



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

On MDS One Digit Extension of GTRS Codes

O.P.Vinocha¹, J.S.Bhullar², B.S.Brar³

¹Ferozepur College of Engineering and Technology, Ferozepur, Punjab, India

² Department of Applied Sciences, Malout Institute of Management and Information Technology (MIMIT),
Malout, Punjab, India

³Department of Applied Sciences, Baba Farid College of Engineering and Technology, Bathinda, Punjab, India

Abstract: An (n, k, d) Generalised Doubly Extended Reed-Solomon (GDRS) code such that $2 \leq k \leq n - \left\lfloor \frac{(q-1)}{2} \right\rfloor$, ($k \neq 3$ if q is even) can be extended by one digit while preserving the MDS property if and only if the resulting extended code is also Generalised Reed-Solomon code. In this paper, we have extended Generalised Triply Extended Reed-Solomon (GTRS) code by one digit, and analysed the conditions under which this resulting extended GTRS code becomes MDS or otherwise. In this analysis, we have used the relation $2 \leq k \leq (n+2) - \left\lfloor \frac{(q+1)}{2} \right\rfloor$.

Keywords: Reed-Solomon code, Generalised Reed-Solomon code, Generalised Doubly Extended Reed-Solomon code, Generalised Triply Extended Reed-Solomon code, canonical generator matrix, singular column, regular column, linear combination.

I. Introduction

For every linear code (n, k, d) , we have: $d \leq n - k + 1$. This is known as The Singleton Bound. If $d = n - k + 1$, then (n, k, d) code C over finite field $F = GF(q)$, where q is a positive power of a prime, say $q = p^n$, p being prime, n being a positive integer, is called Maximum Distance Separable (MDS) code. The MDS codes are optimal. It means that they achieve the maximum possible minimum distance for given length(n) and dimension(k). It is known that for $k > 1$, the length of MDS codes of dimension k over finite field $F = GF(q)$ has maximum upper bound. It is denoted by symbol $m(q, k)$. It means that MDS codes of dimension k over finite field $F = GF(q)$ has maximum length, denoted by $m(q, k)$. For $k \geq q$, it has been verified that $m(q, k) = k + 1$. To find the exact value of $m(q, k)$ for $2 \leq k < q$, is an open problem. The generally believed conjecture is that for $2 \leq k < q$, $m(q, k) = q + 1$, except for the cases $k = 3$ and $k = q - 1$ with q even, in which case $m(q, k) = q + 2$. This conjecture has been proved for some values of q and k . Reed-Solomon (RS) codes are a special case of a larger family of MDS codes, which are called Generalised Reed-Solomon (GRS) codes. A code C is called GRS code, if it has a generator matrix:

$G = [g_{ij}]$,
where $g_{ij} = v_j \alpha_i^{j-1}$, $1 \leq i \leq k$, $1 \leq j \leq n$. Therefore, $G = [g_{ij}] = [v_j \alpha_i^{j-1}]$, $1 \leq i \leq k$, $1 \leq j \leq n$.

$$= \begin{bmatrix} g_{11} & g_{12} & g_{13} & \dots & g_{1n} \\ g_{21} & g_{22} & g_{23} & \dots & g_{2n} \\ g_{31} & g_{32} & g_{33} & \dots & g_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k-1,1} & g_{k-1,2} & g_{k-1,3} & \dots & g_{k-1,n} \\ g_{k1} & g_{k2} & g_{k3} & \dots & g_{kn} \end{bmatrix}_{k \times n} = \begin{bmatrix} v_1 & v_2 & \dots & v_n \\ v_1 \alpha_1 & v_2 \alpha_2 & \dots & v_n \alpha_n \\ v_1 \alpha_1^2 & v_2 \alpha_2^2 & \dots & v_n \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1 \alpha_1^{k-2} & v_2 \alpha_2^{k-2} & \dots & v_n \alpha_n^{k-2} \\ v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \dots & v_n \alpha_n^{k-1} \end{bmatrix}_{k \times n} \quad (1)$$

In this definition, α_i 's are distinct elements of field $F = GF(q)$; v_i 's are non-zero but not necessarily distinct elements of field $F = GF(q)$. Also α_i 's are called column generators of G ; v_i 's are called column multipliers of G . And G is called canonical generator matrix of code C . GRS codes exist for any length $n \leq q$. GRS codes can be extended by appending an extra column of the form:

$$(0, 0, 0, \dots, v)^T, v \neq 0. \quad (2)$$

to generator matrix G of the GRS code, while preserving MDS property. It means that if we append an extra column of the form (2) to generator matrix G of GRS code, then new generator matrix so obtained will be a generator matrix of new GRS code which is MDS. Therefore, extended GRS code will have a generator matrix G_1 of the form:

$$G_1 = \begin{bmatrix} v_1 & v_2 & \dots & v_n & 0 \\ v_1 \alpha_1 & v_2 \alpha_2 & \dots & v_n \alpha_n & 0 \\ v_1 \alpha_1^2 & v_2 \alpha_2^2 & \dots & v_n \alpha_n^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_1 \alpha_1^{k-2} & v_2 \alpha_2^{k-2} & \dots & v_n \alpha_n^{k-2} & \cdot \\ v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \dots & v_n \alpha_n^{k-1} & v \end{bmatrix}_{k \times (n+1)} \quad (3)$$

It should be noted that index of the extra column $(0,0,0,\dots,v)'$, $v \neq 0$, may be any. Here we have put it as the last column of G_1 .

It will be said that the extra column $(0,0,0,\dots,v)'$, $v \neq 0$, has v as column multiplier, and ∞ as column generator. The resulting code having G_1 as generator matrix, is called Generalised Doubly Extended Reed-Solomon(GDRS) code. The basic RS codes are defined as having non-zero elements of the field $F=GF(q)$ as column generators, that is, α_i 's are non-zero elements of the field $F=GF(q)$. The generators are successive powers of a field element, say α , whose order is the code-length n , i.e. $\alpha^n = e$ (identity element of field) $=1$. So, column generators of RS codes are like $\alpha^0(=1)$, α^1 , α^2 , α^3 , $\dots$. So, as a result, RS code becomes cyclic. For GRS codes, the column generators α_i 's are distinct elements of field $F=GF(q)$ including zero element of the field. Moreover, one column $(0,0,0,\dots,v)'$, $v \neq 0$, is appended to generator matrix G to have generator matrix G_1 of GDRS code. This explains why we call the resulting code as Generalised Doubly Extended Reed-Solomon(GDRS) code.

GDRS codes exist for any length $n \leq (q+1)$. Seroussi and Roth (1986) have proved that for $2 \leq k \leq \left\lfloor \frac{q}{2} \right\rfloor + 2$, except for $k = 3$ when q is even, GDRS codes of length $(q+1)$ cannot be further extended while preserving the MDS property. This means that for $2 \leq k \leq \left\lfloor \frac{q}{2} \right\rfloor + 2$, if a unique $(n = q+1, k)$ MDS code exists

over field $F=GF(q)$, then $m(q,k)=q+1$. This uniqueness is defined upto the equivalence relation which is as follows: Two codes C_1, C_2 over field $F = GF(q)$ are equivalent, if a permutation π on n symbols $\{1,2,3,\dots,n\}$ and n non-zero constants $a_1, a_2, \dots, a_n \in F = GF(q)$ exist, such that $C_2 = \{ a_1 c_{\pi(1)}, a_2 c_{\pi(2)}, \dots, a_n c_{\pi(n)} : (c_1, c_2, \dots, c_n) \in C_1 \}$.

For odd q , almost all known MDS codes of length $(q+1)$ are GDRS. In this connection, an example is given by Casse and Glynn, and presented by Hirschfeld(1983), which shows a $(n=q+1=10, k=5)$ MDS code, which is not GDRS code. This example falsifies the earlier believed conjecture that MDS codes of length $n=q+1$ over field $F=GF(q)$ are GDRS.

Seroussi and Roth (1986) have proved that a GDRS code of length n and dimension k , such that $2 \leq k \leq n - \left\lfloor \frac{(q-1)}{2} \right\rfloor$, can be extended by one digit while preserving MDS property, iff the resulting code is also MDS. It means that an (n,k) GDRS code over field $F=GF(q)$ with $2 \leq k \leq n - \left\lfloor \frac{(q-1)}{2} \right\rfloor$, can be uniquely extended to an MDS code of length $n=q+1$, which is GRS, and which cannot be extended further.

If length of GRS code is n , then length of GDRS code will be $(n+1)$. Let C be an $(n+1, k, d=(n+1)-k+1=n+2-k)$ GDRS code over field $F=GF(q)$. Let the vector of column generators of C be denoted by α , where $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1})$, α_i 's, $1 \leq i \leq (n+1)$ being distinct elements of field $F=GF(q) \cup \{\infty\}$. Let the vector of column multipliers of code C be denoted by v , where $v = (v_1, v_2, \dots, v_n, v_{n+1})$, v_i 's, $1 \leq i \leq (n+1)$ being non-zero elements of field $F=GF(q)$. Then we denote GDRS code by $GDRS(n+1, k, \alpha, v)$.

Let k be any positive integer. Let β be an element of field $F=GF(q)$. Then we denote the column vector $(1, \beta, \beta^2, \dots, \beta^{k-1})'_{k \times 1}$ by $u^k(\beta)$. So, $u^k(\beta) = (1, \beta, \beta^2, \dots, \beta^{k-1})'_{k \times 1}$. Also we define $u^k(\infty)$ as: $u^k(\infty) = (0, 0, 0, \dots, 1)_{k \times 1}$.

The canonical generator matrix of $GDRS(n+1, k, \alpha, v)$ code C is given by(in terms of above notations):

$$G_1 = [v_1 \cdot u^k(\alpha_1), v_2 \cdot u^k(\alpha_2), \dots, v_n \cdot u^k(\alpha_n), v \cdot u^k(\infty)]$$

$$= \begin{bmatrix} \begin{bmatrix} 1 \\ \alpha_1 \\ \alpha_1^2 \\ \vdots \\ \alpha_1^{k-1} \end{bmatrix} & \begin{bmatrix} 1 \\ \alpha_2 \\ \alpha_2^2 \\ \vdots \\ \alpha_2^{k-1} \end{bmatrix} & \dots & \begin{bmatrix} 1 \\ \alpha_n \\ \alpha_n^2 \\ \vdots \\ \alpha_n^{k-1} \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & \dots & v_n & 0 \\ v_1 \alpha_1 & v_2 \alpha_2 & \dots & v_n \alpha_n & 0 \\ v_1 \alpha_1^2 & v_2 \alpha_2^2 & \dots & v_n \alpha_n^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_1 \alpha_1^{k-2} & v_2 \alpha_2^{k-2} & \dots & v_n \alpha_n^{k-2} & \vdots \\ v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \dots & v_n \alpha_n^{k-1} & v \end{bmatrix}_{k \times (n+1)}$$

, which is same as (3).

In GDRS codes, we take column generators α_i 's as distinct elements of field $F=GF(q)$ including zero element of field. So, we can take one of the α_i 's equal to zero element of field. Let us take $\alpha_n = 0$. Then a generator matrix of GDRS code will become as:

$$G_1 = \begin{bmatrix} v_1 & v_2 & \dots & v_n & 0 \\ v_1\alpha_1 & v_2\alpha_2 & \dots & 0 & 0 \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_1\alpha_1^{k-2} & v_2\alpha_2^{k-2} & \dots & 0 & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & 0 & v \end{bmatrix}_{k \times (n+1)} \quad (4)$$

If we append one more column of the form $(0, 0, \dots, v_\infty)_{k \times 1}$, $v_\infty \neq 0 \in F = GF(q)$ to G_1 , then it will become a generator matrix G_2 of new code, called Generalised Triply Extended Reed-Solomon (GTRS) code. Therefore,

$$G_2 = \begin{bmatrix} v_1 & v_2 & \dots & v_n & 0 & 0 \\ v_1\alpha_1 & v_2\alpha_2 & \dots & 0 & 0 & 0 \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ v_1\alpha_1^{k-2} & v_2\alpha_2^{k-2} & \dots & 0 & \vdots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & 0 & v & v_\infty \end{bmatrix}_{k \times (n+2)} \quad (5)$$

Clearly, length of GTRS code will be $(n+2)$.

II. Some Lemmas and Definition As Pre-requisites

Lemma 1: An (n, k, d) code C is MDS iff every k columns of a generator matrix G of code C are L.I.

Lemma 2: Let $F = GF(q)$, $q > 3$ be the finite field. Let S be a subset of r distinct elements of $F = GF(q)$ such that

$$\left\lfloor \frac{(q+1)}{2} \right\rfloor + 2 < r \leq q. \text{ Let } a \in F - \{0\}, \text{ i.e. } a \text{ be a non-zero element of field } F = GF(q). \text{ Let } k \text{ be an integer such}$$

that $2 < k \leq r - \left\lfloor \frac{(q+1)}{2} \right\rfloor$. Then, for any subset $S' = \{ \alpha_1, \alpha_2, \dots, \alpha_{k-2} \}$ of set S of cardinality $(k-2)$, there

exist two elements α_{k-1}, α_k in S such that the vector

$$\mathbf{w} = \mathbf{u}^k(\alpha_1) + a \cdot \mathbf{u}^k(\infty) \quad (6)$$

lies in the linear span over field $F = GF(q)$ of the vectors $\mathbf{u}^k(\alpha_2), \mathbf{u}^k(\alpha_3), \dots, \mathbf{u}^k(\alpha_k)$.

Def. 1 : Let G_2 be the canonical generator matrix of GTRS $(n+2, k, \alpha, v)$ code over field $F = GF(q)$. Then we say that a column $v_i \cdot \mathbf{u}^k(\alpha_i) = v_i \cdot [1, \alpha_i, \alpha_i^2, \dots, \alpha_i^{k-1}]_{k \times 1}^T$ is singular if $\alpha_i = \infty$, and is regular otherwise.

Lemma 3: Let G_2 be the canonical generator matrix of GTRS $(n+2, k, \alpha, v)$ code over field $F = GF(q)$, where $2 \leq k$

$\leq n+2 - \left\lfloor \frac{(q+1)}{2} \right\rfloor$, and let $\mathbf{h} \in F^k$ be a column vector such that $\mathbf{h} \neq a \cdot \mathbf{u}^k(\infty)$ for any $a \in F = GF(q)$, and $\mathbf{h}$

can be expressed as a linear combination of $(k-1)$ columns of G_2 . Then $\mathbf{h}$ can be expressed as a linear combination of $(k-1)$ regular columns of G_2 .

III. Extension of GTRS $(n+2, k, \alpha, v)$ Code

Theorem 1 : Let C be a GTRS $(n+2, k, \alpha, v)$ code over finite field $F = GF(q)$, such that $2 \leq k \leq (n+2) -$

$\left\lfloor \frac{(q+1)}{2} \right\rfloor$. Let G_2 be canonical generator matrix of code C . Let $\mathbf{h}$ be a k -dimensional column vector over

field $F = GF(q)$.

(i) When $k=2$, and every non-zero column vector $\mathbf{h} \in F^k = F^2$ is equal to $v \cdot \mathbf{u}^2(\beta)$ for some $\beta \in F \cup \{\infty\}$, $v \in F - \{0\}$, and if β is not a column generator of G_2 , then extension of C generated by matrix $[G_2 | \mathbf{h}]$ will generate MDS code. (ii)

When $k=2$, and every non-zero column vector $\mathbf{h} \in F^k = F^2$ is equal to $v \cdot \mathbf{u}^2(\beta)$ for some $\beta \in F \cup \{\infty\}$, $v \in F - \{0\}$, and if β is a column generator of G_2 , then extension of C generated by matrix $[G_2 | \mathbf{h}]$ will not generate an MDS code.

(iii) Let G_2' is generator matrix of GTRS $(n+2, k+1, \alpha, v)$ code, G_2 being generator matrix of GTRS $(n+2, k, \alpha, v)$ code. Let $\mathbf{h} \in F^{k+1}$ be a column vector. Let $\mathbf{h}^k \in F^k$ be the vector obtained by deleting the last co-ordinate of $\mathbf{h}$. Let $\mathbf{h}^k = a \cdot \mathbf{u}^k(\infty)$ for some $a \in F = GF(q)$, and $a \neq 0$, i.e. if a is a zero element of field $F = GF(q)$. Then extension of

C generated by matrix $[G_2|\mathbf{h}]$ will generate an MDS code. If $a \neq 0$, i.e. if a is not zero element of field $F=GF(q)$, then extension of C generated by matrix $[G_2'|\mathbf{h}]$ will not generate an MDS code.

(iv) Let $\mathbf{h}^k \neq a \cdot \mathbf{u}^k(\infty)$ for some $a \in F=GF(q)$ and $\mathbf{h}^k$ can be expressed as a linear combination of $(k-1)$ columns of G_2 . Then extension of C generated by matrix $[G_2'|\mathbf{h}]$ will not generate an MDS code.

(v) Let $\mathbf{h}^k \neq a \cdot \mathbf{u}^k(\infty)$ for some $a \in F=GF(q)$, let $\mathbf{h}^k$ can not be expressed as a linear combination of $(k-1)$ columns of G_2 , and let $a=0$. Then extension of C generated by matrix $[G_2'|\mathbf{h}]$ will generate an MDS code. If $a \neq 0$, then extension of C generated by matrix $[G_2'|\mathbf{h}]$ will not generate an MDS code.

Proof : Here C is GTRS($n+2, k, \alpha, \mathbf{v}$) code, over finite field $F=GF(q)$, with canonical generator matrix G_2 , such that $2 \leq k \leq (n+2) - \left\lfloor \frac{(q+1)}{2} \right\rfloor$.

(i) Let $k=2$. Let $\beta \in F \cup \{\infty\}$. Now $\mathbf{u}^k(\beta) = (1, \beta, \beta^2, \dots, \beta^{k-1})_{k \times 1}$.

Therefore, $\mathbf{u}^2(\beta) = (1, \beta)_{2 \times 1} = \begin{bmatrix} 1 \\ \beta \end{bmatrix}$.

So, $\mathbf{v} \cdot \mathbf{u}^2(\beta) = \mathbf{v} \cdot \begin{bmatrix} 1 \\ \beta \end{bmatrix} = \begin{bmatrix} v \\ v \cdot \beta \end{bmatrix} \in F^2$, $\begin{bmatrix} v \\ v \cdot \beta \end{bmatrix}$ being non-zero, because $v \neq 0$. Let it be $\mathbf{h}$, being non-zero.

Therefore, non-zero $\mathbf{h} \in F^2 = \mathbf{v} \cdot \mathbf{u}^2(\beta)$.

Hence, when $k=2$, then every non-zero column vector $\mathbf{h} \in F^k = F^2$ is equal to $\mathbf{v} \cdot \mathbf{u}^2(\beta)$ for some $\beta \in F \cup \{\infty\}$. If β is not a column generator of G_2 , then vector $\mathbf{h} \in F^k = F^2$ will be some singular column. Therefore, $[G_2|\mathbf{h}]$ will be canonical generator matrix of further extended code. So, extension of C generated by matrix $[G_2|\mathbf{h}]$ will generate an MDS code.

(ii) But if β is a column generator of G_2 , then:

$$\mathbf{h} = \mathbf{v} \cdot \mathbf{u}^2(\beta) = \mathbf{v} \cdot (1, \beta) = \begin{bmatrix} v \\ v \cdot \beta \end{bmatrix} = (1) \cdot \begin{bmatrix} v \\ v \cdot \beta \end{bmatrix} \text{ is a linear combination of one column of } G_2$$

(because β being column generator of G_2 and $k=2$, so $\begin{bmatrix} v \\ v \cdot \beta \end{bmatrix}$ will be a column of G_2).

= a linear combination of $2-1=k-1$ column of G_2 .

Therefore, $[G_2|\mathbf{h}]$ will have $k=2$ columns, which will be L.D. (This follows from a result of Linear Algebra, which states: "Let $m > 1$. Then the vectors $v_1, v_2, \dots, v_m$ are LD iff one of them is a linear combination of the others"). Hence, $k=2$ columns of $[G_2|\mathbf{h}]$ will not be LI. So, according to Lemma 1, $[G_2|\mathbf{h}]$ will not generate an MDS code.

Let $k \geq 2$ when q is odd, and for some $k \geq 4$ when q is even.

(iii) Let G_2' is generator matrix of GTRS($n+2, k+1, \alpha, \mathbf{v}$) code, where $k+1 \leq (n+2) - \left\lfloor \frac{(q+1)}{2} \right\rfloor$. We have

already taken G_2 as generator matrix of GTRS($n+2, k, \alpha, \mathbf{v}$) code. It is clear that G_2 is of order $k \times (n+2)$ and G_2' is of order $(k+1) \times (n+2)$. Therefore, it should be noted that G_2 consists of the first k rows of G_2' except in the singular column where $\mathbf{v} \cdot \mathbf{u}^k(\infty)$ replaces the first k entries (zeros) of $\mathbf{v} \cdot \mathbf{u}^{k+1}(\infty)$, and $\mathbf{v}_\infty \cdot \mathbf{u}^k(\infty)$ replaces the first k entries (zeros) of $\mathbf{v}_\infty \cdot \mathbf{u}^{k+1}(\infty)$. This fact can be seen from the figures of G_2 and G_2' as follows:

$$G_2 = \begin{bmatrix} v_1 & v_2 & \dots & v_n & 0 & 0 \\ v_1\alpha_1 & v_2\alpha_2 & \dots & 0 & 0 & 0 \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ v_1\alpha_1^{k-2} & v_2\alpha_2^{k-2} & \dots & 0 & \vdots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & 0 & v & v_\infty \end{bmatrix}_{k \times (n+2)} \quad \text{and} \quad G_2' = \begin{bmatrix} v_1 & v_2 & \dots & v_n & 0 & 0 \\ v_1\alpha_1 & v_2\alpha_2 & \dots & 0 & 0 & 0 \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ v_1\alpha_1^{k-2} & v_2\alpha_2^{k-2} & \dots & 0 & 0 & 0 \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & 0 & 0 & 0 \\ v_1\alpha_1^k & v_2\alpha_2^k & \dots & 0 & v & v_\infty \end{bmatrix}_{(k+1) \times (n+2)} \quad (7)$$

Let $\mathbf{h} \in F^{k+1}$ be a column vector. Let $\mathbf{h}^k \in F^k$ be the vector obtained by deleting the last co-ordinate of $\mathbf{h}$. Therefore, we can write:

$$\mathbf{h} = \begin{bmatrix} \mathbf{h}^k \\ \eta \end{bmatrix}, \text{ where } \eta \in F=GF(q).$$

Let $\mathbf{h}^k = a \cdot \mathbf{u}^{k(\infty)}$ for some $a \in F = GF(q)$. If $a=0$, i.e. if a is zero element of field $F = GF(q)$, then:

$$\mathbf{h}^k = 0 \cdot \mathbf{u}^{k(\infty)} = 0 \cdot \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} = [0 \ 0 \ \dots \ 0]_{k \times 1}^T.$$

Therefore, $\mathbf{h} = \begin{bmatrix} h^k \\ \eta \end{bmatrix}_{(k+1) \times 1} = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ \eta \end{bmatrix}_{(k+1) \times 1} = \eta \cdot \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 1 \end{bmatrix}_{(k+1) \times 1}$

Hence, $\mathbf{h} = \eta \cdot \mathbf{u}^{k+1(\infty)}$, $\eta \in F = GF(q)$, not necessarily column generator of G_2' . So, vector $\mathbf{h}$ will be some singular column G_2' . Therefore, $[G_2' | \mathbf{h}]$ will be canonical generator matrix of further extended code. So, extension of C generated by matrix $[G_2' | \mathbf{h}]$ will generate an MDS code. Let $\mathbf{h}^k = a \cdot \mathbf{u}^{k(\infty)}$ for some $a \in F = GF(q)$, and $a \neq 0$, i.e. if a is not zero element of field $F = GF(q)$.

$$\begin{aligned} \text{Then: } \mathbf{h} &= \begin{bmatrix} h^k \\ \eta \end{bmatrix}, \eta \in F = GF(q) \\ &= \begin{bmatrix} a \cdot u^{k(\infty)} \\ \eta \end{bmatrix}, a \in F = GF(q) \end{aligned}$$

$$= \begin{bmatrix} a \cdot [0 \ 0 \ 0 \ \dots \ 0 \ 1]_{k \times 1}^T \\ \eta \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 1 \end{bmatrix}_{k \times 1} \\ \eta \end{bmatrix} = a \cdot \begin{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ a \end{bmatrix}_{k \times 1} \\ \eta \end{bmatrix} = a \cdot \begin{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 1 \\ \eta/a \end{bmatrix}_{(k+1) \times 1} \\ \eta \end{bmatrix} = a \cdot \begin{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 1 \\ \delta \end{bmatrix}_{(k+1) \times 1} \\ \delta \end{bmatrix}_{(k+1) \times 1},$$

where $\delta = \eta/a$, $a \neq 0$, $a \in F$.

Let us take $\delta = \sum_{i=1}^k \alpha_{ji}$.

Therefore, $\mathbf{h} = a \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 1 \\ \sum_{i=1}^k \alpha_{ji} \end{bmatrix}_{(k+1) \times 1} = a \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 1 \\ \alpha_{j1} + \alpha_{j2} + \dots + \alpha_{jk} \end{bmatrix}_{(k+1) \times 1}$

$$= a. \left(\begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 1 \\ \alpha_{j1} \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ \alpha_{j2} \end{bmatrix} + \dots + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ \alpha_{jk} \end{bmatrix} \right)_{(k+1) \times 1} = a. [0 \ 0 \ 0 \ \dots \ 0 \ 1 \ \alpha_{j1}]'_{(k+1) \times 1} + a. [0 \ 0 \ 0 \ \dots \ 0 \ 0 \ \alpha_{j2}]'_{(k+1) \times 1} + \dots + a. [0 \ 0 \ 0 \ \dots \ 0 \ 0 \ \alpha_{jk}]'_{(k+1) \times 1}.$$

Therefore, **h** is a linear combination of **k** vectors:

$$[0 \ 0 \ 0 \ \dots \ 0 \ 1 \ \alpha_{j1}]'_{(k+1) \times 1}, [0 \ 0 \ 0 \ \dots \ 0 \ 0 \ \alpha_{j2}]'_{(k+1) \times 1}, \dots, [0 \ 0 \ 0 \ \dots \ 0 \ 0 \ \alpha_{jk}]'_{(k+1) \times 1}.$$

Let $\alpha_{j1}, \alpha_{j2}, \dots, \alpha_{jk-2}$ be $(k-2)$ distinct regular column generators of G_2' . We need that these $\alpha_{j1}, \alpha_{j2}, \dots, \alpha_{jk-2}$ do not add upto δ , because $\delta = \sum_{i=1}^k \alpha_{ji}$.

$$\text{Let us define: } \mu = \delta - \sum_{i=1}^{k-2} \alpha_{ji}. \quad (8)$$

Claim : There exist two distinct regular column generator $\alpha_{jk-1}, \alpha_{jk}$ of G_2' , which are not in the set:

$$\{\alpha_{j1}, \alpha_{j2}, \dots, \alpha_{jk-2}\} \text{ and which satisfy: } \alpha_{jk-1} + \alpha_{jk} = \mu. \quad (9)$$

Hence $\mu = \sum_{i=1}^k \alpha_{ji}$ and **h** will be a linear combination of **k** columns of G_2' .

Proof of Claim :

We note that the elements of field $F=GF(q)$ can be arranged in $\left\lfloor \frac{(q+1)}{2} \right\rfloor$ pairwise unordered and disjoint pairs: $P_i = \{a_i, b_i\}, 1 \leq i \leq \left\lfloor \frac{(q+1)}{2} \right\rfloor$,

$$\text{such that } a_i + b_i = \mu. \quad (11)$$

When q is odd, then there is exactly one such pair in which $a_i = b_i$. For example, because $q > 3$, so let $q = 5 = \{0, 1, 2, 3, 4\}$. Then $\mu = (3+4) \pmod{5} = 2$. Then unordered and disjoint pairs of the field $F=GF(q=5=5^1)$ elements such that $a_i + b_i = \mu = 2$ are: $\{0, 2\}, \{1, 1\}, \{3, 4\}$. So, there is exactly one pair $\{1, 1\}$, in which $a_i = b_i = 1$. If $\mu = (2+3) \pmod{5} = 0$, then unordered and disjoint pairs of the field $F=GF(q=5=5^1)$ elements such that $a_i + b_i = \mu = 2$ are: $\{0, 0\}, \{1, 4\}, \{2, 3\}$. So again there is exactly one pair $\{0, 0\}$ in which $a_i = b_i = 0$. Similarly, by choosing different elements of different fields $F=GF(q), q > 3, q$ is odd, and hence taking different values of μ , we can show that when q is odd, then there is exactly one pair in which $a_i = b_i$.

When q is even, then $a_i \neq b_i$ for all i . For example, because $q > 3$, so let $q = 8 = 2^3 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Then $\mu = (4+5) \pmod{8} = 1$. Then unordered and disjoint pairs of the field $F=GF(q=8=2^3)$ elements such that $a_i + b_i = \mu = 1$ are: $\{0, 1\}, \{2, 7\}, \{3, 6\}, \{4, 5\}$. If $\mu = (6+7) \pmod{8} = 5$, then unordered and disjoint pairs of the field $F=GF(q=8)$ elements such that $a_i + b_i = \mu = 5$ are: $\{0, 5\}, \{1, 4\}, \{2, 3\}, \{6, 7\}$. If $\mu = (4+4) \pmod{8} = 0$, then unordered and disjoint pairs of the field $F=GF(q=8)$ elements such that $a_i + b_i = \mu = 0$ are: $\{0, 0\}, \{1, 7\}, \{2, 6\}, \{3, 5\}, \{4, 4\}$. Therefore, if μ is taken as 0, then there is $a_i = b_i$ in one pair. If μ is not taken as 0, then $a_i \neq b_i$ for all i .

Therefore, we conclude that when q is odd (q being greater than 3), then there is exactly one such pair $\in P_i$, in which $a_i = b_i$. When q is even (q being greater than 3), $\mu \neq 0$, then $a_i \neq b_i$ for all i , and μ should

not be equal to zero, otherwise $\delta = \sum_{i=1}^{k-2} \alpha_{ji}$, which is not permissible, because $\delta = \sum_{i=1}^k \alpha_{ji}$.

Now in the Theorem, we have the condition: $2 \leq k \leq (n+2) - \left\lfloor \frac{(q+1)}{2} \right\rfloor$.

With respect to G_2' being a generator matrix of $GTRS(n+2, k+1, \mathbf{a}, \mathbf{v})$ code, the above condition becomes as:

$$2 \leq k+1 \leq (n+2) - \left\lfloor \frac{(q+1)}{2} \right\rfloor \Rightarrow k+1 \leq (n+2) - \left\lfloor \frac{(q+1)}{2} \right\rfloor \Rightarrow n+2-k-1 \geq \left\lfloor \frac{(q+1)}{2} \right\rfloor$$

$$\Rightarrow n-k+1 \geq \left\lfloor \frac{(q+1)}{2} \right\rfloor \Rightarrow (n)-(k-1) \geq \left\lfloor \frac{(q+1)}{2} \right\rfloor$$

So, we see that at least one of the pairs P_i will contain two distinct regular generators of G_2' , which are different from $\alpha_{j1}, \alpha_{j2}, \dots, \alpha_{jk-2}$, i.e. which are not in the set $\{\alpha_{j1}, \alpha_{j2}, \dots, \alpha_{jk-2}\}$ and which satisfy $\alpha_{jk-1} +$

$\alpha_{jk} = \mu$. Hence $\delta = \sum_{i=1}^k \alpha_{ji}$. So, $\mathbf{h}$ is a linear combination of k columns of G_2' , and hence $k+1$ columns of

$[G_2' | \mathbf{h}]$ are L.D. Hence $k+1$ columns of $[G_2' | \mathbf{h}]$ are not L.I. Hence by Lemma 1, $[G_2' | \mathbf{h}]$ will not generate an MDS code.

(iv) Let $\mathbf{h}^k \neq a \cdot \mathbf{u}^{k(\infty)}$ for some $a \in F = GF(q)$ and $\mathbf{h}^k$ can be expressed as a linear combination of $(k-1)$ columns of G_2 .

Here we see that conditions of Lemma 3 are satisfied. Therefore, $\mathbf{h}^k$ can be expressed as a linear combination of $(k-1)$ regular columns of G_2 . So, this linear combination does not include the singular columns of G_2 .

Therefore, $\mathbf{h}$ can be expressed as a linear combination of $(k-1)$ columns of G_2 , which give $\mathbf{h}^k$ in G_2 , extended to length $k+1$, plus, a suitable scalar multiple of $\mathbf{u}^{k+1(\infty)} = [0, 0, 0, \dots, 0, 0, 1]_{(k+1) \times 1}^T$, which is chosen such that the value of η is obtained in the $(k+1)^{st}$ entry.

Therefore, $\mathbf{h}$ may be like this:

$$\mathbf{h} = a_1 \begin{bmatrix} v_1 \\ v_1 \alpha_1 \\ v_1 \alpha_1^2 \\ \vdots \\ v_1 \alpha_1^{k-2} \\ v_1 \alpha_1^{k-1} \\ v_1 \alpha_1^k \end{bmatrix}_{(k+1) \times 1} + a_2 \begin{bmatrix} v_2 \\ v_2 \alpha_2 \\ v_2 \alpha_2^2 \\ \vdots \\ v_2 \alpha_2^{k-2} \\ v_2 \alpha_2^{k-1} \\ v_2 \alpha_2^k \end{bmatrix}_{(k+1) \times 1} + \dots + a_{k-1} \begin{bmatrix} v_{k-1} \\ v_{k-1} \alpha_{k-1} \\ v_{k-1} \alpha_{k-1}^2 \\ \vdots \\ v_{k-1} \alpha_{k-1}^{k-2} \\ v_{k-1} \alpha_{k-1}^{k-1} \\ v_{k-1} \alpha_{k-1}^k \end{bmatrix}_{(k+1) \times 1} + a_k \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 1 \end{bmatrix}_{(k+1) \times 1} \quad (12)$$

where a_i 's are scalars $\in$ field $F = GF(q)$. Clearly η will be given by the $(k+1)^{st}$ entry of $\mathbf{h}$, that is,

$$\eta = a_1 \cdot (v_1 \alpha_1^k) + a_2 \cdot (v_2 \alpha_2^k) + \dots + a_{k-1} \cdot (v_{k-1} \alpha_{k-1}^k) + a_k \cdot (1). \quad (13)$$

Therefore, $\mathbf{h}$ can be written as:

$$\mathbf{h} = a_1 \begin{bmatrix} v_1 \\ v_1 \alpha_1 \\ v_1 \alpha_1^2 \\ \vdots \\ v_1 \alpha_1^{k-2} \\ v_1 \alpha_1^{k-1} \end{bmatrix} + a_2 \begin{bmatrix} v_2 \\ v_2 \alpha_2 \\ v_2 \alpha_2^2 \\ \vdots \\ v_2 \alpha_2^{k-2} \\ v_2 \alpha_2^{k-1} \end{bmatrix} + \dots + a_{k-1} \begin{bmatrix} v_{k-1} \\ v_{k-1} \alpha_{k-1} \\ v_{k-1} \alpha_{k-1}^2 \\ \vdots \\ v_{k-1} \alpha_{k-1}^{k-2} \\ v_{k-1} \alpha_{k-1}^{k-1} \end{bmatrix} + a_k \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

$$a_1 (v_1 \alpha_1^k) + a_2 (v_2 \alpha_2^k) + \dots + a_{k-1} (v_{k-1} \alpha_{k-1}^k) + a_k (1)$$

$$= \begin{bmatrix} a_1 \begin{bmatrix} v_1 \\ v_1 \alpha_1 \\ v_1 \alpha_1^2 \\ \vdots \\ v_1 \alpha_1^{k-2} \\ v_1 \alpha_1^{k-1} \end{bmatrix} + a_2 \begin{bmatrix} v_2 \\ v_2 \alpha_2 \\ v_2 \alpha_2^2 \\ \vdots \\ v_2 \alpha_2^{k-2} \\ v_2 \alpha_2^{k-1} \end{bmatrix} + \dots + a_{k-1} \begin{bmatrix} v_{k-1} \\ v_{k-1} \alpha_{k-1} \\ v_{k-1} \alpha_{k-1}^2 \\ \vdots \\ v_{k-1} \alpha_{k-1}^{k-2} \\ v_{k-1} \alpha_{k-1}^{k-1} \end{bmatrix} + a_k \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \\ \eta \end{bmatrix} = \begin{bmatrix} h^k \\ \eta \end{bmatrix},$$

where $\mathbf{h}^k$ is a linear combination of (k-1) regular columns of G_2 .

Therefore, $\mathbf{h}$ can be expressed as a linear combination of k columns of G_2' , and hence k+1 columns of $[G_2'|\mathbf{h}]$ are L.D. Hence k+1 columns of $[G_2'|\mathbf{h}]$ are not L.I. Hence by Lemma 1, $[G_2'|\mathbf{h}]$ will not generate an MDS code.

(v) Let $\mathbf{h}^k \neq \mathbf{a} \cdot \mathbf{u}^{k(\infty)}$ for some $\mathbf{a} \in \mathbb{F} = \text{GF}(q)$ and let $\mathbf{h}^k$ can not be expressed as a linear combination of (k-1) columns of G_2 , and let $\mathbf{a} = 0$.

So, in this case, $\mathbf{h}^k$ can be appended to G_2 , while preserving MDS property.

Because $\mathbf{h}^k \neq \mathbf{a} \cdot \mathbf{u}^{k(\infty)}$ (given), so we can have:

$\mathbf{h}^k = \mathbf{v} \cdot \mathbf{u}^k(\lambda)$, where $v \neq 0$, and λ is not a column generator of G_2 and hence also not of G_2' .

$$\text{Consider: } \mathbf{h} = \mathbf{v} \cdot [\mathbf{u}^{k+1}(\lambda) + \mathbf{a} \cdot \mathbf{u}^{k+1}(\infty)] = \mathbf{v} \cdot \left(\begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \vdots \\ \lambda^{k-1} \\ \lambda^k \end{bmatrix} + \mathbf{a} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} v \\ v\lambda \\ v\lambda^2 \\ \vdots \\ \vdots \\ v\lambda^{k-1} \\ v\lambda^k + v\mathbf{a} \end{bmatrix}$$

If $\mathbf{a} = (\eta/v) - \lambda^k$, then $\mathbf{h}$ will become as:

$$\mathbf{h} = \begin{bmatrix} v \\ v\lambda \\ v\lambda^2 \\ \vdots \\ \vdots \\ v\lambda^{k-1} \\ v\lambda^k + v(\eta/v - \lambda^k) \end{bmatrix} = \begin{bmatrix} v \\ v\lambda \\ v\lambda^2 \\ \vdots \\ \vdots \\ v\lambda^{k-1} \\ v\lambda^k + \eta - v\lambda^k \end{bmatrix} = \begin{bmatrix} v \\ v\lambda \\ v\lambda^2 \\ \vdots \\ \vdots \\ v\lambda^{k-1} \\ \eta \end{bmatrix}$$

Therefore, difference between $\mathbf{h}^k$ and $\mathbf{h}$ is that if we delete η , i.e. (k+1)st entry of $\mathbf{h}$, from $\mathbf{h}$, we get $\mathbf{h}^k$, which is:

$$\mathbf{h}^k = \begin{bmatrix} v \\ v\lambda \\ v\lambda^2 \\ \vdots \\ \vdots \\ v\lambda^{k-1} \end{bmatrix} = \mathbf{v} \cdot \begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \vdots \\ \lambda^{k-1} \end{bmatrix}.$$

Therefore, $\mathbf{h}^k = \mathbf{v} \cdot \mathbf{u}^k(\lambda)$, which is there.

So, we can take $a = (\eta/v) - \lambda^k$. (14)

If $a=0$, then: $\mathbf{h} = v \cdot [\mathbf{u}^{k+1}(\lambda) + a \cdot \mathbf{u}^{k+1}(\infty)] = v \cdot \mathbf{u}^{k+1}(\lambda)$

Because λ is not a column generator of G_2 and hence also not of G_2' , therefore, $\mathbf{h}$ will be some singular column. Therefore, $[G_2'|\mathbf{h}]$ will be canonical generator matrix of further extended code. So, extension of C generated by matrix $[G_2'|\mathbf{h}]$ will generate an MDS code.

Let $\mathbf{h}^k \neq a \cdot \mathbf{u}^k(\infty)$ for some $a \in F = GF(q)$, let $\mathbf{h}^k$ can not be expressed as a linear combination of $(k-1)$ columns of G_2 , and let $a \neq 0$.

In this situation, we use Lemma 2 by taking number of elements of set S as $r = n+2$, so that S is: $S = \{\lambda, \alpha_2, \alpha_3, \dots, \alpha_n, \alpha_{n+1}, \alpha_{n+2}\}$ and S' (as subset of set S) = $\{\lambda, \alpha_2, \alpha_3, \dots, \alpha_{k-1}\}$, and because $\mathbf{h} = v \cdot [\mathbf{u}^{k+1}(\lambda) + a \cdot \mathbf{u}^{k+1}(\infty)]$, we see that $\mathbf{h}$ lies in the linear span over field $F = GF(q)$ of the vectors $v \cdot \mathbf{u}^{k+1}(\alpha_2)$, $v \cdot \mathbf{u}^{k+1}(\alpha_3)$, $\dots, v \cdot \mathbf{u}^{k+1}(\alpha_{k+1})$, that is, $\mathbf{h}$ can be expressed as a linear combination of vectors: $v \cdot \mathbf{u}^{k+1}(\alpha_2)$, $v \cdot \mathbf{u}^{k+1}(\alpha_3)$

$$), \dots, v \cdot \mathbf{u}^{k+1}(\alpha_{k+1}) \quad \text{i.e. of vectors:} \quad v \cdot \begin{bmatrix} 1 \\ \alpha_2 \\ \alpha_2^2 \\ \vdots \\ \alpha_2^k \end{bmatrix}, \quad v \cdot \begin{bmatrix} 1 \\ \alpha_3 \\ \alpha_3^2 \\ \vdots \\ \alpha_3^k \end{bmatrix}, \dots, \quad v \cdot \begin{bmatrix} 1 \\ \alpha_{k+1} \\ \alpha_{k+1}^2 \\ \vdots \\ \alpha_{k+1}^k \end{bmatrix} \quad \text{i.e. of vectors:}$$

$$\begin{bmatrix} v \\ v\alpha_2 \\ v\alpha_2^2 \\ \vdots \\ v\alpha_2^k \end{bmatrix}, \quad \begin{bmatrix} v \\ v\alpha_3 \\ v\alpha_3^2 \\ \vdots \\ v\alpha_3^k \end{bmatrix}, \dots, \quad \begin{bmatrix} v \\ v\alpha_{k+1} \\ v\alpha_{k+1}^2 \\ \vdots \\ v\alpha_{k+1}^k \end{bmatrix} \quad \text{i.e. of } k \text{ columns of } G_2'.$$

Therefore, $\mathbf{h}$ can be expressed as a linear combination of k columns of G_2' , and hence $k+1$ columns of $[G_2'|\mathbf{h}]$ are L.D. Hence $k+1$ columns of $[G_2'|\mathbf{h}]$ are not L.I. Hence by Lemma 1, $[G_2'|\mathbf{h}]$ will not generate an MDS code.

References

1. MacWilliams, F.J. and Sloane, N.J.A. (1977): "The Theory of Error-Correcting Codes". Amsterdam: North Holland, 1977.
2. Hirschfeld, J.W.P. (1983): "Maximum Sets in Finite Projective Spaces", in Surveys in Combinatorics, LMS Lecture Notes Series, E.K. Lloyd, Ed. Cambridge: Cambridge Univ. Press, 1983, pp. 55-76.
3. Seroussi, Gadiel and Roth, Ron M. (1986): "On MDS Extensions of Generalised Reed Solomon Codes", IEEE Transactions on Information Theory, Vol. IT-32, No. 3, May, 1986.