International Journal of Engineering, Science and Mathematics
Vol. 7 Issue 5, May 2018,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A Construction of GTRS Code

B.S.Brar*

Abstract: The length of the GRS code is enlarged in relation to the increasing of the columns of the systematic generator GC matrix, thereby transmission of the information becoming more safe. A new GTRS code is constructed having enlarged length and having both enlarged length and increased number of message-symbols, thereby making transmission of the information more safe; increasing the number of message-symbols to be transmitted; and increasing the number of codewords within the code resulting in enhancing the utility of the code.

Keywords: MDS code, RS code, GRS code, GDRS code, GTRS code, systematic generator matrix, non-singular matrix, finite field.

---

*Department of Applied Sciences, Baba Farid College of Engineering and Technology, Bathinda, Punjab (India)

---

1. Introduction

If d = n – k + 1, then a linear code depicted as [n, k, d], is known as Maximum Distance Separable (MDS) code over finite field F.[1]. If C be an [n, k, d] code, having systematic generator matrix G given by G = [I | A], I being the identity matrix of order k, A being k × (n - k) matrix, then code C will be MDS if and only if every square submatrix of matrix A is non-singular. If $a_{ij} = 1/(x_i + y_j)$, where $x_1, x_2, . . . , x_m$; $y_1, y_2, ... , y_n$ all from finite field F, then the matrix A having order m × n, is known as a Cauchy matrix.[4]. If the matrix A has one row (or column) of 1s, and deletion of such a row (or column) of 1s changes the A into $\widehat{A}$, where matrix $\widehat{A}$ is Cauchy matrix, then the matrix A is known as Extended Cauchy matrix. Each square sub-matrix of the Extended Cauchy matrix A will be non-singular if each square sub-matrix of Cauchy matrix $\widehat{A}$ is non-singular and vice-versa. Let any vector **z** be: **z** = $(z_1, z_2, ... , z_\ell)$. If D(**z**) is the diagonal matrix having order ℓ with $D_{ii} = z_i$ as diagonal entries, then matrix A of order m × n is known as Generalised Cauchy matrix, if A = D(**c**).$\bar{A}$.D(**d**), where $\bar{A}$ is an m × n Cauchy matrix, **c** = $(c_1, c_2, . . . , c_m)$, **d** = $(d_1, d_2, ... , d_n)$ are the vectors having non-zero elements from the finite field F. So, A will be equal to $\left[\frac{c_i\, d_j}{x_i + y_j}\right]_{m\times n}$; c_i, d_j, x_i, y_j belonging to the finite field F, values of i and j varying from 1 to m and from 1 to n respectively. If all the square sub-matrices of $\bar{A}$ are not singular, then all square sub-matrices of the matrix A will also be non singular. So for MDS code having parameters n, k, and d, a systematic generator matrix can be constructed by the process of linkage of I_k with Generalised Cauchy matrix having order k × (n - k), where GC matrix is suitably defined. If $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, ... , \alpha_n)$ be the vector having different elements from the finite field F, if $\mathbf{v} = (v_1, v_2, ... , v_n)$ be the vector of non-zero elements from the finite field F, these non-zero elements may not be necessarily different elements, then the code C is known as GRS [4], which is written as GRS (n, k, **α, v**), if it has generator matrix of the kind: G = $[G_1\, G_2\, . . . G_n]$, where G_i s are the columns of the kind: $G_i = [v_i, v_i\alpha_i, v_i\alpha_i^2, ... , v_i\alpha_i^{k-1}]'_{k\times 1}$. And Roth and Seroussi [2] showed that the GRS code will have a systematic generator matrix of the kind [I | A], A being a GC matrix, and vice-versa [5].

Theorem 1. [Vinocha, Bhullar, Brar] [5] If there is code, which is GRS having parameters (n + 1) and k, and determined by vectors **α** and **v**, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, . . . ,\alpha_n, \alpha_{n+1})$, $\mathbf{v} = (v_1, v_2, ... , v_n, v_{n+1})$, then the code will have systematic generator matrix of the kind [I | A], A being Generalised Cauchy (GC) matrix having order k × (n + 1 - k) so that $A_{ij} = \frac{c_i\, d_j}{x_i + y_j}$, where:

$$x_i = -\alpha_i, \quad \text{i varies from 1 to k} \tag{1.2}$$

$$y_j = \alpha_{j+k}, \quad \text{j varies from 1 to (n + 1 - k)} \tag{1.3}$$

$$c_i = \frac{v_i^{-1}}{\prod_{1\le t\le k;\, t\ne i}(\alpha_i - \alpha_t)}, \quad \text{i varies from 1 to k} \tag{1.4}$$

$$d_j = v_{j+k} \,.\, \prod_{1\le t\le k}(\alpha_{j+k} - \alpha_t), \text{ j varies from 1 to (n + 1 - k)} \tag{1.5}$$

and conversely, if A is Generalised Cauchy (GC) matrix having k rows and (n + 1 - k) columns which is determined by the vectors **x**, **y**, **c**, **d** where $\mathbf{x} = (x_i)_{i=1}^{k}$, $\mathbf{y} = (y_j)_{j=1}^{n+1-k}$, $\mathbf{c} = (c_i)_{i=1}^{k}$, $\mathbf{d} = (d_j)_{j=1}^{n+1-k}$, so that each square sub-matrix of the matrix A will be non-singular, then [I | A] will generate a code which will be GRS code having parameters (n + 1) and k, and determined by vectors **α**, **v**, where:

$$\alpha_i = -x_i, \quad \text{i varies from 1 to k} \tag{1.6}$$

$$\alpha_j = y_{j-k}, \quad \text{j varies from (k + 1) to (n + 1)} \tag{1.7}$$

$$v_i = \frac{c_i^{-1}}{\prod_{1\le t\le k;t\ne i}(x_t - x_i)}, \quad \text{i varies from 1 to k} \tag{1.8}$$

$$v_j = \frac{d_{j-k}}{\prod_{i\le t\le k}(x_t + y_{j+k})}, \quad \text{j varies from (k + 1) to (n + 1)} \tag{1.9}$$

A matrix A of order m × n is known as GEC matrix, if this is of the kind: A = D(**c**).Ā.D(**d**), where Ā is Extended Cauchy matrix of order m × n, and vector $\mathbf{c} = (c_1, c_2, \ldots, c_m)$, vector $\mathbf{d} = (d_1, d_2, \ldots, d_n)$ having elements which are non-zero from the finite field F. If each square sub-matrix of the matrix Ā which is Extended Cauchy matrix, is not singular, then each square sub-matrix of the matrix A will also be not singular. Hence, generator matrix in systematic form, of the [n, k, d] MDS code can be constructed by the process of linkage of I_k of order k with GEC matrix of order k × (n - k), which is suitably defined. Further, the Extended GRS code will have a generator matrix, which will be generator matrix of the GRS code having parameters n and k and is determined by vectors **α, v**, whenever one of α_i s will be zero. Let $\alpha_n = 0$. Further extension of the code can be accomplished when matrix G will have a column of kind: $G_\infty = (0\ 0\ 0\ \ldots\ 0\ v_\infty)^{/}$, v_∞ being a non-zero element from the finite field F, so that MDS property is maintained. The resulting new code will be known as Generalised Doubly Extended Reed-Solomon code written as GDRS having parameters (n + 1) and k and is determined by vectors **α, v**, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_{s-1}, \alpha_\infty, \alpha_s, \ldots, \alpha_n)$, $\mathbf{v} = (v_1, v_2, \ldots, v_{s-1}, v_\infty, v_s, \ldots, v_n)$, s being index of G_∞ within the matrix G. And Roth and Serorussi [2] have showed that the GDRS code will have systematic generator matrix of the kind [I | A], A being GEC matrix, and vice-versa.[5].

2. GTRS Codes and GDC Matrices

A matrix A having order m × n is known as Doubly Extended Cauchy matrix, when matrix A will have two rows (or columns) of 1s, and if we delete these, then A changes to matrix $\hat{\hat{A}}$, where $\hat{\hat{A}}$ is a Cauchy matrix. Hence doubly extended Cauchy matrix, having two rows of 1s will be of the form:

$$\begin{bmatrix} 1 & 1 & . & . & . & 1 \\ 1 & 1 & . & . & . & 1 \\ \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & . & . & . & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & . & . & . & \frac{1}{x_2+y_n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \frac{1}{x_{m-2}+y_1} & \frac{1}{x_{m-2}+y_2} & . & . & . & \frac{1}{x_{m-2}+y_n} \end{bmatrix}_{m\times n}, \tag{2.10}$$

so that

$$\hat{\hat{A}} = \begin{bmatrix} \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & . & . & . & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & . & . & . & \frac{1}{x_2+y_n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \frac{1}{x_{m-2}+y_1} & \frac{1}{x_{m-2}+y_2} & . & . & . & \frac{1}{x_{m-2}+y_n} \end{bmatrix}_{(m-2)\times n}$$

is a Cauchy matrix.

A matrix A having order m × n, is known as Generalised Doubly Extended Cauchy matrix, briefly written as GDC, if it is of the kind: A = D(**c**).$\bar{\bar{A}}$.D(**d**), $\bar{\bar{A}}$ being doubly extended Cauchy matrix of order m × n, and vectors **c** and **d** are as: $\mathbf{c} = (c_1, c_2, \ldots, c_m)$, $\mathbf{d} = (d_1, d_2, \ldots, d_n)$ having non-zero elements from finite field F.[5]. So,

$$A=\begin{bmatrix} c_1 & 0 & . & . & . & 0 \\ 0 & c_2 & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & c_m \end{bmatrix}_{m\times m} \cdot \begin{bmatrix} 1 & 1 & . & . & . & 1 \\ 1 & 1 & . & . & . & 1 \\ \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & . & . & . & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & . & . & . & \frac{1}{x_2+y_n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \frac{1}{x_{m-2}+y_1} & \frac{1}{x_{m-2}+y_2} & . & . & . & \frac{1}{x_{m-2}+y_n} \end{bmatrix}_{m\times n} \begin{bmatrix} d_1 & 0 & . & . & . & 0 \\ 0 & d_2 & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & d_n \end{bmatrix}_{n\times n}$$

i.e.
$$A=\begin{bmatrix} c_1d_1 & c_1d_2 & . & . & . & c_1d_n \\ c_2d_1 & c_2d_2 & . & . & . & c_2d_n \\ \frac{c_3d_1}{x_1+y_1} & \frac{c_3d_2}{x_1+y_2} & . & . & . & \frac{c_3d_n}{x_1+y_n} \\ \frac{c_4d_1}{x_2+y_1} & \frac{c_4d_2}{x_2+y_2} & . & . & . & \frac{c_4d_n}{x_2+y_n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \frac{c_md_1}{x_{m-1}+y_1} & \frac{c_md_2}{x_{m-1}+y_2} & . & . & . & \frac{c_md_n}{x_{m-1}+y_n} \end{bmatrix}_{m\times n} \tag{2.11}$$

If all the square sub-matrices (having order greater than 2) of this Cauchy matrix $\bar{\bar{A}}$ which is Doubly Extended are not singular that is non-singular, then all the square sub-matrices (having order greater than 2) of A will also be non-singular. Hence, we can construct generator matrix, which is systematic in nature, for [n, k, d] MDS code by the process of linkage of I_k with GDC matrix having order k × (n - k) which is suitably defined.[5].

Generator matrix of the code GDRS having parameters (n + 1) and k, and determined by vectors **α, v**, may be extended further if we take a more column of matrix G of type: $G_\infty^{/} = (0\ 0\ 0\ .\ .\ .\ 0\ v_\infty^{/})^{/}$, $v_\infty^{/}$ is non-zero element from the finite field F, so that property of being MDS is retained. The resulting new code will be known as GTRS, which we can denote as GTRS having parameters (n + 2) and k, and is determined by vectors **α, v**, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ .\ .\ .\ , \alpha_{s-1}, \alpha_\infty, \alpha_\infty^{/}, \alpha_s, \ .\ .\ ., \alpha_n)$, $\mathbf{v} = (v_1, v_2, \ .\ .\ .\ , v_{s-1}, v_\infty, v_\infty^{/}, v_s, \ .\ .\ .\ , v_n)$, s being index of G_∞ and $G_\infty^{/}$ inside G. Hence, code GTRS will have generator matrix as:

$$G=\begin{bmatrix} v_1 & v_2 & . & . & . & v_n & 0 & 0 \\ v_1\alpha_1 & v_2\alpha_2 & . & . & . & 0 & 0 & 0 \\ v_1\alpha_1^{\ 2} & v_2\alpha_2^{\ 2} & . & . & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ v_1\alpha_1^{\ k-1} & v_2\alpha_2^{\ k-1} & . & . & . & 0 & v_\infty & v_\infty^{\ /} \end{bmatrix}_{k\times(n+2)}$$

Theorem 2. [Vinocha, Bhullar, Brar] [5]

(i) If code is GTRS having parameters (n + 2) and k, and determined by the vectors **α, v**, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ .\ .\ .\ , \alpha_{s-1}, \alpha_\infty, \alpha_\infty^{/}, \alpha_s, \ .\ .\ .\ , \alpha_n)$ and $\mathbf{v} = (v_1, v_2, \ .\ .\ ., v_{s-1}, v_\infty, v_\infty^{/}, v_s, \ .\ .\ .\ ., v_n)$, where s varies from k to (n + 2), then code will have $[I|\bar{\bar{A}}]$ as a form of generator matrix, $\bar{\bar{A}} = [A_1, A_2, \ .\ .\ .\ , A_{s-k-1}, A_\infty, A_\infty^{/}, A_{s-k}, \ .\ .\ .\ , A_{n-k}]$ and it is GDC matrix of order k × (n + 2 – k) having the following two additional columns compared with generator matrix of GRS code having length n: $A_\infty = d_\infty(c_1, c_2, \ .\ .\ .\ , c_k)^{/}$, $A_\infty^{/} = d_\infty^{/}(c_1, c_2, \ .\ .\ .\ , c_k)^{/}$ before (s - k)th column of the matrix A, whenever s is less than (n + 2), or as last column if s is equal to (n + 2), $d_\infty = v_\infty$, $d_\infty^{/} = v_\infty^{/}$, and c_i s are as in (1.4).

(ii) Conversely, given GDC matrix $\bar{\bar{A}}$ so that each square sub-matrix of $\bar{\bar{A}}$ is not singular, there exist vectors **α** and **v** which determine code GTRS which is generated by matrix $[I \mid \bar{\bar{A}}]$.

Theorem 3:

(i) If C is GTRS code, denoted as GTRS having parameters (n + 2) and (k + 2), which is determined by vectors **α** and **v** same as in Theorem 2 i.e. $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_{s-1}, \alpha_\infty, \alpha_\infty', \alpha_s, \ldots, \alpha_n)$,

$\mathbf{v} = (v_1, v_2, \ldots, v_{s-1}, v_\infty, v_\infty', v_s, \ldots, v_n)$,

but with $1 \le s \le k+2$, then code C will have generator matrix of kind $[I \mid \bar{\bar{A}}]$, $\bar{\bar{A}}$ being:

$$\bar{\bar{A}} = [a_1, a_2, \ldots, a_{s-1}, a_\infty, a_\infty', a_s, \ldots, a_k]'$$

is $(k+2) \times (n-k)$ GDC matrix which is got from GC (Generalised Cauchy) matrix of Theorem 1 having order $k \times (n-k)$ by inserting the rows:

$$a_\infty = c_\infty[(-1)^{k+2}.(\alpha_{k+1})^{-1}.v_{k+1}.\textstyle\prod_{i=1}^{k+1}\alpha_i, (\alpha_{k+2})^{-1}.(d_2(\alpha_{k+2}-\alpha_{k+1}) + v_{k+2}.(-1)^{k+2}.\prod_{i=1}^{k+1}\alpha_i),$$

$$\ldots, (\alpha_n)^{-1}.(d_{n-k}(\alpha_n-\alpha_{k+1}) + v_n.(-1)^{k+2}.\textstyle\prod_{i=1}^{k+1}\alpha_i)];$$

$$a_\infty' = c_\infty'(d_1, d_2, \ldots, d_{n-k})$$

before the sth row of the matrix A if s is less than $(k+2)$, or as last rows if s is equal to $(k+2)$, $c_\infty = v_\infty^{-1}$, $c_\infty' = (v_\infty')^{-1}$, the d_j's are the same as defined in equation (1.5) with $1 \le j \le (n-k)$.

(ii) Conversely, given GDC matrix $\bar{\bar{A}}$ so that each square sub-matrix of the matrix $\bar{\bar{A}}$ is not singular, then there will exist vectors $\boldsymbol{\alpha}$ and $\mathbf{v}$ which will determine GTRS code C which is generated by matrix $[I \mid \bar{\bar{A}}]$.

Proof: (i) Here C is the GTRS $(n+2, k+2, \boldsymbol{\alpha}, \mathbf{v})$, which is determined by the vectors:

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

$\mathbf{v} = (v_1, v_2, \ldots, v_{s-1}, v_\infty, v_\infty', v_s, \ldots, v_n)$

Here the dimension of code C is $k+2$, whereas in Theorem 2, it was k. Length of C is $(n+2)$, whereas in Theorem 2, it was also the same i.e. $(n+2)$. Because here $1 \le s \le (k+2)$, and number of message-symbols are $k+2$, therefore, G_∞ and G_∞' would be there among columns of the generator matrix G which corresponds to message-symbols. Take case of $s = (k+2)$ for convenience, the other case of $s < (k+2)$ would be similar.

Now generator matrix will be:

$G = [\bar{\bar{P}} \mid \bar{\bar{Q}}].D(\mathbf{v})$, where :

$$P = \begin{bmatrix} 1 & 1 & 1 & . & . & . & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & . & . & . & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & . & . & . & \alpha_k^2 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ \alpha_1^{k-1} & \alpha_2^{k-1} & . & . & . & . & \alpha_k^{k-1} \end{bmatrix}_{k\times k}, \quad Q = \begin{bmatrix} 1 & . & . & . & 1 \\ \alpha_{k+1} & . & . & . & \alpha_n \\ \alpha_{k+1}^2 & . & . & . & \alpha_n^2 \\ . & . & . & . & . \\ . & . & . & . & . \\ \alpha_{k+1}^{k-1} & . & . & . & \alpha_n^{k-1} \end{bmatrix}_{k\times(n-k)}$$

$$\bar{P} = \begin{bmatrix} & & & & & 0 \\ & & P & & & . \\ & & & & & . \\ & & & & & 0 \\ \alpha_1^k & \alpha_2^k & . & . & \alpha_k^k & 1 \end{bmatrix}_{(k+1)\times(k+1)}, \quad \bar{Q} = \begin{bmatrix} & & Q & & \\ \alpha_{k+1}^k & \alpha_{k+2}^k & . & . & \alpha_n^k \end{bmatrix}_{(k+1)\times(n-k)}$$

$$\bar{\bar{P}} = \begin{bmatrix} & & & & & 0 \\ & & & & & . \\ & & \bar{P} & & & 0 \\ & & & & & 0 \\ \alpha_1^{k+1} & \alpha_2^{k+1} & . & . & . & \alpha_k^{k+1} & \alpha_{k+1}^{k+1} & 1 \\ & & & & & (=0) & \end{bmatrix}_{(k+2)\times(k+2)} \quad \bar{\bar{Q}} = \begin{bmatrix} & & \bar{Q} & & \\ \alpha_{k+1}^{k+1} & \alpha_{k+2}^{k+1} & . & . & \alpha_n^{k+1} \end{bmatrix}_{(k+2)\times(n-k)}$$

By considering the polynomial

$$f_i(z) = \textstyle\prod_{1\le t\le k;\, t\ne i}(z-\alpha_t) = \sum_{0\le r\le k-1} f_{ir}.z^r,$$

P^{-1} will be found, and by considering the polynomial

$$g(z) = \textstyle\prod_{t=1}^{k}(z-\alpha_t) = \sum_{r=0}^{k} g_r.z^r,$$

$(\bar{P})^{-1}$ will be found as: $(\bar{P})^{-1} = \begin{bmatrix} & & & P^{-1} & & & & 0 \\ & & & & & & & . \\ & & & & & & & . \\ & & & & & & & . \\ & & & & & & & 0 \\ g_0 & g_1 & . & . & . & . & g_{k-1} & g_k \end{bmatrix}$

If P is taken as: $P = \begin{bmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{bmatrix}$,

then P^{-1} will be as :

$$P^{-1} = \begin{bmatrix} \frac{-\alpha_2\alpha_3}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & \frac{\alpha_2+\alpha_3}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & \frac{-1}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} \\ \frac{-\alpha_3\alpha_1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & \frac{\alpha_3+\alpha_1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & \frac{-1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} \\ \frac{-\alpha_1\alpha_2}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & \frac{\alpha_1+\alpha_2}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & \frac{-1}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} \end{bmatrix}$$

If $\bar{P}$ is taken as: $\bar{P} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ \alpha_1 & \alpha_2 & \alpha_3 & 0 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & 0 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & 1 \end{bmatrix}$,

then we will have $(\bar{P})^{-1}$ as:

$$(\bar{P})^{-1} = \begin{bmatrix} \frac{-\alpha_2\alpha_3}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & \frac{\alpha_2+\alpha_3}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & \frac{-1}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & 0 \\ \frac{-\alpha_3\alpha_1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & \frac{\alpha_3+\alpha_1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & \frac{-1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & 0 \\ \frac{-\alpha_1\alpha_2}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & \frac{\alpha_1+\alpha_2}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & \frac{-1}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & 0 \\ g_0 & g_1 & g_2 & g_3 \\ (=-\alpha_1\alpha_2\alpha_3) & (=\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1) & (=-(\alpha_1+\alpha_2+\alpha_3)) & (=1) \end{bmatrix}$$

or as: $(\bar{P})^{-1} = \begin{bmatrix} & P^{-1} & & 0 \\ & & & 0 \\ & & & 0 \\ g_0 & g_1 & g_2 & g_3 \end{bmatrix}$

Now concrete ($\bar{\bar{P}}$) will be: $(\bar{\bar{P}}) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ \alpha_1 & \alpha_2 & \alpha_3 & 0 & 0 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & 0 & 0 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & 1 & 0 \\ \alpha_1^4 & \alpha_2^4 & \alpha_3^4 & 0 & 1 \end{bmatrix}_{5\times5}$,

And inverse of ($\bar{\bar{P}}$) will be obtained as:

$$(\bar{\bar{P}})^{-1} = \begin{bmatrix} \frac{-\alpha_2\alpha_3}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & \frac{\alpha_2+\alpha_3}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & \frac{-1}{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)} & 0 & 0 \\ \frac{-\alpha_3\alpha_1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & \frac{\alpha_3+\alpha_1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & \frac{-1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)} & 0 & 0 \\ \frac{-\alpha_1\alpha_2}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & \frac{\alpha_1+\alpha_2}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & \frac{-1}{(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)} & 0 & 0 \\ -\alpha_1\alpha_2\alpha_3 & \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1 & -(\alpha_1+\alpha_2+\alpha_3) & 1 & 0 \\ -\alpha_1\alpha_2\alpha_3.(\alpha_1+\alpha_2+\alpha_3) & (\alpha_1+\alpha_2)(\alpha_2+\alpha_3).(\alpha_3+\alpha_1) & -(\alpha_1^2+\alpha_2^2+\alpha_3^2 +\alpha_1\alpha_2+\alpha_2\alpha_3 & 0 & 1 \end{bmatrix}$$

or as:

$$(\bar{\bar{P}})^{-1} = \begin{bmatrix} & & & 0 & 0 \\ & P^{-1} & & 0 & 0 \\ & & & 0 & 0 \\ -\alpha_1\alpha_2\alpha_3 & (\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1) & -(\alpha_1+\alpha_2+\alpha_3) & 1 & 0 \\ -\alpha_1\alpha_2\alpha_3.(\alpha_1+\alpha_2+\alpha_3) & (\alpha_1+\alpha_2)(\alpha_2+\alpha_3).(\alpha_3+\alpha_1) & -(\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1) & 0 & 1 \end{bmatrix} \quad (2.12)$$

Consider the polynomial:

$$h(z) = \prod_{t=1}^{k+1}(z-\alpha_t) = \sum_{r=0}^{k+1} h_r . z^r$$

Therefore $(z - \alpha_1).(z - \alpha_2) \; . \; . \; . \; (z - \alpha_k).(z - \alpha_{k+1})$

$$= h_0.z^o + h_1.z^1 + h_2.z^2 + \; . \; . \; . \; + h_{k+1}.z^{k+1}.$$

$$\Rightarrow \quad z^{k+1} - (\alpha_1 + \alpha_2 + \; . \; . \; . \; + \alpha_k + \alpha_{k+1}).z^k + (\alpha_1\alpha_2 + \; . \; . \; . \;).z^{k-1} + \; . \; . \; .$$

$$+ (-1)^{k+1}.(\alpha_1\alpha_2 \; . \; . \; . \; \alpha_k\alpha_{k+1})$$

$$= h_0 + h_1.z + h_2.z^2 + \; . \; . \; . \; + h_k.z^k + h_{k+1}.z^{k+1}$$

Comparing:

$h_{k+1} = 1$; $h_k = -(\alpha_1 + \alpha_2 + \; . \; . \; . \; + \alpha_k + \alpha_{k+1})$; $h_{k-1} = \alpha_1\alpha_2 + \; . \; . \; .$

$h_{k-2} = -(\alpha_1\alpha_2\alpha_3 + \; . \; . \; .)$; . . . . . $h_0 = (-1)^{k+1}.(\alpha_1\alpha_2 \; . \; . \; . \; \alpha_k\alpha_{k+1})$

Since in the considered concrete example, the subscript of α_i s is at the most 3, so taking k = 3, we get from above:

$h_4 = 1$; $h_3 = -(\alpha_1 + \alpha_2 + \alpha_3)$; $h_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1$; $h_1 = -\alpha_1\alpha_2\alpha_3$; $h_0 = +\alpha_1\alpha_2\alpha_3$

Therefore $(\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)$

i.e. $(-h_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2(h_2)$

i.e. $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = h_3^2 - 2h_2$

i.e. $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) = h_3^2 - 2h_2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)$

$$= h_3^2 - 2h_2 + h_2$$

$$= h_3^2 - h_2$$

and $(\alpha_1 + \alpha_2).(\alpha_2 + \alpha_3).(\alpha_3 + \alpha_1) = (-h_3 - \alpha_3).(-h_3 - \alpha_1).(-h_3 - \alpha_2)$

$$= -(h_3 + \alpha_1).(h_3 + \alpha_2).(h_3 + \alpha_3)$$

$$= -[h_3^2 + h_3\alpha_2 + h_3\alpha_1 + \alpha_1\alpha_2].(h_3 + \alpha_3)$$

$$= -[h_3^3 + h_3^2\alpha_3 + h_3^2\alpha_2 + h_3\alpha_2\alpha_3 + h_3^2\alpha_1 + h_3\alpha_1\alpha_3 + h_3\alpha_1\alpha_2 + \alpha_1\alpha_2\alpha_3]$$

$$= -[h_3^3 + h_3^2(\alpha_1 + \alpha_2 + \alpha_3) + h_3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) + \alpha_1\alpha_2\alpha_3]$$

$$= -[h_3^3 + h_3^2(-h_3) + h_3(h_2) + (-h_1)]$$

$$= h_1 - h_2h_3$$

and $-\alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3) = (h_1).(-h_3) = -h_1h_3$

and $h_0 + h_1 = 0$

Hence (2.12) implies:

$$(\bar{\bar{P}})^{-1} = \begin{bmatrix} & & & 0 & 0 \\ & P^{-1} & & 0 & 0 \\ & & & 0 & 0 \\ h_1 & h_2 & h_3 & h_4(=1) & 0 \\ -h_1h_3 & h_1 - h_2h_3 & h_2 - h_3^2 & h_0 + h_1 & h_4(=1) \end{bmatrix}$$

$$= \begin{bmatrix} & P^{-1} & & 0 & 0 \\ & & & 0 & 0 \\ & & & 0 & 0 \\ h_1 & h_2 & h_3 & h_4(=1) & 0 \\ h_0^{/} & h_1^{/} & h_2^{/} & h_3^{/} & h_4^{/}(=1) \end{bmatrix},$$

where $h_i^{/}$ s are some functions of h_i s.

Generalising, we shall have:

$$(\bar{\bar{P}})^{-1} = \begin{bmatrix} & & P^{-1} & & & & 0 & 0 \\ & & & & & & 0 & 0 \\ & & & & & & 0 & 0 \\ h_1 & h_2 & h_3 & . & . & . & h_{k+1}(=1) & 0 \\ h_0^{/} & h_1^{/} & h_2^{/} & . & . & . & h_k^{/} & h_{k+1}^{/}(=1) \end{bmatrix}, \quad (2.13)$$

where $h_i^{/}$ s are some functions of $h_i^{,}$s.

In this theorem, a generator matrix of the GTRS (n + 2, k + 2, **α, v**) code in systematic form will be [I | $\bar{\bar{A}}$], where $\bar{\bar{A}}$ will be:

$$\bar{\bar{A}} = (D[\mathbf{u}|v_\infty|v_\infty^{/}])^{-1}).(\bar{\bar{P}})^{-1}.\bar{\bar{Q}}.D(\mathbf{w})$$

$$= \begin{bmatrix} \frac{1}{v_1} & 0 & . & . & . & 0 \\ 0 & \frac{1}{v_2} & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \frac{1}{v_k} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{v_\infty} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{v_\infty^{/}} \end{bmatrix}_{(k+2)\times(k+2)} . \begin{bmatrix} & P^{-1} & & & 0 & 0 \\ & & & & 0 & 0 \\ & & & & 0 & 0 \\ h_1 & h_2 & h_3 & .. & h_{k+1}(=1) & 0 \\ h_0^{/} & h_1^{/} & h_2^{/} & .. & h_k^{/} & h_{k+1}^{/}(=1) \end{bmatrix}_{(k+2)\times(k+2)} .$$

$$. \begin{bmatrix} & & \bar{Q} & & \\ \alpha_{k+1}^{k+1} & \alpha_{k+2}^{k+1} & . & . & . & \alpha_n^{k+1} \end{bmatrix}_{(k+2)\times(n-k)} \begin{bmatrix} v_{k+1} & 0 & . & . & . & 0 \\ 0 & v_{k+2} & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & v_{n-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & v_n \end{bmatrix}_{(n-k)\times(n-k)}$$

$$= \begin{bmatrix} \frac{1}{v_1} & 0 & . & . & . & 0 \\ 0 & \frac{1}{v_2} & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \frac{1}{v_k} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{v_\infty} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{v_\infty^{/}} \end{bmatrix}_{(k+2)\times(k+2)} . \begin{bmatrix} & & & P^{-1} & & 0 & 0 \\ & & & & & 0 & 0 \\ & & & & & 0 & 0 \\ h_1 & h_2 & h_3 & . & . & h_{k+1}(=1) & 0 \\ h_0^{/} & h_1^{/} & h_2^{/} & . & . & h_k^{/} & h_{k+1}^{/}(=1) \end{bmatrix}_{(k+2)\times(k+2)}$$

$$. \begin{bmatrix} 1 & 1 & 1 & . & . & . & 1 & 1 & 1 \\ \alpha_{k+1} & \alpha_{k+2} & \alpha_{k+3} & . & . & . & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \alpha_{k+1}^2 & \alpha_{k+2}^2 & \alpha_{k+3}^2 & . & . & . & \alpha_{n-2}^2 & \alpha_{n-1}^2 & \alpha_n^2 \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . \\ \alpha_{k+1}^{k-1} & \alpha_{k+2}^{k-1} & \alpha_{k+3}^{k-1} & . & . & . & \alpha_{n-2}^{k-1} & \alpha_{n-1}^{k-1} & \alpha_n^{k-1} \\ \alpha_{k+1}^{k} & \alpha_{k+2}^{k} & \alpha_{k+3}^{k} & . & . & . & \alpha_{n-2}^{k} & \alpha_{n-1}^{k} & \alpha_n^{k} \\ \alpha_{k+1}^{k+1} & \alpha_{k+2}^{k+1} & \alpha_{k+3}^{k+1} & . & . & . & \alpha_{n-2}^{k+1} & \alpha_{n-1}^{k+1} & \alpha_n^{k+1} \end{bmatrix}_{(k+2)\times(n-k)} . \begin{bmatrix} v_{k+1} & 0 & . & . & . & 0 \\ 0 & v_{k+2} & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & v_{n-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & v_n \end{bmatrix}_{(n-k)\times(n-k)}$$

$$= \begin{bmatrix} . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \frac{1}{v_\infty}h_1 & \frac{1}{v_\infty}h_2 & \frac{1}{v_\infty}h_3 & . & . & \frac{1}{v_\infty}h_{k+1} & 0 \\ \frac{1}{v_\infty^{/}}h_0^{/} & \frac{1}{v_\infty^{/}}h_1^{/} & \frac{1}{v_\infty^{/}}h_2^{/} & . & . & \frac{1}{v_\infty^{/}}h_k^{/} & \frac{1}{v_\infty^{/}}h_{k+1}^{/} \end{bmatrix}_{(k+2)\times(k+2)}$$

$$\begin{bmatrix} v_{k+1} & v_{k+2} & . & . & v_{n-1} & v_n \\ \alpha_{k+1}v_{k+1} & \alpha_{k+2}v_{k+2} & . & . & \alpha_{n-1}v_{n-1} & \alpha_n v_n \\ \alpha_{k+1}^2 v_{k+1} & \alpha_{k+2}^2 v_{k+2} & . & . & \alpha_{n-1}^2 v_{n-1} & \alpha_n^2 v_n \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \alpha_{k+1}^k v_{k+1} & \alpha_{k+2}^k v_{k+2} & . & . & \alpha_{n-1}^k v_{n-1} & \alpha_n^k v_n \\ \alpha_{k+1}^{k+1} v_{k+1} & \alpha_{k+2}^{k+1} v_{k+2} & . & . & \alpha_{n-1}^{k+1} v_{n-1} & \alpha_n^{k+1} v_n \end{bmatrix}_{(k+2)\times(n-k)}$$

So, $\bar{\bar{A}}$ =

$$\begin{bmatrix} \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \frac{1}{v_\infty}h_1 v_{k+1} + \frac{1}{v_\infty}h_2\alpha_{k+1}v_{k+1} & . \; . \; . & \frac{1}{v_\infty}h_1 v_{n-1} + \frac{1}{v_\infty}h_2\alpha_{n-1}v_{n-1} & \frac{1}{v_\infty}h_1 v_n + \frac{1}{v_\infty}h_2\alpha_n v_n \\ +\ldots+\frac{1}{v_\infty}h_{k+1}\alpha_{k+1}^k v_{k+1} + 0 & & +\ldots+\frac{1}{v_\infty}h_{k+1}\alpha_{n-1}^k v_{n-1} + 0 & + \;\ldots\; + \frac{1}{v_\infty}h_{k+1}\alpha_n^k v_n + 0 \\ \frac{1}{v'_\infty}h'_0 v_{k+1} + \frac{1}{v'_\infty}h'_1\alpha_{k+1}v_{k+1} & . \; . \; . & \frac{1}{v'_\infty}h'_0 v_{n-1} + \frac{1}{v'_\infty}h'_1\alpha_{n-1}v_{n-1} & \frac{1}{v'_\infty}h'_0 v_n + \frac{1}{v'_\infty}h'_1\alpha_n v_n \\ +\ldots+\frac{1}{v'_\infty}h'_k\alpha_{k+1}^k v_{k+1} & & +\ldots+\frac{1}{v'_\infty}h'_k\alpha_{n-1}^k v_{n-1} & +\ldots+\frac{1}{v'_\infty}h'_k\alpha_n^k v_n \\ +\frac{1}{v'_\infty}h'_{k+1}\alpha_{k+1}^{k+1}v_{k+1} & & +\frac{1}{v'_\infty}h'_{k+1}\alpha_{n-1}^{k+1}v_{n-1} & +\frac{1}{v'_\infty}h'_{k+1}\alpha_n^{k+1}v_n \end{bmatrix}_{(k+2)\times(n-k)}$$

Therefore, it will be seen that rows of $\bar{\bar{A}}$ from first row to the kth row will be identical with rows of matrix A from first to kth row of matrix A of Theorem 1. The two rows, (k + 1)th and (k + 2)th, of $\bar{\bar{A}}$ will respectively be:

$$a_{\infty j} = (v_\infty)^{-1}\left(\textstyle\sum_{r=1}^{k+2} h_r.\alpha_{j+k}^{r-1}\right).v_{j+k}, \quad \text{where } 1 \le j \le (n-k)$$

$$a'_{\infty j} = (v'_\infty)^{-1}\left(\textstyle\sum_{r=1}^{k+2} h'_{r-1}.\alpha_{j+k}^{r-1}\right).v_{j+k}, \quad \text{where} 1 \le j \le (n-k)$$

Therefore, various entries of (k + 1)th row of $\bar{\bar{A}}$ will be given by:

$$a_{\infty j} = (v_\infty)^{-1}\left(\textstyle\sum_{r=1}^{k+2} h_r.\alpha_{j+k}^{r-1}\right).v_{j+k}, \quad \text{where } 1 \le j \le (n-k)$$

$$= (v_\infty)^{-1}.v_{j+k}.\left(\textstyle\sum_{r=1}^{k+2} h_r.\alpha_{j+k}^{r-1}\right).$$

$$= (v_\infty)^{-1}.v_{j+k}.\frac{1}{\alpha_{j+k}}.(h.(\alpha_{j+k}) - h_0)$$

[since $h(z) = \prod_{t=1}^{k+1}(z-\alpha_t) = \sum_{r=0}^{k+1} h_r z^r$

implies that $\sum_{r=0}^{k+1} h_r z^r = h(z)$

i.e. $h_0.z^0 + \sum_{r=1}^{k+1} h_r z^r = h(z)$

i.e. $h_0.(1) + (\sum_{r=1}^{k+2} h_r z^r) - h_{k+2}.z^{k+2} = h(z)$

i.e. $h_0 + (\sum_{r=1}^{k+2} h_r z^r) - (0).z^{k+2} = h(z)$,

(since note that $(v_\infty)^{-1}.h_{k+2}.\alpha_{k+2}^{k+1}.v_{k+2}$ etc. = 0, which implies that in general $(v_\infty)^{-1}.h_{k+2}.\alpha_{j+k}^{k+1}.v_{j+k} = 0$, which means that $h_{k+2} = 0$).

i.e. $\sum_{r=1}^{k+2} h_r z^r = h(z) - h_0$

i.e. $(\sum_{r=1}^{k+2} h_r z^{r-1}).z = h(z) - h_0$

i.e. $(\sum_{r=1}^{k+2} h_r z^{r-1}) = \frac{1}{z}.(h(z) - h_0)$

i.e. $\left(\sum_{r=1}^{k+2} h_r.\alpha_{j+k}^{\,r-1}\right) = \frac{1}{\alpha_{j+k}}.(h.(\alpha_{j+k}) - h_0)$]

Therefore, $a_{\infty j} = (v_\infty)^{-1}.v_{j+k}.\frac{1}{\alpha_{j+k}}.(h(\alpha_{j+k}) - h_0)$

$$= (v_\infty)^{-1}.v_{j+k}.\frac{1}{\alpha_{j+k}}.[\textstyle\prod_{t=1}^{k+1}(\alpha_{j+k}-\alpha_t) - h_0]$$

(since $h(z) = \prod_{t=1}^{k+1}(z-\alpha_t)$ i.e. $h(\alpha_{j+k}) = \prod_{t=1}^{k+1}(\alpha_{j+k}-\alpha_t)$)

$$= (v_\infty)^{-1}.v_{j+k}.\textstyle\prod_{t=1}^{k+1}(\alpha_{j+k}-\alpha_t).\frac{1}{\alpha_{j+k}} - (v_\infty)^{-1}.v_{j+k}.\frac{1}{\alpha_{j+k}}.h_0$$

$$= (v_\infty)^{-1}.v_{j+k}.(\textstyle\prod_{t=1}^{k}(\alpha_{j+k}-\alpha_t)).(\alpha_{j+k}-\alpha_{k+1}).\frac{1}{\alpha_{j+k}} - (v_\infty)^{-1}.v_{j+k}.\frac{1}{\alpha_{j+k}}.h_0$$

$$= (v_\infty)^{-1}.(d_j).(\alpha_{j+k}-\alpha_{k+1}).\frac{1}{\alpha_{j+k}} - (v_\infty)^{-1}.v_{j+k}.\frac{1}{\alpha_{j+k}}.h_0$$

[since (1.5) is $d_j = v_{j+k}.\prod_{t=1}^{k}(\alpha_{j+k}-\alpha_t)$, with $1 \le j \le (n-k)$]

$$= ((v_\infty)^{-1}.\frac{1}{\alpha_{j+k}}).[d_j.(\alpha_{j+k}-\alpha_{k+1}) - v_{j+k}.h_0]$$

$$= (v_\infty)^{-1}.(\alpha_{j+k})^{-1}.[d_j.(\alpha_{j+k}-\alpha_{k+1}) - v_{j+k}.h_0]$$

So, $a_{\infty j} = c_\infty.(\alpha_{j+k})^{-1}.[d_j.(\alpha_{j+k}-\alpha_{k+1}) - v_{j+k}.h_0]$ [since given is: $(v_\infty)^{-1} = c_\infty$]

Therefore,

$a_\infty = c_\infty.[(\alpha_{1+k})^{-1}.(d_1.\ (\alpha_{1+k} - \alpha_{k+1})\ - v_{1+k}\ .h_0),\ (\alpha_{2+k})^{-1}.(d_2.\ (\alpha_{2+k} - \alpha_{k+1})\ - v_{2+k}\ .h_0),$
$\quad . \ . \ . \ , (\alpha_{(n-k)+k})^{-1}.(d_{n-k}.\ (\alpha_{(n-k)+k} - \alpha_{k+1})\ - v_{(n-k)+k}\ .h_0)]$
$= c_\infty.[-(\alpha_{k+1})^{-1}.v_{k+1}\ .h_0),\ (\alpha_{k+2})^{-1}.(d_2.\ (\alpha_{k+2} - \alpha_{k+1})\ - v_{k+2}\ .h_0),$
$\quad . \ . \ . \ , (\alpha_n)^{-1}.(d_{n-k}.\ (\alpha_n - \alpha_{k+1}) - v_n\ .h_0)],$

where $h_0 = (-1)^{k+1}.(\alpha_1.\alpha_2,\alpha_3\ \ . \ . \ .\ \ \alpha_k,\alpha_{k+1}) = (-1)^{k+1}.\ \prod_{i=1}^{k+1} \alpha_i.$

i.e. $a_\infty = c_\infty.[-(\alpha_{k+1})^{-1}.v_{k+1}\ .(-1)^{k+1}\ \prod_{i=1}^{k+1} \alpha_i,\ (\alpha_{k+2})^{-1}.(d_2.\ (\alpha_{k+2} - \alpha_{k+1}) - v_{k+2}\ .(-1)^{k+1} \prod_{i=1}^{k+1}\ \alpha_i),$
$\quad . \ . \ . \ ,(\alpha_n)^{-1}.(d_{n-k}.\ (\alpha_n - \alpha_{k+1}) - v_n\ .(-1)^{k+1}\prod_{i=1}^{k+1} \alpha_i)],$

i.e. $a_\infty = c_\infty.[(-1)^{k+2}.\ (\alpha_{k+1})^{-1}.v_{k+1}.\ \prod_{i=1}^{k+1} \alpha_i,\ (\alpha_{k+2})^{-1}.(d_2.(\alpha_{k+2} - \alpha_{k+1}) + v_{k+2}\ .(-1)^{k+2}.\ \prod_{i=1}^{k+1} \alpha_i),$
$\quad . \ . \ . \ , (\alpha_n)^{-1}.\ (d_{n-k}.(\alpha_n - \alpha_{k+1}) + v_n\ .(-1)^{k+2} \prod_{i=1}^{k+1} \alpha_i)]$

Various entries of (k + 2)th row of $\bar{\bar{A}}$ will be given by:

$a'_{\infty j} = (v'_\infty)^{-1}\ (\ \sum_{r=1}^{k+2}\ h'_{r-1}.\ \alpha_{j+k}^{r-1}).v_{j+k}\ ,\qquad 1 \le j \le (n - k)$

$= (v'_\infty)^{-1}\ .v_{j+k}\ .\ h(\alpha_{j+k}).$

[since $h(z) = \prod_{t=1}^{k+1}(z - \alpha_t) = \sum_{r=0}^{k+1} h_r\ .\ z^r\ \sim\ \sum_{r=0}^{k+1} h'_r\ .\ z^r$,

where h_i''s are functions of h_i's, and hence h_i's are functions of h_i''s.

i.e. $\sum_{r=0}^{k+1} h'_r.z^r = h(z)$

i.e. $\sum_{r-1=0}^{k+2} h'_{r-1}.z^{r-1} = h(z)$

i.e. $\sum_{r=1}^{k+2} h'_{r-1}.z^{r-1} = h(z)$

i.e. $h(z) = \sum_{r=1}^{k+2} h'_{r-1}.z^{r-1}$

i.e. $h(\alpha_{j+k}) = \sum_{r=1}^{k+2} h'_{r-1}.\ \alpha_{j+k}^{r-1}$]

$= (v'_\infty)^{-1}\ .v_{j+k}\ .\ \prod_{t=1}^{k+1}(\alpha_{j+k} - \alpha_t)$

[since $h(z) = \prod_{t=1}^{k+1}(z - \alpha_t)$ i.e. $h(\alpha_{j+k}) = \prod_{t=1}^{k+1}(\alpha_{j+k} - \alpha_t)$]

$= (v_\infty')^{-1}.d_j$ (using (1.5))

$= c_\infty'.d_j$ [since given is $c_\infty' = (v_\infty')^{-1}$]

Therefore $a'_{\infty j} = c_\infty'.d_j\ ,\ \ 1 \le j \le (n - k).$

$\Rightarrow\quad a'_{\infty j} = c_\infty'.(d_1,\ d_2\ ,\ \ . \ . \ . \ . \ , d_{n-k}).$

Therefore, the code GTRS (n + 2, k + 2, **α, v**) has $[I\,|\,\bar{\bar{A}}]$ as a form of generator matrix, $\bar{\bar{A}} = [\ a_1, a_2,\ . \ . \ . \ , a_{s-1},\ a_\infty,\ a_\infty',\ a_s, . \ . \ . \ , a_k]'$ which is GDC matrix having order (k + 2) × (n - k) got from GC matrix by inserting the rows:

$a_\infty = c_\infty.[(-1)^{k+2}.\ (\alpha_{k+1})^{-1}.v_{k+1}\ .\ \prod_{i=1}^{k+1} \alpha_i,\ (\alpha_{k+2})^{-1}.(d_2.\ (\alpha_{k+2} - \alpha_{k+1}) + v_{k+2}\ .(-1)^{k+1}\prod_{i=1}^{k+1} \alpha_i),$
$\quad . \ . \ . \ , (\alpha_n)^{-1}.(d_{n-k}.\ (\alpha_n - \alpha_{k+1})\ + v_n\ .(-1)^{k+2}\ \prod_{i=1}^{k+1} \alpha_i)];\qquad (2.14)$

$a_\infty' = c_\infty'(d_1,\ d_2,\ \ . \ . \ . \ . \ , d_{n-k})\qquad (2.15)$

before the sth row of A when s < k + 2, or as last row when s = k + 2, $c_\infty = v_\infty^{-1}$, $c_\infty' = (v_\infty')^{-1}$, and d_j's are the same as defined in equation (1.5).

(ii) Now $\bar{\bar{A}}$ is a GDC matrix having order (k + 2) × (n - k) where every square sub-matrix of the matrix $\bar{\bar{A}}$ is not singular. And reversing the steps of proof of the part **(i)**, conclusion can be obtained that the matrix $[I\,|\,\bar{\bar{A}}]$ will generate GTRS code having parameters n + 2 and k + 2, and is determined by vectors **α** and **v**, where the vectors **α** and **v** can be derived from equations (1.6), (1.7), (1.8), and (1.9). Note that in this way, all the co-ordinates of vectors **α** and **v** will be derived.

As far as α_∞, α_∞' and v_∞, v_∞' are concerned, the index of α_∞, α_∞' in **α** and that of v_∞, v_∞' in **v** will be determined by the fact whether Cauchy matrix which underlines $\bar{\bar{A}}$ and which is doubly extended has two rows or two columns of 1s, and by index of those rows or columns. It means that if the Cauchy matrix which underlines $\bar{\bar{A}}$ and which is doubly extended is having two rows of 1s, then index of these rows of 1s will tell the index of α_∞, α_∞' in vector **α**, and if the Cauchy matrix which underlines $\bar{\bar{A}}$ and which is doubly extended is having two columns of 1s, then index of these columns of 1s will tell the index of v_∞, v_∞' in vector **v**.

3. Conclusion

If C is the GTRS code having (n + 2) and k as parameters, and is determined by vectors **α** and **v**, **α** = $(\alpha_1, \alpha_2,\ \ . \ . \ . \ \ , \alpha_{s-1}, \alpha_\infty, \alpha_\infty', \alpha_s,\ \ . \ . \ . \ . \ , \alpha_n)$, **v** = $(v_1, v_2,\ \ . \ . \ . \ . \ , v_{s-1}, v_\infty, v_\infty', v_s,\ \ . \ . \ . \ . \ , v_n)$, where s varies from k to (n + 2), then code C will have $[I\,|\,\bar{\bar{A}}]$ as a form of generator matrix, $\bar{\bar{A}}$ is GDC matrix of order k × (n + 2 - k) which is obtained from GC matrix A, where matrix A is having order k × (n - k). And if C is GTRS code having (n + 2) and (k + 2) as parameters, and is determined by vectors **α** and **v** which are same as above, but 1≤ s ≤ k + 2, then C will have generator matrix of kind $[I\,|\,\bar{\bar{A}}]$, $\bar{\bar{A}}$ is GDC matrix having order (k + 2) × (n - k) obtained from GC matrix A, A is having order k × (n - k). And conversely, if the given GDC matrix $\bar{\bar{A}}$ is such that each square sub-matrix of $\bar{\bar{A}}$ is not singular, then there will exist vectors **α** and **v** which will determine the GTRS code C which is generated by $[I\,|\,\bar{\bar{A}}]$. Thus a new

GTRS code is constructed having enlarged length and increased number of message-symbols. As a result, transmission of the information becomes more safe; more number of message-symbols are transmitted; and number of codewords within the code increases thereby enhancing the utility of the code.

References

[1] MacWilliams, F.J. and Sloane, N.J.A. (1977): "The Theory of Error-Correcting Codes". Amsterdam: North Holland,1977.

[2] Roth, Ron M. and Seroussi, Gadiel (1985): "On Generator Matrices of MDS Codes, *IEEE Transactions on Information Theory*, ISSN 0018-9448, Vol. IT-31, No. 6, November 1985.

[3] Knuth , D.E.(1969):The Art of Computer Programming, Vol. 1: Fundamental Algorithm. Reading MA: Addison-Wesley, 1969.

[4] Vinocha, O. P., Bhullar, J. S., and Brar, B.S., (2011), "A Construction of Generalised Non- Reed-Solomon Codes", *Arya Bhatta Journal of Mathematics & Informatics*, ISSN 0975-7139, vol. 3, No. 1, pp. 97-106.

[5] Vinocha, O.P., Bhullar, J.S., Brar, B.S., (2012), "On Generator Cauchy Matrices of GDRS/GTRS Codes", *International Journal of Contemporary Mathematical Sciences*, (Bulgaria), ISSN 1312-7586, vol. 7, **No.** 45-48, pp. 2317-2326.(Also online: www.m-hikari.com).