix $m_{ii} \in F^*_{p^t}$ where $F^*_{p^t} = F_{p^t} - \{0\}$. If $l(M) = 1$, it called distance holder matrix. If $l(M) = s$, M is a s-distance holder matrix ($s - dh$-matrix).

The aim of the distance holder matrix is to satisfy the diversity of generators. This means it helps de define different generators for applications of MDS codes. These variations of matrices can be used by the security and multi-node communications systems.

Lemma 2.3 Let D be an MDS code generation matrix over F_{p^t}, then D' is obtained by multiplying a row (or column) of D by any element of $F^*_{p^t}$, D will also be an MDS code generator matrix.

Lemma 2.3 is generalized as follows.

Corollary 2.4 Let D be a generator matrix of a MDS code, then for any nonsingular diagonal matrices M_1 and M_2, M_1DM_2 will also be a MDS matrix.

" $\cdot_{F_{p^t}}$ " denote that matrix product operations is over F_{p^t}.

Definition 2.5 Let G be a generator matrix of C that is $[n, k, d]$ MDS code over F_p. $G \cdot_{F_{p^t}} M$ is generator of C' that is a Lifted MDS code of C over F_{p^t} where M is a $n \times n$ dh-matrix over F_{p^t} and $p^t > n$.

In the following theorem, codes are lifted to an extension of finite field under some restriction. Then, the hamming distance is protected in new codes by using Lifted MDS code and they are still MDS code over the extension of finite field.

Theorem 2.6 Let C be a $[n,k,d]_p$ MDS code over F_p. Lifted MDS code of C is C' has parameter $[n,k,d]_q$.

Proof. Let C be a $[n,k,d]$ MDS code over F_p. d has been changed by changing column entries of the generator matrix G. In column case, changing the distance is a connected characteristic of F_p. Because p is prime, there is no polynomial identification for elements. Then there is no restriction for d except characteristic. Then, operation in field extension to F_{p^t} that same characteristic as F_p and $p^t > n$ is protect the distance at least d.

By Lemma 2.3 and Corollary 2.4, the matrix and element operation preserve MDS property over finite field extension. Moreover, In Theorem 2.6, distance preservation is satisfied over finite field extension.

Remark 2.7 Diversity of generator matrix are satisfied by using finite field F_{p^t} $(p^t > n)$ in Theorem 2.6. Then number of different generator matrices is $\binom{p^t - 1}{n}$.

Example 2.8 Let G be a generator matrix of code C over F_7.

$$\begin{bmatrix} 1 & 0 & 0 & 6 & 4 & 2 & 5 & 3 \\ 0 & 1 & 0 & 3 & 1 & 5 & 1 & 3 \\ 0 & 0 & 1 & 3 & 5 & 2 & 4 & 6 \end{bmatrix}$$

C is a [8,3,6] MDS code over F_{7^3}.

Let M be a matrix dh-matrix $M = diag(w^{244}, w^{28}, w^{326}, w^{294}, w^{239}, w^{76}, w^{212}, w^{84})$ over F_{7^3}.

$$G' = G \cdot_{F_{p^t}} M = \begin{bmatrix} 1 & 0 & 0 & w^{221} & w^{223} & w^{288} & w^{253} & w^{239} \\ 0 & 1 & 0 & w^{323} & w^{211} & w^{333} & w^{184} & w^{113} \\ 0 & 0 & 1 & w^{25} & w^{198} & w^{206} & 2 & w^{271} \end{bmatrix}$$

G' generate a [8,3,6] MDS code over F_{7^3}.

Another example for same code over F_7:

Let M be a matrix dh-matrix $M = diag(w^{108}, w^{191}, w^{261}, w^{312}, w^{95}, w^{249}, w^{278}, w^{47})$ over F_{7^3}.

$$G'' = G \cdot_{F_{p^t}} M = \begin{bmatrix} 1 & 0 & 0 & w^{33} & w^{215} & w^{255} & w^{113} & w^{338} \\ 0 & 1 & 0 & w^{178} & w^{246} & w & w^{87} & w^{255} \\ 0 & 0 & 1 & w^{108} & w^{119} & w^{102} & w^{245} & w^{299} \end{bmatrix}$$

G'' generate a [8,3,6] MDS code over F_{7^3}.

By Example 2.8, distance has been preserved. Moreover, diversity for components of the codes and a MDS code over F_{7^3} have been obtained. By Remark 2.7, lots of different codes that have the same distance can be generated. This situation has importance in security and communication systems.

3. Conclusion

In this paper, a method called lifted MDS codes is introduced. It satisfies that protection the distance, variation of code components, keep the MDS property in higher finite fields. Moreover, complexity for calculation is less than the previous recursive method which is clear, because there are only matrix multiplications for the generation of new MDS code.

References

[1] MacWilliams, F. J., Sloane, N. J. A., "The theory of error-correcting codes", Amsterdam: North-Holland (1977).

[2] Hurley, T., "MDS codes over finitefields", arXiv:1903.05265 [cs.IT].

[3] Gupta, K. C., Pandey, S. K., Ray, I. G., Samanta, S. "Crypto- graphically significant mds matrices over finite fields: A brief survey and some generalized results", Advances in Mathematics of Communications 13 (4) (2019) : 779-843.

[4] Daemen, J., Rijmen, V., "The design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag (2002).

[5] Hu, Y., Zhang, X., Lee, P. P. C., Zhou, P., "Generalized optimal storage scaling via network coding", IEEE International Symposium on Information Theory - Proceedings, 2018-June, art. no. 8437684 (2018) : 956-960.

[6] Guang, X., Yeung, R.W., "Linear network error correction coding revisited", IEEE International Symposium on Information Theory - Proceedings, 2020-June, art. no. 9174493 (2020) : 1635-1640.

[7] Wu, X., Li, Q., Leung, V. C. M., Ching, P. C., "Joint Fronthaul multicast and cooperative beam- forming for cache-enabled cloud-based small cell networks: An MDS codes-aided approach", IEEE Transactions on Wireless Communications 18(10) art. no. 8786923 (2019) : 4970-4982.

[8] Ko, D., Hong, B., Choi, W. "Probabilistic caching based on maximum distance separable code in a user-centric clustered cache-aided wireless network", IEEE Transactions on Wireless Communications 18(3) art. no. 8638790 (2019) : 1792-1804.

[9] Gu, S., Li, J., Wang, Y., Wang, N., Zhang, Q. "DR-MDS: An energy-efficient coding scheme in D2D distributed storage network for the internet of things", IEEE Access 7 art. no. 8648336 (2019) : 24179-24191.

[10] Pedersen, J., Graell Amat, A.I., Andriyanova, I., Brannstrom, F. "Optimizing MDS coded caching in wireless networks with device-to-device communication", IEEE Transactions on Wireless Communications 18(1) art. no. 8551275 (2019) : 286-295.

[11] Mousavi, S., Zhou, T., Tian, C. "Delayed parity generation in MDS storage codes", IEEE International Symposium on Information Theory - Proceedings 8437700 (2018) : 1889-1893.

[12] Heidarpour, A. R., Ardakani, M., Tellambura, C., "Network coded cooperation based on relay selection with imperfect CSI", IEEE Vehicular Technology Conference 2017-September, (2018) : 1-5.

[13] Tamo, I., Wang, Z., Bruck, J. "Zigzag codes: MDS array codes with optimal rebuilding", IEEE Transactions on Information Theory 59(3) art. no. 6352912 (2013) : 1597-1616.

[14] Guang, X., Fu, F.-W., Zhang, Z. "Construction of network error correction codes in packet networks", IEEE Transactions on Information Theory 59(2) art. no. 6320693, (2013) : 1030-1047.

[15] Shah, N. B., Rashmi, K. V., Kumar, P. V., Ramchandran, K. "Interference alignment in regenerating codes for distributed storage: Necessity and code constructions", IEEE Transactions on Information Theory 5(4) art. no. 6096412 (2012) : 2134-2158.

[16] Hu, Y., Xu, Y., Wang, X., Zhan, C., Li, P. "Cooperative recovery of distributed storage systems from multiple losses with network coding", IEEE Journal on Selected Areas in Communica tions 28 (2) art. no. 5402494 (2010) : 268-276.

[17] Silva, D., Kschischang, F. R. "Security for wiretap networks via rank-metric codes", IEEE International Symposium on Information Theory - Proceedings art. no. 4594971 (2008) : 176-180.

[18] Fragouli, C., Soljanin, E. "Information flow decomposition for network coding", IEEE Trans- actions on Information Theory 52(3) (2006) : 829-848.

[19] Gupta, K. C., Ray, I. G., "Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications", Cryptography and Communications 7 (2015) : 257-287.

[20] Liu, M., Sim, S. M., "Lightweight MDS generalized circulant matrices", International Conference on Fast Software Encryption, Lecture Notes in Computer Science 9783 Springer, Berlin, Heidelberg (2016) : 101-120.

[21] Sarkar, S., Syed, H., "Lightweight diffusion layer: Importance of Toeplitz matrices", IACR Trans. Symmetric Cryptol. (2016) : 95-113.

[22] Sarkar, S., Syed, H., "Analysis of toeplitz MDS matrices", ACISP 2017, LNCS 10343 (2017) : 3-18.