1-1-1980

# On code construction via interpolation.

Loc Van Ngo

# ON CODE CONSTRUCTION VIA INTERPOLATION

by

Loc Van Ngo

A Thesis

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

Master of Science

in

Electrical Engineering

Lehigh University

1980

CERTIFICATE OF APPROVAL

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering.

May 9, 1980
(date)

Professor in Charge

Chairman of Department

## Acknowledgement

I would like to thank Dr. Kenneth Kai-Ming Tzeng for his helpful suggestions, the National Science Foundation for support under Grant ENG-76-10758 and Lehigh University for the Byllesby fellowship.

Table of Contents

## Abstract

Several bases for constructing error-correcting codes such as the matrix alternants, the Mattson - Solomon polynomial, and the Lagrange's interpolation, and lately the generalized interpolation introduced by Mandelbaum have been proposed.

The relationship between the generalized interpolation and the other approaches in constructing error-correcting codes has been investigated in this thesis. We have shown that most of the important classes of codes can be defined in terms of the generalized interpolation, which, indeed, provides a unified framework for the previous methods. Dual codes of these codes have also been derived in terms of the new interpolation.

## I. Introduction

Coding theory began with the work of Shannon Hamming. Since the first papers on information theory were published in 1948 by Shannon, a great deal of research has been conducted on the problem of designing efficient schemes by which information can be coded for reliable transmission across noisy channels. A very important result which Shannon had demonstrated was that by proper encoding and decoding of the data, it is possible to reduce errors induced by a noisy channel to any desired level without sacrificing the data transmission rate. As a result, numerous papers had been published on the subject of constructing error-correcting codes using more and more sophisticated mathematical techniques as well as on the problem of devising an efficient decoder. A very powerful mathematical tool which has been extensively used in coding theory is the Galois field. It is possible, by associating each symbol of certain codes with an element in a Galois field, to derive an algebraic equation whose roots represent the locations of the errors induced during transmission. The decoding problem is then reduced to two basic tasks, namely to set up the mentioned algebraic equation and compute its roots. Still, there exists several different approaches which one can take in defining error-correcting codes. Typically, codes are constructed either

via matrix approach or through a certain transformation of the codeword. In the former approach, it is very common to first define an n x m parity check matrix H, n being the length of the codeword; a code c is said to belong to the code defined by H if and only if cH is a null n x 1 matrix. Alternatively, a codeword or an n-tuple of elements in a Galois field K, is first transformed through a predefined formula into a polynomial with coefficients over K, which, in turn, must satisy a certain condition. Typical examples of such transformation or interpolation are Mattson-solomon polynomial, Lagrange's interpolation and lately, a generalized method of interpolation proposed by Mandelbaum.[10]

The purpose of this thesis is primarily centered on these bases of constructing error-correcting codes. Although the relationship between the matrix approach and the Lagrange's interpolation as well as Mattson-Solomon polynomials is well established, neither a connection of the generalized interpolation proposed by Mandelbaum with the previous approaches is yet firmly identified nor an extensive study of all the important existing codes via the latter approach has been attempted. It is the goal of this thesis to expand on these tasks.

An interesting point is that Mandelbaum defined error-correcting codes using the Chebyshev system of functions which is

later referenced to as c-system. A study of existing codes through the above approach eventually leads to defining their respective generator matrices. On the other hand, it is possible to show, by extending the Langrange's interpolation formula, that dual codes can be easily defined in terms of their parity check matrices. Since the parity check matrix of the dual code is identical to the generator matrix of the corresponding original code, a direct comparison between these two matrices is possible. Finally, it is also possible to investigate whether the dual of a certain class of code belongs to this class, which is the third task attempted in this thesis. In the following section, a review of important classes of codes as well as different bases of code construction, including the generalized interpolation, is briefly presented. The first part of the third section is centered on the relationship of generalized interpolation with the matrix approach and Lagrange's interpolation; in the second part, existing codes are studies through the generalized interpolation. In the fourth section, it is shown that dual codes can be obtained from Lagrange's interpolation, consequently, it is possible to derive their respective parity check matrix.

## II. Preliminaries

Of the numerous classes of random-error-correcting codes proposed to date, the class discovered by Helgert - the alternant codes - and first presented in one of his papers[5] in 1974 is one of the most extensive and powerful ones. Obtained by a small modification of the parity check matrix of the BCH codes, it includes other important subclasses, namely Goppa, Srivastava and Chien-Choy generalized BCH codes.

It should be noted that the relationship between these codes has been studied and derived in several papers.[4],[7] and [1] The purpose of this section is doublefold:

i) to introduce important classes of existing error-correcting codes by first presenting a summarized and brief review of these codes and then indicating how one can derive a code from another. Such a summary will serve as a helpful reference for the following section.

ii) to present different approaches of defining error-correcting codes as was mentioned previously, namely the matrix approach and interpolation methods.

In the first part of the section, important families of error-correcting codes will be introduced following the matrix approach e.g. defining codes in terms of the parity check matrix.

The other two parts are devoted to the characterization of codes through interpolation methods, the Lagrange's interpolation formula and the generalized transformation proposed by Mandelbaum.

## A. Matrix Approach

Due to the large extent of the alternant codes it seems to be more appropriate to first introduce this family of codes and then present other codes as special cases.

### 1. Alternant codes

The alternant code is defined by a parity check matrix of the form:

$$H_{alt} = \begin{bmatrix} y_1 g_1(x_1) & y_2 g_1(x_2) \cdots y_n g_1(x_n) \\ y_1 g_2(x_1) & y_2 g_2(x_2) \cdots y_n g_2(x_n) \\ \vdots & \vdots \\ y_1 g_t(x_1) & y_2 g_t(x_2) \cdots y_n g_t(x_n) \end{bmatrix} \quad (1)$$

where the $y_i$, $1 \leq i \leq n$ are any (not necessarily distinct) non-zero elements of $GF(q^m)$, the $x_i$, $1 \leq i \leq n$ are distinct elements of $GF(q^m)$ and

$$g_k(x) = C_{0k} + C_{1k}x + C_{2k}x^2 + \ldots + C_{t-1,k}x^{t-1} \quad (2)$$

is a polynomial of degree less than or equal to t-1 with coefficients from $GF(q^m)$ for k = 1,2,...t. The alternant code thus defined is a linear code over GF(q) with length n, minimum distance $d \geq t + 1$ and having k information symbols, $k \geq n - mt$. The matrix of form (1) can be rewritten as:

$$H_{ALT} = \begin{bmatrix} g_1(x_1) & g_1(x_2)\ldots g_1(x_n) \\ g_2(x_1) & g_2(x_2)\ldots g_2(x_n) \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ g^t(x_1) & g^t(x_2)\ldots g^t(x_n) \end{bmatrix} \begin{bmatrix} y_1 & 0 \ldots 0 \\ 0 & y_2 \ldots 0 \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ 0 & 0 \ldots y_n \end{bmatrix}$$

By replacing each entry $g_i(x_j)$ for i = 1,2,...t and j = 1,2,...,n, it is easily seen that H can be factored into the form:

$$H_{ALT} = cxy$$

where

$$c = \begin{bmatrix} c_{01} & c_{11} \cdots c_{t-1,1} \\ c_{02} & c_{12} \cdots c_{t-1,2} \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ \cdot & \cdot \quad\quad \cdot \\ c_{0t} & c_{1t} \cdots c_{t-1,t} \end{bmatrix}$$

$$X = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{t-1} & x_2^{t-1} & \cdots & x_n^{t-1} \end{bmatrix}$$

and

$$Y = \begin{bmatrix} y_1 & 0 & \cdots & 0 \\ 0 & y_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & y_n \end{bmatrix}$$

A fairly simple proof (see Appendix) shows that codes derived from matrices of the form (1) and the form XY, namely

$$H_{ALT} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{t-1} & x_2^{t-1} & \cdots & x_n^{t-1} \end{bmatrix} \begin{bmatrix} y_1 & 0 & \cdots & 0 \\ 0 & y_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & y_n \end{bmatrix} \quad (3)$$

are identical. Hence both forms (1), (3) are equivalent and will be referenced to indicate the alternant codes, whichever form is more appropriate.

2. Subclasses of alternant codes

a) BCH codes

The BCH codes were first discovered by Hocquenghem in 1959 and independently by Bose and Chandhuri in 1960. These codes are cyclic, namely if $(v_0,v_1,\ldots,v_{n-1})$ is a codeword, then its cyclic shift $(v_1,v_2,\ldots,v_{n-1},v_0)$ is also a codeword.

For any positive integers m and t ($t < q^{m-1}$), there exists a BCH code over GF(q) of length $n \leq q^m - 1$, with minimum distance $d \geq t + 1$ and having k information symbols, with $k \geq n - mt$.

Such a BCH code is generated by a polynomial g(x) over GF(q) having $\alpha^b$, $\alpha^{b+1}$, $\alpha^{b+t-1}$ as zeroes, where $\alpha$ is a nonzero element of $GF(q^m)$ of order n and b, an arbitrary integer. Its parity check matrix, which can be derived rather easily, (see Appendix) is of the form:

$$H_{BCH} = \begin{bmatrix} 1 & \alpha^{b} & (\alpha^{b})^2 & \cdots & (\alpha^{b})^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & \cdots & (\alpha^{b+1})^{n-1} \\ 1 & \alpha^{b+2} & (\alpha^{b+2})^2 & \cdots & (\alpha^{b+2})^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+(t-1)} & (\alpha^{b+(t-1)})^2 & \cdots & (\alpha^{b+(t-1)})^{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^{1} & \alpha^{2} & \cdots & \alpha^{(n-1)} \\ 1 & \alpha^{2} & \alpha^{4} & & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{(t-1)} & \alpha^{(t-1)2} & \cdots & \alpha^{(t-1)(n-1)} \end{bmatrix} \times$$

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha^{b} & 0 & \cdots & 0 \\ 0 & 0 & \alpha^{2b} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \alpha^{(n-1)b} \end{bmatrix} \qquad (4)$$

The case b-1 has been referred to as the narrow-sense BCH codes. Codes of length $n = q^m-1$ are called primitive BCH codes.

It is obvious from comparing both parity check matrices of form (3) and (4) that the BCH codes are special cases of the alternant codes characterized by

$$x_i = \alpha^{i-1} \quad , \quad i = 1,2,\ldots,n$$

and $$y_i = (\alpha^b)^{i=1}$$

$$= x_i^b \quad , \quad i = 1,2,\ldots,n$$

b) Generalized BCH codes

Let x be a primitive nth root of unity in $GF(q^m)$, then for any $a(x) = \sum_{i=0}^{n-1} a_i x^i$ with $a_0, a_1, \ldots, a_{n-1}$ in GF(q), the Mattson-Solomon polynomial - Fourier transform - a(x) with respect to $\alpha$ is defined as

$$A(Z) = \sum_{i=0}^{n-1} A_i Z^i \text{ , with } A_i \in GF(q),\ i=0,1,\ldots,n-1$$

where $A_i = a(\alpha^i)$. Conversely, the inverse Fourier transform of any A(Z) is $a(x) = \sum_{i=0}^{n-1} a_i x^i$, where $a_i = n^{-1} A(\alpha^{-i})$, $i=0,1,2,\ldots,n-1$. Based on the Mattson-Solomon polynomial, another class of error-correcting codes is proposed in 1975 by Chien-Choy as algebraic generalization of BCH codes. The generalized BCH code of length n over GF(q) associated with polynomials P(Z) and G(Z) is defined as follows - P(Z) and G(Z) being polynomials with coefficients in GF(q) relatively prime to $x^n-1$ with deg $P(Z) \leq n - 1$ and

deg $G(Z) \leq n - 1$. The code consists of all $v(x)$ with coefficients in GF(q) and degree less than n-1 such that the Mattson-Solomon polynomial $V(Z)$, derived from $v(x)$ satisfies:

$$[V(Z)P(Z)]_n \equiv 0 \mod G(Z)$$

where $[V(Z)P(Z)]_n = V(Z)P(Z) \mod x^n-1$. Let $p(x)$ and $g(x)$ be polynomials over GF(q) associated with the Mattson-Solomon polynomials $P(Z)$ and $G(Z)$, respectively such that:

$$p(x) = p_0 + p_1x + p_2x^2 + \ldots + p_{n-1}x^{n-1}$$

$$g(x) = g_0 + g_1x + g_2x^2 + \ldots + g_{n-1}x^{n-1}$$

The parity check matrix of GBCH code with associated polynomials $P(Z)$ and $G(Z)$ is derived as

$$\begin{bmatrix} p_0g_0^{-1} & p_1g_1^{-1}\alpha^{-1} & p_2g_2^{-1}\alpha^{-2} & \ldots & p_ng_n^{-1}\alpha^{-(n-1)} \\ p_0g_0^{-1} & p_1g_1^{-1}\alpha^{-2} & p_2g_2^{-1}\alpha^{-4} & \ldots & p_ng_n^{-1}\alpha^{-2(n-1)} \\ p_0g_0^{-1} & p_1g_1^{-1}\alpha^{-3} & p_2g_2^{-1}\alpha^{-6} & \ldots & p_ng_n^{-1}\alpha^{-3(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ p_0g_0^{-1} & p_1g_1^{-1}\alpha^{-t} & p_2g_2^{-1}\alpha^{-2t} & \ldots & p_ng_n^{-1}\alpha^{-t(n-1)} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(n-1)} \\ 1 & \alpha^{-3} & \alpha^{-6} & \cdots & \alpha^{-3(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{-t} & \alpha^{-2t} & \cdots & \alpha^{-t(n-1)} \end{bmatrix} \times$$

$$\begin{bmatrix} p_0 g_0^{-1} & 0 & 0 & \cdots & 0 \\ 0 & p_1 g_1^{-1} & 0 & \cdots & 0 \\ 0 & 0 & p_2 g_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & p_{n-1} g_{n-1}^{-1} \end{bmatrix} \qquad (5)$$

with $t = \deg G(Z)$.

Notice that the GBCH code with associated polynomials $P(Z) = Z^{b+(t-1)}$ and $G(Z) = Z^t$ is the BCH code with $\alpha^{-b}$, $\alpha^{-(b+1)}$, $\alpha^{-[b+(t-1)]}$ being the zeroes of its generator polynomial. In fact, let $p(x)$ and $g(x)$ be polynomials associated with $P(Z)$ and $G(Z)$ respectively:

$$p(x)=\frac{1}{n}[1+x^{-[b+(t-1)]}x+\alpha^{-2[b+(t-1)]}x^2+\ldots+\alpha^{-(n-1)[b+(t-1)]}x^{n-1}]$$

and

$$g(x)=\frac{1}{n}[1+\alpha^{-t}x+\alpha^{-2t}x^2+\ldots+\alpha^{-(n-1)t}x^{n-1}]$$

Substituting each $p_i = \frac{\alpha}{n}^{-i[b+(t-1)]}$ and $g_i = \frac{\alpha}{n}^{-it}$ ;
$i = 0,1,2,\ldots,n-1$ in $H_{GBCH}$ (5) yields: $p_i g_i^{-1} = \alpha^{-i(b-1)}$.

$$\begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(n-1)} \\ 1 & \alpha^{-3} & \alpha^{-6} & \cdots & \alpha^{-3(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{-t} & \alpha^{-2t} & \cdots & \alpha^{-t(n-1)} \end{bmatrix} \quad x$$

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha^{-(b-1)} & 0 & \cdots & 0 \\ 0 & 0 & \alpha^{-2(b-1)} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \alpha^{-(n-1)(b-1)} \end{bmatrix}$$

or

$$\begin{bmatrix} 1 & \alpha^{-b} & \alpha^{-2b} & \cdots & \alpha^{-(n-1)b} \\ 1 & \alpha^{-(b+1)} & \alpha^{-2(b+1)} & \cdots & \alpha^{-(n-1)(b+1)} \\ 1 & \alpha^{-(b+2)} & \alpha^{-2(b+2)} & \cdots & \alpha^{-(n-1)(b+2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{-[b+(t-1)]} & \alpha^{-2[b+(t-1)]} & \cdots & \alpha^{-(n-1)[b+(t-1)]} \end{bmatrix}$$

which is identical to $H_{BCH}$ (4) except that $\alpha$ is replaced by $\alpha^{-1}$.

By letting $x_i = \alpha^{-(i-1)}$ and $y_i = p_{i-1} g_{i-1}^{-1} \alpha^{-(i-1)}$ in (5) $i = 1,2,\ldots,n$ and comparing with the matrix in (3), it is seen that, indeed, the generalized BCH codes are subcodes of the alternant codes.

c) Generalized Srivastava codes

Another important class of alternant codes are the generalized Srivastava codes.

It is a linear code with symbols from GF(q), having the following parameters:

| | |
|---|---|
| Block length: | $n \leq q^m - 1$ |
| Number of information symbols: | $k \geq n - mst$ |
| Minimum distance: | $d \geq st + 1$ |

given $n + s$ distinct elements $\alpha_1,\alpha_2,\ldots,\alpha_n,w_1,w_2,\ldots,w_s$ of $GF(q^m)$ and $n$ nonzero elements $z_1,z_2,\ldots,z_n$ of $GF(q^m)$, $t$ being a positive integer. It is defined by the parity check matrix:

$$H_{GSR} = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_s \end{bmatrix} \tag{6}$$

where

$$H_\ell = \begin{bmatrix} \frac{z_1}{\alpha_1 - w_\ell} & \frac{z_2}{\alpha_2 - w_\ell} & \cdots & \frac{z_n}{\alpha_n - w_\ell} \\ \frac{z_1}{(\alpha_1 - w_\ell)^2} & \frac{z_2}{(\alpha_2 - w_\ell)^2} & \cdots & \frac{z_n}{(\alpha_n - w_\ell)^2} \\ \vdots & \vdots & & \vdots \\ \frac{z_1}{(\alpha_1 - w_\ell)^t} & \frac{z_2}{(\alpha_2 - w_\ell)^t} & \cdots & \frac{z_n}{(\alpha_n - w_\ell)^t} \end{bmatrix} \tag{7}$$

for $\ell = 1,2,\ldots,s$.

The original Srivastava codes are the special case $t = 1$, $z_i = \alpha_i^{\mu}$ for some integer $\mu$ and have the parity check matrix

$$H_{SR} = \begin{bmatrix} \frac{\alpha_1^{\mu}}{\alpha_1 - w_1} & \frac{\alpha_2^{\mu}}{\alpha_2 - w_1} & \cdots & \frac{\alpha_n^{\mu}}{\alpha_n - w_1} \\ \frac{\alpha_1^{\mu}}{\alpha_1 - w_2} & \frac{\alpha_2^{\mu}}{\alpha_2 - w_2} & \cdots & \frac{\alpha_n^{\mu}}{\alpha_n - w_2} \\ \vdots & \vdots & & \vdots \\ \frac{\alpha_1^{\mu}}{\alpha_1 - w_s} & \frac{\alpha_2^{\mu}}{\alpha_2 - w_s} & \cdots & \frac{\alpha_n^{\mu}}{\alpha_n - w_s} \end{bmatrix} . \tag{8}$$

By substituting $g_{(\ell-1)t+k}(x) = \dfrac{\prod_{j=1}^{s}(x-w_j)^t}{(x-w_\ell)^k}$ and

$y_i = \dfrac{Z_k}{\prod_{j=1}^{s}(\alpha_i-w_j)^t}$ for $\ell = 1,2,\ldots,s$, $k = 1,2,\ldots,t$ and

$i = 1,2,\ldots,n$ in the parity check matrix (1), one obtains a parity check matrix identical to the one on the previous page (8). This shows that the generalized Sristava codes are indeed, subclasses of the alternant codes characterized by these st polynomials $g_i(x)$ over $GF(q^m)$ $i = 1,2,\ldots,st$.

d) Goppa codes

This is an interesting subclass of alternant codes, which is specified by a Goppa polynomial $G(x)$ with coefficients from $GF(q^m)$ and a subset $L = \{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of $GF(q^m)$ such that all $\alpha_i$ in L are not zeroes of $G(x)$.

The Goppa code consists of all codewords $(a_1,a_2,\ldots,a_n)$ over $GF(q)$ such that

$$\sum_{i=1}^{w} \frac{a_i}{x - \alpha_i} \equiv 0 \mod G(x) \qquad (9)$$

and has the following parameters:

| | |
|---|---|
| Block length: | $n = \lvert L\rvert \leq q^m - 1$ |
| Number of information symbols: | $k \geq n - mt$, $t = \deg G(x)$ |
| Minimum distance: | $d \geq t + 1$ |

The parity check matrix, derived from the above relation (9) is defined as follows:

$$H_{Goppa} = \begin{bmatrix} g_t G(\alpha_1)^{-1} & \cdots & g_t G(\alpha_n)^{-1} \\ (g_{t-1}+\alpha_1 g_t)G(\alpha_1)^{-1} & \cdots & (g_{t-1}+\alpha_n g_t)G(\alpha_n)^{-1} \\ \vdots & & \vdots \\ (g_1+\alpha_1 g_2+\ldots+\alpha_1^{t-1} g_t)G(\alpha_1)^{-1} & \cdots & (g_1+\alpha_n g_2+\ldots+\alpha_n^{t-1} g_t)G(\alpha_n)^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} g_t & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ g_{t-1} & g_t & \cdots & 0 & \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ g_1 & g_2 & \cdots & g_t & \alpha_1^{t-1} & \alpha_2^{t-1} & \cdots & \alpha_n^{t-1} \end{bmatrix} \times$$

$$\begin{bmatrix} G(\alpha_1)^{-1} & 0 & \cdots & 0 \\ 0 & G(\alpha_2)^{-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & G(\alpha_n)^{-1} \end{bmatrix} \qquad (10)$$

As is shown in the Appendix, a much simpler parity check matrix which defines an identical code is

$$H'_{Goppa} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \cdots & \alpha_n^{t-1} \end{bmatrix} \times$$

$$\begin{bmatrix} G(\alpha_1)^{-1} & 0 & \cdots & 0 \\ 0 & G(\alpha_2)^{-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & G(\alpha_n)^{-1} \end{bmatrix} \qquad (11)$$

since the matrix

$$\begin{bmatrix} g_t & 0 & \cdots & 0 \\ g_{t-1} & g_t & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ g_1 & g_2 & \cdots & g_t \end{bmatrix}$$

is nonsingular.

By comparing with the parity check matrix (3), this is obviously an alternant code of length n with $x_i = \alpha_i$ and $y_i = G(\alpha_i)^{-1}$, $i = 1,2,3,\ldots,n$.

3. Relationship between subclasses of alternant codes

Some of the very interesting classes of code, namely the generalized BCH codes, Goppa codes and generalized Srivastava codes, have been reviewed and briefly discussed in the preceding section, but in addition to being subclasses of the alternant codes, these error-correcting codes do exhibit certain connections between each other.

In this section, we consider primarily codes which are included in several classes of codes.

a) Generalized BCH codes and Goppa codes

Recall the parity check matrix of Goppa code defined in (11). Let $\alpha_i = \alpha^{-(i-1)}$ with $\alpha$ being a nonzero element of $GF(q^m)$ of order n, for $i = 1,2,3,\ldots,n$ and the Goppa polynomial $G(x) = x^t$. Substitution in (11) yields:

$$H_{Goppa} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(t-1)} & \cdots & \alpha^{-(n-1)(t-1)} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \alpha^{t} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \alpha^{(n-1)t} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^{t} & \cdots & \alpha^{(n-1)t} \\ 1 & \alpha^{t-1} & \cdots & \alpha^{(n-1)(t-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha & \cdots & \alpha^{n-1} \end{bmatrix}$$

after reordering of the matrix rows:

$$= \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{1} & \cdots & \alpha^{(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{(t-1)} & \cdots & \alpha^{(t-1)(n-1)} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \alpha & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \alpha^{n-1} \end{bmatrix}$$

A quick glance at the parity check matrix (4) reveals that this is a BCH code corresponding to the case b = 1. Hence, the narrow-sense BCH codes are contained in both the classes of generalized BCH codes and Goppa codes.

Another class of codes is found to be included in both generalized BCH codes and Goppa codes. Consider the parity check matrix of the generalized BCH codes of form (5).

Substituting $p_i = n^{-1} P(\alpha^{-i})$ and $g_i = n^{-1} G(\alpha^{-i})$ into (5) yields:

$$H_{GBCH} = \begin{bmatrix} 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-t} & \cdots & \alpha^{-t(n-1)} \end{bmatrix} \quad x$$

$$\begin{bmatrix} P(1)G^{-1}(1) & 0 & \cdots & \\ 0 & P(\alpha^{-1})G^{-1}(\alpha^{-1}) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & P(\alpha^{-(n-1)})G^{-1}(\alpha^{-(n-1)}) \end{bmatrix}$$

$$= \begin{bmatrix} P(1) & \alpha^{-1}P(\alpha^{-1}) & \cdots & \alpha^{-(n-1)}P(\alpha^{-(n-1)}) \\ P(1) & \alpha^{-2}P(\alpha^{-1}) & \cdots & \alpha^{-2(n-1)}P(\alpha^{-(n-1)}) \\ \vdots & \vdots & & \vdots \\ P(1) & \alpha^{-t}P(\alpha^{-1}) & \cdots & \alpha^{-t(n-1)}P(\alpha^{-(n-1)}) \end{bmatrix} \quad x$$

Substituting $p_i = n^{-1} P(\alpha^{-i})$ and $g_i = n^{-1} G(\alpha^{-i})$ into (5) yields:

$$H_{GBCH} = \begin{bmatrix} 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-t} & \cdots & \alpha^{-t(n-1)} \end{bmatrix} \quad x$$

$$\begin{bmatrix} P(1)G^{-1}(1) & 0 & \cdots & \\ 0 & P(\alpha^{-1})G^{-1}(\alpha^{-1}) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & P(\alpha^{-(n-1)})G^{-1}(\alpha^{-(n-1)}) \end{bmatrix}$$

$$= \begin{bmatrix} P(1) & \alpha^{-1}P(\alpha^{-1}) & \cdots & \alpha^{-(n-1)}P(\alpha^{-(n-1)}) \\ P(1) & \alpha^{-2}P(\alpha^{-1}) & \cdots & \alpha^{-2(n-1)}P(\alpha^{-(n-1)}) \\ \vdots & \vdots & & \vdots \\ P(1) & \alpha^{-t}P(\alpha^{-1}) & \cdots & \alpha^{-t(n-1)}P(\alpha^{-(n-1)}) \end{bmatrix} \quad x$$

$$\begin{bmatrix} G^{-1}(1) & 0 & \cdots & 0 \\ 0 & G^{-1}(\alpha^{-1}) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & G^{-1}(\alpha^{-(n-1)}) \end{bmatrix}$$

Let $P(x) = x^{n-1}$, then $P(\alpha^{-i}) = \alpha^{i}$, $i = 0,1,2,\ldots,n-1$.

$$H_{GB} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(t-1)} & \cdots & \alpha^{-(t-1)(n-1)} \end{bmatrix} \times$$

$$\begin{bmatrix} G^{-1}(1) & 0 & \cdots & 0 \\ 0 & G^{-1}(\alpha^{-1}) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & G^{-1}(\alpha^{-(n-1)}) \end{bmatrix}$$

A comparison with the parity check matrix in (11) shows that this is the special case of Goppa codes with $\alpha_i = \alpha^{-(i-1)}$, for $i = 1,2,3,\ldots,n$ , $\alpha$ being an element in $GF(q^m)$ of order n, and the Goppa polynomial G(x).

b) Goppa codes and generalized Srivastava codes

Recall that the original Srivastava codes are the special case of the class of generalized Srivastava codes with $z_i = \alpha_i^{\mu}$ and $t = 1$, $\mu$ being an arbitrary integer and defined by the parity check matrix (8). It is interesting to note that a particular subclass of the above code, namely the one characterized by $\mu = 1$, is contained in the class of Goppa codes. In fact, after substitution $\mu = 1$ into (8):

$$H_{SR}(\mu=1) = \begin{bmatrix} \frac{\alpha_1}{\alpha_1 - w_1} & \frac{\alpha_2}{\alpha_2 - w_1} & \cdots & \frac{\alpha_n}{\alpha_n - w_1} \\ \frac{\alpha_1}{\alpha_1 - w_2} & \frac{\alpha_2}{\alpha_2 - w_2} & \cdots & \frac{\alpha_n}{\alpha_n - w_2} \\ \vdots & \vdots & & \vdots \\ \frac{\alpha_1}{\alpha_1 - w_s} & \frac{\alpha_2}{\alpha_2 - w_s} & \cdots & \frac{\alpha_n}{\alpha_n - w_s} \end{bmatrix}$$

Since the row space of the parity check matrix is invariant by multiplication of any row of the matrix by a nonzero element of $GF(q^m)$, multiplying every $i^{th}$ row of the above $H_{SR}(\mu=1)$ by $w_i$. $w_i$, $i = 1,2,3,\ldots s$ being distinct and nonzero elements of $GF(q^m)$, gives:

$$\begin{bmatrix} \frac{\alpha_1 w_1}{\alpha_1 - w_1} & \frac{\alpha_2 w_1}{\alpha_2 - w_1} & \cdots & \frac{\alpha_n w_1}{\alpha_n - w_1} \\ \frac{\alpha_1 w_2}{\alpha_1 - w_2} & \frac{\alpha_2 w_2}{\alpha_2 - w_2} & \cdots & \frac{\alpha_n w_2}{\alpha_n - w_2} \\ \vdots & \vdots & & \vdots \\ \frac{\alpha_1 w_s}{\alpha_1 - w_s} & \frac{\alpha_2 w_s}{\alpha_2 - w_s} & \cdots & \frac{\alpha_n w_s}{\alpha_n - w_s} \end{bmatrix}$$

or, since $\alpha_i w_j \neq 0$ for $i = 1,2,3,\ldots,n$ , $j = 1,2,3,\ldots,s$.

$$\begin{bmatrix} \frac{1}{w_1^{-1} - \alpha_1^{-1}} & \frac{1}{w_1^{-1} - \alpha_2^{-1}} & \cdots & \frac{1}{w_1^{-1} - \alpha_n^{-1}} \\ \frac{1}{w_2^{-1} - \alpha_1^{-1}} & \frac{1}{w_2^{-1} - \alpha_2^{-1}} & \cdots & \frac{1}{w_2^{-1} - \alpha_n^{-1}} \\ \vdots & \vdots & & \vdots \\ \frac{1}{w_s^{-1} - \alpha_1^{-1}} & \frac{1}{w_s^{-1} - \alpha_2^{-1}} & \cdots & \frac{1}{w_s^{-1} - \alpha_n^{-1}} \end{bmatrix}$$

which is the alternate form of the parity check matrix of the Goppa code specified by the subset $L = \{\alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_n^{-1}\}$ in $GF(q^m)$ and the Goppa polynomial $G(x) = \prod_{i=1}^{s} (x - w_i^{-1})$ (see Appendix on the Tzeng and Zimmerman derivation). Adopting the same terminology as when we discussed the relationship between GBCH and

Goppa codes, we would say that the narrow-sense Srivastava codes are contained in both Goppa and generalized Srivastava codes.

c) Generalized BCH and Srivastava codes

A much larger class is found to be included in both the generalized BCH and Srivastava codes. Consider the parity check matrix of the generalized BCH codes in (5) and let $\{z_1, z_2, \ldots, z_n\}$ be nonzero elements of $GF(q^m)$ and all distincts from the $\alpha^i$, $i = 0,1,2,\ldots,n-1$ and the associated polynomials $P(x)$ and $G(x)$ be

$$P(x) = \sum_{j=0}^{n-1} \frac{\alpha^{+j} z_{j+1} \prod_{\substack{i=0 \\ i\neq j}}^{n-1} (x-\alpha^i)}{\prod_{\substack{i=0 \\ i\neq j}}^{n-1} (\alpha^j - \alpha^i)}$$

and

$G(x) = \prod_{i=1}^{s} (x-w_i)^t$, $w_1, w_2, \ldots, w_s$ being distinct elements from the $\alpha_i$, $i = 0,1,\ldots,n-1$. Since $P(\alpha^i) = \alpha^{-i} z_{i+1} \neq 0$ for $i = 0,1,2,\ldots,n-1$, it is obvious that $P(x)$, thus defined, is relatively prime to $x^n - 1$, hence satisfying the restriction on $P(x)$. Similarly, $G(\alpha^k) = \prod_{i=1}^{s} (\alpha^k - w_i)^t \neq 0$, $G(x)$ is also relatively prime to $x^n - 1$.

Substitution of $P(\alpha^i) = \alpha^{-i} z_i$ and $G(\alpha^i) = \prod_{j=1}^{s} (\alpha^i - w_j)^t$ in the parity check matrix (5) yields:

$$\begin{bmatrix} 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-st} & \cdots & \alpha^{-st(n-1)} \end{bmatrix} \quad x$$

$$\begin{bmatrix} z_1 G^{-1}(1) & 0 & \cdots & 0 \\ 0 & z_2 G^{-1}(\alpha^{-1}) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \alpha^{(n-1)} z_n G^{-1}(\alpha^{-(n-1)}) \end{bmatrix}$$

or

$$\begin{bmatrix} G^{-1}(1) & G^{-1}(\alpha^{-1}) & \cdots & G(\alpha^{-(n-1)}) \\ G^{-1}(1) & G^{-1}(\alpha^{-1})\alpha^{-1} & \cdots & G(\alpha^{-(n-1)})\alpha^{-(n-1)} \\ \vdots & \vdots & & \vdots \\ G^{-1}(1) & G^{-1}(\alpha^{-1})\alpha^{-(st-1)} & \cdots & G(\alpha^{-(n-1)})\alpha^{-(n-1)(st-1)} \end{bmatrix} \quad x$$

$$\begin{bmatrix} z_1 & 0 & \cdots & 0 \\ 0 & z_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & z_n \end{bmatrix}$$

$= AZ.$

As was shown by Tzeng and Zimmerman (see Appendix) the matrix A is row equivalent to

$$\begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ \vdots \\ A_s \end{bmatrix}$$

where

$$A_\ell = \begin{bmatrix} \frac{1}{(1 - w_\ell)} & \frac{1}{(\alpha^{-1} - w_\ell)} & \cdots & \frac{1}{(\alpha^{-(n-1)} - w_\ell)} \\ \frac{1}{(1 - w_\ell)^2} & \frac{1}{(\alpha^{-1} - w_\ell)^2} & \cdots & \frac{1}{(\alpha^{-(n-1)} - w_\ell)^2} \\ \vdots & \vdots & & \vdots \\ \frac{1}{(1 - w_\ell)^t} & \frac{1}{(\alpha^{-1} - w_\ell)^t} & \cdots & \frac{1}{(\alpha^{-(n-1)} - w_\ell)^t} \end{bmatrix}$$

for $\ell = 1,2,3,\ldots,s$ , which, multiplied by z, gives:

$$\begin{bmatrix} H_1 \\ H_2 \\ H_3 \\ \vdots \\ H_s \end{bmatrix}$$

where

$$H_\ell = \begin{bmatrix} \frac{z_1}{(1 - w_\ell)} & \frac{z_2}{(\alpha^{-1} - w_\ell)} & \cdots & \frac{z_n}{(\alpha^{-(n-1)} - w_\ell)} \\ \frac{z_1}{(1 - w_\ell)^2} & \frac{z_2}{(\alpha^{-1} - w_\ell)^2} & \cdots & \frac{z_n}{(\alpha^{-(n-1)} - w_\ell)} \\ \vdots & \vdots & & \vdots \\ \frac{z_1}{(1 - w_\ell)^t} & \frac{z_2}{(\alpha^{-1} - w_\ell)^t} & \cdots & \frac{z_n}{(\alpha^{-(n-1)} - w_\ell)^t} \end{bmatrix}$$

Obviously, in comparing with the parity check matrix in (7), it can be seen that the above matrix defines a special class of generalized Srivastava codes specified by:

$z_1, z_2, \ldots, z_n$

$1, \alpha^{-1}, \alpha^{-2}, \ldots, \alpha^{-(n-1)}$ $\quad (\alpha_i = \alpha^{-(i-1)}, \ i = 1,2,3,\ldots,n)$

$w_1, w_2, \ldots, w_s$

where $\alpha$ is an element of $GF(q^m)$ of order n.

B. Constructing error-correcting codes by Lagrange's interpolation

In addition to defining error-correcting codes by means of the parity check matrix as we have so far presented, there are other basis of defining codes, namely the Lagrange's interpolation proposed by Tzeng and Zimmerman[3] and the generalized interpolation and transformation method introduced by Mandelbaum.[10]

The equivalence between the alternant codes and the generalized Goppa codes, which are the generalization of Goppa codes based on the Lagrange's interpolation is established by Tzeng and Zimmerman[3]; the purpose of the following section is to present a description of the Lagrange's interpolation formula, a proof of how the Mattson - Solomon can be derived as a special case as well as a brief summary of the relationship of generalized Goppa codes with other codes.

1) Generalized Goppa codes:

Let $(a_1, a_2, a_3, \ldots, a_n)$ be an n-tuple with $a_i$ in $GF(q)$, $i = 1,2,3,\ldots,n$ , q being a power of a prime, and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subset of $GF(q^m)$. Then the Lagrange's interpolation formula

associated with $(a_1,a_2,\ldots,a_n)$ is defined as follows:

$$B(x) = \sum_{i=1}^{n} a_i \left( \prod_{\substack{j=1 \\ j\neq i}}^{n} (x-\alpha_j) \Big/ \prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha_i-\alpha_j) \right) \qquad (12)$$

This is a polynomial of degree less than or equal to n-1 over $GF(q^m)$ such that $B(\alpha_i) = a_i$ for $i = 1,2,\ldots,n$. Let $L(x) = \prod_{i=1}^{n} (x-\alpha_i)$ and $L_i(x) = \prod_{\substack{j=1 \\ j\neq i}}^{n} (x-\alpha_i) = \frac{L(x)}{x-\alpha_i}$, then

$$B(x) = \sum_{i=1}^{n} a_i \frac{L_i(x)}{L_i(\alpha_i)}$$

It is rather easy to show that the Lagrange's interpolation formula, thus defined, (12) or (13), is the generalization of the Mattson - Solomon transform.

Recall that the Mattson - Solomon polynomial of the polynomial $a(x) = \sum_{i=1}^{n} a_i x^{i-1}$ with coefficients $a_i$ in $GF(q^m)$, or of the n-tuple $(a_1,a_2,\ldots,a_n)$ is:

$$A(x) = \sum_{j=0}^{n-1} A_j x^j$$

where $A_j = a(\alpha^j)$, $\alpha$ being a primitive $n^{th}$ root of unity in $GF(q^m)$.

Thus:

$$A(x) = \sum_{j=0}^{n-1} \sum_{k=1}^{n} a_k \alpha^{j(k-1)} x^j$$

$$= \sum_{k=1}^{n} a_k \sum_{j=0}^{n-1} \alpha^{j(k-1)} x^j$$

$$= \sum_{k=1}^{n} a_k \sum_{j=0}^{n-1} (\alpha^{k-1} x)^j$$

$$= \sum_{k=1}^{n} a_k \frac{(\alpha^{k-1}x)^n - 1}{\alpha^{k-1}x - 1} = \sum_{k=0}^{n-1} a_{k+1} \frac{(\alpha^k x)^n - 1}{\alpha^k x - 1}$$

Let $\alpha^{-i}$ be the $n^{th}$ root of unity for $i = 0,1,2,\ldots,n-1$, then

$$\frac{(\alpha^k x)^n - 1}{\alpha^k x - 1} = \frac{(\alpha^k x - 1)(\alpha^k x - \alpha^{-1}) \ldots (\alpha^k x - \alpha^{-(n-1)})}{\alpha^k x - 1}$$

$$= \alpha^{k(n-1)} \prod_{i=1}^{n-1} (x - \alpha^{-(i+k)})$$

or, changing the index:

$$= \frac{\prod_{\substack{i=0 \\ i \neq k}}^{n-1} (x - \alpha^{-i})}{\alpha^{-k(n-1)}} \qquad (14)$$

Since $\frac{d}{dx}(x^n - 1) = nx^{n-1}$

$$= \frac{d}{dx}[(x-1)(x-\alpha^{-1})\ldots(x-\alpha^{-(n-1)})]$$

$$= \sum_{k=0}^{n-1} \prod_{\substack{i=0 \\ i\neq k}}^{n-1} (x-\alpha^{-i})$$

it follows that letting $x = \alpha^{-k}$ gives:

$$n\alpha^{-k(n-1)} = \prod_{\substack{i=0 \\ i\neq k}}^{n-1} (\alpha^{-k}-\alpha^{-i})$$

or $$\alpha^{-k(n-1)} = \frac{1}{n} \prod_{\substack{i=0 \\ i\neq k}}^{n-1} (\alpha^{-k}-\alpha^{-i})$$

Substitution into (14) yields:

$$\frac{(\alpha^k x)^n - 1}{\alpha^k x - 1} = n \frac{\prod_{\substack{i=0 \\ i\neq k}}^{n-1} (x-\alpha^{-i})}{\prod_{\substack{i=0 \\ i\neq k}}^{n-1} (\alpha^{-k}-\alpha^{-i})}$$

Hence:

$$\sum_{k=0}^{n-1} a_{k+1} \frac{(\alpha^k x)^n - 1}{\alpha^k x - 1} = n \sum_{k=0}^{n-1} a_{k+1} \frac{\prod_{\substack{i=0 \\ i\neq k}}^{n-1} (x-\alpha^{-i})}{\prod_{\substack{i=0 \\ i\neq k}}^{n-1} (\alpha^{-k}-\alpha^{-i})}$$

and after replacing k + 1 by i and i + 1 by j

$$= n \sum_{i=1}^{n} a_i \frac{\prod_{\substack{j=1 \\ j\neq i}}^{n} (x-\alpha^{-(j-1)})}{\prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha^{-(i-1)}-\alpha^{-(j-1)})}$$

Let $\alpha^{-(k-1)} = \alpha_k$ for k = 1,2,3,...,n , one gets:

$$A(x) = n \sum_{i=1}^{n} a_i \frac{\prod_{\substack{j=1 \\ j\neq i}}^{n} (x-\alpha_j)}{\prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha_i-\alpha_j)}$$

and from (12) = B(x). This shows that the Mattson - Solomon polynomial is a special case of the Lagrange's interpolation by restricting $\alpha_i = \alpha^{-(i-1)}$, for i = 1,2,3,...,n, where $\alpha$ is the primitive $n^{th}$ root of unity.

Let P(x), G(x) be polynomials over GF($q^m$) of degree less than or equal to n - 1 and relatively prime to L(x). The generalized Goppa codes are defined as the set of $(a_1,a_2,...,a_n)$ over GF(q) such that

$$[B(x)P(x)]_{L(x)} \equiv 0 \bmod G(x) \qquad (14)$$

where $B(x)$ is the Lagrange's interpolation formula of the n-tuple $(a_1,a_2,\ldots,a_n)$ and

$$B(x)P(x) \equiv [B(x)P(x)]_{L(x)} \bmod L(x)$$

Let $(p_1,p_2,\ldots,p_n)$ and $(g_1,g_2,\ldots,g_n)$ be the n-tuple obtained by the inverse Lagrange's interpolation formula of $P(x)$ and $G(x)$ respectively, the generalized Goppa code described by (14) is specified by the parity check matrix.

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \cdots & \alpha_n^{n-1} \end{bmatrix} \begin{bmatrix} \frac{p_1 g_1^{-1}}{L'(\alpha_1)} & 0 & \cdots & 0 \\ 0 & \frac{p_2 g_2^{-1}}{L'(\alpha_2)} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{p_n g_n^{-1}}{L'(\alpha_n)} \end{bmatrix} \tag{15}$$

where deg $G(x) = t$. Comparing with (3), it can be seen that the equivalence between the generalized Goppa codes and alternant codes is easily established by letting $x_i = \alpha_i$ and

$$y_i = \frac{p_i g_i^{-1}}{L'(\alpha_i)} \quad \text{for } i = 1,2,3,\ldots,n \tag{16}$$

Applying the Lagrange's interpolation on both sides of (16) yields:

$$Y(x) = \frac{P(x)G^{-1}(x)}{L'(x)} \qquad (17)$$

Y(x) being the Lagrange's polynomial associated to the n-tuple $(y_1, y_2, \ldots, y_n)$. Relation (17) can be rewritten as:

$$P(x) = Y(x)L'(x)G(x) \mod L(x) \qquad (18)$$

Given the alternant codes as specified by the parity check matrix (3), one can construct the equivalent generalized Goppa codes as follows:

i) Select the subset $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ as defined by (3).

ii) Then select a polynomial G(x) of degree t with coefficients in $GF(q^m)$ which is relatively prime to $L(x) = \prod_{i=1}^{n} (x-\alpha_i)$. An easier way to define G(x) is:

$$G(x) = \prod_{i=1}^{t} (x-\beta_i)$$

with $\beta_i \in GF(q^m) - \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$

iii) Compute P(x) as

$$P(x) = Y(x)L'(x)G(x) \text{ modulo } L(x)$$

where

$$Y(x) = \sum_{i=1}^{n} y_i \frac{\prod_{\substack{k=1 \\ k\neq i}}^{n} (x-\alpha_k)}{\prod_{\substack{k=1 \\ k\neq i}}^{n} (\alpha_i-\alpha_k)}$$

Since $L'(x)$ is relatively prime to $L(x)$ and $Y(x_i) = y_i \neq o$ for $1 = 1,2,3,\ldots,n$, hence $Y(x)$ is also relatively prime to $L(x)$, $P(x) = Y(x)L'(x)G(x)$ is relatively prime to $L(x)$ as required.

Thus the equivalence between both codes is completely established.

2. Subcodes of the generalized Goppa codes

a) Goppa codes

Let $P(x) = L'(x)$ , then

$$\frac{p_i g_i^{-1}}{L'(\alpha_i)} = \frac{P(\alpha_i)G^{-1}(\alpha_i)}{L'(\alpha_i)} = G^{-1}(\alpha_i)$$

and the parity check matrix (15) becomes:

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \ldots & \alpha_n^{t-1} \end{bmatrix} \begin{bmatrix} G^{-1}(\alpha_1) & 0 & \ldots & 0 \\ 0 & G^{-i}(\alpha_2) & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & G^{-1}(\alpha_n) \end{bmatrix}$$

This is the Goppa codes specified by the subset $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $GF(q^m)$ and the Goppa polynomial $g(x) = G(x)$ over $GF(q^m)$ of degree t. The relation defined in (14) thus becomes:

$$[B(x)L'(x)]_{L(x)} \equiv 0 \mod G(x)$$

b) Generalized BCH codes

If one restricts the $\alpha_i$ to be $\alpha^{-(i-1)}$, with $\alpha$ being a primitive $n^{th}$ root of unity, then the Lagrange's polynomial becomes the Mattson - Solomon polynomial and $L'(\alpha_i) = n\alpha_i^{n-1} = n\alpha^{+(i-1)}$. The parity check matrix in (15) thus becomes:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(t-1)} & \cdots & \alpha^{-(t-1)(n-1)} \end{bmatrix} \times$$

$$\begin{bmatrix} \frac{p_1 g_1^{-1}}{n} & & \cdots & 0 \\ 0 & \frac{p_2 g_2^{-1}}{n\alpha^{+1}} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{p_n g_n^{-1}}{n\alpha^{+(n-1)}} \end{bmatrix}$$

or

$$n \times \begin{bmatrix} 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-t} & \cdots & \alpha^{-t(n-1)} \end{bmatrix} x \begin{bmatrix} p_1 g_1^{-1} & 0 & \cdots & 0 \\ 0 & p_2 g_2^{-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & p_n g_n^{-1} \end{bmatrix} \qquad (19)$$

where $p_i, g_i$ $i = 1,2,\ldots,n$ are coefficients of the polynomials $\sum_{j=0}^{n-1} p_{j+1} x^j$, $\sum_{j=0}^{n-1} g_{j+1} x^j$ associated with the Mattson - Solomon polynomials $P(x)$ and $G(x)$ respectively.

After multiplying the parity check matrix in (19) by $n^{-1}$, which leaves its row space invariant, it is easily seen that the above matrix defines the generalized BCH codes specified by the subset $\{1,\alpha^{-1},\alpha^{-2},\ldots,\alpha^{-(n-1)}\}$ in $GF(q^m)$ and the pair $(P(x),G(x))$ both being polynomials over $GF(q^m)$ and deg $P(x) \leq n - 1$ deg $g(x)=t$.

Since the BCH codes are contained in the generalized BCH codes, it is obvious that they are also subcodes of the generalized Goppa codes.

C. Method of generalized interpolation and transformation proposed by Mandelbaum

Another approach, which was introduced by Mandelbaum recently[10], in defining error-correcting codes is based on Chebyshev system which is essentially a set of selected polynomials over $GF(q^m)$ called the generating polynomials of the codes.

In a sense, codes generated by this method can be regarded as a generalized version of polynomial codes proposed by Goethals.[9]

1. Polynomial codes

Let $\alpha_1,\alpha_2,\alpha_3,\ldots,\alpha_n$ be n distinct elements of $GF(q^m)$ and $L(x) = \prod_{i=1}^{n} (x-\alpha_i)$. Let $F(x)$ be a polynomial with coefficients in $GF(q^m)$ and denote $\overline{F}(x)$, the reduced form of $F(x)$ modulo $L(x)$. Then, from the Chinese Remainder Theorem,

$$\overline{F}(x) = \sum_{i=1}^{n} F(\alpha_i)\, L_i(x)/L_i(\alpha_i) \qquad (20)$$

where

$$L_i(x) = \frac{L(x)}{(x-\alpha_i)}, \quad i = 1,2,3,\ldots,n$$

(Notice this is the Lagrange's polynomial associated with the n-tuple $(F(\alpha_1),F(\alpha_2),\ldots,F(\alpha_n))$. Hence, the set of n polynomials $\{n_i(x) = \frac{L_i(x)}{L_i(\alpha_i)}, i = 1,2,3,\ldots,n\}$ form a basis of the polynomial

algebra $GF(q^m)[x]/L(x)$, where $GF(q^m)[x]$ is the set of polynomials with coefficients in $GF(q^m)$, on the other hand, any polynomial $F(x)$ is uniquely expressed in $GF(q^m)[x]/L(x)$ as a polynomial of degree less than n:

$$\bar{F}(x) = \sum_{i=0}^{n-1} c_i x^i \tag{21}$$

Thus, equating (20) and (21):

$$\sum_{i=1}^{n} F(\alpha_i) n_i(x) = \sum_{i=0}^{n-1} c_i x^i \tag{22}$$

The relation (22) describes the transformation between two basis, namely the basis $\{n_i(x),\ i = 1,2,\ldots,n\}$ and the one $\{x^i,\ i = 0,1,2,\ldots,n-1\}$; in other words, relatively to the basis $\{n_i(x),\ i = 1,2,\ldots,n\}$ $\bar{F}(x)$ has as coordinates with respect to the basis $\{x^i,\ i = 0,1,2,\ldots,n-1\}$ take the values $c_i$, $i = 0,1,2,\ldots,n$. Let $I = \{i_1,i_2,\ldots,i_k\}$ be a subset of the set of integers $\{0,1,2,\ldots,n-1\}$ and $\{F(x)\}$ be polynomials with coefficients in $GF(q^m)$ such as:

$$F(x) = \sum_{i\in I} c_i x^i$$

The polynomial codes specified by the subsets $L = \{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ and $I = \{i_1,i_2,\ldots,i_k\}$ consist of codewords $(F(\alpha_1),F(\alpha_2),\ldots,F(\alpha_n))$

with $F(\alpha_i)$ being element of $GF(q^m)$, $i = 1,2,\ldots,n$. Goethals called these codes the images of subspaces of $GF(q^m)[x]/L(x)$ with respect to the Lagrangian basis $\{n_i(x), i = 1,2,\ldots,n\}$. Since $F(\alpha_k) = \sum_{i \in I} c_1 \alpha_k^i$, $k = 1,2,\ldots,n$, it can be seen that:

$$(F(\alpha_1),F(\alpha_2),\ldots,F(\alpha_n)) =$$

$$(c_{i_1},c_{i_2},c_{i_3},\ldots,c_{i_k}) \begin{bmatrix} \alpha_1^{i_1} & \alpha_2^{i_1} & \ldots & \alpha_n^{i_1} \\ \alpha_1^{i_2} & \alpha_2^{i_2} & \ldots & \alpha_n^{i_2} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{i_k} & \alpha_2^{i_k} & \ldots & \alpha_n^{i_k} \end{bmatrix} \qquad (23)$$

$$= c \times G$$

If one considers the coefficients $c_{i_j}$, $j = 1,2,3,\ldots,k$ as the k information symbols, then the polynomial code has the following parameters:

| | |
|---|---|
| Block length: | $n \leq q^m - 1$ |
| Number of parity check symbols: | $n - k$ |
| Minimum distance: | $d \geq k + 1$ |

having as generator matrix, the matrix G.

2. Mandelbaum's codes

Let's generalize each of the $x^{i_j}$ into $g_j(x)$ $i = 1,2,3,\ldots,k$ with $g_j(x)$ being polynomial over $GF(q^m)$. An additional requirement is that these $g_j(x)$ are independent functions and that no non-tivial function $\phi(x) = \sum_{i=1}^{k} c_i g_i(x)$, e.g. not all the $c_i$'s are zeroes, has more than $k - 1$ different roots in $GF(q^m)$. Hence, from (23):

$$(F(\alpha_1),F(\alpha_2),\ldots,F(\alpha_n)) =$$

$$(c_1,c_2,\ldots,c_k) \begin{bmatrix} g_1(\alpha_1) & g_1(\alpha_2) & \ldots & g_1(\alpha_n) \\ g_2(\alpha_1) & g_2(\alpha_2) & \ldots & g_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ g_k(\alpha_1) & g_k(\alpha_2) & \ldots & g_k(\alpha_n) \end{bmatrix} \qquad (24)$$

The codes, as defined in (24) by Mandelbaum,[10] are characterized by the following parameters:

| | |
|---|---|
| Block length: | $n \leq q^m - 1$ |
| Number of parity check symbols: | $n - k$ |
| Minimum distance: | $d \geq k + 1$ |

as in case of polynomial codes. In a sense, polynomial codes are said to be special cases of Mandelbaum's codes (24). Mandelbaum called the set of the above k functions, as defined previously,

a c-system (Chebyshev system). If one allows the original c-system $\{g_1(x),g_2(x),\ldots,g_k(x)\}$ to be lengthened to a larger c-system $\{g_1(x),g_2(x),\ldots,g_k(x),g_{k+1}(x),\ldots,g_n(x)\}$, then the relation (24) can be rewritten as:

$$\begin{aligned}
c_1g_1(\alpha_1) + c_2g_2(\alpha_1) + \ldots + c_ng_n(\alpha_1) - F(\alpha_1) &= 0 \\
c_1g_1(\alpha_2) + c_2g_2(\alpha_2) + \ldots + c_ng_n(\alpha_2) - F(\alpha_2) &= 0 \\
&\qquad (25) \\
c_1g_1(\alpha_n) + c_2g_2(\alpha_n) + \ldots + c_ng_n(\alpha_n) - F(\alpha_n) &= 0 \\
c_1g_1(x) + c_2g_2(x) + \ldots + c_ng_n(x) - F(x) &= 0
\end{aligned}$$

This is the set of n + 1 homogeneous equations having nontrivial solution $(c_1,c_2,c_3,\ldots,c_n,-1)$. The determinant must then vanish.

$$\begin{vmatrix}
g_1(\alpha_1) & g_2(\alpha_1) & \ldots & g_n(\alpha_1) & F(\alpha_1) \\
g_1(\alpha_2) & g_2(\alpha_2) & \ldots & g_n(\alpha_2) & F(\alpha_2) \\
\vdots & \vdots & & \vdots & \vdots \\
g_1(\alpha_n) & g_2(\alpha_n) & \ldots & g_n(\alpha_n) & F(\alpha_n) \\
g_1(x) & g_2(x) & \ldots & g_n(x) & F(x)
\end{vmatrix} = 0$$

Expanding on the last row gives:

$$DF(x) =$$

$$- \begin{vmatrix} g_1(\alpha_1) & g_2(\alpha_1) & \cdots & g_n(\alpha_1) & F(\alpha_1) \\ g_1(\alpha_2) & g_2(\alpha_2) & \cdots & g_n(\alpha_2) & F(\alpha_2) \\ \vdots & \vdots & & \vdots & \vdots \\ g_1(\alpha_n) & g_2(\alpha_n) & \cdots & g_n(\alpha_n) & F(\alpha_n) \\ g_1(x) & g_2(x) & \cdots & g_n(x) & 0 \end{vmatrix}$$

with

$$D = \begin{vmatrix} g_1(\alpha_1) & g_2(\alpha_1) & \cdots & g_n(\alpha_1) \\ g_1(\alpha_2) & g_2(\alpha_2) & \cdots & g_n(\alpha_2) \\ \vdots & \vdots & & \vdots \\ g_1(\alpha_n) & g_2(\alpha_n) & \cdots & g_n(\alpha_n) \end{vmatrix} \tag{26}$$

Solving for F(x) after expanding (26) on the last column:

$$F(x) = + \sum_{i=1}^{n} F(\alpha_i)\, v_i(x) \tag{27}$$

with

$$v_i(x)=(-1)^{n+i}D^{-1}\begin{vmatrix} g_1(\alpha_1) & g_2(\alpha_1) & \cdots & g_n(\alpha_1) \\ \vdots & \vdots & & \vdots \\ g_1(\alpha_{i-1}) & g_2(\alpha_{i-1}) & & g_n(\alpha_{i-1}) \\ g_1(\alpha_{i+1}) & g_2(\alpha_{i+1}) & & g_n(\alpha_{i+1}) \\ \vdots & \vdots & & \vdots \\ g_1(\alpha_n) & g_2(\alpha_n) & & g_n(\alpha_n) \\ g_1(x) & g_2(x) & \cdots & g_n(x) \end{vmatrix} \quad (28)$$

Hence, the basis of constructing error-correcting codes proposed by Mandelbaum is another form of interpolation which maps the n-tuple $(F(\alpha_1),F(\alpha_2),\ldots,F(\alpha_n))$ relative to the basis $\{v_1(x),v_2(x),\ldots,v_n(x)\}$ into the n-tuple $(c_1,c_2,\ldots,c_n)$ relative to $\{g_1(x),g_2(x),\ldots,g_n(x)\}$.

The purpose of the next section is to identify the relationship between both interpolation formulae; namely the ones proposed by Tzeng, Zimmerman and Mandelbaum (13), (28). Once the relationship is established, codes constructed on these basis will be shown to be equivalent; furthermore, since the connection between the alternant codes and the generalized Goppa codes is already identified, establishing the equivalence between Mandelbaum's codes and the alternant codes is rather straight-forward.

## III. Relationship Between Codes Based on Lagrange's Interpolation and Generalized Interpolation

### A. Generalized Srivastava codes as subcodes of generalized Goppa codes

Several important classes of codes have been identified by Tzeng and Zimmerman[3] as subcodes of generalized Goppa codes, including Goppa codes, generalized BCH codes as well as BCH codes. There is, however, an important class of codes which has not been explicitly mentioned among subcodes of generalized Goppa codes, namely the class of generalized Srivastava codes.

Recall that by letting $y_i = \frac{z_i}{\prod_{j=1}^{s} (\alpha_i - w_j)^t}$, $i = 1,2,3,\ldots,n$ (29)

and

$$g_{(\ell-1)t+k}(x) = \frac{\prod_{j=1}^{s} (x-w_j)^t}{(x-w_\ell)^k} \quad \text{for } \ell = 1,2,3,\ldots,s, \text{ and}$$

$k = 1,2,\ldots,t$ (8), it was shown that the generalized Srivastava codes are subcodes of the family of alternant codes. On the other hand, the equivalence between the alternant and generalized Goppa codes implies that the latter must also contain the generalized Srivastava codes as its subclass.

Let $G(x) = \prod_{j=1}^{s} (x-w_j)^t$ and $y(x)$ be the Lagrange's polynomial associated with the n-tuple $(y_1, y_2, \ldots, y_n)$ as specified in (29).

Let $P(x) = y(x)L'(x)G(x) \bmod L(x)$ where $L(x)$ denotes the familiar polynomial $\prod_{i=1}^{n} (x-\alpha_i)$ over $GF(q^m)$.

The generalized Goppa codes specified by $(G(x),P(x))$ and the subset $L = \{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of $GF(q^m)$ have as parity check matrix (from (15)):

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \cdots & \alpha_n^3 \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_1^{st-1} & \alpha_2^{st-1} & \alpha_3^{st-1} & \cdots & \alpha_n^{st-1} \end{bmatrix} \times \begin{bmatrix} \frac{p_1 g_1^{-1}}{L'(\alpha_1)} & 0 & \cdots & 0 \\ 0 & \frac{p_2 g_2^{-1}}{L'(\alpha_2)} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{p_n g_n^{-1}}{L'(\alpha_n)} \end{bmatrix} \qquad (30)$$

Let P(x) and G(x), as defined above, be the pair of polynomials of generalized Goppa codes. Then:

$$\frac{p_i g_i^{-1}}{L'(\alpha_i)} = \frac{p(\alpha_i)G^{-1}(\alpha_i)}{L'(\alpha_i)}$$

$$= y(\alpha_i)$$

$$= \frac{z_i}{\prod_{j=1}^{s} (\alpha_i - w_j)^t}$$

for i = 1,2,3,...,n.

Substitution into (15) yields:

$$\begin{bmatrix} \frac{1}{\prod_{j=1}^{s}(\alpha_1-w_j)^t} & \frac{1}{\prod_{j=1}^{s}(\alpha_2-w_j)^t} & \cdots & \frac{1}{\prod_{j=1}^{s}(\alpha_n-w_j)^t} \\ \frac{\alpha_1}{\prod_{j=1}^{s}(\alpha_1-w_j)^t} & \frac{\alpha_1}{\prod_{j=1}^{s}(\alpha_2-w_j)^t} & \cdots & \frac{\alpha_1}{\prod_{j=1}^{s}(\alpha_n-w_j)^t} \\ \vdots & \vdots & & \vdots \\ \frac{\alpha_1^{st-1}}{\prod_{j=1}^{s}(\alpha_1-w_j)^t} & \frac{\alpha_2^{st-1}}{\prod_{j=1}^{s}(\alpha_2-w_j)^t} & \cdots & \frac{\alpha_n^{st-1}}{\prod_{j=1}^{s}(\alpha_n-w_j)^t} \end{bmatrix} \begin{bmatrix} z_1 & 0 & \cdots & 0 \\ 0 & z_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & z_n \end{bmatrix} \quad (31)$$

$$= AZ$$

A comparison with (11) shows that the matrix A, as defined by (31), is, in fact, the parity check matrix of the Goppa code specified by the Goppa polynomial $G(x) = \prod_{j=1}^{s} (x-w_j)^t$ and the subset $L = \{\alpha_1,\alpha_2,\ldots,\alpha_n\}$. Such Goppa code is the intersection of the codes with $G_j(x) = (x-w_j)^t$ for $j = 1,2,3,\ldots,s$.

Hence, the matrix A is row equivalent to:

$$\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_s \end{bmatrix}$$

where

$$A_k = \begin{bmatrix} \frac{1}{(\alpha_1 - w_k)^t} & \frac{1}{(\alpha_2 - w_k)^t} & \cdots & \frac{1}{(\alpha_n - w_k)^t} \\ \frac{\alpha_1}{(\alpha_1 - w_k)^t} & \frac{\alpha_2}{(\alpha_2 - w_k)^t} & \cdots & \frac{\alpha_n}{(\alpha_n - w_k)^t} \\ \vdots & \vdots & & \vdots \\ \frac{\alpha_1^{t-1}}{(\alpha_1 - w_k)^t} & \frac{\alpha_2^{t-1}}{(\alpha_2 - w_k)^t} & \cdots & \frac{\alpha_n^{t-1}}{(\alpha_n - w_k)^t} \end{bmatrix}$$

for $k = 1,2,3,\ldots,s$, which in turn, is row equivalent to (see Appendix):

$$A_k' = \begin{bmatrix} \frac{1}{(\alpha_1 - w_k)} & \frac{1}{(\alpha_2 - w_k)} & \cdots & \frac{1}{(\alpha_n - w_k)} \\ \frac{1}{(\alpha_1 - w_k)^2} & \frac{1}{(\alpha_2 - w_k)^2} & \cdots & \frac{1}{(\alpha_n - w_k)^2} \\ \vdots & \vdots & & \vdots \\ \frac{1}{(\alpha_1 - w_k)^t} & \frac{1}{(\alpha_2 - w_k)^t} & \cdots & \frac{1}{(\alpha_n - w_k)^t} \end{bmatrix}$$

for k = 1,2,3,...,s. Consequently, codes defined by AZ are identical to those defined by the following parity check matrix:

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_s \end{bmatrix}$$

where

$$H_k = \begin{bmatrix} \frac{z_1}{(\alpha_1 - w_k)} & \frac{z_2}{(\alpha_2 - w_k)} & \cdots & \frac{z_n}{(\alpha_n - w_k)} \\ \frac{z_1}{(\alpha_1 - w_k)^2} & \frac{z_2}{(\alpha_2 - w_k)^2} & \cdots & \frac{z_n}{(\alpha_n - w_k)^2} \\ \vdots & \vdots & & \vdots \\ \frac{z_1}{(\alpha_1 - w_k)^t} & \frac{z_2}{(\alpha_2 - w_k)^t} & & \frac{z_n}{(\alpha_n - w_k)^t} \end{bmatrix}$$

for $k = 1,2,3,\ldots,s$, which is dentical to (7). It shows that this is, indeed, the generalized Srivastava code specified by $\alpha_1,\alpha_2,\ldots,\alpha_n,w_1,w_2,\ldots,w_s$, all distinct elements in $GF(q^m)$ and n nonzero elements $z_1,z_2,\ldots,z_n$ of $GF(q^m)$. Hence, the code is a subclass of generalized Goppa codes.

B. Connection between generalized interpolation and Lagrange's interpolation formula

1) A special case of generalized interpolation

Recall the interpolation formula introduced by Mandelbaum in (27)

$$F(x) = \sum_{i=1}^{n} F(\alpha_i)v_i(x)$$

where

$$F(x) = \sum_{i=1}^{n} c_i g_i(x)$$

A special case of generalized interpolation, namely that all the functions $g_1(x),g_2(x),\ldots,g_n(x)$ are restricted to be polynomials of degree n - 1 or less over $GF(q^m)$ will be considered in this section.

Let each $g_i(x) = \sum_{k=0}^{n-1} \sigma_{ki}x^k$ where $\sigma_{ki}$ are coefficients in $GF(q^m)$ for $i = 1,2,3,\ldots,n$ and $k = 0,1,2,\ldots,n-1$. Then $v_i(x)$, as defined in (28), is reduced to:

$$v_i(x) = (-1)^{n+i} \frac{\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_{i-1} & \alpha_{i-1}^2 & \cdots & \alpha_{i-1}^{n-1} \\ 1 & \alpha_{i+1} & \alpha_{i+1}^2 & \cdots & \alpha_{i+1}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \\ 1 & x & x^2 & \cdots & x^{n-1} \end{vmatrix}}{\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix}}$$

Notice that the numerator of $v_i(x)$ is a Van der Monde determinant and vanishes whenever $x = \alpha_j$, $j = 1,2,3,\ldots,i-1,i+1,\ldots,n$, it must contain as factor the difference product:

$$\prod_{\substack{j=1 \\ j\neq i}}^{n} (x-\alpha_j)$$

On the other hand, the denominator can be obtained from the numerator after exchanging the $i^{th}$ and $n^{th}$ rows and substituting x by $\alpha_i$. Since interchanging the rows in a determinant leaves its absolute value invariant, the denominator also contains as factor the difference product.

$$\prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha_i - \alpha_j)$$

Then:

$$v_i(x) = (-1)^{n+i} \frac{\prod_{\substack{j=1 \\ j\neq i}}^{n} (x-\alpha_j)}{\prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha_i - \alpha_j)}$$

and the interpolation polynomial (27) is reduced to:

$$F(x) = \sum_{i=1}^{n} F(\alpha_i) \times \frac{\prod_{\substack{j=1 \\ j\neq i}}^{n} (x-\alpha_j)}{\prod_{\substack{j=1 \\ j\neq i}}^{n} (\alpha_i - \alpha_j)}$$

or

$$= \sum_{i=1}^{n} F(\alpha_i) \frac{L_i(x)}{L_i(\alpha_i)} \qquad (32)$$

This is the familiar formula of the Lagrange's interpolation which was presented previously. In particular, since $c_{k+1} = c_{k+2} = \ldots = c_n = 0$ and each $q_i(x)$ is a polynomial over $GF(q^m)$ of degree k - 1 or less, for i = 1,2,...,k.

$$\deg [F(x) = \sum_{i=1}^{n} F(\alpha_i) \frac{L_i(x)}{L_i(\alpha_i)} ] \leq k - 1 \qquad (33)$$

Let $L(x) = \sum_{i=0}^{n} \sigma_i x^i$ and $L_i(x) \sum_{j=0}^{n-1} i\sigma_j x^j$

Then $L_i(x) = \frac{L(x) - L(\alpha_i)}{x - \alpha_i}$

$$= \sum_{j=1}^{n} \sigma_j \left(\frac{x^j - \alpha_i^j}{x - \alpha_i}\right)$$

$$= \sum_{j=1}^{n} \sigma_j \sum_{m=0}^{j-1} \alpha_i^{j-1-m} x^m$$

$$= \sigma_1$$

$$+ \sigma_2 (\alpha_i + x)$$

$$+ \sigma_3 (\alpha_i^2 + \alpha_i x + x^2)$$

$$+ \sigma_m (\alpha_i^{m-1} + \alpha_i^{m-2} x + \alpha_i^{m-3} x^2 + \ldots + x^{m-1})$$

$$+ \sigma_n (\alpha_i^{n-1} + \alpha_i^{n-2} x + \alpha_i^{n-3} x^2 + \ldots + x^{n-1})$$

$$= \sum_{j=0}^{n-1} \left( \sum_{m=j+1}^{n} \sigma_m \alpha_i^{m-(j+1)} \right) x^j$$

which shows that:

$$i\sigma_j = \sum_{m=j+1}^{n} \sigma_m \alpha_i^{m-(j+1)} \tag{34}$$

for $i = 1,2,3,\ldots,n$ and $j = 0,1,2,\ldots,n-1$.

The restriction on $F(x)$ in (33) implies, on the other hand, that

$$\sum_{i=1}^{n} F(\alpha_i) \frac{i\sigma_j}{L_i(\alpha_i)} = 0 \tag{35}$$

for $j = k,k+1,\ldots,n-1$. By noticing that

$$\frac{d}{dx} L(x) = L'(x)$$

$$= \sum_{i=1}^{n} L_i(x)$$

and $L_i(\alpha_j) = 0$ if $i \neq j$, it follows that $L(\alpha_i) = L'(\alpha_i)$ for $i = 1,2,3,\ldots,n$. Whence, after substitution into (35):

$$\sum_{i=1}^{n} F(\alpha_i) \frac{i\sigma_j}{L'(\alpha_i)} = 0$$

The parity check matrix of the above code would be:

$$\begin{bmatrix} \frac{1\sigma k}{L'(\alpha_1)} & \frac{2\sigma k}{L'(\alpha_2)} & \cdots & \frac{n\sigma k}{L'(\alpha_n)} \\ \frac{1\sigma k+1}{L'(\alpha_1)} & \frac{2\sigma k+1}{L'(\alpha_2)} & \cdots & \frac{n\sigma k+1}{L'(\alpha_n)} \\ \vdots & \vdots & & \vdots \\ \frac{1\sigma n-1}{L'(\alpha_1)} & \frac{2\sigma n-1}{L'(\alpha_2)} & \cdots & \frac{n\sigma n-1}{L'(\alpha_n)} \end{bmatrix}$$

or

$$\begin{bmatrix} 1\sigma k & 2\sigma k & \cdots & n\sigma k \\ 1\sigma k+1 & 2\sigma k+1 & \cdots & n\sigma k+1 \\ \vdots & \vdots & & \vdots \\ 1\sigma n-1 & 2\sigma n-1 & \cdots & n\sigma n-1 \end{bmatrix} \begin{bmatrix} \frac{1}{L'(\alpha_1)} & 0 & \cdots & 0 \\ 0 & \frac{1}{L'(\alpha_2)} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{1}{L'(\alpha_n)} \end{bmatrix}$$

$$= A\ K$$

After substitution of $i\sigma j$, in (34), into A:

$$A = \begin{bmatrix} \sigma_{k+1} & \sigma_{k+2} & \cdots & \sigma_{n-1} & \sigma_n \\ \sigma_{k+2} & \sigma_{k+3} & \cdots & \sigma_n & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma_n & 0 & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-k} & \alpha_2^{n-k} & \cdots & \alpha_n^{n-k} \end{bmatrix}$$

$= BX$

It is obvious that B is nonsingular since det $B \neq 0$. In fact

$$\det B = \sigma_n^{n-k}$$

$$= 1 \qquad (\sigma_n = 1)$$

Hence, the parity check matrix AK is row equivalent to XK where

$$XK = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \cdots & \alpha_n^{t-1} \end{bmatrix} \times \begin{bmatrix} \frac{1}{L'(\alpha_1)} & 0 & \cdots & 0 \\ 0 & \frac{1}{L'(\alpha_2)} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{1}{L'(\alpha_n)} \end{bmatrix} \tag{36}$$

$t = n - k + 1$

Comparing with the parity check matrix in (15) shows that codes defined by (36) are special cases of generalized Goppa codes having the following parameters:

i) the subset $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $GF(q^m)$

ii) $p_i g_i^{-1} = 1$ for $i = 1,2,\ldots,n$ or $P(x) = G^{-1}(x)$

iii) $\deg G(x) = t$

$= n - k + 1$

where $G(x)$ is any arbitrary polynomial of degree $t$ over $GF(q^m)$ and relatively prime to $L(x)$. Notice on the other hand that the parity check natrix in (36) depends only on the subset $L$ and degree of $G(x)$.

2. A more general relationship between two classes of codes

Without restricting $\{g_i(x)\}$ to be polynomials over $GF(q^m)$ a more general relationship between codes constructed by generalized interpolation and generalized Goppa codes can be derived.

Recall that the generalized Goppa codes defined by a pair $(P(x),G(x))$ are the set of n-tuples $(a_1,a_2,\ldots,a_n)$ such that:

$$[B(x)P(x)]_{L(x)} = 0 \mod G(x) \qquad (14)$$

where $B(x)$ is the Lagrange polynomial associated with $(a_1,a_2,\ldots,a_n)$. In order to satisfy the above relation, there must exist a polynomial $K(x)$ over $GF(q^m)$ such that:

$$[B(x)P(x)]_{L(x)} = K(x)G(x)$$

and degree $K(x) \leq n - \deg G(x) - 1$. Whence:

$$[B(x)P(x)G^{-1}(x)]_{L(x)} = K(x)$$

$$\text{and deg } [B(x)P(x)G^{-1}(x)]_{L(x)} \leq n - \deg G(x) - 1 \qquad (37)$$

By noticing that $k(x)$ is any arbitrary polynomial over $GF(q^m)$, it follows that the last relation,(37), is another equivalent form, besides the one in (14), of defining the generalized Goppa codes.

Let c be the code generated by k independent functions $\{g_i(x)\}$ over $GF(q^m)$ and the set of n distinct elements $\alpha_1,\alpha_2,\ldots,\alpha_n$ in $GF(q^m)$. Let $(f_1,f_2,\ldots,f_n)$ be a codeword in c; then

$$f_i = \sum_{j=1}^{k} c_j g_j(\alpha_i) , \quad i = 1,2,3,\ldots,n$$

where $c_1,c_2,\ldots,c_k$ are coefficients in $GF(q^m)$.

Taking the Lagrange's transform of $(f_1,f_2,\ldots,f_n)$, one gets:

$$F(x) = \sum_{i=1}^{n} f_i \frac{L_i(x)}{L_i(\alpha_i)}$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{k} c_j g_j(\alpha_i) \frac{L_i(x)}{L_i(\alpha_i)}$$

after interchanging indexes i, j:

$$F(x) = \sum_{j=1}^{k} c_j \sum_{i=1}^{n} g_j(\alpha_i) \frac{L_i(x)}{L_i(\alpha_i)}$$

$$= \sum_{j=1}^{k} c_j g_j(x)$$

In order that the n-tuple $(f_1,f_2,\ldots,f_n)$ is a codeword of the generalized Goppa codes defined by $(P(x),G(x))$, $F(x)$ must satisfy the relation (37):

$$\deg [F(x)P(x)G^{-1}(x)]_{L(x)} \leq n - \deg G(x) - 1$$

or

$$\deg [\sum_{j=1}^{k} c_j g_j(x)P(x)G^{-1}(x)]_{L(x)} \leq n - \deg G(x) - 1$$

Since $c_1,c_2,\ldots,c_n$ are arbitrary coefficients in $GF(q^m)$

$$\deg [g_j(x)P(x)G^{-1}(x)]_{L(x)} \leq m$$

where $m = n - \deg G(x) - 1$. An obvious solution can be obtained as follows

$$k = m + 1$$

and $$g_i(x)P(x)G^{-1}(x) = x^{i-1}$$

or $$g_i(x) = x^{i-1}P^{-1}(x)G(x),\ i = 1,2,3,\ldots,n-\deg G(x) \qquad (38)$$

To complete the identification, one still has to show that the set of $m + 1$ functions, defined in (38), form a c-system; in other words, any linear combination of $\{g_i(x)\}$ can have no more than $m$ (or $k-1$) roots in the subset $L' = \{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of $GF(q^m)$.

Let $\phi(x)$ be an arbitrary linear combination of $m + 1$ functions $g_1(x),g_2(x),\ldots,g_{p+1}(x)$.

$$\phi(x) = \sum_{i=1}^{m+1} c_i g_i(x)$$

$$= \sum_{i=1}^{m+1} c_i x^{i-1} P^{-1}(x) G(x)$$

$$= P^{-1}(x) G(x) \sum_{i=1}^{p+1} c_i x^{i-1}$$

where $c_1, c_2, \ldots, c_{m+1}$ are coefficients in $GF(q^m)$. Since both polynomials $P(x)$ and $G(x)$ are relatively prime to $L(x)$, $P^{-1}(\alpha_i)G(\alpha_i)$ is nonzero for $i = 1,2,3,\ldots,n$ $\sum_{i=1}^{m+1} c_i x^{i-1}$, hence $P^{-1}(x)G(x) \sum_{i=1}^{m+1} c_i x^{i-1} = \phi(x)$ can have no more than m roots in $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

Hence, the set of m + 1 functions $\{g_i(x)\}$, as described in (38), does, indeed, form a c-system. It sollows that every code which is constructed based on the Lagrange's transform can be described in terms of the generalized interpolation.

C. Relationship between alternant codes and codes constructed via generalized interpolation.

Let A be alternant code described by the parity check matrix (3).

Recall that the relationship between the alternant and generalized Goppa codes was previously established by:

$$P(x) = y(x)L'(x)G(x) \qquad (39)$$

It is very straightforward to extend the connection to codes constructed on the generalized interpolation.

From (18)

$$y^{-1}(x)L^{-1}{}'(x) = P(x)^{-1}G(x)$$

After replacing in (38):

$$g_k(x) = x^{k-1}y^{-1}(x)L^{-1}{}'(x),\ k = 1,2,\ldots,n-t$$

It is a rather simple matter to verify that the set of $\{g_i(x)\}$ does also form a c-system by noting that $y^{-1}(\alpha_i)L^{-1}{}'(\alpha_i) = \frac{1}{y_i L'(\alpha_i)}$ is nonzero, for $i = 1,2,3,\ldots,n$.

D. Subcodes of Mandelbaum's codes

Since important classes of codes, such as the BCH codes, the generalized BCH codes, the Goppa codes, etc. are contained in the family of alternant codes, and of generalized Goppa codes, it would be interesting to describe these codes in terms of the generalized interpolation and henceforth, derive their respective generator matrix.

1. BCH codes

It was shown that the BCH code generated by a polynomial over $GF(q^m)$ having $\alpha^b,\alpha^{b+1},\ldots,\alpha^{b+t-1}$ as zeroes is the special case of alternant codes having as parameters:

$$\alpha_i = \alpha^{i-1} \quad , \quad i = 1,2,3,\ldots,n$$

and $$y_i = (\alpha^b)^{i-1} \quad , \quad i = 1,2,3,\ldots,n$$

It follows from (39) that the above code can be generated by a set of n - t functions $\{g_i(x)\}$ over $GF(q^m)$; each of the $g_i(x)$ is defined as follows:

$$g_i(x) = x^{i-1}x^{-b(i-1)}L^{-1}(x)$$

for i = 1,2,3,...,n-t, the subset L of $GF(q^m)$ consisting of all $n^{th}$ roots of unity, namely $1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{n-2}$. Note that

$$L(x) = \prod_{i=0}^{n-1} (x-\alpha_i)$$

$$= x^n - 1$$

and $$L'(x) = nx^{n-1}$$

$$= nx^{-1}$$

for $x = 1,\alpha,\alpha^2,\ldots,\alpha^{n-2}$

Whence:

$$g_i(x) = x^{i(1-b)+b} \quad , \quad i = 1,2,3,\ldots,n-t$$

ignoring the constant $n^{-1}$.

The generator matrix of the BCH code is:

$$G_{BCH} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta & \cdots & \beta^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{n-t-1} & \cdots & \beta^{(n-1)(n-t-1)} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \alpha & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \alpha^{n-1} \end{bmatrix} \quad (40)$$

where $\beta = \alpha^{1-b}$

In particular, if n is prime and b different from 1, there exists an integer b' such that $(1-b)b' \equiv 1 \bmod n$ and $\alpha = \beta^{b'}$. Whence:

$$G_{BCH} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \beta & \beta^{n-1} \\ \vdots & \vdots & \vdots \\ 1 & \beta^{n-t-1} & \beta^{(n-1)(n-t-1)} \end{bmatrix} \times$$

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \beta^{b'} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \beta^{(n-1)b'} \end{bmatrix} \quad (41)$$

2. Generalized BCH codes

Following the same procedure as in the previous section, it can be shown that the generalized BCH codes specified by the pair

of polynomials $(P(x),G(x))$ over $GF(q^m)$ are generated by the set of $n - t$ $q_i(x)$ functions having coefficients in $GF(q^m)$, $t$ being the degree of $G(x)$, and the subset $L = \{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of $GF(q^m)$ defined as follows:

$$g_i(x) = x^{i-1}P^{-1}(x)G(x) \quad , \; i = 1,2,3,\ldots,n-t$$

and $$\alpha_j = \alpha^{-(j-1)} \quad , \; j = 1,2,3,\ldots,n$$

The codes are defined by the generator matrix:

$$G_{GBCH} =$$

$$\begin{bmatrix} P^{-1}(\alpha_1)G(\alpha_1) & P^{-1}(\alpha_2)G(\alpha_2) & \cdots & P^{-1}(\alpha_n)G(\alpha_n) \\ \alpha_1 P^{-1}(\alpha_1)G(\alpha_1) & \alpha_2 P^{-1}(\alpha_2)G(\alpha_2) & \cdots & \alpha_n P^{-1}(\alpha_n)G(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-t-1}P^{-1}(\alpha_1)G(\alpha_1) & \alpha_2^{n-t-1}P^{-1}(\alpha_2)G(\alpha_2) & \cdots & \alpha_n^{n-t-1}P^{-1}(\alpha_n)G(\alpha_n) \end{bmatrix}$$

which, after substitution of $\alpha_i$, becomes:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(n-t-1)} & \cdots & \alpha^{-(n-t-1)(n-1)} \end{bmatrix} \times$$

$$\begin{bmatrix} p_0^{-1}g_0^{-1} & 0 & \cdots & 0 \\ 0 & p_1^{-1}g_1^{-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & p_{n-1}^{-1}g_{n-1}^{-1} \end{bmatrix} \qquad (42)$$

where $\sum_{i=0}^{n-1} p_i x^i$ and $\sum_{i=0}^{n-1} g_i x^i$ are polynomials associated with P(x) and G(x), respectively.

3. Goppa codes

Let G(x) be the Goppa polynomial of degree t over $GF(q^m)$ and L, the subset of $GF(q^m)$ consisting of $\alpha_1, \alpha_2, \ldots, \alpha_n$. The Goppa code having the above parameters is also generated by the following set of $(n - t)$ $g_i(x)$:

$$g_i(x) \quad x^{i-1} G(x)/L'(x)$$

$i = 1,2,3,\ldots,n-t$

and is specified by the generator matrix:

$$G_{Goppa} =$$

$$\begin{bmatrix} G(\alpha_1)L'^{-1}(\alpha_1) & G(\alpha_2)L'^{-1}(\alpha_2) & \cdots & G(\alpha_n)L'^{-1}(\alpha_n) \\ \alpha_1 G(\alpha_1)L'^{-1}(\alpha_1) & {}_2G(\alpha_2)L'^{-1}(\alpha_2) & \cdots & \alpha_n G(\alpha_n)L'^{-1}(\alpha_n) \\ \vdots & & & \vdots \\ \alpha_1^{n-t-1} G(\alpha_1)L'^{-1}\ \alpha_1) & \alpha_2^{n-t-1} G(\alpha_2)L'^{-1}(\alpha_2) & \cdots & \alpha_n^{n-t-1} G(\alpha_n)L'^{-1}(\alpha_n) \end{bmatrix}$$

or

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-t-1} & \alpha_2^{n-t-1} & \cdots & \alpha_n^{n-t-1} \end{bmatrix} \quad x$$

$$\begin{bmatrix} G(\alpha_1)L'^{-1}(\alpha_1) & & \cdots & 0 \\ 0 & G(\alpha_2)L'^{-1}(\alpha_2) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & G(\alpha_n)L'^{-1}(\alpha_n) \end{bmatrix} \qquad (43)$$

4. Generalized Srivastava codes

The last important subcode is the generalized srivastava code. Let the code be defined, as in (6), (7), by a given set of $n + s$ distinct elements $\alpha_1,\alpha_2,\ldots,\alpha_n,w_1,w_2,w_3,\ldots,w_s$, and n non-zero elements $z_1,z_2,\ldots,z_n$ of $GF(q^m)$.

Recall that is was already shown that the generalized Srivastava code is a subcode of the generalized Goppa codes specified by:

$$G(x) = \prod_{j=1}^{s} (x-w_j)^t$$

and $$P(x) = y(x)L'(x)G(x)$$

where y(x) is the Lagrange's polynomial associated with n-tuple:

$$\frac{z_1}{\prod_{j=1}^{s} (\alpha_1-w_j)^t}, \frac{z_2}{\prod_{j=1}^{s} (\alpha_2-w_j)^t}, \ldots \frac{z_n}{\prod_{j=1}^{s} (\alpha_n-w_j)^t}$$

Again, it is rather straightforward to prove that the generalized Srivastava code, thus defined, is a subcode of Mandelbaum's code generated by the following n - st functions $g_i(x)$:

$$g_i(x) = x^{i-1}y^{-1}(x)L'^{-1}(x)$$

for i = 1,2,3,...,n-st.

The generator matrix is defined by:

$$G_{\text{Gen. Sriv.}} =$$

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-st-1} & \alpha_2^{n-st-1} & \cdots & \alpha_n^{n-st-1} \end{bmatrix} \quad x$$

$$\begin{bmatrix} \frac{\prod_{j=1}^{s}(\alpha_1 - w_j)^t}{Z_1 L'(\alpha_1)} & 0 & \cdots & 0 \\ 0 & \frac{\prod_{j=1}^{s}(\alpha_2 - w_j)^t}{Z_2 L'(\alpha_2)} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{\prod_{j=1}^{s}(\alpha_n - w_j)^t}{Z_n L'(\alpha_n)} \end{bmatrix} \qquad (44)$$

The generator matrix of the original Srivastava code can be obtained by letting $t = 1$ and $Z_i = \alpha_i^{\mu}$ for $i = 1,2,3,\ldots,n$.

5. Alternant codes

The derivation of the generator matrix of the alternant codes defined in (3) is straightforward from relation:

$$g_k(x) = x^{k-1}y^{-1}(x)L'^{-1}(x),\ k = 1,2,\ldots,n-t.$$

$$G_{Alter} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-t-1} & \alpha_2^{n-t-1} & \cdots & \alpha_n^{n-t-1} \end{bmatrix} \times$$

$$\begin{bmatrix} y_1^{-1}L'^{-1}(\alpha_1) & & \cdots & 0 \\ 0 & y_2^{-1}L'^{-1}(\alpha_2) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & y_n^{-1}L'^{-1}(\alpha_n) \end{bmatrix} \qquad (45)$$

6. Generalized Goppa codes

Lastly, the generalized Goppa codes defined by (P(x),G(x)) are generated by the set of functions

$$g_k(x) = x^{i-1}P^{-1}(x)G(x)$$

for k = 1,2,...,n-t, t being deg of G(x). Its generator matrix is:

$$G_{\text{Gen. Goppa}} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-t-1} & \alpha_2^{n-t-1} & \cdots & \alpha_n^{n-t-1} \end{bmatrix} \quad x$$

$$\begin{bmatrix} p_1^{-1}g_1 & 0 & \cdots & 0 \\ 0 & p_2^{-1}g_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & p_n^{-1}g_n \end{bmatrix} \qquad (46)$$

## IV. Dual Codes of Generalized Goppa Codes

In this section, we will investigate the dual codes of generalized Goppa codes and show how one can derive their parity check matrices.

As validation, a check of the parity check matrix of the dual codes against the generator matrix of their original codes is made, which has been derived through the set of defined $\{g_i(x)\}$.

Recall that the generalized Goppa codes associated with $(P(x),G(x))$ can be described either in terms of a parity check matrix H as in (15) or by the relation (37):

$$\deg [B(x)P(x)G^{-1}(x)]_{L(x)} \leq n - \deg G(x) + 1$$

where $B(x)$ is the Lagrange's polynomial of the codeword $(b_1,b_2,\ldots,b_n)$.

A codeword $c = (c_1,c_2,\ldots,c_n)$ is in the dual of the generalized Goppa code if it is contained in the row space of H, or equivalently.

$$c = (a_0,a_1,\ldots,a_{t-1})\, H$$

where $t = \deg G(x)$ and $a_0,a_1,\ldots,a_{t-1}$ are elements of $GF(q^m)$ and H, parity check matrix defined in (15). Then:

$$c_i = \sum_{k=0}^{t-1} \alpha_k \alpha_i^k \frac{p_i g_i^{-1}}{L'(\alpha_i)} \quad \text{for } i = 1,2,3,\ldots,n$$

or $$p_i^{-1} g_i L'(\alpha_i) c_i = \sum_{k=0}^{t-1} a_k \alpha_i^k$$

Taking the Lagrange's transform of both sides gives:

$$P^{-1}(x)G(x)L'(x)c(x) = A(x)$$

where $A(x) = \sum_{k=0}^{t-1} a_k x^k$ and $\deg [A(x)] \leq t - 1 = n - (n-t) - 1$.
Whence:

$$\deg [c(x)P^{-1}(x)L'(x)G(x)] \leq n - (n-t) - 1 \qquad (47)$$

Let $G^{\perp}(x) \equiv G^{-1}(x) \bmod L(x)$ and $P^{\perp}(x) \equiv P(x)^{-1}L'(x)$. Obviously, $\deg G^{\perp}(x) = n - t = t'$ and, from (4 ):

$$\deg [c(x)P^{\perp}(x)G^{\perp -1}(x)] \leq n - t' - 1$$

Notice also that since $P(x)$, $G(x)$ and $L'(x)$ are all relatively prime to $L(x)$, it follows that $P^{\perp}(x)$ and $G^{\perp}(x)$, as defined above are also relatively prime to $L(x)$. The codeword $c = (c_1, c_2, \ldots, c_n)$ must then be in the generalized Goppa code associated with polynomials $P^{\perp}(x)$ and $G^{\perp}(x)$; the subset $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ remains unchanged. The dual code has as parity check matrix:

$$H_{dual} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-t-1} & \alpha_2^{n-t-1} & \cdots & \alpha_n^{n-t-1} \end{bmatrix} \quad x$$

$$\begin{bmatrix} p_1^{-1}g_1 & 0 & \cdots & 0 \\ & p_2^{-1}g_2 & \cdots & \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & p_n^{-1}g_n \end{bmatrix}$$

A check against the generator matrix in (46) shows that both matrices are identical, which was expected as:

$$H_{\text{dual } c} = G_c$$

$G_c$ being the generator matrix of an arbitrary code c.

A. Dual of alternant codes

It is very straightforward to extend the result over the class of alternant code from the relation (17) which established the equivalence between the alternant codes and generalized Goppa codes.

The parity check matrix of the dual codes is:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-t-1} & \alpha_2^{n-t-1} & \cdots & \alpha_n^{n-t-1} \end{bmatrix} \quad x$$

$$\begin{bmatrix} \frac{1}{y_k L'(\alpha_1)} & 0 & \cdots & 0 \\ 0 & \frac{1}{y_2 L'(\alpha_2)} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{1}{y_n L'(\alpha_n)} \end{bmatrix}$$

which is identical to the matrix derived in (45). Whence, the dual of alternant codes associated with the n-tuple $(y_1, y_2, \ldots, y_n)$ is also an alternant code; the n-tuple of which is, however,

$$y' = \left( \frac{1}{y_i L'(\alpha_1)}, \frac{1}{y_2 L'(\alpha_2)}, \ldots, \frac{1}{y_n L'(\alpha_n)} \right)$$

B. Dual of BCH codes

Extending the procedure of defining dual codes to BCH codes obviously gives a parity check matrix which is identical to the generator matrix in (40) since the codes are subcodes of generalized Goppa codes.

Particularly, if $b \neq 1$ and n is prime, it is possible to express $\alpha$ in function of $\beta$ and obtain the parity check matrix of the dual code identical to the one in (41). It follows then that the dual of the BCH code as defined in (4), e.g. generated by a polynomial over $GF(q^m)$ having $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+t-1}$ as zeroes, is a

BCH code having following parameters:

Code length: $n$

Minimum distance: $d \geq n - t + 1$

and being generated by a polynomial over $GF(q^m)$ having as zeroes $\beta^{b'}, \beta^{b'+1}, \ldots, \beta^{b'+(n-t)-1}$, with $\beta^{b'} = \alpha$

C. Dual of generalized BCH codes

Note that in case of generalized BCH codes, $\alpha_i = \alpha^{i-1}$ for $i = 1,2,3,\ldots,n$ and $L(x) = x^n - 1$. Consequently $L'(x) = nx^{n-1}$. Hence, from (47), the dual of the generalized BCH code defined by the pair of polynomials $(P(x),G(x))$ is also a generalized BCH code associated with $(P(x),G(x))$ such that:

$$P(x) = P(x)^{-1}L'(x)$$

$$= P(x)^{-1}nx^{n-1}$$

or simply $P(x) = x^{n-1}P(x)^{-1}$

and $G(x) \equiv G^{-1}(x) \bmod (x^n-1)$, from (5), its parity check matrix is:

$H_{\text{dual GBCH}} =$

$$\begin{bmatrix} 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(n-t)} & \cdots & \alpha^{-(n-t)(n-1)} \end{bmatrix} \quad x$$

$$\begin{bmatrix} p_0^{-1}g_0 & 0 & \cdots & 0 \\ 0 & \alpha p_1 g_1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \alpha^{(n-1)} p_{n-1}^{-1} g_{n-1} \end{bmatrix}$$

since $P(x) = x^{n-1} P(x)^{-1}$

$= x^{-1} P(x)^{-1} \qquad (x^n = 1)$

or:

$$= \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(n-t-1)} & \cdots & \alpha^{-(n-1)(n-t-1)} \end{bmatrix}$$

$$\begin{bmatrix} p_0^{-1}g_0 & 0 & \cdots & 0 \\ 0 & p_1^{-1}g_1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & p_{n-1}^{-1}g_{n-1} \end{bmatrix}$$

which is identical to the generator matrix of the original code defined in (42).

D. Dual of Goppa codes

This is the special case of generalized Goppa codes with $P(x) = L'(x)$. It is very easy to show that the dual of the Goppa code specified by the Goppa polynomial $G(x)$ is also a Goppa code; the Goppa polynomial of the dual code is defined as:

$$G(x) = L'(x)G^{-1}(x)$$

The derived parity check matrix of the dual code is, as expected, identical to the one in (43).

E. Dual of generalized Srivastava codes

Finally, repeating the procedure of finding the dual code based on (47) on generalized Srivastava code leads to a parity check matrix of the dual code, which, again is identical to the matrix in (44).

Unfortunately, unlike other classes of code, whether the dual of the generalized Srivastava code remains to be determined, although the dual code does belong to the family of generalized Goppa codes.

The dual of the original Srivastava codes can be obtained by letting $t = 1$ and $z_i = \alpha_i^{\mu}$, in (44), $i = 1,2,\ldots,n$ and $\mu$, an arbitrary interger. However, it still remains to determine whether the dual of the Srivastava code is also a Srivastava code.

## V. Conclusion

We have shown that codes constructed on the basis of generalized interpolation proposed by Mandelbaum include many important error-correcting codes discussed in this thesis. It is also shown how these codes can be defined in terms of the generalized interpolation which is characterized by a Chebyshev systems of functions over $GF(q^m)$. Particularly, if these functions are restricted to be polynomials of degree less than or equal to n-1, the generalized interpolation is reduced to Lagrange's interpolation; since many important codes discussed in this thesis can be constructed via Lagrange's interpolation, in general case, it is expected that the codes constructed via generalized interpolation include other codes. But it still remains to determine how extensive and powerful these codes are.

## Appendix

A. If c is a nonsingular matrix, then codes defined by parity check matices cxy and xy are exactly identical.

Proof:

Let A, A′ being codes defined by cxy and xy, respectively.

It is obvious that $A' \subseteq A$ since, for any $v \in A'$ $v(xy)^T = vy^Tx^T = 0$ implies that $vy^Tx^Tc^T = 0 = v(cxy)^T$.

Assume now that $A \subseteq A'$. Then there exists a codeword $v_0$ such that $v_0$ is in A, but not in A′ or, equivalently:

$$v_0(cxy)^T = 0 \quad \text{and} \quad v_0(xy)^T \neq 0$$

Thus, $v_0(xy)^T = vy^Tx^T = v_0' \neq 0$. However, $v_0(cxy)^T = v_0y^Tx^Tc^T = v_0'c^T = 0$ implies that $c^T$, hence c, is singular, which is a contradiction.

A must then be contained in A′, whence:

$$A = A'$$

Q.E.D.

B. Let H be a matrix of the form:

$$H = \begin{bmatrix} g^{-1}(\alpha_1) & g^{-1}(\alpha_2) & \cdots & g^{-1}(\alpha_n) \\ g^{-1}(\alpha_1)\alpha_1 & g^{-1}(\alpha_2)\alpha_2 & \cdots & g^{-1}(\alpha_n)\alpha_n \\ \vdots & \vdots & & \vdots \\ g^{-1}(\alpha_1)\alpha_1^{r-1} & g^{-1}(\alpha_2)\alpha_2^{r-1} & \cdots & g^{-1}(\alpha_n)\alpha_n^{r-1} \end{bmatrix}$$

where $g(x)$ is a polynomial over $GF(q^m)$ of degree $r$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ are elements of $GF(q^m)$ distinct from the roots of $g(x)$.

Particularly, if $g(x) = g_i(x) = (x - \beta_i)^{r_i}$, then:

$$H_i = \begin{bmatrix} (\alpha_1-\beta_i)^{-r_i} & (\alpha_2-\beta_i)^{-r_i} & \cdots & (\alpha_n-\beta_i)^{-r_i} \\ (\alpha_1-\beta_i)^{-r_i}\alpha_1 & (\alpha_2-\beta_i)^{-r_i}\alpha_2 & \cdots & (\alpha_n-\beta_i)^{-r_i}\alpha_n \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_i)^{-r_i}\alpha_1^{r_i-1} & (\alpha_2-\beta_i)^{-r_i}\alpha_2^{r_i-1} & \cdots & (\alpha_n-\beta_i)^{-r_i}\alpha_n^{r_i-1} \end{bmatrix}$$

which is row equivalent to:

$$\begin{bmatrix} (\alpha_1-\beta_i)^{-r_i} & (\alpha_2-\beta_i)^{-r_i} & \cdots & (\alpha_n-\beta_i)^{-r_i} \\ (\alpha_1-\beta_i)^{-r_i}(\alpha_1-\beta_i) & (\alpha_2-\beta_i)^{-r_i}(\alpha_2-\beta_i) & \cdots & (\alpha_n-\beta_i)^{-r_i}(\alpha_n-\beta_i) \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_i)^{-r_i}(\alpha_1-\beta_i)^{r_{i-1}} & (\alpha_2-\beta_i)^{-r_i}(\alpha_2-\beta_i)^{+r_{i-1}} & \cdots & (\alpha_n-\beta_i)^{-r_i}(\alpha_n-\beta_i)^{r_{i-1}} \end{bmatrix}$$

$$= \begin{bmatrix} (\alpha_1-\beta_i)^{-r_i} & (\alpha_2-\beta_i)^{-r_i} & \cdots & (\alpha_n-\beta_i)^{-r_i} \\ (\alpha_1-\beta_i)^{-(r_i-1)} & (\alpha_2-\beta_i)^{-(r_i-1)} & \cdots & (\alpha_n-\beta_i)^{-(r_i-1)} \\ \vdots & \vdots & & \\ (\alpha_1-\beta_i)^{-1} & (\alpha_2-\beta_i)^{-1} & \cdots & (\alpha_n-\beta_i)^{-1} \end{bmatrix}$$

The above result was derived by Tzeng and Zimmerman.

## References


[ 1] K.K. Tzeng and C.Y. Yu, Characterization theorems for extending Goppa codes to cyclic codes, IEEE Trans. Inform. Theory, IT-25, pp. 246-250, March 1979.

[ 2] K.K. Tzeng and K. Zimmerman, On extending Goppa codes to cyclic codes, IEEE Trans. Inform. Theory, IT-21, pp. 712-716, Nov. 1975.

[ 3] K.K. Tzeng and K. Zimmerman, Lagrange's interpolation formula and the generalization of Goppa codes, presented at the IEEE International Symposium on Inform. Theory, Ronneby, Sweden, June 1976.

[ 4] Philippe Delsartes, On subfield subcodes of modified Reed-Solomon codes, IEEE Trans. Inform. Theory, IT-21, pp. 575-576, Sept. 1975.

[ 5] H.J. Helgert, Alternant codes, Information and Control, 26, pp. 369-380, Dec. 1974.

[ 6] H.J. Helgert, Noncyclic generalization of BCH and Srivastava codes, Information and Control, 21, pp. 280-290, Oct. 1972.

[ 7] H.J. Helgert, Srivastava codes, IEEE Trans. Inform. Theory, IT-18, pp. 292-297, March 1972.

[ 8] R.T. Chien and D.M. Choy, Algebraic generalizations of BCH-Goppa-Helgert codes, IEEE Trans. Inform. Theory, IT-21, pp. 70-79, Jan. 1975.

[ 9] J.M. Goethals, A polynomial approach to linear codes, Philips Res. Rep., 24, pp. 145-159, 1969.

[10] D.M. Mandelbaum, Construction of error-correcting codes by interpolation, IEEE Trans. Inform. Theory, IT-25, pp. 27-35, Jan. 1979.

[11] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North Holland, New York.

## Vita

Loc Van Ngo was born in Bac Giang, Viet Nam on September 6, 1953. He graduated from Marie Curie High School in 1972 and attended the National Institute of Technology in Saigon from 1972 to 1975. Since 1976, he has attended Lehigh University and received his Bachelor of Science Degree in Electrical Engineering in 1978. From 1978 to 1980, he has been a teaching and research assistant in the Department of Electrical Engineering and is also a recipient of a University fellowship. Loc is a member of Eta Kappa Nu.