Int. J. Contemp. Math. Sciences, Vol. 7, 2012, no. 47, 2317 - 2326

On Generator Cauchy Matrices of GDRS/GTRS Codes

O. P. Vinocha[1], J. S. Bhullar[2] and B. S. Brar[3]

1. Principal, Ferozepur College of Engineering and Technology
Ferozepur, Punjab, India
vinochar@yahoo.com

2. Department of Applied Sciences, Malout Institute of Management and Information Technology (MIMIT), Malout, Punjab, India
bhullarjaskarn@rediffmail.com

3. Department of Applied Sciences, Baba Farid College of Engineering and Technology, Bathinda, Punjab, India
hodas.bfcet@yahoo.in

Abstract

We show that every GDRS/GTRS codes have systematic generator matrices of the form $[\, I \,/\, \bar{A}] \,/\, [\, I \,/\, \bar{\bar{A}}\,]$, where A is a GC (Generalised Cauchy) matrix, $\bar{A}$ is GEC (Generalised Extended Cauchy) matrix , and $\bar{\bar{A}}$ is GDC (Generalised Doubly Extended Cauchy) matrix ; and conversely every systematic generator matrix of that form generates GDRS/GTRS codes.

Keywords: Cauchy matrix, Generalised Cauchy Matrix, Generalised Extended Cauchy matrix, Generalised Doubly Extended Cauchy matrix, Generalised Doubly Extended Reed-Solomon code, Generalised Triply Extended Reed-Solomon code.

I. Introduction

An [n,k,d] linear code over the finite field F=GF(q) is called MDS if d=n-k+1, where q is a positive power of a prime number. MDS codes can be characterized in terms of their systematic generator matrices. If C be an [n,k,d] code, whose systematic generator matrix G is given by G=[I|A], where I is the identity matrix of order k, A is k × (n-k) matrix, then code C is MDS if and only if every square submatrix of A is non-singular. There may be many systematic ways of building matrices with the property that every square submarix is non-singular. One systematic way of doing this, is the Cauchy matrix construction. A matrix $A=[a_{ij}]_{m\times n}$ is called a Cauchy matrix, if $a_{ij}=1/\ x_i+y_j$, where $x_1,x_2,\ldots,x_m$; $y_1,y_2,\ldots,y_n$ belong to field F=GF(q). Therefore, Cauchy matrix $A_0=[a_{ij}]_{m\times n}$ $a_{ij} =1/x_i+y_j$, will be as:

$$A_0=\begin{bmatrix} \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & . \ . & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & . \ . & \frac{1}{x_2+y_n} \\ . & . & . \ . & . \\ \frac{1}{x_m+y_1} & \frac{1}{x_m+y_2} & . \ . & \frac{1}{x_m+y_n} \end{bmatrix}_{m\times n} \qquad (1)$$

Further, a matrix $A=[a_{ij}]_{m\times n}$ is called an Extended Cauchy matrix, if A has a row(column) of 1's, and, deleting this row(column) of 1's changes matrix A to another matrix $\hat{A}$, which is a Cauchy matrix. Therefore, this Extended Cauchy matrix A (having one row of 1's) may be as:

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

Similarly Extended Cauchy matrix $A=[a_{ij}]_{m\times n}$, having one column of 1's can be displayed. Every square submatrix of an Extended Cauchy matrix A is non-singular if and only if every square submatrix of the underlying Cauchy matrix $\hat{A}$ (obtained by deleting row (column) of 1's from A) is non-singular.

II. Relation Between GC Matrices and GRS Codes

Let any vector z be: $\mathbf{z}=(z_1,z_2,\ldots,z_r)$. Let $D(\mathbf{z})$ denote the diagonal matrix of order r with diagonal entries $D_{ii} = z_i$. Then an m×m matrix A is called a Generalized Cauchy matrix(GC), if A is of the form:

$$A=D(c).A_1.D(d), \tag{3}$$

where A_1 is an m×n Cauchy matrix, $\mathbf{c}=(c_1,c_2,\ldots,c_m)$, $d=(d_1,d_2,\ldots.d_n)$ are vectors of non-zero elements of field F=GF(q).Therefore,

$$A=\left[\frac{c_i d_j}{x_i + y_j}\right]_{m\times n}; \tag{4}$$

where c_i, d_j, x_i, y_j belong to field F=GF(q),$1\le i\le m$, $1\le j\le n$.
If all square submatrices of Cauchy matrix A_1 are non-singular, then all square submatrices of A are also non-singular. Therefore, we can construct a systematic generator matrix for an [n,k] MDS code by linking the identity matrix I_k with a suitably defined k×(n-k) Generalised Cauchy(GC) matrix.

Let $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ be a vector of distinct elements of field F=GF(q). Let $v=(v_1,v_2,\ldots,v_n)$ be a vector of non-zero, but not necessarily distinct elements of field F=GF(q). Then code C is called GRS, denoted by GRS(n,k,**α,v**), if it has a generator matrix of the form: $G=[G_1\ G_2 \ldots G_n]$, where the G_i's are columns of the form: $G_i=[v_i,v_i\alpha_i,v_i\alpha_i^2,\ldots v_i\alpha_i^{k-1}]'_{k\times 1}$.

Roth and Seroussi (1985) proved that GRS code has a systematic generator matrix of the form [I|A], where A is a Generalised Cauchy(GC) matrix, and conversely every systematic matrix of that form generates a Generalised Reed Solomon(GRS) code.

Theorem 1: Let C be a GRS(n+1,k,**α,v**) code defined by $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$,$\mathbf{v}=(v_1,v_2,\ldots,v_n,v_{n+1})$.Then code C has a systematic generator matrix of the form [I|A], where A is a k×(n+1-k) GC matrix such that $A_{ij}=\frac{c_i d_j}{x_i + y_j}$ with:

$$x_i=-\alpha_i, 1\le i\le k \tag{5}$$

$$y_j=\alpha_{j+k}, 1\le j\le (n+1-k) \tag{6}$$

$$c_i=\frac{v_i^{-1}}{\prod_{1\le t\le k\,;\,t\ne i}(\alpha_i-\alpha_t)},\ 1\le i\le k \tag{7}$$

$$d_j=v_{j+k}\cdot\prod_{1\le t\le k}(\alpha_{j+k}-\alpha_t)\ ,\ 1\le j\le (n+1-k) \tag{8}$$

Conversly,if A is a $k\times(n+1-k)$ GC matrix defined by vectors $\mathbf{x}=(x_i)_{i=1}^{k}$, $\mathbf{y}=(y_j)_{j=1}^{n+1-k}$, $\mathbf{c}=(c_i)_{i=1}^{k}$, $\mathbf{d}=(d_j)_{j=1}^{n+1-k}$, such that every square submatrix of A is non-singular, then [I|A] generates a GRS($n+1,k,\boldsymbol{\alpha},\mathbf{v}$) code with:

$$\alpha_i=-x_i, 1\le i\le k \tag{9}$$

$$\alpha_j=y_{j-k}, k+1\le j\le n+1 \tag{10}$$

$$v_i=\frac{c_i^{-1}}{\prod_{1\le t\le k\,;\,t\ne i}(x_t-x_i)},\ 1\le i\le k \tag{11}$$

$$v_j=\frac{d_{j-k}}{\prod_{i\le t\le k}(x_t+y_{j+k})}\ ,\ (k+1)\le j\le n+1 \tag{12}$$

Proof: Here C is a GRS($n+1,k,\boldsymbol{\alpha},\mathbf{v}$) code defined by: $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$, $\mathbf{v}=(v_1,v_2,\ldots,v_n,v_{n+1})$, where $\boldsymbol{\alpha}$ is a vector of distinct elements of field F=GF(q), $\mathbf{v}$ is a vector of non-zero(not necessarily distinct)elements of field F=GF(q). Because code C is GRS, therefore C has a generator matrix of the form:$G=[G_1, G_2,\ldots\ldots, G_n, G_{n+1}]$,where the G_i's are columns of the form: $G_i=(v_i, v_i\alpha_i, v_i\alpha_i^2,\ldots, v_i\alpha_i^{k-1})'$.

Therefore,$G=[G_1, G_2,\ldots\ldots, G_n, G_{n+1}]$

$=[\alpha_j^{i-1}]_{k\times(n+1)}\,.\,D(v_1,v_2,\ldots,v_n,v_{n+1})$,$1\le j\le n+1$, $1\le i\le k$.

$=\overline{G}\,.D(\mathbf{v})$,where $D(\mathbf{v})=D(v_1,v_2,\ldots,v_n,v_{n+1})$ and $\overline{G}=[\alpha_j^{i-1}]_{k\times(n+1)}$,$1\le j\le n+1, 1\le i\le k$.

Now $\overline{G}=[\alpha_j^{i-1}]_{k\times(n+1)}$,($1\le j\le n+1$, $1\le i\le k$) = [P|Q]

where: $P=[\alpha_j^{i-1}]_{k\times k}$, $1\le i,j\le k$, a $k\times k$ Vandermonde matrix, and

$Q=[\alpha_{j+k}^{i-1}]_{k\times(n+1-k)}$, $1\le i\le k$, $1\le j\le(n+1-k)$, a $k\times(n+1-k)$ matrix.

Therefore, a generator matrix of code C=GRS($n+1,k,\boldsymbol{\alpha},\mathbf{v}$) is:

$G=\overline{G}\,.\,D(\mathbf{v})=[P|Q].\,D(\mathbf{v})$, where $\overline{G}=[\alpha_j^{i-1}]$, $1\le i,j\le k$, $1\le j\le(n+1)$,

$$P=[\alpha_j^{i-1}]_{k\times k}, 1\le i,j\le k,\ \text{a } k\times k \text{ Vandermonde matrix.} \tag{13}$$

$$Q=[\alpha_{j+k}^{i-1}]_{k\times(n+1-k)}, 1\le i\le k, 1\le j\le(n+1-k) \tag{14}$$

Let systematic generator matrix of code C is [I|A],where I is I_k, A is $A_{k\times(n+1-k)}$. Therefore:

$$[I_k|A_{k\times(n+1-k)}]\ \sim\ G\ \sim\ \overline{G}\,.\,D(\mathbf{v})\sim[P|Q].\,D(\mathbf{v}) \tag{15}$$

Clearly P is a Vandermonde matrix of order k. P^{-1} is given by(D.E. Knuth(1969):

$$(P^{-1})_{ij} = \frac{f_{i,j-1}}{\prod_{1\le t\le k; t\ne i} (\alpha_i - \alpha_t)}, \ 1 \le i, j \le k \tag{16}$$

where $f_i(z)= \prod_{1\le t\le k; t\ne i} (z-\alpha_t) = \sum_{0\le r\le k-1} f_{ir}.z^r$ (17)

We can take Vandemonde matrices of various orders , verify that all the entries of these matrices are in accordance with (16)-(17),and hence we can verify the formulations (16)-(17). We can also verify that $A = (D(\mathbf{u}))^{-1}.P^{-1}.Q.D(\mathbf{w})$, by taking any values of (n+1) and k, and by making generalization. Therefore, systematic generator matrix of GRS(n+1,k,**α,v**) code C is [I | A], where:

$$A=(D(\mathbf{u}))^{-1}.P^{-1}.Q.D(\mathbf{w}) \tag{18}$$

So,using (5),(6),(7),(8)(14),(16),(17), we will obtain $(i,j)^{th}$ entry of A as:

$$A_{ij}=[(D(\mathbf{u}))^{-1}.P^{-1}.Q.D(\mathbf{w})]_{ij} = \frac{c_i d_j}{x_i + y_j}, \ 1\le i\le k, \ 1\le j\le (n+1-k).$$

Therefore, A is a k×(n+1-k) GC matrix.

Conversely:

Now given is that A is a k×(n+1-k) GC matrix defined by vectors $x = (x_i)_{i=1}^{k}$, $y = (y_j)_{j=1}^{(n+1-k)}$, $c = (c_i)_{i=1}^{k}$, $d=(d_j)_{j=1}^{(n+1-k)}$, such that every square submatrix of A is non-singular. Then reversing the steps in the first part of proof, we shall arrive at the conclusion that [I |A] generates a GRS(n+1,k, **α,v**) code , where **α** and **v** can be derived from equations (5)-(8) as follows:

Equation (5) is: $x_i=-\alpha_i$,$(1\le i\le k) \Rightarrow \alpha_i = -x_i$,$(1\le i\le k)$, which is equation (9).

Equation(6)is:$y_j=\alpha_{j+k}$,$(1\le j\le (n+1-k))$.Changing j to (j-k),we get: $y_{j-k}=\alpha_{(j-k)+k}$,$(1\le j-k\le (n+1-k)) \Rightarrow y_{j-k}=\alpha_j$, $(k+1\le k+j-k\le k+(n+1-k)) \Rightarrow \alpha_j = y_{j-k}$, $(k+1\le j\le n+1)$, which is equation (10).

Equation(7)is: $c_i = \dfrac{v_i^{-1}}{\prod_{1\le t\le k;\ t\ne i} (\alpha_i - \alpha_t)}, \ 1 \le i \le k \Rightarrow$

$v_i = \dfrac{c_i^{-1}}{\prod_{1\le t\le k;\ t\ne i} (-x_i - (-x_t))}, \ 1 \le i \le k$ (using(9)) $= \dfrac{c_i^{-1}}{\prod_{1\le t\le k;\ t\ne i} (x_i - x_t))}, \ 1 \le i \le k$,which is equation (11).

Equation(8)is:

$$d_j = v_{j+k} . \prod_{1\le t\le k} (\alpha_{j+k} - \alpha_t) \ , 1 \le j \le (n+1-k)$$

$$\Rightarrow v_{j+k} = \frac{d_j}{\prod_{1\le t\prec} (\alpha_{j+k} - \alpha_t)}, 1 \le j \le n+1-k$$

Changing j to j-k, and using (9),(10), we will get:

$\Rightarrow v_j = \dfrac{d_{j-k}}{\prod_{1\le t\le k}(x_t + y_{j-k})}, k+1 \le j \le n+1$, which is equation (12).

III. Relation Between GEC Matrices and GDRS Codes

An m×n matrix A is called a Generalised Extended Cauchy (GEC) matrix, if A is of the form:

A=D(c).A_2.D(d),

where A_2 is an m×n extended cauchy matrix, **c**=(c_1,$c_{2,......,}$$c_m$), d= ($d_1$,$d_2$,…..$d_n$) are vectors of non-zero elements of field F=GF(q). Therefore,

$$A=\begin{bmatrix} c_1d_1 & c_1d_2 & . \ . & c_1d_n \\ \dfrac{c_2d_1}{x_1+y_1} & \dfrac{c_2d_2}{x_1+y_2} & . \ . & \dfrac{c_2d_n}{x_1+y_n} \\ \dfrac{c_3d_1}{x_2+y_1} & \dfrac{c_3d_2}{x_2+y_2} & . \ . & \dfrac{c_3d_n}{x_2+y_n} \\ . & . & . \ . & . \\ \dfrac{c_md_1}{x_{m-1}+y_1} & \dfrac{c_md_2}{x_{m-1}+y_2} & . \ . & \dfrac{c_md_n}{x_{m-1}+y_n} \end{bmatrix}_{m\times n} \tag{19}$$

If all square submatrices of Extended Cauchy matrix A_2 are non-singular, then all square submatrices of A are also non-singular. Therefore, we can construct a systematic generator for an [n,k] MDS code by linking the identity matrix I_k with a suitably defined k×(n-k) Generalised Extended Cauchy(GEC) matrix.

A generator matrix of Extended GRS code is a generator matrix of GRS(n,k,**α,v)** code, when one of α_i's is zero. Suppose α_n=0. So, a generator matrix of Extended GRS code will be:

$$G=\begin{bmatrix} v_1 & v_2 & . \ . & v_n \\ v_1\alpha_1 & v_2\alpha_2 & . \ . & 0 \\ v_1\alpha_1^{\ 2} & v_2\alpha_2^{\ 2} & . \ . & 0 \\ . & . & . \ . & . \\ v_1\alpha_1^{\ k-1} & v_2\alpha_2^{\ k-1} & . \ . & 0 \end{bmatrix}_{k\times n} \tag{20}$$

Code can be further extended by allowing a column of G of the form: $G_\infty = (0\ 0\ 0 \ldots 0, v_\infty)'$,where v_∞ is a non-zero element of field F = GF(q), as a result of which MDS propery is preserved. The resulting code is called Generalised Doubly Extended Reed-Solomon code, denoted by GDRS (n+1,k,**α,v**) , where $\boldsymbol{\alpha} = (\alpha_1,\alpha_2,\ldots,\alpha_{s-1}, \alpha_\infty, \alpha_s, \ldots,\alpha_n)$ and $\mathbf{v} = (v_1,v_2,\ldots,v_{s-1}, v_\infty, v_s, \ldots,v_n)$, where s is the index of G_∞ in G. Therefore, a generator matrix of GDRS (n+1,k,**α,v**) may be:

$$G = \begin{bmatrix} v_1 & v_2 & .. & v_n & 0 \\ v_1\alpha_1 & v_2\alpha_2 & .. & 0 & 0 \\ v_1\alpha_1^{\ 2} & v_2\alpha_2^{\ 2} & .. & 0 & 0 \\ . & . & .. & . & . \\ v_1\alpha_1^{\ k-1} & v_2\alpha_2^{\ k-1} & .. & 0 & v_\infty \end{bmatrix}_{k\times(n+1)} \tag{21}$$

Roth and Serorussi (1985) proved that GDRS code has a generator systematic matrix of the form [I|A], where A is a Generalised Extended Cauchy(GEC) matrix, and, conversely , every systematic generator matrix of that form generates a GDRS code.

IV. Relation Between GDC Matrices and GTRS Codes

An m×n matrix A is called a Doubly Extended Cauchy matrix, if A has two rows(columns) of 1's, and deleting these two rows (columns) of 1's changes matrix A into another matrix $\hat{\hat{A}}$, which is a Cauchy matrix. Therefore, a Doubly Extended Cauchy matrix, having two rows of 1's will be as:

$$\begin{bmatrix} 1 & 1 & . & . & 1 \\ 1 & 1 & . & . & 1 \\ \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & . & . & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & . & . & \frac{1}{x_2+y_n} \\ . & . & . & . & . \\ \frac{1}{x_{m-2}+y_1} & \frac{1}{x_{m-2}+y_2} & . & . & \frac{1}{x_{m-2}+y_n} \end{bmatrix}_{m\times n} \tag{22}$$

An $m\times n$ matrix A is called a Generalised Doubly Extended Cauchy(GDC) matrix, if it is of the form: $A=D(c).A_3.D(d)$, where A_3 is an $m\times n$ Doubly Extended Cauchy matrix, $\mathbf{c}=(c_1,c_2,\ldots,c_m)$, $d=(d_1,d_2,\ldots.d_n)$ are vectors of non-zero elements of field $F=GF(q)$.

If all square submatrices (of order >2) of Doubly Extended Cauchy matrix A_3 are non-singular, then all square submatrices(of order >2) of A are also non-singular. Therefore, we can construct a systematic generator for an [n,k] MDS code by linking the identity matrix I_k with a suitably defined $k\times(n-k)$ Generalised Doubly Extended Cauchy(GDC) matrix.

The generator matrix of code GDRS(n+1,k, **α,v**) can be further extended by allowing a more column of G of the form: $G_\infty^{/}=(0\ 0\ 0\ldots.0\ \ v_\infty^{/})^{/}$, where $v_\infty^{/}$ is a non-zero element of field $F=GF(q)$, such that MDS property is preserved. The resulting code is called Generalised Triply Extended Reed-Solomon code, denoted by GTRS (n+2,k, **α,v**), where $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_{s-1},\alpha_\infty,\alpha_\infty^{/},\alpha_s,\ldots,\alpha_n)$ and $\mathbf{v}=(v_1,v_2,\ldots,v_{s-1},v_\infty,v_\infty^{/},v_s,\ldots,v_n)$, where s is the index of G_∞ ,$G_\infty^{/}$ in G.

Theorem 2: Let C be a GTRS (n+2,k, **α,v**) code defined by $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_{s-1},\alpha_\infty,\alpha_\infty^{/},\alpha_s,\ldots,\alpha_n)$ and $\mathbf{v}=(v_1,v_2,\ldots,v_{s-1},v_\infty,v_\infty^{/},v_s,\ldots,v_n)$, where $k\le s\le n+2$. Then C has a generator matrix of the form $[I\,|\,\overline{\overline{A}}\,]$, where $\overline{\overline{A}}=[A_1, A_2,\ldots,A_{s-k-1},A_\infty, A_\infty^{/}, A_{s-k}\ldots., A_{n-k}]$ is a $k\times(n+2-k)$ GDC matrix obtained from the GC matrix A of Theorem 1 by inserting the columns $A_\infty=d_\infty(c_1,c_2,\ldots,c_k)^{/}$, $A_\infty^{/}=d_\infty^{/}(c_1,c_2,\ldots,c_k)^{/}$ before the (s-k)th column of A if $s<n+2$, or as the last column if $s=n+2$,and $d_\infty=v_\infty$, $d_\infty^{/}=v_\infty^{/}$, and c_i's are as defined in (7).

Proof: In Theorem 1, code C was GDRS(n+1,k, **α,v**). Here, code C is GTRS (n+2,k, **α,v**), defined by $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_{s-1},\alpha_\infty,\alpha_\infty^{/},\alpha_s,\ldots,\alpha_n)$ and $\mathbf{v}=(v_1,v_2,\ldots,v_{s-1},v_\infty,v_\infty^{/},v_s,\ldots,v_n)$, where $k\le s\le n+2$. So, generator matrix of GTRS(n+2,k, **α,v**) code contains two additional columns: $G_\infty=(0\ 0\ 0\ldots.0\ \ v_\infty)^{/}$ and $G_\infty^{/}=(0\ 0\ 0\ldots.0\ \ v_\infty^{/})^{/}$ as compared to that of GRS code. Therefore, generator matrix of GTRS (n+2,k,**α,v**) code may be like this:

$$G=\begin{bmatrix} v_1 & v_2 & . & . & v_{s-1} & 0 & 0 & v_s & . & . & v_n \\ v_1\alpha_1 & v_2\alpha_2 & . & . & v_{s-1}\alpha_{s-1} & 0 & 0 & v_s\alpha_s & . & . & v_n\alpha_n \\ v_1\alpha_1^{\,2} & v_2\alpha_2^{\,2} & . & . & v_{s-1}\alpha_{s-1}^2 & 0 & 0 & v_s\alpha_s^2 & . & . & v_n\alpha_n^2 \\ . & . & . & . & . & . & . & . & . & . & . \\ v_1\alpha_1^{\,k-1} & v_2\alpha_2^{\,k-1} & . & . & v_{s-1}\alpha_{s-1}^{k-1} & v_\infty & v_\infty^{/} & v_s\alpha_s^{k-1} & . & . & v_n\alpha_n^{k-1} \end{bmatrix}_{k\times(n+2)} \tag{23}$$

Because $k\le s\le n+2$, and k is the number of message-symbols, so G_∞ and $G_\infty^{/}$ will appear among the columns of G corresponding to check-digits.

Therefore, G_∞ and $G_\infty^{/}$ will correspond respectively to columns A_∞ and $A_\infty^{/}$ given by:

$$A_\infty = D(\mathbf{u})^{-1} . P^{-1} . G_\infty \ ; \quad A_\infty^{/} = D(\mathbf{u})^{-1} . P^{-1} . G_\infty^{/}$$

in the systematic generator matrix of code C i.e. in $[\, I_{k\times k} \mid A_{k\times(n-k++2)}\,]$.

So, $A_\infty = D(\mathbf{u})^{-1} .(P^{-1})_k . v_\infty$ and $A_\infty^{/} = D(\mathbf{u})^{-1} .(P^{-1})_k . v_\infty^{/}$,
where $(P^{-1})_k$ denotes the kth column of P^{-1}, and $\mathbf{u}=(v_1,v_2,\ldots,v_k)$. Therefore,

$$A_{i\infty} = v_i^{-1} .(P^{-1})_{ik} . v_\infty \qquad (24)$$

and $$A_{i\infty}^{/} = v^{-1} .(P^{-1})_{ik} . v_\infty^{/}, \qquad (25)$$

Consider the polynomial: $$f_i(z)=\prod_{1\le t\le k;t\ne i} (z-\alpha_t) = \sum_{0\le r\le k-1} f_{ir} .z^r \qquad (26)$$

P^{-1} is given by [D.E.Knuth (1969)]: $$(P^{-1})_{ij} = \frac{f_{i,j-1}}{\prod_{1\le t\le k;t\ne i}(\alpha_i-\alpha_t)},\ 1\le i, j\le k \qquad (27)$$

Therefore (24) implies:

$$A_{i\infty}=v_i^{-1}. \frac{f_{i,k-1}}{\prod_{1\le t\le k;t\ne i}(\alpha_i-\alpha_t)} .v_\infty ,\quad 1 \le i \le k \qquad (28)$$

Using (26) and (7) in (28),we get: $$A_{i\infty}= \frac{v_i^{-1}}{\prod_{1\le t\le k;t\ne i}(\alpha_i-\alpha_t)} .v_\infty ,\quad 1 \le i \le k$$

$$=(d_\infty).(c_1, c_2,\ldots, c_k).$$

Therefore, $A_\infty=(d_\infty).(c_1, c_2,\ldots, c_k)^{/}$.

Similarly (25) implies (using (7): $A_{i\infty}^{/} = v^{-1}(P^{-1})_{ik}.v_\infty^{/} = (d_\infty^{/}).(c_1, c_2,\ldots,c_k)$.

Therefore, $A_\infty^{/}=(d_\infty^{/}).(c_1, c_2,\ldots, c_k)^{/}$.

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, 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.

Received: September, 2012