1-1-1978

On the relationship between generalized Goppa codes and cyclic codes.

Mark Edward Scheitrum

ON THE RELATIONSHIP BETWEEN GENERALIZED GOPPA CODES AND CYCLIC CODES

by

Mark Edward Scheitrum

A Thesis

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

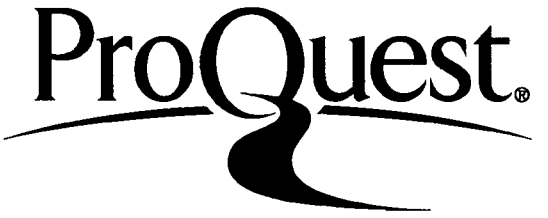
Master of Science

in

Electrical Engineering

Lehigh University

1978



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

April 1, 1975
Date

Professor in Charge

Chairman of Department

ACKNOWLEDGEMENTS

I wish to take this time to express my deep gratitude to my thesis advisor, Professor Tzeng, for the guidance he gave me in my studies of coding theory.

The support extended by the National Science Foundation and the Department of Electrical Engineering, Lehigh University, is gratefully acknowledged.

I would also like to thank my wife, Margaret, for her support and understanding during my graduate career.

Finally, I wish to thank Ms. Jeanne Loosbrock for typing the manuscript.

TABLE OF CONTENTS

		Page
ABSTRACT		1
I.	INTRODUCTION	3
	1. Error-Correcting Coding	3
	2. Organization of the Investigation	5
II.	PRELIMINARIES	7
	1. Background	7
	1.1 Goppa Codes	7
	1.2 LaGrange's Interpolation Formula	8
	1.3 Parity-Check Matrices	10
	1.4 The H Matrix for Generalized Goppa Codes	13
	1.5 Cyclic Codes	15
	1.6 Results to Date	16
III.	GENERALIZED GOPPA CODES WITH L = $GF(q^m)$	18
	1. Characterization	18
	1.1 Description	18
	1.2 Relation to Cyclic Codes	18
IV.	GENERALIZED GOPPA CODES WITH L⊂$GF(q^m)$	25
	1. Generalized Goppa Codes with L=$GF(q^m)$-$\{\beta\}$	25
	2. Generalized Goppa Codes with L=$GF(q^m)$-$\{\beta_1,\beta_2\}$	28
	2.1 Case 1: d=2	31
	2.2 Case 2: d=-1	37

Page

C. CONCLUSIONS 42

1. Results 42

2. Further Research 43

REFERENCES 45

VITA 46

ABSTRACT

This investigation determines some relationships between the class of generalized Goppa codes described by Tzeng and Zimmermann and cyclic codes. A new form of the parity-check matrix for generalized Goppa Codes is described, which lends itself to this type of investigation. It is shown that of the class of generalized Goppa Codes with the location set L an entire field and g(z) having no repeated roots, the only codes that can be extended to be cyclic are the subclass of Goppa Codes with g(z) a quadratic polynomial. For the class of generalized Goppa Codes with $L = GF(q^m) - \{\beta\}$ and $g(z) = (z-\beta)^a$ it is shown that the subclass of codes with $P(z) = [L'(z)]^b$, where b is an integer relative prime to q^m-1 and a any positive integer, is cyclic. Some results are presented for the class of generalized Goppa Codes with $L = GF(q^m) - \{\beta_1, \beta_2\}$ and $g(z) = (z-\beta_1)(z-\beta_2)$. They are:

(1) that the subclass of codes with $P(z) = k/(z-\beta_2)^2$, where k is any element of an extension field of $GF(q^m)$, can be extended to be cyclic by appending an overall parity check.

(2) that the subclass of codes with $P(z) = k(z-\beta_1)/(z-\beta_2)^2$ with k as above can be extended to be cyclic.

(3) that the subclass of codes with $P(z) = k(z-\beta_1)/(z-\beta_2)$ can be extended to be cyclic.

Finally, some related problems for further investigation have been suggested.

CHAPTER I

INTRODUCTION

1. Error-Correction Coding

Since the advent of the electronic digital computer in the late 1940's the information handling capability of man has grown phenomenally. With this increasing traffic in data comes the responsibility of guarding the information against corruption from noise during transfer and storage. To this end the field of error-correction coding has been developed.

Error-correction coding concerns the adding of redundancy to information in such a way that if errors occur during transmission or storage, either the errors can be detected, or they can be detected and corrected.

Of the two possibilities, the first case, error-detection, is the simplest to accomplish. At present, error-detecting codes in the form of 'single-parity-check' codes are the most prevalent type in use.

Typically, a single-parity-check code is a single-error detecting code which uses one redundant digit as an overall parity check. If the information is in the form of a string of base b digits, the parity (redundant) bit is chosen so that the sum of the information digits plus the check digit equals zero modulo b.

Single-parity-check codes are not useful, however, in

applications where more than one error per information 'block' is likely. Moreover, error-detecting codes generally are not desirable in situations where retransmission of information after error detection is not feasible, such as in information storage elements (e.g. magnetic tapes and disks) or one way transmission channels. For these and other reasons, which will be presented, much research is ongoing in the design of codes with greater error detection and correction capabilities.

The most important result in the area of information transfer and the basis for coding theory is Shannon's "Coding Theorem." [10] The theorem states that every channel has a definite information transfer capacity C, and that for any rate R less than C there exist codes of rate R which have an arbitrarily small probability of erroneous decoding. This probability is a function of the code length, and by increasing the length in the proper way we can decrease the probability of erroneous decoding.

This theorem and other application considerations allows us to formulate three goals in coding theory: (1) to find long good codes; (2) to find a practical method of encoding; and (3) to find a practical method of decoding.

Since recent year much of the research in coding is in the area of cyclic codes. Cyclic codes are a subclass

of linear block codes possessing an inherent algebraic structure which allows them to be encoded and decoded by means of relatively simple digital hardware or software techniques. Thus this class of codes satisfies goals (2) and (3) stated above.

Another area of recent interest in coding theory is the class of linear block codes called Goppa codes [1] and [2]. Subclasses of Goppa and other related codes have been shown to satisfy goal (1) above.

Thus there is much interest in determining how Goppa and generalized Goppa codes relate to cyclic codes in order to take advantage of the good properties of both. To the second case (generalized Goppa codes) this thesis is addressed.

2. Organization of the Investigation

The presentation is organized in the following manner:

Chapter II consists of background material for the Goppa codes and a review of cyclic codes. This material developed is used to define a parity-check matrix for generalized Goppa codes. It also lists some of the results achieved in relating Goppa and cyclic codes.

Chapter III considers the case of generalized Goppa codes with the location set an entire field and their cyclic properties.

Chapter IV deals with generalized Goppa codes with the location set L a subset of a field and their cyclic properties before and after extension by an overall parity check. Some examples are presented.

Chapter V presents the conclusions drawn from this investigation and suggests some areas of further research.

CHAPTER II

PRELIMINARIES

1. Background

1.1 Goppa Codes

In 1970 and 1971 V. D. Goppa [1], [2] introduced a class of linear error-correcting codes based on rational functions. This class has been shown to possess codes which are asymptotically good. This means that as the block length n approaches infinity the minimum distance of the code tends to the Varsharmov-Gilbert bound. This is the lower bound on the minimum distance attainable with an (n,k) block code. Goppa codes contain the class of Bose-Chaudhuri-Hocquenghem codes which are the only known cyclic Goppa codes. Goppa codes may be represented by a location set L and a generator polynomial g(z), called the Goppa polynomial.

Let $L = \{a_1, a_2, \ldots, a_n\}$ be a subset of the Galois field of q^m elements, $GF(q^m)$ where q is a power of a prime P, m is any integer ≥ 0 and $GF(q^m)$ is the smallest field containing L. Let g(z) be a polynomial in z over $GF(q^m)$ such that g(z) has no root in L and the degree of g(z) is less than n. A Goppa code is then defined as the set of n-tuples $(b_1, b_2, \ldots, b_n)$, with b_i GF(q) such that

$$\sum_{i=1}^{n} \frac{b_i}{z-a_i} \equiv 0 \text{ modulo } g(z) \qquad 1.1.1$$

The minimum distance for this code is greater than or equal to deg[g(z)]+1.

1.2 LaGrange's Interpolation Formula

Recent work by Tzeng and Zimmermann [3] has determined the relationship between Goppa codes and LaGrange's Interpolation formula. A new representation of Goppa codes and a generalization of these codes has been shown via LaGrange's Interpolation formula.

If $(b_1, b_2, \ldots, b_n)$ is a code vector from a Goppa code C where $b_i \in GF(q)$ and $L = \{a_1, a_2, \ldots, a_n\}$ is the location set, then there exists a unique polynomial B(z) of degree $\leq (n-1)$ such that

$$B(a_i) = b_i \qquad \text{for } i = 1, 2, \ldots, n.$$

This polynomial is given by

$$B(z) = \sum_{i=1}^{n} b_i \frac{\prod_{\substack{j=1 \\ j \neq i}}^{n} (z - a_j)}{\prod_{\substack{j=1 \\ j \neq i}}^{n} (a_i - a_j)} \qquad 1.2.1$$

This is known as LaGrange's Interpolation polynomial.

Let

$$L(z) = \prod_{i=1}^{n} (z - a_i) \qquad 1.2.2$$

This shall be called the location polynomial. Let

$$L_i(z) = \frac{L(z)}{(z - a_i)} \qquad 1.2.3$$

Let $L'(z)$ be the formal derivative of $L(z)$ with respect to z, then

$$L'(z) = \sum_{i=1}^{n} L_i(z) \qquad 1.2.4$$

Now

$$\sum_{i=1}^{n} \frac{b_i}{z-\alpha_i} = \frac{1}{L(z)} \sum_{i=1}^{n} b_i L_i(z) \qquad 1.2.5$$

Since $(L(z)|g(z)) = 1$, 1.2.6

we have $(b_1, b_2, \ldots b_n) \in C$ if and only if

$$\sum_{i=1}^{n} b_i L_i(z) \equiv 0 \bmod g(z) \qquad 1.2.7$$

It has been shown that

$$\sum_{i=1}^{n} b_i L_i(z) = B(z) L'(z) \text{ modulo } L(z) \qquad 1.2.8$$

$$= [B(z) L'(z)]_{L(z)} \qquad 1.2.9$$

Therefore the Goppa code can be defined as the set of $b(x)$ such that

$$[B(z) L'(z)]_{L(z)} \equiv 0 \bmod g(z) \qquad 1.2.10$$

Using this description of Goppa codes a generalization is arrived at by replacing $L'(z)$ with $P(z)$ where $P(z)$ is any polynomial over $GF(q^m)$ which is also relatively prime to $L(z)$. The generalized Goppa code is thus defined as the set of $b(x)$ over $GF(q)$ such that

$$[B(z)P(z)]_{L(z)} \equiv 0 \bmod g(z) \qquad 1.2.11$$

where $(P(z)|L(z)) = 1$ 1.2.12

1.3 Parity Check Matrices

One form of the parity check matrix of a Goppa code given in [1] and [2] is

$$H = \begin{bmatrix} g^{-1}(a_1) & g^{-1}(a_2) & \cdots & g^{-1}(a_n) \\ g^{-1}(a_1)a_1 & g^{-1}(a_2)a_2 & \cdots & g^{-1}(a_n)a_n \\ \vdots & \vdots & & \vdots \\ g^{-1}(a_1)a_1^{r-1} & g^{-1}(a_2)a_2^{r-1} & & g^{-1}(a_n)a_n^{r-1} \end{bmatrix} \quad 1.3.1$$

where r is the degree of g(z).

The derivation of another form credited to Tzeng and Zimmermann [4] is as follows:

For a code with $g_\ell(z) = (z-\beta_\ell)^{r_\ell}$ the H matrix is

$$H = \begin{bmatrix} (a_1-\beta_\ell)^{-r_\ell} & (a_2-\beta_\ell)^{-r_\ell} & \cdots & (a_n-\beta_\ell)^{-r_\ell} \\ (a_1-\beta_\ell)^{-r_\ell}a_1 & (a_2-\beta_\ell)^{-r_\ell}a_2 & \cdots & (a_n-\beta_\ell)^{-r_\ell}a_n \\ \vdots & \vdots & & \vdots \\ (a_1-\beta_\ell)^{-r_\ell}a_1^{r_\ell-1} & (a_2-\beta_\ell)^{-r_\ell}a_2^{r_\ell-1} & \cdots & (a_n-\beta_\ell)^{-r_\ell}a_n^{r_\ell-1} \end{bmatrix} \quad 1.3.2$$

which is row equivalent to

$$H_\ell = \begin{bmatrix} (\alpha_1-\beta_\ell)^{-1} & (\alpha_2-\beta_\ell)^{-1} & \cdots & (\alpha_n-\beta_\ell)^{-1} \\ (\alpha_1-\beta_\ell)^{-2} & (\alpha_2-\beta_\ell)^{-2} & \cdots & (\alpha_n-\beta_\ell)^{-2} \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_\ell)^{-r_\ell} & (\alpha_2-\beta_i)^{-r_i} & \cdots & (\alpha_n-\beta_\ell)^{-r_\ell} \end{bmatrix} \qquad 1.3.3$$

Consequently, for $g(z) = \prod_{\ell=1}^{s} (z-\beta_\ell)^{r_\ell}$ 1.3.4

$$= \prod_{\ell=1}^{s} g_\ell(z)$$

The Goppa code is the intersection of the codes with

$$g_\ell(z) = (z-\beta_\ell)^{-r_\ell} \text{ for } \ell = 1,2,\ldots,s. \qquad 1.3.5$$

Therefore

$$H = \begin{bmatrix} (\beta_1-\alpha_1)^{-1} & (\beta_1-\alpha_2)^{-1} & \cdots & (\beta_1-\alpha_n)^{-1} \\ (\beta_1-\alpha_1)^{-2} & (\beta_1-\alpha_2)^{-2} & \cdots & (\beta_1-\alpha_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (\beta_1-\alpha_1)^{-r_1} & (\beta_1-\alpha_2)^{-r_1} & \cdots & (\beta_1-\alpha_n)^{-r_1} \\ (\beta_2-\alpha_1)^{-1} & (\beta_2-\alpha_2)^{-1} & \cdots & (\beta_2-\alpha_b)^{-1} \\ \vdots & \vdots & & \vdots \\ (\beta_2-\alpha_1)^{-r_2} & (\beta_2-\alpha_2)^{-r_2} & \cdots & (\beta_2-\alpha_n)^{-r_2} \\ \vdots & \vdots & & \vdots \\ (\beta_s-\alpha_1)^{-1} & (\beta_s-\alpha_2)^{-1} & \cdots & (\beta_s-\alpha_n)^{-1} \\ \vdots & \vdots & & \vdots \\ (\beta_s-\alpha_1)^{-r_s} & (\beta_s-\alpha_2)^{-r_s} & \cdots & (\beta_s-\alpha_n)^{-r_s} \end{bmatrix} \qquad 1.3.6$$

The H matrix in this form has advantages for studying the cyclic properties of extended Goppa codes. One result of this presentation will be the determination of a similar form of the parity check matrix for generalized Goppa codes.

The parity check matrix for generalized Goppa codes as derived in 3 is as follows:

$$H = \begin{bmatrix} \frac{P_1 g_1^{-1}}{L'(\alpha_1)} & \frac{P_2 g_2^{-1}}{L'(\alpha_2)} & \cdots & \frac{P_n g_n^{-1}}{L'(\alpha_n)} \\ \frac{P_1 g_1^{-1}}{L'(\alpha_1)}\alpha_1 & \frac{P_2 g_2^{-1}}{L'(\alpha_2)}\alpha_2 & \cdots & \frac{P_n g_n^{-1}}{L'(\alpha_n)}\alpha_n \\ \vdots & \vdots & & \vdots \\ \frac{P_1 g_1^{-1}}{L'(\alpha_1)}\alpha_1^{r-1} & \frac{P_2 g_2^{-1}}{L'(\alpha_2)}\alpha_2^{r-1} & \cdots & \frac{P_n g_n^{-1}}{L'(\alpha_n)}\alpha_n^{r-1} \end{bmatrix} \qquad 1.3.7$$

where $p_i = P(\alpha_i)$, $g_i^{-1} = \frac{1}{g(\alpha_i)}$

and $L'(\alpha_i) = L_i(\alpha_i)$, deg $[g(z)] = r$.

As expected, when $P(z) = L'(z)$ this gives

$$p_i = L'(\alpha_i) \qquad 1.3.8$$

and

$$\frac{p_i g_i^{-1}}{L'(\alpha_i)} = g_i^{-1} \qquad 1.3.9$$

and the code is equivalent to a Goppa code.

1.4 The H Matrix for Generalized Goppa Codes

At this point we can take the parity check matrix as presented in matrix 1.3.7 and manipulate it into a form more suited to this presentation. The matrix cited above can be separated into the product of two matrices and written as:

$$H = \begin{bmatrix} g_1^{-1} & g_2^{-1} & \cdots & g_n^{-1} \\ g_1^{-1}\alpha_1 & g_2^{-1}\alpha_2 & \cdots & g_n^{-1}\alpha_n \\ \vdots & \vdots & & \vdots \\ g_1^{-1}\alpha_1^{r} & g_2^{-1}\alpha_2^{r} & \cdots & g_n^{-1}\alpha_n^{r} \end{bmatrix} \qquad 1.4.1$$

$$\begin{bmatrix} P_1 L'^{-1}(\alpha_1) & 0 & \cdots & 0 \\ 0 & P_2 L'^{-1}(\alpha_2) & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & P_n L'^{-1}(\alpha_n) \end{bmatrix}$$

In this form, the first matrix can be recognized as the H matrix for Goppa codes. Rewriting the first matrix as in matrix 1.3.6 where g(z) is defined as

$$g(z) = (z-\beta_1)^{r_1}(z-\beta_2)^{r_2}\ldots(z-\beta_s)^{r_s} \qquad 1.4.2$$

and substituting for $p_i L'^{-1}(\alpha_1)$

$$p_i L'^{-1}(\alpha_i) = x_i \qquad 1.4.3$$

yields

$$H = \begin{bmatrix} (\beta_1-\alpha_1)^{-1} & (\beta_1-\alpha_2)^{-1} & \ldots & (\beta_1-\alpha_n)^{-1} \\ \vdots & \vdots & & \vdots \\ (\beta_1-\alpha_1)^{-r_1} & (\beta_1-\alpha_2)^{-r_2} & \ldots & (\beta_1-\alpha_n)^{-r_1} \\ \vdots & \vdots & & \vdots \\ (\beta_s-\alpha_1)^{-1} & (\beta_s-\alpha_2)^{-1} & \ldots & (\beta_s-\alpha_n)^{-1} \\ \vdots & \vdots & & \vdots \\ (\beta_s-\alpha_1)^{-r_s} & (\beta_s-\alpha_2)^{-r_s} & \ldots & (\beta_s-\alpha_n)^{-r_s} \end{bmatrix} \qquad 1.4.4$$

$$\begin{bmatrix} x_1 & 0 & \ldots & 0 \\ 0 & x_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x_n \end{bmatrix}$$

Since P(z) is defined to be a polynomial over $GF(q^m)$ and

$$(P(z),L(z)) = 1$$

thus p_1 must be an element of $GF(q^m) - \{0\}$. If $p_i = P(\alpha_i)$ were 0 then $P(z),L(z))$ would not be 1. Also since L(z) has no repeated roots $(L(z),L'(z)) = 1$ and $L'^{-1}(\alpha_i)$ must also be an element of $GF(q^m) - \{0\}$. Hence

$x_i \in GF(q^m) - \{0\}$ for all $0 < i \leq n$ 1.4.5

The matrix 1.2.4 is equivalent to matrix 1.2.1 and shall be used throughout the remainder of this presentation.

1.5 Cyclic Codes

Definition 1.1. An (n,k) linear code C is called a cyclic code if it has the following property: If an n-tuple

$$V = (v_1, v_2, \ldots v_n) \quad 1.5.1$$

is a code vector of C then the n-tuple

$$V^{(1)} = (v_n, v_1, v_2, \ldots v_{n-1}) \quad 1.5.2$$

obtained by shifting V cyclically one place to the right is also a code vector of C.

There exists an isomorphism between the code vectors and polynomials in x as below.

$$V = (v_1, v_2, \ldots, v_n) \Leftrightarrow V(x) = v_1 + v_2 + \ldots + v_n x^{n-1} \quad 1.5.3$$

and for any cyclic code there exists one and only one code polynomial g(x) of degree n-k and every other code polynomial is a multiple of g(x).

For the code with $v_i \in GF(q)$, g(x) can be written as $(x-\gamma_1)(x-\gamma_2)\ldots(x-\gamma_{n-k})$ where γ_i are elements of an extension field of GF(q) and g(x) is a divisor of x^n-1.

It is true then that every polynomial f(x) that satisfies $f(\gamma_i)=0$ for all $0<i\leq n-k$ must be a multiple of g(x) and hence a code polynomial of C. This allows the parity check matrix for the code C to be written as follows.

$$H = \begin{bmatrix} \gamma_1^0 & \gamma_1^1 & \cdots & \gamma_1^{n-1} \\ \gamma_2^0 & \gamma_2^1 & \cdots & \gamma_2^{n-1} \\ & & & \\ \gamma_{n-k}^0 & \gamma_{n-k}^1 & \cdots & \gamma_{n-k}^{n-1} \end{bmatrix} \qquad 1.5.4$$

where the γ_i's are roots of $g(x)$.

It is true in general that any code with code elements from GF(q) that can be described by a parity check matrix

$$H = \begin{bmatrix} \gamma_1^0 & \gamma_1^1 & \cdots & \gamma_1^{n-1} \\ \gamma_2^0 & \gamma_2^1 & \cdots & \gamma_1^{n-1} \\ & & & \\ \gamma_r^0 & \gamma_r^1 & \cdots & \gamma_r^{n-1} \end{bmatrix} \qquad 1.5.5$$

where the γ_i are elements of an extension field of GF(q) and for all i, $\gamma_i^n = 1$, is cyclic.

1.6 Results to Date

V. D. Goppa in 1970 showed that the only cyclic Goppa codes are BCH codes.

Berlekamp and Moreno [5] in 1973 showed that the double-error-correcting binary Goppa codes, defined by $L = GF(2^m)$ and $g(z)$ an irreducible polynomial over $GF(2^m)$ become cyclic when extended by an overall parity check.

Tzeng and Zimmermann [4] in 1975 showed that:

1) The class of q-ary multiple-error-correcting reversible Goppa codes with $L = GF(q^m)$ and $g(z)$ irreducible over $GF(q^m)$

$$g(z) = [(z-\beta)(z-\beta^{q^m})]^a \qquad 1.6.1$$

where the exponent a is a positive integer less than or equal to $(q^m-1)/2$, is made cyclic when extended by an overall parity bit. This result is a generalization of that by Berlekamp and Moreno.

2) The class of q-ary multiple-error-correcting reversible Goppa codes with $L = GF(q^m) - \{\beta_1, \beta_2\}$ and

$$g(z) = [(z-\beta_1)(z-\beta_2)]^a \qquad 1.6.2$$

is made cyclic when extended by an overall parity check.

Tzeng and Yu [6] in 1975 determined some necessary conditions for Goppa codes in order that they be extendable to cyclic codes.

CHAPTER III

GENERALIZED GOPPA CODES WITH L = $GF(q^m)$

1. Characterization

1.1 Description

For generalized Goppa codes with L = $GF(q^m)$ we have an added condition imposed on the Goppa polynomial g(z). The coefficients of g(z) must be from $GF(q^m)$ and since the roots of g(z) cannot be from L = $GF(q^m)$, g(z) must have its roots in an extension field of $GF(q^m)$. Thus g(z) can be expressed as $g(z) = m_1(z)m_2(z)\ldots m_s(z)$ where $m_i(z)$ is the minimum polynomial of β_i in an extension field of $GF(q^m)$. In this chapter we shall consider the case where g(z) = m(z) where m(z) is the minimum polynomial of β in $GF(q^{rm})$, where r = [deg m(z)].

1.2 Relation to Cyclic Codes

Let C be a generalized Goppa code with L = $GF(q^m)$ and g(z) = m(z) is the minimum polynomial of β over $GF(q^{rm})$.

$$g(z) = (z-\beta)(z-\beta^{q^m})\ldots(z-\beta)^{q^m-1} \qquad 1.2.2$$

The degree of g(z) = r is greater than or equal to 2. Let us consider first the case where deg[g(z)] = 2. That is g(z) is a quadratic polynomial over $GF(q^m)$ with roots in $GF(q^{2m})$. For this case, we can state the following.

Theorem 1. For generalized Goppa codes with L = $GF(q^m)$

and g(z) an irreducible quadratic polynomial over $GF(q^m)$, only Goppa codes become cyclic when extended by an overall parity check.

Proof. From Chapter II (matrix 1.4.4) the parity check matrix for this case can be written as

$$H = \begin{bmatrix} \frac{x_1}{(\beta-\alpha_1)} & \frac{x_2}{(\beta-\alpha_2)} & \cdots & \frac{x_n}{(\beta-\alpha_n)} \\ \frac{x_2}{(\beta^n-\alpha_1)} & \frac{x_2}{(\beta^n-\alpha_2)} & \cdots & \frac{x_n}{(\beta^n-\alpha_n)} \end{bmatrix} \qquad 1.2.2$$

where $n = q^m$, $x_i = p_i L'^{-1}(\alpha_i)$.

Consider the element from row 1, column i. If this term is raised to the q^mth power we have:

$$\left(\frac{x_i}{(\beta-\alpha_1)}\right)^{q^m} = \frac{{x_i}^{q^m}}{\beta^{q^m}-{\alpha_i}^{q^m}} \qquad 1.2.3$$

Then since the $x_i, \alpha_i \in GF(q^m)$ it is true that ${x_i}^{q^m} = x_i$ and ${\alpha_i}^{q^m} = \alpha_i$. Therefore

$$\left(\frac{x_i}{(\beta-\alpha_i)}\right)^{q^m} = \frac{x_i}{\beta^{q^m}-\alpha_i} \qquad 1.2.4$$

which is the element of row 2, column i. Thus it can be seen that the row formed by the conjugate root of β, β^{q^m} is equivalent to the row formed by β raised to the q^mth power. Hence the second row is dependent on the first

and the matrix can be written as

$$H = \left[\frac{x_1}{(\beta-\alpha_1)} \quad \frac{x_2}{(\beta-\alpha_2)} \quad \cdots \quad \frac{x_n}{(\beta-\alpha_n)} \right] \qquad 1.2.5$$

Extending H by an overall parity check gives us

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & \frac{x_1}{(\beta-\alpha_1)} & \frac{x_2}{(\beta-\alpha_2)} & & \frac{x_n}{(\beta-\alpha_n)} \end{bmatrix} \qquad 1.2.6$$

Since any cyclic code can be represented by a matrix of the form shown in Chapter II (matrix 1.5.5) where all elements in the first column are 1, let us put H_E into the same form. Most generally:

$$H_E = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1+\frac{kx_1}{(\beta-\alpha_1)} & 1+\frac{kx_2}{(\beta-\alpha_2)} & \cdots & 1+\frac{kx_n}{(\beta-\alpha_n)} \end{bmatrix} \qquad 1.2.7$$

where $k \in GF(q^{2m})$

If this code is to be cyclic, the second row must consist of all the distinct $(n+1)$th roots of unity. Without loss of generality we can reorder the location set L such that:

$$1 + \frac{kx_i}{(\beta-\alpha_i)} = \gamma^{(n-1)i} \qquad 1.2.8$$

where γ is primitive in $GF(q^{2m})$, $n = q^m$.

Thus, for a cyclic code:

$$1 + \frac{kx_i}{(\beta-\alpha_i)}^{n+1} = 1 \qquad 1.2.9$$

for $i = 1,2,\ldots,n$.

Equivalently

$$\left(1 + \frac{kx_i}{(\beta-\alpha_i)}\right)^n \left(1 + \frac{kx_i}{(\beta-\alpha_i)}\right) = 1 \qquad 1.2.10$$

or

$$\left(1 + \frac{k^n x_i}{(\beta^n-\alpha_i)}\right)\left(1 + \frac{kx_i}{(\beta-\alpha_i)}\right) = 1 \qquad 1.2.11$$

and

$$\frac{(\beta^n-\alpha_i+k^n x_i)}{(\beta^n-\alpha_i)} \frac{(\beta-\alpha_i+kx_i)}{(\beta-\alpha_i)} - 1 = 0 \qquad 1.2.12$$

Thus:

$$\frac{k^{n+1}x_i^{\,2}+k^n x_i(\beta-\alpha_i)+kx_i(\beta^n-\alpha_i)}{(\beta^n-\alpha_i)(\beta-\alpha_i)} = 0 \qquad 1.2.13$$

Reordering and simplifying:

$$k^{n+1}x_i-\alpha_i(k^n+k)+k^n+{}^n k = 0 \qquad 1.2.14$$

Solving for x_i

$$x_i = \alpha_i\frac{(k^n+k)-(\beta k^n+\beta^n k)}{k^n+1} \qquad 1.2.15$$

Assume that for $i \neq j$, $i \neq k$; $x_j = x_k$. Solving for x_j we have:

$$x_j = \frac{\alpha_j(k^n+k)-(\beta k^n+\beta^n k)}{k^n+1}$$

$$= \frac{\alpha_k(k^n+k)-(\beta k^n+\beta^n k)}{k^n+1} \qquad 1.2.16$$

This gives

$$\alpha_j(k^n+k) = \alpha_k(k^n+k) \qquad 1.2.17$$

and since $\alpha_j \neq \alpha_k$ this implies that $k^n+k = 0$ and $k^n=-k$. Replacing k^n in equation 1.2.15 by $(-k)$ gives:

$$x_i = \frac{k(\beta-\beta^n)}{-k^2} = \frac{\beta^n-\beta}{k} \qquad 1.2.18$$

Thus, if the extended code is cyclic and if any two x_i's are alike, then all x_i's are alike and equal to $(\beta^{q^m}-\beta)/k$. This is equivalent to the statement that if the extended code is cyclic and any two x_i's are equal, the code before extension must have been a Goppa code.

Thus, for generalized Goppa codes which are not Goppa codes, if they are to be cyclic after extension then all the x_i must be different. $x_i \neq x_j$ for $i \neq j$. Since $\{x_i \mid 1 \leq i \leq q^m\} = q^m$ and $x_i \in GF(q^m)-\{0\}$ which has order (q^m-1) there is no way to pick q^m distinct x_i's and hence these codes are not cyclic.

Concluding, any generalized Goppa code with L = $GF(q^m)$ and g(z) an irreducible quadratic polynomial which is to be cyclic by extension, must have $x_i = x_j$ for some $i \neq j$. Hence, by reasoning above, it must be a Goppa code which is known to be cyclic after extension. Q.E.D.

We can continue with the same reasoning on the case where deg[g(z)]>2 and pose the following:

Corollary 1. No generalized Goppa code with L = $GF(q^m)$ and g(z) an irreducible polynomial over $GF(q^m)$ of degree s>2 can be made cyclic by extension with an overall parity check.

Proof. As in the case where deg[g(z)] = 2, the rows of the parity check matrix generated by the conjugate roots $\beta, \beta^{q^m}, \ldots \beta^{q^{(r-1)m}}$ are equivalent and only one need be included in the H matrix. Also as in the proof of Theorem 1, our defining condition for the extended code to be cyclic is equation 1.2.15 and we get again that $x_i = (\beta^n-\beta)/k$ for all i. Thus if any codes can be made cyclic they must be Goppa codes. Proceeding as in [6] we have

$$x_i k = \beta^n - \beta \qquad 1.2.19$$

$$\text{Now } (x_i k)^n = (\beta^n-\beta)^n = -x_i k = -(\beta^n-\beta) \qquad 1.2.20$$

$$\text{or} \quad \beta^{2n}-\beta^n+\beta^n-\beta = 0 \qquad 1.2.21$$

Remembering that $n=q^m$ this gives $\beta^{2q^m} = \beta$.

Hence g(z) must be quadratic. Q.E.D.

Concluding, the only full length generalized Goppa codes which can be extended to be cyclic are Goppa codes with g(z) an irreducible quadratic polynomial.

CHAPTER IV

GENERALIZED GOPPA CODES WITH L⊂GF(q^m)

1. Generalized Goppa Codes with L = GF(q^m)-{β}

For generalized Goppa Codes with L = GF(q^m)-{β}, there exists a subclass of codes with $g(z) = (z-\beta)^a$ and $P(z) = [L'(z)]^b$ which is cyclic as proved in the following:

Theorem 2. If C is a generalized Goppa Code with L = GF(q^m)-{β} and $g(z) = (z-\beta)^a$ and $P(z) = [L'(z)]^b$ where a is any positive integer $< q^m-2$, and b is any integer relatively prime to q^m-1, then the code is cyclic.

Proof. The parity check matrix for this code is of the form:

$$H = \begin{bmatrix} \frac{1}{\beta-\alpha_1} & \frac{1}{\beta-\alpha_2} & \cdots & \frac{1}{(\beta-\alpha_n)} \\ \vdots & \vdots & & \vdots \\ \frac{1}{(\beta-\alpha_1)^a} & \frac{1}{(\beta-\alpha)^a} & \cdots & \frac{1}{(\beta-\alpha_n)^a} \end{bmatrix} \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x_n \end{bmatrix} \quad 1.1$$

where $x_i = p_i L'^{-1}(\alpha_i)$ and $n = q^m-1$. Since $p_i = [L'(\alpha_i)]^b$ we have that $x_i = L'^{b-1}(\alpha_i)$.

Let us determine what $L'(\alpha_i)$ is for this case. Since

$$L(z) = \prod_{j=1}^{n} (Z-\alpha_i) \text{ where } \alpha_i \in L$$

and L = GF(q^m)-{β} for this case, we can rewrite L(z) as

$$L(z) = \frac{z^{q^m} - z}{z-\beta} \qquad 1.2$$

Taking the derivative, we get

$$L'(z) = \frac{-1}{(z-\beta)} - \frac{z^{q^m} - z}{(z-\beta)^2}$$

$$= \frac{-1}{(z-\beta)} - \frac{L(z)}{(z-\beta)} \qquad 1.3$$

Thus since $L(\alpha_i) = 0$ for all $\alpha_i \in L$ we have

$$L'(\alpha_i) = \frac{1}{(\alpha_i-\beta)} = \frac{1}{(\beta-\alpha_i)} \qquad 1.4$$

Using this result, it is true that

$$x_i = \frac{1}{(\beta-\alpha_i)^{b-1}} \qquad 1.5$$

and matrix 1.1 can be rewritten as:

$$H = \begin{bmatrix} \frac{1}{(\beta-\alpha_1)^b} & \frac{1}{(\beta-\alpha_2)^b} & \cdots & \frac{1}{(\beta-\alpha_n)^b} \\ \vdots & \vdots & & \vdots \\ \frac{1}{(\beta-\alpha_1)^{a+b-1}} & \frac{1}{(\beta-\alpha_2)^{a+b-1}} & \cdots & \frac{1}{(\beta-\alpha_n)^{a+b-1}} \end{bmatrix} \qquad 1.6$$

The elements $(\beta-\alpha_i)^{-1}$ for $1 \leq i \leq q^m - 1$ are all the non-zero elements of $GF(q^m)$. Therefore the α_i can be ordered such that matrix 1.6 is equal to

$$H = \begin{bmatrix} 1 & \gamma^{b} & \gamma^{2b} & \cdots & \gamma^{(n-1)^{n}} \\ 1 & \gamma^{b+1} & \gamma^{(b+1)} & \cdots & \gamma^{(n-1)(b+1)} \\ \vdots & & & & \\ 1 & \gamma^{b+a-1} & \gamma^{2(b+a-1)} & \cdots & \gamma^{(n-1)(b+a-1)} \end{bmatrix} \quad 1.7$$

for γ a primitive element of $GF(q^m)$. Since $\gamma^n = 1$, the code is cyclic Q.E.D.

For the case where b = 1 we have $P(z) = L'(z)$ and $x_i = 1$ for all i. Thus for this case, the codes degenerate to Goppa Codes.

Example 1. Let $L = GF(3^2) - \{1\} = 0, \alpha^5, \alpha^3, \alpha^7, \alpha^4, \alpha^6, \alpha, \alpha^2$ where α is primitive in $GF(3^2)$ and $\alpha^2 + \alpha + 2 = 0$. Let $g(z) = (z-1)^3$ and $P(z) = [L'(z)]^3 = (1-z)^{-3}$.

The elements of $GF(3^2)$ are

0

1

α

$\alpha^2 = 2\alpha + 1$

$\alpha^3 = 2\alpha + 2$

$\alpha^4 = 2$

$\alpha^5 = 2\alpha$

$\alpha^6 = \alpha + 2$

$\alpha^7 = \alpha + 1$

From matrix 1.6

$$H = \begin{bmatrix} (1+0)^{-3} & (1-\alpha^5)^{-3} & (1-\alpha^3)^{-3} & (1-\alpha^7)^{-3} & (1-\alpha^4)^{-3} \\ (1-0)^{-4} & (1-\alpha^5)^{-4} & (1-\alpha^3)^{-4} & (1-\alpha^7)^{-4} & (1-\alpha^4)^{-4} \\ (1-0)^{-5} & (1-\alpha^5)^{-5} & (1-\alpha^3)^{-5} & (1-\alpha^7)^{-5} & (1-\alpha^4)^{-5} \end{bmatrix}$$

$$\begin{bmatrix} (1-\alpha^6)^{-3} & (1-\alpha\ )^{-3} & (1-\alpha^2)^{-3} \\ (1-\alpha^6)^{-4} & (1-\alpha\ )^{-4} & (1-\alpha^2)^{-4} \\ (1-\alpha^6)^{-5} & (1-\alpha\ )^{-5} & (1-\alpha^2)^{-5} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \\ 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 \\ 1 & \alpha^5 & \alpha^2 & \alpha^7 & \alpha^4 & \alpha & \alpha^6 & \alpha^3 \end{bmatrix}$$

This generalized Goppa Code is an (8,3) cyclic code over GF(3).

2. Generalized Goppa Codes with $L = GF(q^m) - \{\beta_1, \beta_2\}$

Let C be a generalized Goppa Code with $L = GF(q^m) - \{\beta_1, \beta_2\}$ and $g(z) = (z-\beta_1)(z-\beta_2)$ with P(z) to be defined. One form of the parity check matrix for this code is:

$$H = \begin{bmatrix} \frac{x_1}{(\beta_1-\alpha_1)} & \frac{x_2}{(\beta_1-\alpha_2)} & \cdots & \frac{x_n}{(\beta_1-\alpha_n)} \\ \frac{x_1}{(\beta_2-\alpha_1)} & \frac{x_1}{(\beta_2-\alpha_2)} & \cdots & \frac{x_n}{(\beta_2-\alpha_n)} \end{bmatrix} \qquad 2.1$$

which after extending by an overall parity check can be represented as:

$$H_E = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1+\frac{x_1}{(\beta_1-\alpha_1)} & \cdots & 1+\frac{x_n}{(\beta_1-\alpha_n)} \\ 1 & 1+\frac{k_1x_1}{(\beta_1-\alpha_1)}+\frac{k_2x_1}{(\beta_2-\alpha_1)} & \cdots & 1+\frac{k_1x_n}{(\beta_1-\alpha_n)}+\frac{k_2x_n}{(\beta_2-\alpha_n)} \end{bmatrix} \quad 2.2$$

where k_1, k_2 are elements of an extension field of $GF(q^m)$, $k_2 \neq 0$. For any ordering of the location set, the x_i can be picked so that

$$1 + \frac{x_i}{(\beta_1-\alpha_i)} = \gamma^i \quad 2.3$$

where γ is primitive in $GF(q^m)$. Solving for x_i we get

$$x_i = (\gamma^i-1)(\beta_1-\alpha_i) \quad 2.4$$

If k_1 and k_2 are such that

$$1 + \frac{k_1x_i}{(\beta_1-\alpha_i)} + \frac{k_2x_i}{(\beta_2-\alpha_i)} = \gamma^{di} \quad 2.5$$

then the extended code will be cyclic.

Substituting x_i from equation 2.4 into equation 2.5 we have

$$1+k_1(\gamma^i-1) + k_2\frac{(\gamma^i-1)(\beta_1-\alpha_1)}{(\beta_2-\alpha_i)} = \gamma^{di} \quad 2.6$$

This gives

$$k_1+k_2\,\frac{(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)} = \frac{\gamma^{di}-1}{\gamma^{i}-1} \qquad 2.7$$

and, solving for α_i in the above equation we have

$$k_2(\beta_1-\alpha_i) = [(\gamma^{di}-1)/(\gamma^{i}-1)-k_1](\beta_2-\alpha_i)$$

giving

$$\alpha_i = \frac{k_2\beta_1-[(\gamma^{di}-1)/(\gamma^{i}-1)-k_1]\beta_2}{k_1+k_2-(\gamma^{di}-1)/(\gamma^{i}-1)} \qquad 2.8$$

Substituting α_i from equation 2.8 into equation 2.4 we get

$$x_i = (\gamma^{i}-1)\,\frac{\beta_1[k_1+k_2-\frac{\gamma^{di}-1}{\gamma^{i}-1}]-k_2\beta_1+[\frac{\gamma^{di}-1}{\gamma^{i}-1}-k_1]\beta_2}{k_1+k_2-(\gamma^{di}-1)/(\gamma^{i}-1)}$$

$$x_i = \frac{[(\gamma^{di}-1)/(\gamma^{i}-1)-k_1](\beta_2-\beta_1)(\gamma^{i}-1)}{k_2+k_1-(\gamma^{di}-1)/(\gamma^{i}-1)} \qquad 2.9$$

From equation 2.7 we can determine if there exists k_1 and k_2 for different values of d. If, for a given value of d, k_1 and k_2 can be found we can determine the necessary α_i and x_i and hence P(z) for the code from equations 2.8 and 2.9 respectively.

2.1 Case 1 : d=2

Consider the case where d=2. For this case equation 2.7 becomes

$$k_1+k_2\frac{(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)} = \frac{\gamma^{2i}-1}{\gamma^i-1} = \gamma^i+1 \qquad 2.1.1$$

Let us determine the elements of the set $\{\gamma^i+1 \mid 1\leq i\leq n\}$ where $n=q^m-2$. For $1\leq i\leq n$, γ^i takes on all values of $GF(q^m)$ except 0 and 1. Therefore $\{\gamma^i+1 \mid 1\leq i\leq n\}$ is equal to $GF(q^m)-\{1,2\}$.

Now, if there exists k_1 and k_2 such that the set $\{k_1+k_2(\beta_1-\alpha_i)/(\beta_2-\alpha_i) \mid 1\leq i\leq n\}$ is equal to $\{\gamma^i+1 \mid 1\leq i\leq n\}$ then for some ordering of the location set the extended code will be cyclic.

For any q, the set $\{(\beta_1-\alpha_i)/(\beta_2-\alpha_i) \mid 1\leq i\leq n\}$ consists of all the elements of $GF(q^m)$ except 0 and 1 (since $\beta_1\neq\alpha_i$ and $\beta_1-\alpha_i\neq\beta_2-\alpha_i$ for all i). Repeating,

$$\{\frac{(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)} \mid 1\leq i\leq n\} = GF(q^m)-\{0,1\} \qquad 2.1.2$$

The set $\{k_1+k_2(\beta_1-\alpha_i)/(\beta_2-\alpha_i) \mid 1\leq i\leq n\}$ is equal to $GF(q^m)-\{1,2\}$ if $k_1=1$, $k_2=1$ or $k_1=2$, $k_2=-1$.

Let us first set $k_1=1$ and $k_2=1$ in equation 2.9 with d=2. In so doing, we get

$$x_i = \frac{\gamma^i(\beta_2-\beta_1)(\gamma^i-1)}{2-(\gamma^i+1)} = \frac{\gamma^i(\beta_2-\beta_1)(\gamma^i-1)}{-(\gamma^i-1)}$$

$$= \gamma^i(\beta_1-\beta_2) \qquad 2.1.3$$

From the above and from equation 2.4 we have

$$x_i = \frac{(\beta_1-\beta_2)(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)} \qquad 2.1.4$$

Thus the code with $L = GF(q^m)-\{\beta_1,\beta_2\}$ and $g(z) = (z-\beta_1)(z-\beta_2)$ will be cyclic for some ordering of the location set if the x_i are defined as in equation 2.1.4. To determine P(z) for this code we must first determine $L'(z)$.

For the code with $L = GF(q^m)-\{\beta_1,\beta_2\}$ it is true that

$$L(z) = \frac{(z^{q^m}-z)}{(z-\beta_1)(z-\beta_2)} \qquad 2.1.5$$

Thus

$$L'(z) = \frac{1}{(z-\beta_1)(z-\beta_2)} - \frac{L(z)}{(z-\beta_1)} + \frac{L(z)}{(z-\beta_2)}$$

Since the second term is zero for all $\alpha_i \in L$, we have

$$L'(\alpha_i) = -\frac{1}{(\alpha_i-\beta_1)(\alpha_i-\beta_2)} \quad \text{for all } \alpha_i \in L \qquad 2.1.6$$

Now

$$P_i = x_i L'(\alpha_i) \qquad 2.1.7$$

$$= (\beta_1-\beta_2)\frac{(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)} \quad \frac{-1}{(\beta_1-\alpha_i)(\beta_2-\alpha_i)}$$

$$= \frac{\beta_2-\beta_1}{(\beta_2-\alpha_i)^2} \qquad 2.1.8$$

Thus it can be seen that

$$P(z) = \frac{k}{(z-\beta)^2} \qquad 2.1.9$$

where $k = (\beta_2-\beta_1)$.

Now, since multiplying any row of the parity-check matrix by a constant will not change the code, we have proven the following:

Theorem 2. For the generalized goppa codes with $L = GF(q^m)-\{\beta_1,\beta_2\}$, $g(z) = (z-\beta_1)(z-\beta_2)$ and $P(z) = k/(z-\beta_2)^2$ the code after extension is equivalent to a cyclic code with the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \gamma & \gamma^2 & \cdots & \gamma^n \\ 1 & \gamma^2 & \gamma^4 & & \gamma^{2n} \end{bmatrix}$$

where k is any non-zero element of $GF(q^m)$ and γ is a primitive element of $GF(q^m)$.

Example 2. Let $L = GF(2^3)-\{0,\alpha\}$, $g(z) = (z-0)(z-\alpha)$ and 1) $P(z) = (z-\beta_2)^2$.

The elements of $GF(2^3)$ with α primitive and $\alpha^3+\alpha+1 = 0$ are

0	$\alpha^3 = \alpha+1$
1	$\alpha^4 = \alpha^2+\alpha$
α	$\alpha^5 = \alpha^2+\alpha+1$
α^2	$\alpha^6 = \alpha^2+1$

Let $a_1 = \alpha^6, a_2 = \alpha^4, a_3 = \alpha^3, a_4 = 1, a_5 = \alpha^2, a_6 = \alpha^5$

and $x_i = (a_1 - a_2)(a_1 - a_i)/(a_2 - a_i)$

$x_1 = \alpha^2, x_2 = \alpha^3, x_3 = \alpha^4, x_4 = \alpha^5, x_5 = \alpha^6, x_6 = 1$

Then:

$$H = \begin{bmatrix} \frac{\alpha^2}{(\alpha^6-0)} & \frac{\alpha^3}{(\alpha^4-0)} & \frac{\alpha^4}{(\alpha^3-0)} & \frac{\alpha^5}{(1-0)} & \frac{\alpha^6}{(\alpha^2-0)} & \frac{1}{(\alpha^5-0)} \\ \frac{\alpha^2}{(\alpha^6-\alpha)} & \frac{\alpha^3}{(\alpha^4-\alpha)} & \frac{\alpha^4}{(\alpha^3-\alpha)} & \frac{\alpha^5}{(1-\alpha)} & \frac{\alpha^6}{(\alpha^2-\alpha)} & \frac{1}{(\alpha^5-\alpha)} \end{bmatrix}$$

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha & \alpha^5 & \alpha^4 & \alpha^2 \\ 0 & \alpha^4 & \alpha & \alpha^4 & \alpha^2 & \alpha^2 & \alpha \end{bmatrix}$$

Putting this matrix in the form of matrix 2.2 with $k_1 = k_2 = 1$ we have

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1+\alpha^3 & 1+\alpha^6 & 1+\alpha & 1+\alpha^5 & 1+\alpha^4 & 1+\alpha^2 \\ 1 & 1+\alpha^3+\alpha^4 & 1+\alpha^6+\alpha & 1+\alpha+\alpha^4 & 1+\alpha^6+\alpha^2 & 1+\alpha^4+\alpha^2 & 1+\alpha^2+\alpha \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix}$$

which is a (7,3) cyclic code.

Let us consider the other possibility for k_1 and k_2 for the codes under examination. Setting $k_1=2$ and $k_2=-1$ in equation 2.9 gives

$$x_i = \frac{(\gamma^i-1)(\beta_2-\beta_1)(\gamma^i-1)}{-\gamma^i}$$

$$= \frac{(\gamma^i-1)^2(\beta_1-\beta_2)}{\gamma^i}$$

Substituting for γ^i above, from equation 2.3, we get

$$x_i = \frac{x_i^2}{(\beta_1-\alpha_i)^2} \quad \frac{(\beta_1-\beta_2)}{(x+\beta_1-\alpha_i)} \quad (\beta_1-\alpha_i) \qquad 2.1.10$$

or:

$$(\beta_1-\alpha_i)(x_i+\beta_1-\alpha_i) = x_i(\beta_1-\beta_2)$$

$$x_i(\beta_1-\alpha_i+\beta_2-\beta_1) = -(\beta_1-\alpha_i)^2$$

finally:

$$x_i = \frac{-(\beta_1-\alpha_i)^2}{(\beta_2-\alpha_i)} \qquad 2.1.11$$

and $$\gamma_i = 1 - \frac{(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)} = \frac{(\beta_2-\beta_1)}{(\beta_2-\alpha_i)} \qquad 2.1.12$$

Solving for P(z)

$$P_i = x_i L'(\alpha_i)$$

$$= \frac{(\beta_1-\alpha_i)^2}{(\beta_2-\alpha_i)} \quad \frac{-1}{\beta_1-\alpha_i)(\beta_2-\alpha_i)}$$

$$= \frac{(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)}^{-2} \qquad 2.1.13$$

Hence

$$P(z) = -\frac{(z-\beta_1)}{(z-\beta_2)}^2 \qquad 2.1.14$$

This proves the following:

Theorem 3. The generalized Goppa codes with $L=GF(q^m)-\{\beta_1,\beta_2\}$, $g(z) = (z-\beta_1)(z-\beta_2)$ and $P(z) = k(z-\beta_1)(z-\beta_2)^{-2}$ can be made cyclic by extension with the resulting parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \gamma & \gamma^2 & \cdots & \gamma^n \\ 1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{2n} \end{bmatrix} \qquad 2.1.15$$

Example 3. Let us modify the code in example 2 by making $P(z) = (z-\beta_1)(z-\beta_2)^{-2}$.

Let $\alpha_1 = \alpha^3$, $\alpha_2 = \alpha^5$, $\alpha_3 = \alpha^6$, $\alpha_4 = \alpha^2$, $\alpha_5 = 1$, $\alpha_6 = \alpha^4$

and $x_i = -(\beta_1-\alpha_i)^2/(\beta_2-\alpha_i)$

$x_i = \alpha^6$, $x_2 = \alpha^4$, $x_3 = 1$, $x_4 = 1$, $x_5 = \alpha^4$, $x_6 = \alpha^6$

$$H = \begin{bmatrix} \frac{\alpha^6}{(\alpha^3-0)} & \frac{\alpha^4}{(\alpha^5-0)} & \frac{1}{(\alpha^5-0)} & \frac{1}{(\alpha^2-0)} & \frac{\alpha^4}{(1-0)} & \frac{\alpha^6}{(\alpha^4-0)} \\ \frac{\alpha^6}{(\alpha^3-\alpha)} & \frac{\alpha^4}{(\alpha^5-\alpha)} & \frac{1}{(\alpha^6-\alpha)} & \frac{1}{(\alpha^3-\alpha)} & \frac{\alpha^4}{(1-\alpha)} & \frac{\alpha^6}{(\alpha^4-\alpha)} \end{bmatrix}$$

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha & \alpha^5 & \alpha^4 & \alpha^2 \\ 0 & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^3 & \alpha & \alpha^4 \end{bmatrix}$$

Now with $k_2=1$, $k_1=0$ we have

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1+\alpha^3 & 1+\alpha^6 & 1+\alpha & 1+\alpha^5 & 1+\alpha^4 & 1+\alpha^2 \\ 1 & 1+\alpha^6 & 1+\alpha^5 & 1+\alpha^2 & 1+\alpha^3 & 1+\alpha & 1+\alpha^4 \end{bmatrix}$$

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix}$$

2.2 Case 2: d = -1

Consider the case where d = -1. For this case, after extension, the codes can be set equal to the cyclic codes with

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^n \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-n} \end{bmatrix} \qquad 2.2.1$$

The defining condition for these codes, equation 2.1.7, becomes

$$k_1 + k_2 \frac{(\beta_1 - \alpha_i)}{(\beta_2 - \alpha_i)} = \frac{\gamma^{-i} - 1}{\gamma^i - 1} = -\frac{1}{\gamma^i} \qquad 2.2.2$$

and the set $\{-\gamma^{-i} \mid 1 \leq i \leq q^m - 2\} = GF(q^m) - \{0, -1\}$.
Thus the parity check matrix for the code C can be put in the form of a cyclic code if the set

$$\{k_1 + k_2 \frac{(\beta_1 - \alpha_i)}{(\beta_2 - \alpha_i)} \mid 1 \leq i \leq q^m - 2\} \text{ is equal to } GF(q^m) - \{0, -1\}$$

This will be true if (1) $k_1 = 0$, $k_2 = -1$ or (2) $k_1 = -1$, $k_2 = 1$.
If (1) $k_1 = 0$, $k_2 = -1$ equation 2.1.10 becomes

$$x_i = -\frac{\gamma^{-i}(\beta_2 - \beta_1)(\gamma^i - 1)}{-1 + \gamma^{-i}} = (\beta_2 - \beta_1) \qquad 2.2.3$$

For this case the x_i's are equal to a constant and the code is an extended Goppa code as described by Tzeng and Zimmermann [4].

If (2) $k_1 = -1$, $k_2 = 1$ equation 2.1.10 becomes

$$x_i = \frac{[-\gamma^{-i}+1](\beta_2-\beta_1)(\gamma^i-1)}{+\gamma^{-i}} \qquad 2.2.4$$

$$= (\gamma^i-1)^2(\beta_2-\beta_1) \qquad 2.2.5$$

Substituting for (γ^i-1) from equation 2.1.4. we have

$$x_i = \frac{x_i^2(\beta_2-\beta_1)}{(\beta_1-\alpha_i)^2} \qquad 2.2.6$$

$$x_i = \frac{(\beta_1-\alpha_i)^2}{(\beta_2-\beta_i)} \qquad 2.2.7$$

Solving for p_i

$$p_i = \frac{(\beta_1-\alpha_i)^2}{(\beta_2-\beta_1)} \quad \frac{-1}{(\beta_1-\alpha_i)(\beta_2-\alpha_i)} \qquad 2.2.8$$

$$= \frac{(\beta_1-\alpha_i)}{(\beta_2-\alpha_i)(\beta_1-\beta_2)} \qquad 2.2.9$$

Thus the code is cyclic when

$$P(z) = k\frac{(z-\beta_1)}{(z-\beta_2)}$$

which proves:

Theorem 4. The generalized Goppa codes with $L = GF(q^m) - \{\beta_1, \beta_2\}$, $g(z) = (z-\beta_1)(z-\beta_2)$ and $P(z) = k(z-\beta_1)/(z-\beta_2)$ can be made cyclic when extended by an overall parity check with

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \gamma & \gamma^2 & \cdots & \gamma^n \\ 1 & \gamma^{-1} & \gamma^{-2} & \cdots & \gamma^{-n} \end{bmatrix}$$

where γ is primitive in $GF(q^m)$.

Example 3. Let L and g(z) be as in example 2, and $P(z) = \frac{(z-\beta_1)}{(z-\beta_2)} = \frac{(z-0)}{(z-\alpha)}$

Let $\alpha_1 = \alpha^4$, $\alpha_2 = 1$, $\alpha_3 = \alpha^2$, $\alpha_4 = \alpha^6$, $\alpha_5 = \alpha^5$, $\alpha_6 = \alpha^5$

$$H = \begin{bmatrix} \frac{1}{(\alpha^4-0)} & \frac{\alpha^6}{(1-0)} & \frac{\alpha^3}{(\alpha^2-0)} & \frac{\alpha^4}{(\alpha^6-0)} & \frac{\alpha^2}{(\alpha^3-0)} & \frac{\alpha^5}{(\alpha^3-0)} \\ \frac{1}{(\alpha^4-\alpha)} & \frac{\alpha^6}{(1-\alpha)} & \frac{\alpha^3}{(\alpha^2-\alpha)} & \frac{\alpha^4}{(\alpha^6-\alpha)} & \frac{\alpha^2}{(\alpha^5-\alpha)} & \frac{\alpha^5}{(\alpha^3-\alpha)} \end{bmatrix}$$

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha & \alpha^5 & \alpha^4 & \alpha^2 \\ 0 & \alpha^5 & \alpha^3 & \alpha^6 & \alpha^6 & \alpha^3 & \alpha^5 \end{bmatrix}$$

Now with $k_1 = -1$, $k_2 = 1$ we have

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1+\alpha^3 & 1+\alpha^6 & 1+\alpha & 1+\alpha^5 \\ 1 & 1-\alpha^3+\alpha^5 & 1-\alpha^6+\alpha^3 & 1-\alpha+\alpha^6 & 1-\alpha^5+\alpha^6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1+\alpha^4 & 1+\alpha^2 \\ 1-\alpha^4+\alpha^3 & 1-\alpha^2+\alpha^5 \end{bmatrix}$$

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix}$$

CHAPTER V

CONCLUSIONS

1. Results

A new form of the parity-check matrix for generalized Goppa codes is shown. This form is similar to that derived by Tzeng and Zimmermann [4] for Goppa codes. The matrix in this form facilitates comparison between generalized Goppa codes and cyclic codes and by means of it, the following results have been obtained.

1) For generalized Goppa codes with $L = GF(q^m)$ and $g(z) = m(z)$ is the minimum polynomial of some nonzero element β over $GF(q^{rm})$ and $P(z)$ a polynomial with coefficients in $GF(q^m)$, relatively prime to $L(z)$, the following statement can be made. Of this class of codes, the only codes that can be made cyclic by extension are in the subclass of Goppa codes. They are the Goppa codes with $g(z)$ a quadratic ($r=2$). The Goppa codes are generalized-Goppa codes with $P(z) = L'(z)$ where $L'(x)$ is the derivative of $L(z)$, the location polynomial.

2) For generalized-Goppa codes with $L = GF(q^m)-\{\beta\}$, $g(z) = (z-\beta)^a$ and $P(z) = [L'(z)]^b$ where a is a positive integer and b is any integer relative prime to q^m-1, the codes are shown to be cyclic.

3) For generalized-Goppa codes with $L = GF(q^m)-\{\beta_1,\beta_2\}$, $g(z) = (z-\beta_1)(z-\beta_2)$ and $P(z) = k/(z-\beta_2)^2$ where

k is any element from an extension field of $GF(q^m)$ the code can be made cyclic by the addition of an overall parity check.

4) For generalized-Goppa codes with $L = GF(q^m) - \{\beta_1, \beta_2\}$, $g(z) = (z-\beta_1)(z-\beta_2)$ and $P(z) = k(z-\beta)/(z-\beta_2)^2$ the code can be extended to be cyclic.

5) For generalized Goppa codes with $L = GF(q^m) - \{\beta_1, \beta_2\}$, $g(z) = (z-\beta_1)(z-\beta_2)$ and $P(z) = k(z-\beta_1)/(z-\beta_2)$, the code after extension by an overall parity check is cyclic.

2. Further Research

The investigation for this presentation has uncovered other problems for further study in the area of generalized Goppa codes and their relation to cyclic codes. Some of these are presented below.

For the case of codes considered in Chapter IV, section 2, it was determined that there existed codes that after extension could be put into the form of

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \gamma & \gamma^2 & & \gamma^n \\ 1 & \gamma^d & \gamma^{2d} & & \gamma^{2n} \end{bmatrix}$$

for values of $d = 2$ and $d = 1$, it can be shown that there are codes that cannot be put in this form by manipulation of matrix 2.2 (Chapter IV) for $d \neq 2$ or -1.

However, matrix 2.2 is not the most general form of the parity check matrix for these codes. It remains to be seen what results can be achieved for the parity check matrix in its most general form.

Also for the codes considered in Chapter IV, section 2, it remains to be seen if the codes can be made cyclic by extension when $g(z) = [(z-\beta_1)(z-\beta_2)]^a$ where a is an integer > 1.

Finally, the relationships between generalized Goppa codes and shortened cyclic codes or nonprimitive cyclic codes remain to be examined.

REFERENCES

1. Goppa, V. D., "A new class of linear error-correcting codes," Probl. Pederach. Inform., Vol. 6 #3, 24-30, 1970.

2. Goppa, V. D., "Rational representation of codes and (L,G) codes," Probl. Pederach. Inform., Vol. 7 #3, 41-49, 1971.

3. Tzeng, K. K., and Zimmermann, K., "LaGrange's interpolation formula and generalized Goppa Codes," IEEE Intl. Symp. Inform. Theory, Ronneby, Sweden, June 1976.

4. Tzeng, K. K., and Zimmerman, K., "On extending Goppa Codes to Cyclic Codes," IEEE Trans., IT-19, 712-716, Nov., 1975.

5. Berlekamp, E. R., and Moreno, O., "Extended double-error-correcting binary Goppa codes are cyclic," IEEE Trans., IT-19, 817-818, 1973.

6. Tzeng, K. K., and Yu, C. Y., "Characterization theorems for extending Goppa Codes to Cyclic Codes," Proc. 1975 Conf. on Info. Sciences and Systems, 401-404, Johns Hopkins U., 1975.

7. Chen, C. L., "Equivalent irreducible Goppa Codes," IEEE Intl. Symp. on Info. Theory, Ithaca, NY, Oct. 1977.

8. Peterson, W. W., and Welden, E. J., "Error-correcting codes," 2nd ed., MIT Press, Cambridge, MA, 1972.

9. Lin, S., "An introduction to error-correcting codes," Prentice-Hall, Englewood, CA, 1970.

10. Shannon, C. E., and Weaver, W., "A Mathematical Theory of Communication," BSTJ, 27, 1948.

VITA

Place of birth:	Tamaqua, Pennsylvania
Date of birth:	January 8, 1953
Parents:	Julia and Paul Scheitrum
Education:	Lehigh University, Bethlehem, Pa.
Degrees:	1974 BS in Electrical Engineering
Experience:	1977-1978 Lehigh University, Teaching and Research Assistant
	1974-1976 Aeronutronic-Ford Corp. (formerly Philco-Ford Corp.) Design Engineer