ELEMENTS OF MDS CODES VIA EXTENDED CAUCHY MATRICES

[1]Dr. Rajesh Kumar Saini, [2]Dr.Binny Gupta

[1]Seth R. N. Ruia Govt. College, Ramgarh Shekhawati
[2]SGN Khalsa P.G. College, Sri Ganganagar

ABSTRACT: An (n,k,d) linear code over the finite field F = GF(q) is maximum- distance separable(MDS) if it attains the Singleton bound d ≤ n-k+1. A k × n matrix G over F is a generator matrix of an MDS code if and only if every k columns of G are linearly Independent. In most cases, error patterns with slightly more than D/2 error can be corrected by an (N, K) maximum- distance separable (MDS) code. Earlier the complexity of computation increased with number of additional errors, where a single error could be amended with an acceptable degree of computation. To fight out this problem Sudan's algorithm (1997) more errors can be corrected, in addition to this provides proof that for a limited number of errors, the correct codeword is always on a very small list of possible transmitted words. The right codeword is always on a very small list of possible transmitted words.

Keywords: Maximum- distance separable, transmitted words, codes, element

1. INTRODUCTION

An (n,k,d) linear code over the finite field F = GF(q) is maximum- distance separable(MDS) if it attains the Singleton bound d ≤ n-k+1. A k × n matrix G over F is a generator matrix of an MDS code if and only if all k columns of G are linearly Independent. If G is a systematic generator matrix i.e., G = [I, A], I being the identity matrix of order k, and A is a k×(n-k) matrix, then G generates an MDS code if and only if every square submatrix of A is nonsingular. Such matrix A will be called super regular.

When k = 1, there exist arbitrarily long MDS codes, e.g., repetition codes, and

when k ≥ q, a code is MDS only if it has minimum distance ≤ 2. Therefore, Roth and Lempel (1989) worked only with codes of dimension k, 2 ≤ k ≤ q-1. In this case, it is known that MDS codes cannot be arbitrarily long. Let $N_{max}(k,q)$, 2 ≤ k ≤ q-1,be the maximal length of any MDS code of dimension k over GF(q).Then, q+1 ≤ $N_{max}(k,q)$ ≤ q+k-1. Furthermore, for some special cases of k and q, it can be shown that N_{max} (k, q) = q+1.

A well-known family of MDS codes is the set of generalized Reed-Solomon (GRS) codes. Let $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ be a vector of distinct element of F, and let $v = (v_0, v_1, \cdots, v_{n-1})$ be a vector of nonzero element of F.C is a GRS (n, k, α, v), if it has a generator matrix of the form G = [G_0 G_1 ⋯ G_{n-1}], (1.1)

Where the G_i are columns of the for $G_i = (v_i, v_i\alpha_i, v_i\alpha_i^2, \cdots, v_i\ \alpha_i^{k-1})^T$, $0 \le i \le n-1$.

This definition includes extended GRS codes, for which one of the α_i is 0. A further extension that preserves the MDS property is possible by allowing a column of the form

$$G_\infty = (0, 0, \cdots, 0, v_\infty)^T,$$

Where v_∞ is a nonzero element of Field F. Such a column is said to correspond to the infinity "element". In this case the code is called a generalized doubly extended RS code (GDRS), and the notation

GDRS (n + 1, k, α, v) in terms of the vectors a and v by abusing notation and writing

$$\alpha = (\alpha_1, \alpha_2, ..., \alpha_{s-1}, \infty, \alpha_s, ..., \alpha_n)$$

and

v= (v_1,v_2,….,v_{s-1}, v_∞ ,v_s,…,v_n),

where s is the index of G_∞, in Serge (1955) and Thas (1968) considered GRS codes corresponds to a normal rational curve, in geometric terms.

Roth and Seroussi (1985) told that a matrix of the form G = [I A] generates a GRS code iff A = [a_{ij}] is a Cauchy matrix.i.e.,

$$a_{ij} = \frac{c_i d_j}{x_i + y_j}, \qquad 0 \le i \le k-1, \quad 0 \le j \le n-k-1,$$ Where the x_i and y_j are distinct element of F, $x_i + y_j \neq 0$ for all i and j, and c_i,d_j ≠ 0.Given a k × r Cauchy matrix A = [a_{ij}] over F = GF(q), according to Roth(1989) we can always assume $a_{0j} = d_j$ and $a_{1j} = d_1 y_j^{-1}$,0 ≤ j ≤ r-1. A is called an extended Cauchy matrix if it has a row (column) of ones, and deleting this row (column) transforms A into a Cauchy matrix.

2. LITERATUTRE REVIEW

Binbin Pang(2021) Entanglement-assisted quantum error-correcting codes (EAQECCs) can be obtained from arbitrary classical linear codes based on the entanglement-assisted stabilizer formalism, which greatly promoted the development of quantum coding theory. In this paper, we construct several families of [Formula: see text]-ary entanglement-assisted quantum maximum-distance-separable (EAQMDS) codes of lengths [Formula: see text] with flexible parameters as to the minimum distance [Formula: see text]

and the number [Formula: see text] of maximally entangled states. Most of the obtained EAQMDS codes have larger minimum distances than the codes available in the literature.

Hai Q. Dinh (2021) Symbol-pair codes are used to protect against symbol-pair errors in high density data storage systems. One of the most important tasks in symbol-pair coding theory is to design MDS codes. MDS symbol-pair codes are optimal in the sense that such codes attain the Singleton bound. In this paper, a new class of MDS symbol-pair codes with code-length 5p and optimal pair distance of 7 is established. It is shown that for any prime p ≡ 1 (mod 5), we can always construct four p-ary MDS symbol-pair cyclic codes of length 5p of largest possible pair distance 7. We also completely determined all MDS symbol-pair and MDS b-symbol codes of length p s and 2p s over F p m + uF p m by filling in some missing cases, and rectifying some gaps in Type 3 codes of recent papers. As an applications of our results, we use MAGMA to provide many examples of new MDS codes over F p m and F p m + uF p m

Elif Segah Oztas (2021) MDS codes are elegant constructions in coding theory and have mode important applications in cryptography, network coding, distributed data storage, communication systems et. 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 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 obtain where $n \leq q$. There are some approaches for constructing MDS matrices such that Vandermonde matrix, circulant matrix, Cauchy matrix, Toeplitz matrices etc. [2, 3,10,44–47]. All of them compute and improve their method over the defined field in the papers. However, calculation complexity increases over the field which has high cardinality for any construction methods for MSD codes, especially in the recursive generating method.

Ziling Heng (2020) Recently, subfield codes of geometric codes over large finite fields $\gf(q)$ with dimension 3 and 4 were studied and distance-optimal subfield codes over $\gf(p)$ were obtained, where $q=p^m$. The key idea for obtaining good subfield codes over small fields is to choose very good linear codes over an extension field with small dimension. This paper first presents a general construction of $[q+1, 2, q]$ MDS codes over $\gf(q)$, and then study the subfield codes over $\gf(p)$ of some of the $[q+1, 2,q]$ MDS codes over $\gf(q)$. Several families of distance-optimal codes over small fields are produced

Qiuyan Wang (2020) A linear code with parameters of the form $[n, k, n-k+1]$ is referred to as an MDS (maximum distance separable) code. A linear code with parameters of the form $[n, k, n-k]$ is said to be almost MDS (i.e., almost maximum distance separable) or AMDS for short. A code is said to be near maximum distance separable (in short, near MDS or NMDS) if both the code and its dual are almost maximum distance separable. Near MDS codes correspond to interesting objects in finite geometry and have nice applications in combinatorics and cryptography. In this paper, seven infinite families of $[2^m+1, 3, 2^m-2]$ near MDS codes over $\gf(2^m)$ and seven infinite families of $[2^m+2, 3, 2^m-1]$ near MDS codes over $\gf(2^m)$ are constructed with special oval polynomials for odd m. In addition, nine infinite families of optimal $[2^m+3, 3, 2^m]$ near MDS codes over $\gf(2^m)$ are constructed with oval polynomials in general.

3. BOUNDS ON THE LENGTHS OF MDS CODES

By definition, a GRS code with $2 \leq k \leq q-1$ may be of length at most $q+1$. For $2 \leq k \leq q-1$, let $N_{min}(k,q)$ be minimal integer, if any, such that every [n,k] MDS code over F with $n \geq N_{min}(k,q)$ is GRS; if no such integer exists, $N_{min}(k,q) = q+2$. Clearly, $N_{min}(2,q) = 2$, and so $N_{max}(2,q) = q+1$. To obtain an upper bound on $N_{min}(k,q)$ for larger values of k, we make use of the following result.

Lemma 1.1: If q is even, every [n,3] MDS code over GF(q) with $(q-1)\left(\left(\sqrt{q-1}-7\right)/4\right) < n \leq q$ is GRS.

Lemma 1.2: Given a k × r extended Cauchy matrix A = $[a_{ij}]$ over GF(q), we can always assume $a_{0j} = d_j$ and $a_{1j} = 1, 0 \leq j \leq r-1$.

Proof: Let C be an [r+k, k] GERS code with a given standard generator matrix G of the form (1.1). First, we show that C has another standard generator matrix $\overline{G}$ with G_0 corresponding to infinity and G_1 corresponding to one. Assume that the first column of G corresponds to some element $\alpha_0 \in$ F. MacWilliams and Slone (1977) considered a k × k nonsingular matrix T exits such that the ith column in $\hat{G} = T.G$ is given by

$\hat{G}_i = v_i\left(1 \quad (\alpha_i - \alpha_0) \quad . \quad . \quad . \quad (\alpha_i - \alpha_0)^{k-1}\right)$ The infinity column of G, if any, remains unchanged. Thus, the first column of $\hat{G}$ corresponds to the zero element. Reversing the order of the rows of $\hat{G}$, we obtained a standard generated matrix $\tilde{G}$ with its first column corresponding to infinity. As before, there now exists a linear transformation on the row of $\tilde{G}$ yielding a standard generator matrix $\overline{G}$ with the desired first two columns.

Second, let [I A] be the (unique) systematic generator matrix of C. Then A is a extended Cauchy matrix and its rows, being in a one-to-one correspondence with the first k coordinates of C, can be associated with the first k columns of any standard generator matrix of C. In particular, associating the rows of A with the first k columns of $\overline{G}$ yields $a_{0j} = c_0 d_j$ and $a_{1j} = c_1$. Now, normalizing the parameters involved, we can always set $c_0 = c_1 = 1$.

4. APPLICATION TO SUPERREGULAR MATRI

Let C be a GDRS(n+1, k, α, v) code defined by $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{s-1}, \infty, \alpha_s, \cdots, \alpha_{n-1})$ And $v = (v_0, v_1, \cdots, v_{s-1}, v_\infty, v_s, \cdots, v_{n-1})$, with $k - 1 < s \leq n$. Then C has a generator matrix of the form $[I \ \overline{A}]$, where $\overline{A} = [A_0, A_1, \cdots, A_{s-k}, A_\infty, A_{s-k+1}, \cdots, A_{n-k+1}]$ is a k×(n+1-k) GEC matrix obtained from the Cauchy matrix A by inserting the column. $A_\infty = d_\infty(c_0, c_1, \cdots, c_{k-1})^T$ before the (s-k+1)th column of A if $s < n$, or as the last column if $s = n$. Here $d_\infty = v_\infty$ and take $c_0 = c_1 = 1$.The results of the previous section on MDS codes be expressed in terms of superregular matrix with the subclass of Cauhy matrices corresponding to GRS codes. For instance, the analog of Lemma 5 takes the following form. Suppose there exist integer $s \geq 1$, $t \geq 3$ such that every s×t superregular matrix over F = GF(q) is a extended Cauchy matrix. Then, for every $r \geq t$, each s × r matrix is a superregular matrix if and only if it is a extended Cauchy matrix.

Let A = [a_{ij}] be a k × r matrix over F with $a_{ij} \neq 0$ for all $0 \le i \le k-1$ and $0 \le j \le r-1$, and $0 \le j \le r-1$, and let $A^c = \left[a_{ij}^{-1}\right]$; that is, every entry of A^c is the inverse of the corresponding entry of A.

Lemma 1.3: Let A be a k × (r + 1) matrix over F with nonzero entries. Then A is a Generalized Extended Cauchy (GEC) matrix if and only if A^c satisfies the following two conditions:

1. every 2×2 submatrix of A^c is nonsingular.
2. every 3×3 submatrix of A^c is singular.

Proof: The lemma holds trivially min (k, r + 1) ≤ 2. Therefore, we assume that k, r+1 ≥ 3. First, we prove the "only if" part. Suppose A is a generalized extended Cauchy matrix. So

A = [A_0, A_1, ⋯ ,A_{s-1}, A_∞, A_s, ⋯ , A_{r-1}]

Then, the first row of A^c is given by

$$a_0^c = \left(\frac{1}{d_0} \; \frac{1}{d_1} \; \cdots \; \frac{1}{d_{s-1}} \; \frac{1}{d_\infty} \; \frac{1}{d_s} \; \cdots \; \frac{1}{d_{r-1}}\right) \quad (1.2)$$

The second row of A^c is given by

$$a_1^c = \left(\frac{y_0}{d_0} \frac{y_1}{d_1} \cdots \frac{y_{s-1}}{d_{s-1}} \frac{1}{d_\infty} \frac{y_s}{d_s} \cdots \frac{y_{r-1}}{d_{r-1}}\right) \quad (1.3)$$

And the ith row of A^c, $2 \le i \le k-1$, is given by

$$a_i^c = \left(\frac{x_i + y_0}{c_i d_0} \frac{x_i + y_1}{c_i d_1} \cdots \frac{1}{c_i d_\infty} \cdots \frac{x_i + y_{r-1}}{c_i d_{r-1}}\right),$$

Therefore,

$$a_i^c = \frac{x_i}{c_i} a_o^c + \frac{1}{c_i} a_1^c, \quad 2 \le i \le k-1, \; o \le j \le s-1 \text{and } s \le j \le r-1$$

And $$a_{i\infty}^c = \frac{1}{2c_i} a_{0\infty}^c + \frac{1}{2c_i} a_{1\infty}^c$$

Which means that every row in A^c is a linear combination of its first two rows, thus proving b). Condition a) follows from the fact that a 2 × 2 submatrix of A^c is nonsingular if and only if the corresponding 2 × 2 submatrix of A is nonsingular.

For the "if" part, suppose A^c is a k × r + 1 matrix with nonzero entries satisfying a) and b). Then, the first two rows of A^c are linearly independent and their entries can still be expressed as in (7.3.1) and (7.3.2), with nonzero d_i and nonzero and distinct y_j. Now, b) implies that every row a_i^c, $2 \le i \le k-1$, is linearly depended on the first two rows of A^c, i.e.,

$a_{ij}^c = \alpha_i a_{0j}^c + \beta_i a_{1j}^c, \quad 2 \le i \le k-1, \quad 0 \le j \le r-1,$ For some $\alpha_i, \beta_i \neq 0.$ Define $c_i = \beta_i^{-1}$ and $x_i = \alpha_i \beta_i^{-1}$, $2 \le i \le k-1$. Since every two rows of A^c are linearly independent, the x_i are distinct.

Lemma 1.4 leads to efficient ways of verifying whether a given k × n matrix generates a GRS code. Let G_1 denote a square matrix of order k, and let G = [G_1,G_2]. The first step in the test of G is to verify that G_1 is nonsingular. Then, apply the transformation $G_1^{-1} \cdot G = [I \quad A]$ and check that A = [a_{ij}] satisfies the following two conditions:

1) the ratios a_{0j}/a_{1i}, $0 \le j \le n-k-1$, are all distinct; and
2) the rows of A^c are pairwise independent and are all spanned by the first two rows of A^c. It can be readily verified that these two conditions are equivalent to those of Lemma 6.3.1, together with Theorem7.2.1, implies the following result.

Theorem 1.5: Let F = GF(q), q even, and let A be a k × r matrix over F with $\max(k, r) > q + 1 - \left(\left(\sqrt{q+1} + 5\right)/4\right)$. If all the entries of A are nonzero, then A is super regular if and if every 2×2 submatrix of A^c is nonsingular and every 3×3 submatrix of A^c is singular.

5. CONCLUSION

An (n,k,d) linear code over the finite field F = GF(q) is maximum- distance separable(MDS) if it attains the Singleton bound d ≤ n-k+1. A k × n matrix G over F is a generator matrix of an MDS code if and only if all k columns of G are linearly Independent. If G is a systematic generator matrix i.e., G = [I,A], I being the identity matrix of order k, and A is a k×(n-k) matrix, then G generates an MDS code if and only if every square submatrix of A is nonsingular. Such matrix A will be called superregular. When k = 1, there exist arbitrarily long MDS codes, e.g. repetition codes, and when k ≥ q, a code is MDS only if it has minimum distance ≤ 2. Therefore, Roth and Lempel(1989) worked only with codes of dimension k, 2 ≤ k ≤ q-1. In this case, it is known that MDS codes cannot be arbitrarily long. Let $N_{max}(k,q)$, 2 ≤ k ≤ q-1,be the maximal length of any MDS code of dimension k over GF(q).Then, q+1 ≤ $N_{max}(k,q)$ ≤ q+k-1. Furthermore, for some special cases of k and q, it can be shown that $N_{max}(k, q)$ = q+1. By definition, a GRS code with 2 ≤ k ≤ q-1 may be of length at most q+1. For 2 ≤ k ≤ q-1, let $N_{min}(k,q)$ be minimal integer, if any, such that every [n,k] MDS code over F with n ≥ $N_{min}(k,q)$ is GRS; if no such integer exists, $N_{min}(k,q)$ = q+2. Clearly, $N_{min}(2,q)$ = 2, and so $N_{max}(2,q)$ = q+1. To obtain an upper bound on $N_{min}(k,q)$ for larger values of k, we make use of the following result. Let C be a GDRS(n+1, k, α, v) code defined by α = (α_0,α_1,⋯ ,α_{s-1},∞,α_s, ⋯ ,α_{n-1}) And v = (v_0,v_1, ⋯ ,v_{s-1},v_∞,v_s, ⋯ ,v_{n-1}), with k - 1 < s ≤n. Then C has a generator matrix of the form [I $\overline{A}$], where $\overline{A}$ = [A_0,A_1, ⋯ ,A_{s-k},A_∞,A_{s-k+1}, ⋯ ,A_{n-k+1}] is a k×(n+1-k) GEC matrix obtained from

the Cauchy matrix A by inserting the column. $A_\infty = d_\infty(c_0, c_1, \cdots, c_{k-1})^T$ before the (s-k+1)th column of A if $s < n$, or as the last column if $s = n$. Here $d_\infty = v_\infty$ and take $c_0 = c_1 = 1$.The results of the previous section on MDS codes be expressed in terms of superregular matrix with the subclass of Cauhy matrices corresponding to GRS codes. For instance, the analog of Lemma 5 takes the following form. Suppose there exist integer $s \geq 1$, $t \geq 3$ such that every $s \times t$ superregular matrix over $F = GF(q)$ is a extended Cauchy matrix. Then, for every $r \geq t$, each $s \times r$ matrix is a superregular matrix if and only if it is a extended Cauchy matrix.

REFERENCES

1. Dinh, Hai & Nguyen, Bac & Kumar Singh, Abhay & Yamaka, Woraphon. (2021). MDS Constacyclic Codes and MDS Symbol-Pair Constacyclic Codes. IEEE Access. 9. 10.1109/ACCESS.2021.3117569.
2. Oztas, Elif Segah. (2021). Lifted MDS Codes over Finite Fields.
3. Pang, Binbin & Zhu, Shixin & Wang, Liqi. (2021). New entanglement-assisted quantum MDS codes. International Journal of Quantum Information. 19. 2150016. 10.1142/S0219749921500167.
4. Heng, Ziling & Ding, Cunsheng. (2020). The Subfield Codes of $[q+1, 2, q]$ MDS Codes.
5. Wang, Qiuyan & Heng, Ziling. (2020). Near MDS codes from oval polynomials.
6. Kokkala, Janne & Krotov, Denis & Östergård, Patric. (2015). On the Classification of MDS Codes. IEEE Transactions on Information Theory. 61. 6485-6492. 10.1109/TIT.2015.2488659.
7. Hurley, Ted. (2019). MDS codes over finite fields.
8. Blaum, Mario & Roth, R.M.. (1999). On lowest density MDS codes. Information Theory, IEEE Transactions on. 45. 46 - 59. 10.1109/18.746771.
9. Ezerman, Martianus & Grassl, Markus & Solé, Patrick. (2009). The weights in MDS codes. Information Theory, IEEE Transactions on. 57. 10.1109/TIT.2010.2090246.
10. Glynn, David. (2011). A condition for arcs and MDS codes. Designs Codes and Cryptography. 58. 215-218. 10.1007/s10623-010-9404-x.
11. Dougherty, Steven & Han, Sunghyu. (2010). Higher weights and generalized MDS codes. J. Korean Math. Soc. 47. 1167-1182. 10.4134/JKMS.2010.47.6.1167.
12. Suprijanto, Djoko & Anthony, A.. (2015). New examples of MDS group codes. Applied Mathematical Sciences. 9. 4897-4906. 10.12988/ams.2015.53253.
13. Jin, Lingfei & Xing, Chaoping. (2013). A construction of new quantum MDS codes. Information Theory, IEEE Transactions on. 60. 10.1109/TIT.2014.2299800.