MAJORITY DECODABLE CODES
DERIVED FROM FINITE GEOMETRIES
by
K. J. C. Smith
University of North Carolina
Institute of Statistics Mimeo Series No. 561

December 1967

This research was supported in part by the National Science Foundation Grant No. GP-5790 and the Army Research Office, Durham Grant No. DA-ARD-D-31-124-G910.

DEPARTMENT OF STATISTICS
UNIVERSITY OF NORTH CAROLINA
Chapel Hill, N. C.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>iii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>v</td>
</tr>
<tr>
<td>I INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 The coding problem</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Majority Decoding</td>
<td>3</td>
</tr>
<tr>
<td>II INCIDENCE MATRICES IN FINITE GEOMETRIES</td>
<td>8</td>
</tr>
<tr>
<td>2.1 Introduction</td>
<td>8</td>
</tr>
<tr>
<td>2.2 Rank of an incidence matrix</td>
<td>8</td>
</tr>
<tr>
<td>2.3 Finite fields</td>
<td>10</td>
</tr>
<tr>
<td>2.4 Finite projective geometry PG(t,q)</td>
<td>13</td>
</tr>
<tr>
<td>2.5 Finite affine geometry EG(t,q)</td>
<td>17</td>
</tr>
<tr>
<td>2.6 Incidence matrices of points and (t-1)-flats</td>
<td>21</td>
</tr>
<tr>
<td>2.7 Incidence matrices of points and d-flats in PG(t,q)</td>
<td>36</td>
</tr>
<tr>
<td>2.8 Incidence matrices of points and d-flats in EG(t,q)</td>
<td>54</td>
</tr>
<tr>
<td>III GEOMETRIC CODES</td>
<td>61</td>
</tr>
<tr>
<td>3.1 Introduction</td>
<td>61</td>
</tr>
<tr>
<td>3.2 Cyclic codes</td>
<td>61</td>
</tr>
<tr>
<td>3.3 Majority decoding</td>
<td>67</td>
</tr>
<tr>
<td>3.4 Geometric codes</td>
<td>72</td>
</tr>
<tr>
<td>3.5 Non-primitive geometric codes</td>
<td>86</td>
</tr>
<tr>
<td>3.6 Majority decoding of geometric codes</td>
<td>92</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>105</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

I gratefully acknowledge the guidance and encouragement given me by my adviser, Professor R. C. Bose, during my research. It is a privilege to have attended his stimulating lectures and to study under him in the area of combinatorial mathematics.

I wish also to thank the other members of the faculty of the Department of Statistics who have contributed to my graduate training, in particular Professors I. M. Chakravatri, N. L. Johnson and M. R. Leadbetter. Thanks are also extended to Professor R. R. Kuebler, Jr., for his valuable comments on improving this dissertation and to Professor R. J. Troyer, the other member of my graduate committee.

For financial support during my graduate training, I sincerely thank the Department of Statistics, the National Science Foundation and the U. S. Army Research Office, Durham. To these institutions I gratefully express my appreciation.

I would like to thank Professor D. K. Dale of the Department of Mathematics at Carleton University, Canada, for his encouragement and stimulation of my interest in mathematics and statistics during my undergraduate studies.

For her careful typing of the final manuscript I extend my thanks to Mrs. Margaret Laughlin.
A number of $q$-ary cyclic error-correcting codes to which a majority decoding algorithm is applicable may be called geometric codes in that the incidence vectors of certain flat spaces in the finite projective geometry $PG(t,q)$ or the finite affine geometry $EG(t,q)$ are vectors of the dual code. Such geometric codes are related to incidence matrices of points and $d$-flats in the corresponding geometry. An upper bound is given for the rank of these incidence matrices over $GF(q)$. Exact results are obtained for the case $d = t-1$ and for the case $d \leq t-1$ and prime $q$. Some known geometric cyclic codes are reviewed and several new classes of such codes are constructed. Tables are given which list the parameters of some of the new codes. One-step and multi-step majority decoding algorithms for geometric codes are given. A formula for the number of information symbols in certain Generalized Reed-Muller codes is derived. Some results on the weight distribution of Bose-Chaudhuri-Hocquenghem codes are also obtained.
SUMMARY

The theory of error-correcting codes is concerned with the development of techniques by which messages can be transmitted accurately and efficiently over noisy channels. We shall consider a channel capable of transmitting discrete symbols. A message produced by an information source is encoded into a sequence of symbols which are successively transmitted over the channel. Because of the presence of noise in the channel, a received symbol may differ from the transmitted symbol. At the receiver, an attempt is made to recover the transmitted sequence of symbols, based on the received sequence and the characteristics of the channel. This operation is referred to as decoding.

This dissertation will be concerned with block codes, in which a message corresponds to a block of $k$ symbols. These blocks of $k$ symbols are transformed into blocks of $N = k + r$ symbols, which are then sent over the channel. That is, to each sequence of $k$ information symbols are added $r$ redundant symbols to form a codeword of $N$ symbols. The set of all codewords constitutes the code. The receiver receives the sequence of $N$ symbols, some of which may be in error, and attempts to determine which codeword was transmitted. Because the code does not consist of all possible sequences of $N$ symbols, the occurrence of a few errors does not necessarily change one codeword into another codeword. This allows the receiver frequently to recognize that error has occurred, and to correct a certain number of errors.

We shall assume the channel is capable of transmitting any one of $q$ distinct symbols, where $q$ is a prime power, say $q = p^n$. We put the $q$ symbols into a one-to-one correspondence with the $q$ elements of the
In this case, a block code consists of a subset of \( N \)-vectors with elements from \( \text{GF}(q) \). It is useful to restrict the set of codewords to be a vector subspace of the vector space \( V_N \) of all \( N \)-vectors with elements from \( \text{GF}(q) \). Such a code is called a linear code. The orthogonal complement of a linear code \( C \), in the usual algebraic sense, is also a subspace of \( V_N \) and is referred to as the dual code of \( C \). Each codeword of \( C \) is orthogonal to every vector of the dual code. This fact is used in decoding a linear code.

This dissertation deals primarily with a decoding procedure for certain linear codes called majority decoding, as introduced by Massey [18].

Majority decoding of a linear code is based on a certain "orthogonality structure" the dual code may possess. This orthogonality structure is related to the incidence relationship in an incomplete block design. We may develop this in two directions. First, suppose \( N \) is the \( bxv \) \((0,1)\) incidence matrix of, say, a balanced incomplete block design with \( v \) treatments and \( b \) blocks, each treatment being replicated \( r \) times and any pair of treatments occurring together in \( \lambda \) blocks. The rows of \( N \) generate a vector subspace of the vector space \( V_v \) of all \( v \)-vectors with elements from \( \text{GF}(q) \). The dimension of this subspace is equal to the rank of \( N \) over \( \text{GF}(q) \). We may consider this subspace as the dual code of a linear code \( C \) of length \( v \) and redundancy equal to the rank of \( N \) over \( \text{GF}(q) \). In Chapter III we will describe a majority decoding procedure which may be applied to the code \( C \). The main problem in this approach is the determination of the rank of \( N \) over \( \text{GF}(q) \), i.e., the redundancy of the code \( C \).

1 The numbers in square brackets refer to references listed in the bibliography at the end.
On the other hand, we may consider a given code and determine whether the dual code contains a set of vectors which may be considered as the incidence vectors of a particular incomplete block design, in which case a majority decoding algorithm will be applicable.

In this dissertation we shall consider majority decoding of linear codes whose duals either are derived from incomplete block designs based on certain geometric configurations in a finite geometry over the field $\mathbb{GF}(q)$ or are composed of vectors which are identifiable with the incidence vectors of such a design.

Chapter I serves as an introduction, in which the coding problem for a discrete channel is described. The concept of majority decoding of linear codes is introduced in this chapter through an example.

The purpose of Chapter II is to investigate the rank, over $\mathbb{GF}(q)$, of the incidence matrix of an incomplete block design obtained by considering as treatments the points of the finite projective geometry $\text{PG}(t,q)$ and as blocks the $d$-flats in the geometry. Analogously, we consider also the corresponding design in the finite affine geometry $\text{EG}(t,q)$. We first develop the necessary algebraic and geometric concepts needed to consider these designs analytically. We make use of a representation of $\text{PG}(t,q)$ and $\text{EG}(t,q)$ in terms of an extension field of $\mathbb{GF}(q)$. Corresponding to each $d$-flat in the geometry, we define an incidence polynomial with coefficients one or zero. The rank of the corresponding incidence matrix depends on the zeros of the incidence polynomials in the extension field mentioned above. Through an investigation of the zeros of these incidence polynomials, we obtain an explicit formula for the rank of the incidence matrix of points and $(t-1)$-flats in $\text{PG}(t,q)$ and in $\text{EG}(t,q)$. When $q$ is a prime, i.e., when
q = p^n, n=1, we obtain a formula for the rank of the incidence matrix of points and d-flats in PG(t,p) and EG(t,p) for arbitrary d. In the general case, q = p^n, n ≥ 1, we obtain an upper bound for the rank of the incidence matrix of points and d-flats in PG(t,q) and in EG(t,q).

In Chapter III we return to the coding problem and discuss cyclic codes and majority decoding in more detail. In particular, we generalize Massey's concept of majority decoding and investigate the applicability of majority decoding to some known classes of cyclic codes. Using the results of Chapter II, we give a geometric interpretation of the Generalized Reed-Muller codes [15] and obtain an explicit formula for the number of information symbols for these codes. We define a new class of codes, which we call Non-Primitive Generalized Reed-Muller codes, and give both a geometric interpretation of the dual codes and a formula for the number of information symbols for the codes. Applying the geometric interpretation of the dual code, we show that both the Generalized Reed-Muller and the Non-Primitive Generalized Reed-Muller codes may be decoded by a majority decoding procedure.

Two other classes of codes are defined in Chapter III. We define a class of Projective Geometry codes and show that these codes are the codes considered by Rudolph [21] and investigated recently by Goethals and Delsarte [10]. A lower bound for the number of information symbols and a majority decoding algorithm are given for these codes. Analogously, we define a new class of Affine Geometry codes and obtain similar results for this class of codes.
CHAPTER I

INTRODUCTION

1.1 The coding problem

The theory of error-correcting codes is concerned with the development of techniques by which messages can be transmitted accurately and efficiently over noisy channels. We shall consider a channel which is capable of transmitting any one of \( q \) distinct symbols. Such a channel is called a \( q \)-ary channel. For \( q \) a prime or a prime power, say \( q = p^n \), we may, and do, put the symbols into a one-to-one correspondence with the elements of the finite field \( \mathbb{GF}(q) \). Given a set of \( m \leq q^n \) messages, we set up a one-to-one correspondence between the messages and a set \( C \) of \( m \) distinct \( N \)-vectors with elements from \( \mathbb{GF}(q) \). \( C \) is called a code; each \( N \)-vector of \( C \) is called a code vector. The process of constructing the code \( C \) and the correspondence between code vectors and the messages is referred to as encoding.

To transmit a message over the channel, the \( N \) symbols of the code vector \((c_0, c_1, \ldots, c_{N-1})\) corresponding to the given message are successively transmitted over the channel. Due to the presence of random noise in the channel, a transmitted symbol may be received as one of the other \( q-1 \) symbols. In this case, we say that an error has occurred in transmission. The received vector \((r_0, r_1, \ldots, r_{N-1})\) may differ from the transmitted code vector, and need not necessarily belong to \( C \). At the receiver, a decision is made, based on the
information in the received vector, which specifies a unique vector of C, from which the corresponding message is interpolated. The process of specifying a code vector, based on the received vector, and the associated message is called decoding. The decoding is correct if the code vector specified is the corresponding transmitted code vector. If the decoding procedure necessarily gives a correct result, provided at most t errors have occurred in transmitting the code vector, we say that the code is capable of correcting up to t errors.

It has been found mathematically convenient to restrict C to be a vector subspace of the vector space $V_N$ of all $N$-vectors with elements from $GF(q)$. Such a code is called a linear code. If the dimension of C, regarded as a vector space, is $k \leq N$, the number of code vectors is $q^k$. In essence, $k$ symbols in a code vector may be chosen arbitrarily; the remaining $r=N-k$ symbols must be chosen such that the vector belongs to C. The number $k$ is referred to as the number of information symbols of C and the number $r$ is referred to as the redundancy of C. Essentially, each code vector consists of $k$ information symbols and $r$ redundant symbols. The ratio $k/N$ is called the transmission rate of information.

The general procedure in linear code construction is to construct a code which has a relatively high transmission rate of information and which is capable of correcting a relatively large number of errors. At the same time, it is desirable that the encoding and decoding procedures be simple and economical to implement.

Recent work in coding theory has concentrated on cyclic codes. A linear code C is cyclic if, for every code vector $c'=(c_0,c_1,\ldots,c_{N-1})$

1 The notation $c'$ denotes a row vector; $c$ denotes a column vector.
of \( C \), the vector \((c_{N-1}, c_0, \ldots, c_{N-2})\), obtained from \( c' \) by cyclically permuting the coordinates one unit to the right, is also a code vector of \( C \). Cyclic codes will be discussed in Chapter III. The symmetry induced in a cyclic code simplifies encoding and decoding considerably. This dissertation will deal primarily with a particular type of decoding scheme, called majority decoding, and its applicability to certain classes of cyclic codes. We describe a majority decoding briefly in the next section and in more detail in Chapter III.

1.2 Majority decoding

If \( C \) is a linear code with length \( N \) and \( k \) information symbols, we may consider \( C \) as a vector subspace of \( V_N \) with dimension \( k \). The orthogonal complement of \( C \), in the usual algebraic sense, is a subspace of \( V_N \) with dimension \( r = N - k \) and is denoted here by \( C_D \). \( C_D \) is called the dual code of \( C \). Every code vector of \( C \) is orthogonal to every vector of \( C_D \). Let \( h' = (h_0, h_1, \ldots, h_{N-1}) \) be a vector of \( C_D \). For an arbitrary vector \( g' = (g_0, g_1, \ldots, g_{N-1}) \) of \( V_N \), let

\[
    h'g = h_0g_0 + h_1g_1 + \ldots + h_{N-1}g_{N-1} = s,
\]

say. We shall refer to this equation as a parity check equation on the symbols \( g_0, g_1, \ldots, g_{N-1} \). The vector \( g' \) is a code vector of \( C \) if and only if \( h'g = 0 \) for every \( h' \in C_D \).

Suppose \( t' = (t_0, t_1, \ldots, t_{N-1}) \) is a transmitted code vector and \( r' = (r_0, r_1, \ldots, r_{N-1}) \) is the corresponding received vector. The (unknown) error vector is \( e' = (e_0, e_1, \ldots, e_{N-1}) \), where \( r' = t' + e' \). For each vector \( h' \in C_D \), we have

\[
    s = h'r = h't + h'e = h'e,
\]

since \( h't = 0 \). We may write this as

\[
    h_0e_0 + h_1e_1 + \ldots + h_{N-1}e_{N-1} = s.
\]
By choosing appropriate vectors $h$ of $C_D$, say $h_j$, $j=1,\ldots,b$, we obtain a system of equations

\[(1.2.1) \quad h_j e_0 + h_j e_1 + \cdots + h_j e_{N-1} = s_j, \quad j=1,\ldots,b.\]

If the vectors $h_j$ are known at the receiver, the $s_j$ can be determined for a received vector $r_j$ and, in some cases, the system of equations \((1.2.1)\) may be solved for the unknown error symbols $e_0, e_1, \ldots, e_{N-1}$.

A relatively simple decoding procedure of this nature, called majority decoding, is applicable to some linear codes. Majority decoding of cyclic codes is discussed in detail in Chapter III. We shall illustrate the concept here with an example.

Consider the following system of equations (over $\mathbb{GF}(q)$).

\[
\begin{align*}
e_0 + e_1 + e_3 & = s_1 \\
e_1 + e_2 + e_4 & = s_2 \\
e_2 + e_3 + e_5 & = s_3 \\
e_3 + e_4 + e_6 & = s_4 \\
e_0 + e_4 + e_5 & = s_5 \\
e_1 + e_5 + e_6 & = s_6 \\
e_0 + e_2 + e_6 & = s_7
\end{align*}
\]

(1.2.2)

Suppose at most one of the symbols in the vector $(e_0, e_1, \ldots, e_6)$ is non-zero.

Let us restrict our attention to the first, fifth and seventh equations, viz.,

\[
\begin{align*}
e_0 + e_1 + e_3 & = s_1 \\
e_0 + e_4 + e_5 & = s_5 \\
e_0 + e_2 + e_6 & = s_7
\end{align*}
\]

(1.2.3)

If each of $e_0, e_1, \ldots, e_6$ is zero, then each of $s_1, s_5$ and $s_7$ is
equal to $e_0 = 0$.

If $e_0$ is non-zero and each of the remaining symbols is zero, then again, each of $s_1$, $s_5$, and $s_7$ is equal to $e_0$. If $e_0$ is zero and $e_2$, say, is non-zero, then $s_1$ and $s_5$ are zero and $s_7$ is non-zero. In general, if $e_0$ is zero and one other symbol is non-zero, then at most one of $\{s_1, s_5, s_7\}$ is different from $e_0$, since $e_0$ and any other symbol occur together in exactly one of these three equations. In any case, the majority of $\{s_1, s_5, s_7\}$ will be equal to $e_0$.

Thus the decoding rule which assigns to $e_0$ the value assumed by the majority of $\{s_1, s_5, s_7\}$ will be correct, provided at most one of the symbols $e_0, e_1, \ldots, e_6$ is non-zero, i.e., provided at most one error has occurred in transmission.

Similarly, by considering the first, second and sixth equations in (1.2.2), a majority decision rule which assigns to $e_1$ that value assumed by the majority of $\{s_1, s_2, s_6\}$ will be correct, provided at most one of the symbols $e_0, e_1, \ldots, e_6$ is non-zero. This may also be done for each of the remaining symbols $e_2, \ldots, e_6$.

The above procedure is called majority decoding. It is particularly simple, in this case, and the procedure will correct up to one error. The majority decoding is based on the following structure of equations (1.2.2). Each of the 7 symbols occurs in 3 of the 7 equations. Any two of these symbols occur together in exactly one of the 7 equations. Also each equation contains 3 symbols. Thus, the symbols and equations in (1.2.2) form a balanced incomplete block design with parameters $v=7, b=7, r^*=3, k^*=3$ and $\lambda=1$. Of particular

\[2\] Traditionally, $r$ and $k$ are used as parameters of the design. We use $r^*$ and $k^*$ to avoid confusion with the redundancy and information symbols of a code.
importance here is the property that $r^* = 3$ and $\lambda = 1$.

This suggests constructing a linear code of length $v$ with the property that a set of $b$ parity check equations, which correspond to vectors in the dual code, exists such that the symbols in a $v$-vector and this set of parity check equations form a balanced incomplete block design with parameters $v, b, r^*, k^*, \lambda$, or generally, form any incomplete block design.

Suppose we take such a design of $b$ blocks and $v$ treatments, say, and consider the $b \times v$ incidence matrix, $N$, defined as

$$N = (n_{ij}),$$

where

$$n_{ij} = \begin{cases} 
1, & \text{if the } j\text{th treatment is contained in the } i\text{th block}, \\
0, & \text{otherwise; } i=1,2,\ldots,b, \ j=1,2,\ldots,v.
\end{cases}$$

Define a linear code $C$ with length $v$ and with symbols from $\mathbb{GF}(q)$ such that the row vectors of $N$ generate the dual code of $C$. Each row vector of $N$, which we call the incidence vector of the corresponding block, determines a parity check equation for $C$. A majority decoding procedure for $C$ may be used, depending on the type of design and the parameters of the design.

Of particular interest in this case is the rank of the incidence matrix $N$ over $\mathbb{GF}(q)$. The redundancy $r$ of the code $C$ is the dimension of the dual code, which is equal to the rank of $N$ over $\mathbb{GF}(q)$. For an arbitrary incomplete block design, the rank of the corresponding incidence matrix over $\mathbb{GF}(q)$ is almost entirely unknown and appears to be difficult to treat analytically. However, the algebraic structure of some designs derived from finite geometries provides a
means of investigating the rank of the incidence matrix of such a design. We shall devote most of Chapter II to this study.

The results obtained in Chapter II will be applied in Chapter III to the construction of some new cyclic codes and to an investigation of previously known cyclic codes for which a majority decoding procedure, based on the incidence structure of the dual code, may be used.
CHAPTER II

INCIDENCE MATRICES INFINITE GEOMETRIES

2.1 Introduction

In this chapter, we shall investigate the rank of an incidence matrix of points and d-flats in the finite geometries PG(t,q) and EG(t,q). For most combinatorial purposes, such an incidence matrix would be considered a real (0,1)-matrix. For coding theory purposes, it is appropriate to consider the matrix over the field, GF(q), on which the geometry is based.

We shall briefly sketch the line of attack taken in determining the rank of an incidence matrix over GF(q), and then introduce the necessary algebraic and geometric concepts. In particular, a representation of (t-1)-flats in PG(t,q) and EG(t,q), believed to be new, is used here. We shall attempt to keep this chapter as self-contained as possible, so that a familiarity with coding theory is not essential here.

2.2 The rank of an incidence matrix

Let us consider an incidence matrix of points and d-flats in PG(t,q), say. Suppose the v points and the b d-flats of the geometry are denoted P_0, P_1, ..., P_{v-1} and S_0, S_1, ..., S_{b-1}, respectively. An
incidence matrix, \( N \), of points and \( d \)-flats is defined as
\[
N = ((n_{ij}))_{b \times v}, \text{ where for } i=0,1,...,b-1 \text{ and } j=0,1,...,v-1,
\]
\[
n_{ij} = \begin{cases} 
1, & \text{if the point } P_j \text{ is incident with the flat } \Sigma_i, \\
0, & \text{otherwise.}
\end{cases}
\]

We will regard \( N \) as a \((0,1)\)-matrix over the field \( GF(q) \).

We also define an incidence polynomial of the flat \( \Sigma_i \) as the polynomial \( \theta_i(x) \), given by
\[
\theta_i(x) = \sum_{j=0}^{v-1} n_{ij}x^j, \quad i=0,1,...,b-1.
\]

If the points on the flat \( \Sigma_i \) are \( P_{e_1}, P_{e_2}, ..., P_{e_k} \), then
\[
\theta_i(x) = x^{e_1} + x^{e_2} + ... + x^{e_k}.
\]

Suppose \( \beta_0, \beta_1, ..., \beta_{v-1} \) are the \( v \) distinct roots of \( x^v - 1 = 0 \) in some extension field, \( K \), of \( GF(q) \). Then the matrix \( V \), defined as
\[
V = \begin{bmatrix}
1 & 1 & ... & 1 \\
\beta_0 & \beta_1 & ... & \beta_{v-1} \\
\beta_0^2 & \beta_1^2 & ... & \beta_{v-1}^2 \\
... & ... & ... & ... \\
\beta_0^{v-1} & \beta_1^{v-1} & ... & \beta_{v-1}^{v-1}
\end{bmatrix},
\]
is a non-singular \( v \times v \) Vandermonde matrix over \( K \), and
\[
NV = \begin{bmatrix}
\theta_0(\beta_0) & \theta_0(\beta_1) & ... & \theta_0(\beta_{v-1}) \\
\theta_1(\beta_0) & \theta_1(\beta_1) & ... & \theta_1(\beta_{v-1}) \\
... & ... & ... & ... \\
\theta_{b-1}(\beta_0) & \theta_{b-1}(\beta_1) & ... & \theta_{b-1}(\beta_{v-1})
\end{bmatrix}.
\]

Now the rank of \( NV \) over \( K \) is equal to the rank of \( N \) over \( K \), since \( V \) is non-singular. Certainly the rank of \( NV \) is at most equal to the number of its non-null columns. It is well known [3,p.232] that since the entries of \( N \) are elements of the subfield \( GF(q) \) of \( K \),
the rank of $N$ over $K$ is equal to its rank over $\text{GF}(q)$. Hence the rank of $N$ over $\text{GF}(q)$ is at most equal to the number of integers $u,
0 \leq u \leq v-1$, such that $\theta_i(\beta_u) \neq 0$ for some $i$. Equivalently, the rank of $N$ is at most equal to $v$ minus the number of integers $m,
0 \leq m \leq v-1$, such that $\theta_i(\beta_m) = 0$, for all $i=0,1,\ldots,b-1$.

We shall later show, through an analytical consideration of the incidence polynomials of flats in the geometry, that this upper bound on the rank of $N$ is actually attained.

2.3 Finite fields

Before considering finite geometries, we reproduce here some of the basic results on finite fields, the proofs of which may be found in [7, ch IX] or [9, ch I], for example.

Throughout, we shall let $q$ be a prime or a prime power, say $q = p^n$, where $p$ is a prime and $n$ is a positive integer.

The non-zero elements of $\text{GF}(q)$ are solutions of the equation

$$x^{q-1} - 1 = 0.$$  

If $\gamma$ is a primitive element of $\text{GF}(q)$, i.e., a primitive solution of equation (2.3.1), then the non-zero elements of $\text{GF}(q)$ may be represented by $1=\gamma^0$, $\gamma$, $\ldots$, $\gamma^{q-2}$. We may extend the field $\text{GF}(q)$ to the extension field $\text{GF}(q^N)$, whose non-zero elements satisfy the equation

$$x^{q^N-1} - 1 = 0.$$  

Let $\alpha$ be a primitive element of $\text{GF}(q^N)$. The non-zero elements of $\text{GF}(q^N)$ are represented by $1=\alpha^0, \alpha, \ldots, \alpha^{q^N-2}$.

Now $\text{GF}(q)$ is a subfield of $\text{GF}(q^N)$ and the non-zero elements of $\text{GF}(q^N)$ which satisfy equation (2.3.1) are precisely the non-zero elements of $\text{GF}(q)$; these may be represented as $1=\gamma^0, \gamma, \ldots, \gamma^{q-1}$, where
\( \gamma = \alpha^{(q^N-1)/(q-1)} \). Moreover, \( \gamma \) is a primitive element of \( \text{GF}(q) \).

We may regard \( \text{GF}(q^N) \) as an \( N \)-dimensional vector space over \( \text{GF}(q) \) in the following manner. Every non-zero element of \( \text{GF}(q^N) \) may be expressed uniquely as a polynomial in \( \alpha \), of degree at most \( N-1 \), with coefficients from \( \text{GF}(q) \). Suppose, for fixed \( u, 0 \leq u \leq q^N-2 \),

\[
\alpha^u = a_0 + a_1 \alpha + \ldots + a_{N-1} \alpha^{N-1},
\]

where \( a_0, a_1, \ldots, a_{N-1} \) are elements of \( \text{GF}(q) \). The correspondence

\[
\alpha^u \leftrightarrow (a_0, a_1, \ldots, a_{N-1})
\]

\( 0 \leftrightarrow (0, 0, \ldots, 0) \)

induces a vector space structure on \( \text{GF}(q^N) \) over \( \text{GF}(q) \). Indeed, the elements \( 1, \alpha, \ldots, \alpha^{N-1} \) form a basis for \( \text{GF}(q^N) \). We say that the elements \( \alpha^1, \alpha^2, \ldots, \alpha^k \) of \( \text{GF}(q^N) \) are linearly independent over \( \text{GF}(q) \) if, for every choice of elements \( b_1, b_2, \ldots, b_k \) of \( \text{GF}(q) \),

the equation

\[
b_1 \alpha^1 + b_2 \alpha^2 + \ldots + b_k \alpha^k = 0
\]

implies \( b_1 = b_2 = \ldots = b_k = 0 \). Otherwise, we say that \( \alpha^1, \alpha^2, \ldots, \alpha^k \) are linearly dependent over \( \text{GF}(q) \).

Considering \( \text{GF}(q^N) \) as an \( N \)-dimensional vector space over \( \text{GF}(q) \), most of the following are standard results in linear algebra and are proved in [3], for example.

By linear functional on \( \text{GF}(q^N) \), we mean a mapping \( f: \text{GF}(q^N) \to \text{GF}(q) \) such that

\[
f(x_1 + x_2) = f(x_1) + f(x_2), \quad f(ax_1) = af(x_1)
\]

for any elements \( x_1, x_2 \) of \( \text{GF}(q^N) \) and any element \( a \) of \( \text{GF}(q) \). The set of all linear functionals on \( \text{GF}(q^N) \) is an \( N \)-dimensional vector space over \( \text{GF}(q) \), under the natural operations of addition and scalar
multiplication, called the dual space of $\text{GF}(q^N)$. It is well known that a linear functional is completely determined by the image of any set of basis elements of $\text{GF}(q^N)$. Also, each (non-zero) linear functional on $\text{GF}(q^N)$ is a mapping of $\text{GF}(q^N)$ onto $\text{GF}(q)$.

In particular, the trace $[1]$ of an element $v$ of $\text{GF}(q^N)$ over $\text{GF}(q)$, denoted $T(v)$ here, is defined as

$$T(v) = v + v^q + \ldots + v^{q^{N-1}}.$$ 

It may be shown that the trace function, $T$, is a non-zero linear functional on $\text{GF}(q^N)$. We prove the following useful lemma.

**Lemma 2.3.1.** Every non-zero linear functional from $\text{GF}(q^N)$ onto $\text{GF}(q)$ may be expressed in terms of the trace $T$, in the sense that there exists a non-zero element $\mu$ of $\text{GF}(q^N)$ such that $f(x) = T(\mu x)$, for all $x \in \text{GF}(q^N)$.

**Proof.**

Let $\mu_1$ and $\mu_2$ be non-zero element of $\text{GF}(q^N)$ and suppose that $T(\mu_1 x) = T(\mu_2 x)$ for all $x \in \text{GF}(q^N)$. Then

$$T(\mu_1 x) - T(\mu_2 x) = T((\mu_1 - \mu_2)x) = T((\mu_1 - \mu_2)x) = 0$$

for all $x \in \text{GF}(q^N)$. But $T$ maps $\text{GF}(q^N)$ onto $\text{GF}(q)$. Hence $\mu_1 = \mu_2$ and there are thus $q^{N-1}$ distinct linear functionals of the form $T(\mu_1)$.

Now there are $N$ elements in any basis of $\text{GF}(q^N)$. Since a linear functional is completely determined by the image of $N$ basis elements, there are $q^{N-1}$ distinct non-zero linear functionals from $\text{GF}(q^N)$ onto $\text{GF}(q)$. Thus each non-zero linear functional must be expressible in the form stated in the lemma.

The kernel of a linear functional $f$ on $\text{GF}(q^N)$ is the set of all elements in $\text{GF}(q^N)$ such that $f(x) = 0$. The following, which we state as a lemma, is well known.
Lemma 2.3.2. Two linear functionals, \( f_1 \) and \( f_2 \), on \( \text{GF}(q^N) \) have the same kernel if and only if there exists a non-zero element, \( a \), of \( \text{GF}(q) \) such that \( f_2 = af_1 \), i.e., \( f_2(x) = af_1(x) \) for all \( x \in \text{GF}(q^N) \).

2.4 Finite projective geometry \( \text{PG}(t,q) \)

We first review some of the basic definitions of points and flats of \( \text{PG}(t,q) \), using a coordinate representation [7], [4]. Here, \( t \geq 2 \) and \( q = p^n \), where \( p \) is a prime and \( n \) is a positive integer.

A point, \( P \), of \( \text{PG}(t,q) \) is represented by an ordered \((t+1)\)-tuple, \((x_0, x_1, \ldots, x_t)\), of elements of \( \text{GF}(q) \), not all zero. The \((t+1)\)-tuple \((y_0, y_1, \ldots, y_t)\) represents the same point, \( P \), if and only if there exists a non-zero element, \( p \), of \( \text{GF}(q) \) such that \( y_i = px_i \), \( i = 0, 1, \ldots, t \).

The number of points of \( \text{PG}(t,q) \) is \( v = \frac{(q^{t+1}-1)}{(q-1)} \).

The set of all points whose coordinates satisfy a system of \((t-d)\) linear independent homogeneous equations over \( \text{GF}(q) \),

\[
\begin{align*}
&\alpha_0 x_0 + \alpha_1 x_1 + \cdots + \alpha_{t} x_{t} = 0 \\
&\alpha_{t-2} x_0 + \cdots + \alpha_{t} x_{t-1} = 0 \\
&\alpha_{t-1} x_0 + \cdots + \alpha_{t} x_{t} = 0,
\end{align*}
\]

is said to be a \( \text{\text{d-flat}} \), \( d = 0, 1, \ldots, t-1 \). A 0-flat is a point, a 1-flat is a line, etc. The number of points on a \( d \)-flat is \( (q^{d+1}-1)/(q-1) \), and the number of \( d \)-flats is \( \Phi(t,d,q) \), where

\[
\Phi(t,d,q) = \frac{(q^{t+1}-1)(q^{t}-1) \cdots (q^{t-d+1}-1)}{(q^{d+1}-1)(q^{d}-1) \cdots (q-1)}.
\]

An equivalent representation of points and \( d \)-flats in \( \text{PG}(t,q) \) is given by Carmichael [7, p345] in terms of an extension field \( \text{GF}(q^{t+1}) \) of \( \text{GF}(q) \). Let \( \alpha \) be a primitive element of \( \text{GF}(q^{t+1}) \). Every non-zero element of \( \text{GF}(q^{t+1}) \) may be represented either as a power of \( \alpha \) or as a
unique polynomial in $\alpha$, of degree at most $t$, with coefficients in $\text{GF}(q)$. Suppose, for $u = 0, 1, \ldots, q^{t+1}-2$,

$$\alpha^u = x_0 + x_1\alpha + \ldots + x_t\alpha^t.$$  

The correspondence

$$\alpha^u \mapsto (x_0, x_1, \ldots, x_t)$$

induces a vector space structure on $\text{GF}(q^{t+1})$ over $\text{GF}(q)$.

With the above correspondence, it is easily verified that a point $P$ of $\text{PG}(t, q)$ is represented by a non-zero element, say $\alpha^u$, of $\text{GF}(q^{t+1})$. Since $\alpha^v$ is a primitive element of $\text{GF}(q)$, two elements, $\alpha^u$ and $\alpha^v$, represent the same point $P$ if and only if $u \equiv v \mod v$. We shall denote the point represented by $\alpha^u$ by $(\alpha^u)$ or by $P_u$. It will be understood that the exponent of $\alpha$ is to be reduced mod $v$ to give a standard representative of the point $P$. The $v$ points are thus represented by $(\alpha^0), (\alpha^1), \ldots, (\alpha^{v-1})$ or by $P_0, P_1, \ldots, P_{v-1}$, respectively.

We may re-formulate the definition of a $d$-flat, given by equations (2.4.1), as follows. A $d$-flat is the set of all points $(\alpha^u)$ such that

$$(2.4.3) \quad f_i(\alpha^u) = 0, \quad i=1,2,\ldots,t-d,$$

where $f_1, f_2, \ldots, f_{t-d}$ are non-zero independent linear functionals on $\text{GF}(q^{t+1})$. We shall later make use of this representation of $d$-flats in $\text{PG}(t, q)$ for the case $d=t-1$.

Alternatively, Carmichael [7] shows that a $d$-flat may be defined as the set of points

$$(2.4.4) \quad (a_0\alpha^e_0 + a_1\alpha^e_1 + \ldots + a_d\alpha^e_d),$$

where $\alpha^e_0, \alpha^e_1, \ldots, \alpha^e_d$ are $d+1$ linearly independent elements of $\text{GF}(q^{t+1})$ and where $a_0, a_1, \ldots, a_d$ run independently over the elements.
of $GF(q)$ and are not simultaneously zero. The points
$(\alpha^0), (\alpha^1), ..., (\alpha^d)$ are called defining points of the flat.

The following theorem is due to Rao [22], [23], [24].

**Theorem 2.4.1.** Let the points on a given $d$-flat be represented by

\[(\alpha^1), (\alpha^2), \ldots, (\alpha^k); \quad k = \frac{q^{d+1} - 1}{q-1} \]

Then the points

\[(\alpha^{1+i}), (\alpha^{2+i}), \ldots, (\alpha^{k+i}),\]

for any integer $i$, also constitute some $d$-flat.

**Proof.**

Let the defining points of the $d$-flat (2.4.5) be

\[(\alpha^1), \ldots, (\alpha^{d+1}).\]

It is sufficient to show that $\alpha^{1+i}, \ldots, \alpha^{d+1+i}$

are linearly independent over $GF(q)$. Suppose they are not. Then

there exist elements $b_1, \ldots, b_{d+1}$ of $GF(q)$, not all zero, such that

\[b_1\alpha^{1+i} + \ldots + b_{d+1}\alpha^{d+1+i} = 0.\]

Dividing through by $\alpha^i$, we have that $\alpha^{1+i}, \ldots, \alpha^{d+1+i}$ are dependent,

which is a contradiction.

Theorem 2.4.1 shows that, starting with an initial $d$-flat whose

points are represented by powers of a primitive element, $\alpha$, we may

generate other $d$-flats by successively adding $1, 2, \ldots$ to each ex-

ponent. Not all $d$-flats so generated will be distinct. The smallest

integer, $g$, such that at the $g$th stage, the initial $d$-flat is reproduc-

ed is called the **cycle** of the initial $d$-flat [24]. Clearly, the cycle

of every $d$-flat is at most $v$. Moreover, not all $d$-flats need have the

same cycle. A study of the cycles of $d$-flats is given in [24] and [31],

in which it is shown that every $(t-1)$-flat has full cycle $v$ and that

a necessary and sufficient condition that there exist a $d$-flat in
PG(t, q) with cycle less than v is that t+1 and d+1 have a non-trivial common factor.

Let us restrict our attention to (t-l)-flats and return to the linear functional viewpoint, in which a (t-l)-flat is the set of all points, (α^n), such that

\[(2.4.6) \quad f(α^n) = 0,\]

where f is a non-zero linear functional on GF(q^{t+1}). From Lemma 2.3.1, there exists an element, say α^{-i}, of GF(q^{t+1}), such that for all

\[x \in GF(q^{t+1})\]

\[f(x) = T(α^{-i}x),\]

where

\[(2.4.7) \quad T(x) = x + x^q + \ldots + x^{q^t}.\]

The (t-l)-flat given by equation (2.4.6) is then the set of all points (α^n) such that

\[(2.4.8) \quad T(α^{-i}α^n) = 0.\]

Let us denote this (t-l)-flat by Σ_i. Here, i=0,1,...,q^{t+1}-2.

From Lemma 2.3.2, the linear functionals T(α^{-i}.) and T(α^{-i'}.) have the same kernel if and only if there exists a non-zero element, ρ, of GF(q) such that α^{-i'} = ρα^{-i}. Since α^v is a primitive element of GF(q), this holds if and only if i' ≡ i mod v. Hence, Σ_i = Σ_i' if and only if i' ≡ i mod v. It follows that Σ_0, Σ_1, ..., Σ_{v-1} are the v distinct (t-l)-flats of PG(t, q), where Σ_i is given by equation (2.4.8).

If the point α^n is on the flat Σ_i, then T(α^{-i}α^n) = 0. The point α^{n+1} is on the flat Σ_{i+1} for T(α^{-(i+1)}α^{n+1}) = T(α^{-i}α^n) = 0. Therefore, the process of cyclical generation of (t-l)-flats from the initial (t-l)-flat Σ_0, say, yields the (t-l)-flats Σ_1, Σ_2,..., Σ_{v-1} in order.
We observe that the cycle of the \((t-1)\)-flat \(\Sigma_0\) is therefore equal to \(v\). Likewise, we could generate all the \((t-1)\)-flats by choosing any of the \(\Sigma_i\) as an initial flat, obtaining the flats \(\Sigma_{i+1}, \ldots, \Sigma_{i+v}\) in order. Reducing the subscripts mod \(v\), we see that the flat \(\Sigma_i\) also has cycle equal to \(v\), for any \(i = 0,1,\ldots,v-1\).

2.5. **Finite affine geometry \(\text{EG}(t, q)\)**

We first describe a coordinate representation of \(\text{EG}(t, q)\), as given by Carmichael [7] and Bose [4].

A point of \(\text{EG}(t, q)\) is represented by one and only one ordered \(t\)-tuple, \((x_1, x_2, \ldots, x_t)\), of elements from \(\text{GF}(q)\). There are \(q^t\) points in this geometry. We shall refer to the point represented by the null vector as the origin.

A \(d\)-flat is the set of points whose coordinates satisfy a system of \(t\)-\(d\) consistent non-homogeneous independent equations

\[
\begin{align*}
  a_{10} + a_{11}x_1 + \cdots + a_{1t}x_t &= 0 \\
  a_{20} + a_{21}x_1 + \cdots + a_{2t}x_t &= 0 \\
  \vdots & \vdots \\
  a_{t-1,0} + a_{t-1,1}x_1 + \cdots + a_{t-1,t}x_t &= 0 \\
  a_{t,0} + a_{t,1}x_1 + \cdots + a_{t,t}x_t &= 0
\end{align*}
\]

(2.5.1)

The number of points on a \(d\)-flat is \(q^d\) and the number of \(d\)-flats in \(\text{EG}(t, q)\) is \(q^{t-d}\phi(t-1,d-1,q)\), where \(\phi\) is given by equation (2.4.2).

Alternatively, we may represent \(\text{EG}(t, q)\) in terms of an extension field, \(\text{GF}(q^t)\), of \(\text{GF}(q)\) [24]. Let \(\alpha\) be a primitive element of \(\text{GF}(q^t)\).

A point of \(\text{EG}(t, q)\) is represented by one and only one element of \(\text{GF}(q^t)\). The point represented by the zero element is the origin, which we shall denote by \(P_0\). The point represented by \(\alpha^u\) will be denoted \(P_u\), \(0 \leq u \leq q^t-2\). We shall identify an element of \(\text{GF}(q^t)\) with the point it represents.
Let $\alpha_1, \alpha_2, ..., \alpha_d$ be any set of $d$ independent elements of $GF(q^t)$. The set of points represented by $0$ and the elements $\alpha^u$ where

\[(2.5.2) \quad \alpha^u = a_1\alpha_1 + a_2\alpha_2 + ... + a_d\alpha_d \]

and where $a_1, a_2, ..., a_d$ are elements of $GF(q)$, not all zero, is a $d$-flat passing through the origin.

The set of points represented by those elements $\alpha^w$ where

\[\alpha^w = \alpha^c + a_1\alpha_1 + ... + a_d\alpha_d,\]

and where $a_1, a_2, ..., a_d$ are elements of $GF(q)$ is a $d$-flat passing through the point $\alpha^c$ and belonging to the same parallel bundle as the flat given by equation (2.5.2).

The equivalence of the above definitions of a $d$-flat with that given by equation (2.5.1) may be seen through the correspondence

\[(2.5.4) \quad \alpha^u \leftrightarrow (x_1, x_2, ..., x_t) \quad \text{and} \quad 0 \leftrightarrow (0, 0, ..., 0)\]

where $\alpha^u = x_1 + x_2\alpha + ... + x_t\alpha^{t-1}$ is the unique polynomial representation of $\alpha^u$, $u=0,1, ..., q^t-2$.

The number of $d$-flats passing through the origin is $\phi(t-1,d-1,q)$, and the number of $d$-flats not passing through the origin is equal to $(q^{t-d}-1) \phi(t-1,d-1,q)$.

As in the projective case, we may represent $(t-1)$-flats of $EG(t,q)$ in terms of linear functionals from $GF(q^t)$ onto $GF(q)$, viz., a $(t-1)$-flat of $EG(t,q)$ is the set of all points represented by those elements $x$ of $GF(q^t)$ which satisfy the equation

\[(2.5.5) \quad f(x) = a,\]

where $f$ is a (non-zero) linear functional from $GF(q^t)$ onto $GF(q)$ and $a$ is an element of $GF(q)$. The equivalence of this definition of a
(t-l)-flat with that given by equation (2.5.1) is a consequence of the correspondence (2.5.4).

**Lemma 2.5.1** Let $\Sigma$ be given by equation (2.5.5). Then the kernel of $f$, denoted $\text{Ker}(f)$, satisfies the following equation.

$$\text{Ker}(f) = \{x_0 - x_1 : x_0, x_1 \in \Sigma\}.$$  

**Proof.** Let $x_0$ and $x_1$ be any elements of $\Sigma$. Then $f(x_0 - x_1) = f(x_0) - f(x_1) = 0$. Hence the RHS of equation (2.5.6) is a subset of $\text{Ker}(f)$. Conversely, if $y \in \text{Ker}(f)$ and $x$ is any element of $\Sigma$, then $f(x-y) = f(x) - f(y) = a - 0 = a$. Thus $x-y \in \Sigma$. But $y = x - (x-y)$. Therefore, $y \in \text{RHS}$. This completes the proof of the lemma.

**Lemma 2.5.2.** Let $\Sigma_1$ and $\Sigma_2$ be (t-l)-flats, given by $f_1(x) = a_1$ and $f_2(x) = a_2$, respectively. Then $\Sigma_1 = \Sigma_2$ if and only if there exists a non-zero element, $p$, of $\text{GF}(q)$ such that $f_2 = pf_1$ and $a_2 = pa_1$.

**Proof.** Suppose, for some non-zero element, $p$, of $\text{GF}(q)$, $f_2 = pf_1$ and $a_2 = pa_1$. Then for all $x \in \text{GF}(q^t)$, $f_2(x) - a_2 = p[f_1(x) - a_1]$. Since $p \neq 0$, $f_2(x) = a_2$ if and only if $f_1(x) = a_1$, i.e., $\Sigma_1 = \Sigma_2$.

On the other hand, suppose $\Sigma_1 = \Sigma_2$. From Lemma 2.5.1,

$$\text{Ker}(f_1) = \{x_0 - x_1 : x_0, x_1 \in \Sigma_1\}$$

$$= \{x_0 - x_1 : x_0, x_1 \in \Sigma_2\}$$

$$= \text{Ker}(f_2).$$

Then, from Lemma 2.3.2, there exists a non-zero element, $p$, of $\text{GF}(q)$ such that $f_2 = pf_1$. Let $x \in \Sigma_2$. Then $f_2(x) = a_2$. But $\Sigma_1 = \Sigma_2$. Therefore, $f_1(x) = a_1$. Hence $a_2 = pa_1$ and the lemma is proved.

Let $\Sigma$ be a (t-l)-flat in $\text{EG}(t,q)$ given by equation (2.5.5). From Lemma 2.3.1, there exists a non-zero element of $\text{GF}(q^t)$, say $\alpha^{-1}$, such that $f(x) = T_1(\alpha^{-1}x)$ for all $x \in \text{GF}(q^t)$, where
\[ T_1(x) = x + x^q + \ldots + x^{q^{t-1}}. \]

\( T_1 \) is the trace from \( \text{GF}(q^t) \) to \( \text{GF}(q) \). We use the subscript to distinguish it from the trace from \( \text{GF}(q^{t+1}) \), used in the projective case.

Suppose \( \Sigma' \) is the \((t-1)\)-flat given by the equation \( T_1(\alpha^{-i'}x) = a' \).

From Lemma 2.5.2, \( \Sigma = \Sigma' \) if and only if there exists a non-zero element, \( \rho \), of \( \text{GF}(q) \) such that \( \alpha^{-i'} = \rho \alpha^{-1} \) and \( a' = \rho a \). We may, therefore, without loss of generality, choose the equation of a \((t-1)\)-flat, \( \Sigma \), to be

\[ T_1(\alpha^{-i}x) = a, \]

where either \( a=0 \) or \( a=1 \). Since the trace of 0 is 0, the flat \( \Sigma \) passes through the origin if and only if \( a=0 \).

Let us denote the \((t-1)\)-flat through the origin, given by

\[ T_1(\alpha^{-i}x) = 0, \]

by \( \Sigma_i^0 \), \( i=0,1,\ldots,q^t-2 \). Since \( \alpha^{v'} \) is a primitive element of \( \text{GF}(q) \), where \( v' = (q^t-1)/(q-1) \), it follows from Lemma 2.5.2 that \( \Sigma_i^0 = \Sigma_j^0 \) if and only if \( i' \equiv i \mod v' \). The flats \( \Sigma_0^0, \Sigma_1^0, \ldots, \Sigma_{v'-1}^0 \) are the \( v' \) distinct \((t-1)\)-flats through the origin in \( \text{EG}(t,q) \).

In an analogous manner, let us denote the \((t-1)\)-flat not passing through the origin, given by

\[ T_1(\alpha^{-i}x) = 1, \]

by \( \Sigma_i^1 \). Since the RHS of this equation is taken as 1 for every \((t-1)\)-flat not passing through the origin, it follows from Lemma 2.5.2 that, for \( i,i' = 0,1,\ldots,q^t-2 \), the flat \( \Sigma_i^1 = \Sigma_i^1 \), if and only if \( i'=i \). The flats \( \Sigma_0^1, \Sigma_1^1, \ldots, \Sigma_{q^t-2}^1 \) are the distinct \( q^t-1 \) \((t-1)\)-flats not passing through the origin in \( \text{EG}(t,q) \).
2.6 Incidence matrices of points and \((t-1)\)-flats

We shall treat the projective case first. The representation of points of \(PG(t,q)\) as elements of the extension field, \(GF(q^{t+1})\), of \(GF(q)\), considered as a \((t+1)\)-dimensional vector space over \(GF(q)\); and the representation of \((t-1)\)-flats of \(PG(t,q)\) in terms of the kernel of a linear functional, expressed by the trace from \(GF(q^{t+1})\) to \(GF(q)\), enable us to determine the rank of the incidence matrix of points and \((t-1)\)-flats in \(PF(t,q)\).

Recall that the \((t-1)\)-flat \(\Sigma_i\) is the set of points, \((\alpha^i u)\), such that \(T(\alpha^{-i} u) = 0\), \(i=0,1,\ldots,v-1\), where \(T\) is given by equation (2.4.7) and \(\alpha\) is a primitive element of \(GF(q^{t+1})\).

If we define, for \(i=0,1,\ldots,v-1\), the function

\[
I_i(x) = 1 - [T(\alpha^{-i} x)]^{q-1},
\]

then

\[
I_i(\alpha^j) = \begin{cases} 1, & \text{if the point } (\alpha^j) \text{ is incident with the flat } \Sigma_i, \\ 0, & \text{otherwise, } j=0,1,\ldots,v-1. \end{cases}
\]

Let \(n_{ij} = I_i(\alpha^j)\), for \(i=0,1,\ldots,v-1\) and \(j=0,1,\ldots,v-1\). The matrix, \(N\), defined as

\[
N = ((n_{ij})_{v \times v}
\]

is an incidence matrix of points and \((t-1)\)-flats of \(PG(t,q)\), for

\[
n_{ij} = \begin{cases} 1, & \text{if the point } (\alpha^j) \text{ is incident with the flat } \Sigma_i, \\ 0, & \text{otherwise}. \end{cases}
\]

Moreover, considering subscripts mod \(v\),

\[
n_{i+1,j+1} = I_{i+1}(\alpha^{j+1})
\]

\[
= 1 - [T(\alpha^{-(i+1)} \alpha^{j+1})]^{q-1}
\]

\[
= 1 - [T(\alpha^{-i} \alpha^j)]^{q-1}
\]

\[
(2.6.2)
\]

\[
= n_{ij}.
\]
Hence, N is a circulant matrix. We shall regard N as a \((0,1)\)-matrix over \(\mathbb{GF}(q)\).

The incidence polynomial of the flat \(\Sigma_i\) is defined as

\[
\theta_i(x) = \sum_{j=0}^{v-1} n_{ij}x^j.
\]

From equation (2.6.2), it follows that

\[x\theta_i(x) \equiv \theta_{i+1}(x), \mod x^{v-1},\]

and hence, for any integer \(h\),

\[x^h\theta_i(x) \equiv \theta_{i+h}(x), \mod x^{v-1},\]

the subscripts taken mod \(v\).

Let \(\beta = \alpha^{q-1}\). \(\beta\) is a primitive root of \(x^{v-1}=0\) in \(\mathbb{GF}(q^{t+1})\) and the matrix, \(V\), defined by

\[
V = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \beta & \beta^2 & \cdots & \beta^{v-1} \\
1 & \beta^2 & (\beta^2)^2 & \cdots & (\beta^{v-1})^2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \beta^{v-1} & (\beta^2)^{v-1} & \cdots & (\beta^{v-1})^{v-1}
\end{bmatrix},
\]

is a non-singular Vandermonde matrix over \(\mathbb{GF}(q^{t+1})\) of order \(v\).

From equations (2.6.3) and (2.6.4), it may be verified that

\[NV = VQ,\]

where \(Q\) is a \(v \times v\) diagonal matrix given by

\[
Q = \begin{bmatrix}
\theta_0(1) & \theta_0(\beta) & \cdots \\
\theta_0(\beta) & \theta_0(\beta^2) & \cdots \\
\vdots & \vdots & \ddots \\
\theta_0(\beta^{v-1}) & \theta_0(\beta^{v-2}) & \cdots & \theta_0(1)
\end{bmatrix}.
\]

Since \(V\) is non-singular over \(\mathbb{GF}(q^{t+1})\), the rank of \(N\) over \(\mathbb{GF}(q^{t+1})\)
is equal to the rank of $Q$ over $\mathbb{GF}(q^{t+1})$, which is equal to the number of non-zero elements on its main diagonal. But, as mentioned in Section 2.2, the rank of $N$ over $\mathbb{GF}(q^{t+1})$ is equal to its rank over $\mathbb{GF}(q)$, since the entries of $N$ are all elements of $\mathbb{GF}(q)$. Hence, we have the following theorem.

**Theorem 2.6.1.** The rank, over $\mathbb{GF}(q)$, of the incidence matrix, $N$, of points and $(t-1)$-flats in $\text{PG}(t,q)$ is equal to the number of integers, $m$, $0 \leq m \leq v-1$, such that $\theta_0(\beta^m) \neq 0$, where $\beta = \alpha^{q-1}$, $\alpha$ is a primitive element of $\mathbb{GF}(q^{t+1})$,

$$\theta_0(x) = \sum_{j=0}^{v-1} \left\{1 - [T(\alpha^j)]^{q-1}\right\} x^j,$$

and

$$T(x) = x + x^q + \ldots + x^{q^t}.$$

We are thus led to investigate the roots of $\theta_0(x)$ among the roots of $x^{v-1}$ in $\mathbb{GF}(q^{t+1})$. We may dispense with unity immediately, for $\theta_0(1)$ is equal to the number of points on a $(t-1)$-flat, which is $(q^{t-1})/(q-1)$. In $\mathbb{GF}(q^{t+1})$, an integer is taken mod $p$, where $q = p^n$.

Thus, $\theta_0(1) \neq 0$, for $(q^{t-1})/(q-1) = 1 + q + \ldots + q^{t-1} \equiv 1 \mod p$.

We shall now restrict $m$ such that $1 \leq m \leq v-1$.

The following series of lemmas will lead to the number of integers $m$ such that $\theta_0(\beta^m) \neq 0$.

**Lemma 2.6.1.** Define the function $G(x)$ by

$$(2.6.6) \quad G(x) = \sum_{j=0}^{q^{t+1}-2} \left\{1 - [T(\alpha^j)]^{q-1}\right\} x^j.$$

Then, over $\mathbb{GF}(q^{t+1})$,

$$\theta_0(x) = -G(x) \mod x^{v-1}.$$
Proof. Since $\alpha^v$ is a primitive element of $\mathbb{GF}(q)$, for any integer $h$,

$$
\left[ T(\alpha^{j+h}) \right]^{q-1} = \left[ \alpha^{hv} T(\alpha^j) \right]^{q-1} = \left[ T(\alpha^j) \right]^{q-1}.
$$

Then

$$
\sum_{j=0}^{q^{t+1}-2} \left\{ \sum_{h=0}^{q-2} \sum_{j=0}^{v-1} \left( 1 - \left[ T(\alpha^j) \right]^{q-1} \right) x^{j+h} \right\} = (q-1) \sum_{j=0}^{v-1} \left( 1 - \left[ T(\alpha^j) \right]^{q-1} \right) x^j, \mod x^{v-1}
$$

Since $q-1 \equiv -1 \mod p$, the lemma follows.

We may write $1 - [T(x)]^{q-1}$ as a polynomial in $x$ of degree at most $q^{t+1}-2$ with coefficients in $\mathbb{GF}(q^{t+1})$. Suppose

$$
1 - [T(x)]^{q-1} = 1 - (x + x^{q} + \ldots + x^{q_{t}^{2^{t-1}}})^{q-1}
$$

(2.6.7)

$$
= \sum_{u=0}^{q^{t+1}-2} a_u x^u,
$$

where the coefficients $a_u$ are yet to be determined.

Lemma 2.6.2. For $1 \leq u \leq q^{t+1}-2$, $G(\alpha^{-u}) = -a_u$, where $a_u$ is given by equation (2.6.7).

Proof. From equation (2.6.7),

$$
G(\alpha^{-u}) = \sum_{j=0}^{q^{t+1}-2} \sum_{i=0}^{q^{t+1}-2} a_i \alpha^{ij} \alpha^{-uj}
$$

$$
= \sum_{i=0}^{q^{t+1}-2} a_i \sum_{j=0}^{q^{t+1}-2} \alpha^{(i-u)j}.
$$

Since $\alpha$ is a primitive element of $\mathbb{GF}(q^{t+1})$, it is well known (see Van der Waerden [27, p.115], for example) that
\[
\sum_{j=0}^{q^{t+1}-2} \alpha^{i-u)_j} = \begin{cases} 
-1, & \text{if } i-u \equiv 0 \mod q^{t+1}-1, \\
0, & \text{otherwise}.
\end{cases}
\]

Now for \(1 \leq u \leq q^{t+1}-2\) and \(1 \leq i \leq q^{t+1}-2\), \(i-u \equiv 0 \mod q^{t+1}-1\) if and only if \(i = u\). Hence \(G(\alpha^{-u}) = -a_u\).

We shall need the concept of the \(p\)-adic representation of an integer, details of which may be found in any elementary number theory text, such as [16, pp. 9-12].

Every positive integer \(u\) may be uniquely expressed as a formal power series in \(p\), of the form

\[
u = c_0 + c_1 p + c_2 p^2 + \ldots + c_k p^k,
\]

where \(0 \leq c_i \leq p-1\), \(i=0,1,\ldots,k\). The coefficients \(c_i\) are called the digits of \(u\) to the base \(p\). We shall denote the sum of the digits of \(u\) to the base \(p\) by \(D_p(u)\), i.e., \(D_p(u) = c_0 + c_1 + \ldots + c_k\).

Let us now return to the expansion of \(1 - [T(x)]^{q-1}\) as a polynomial in \(x\). Since the fields in which we are working have characteristic \(p\), we may write

\[
(x + x^q + x^{q^2} + \ldots + x^{q^t})^{q-1} = \prod_{j=0}^{n-1} \left( x^{p^j} + x^{p^{j+n}} + \ldots + x^{p^{j+tn}} \right)^{p-1},
\]

recalling that \(q = p\).

Using the multinomial theorem, the \(j\)th term in the above product is

\[
\sum \binom{p-1}{c_j, c_{j+n}, \ldots, c_{j+tn}} x^{c_j p^j + c_{j+n} p^{j+n} + \ldots + c_{j+tn} p^{j+tn}},
\]

where the summation is taken over all choices of \(c_j, c_{j+n}, \ldots, c_{j+tn}\).
such that

\[(2.6.10) \quad c_j + c_{j+n} + \ldots + c_{j+tn} = p-1; \quad 0 \leq c_{j+in} \leq p-1, \quad i=0,1,\ldots,t.\]

Dickson [8] shows that none of the multinomial coefficients of the form

\[
\binom{p-1}{a_0, a_1, \ldots, a_s},
\]

where \(a_0+a_1+\ldots+a_s=p-1, \quad 0 \leq a_i \leq p-1, \quad i=0,1,\ldots,s,\) are divisible by \(p.\)

Substituting equation (2.6.9) into equation (2.6.8), we have

\[
(x + x^q + \ldots + x^{q^t})^{q-1} = \sum \ldots \sum \left( \binom{p-1}{c_0, c_n, \ldots, c_{tn}} \right) \ldots \left( \binom{p-1}{c_{n-1}, c_{n-1+n}, \ldots, c_{n-1+tn}} \right)
\]

\[
x^{c_0+c_1p^1+\ldots+c_{n-1}p^{t+n}+\ldots+c_{n-1+tn}p^{t+n}},
\]

where each summation is given as in equation (2.6.9). None of the multinomial coefficients in equation (2.6.11) are congruent to zero mod \(p.\) Moreover, each exponent of \(x\) is the unique \(p\)-adic representation of an integer \(u,\) in the range \(1 \leq u \leq q^{t+1}-1,\) in fact, \(u \leq q^{t+1}-2,\) for \(t \geq 2.\)

Let \(S_t\) be the set of all integers \(u,\) \(1 \leq u \leq q^{t+1}-2,\) such that if \(c_0+c_1p^1+\ldots+c_{n-1}p^{t+n}+\ldots+c_{n-1+tn}p^{t+n}\) is the \(p\)-adic representation of \(u,\) the digits of \(u\) satisfy equation (2.6.10), for each \(j=0,1,\ldots,n-1.\) We observe that if \(u \in S_t,\) \(u \equiv (p-1) + (p-1)p + \ldots + (p-1)p^{n-1} = q-1, \mod q-1,\) from equation (2.6.10), i.e., \(u \equiv 0 \mod q-1.\)

We may now write

\[
(x + x^q + \ldots + x^{q^t})^{q-1} = \sum_{u \in S_t} b_u x^u,
\]

where \(b_u \neq 0 \mod p\) for \(u \in S_t.\) Hence

\[
1 - [T(x)]^{q-1} = 1 - \sum_{u \in S_t} b_u x^u,
\]
and the following lemma is immediate.

**Lemma 2.6.3**

\[ l - [T(x)]^{q-1} = \sum_{u=0}^{d_{t+1}-2} a_u x^u, \]

where

(i) \( a_0 = 1; \)

(ii) if \( u \in S_t, \ a_u = -b_u \neq 0, \) over \( GF(q^{t+1}); \)

(iii) otherwise, \( a_u = 0. \)

We are now in a position to return to a consideration of \( \theta_0(x). \)

For mathematical convenience, we shall consider \( \theta_0(\beta^{-m}), \) for \( 1 \leq m \leq v-1. \) From Lemma 2.6.1, \( \theta_0(\beta^{-m}) = -G(\beta^{-m}). \) Setting \( u = m(q-1) \)

\[ G(\beta^{-m}) = G(\alpha^u) = -a_u, \]  from Lemma 2.6.2. Hence, \( \theta_0(\beta^{-m}) = a_u. \) Applying Lemma 2.6.3, we have

**Theorem 2.6.2** \( \theta_0(1) \neq 0; \) for \( 1 \leq m \leq v-1, \ \theta_0(\beta^{-m}) \neq 0 \) if and only if \( m(q-1) \in S_t. \)

We count the number of elements in \( S_t \) as follows. Recall that \( S_t \) is the set of all integers \( u, \) such that if the \( p \)-adic representation of \( u \) is

\[ u = c_0 + c_1 p + \ldots + c_{n-1} p^{n-1+t_n}, \]

then, for each \( j=0,1,\ldots,n-1, \)

\[ c_j + c_{j+n} + \ldots + c_{j+t_n} = p-1. \]

If \( B(t,p) \) is the number of ways of choosing \( t+1 \) integers \( d_0, \ldots, d_t \)

such that \( 0 \leq d_i \leq p-1, i=0,1,\ldots,t, \) and \( d_0 + d_1 + \ldots + d_t = p-1, \) then denoting the number of elements in \( S_t \) by \( |S_t|, \) we have

\[ |S_t| = [B(t,p)]^n. \]

**Lemma 2.6.4**

\[ B(t,p) = \binom{p^{t+1}-1}{t}. \]

**Proof.** It is well known that \( B(t,p) \) is the coefficient of \( x^{p-1} \) in the (real) expansion of \( (1 + x + \ldots + x^{p-1})^{t+1}. \) Now
\[(1 + x + \ldots + x^{p-1})^{t+1} = \left(\frac{1-x^p}{1-x}\right)^{t+1} = (1-x^p)^{t+1}(1-x)^{-(t+1)} = \sum_{g=0}^{t+1} (-1)^g \binom{t+1}{g} x^p \sum_{h=0}^{\infty} \binom{t+h}{t} x^h,\]

and it is easily verified that the coefficient of \(x^{p-1}\) in the above expansion is

\[\binom{t+p-1}{t}.\]

Thus

\[|S_t| = \binom{p+t-1}{t}^n.\]

It was earlier observed that every element in \(S_t\) is a multiple of \(q-1\). Combining Theorems 2.6.1 and 2.6.2 with the above, we have Theorem 2.6.3

The rank of the incidence matrix, \(N\), of points and \((t-1)\)-flats in \(PG(t,q)\), where \(q=p^n\), is

\[1 + \binom{p+t-1}{t}^n.\]

For the case \(t=2\), this result has been obtained by Graham and MacWilliams [11], and, for general \(t\), was conjectured by Rudolph [26]

to be true.

Corollary 2.6.1 If \(\theta_i(x)\) is the incidence polynomial of the \((t-1)\)-flat \(\Sigma_i\) of \(PG(t,q)\), \(i=0,1,\ldots,v-1\), the number of integers \(m\), \(0 \leq m \leq v-1\), such that \(\theta_i(p^m) = 0\) for all \(i=0,1,\ldots,v-1\) is

\[v - \binom{p+t-1}{t}^n \cdot -1.\]

We shall now consider the affine case. Because of difficulties arising in constructing an analytical expression for the incidence relation between the origin and \((t-1)\)-flats in \(EG(t,q)\), we shall
analyze separately the incidence matrix of points and \((t-1)\)-flats passing through the origin and the incidence matrix of points and \((t-1)\)-flats not passing through the origin.

Recall that \(\Sigma^0_1\) is the \((t-1)\)-flat, passing through the origin, which is given by the equation \(T_1(\alpha^{-i}x) = 0\), \(i=0,1,...,v'-1\), where \(v' = (q^t-1)/(q-1)\), and \(\alpha\) is a primitive element of \(GF(q^t)\). We observe that, if \(I^0_1(x)\) is defined as

\[
I^0_1(x) = 1 - [T_1(\alpha^{-i}x)]^{q-1},
\]

then, for \(j = 0,\ldots,q^t-2\),

\[
I^0_1(\alpha^j) = \begin{cases} 1, & \text{if the point } \alpha^j \text{ is incident with the flat } \Sigma^0_1, \\ 0, & \text{otherwise.} \end{cases}
\]

The incidence polynomial of the flat \(\Sigma^0_1\) is defined as the polynomial

\[
(2.6.13) \quad \theta^0_1(x) = \sum_{j=0}^{q^t-2} I^0_1(\alpha^j) x^j.
\]

It could be noted here that if \(t\) is replaced by \(t+1\), the polynomial \(\theta^0_1(x)\) is similar to the polynomial \(G(x)\), defined in equation (2.6.6); in fact, for \(i = 0\), \(\theta^0_0(x) = G(x)\).

From equation (2.6.12), we have

\[
x^h \theta^0_1(x) \equiv \theta^0_{i+1}(x), \mod x^{q^t-1-1},
\]

and therefore, for any integer \(h\),

\[
(2.6.14) \quad x^h \theta^0_1(x) \equiv \theta^0_{i+h}(x), \mod x^{q^t-1-1},
\]

the subscripts being taken mod \(v'\). In particular,

\[
x^{v'} \theta^0_1(x) \equiv \theta^0_1(x), \mod x^{q^t-1-1}.
\]

This implies that

\[
(2.6.15) \quad (x^{v'-1}) \theta^0_1(x) = r(x)(x^{q^t-1-1}),
\]

for some polynomial \(r(x)\).
The origin is not accounted for in the incidence polynomial, \( \theta^0_1(x) \), of the \((t-1)\)-flat, \( \Sigma^0_1 \), passing through the origin. The number of points on \( \Sigma^0_1 \), other than the origin, is \( q^{t-1} - 1 \). Hence, \( \theta^0_1(1) = -1 \), over \( \mathbb{GF}(q^t) \).

From equation (2.6.14), for any integer \( m \), \( 0 \leq m \leq q^t - 2 \),
\[
\theta^0_0(\alpha^{-m}) = (\alpha^{-m})^i \theta^0_1(\alpha^{-m}), \quad i=0,1,\ldots,v'-1.
\]
Therefore, \( \theta^0_1(\alpha^{-m}) = 0 \) if and only if \( \theta^0_0(\alpha^{-m}) = 0 \). It follows from equation (2.6.15) that, unless \( m \equiv 0 \mod q-1 \), \( \theta^0_0(\alpha^m) = 0 \), since \( \alpha^{q-1} \) is a primitive root of \( x^{v'} - 1 = 0 \) in \( \mathbb{GF}(q^t) \).

We observed earlier that if \( t \) is replaced by \( t+1 \), \( \theta^0_0(x) = G(x) \), where \( G(x) \) is defined in equation (2.6.6). We may thus use the previous lemmas to investigate \( \theta^0_0(\alpha^{-m}) \) for \( m \equiv 0 \mod q-1 \). We summarize these results in the following theorem.

**Theorem 2.6.4** Let \( \theta^0_0(x) \) be the incidence polynomial of the \((t-1)\)-flat \( \Sigma^0_0 \) passing through the origin in \( \mathbb{EG}(t,q) \). Then

(i) \( \theta^0_0(1) = -1 \);

(ii) Unless \( m \equiv 0 \mod q-1 \), \( \theta^0_0(\alpha^m) = 0 \);

(iii) For \( 1 \leq m \leq v'-1 \), \( \theta^0_0(\alpha^{-m}(q-1)) \neq 0 \) if and only if \( m(q-1) \in S_{t-1} \).

There are \( q^{t-1} - v' = (q-2)v' \) integers \( h \), \( 0 \leq h \leq q^t - 2 \), such that \( h \not\equiv 0 \mod q-1 \). Since \( |S_{t-1}| = (p+t-2)^n \), the number of integers \( m \), \( 0 \leq m \leq q^t - 2 \), such that \( \theta^0_0(\alpha^{-m}) \neq 0 \) is

\[
1 + \binom{p+t-2}{t-1}^n.
\]

By adjoining a column of ones to the incidence matrix, \( N \), of points other than the origin, and \((t-1)\)-flats passing through the origin in \( \mathbb{EG}(t,q) \), we may correspond the additional column to the origin and
consider the augmented matrix as the incidence matrix of (all) points and (t-1)-flats passing through the origin in $\text{EG}(t,q)$. Denote this augmented matrix by $\mathbf{N}^*$. Since there are $q^{t-1}$ points on a $(t-1)$-flat, this additional column is dependent (over $\text{GF}(q)$) on the columns of the matrix $\mathbf{N}$. Thus the rank of $\mathbf{N}^*$ is equal to the rank of $\mathbf{N}$. From Theorem 2.6.4, we have

**Theorem 2.6.5** Over $\text{GF}(q)$, where $q = p^n$, the rank of the incidence matrices $\mathbf{N}$ and $\mathbf{N}^*$, defined above, of points and (t-1)-flats passing through the origin in $\text{EG}(t,q)$ is equal to $1 + \left(\binom{p+t-2}{t-1}\right)^n$.

Suppose now that $\Sigma^1_1$ is a $(t-1)$-flat in $\text{EG}(t,q)$ which does not pass through the origin. Then $\Sigma^1_1$ is given by

$$T_1(\alpha^{-i}x) = 1,$$

for $i = 0, 1, \ldots, q^t - 2$. Let

$$(2.6.16) \quad I^1_1(x) = 1 - [1 - T_1(\alpha^{-i}x)]^{q-1}.$$ 

Then, for $j = 0, 1, \ldots, q^t - 2$,

$$I^1_1(\alpha^j) = \begin{cases} 1, & \text{if the point } \alpha^j \text{ is incident with } \Sigma^1_1, \\ 0, & \text{otherwise.} \end{cases}$$

The incidence polynomial, $\theta^1_1(x)$, of the flat $\Sigma^1_1$ is given by

$$\theta^1_1(x) = \sum_{j=0}^{q^t-2} I^1_1(\alpha^j)x^j.$$ 

If the $k = q^{t-1}$ points on $\Sigma^1_1$ are $\alpha^1, \alpha^2, \ldots, \alpha^k$, then

$$\theta^1_1(x) = x^{u_1} + x^{u_2} + \ldots + x^{u_k},$$

and $\theta^1_1(1) = k \equiv 0, \mod p$.

Again, since $I^1_1(\alpha^j) = I^1_{i+1}(\alpha^{j+1})$, we have

$$x \cdot \theta^1_1(x) \equiv \theta^1_{i+1}(x), \mod s^{t-1-1}.$$
and consequently, for any integer $h$,

\[ (2.6.17) \quad x^h \theta_1^l(x) \equiv \theta_1^{l+h}(x), \mod x^{q-1}, \]

the subscripts being taken mod $q^{-1}$.

From equation (2.6.17), it follows that, for $0 \leq m \leq q^{-2}$, $\theta_1^l(x^m) = 0$, for all $i=0,1,\ldots,q^{-2}$, if and only if $\theta_0^l(x^m) = 0$.

It will be convenient to consider $\theta_0^l(x^{-h})$, where $1 \leq h \leq q^{-2}$.

\[ \theta_0^l(x^{-h}) = \sum_{j=0}^{q^{-2} - 1} \left[1 - [1 - T_1(x^j)]^{q-1}\right] x^{-jh} \]

\[ (2.6.18) \quad = \sum_{j=0}^{q^{-2} - 1} x^{-jh} \sum_{j=0}^{q^{-2} - 1} [1 - T_1(x^j)]^{q-1} x^{-jh}. \]

Now

\[ \sum_{j=0}^{q^{-2} - 1} x^{-jh} = \begin{cases} -1, & \text{if } h \equiv 0 \mod q^{-1}, \\ 0, & \text{otherwise}. \end{cases} \]

Let us consider the second term in equation (2.6.18).

Recalling that $q = p^n$, we may expand $[1 - T_1(x)]^{q-1}$ as

\[ [1 - T_1(x)]^{q-1} = [1 - (x + x^q + \ldots + x^{q^{-1} q - 1})]^{q-1} \]

\[ (2.6.19) \quad = \prod_{j=0}^{n-1} \left\{1 - (x^j + x^{j+n} + \ldots + x^{j+(t-1)n})\right\}^{p-1} \]

For $j=0,1,\ldots,n-1$, each term under the product in equation (2.6.19) is expanded as

\[ \left\{1 - (x^j + x^{j+n} + \ldots + x^{j+(t-1)n})\right\}^{p-1} \]

\[ (2.6.20) \quad = \sum_{u=0}^{p-1} (-1)^u \binom{p-1}{u} \left[x^j + x^{j+n} + \ldots + x^{j+(t-1)n}\right]^u. \]
We note that none of the binomial coefficients in the above are divisible by $p$. Now, for $0 \leq u \leq p-1$,
\[
\left[ x^{p^j} + x^{p^{j+n}} + \ldots + x^{p^{j+(t-1)n}} \right]^u
\]
\[(2.6.21)\]
\[
= \sum (c_j, c_{j+n}, \ldots, c_{j+(t-1)n})^{c_j p^j + c_{j+n} p^{j+n} + \ldots + c_{j+(t-1)n} p^{j+(t-1)n}}
\]
where the summation is taken over all choices of the $c$'s such that
\[(2.6.22)\]
\[c_j + c_{j+n} + \ldots + c_{j+(t-1)n} = u, \quad 0 \leq c_{j+n} < u, \quad r=0,1,\ldots,t-1.\]
Since $0 \leq u \leq p-1$, none of the multinomial coefficients in equation (2.6.21) are divisible by $p$. Substituting all of the above into equation (2.6.19), we may write
\[(2.6.23)\]
\[
[1 - T_1(x)]^{q-1} = \sum_{w \in R_t} b_w x^w,
\]
where $R_t$ is the set of all integers, $w$, such that if the $p$-adic representation of $w$ is
\[w = c_0 + c_1 p + \ldots + c_{n-1} (t-1) n^{n-1} (t-1) n^p\]
then for each $j=0,1,\ldots,n-1$,
\[0 \leq c_j + c_{j+n} + \ldots + c_{j+(t-1)n} \leq p-1.\]
We note that if $w \in R_t$, then $0 \leq w \leq q^{t-1}$. In fact, for $t \geq 2$,
\[w \leq q^{t-2}.\]
The coefficient $b_w$ is not congruent to zero, mod $p$ for $w \in R_t$.

Returning to equation (2.6.18), we have, for $1 \leq h \leq q^{t-2}$,
\[
\sum_{j=0}^{q^{t-2}} [1 - T_1(\alpha^j)]^{q-1} \alpha^{-jh}
\]
\[ q^{t-2} \sum_{j=0}^{t-2} \sum_{w \in \mathbb{R}_t} b_w \alpha^j w \alpha^{-j} h \]
\[ = \sum_{w \in \mathbb{R}_t} b_w \sum_{j=0}^{t-2} \alpha^{(w-h)j} \]

Now
\[ \sum_{j=0}^{t-2} \alpha^{(w-h)j} = \begin{cases} -1, & \text{if } w-h \equiv 0 \mod q^{t-1}, \\ 0, & \text{otherwise}. \end{cases} \]

Since, for \( 1 \leq h \leq q^{t-2} \) and for \( w \in \mathbb{R}_t \), \( w-h \equiv 0 \mod q^{t-1} \) if and only if \( h = w \),
\[ \sum_{j=0}^{t-2} [1 - T_1(\alpha^j)] q^{t-2} \alpha^{-j} h = \begin{cases} -b_h, & \text{if } h \in \mathbb{R}_t \\ 0, & \text{otherwise}. \end{cases} \]

Equation (2.6.18) becomes, for \( 1 \leq h \leq q^{t-2} \),
\[ \theta_0^l(\alpha^h) = \begin{cases} b_h (\not\equiv 0, \mod p), & \text{if } h \in \mathbb{R}_t \\ 0, & \text{otherwise}. \end{cases} \]

We collect these results in the following theorem.

**Theorem 2.6.6** Let \( \theta_1^l(x) \) be the incidence polynomial of the flat \( \Sigma_1^l \) not passing through the origin in \( \text{EG}(t, q) \), \( i=0, 1, \ldots, q^{t-2} \). Then

(i) \( \theta_1^l(1) = 0 \);

(ii) If \( h \geq 1 \) and \( h \in \mathbb{R}_t \), \( \theta_1^l(\alpha^h) \neq 0, h \leq q^{t-2} \);

(iii) If \( h \geq 1 \) and \( h \in \mathbb{R}_t \), \( \theta_1^l(\alpha^h) = 0, h \leq q^{t-2} \).

We count the number of elements in \( \mathbb{R}_t \) as follows. If \( C(t, p) \) is the number of ways of choosing \( t \) integers, \( d_1, d_2, \ldots, d_t \), such that \( 0 \leq d_i \leq p-1, i=1, 2, \ldots, t, \) and \( 0 \leq d_1 + d_2 + \ldots + d_t \leq p-1 \), then
\[ |\mathbb{R}_t| = (C(t, p))^n. \]
Now if \( d_1 + d_2 + \ldots + d_t = p-l - e \), where \( 0 \leq e \leq p-1 \), we have \( e + d_1 + \ldots + d_t = p-1 \). Hence, \( C(t,p) = B(t,p) \), where \( B(t,p) \) is given by Lemma 2.6.4. Thus,

\[
|R_t| = \binom{p+t-1}{t}.
\]

Since \( 0 \in R_t \), the number of integers \( h, 1 \leq h \leq q^t-2 \) such that \( \theta_1^h(\alpha^h) \neq 0 \) is, from Theorem 2.6.5, equal to \( |R_t| - 1 \), which is

\[
\binom{p+t-1}{t} - 1.
\]

If we define the matrix \( V_1 \) as

\[
V_1 = \begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
1 & \alpha & \alpha^2 & \ldots & \alpha^{q-2} \\
1 & \alpha^2 & (\alpha^2)^2 & \ldots & (\alpha^{q-2})^2 \\
\vdots \\
1 & \alpha^{q-2} & (\alpha^{q-2})^{q-2} & \ldots & (\alpha^{q-2})^{q-2}
\end{bmatrix},
\]

it is easy to verify that \( V_1 \) is a non-singular matrix of order \( q^t-1 \) over \( GF(q^t) \), since \( \alpha \) is a primitive element of \( GF(q^t) \).

Let us define the incidence matrix of points (other than the origin) and \((t-1)\)-flats not passing through the origin in \( EG(t,q) \) as the matrix, \( N \), given by

\[
N = ((\theta_1^h(\alpha^h))).
\]

It follows from equation (2.6.17) that

\[
N V_1 = V_1 Q_1,
\]

where \( Q_1 \) is a diagonal matrix with entries \( \theta_0^1(1), \ldots, \theta_0^{q-2}(\alpha^{q-2}) \).

As has been argued earlier, it is seen that the rank of \( N \) over \( GF(q) \) is equal to the number of integers \( h, 0 \leq h \leq q^t-2 \), such that \( \theta_0^{h}(\alpha^h) \neq 0 \). From Theorem 2.6.6, this is equal to \( \binom{p+t-1}{t} - 1 \),

By adding a column of zeros to \( N \), corresponding to the origin,
the augmented matrix $N^*$ may be viewed as the incidence matrix of (all) points and $(t-1)$-flats not passing through the origin in $E\Gamma(t,q)$. Obviously, the rank of $N^*$ is equal to the rank of $N$. Hence we have

Theorem 2.6.7. The ranks of the incidence matrices $N$ and $N^*$ over $GF(q)$ are both equal to $\binom{p+t-1}{t} - 1$, where $N$ and $N^*$ are defined above.

2.7 Incidence matrices of points and $d$-flats in $PG(t,q)$.

We turn to the problem of determining the rank of the incidence matrix involving points and $d$-flats, where $1 \leq d \leq t-1$. The projective case will be treated first.

We shall use an extension of the methods used by Graham and MacWilliams [11] in our investigation of the rank of the incidence matrix of points and $d$-flats in $PG(t,q)$. In [11], only the case $t = 2$ was considered.

Recall from Section 2.4 that a $d$-flat in $PG(t,q)$ is the set of

$$\left( a_0 \alpha^0 + a_1 \alpha^1 + \ldots + a_d \alpha^d \right),$$

where the defining points $\alpha^0, \alpha^1, \ldots, \alpha^d$ are linearly independent elements of $GF(q^{t+1})$ and $\alpha$ is a primitive element of $GF(q^{t+1})$, and where $a_0, a_1, \ldots, a_d$ run independently over the elements of $GF(q)$, not all zero.

Suppose $(\alpha^1), (\alpha^2), \ldots, (\alpha^k)$ are the $k = (q^{t-d-1}/(q-1)$ points on the $d$-flat $\Sigma$, given by equation (2.7.1). We assume the exponents $a_1, \ldots, a_k$ have been reduced mod $v$, i.e., $0 \leq a_i \leq v-1$, $i=1,\ldots,k$. The incidence polynomial of the $d$-flat $\Sigma$ is defined as the polynomial
\[ \theta(x) = x^1 + x^2 + \ldots + x^k. \]

From Theorem 2.4.1, the polynomial
\[ x^i \theta(x) = x^{1+i} + \ldots + x^{k+i}, \quad i=0,1,\ldots, \]
when reduced mod \( x^v-1 \), also is the incidence polynomial of some \( d \)-flat. If \( g \) is the cycle of the \( d \)-flat \( \Sigma \), then
\[ x^g \theta(x) \equiv \theta(x), \mod x^v-1. \]

It is proved in [24] that all \( d \)-flats in \( PG(t,q) \) may be generated cyclically from a set of initial \( d \)-flats which may be of different cycles. Suppose \( \Sigma_1, \Sigma_2, \ldots, \Sigma_\pi \) is such a set of initial \( d \)-flats, where \( 1 \leq \pi \leq b/v \), where \( b \) is the number of \( d \)-flats in \( PG(t,q) \) and is equal to \( \phi(t,d,q) \). Let the corresponding incidence polynomial of \( \Sigma_i \) be \( \theta_i(x) \), \( i=1,\ldots,\pi \). We say that a given \( d \)-flat \( \Sigma \) belongs to the cycle of the flat \( \Sigma_i \) if \( \Sigma \) can be obtained from \( \Sigma_i \) by the process of cyclical generation, in which case the polynomial of \( \Sigma \), say \( \theta(x) \), satisfies \( x^h \theta_i(x) \equiv \theta(x), \mod x^v-1 \), for some integer \( h \). Suppose the cycle of the flat \( \Sigma_i \) is \( g_i \), \( i=1,\ldots,\pi \). We observe that \( g_1 + \ldots + g_\pi = b \).

We may order the \( d \)-flats of \( PG(t,q) \) such that the first \( g_1 \) flats are \( \Sigma_1 \) and the \( g_1-1 \) distinct \( d \)-flats cyclically generated from it, the next \( g_2 \) flats are \( \Sigma_2 \) and the \( g_2-1 \) distinct flats generated from \( \Sigma_2 \), etc. According to this ordering, we define the incidence matrix of points and \( d \)-flats to be the matrix, \( N \), given by
\[ N = (n_{ij})_{b \times v}, \]
where
\[ n_{ij} = \begin{cases} 1, & \text{if the point } (\alpha^j) \text{ is incident with the } i \text{th } d \text{-flat}, \\ 0, & \text{otherwise,} \end{cases} \]
for \( i=1,2,\ldots,b \) and \( j=0,1,\ldots,v-1 \).

It will be mathematically convenient to disregard the cycle of a \( d \)-flat and consider the \( v \) \( d \)-flats cyclically generated by each of
Not all of these \( n \) d-flats will be distinct, if there exists a d-flat of cycle less than \( v \), but every d-flat will be included in the flats so generated. If \( N \) is the corresponding incidence matrix, then \( N^* \) is a \( nv \times v \) matrix. The matrix \( N \) can be obtained from \( N^* \) by deleting duplicates of rows of \( N^* \). It may be verified that, if \( V \) is the Vandermonde matrix defined in equation (2.6.5), the following equation holds.

\[
(2.7.2) \quad N^* V = \begin{bmatrix}
V & 0 & 0 & \ldots & 0 \\
0 & V & 0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & V
\end{bmatrix}
\begin{bmatrix}
D_1 \\
D_2 \\
\vdots \\
D_v
\end{bmatrix}
\]

where

\[
D_i = \begin{bmatrix}
\theta_i(\beta^0) \\
\theta_i(\beta) \\
\ddots \\
\theta_i(\beta^{v-1})
\end{bmatrix}
\]

for \( i = 1, \ldots, v \).

Since both \( V \) and the composite matrix of \( V \)'s on the RHS of equation (2.7.2) are non-singular matrices over \( GF(q^{t+1}) \), the rank of \( N^* \) is equal to the rank of the second matrix on the RHS of equation (2.7.2). By elementary row operations, the rank of this matrix is equal to \( v \) minus the number of integers \( m \), \( 0 \leq m \leq v-1 \), such that

\[
\theta_i(\beta^m) = 0, \text{ for all } i = 1, \ldots, v.
\]

Because \( N \) may be obtained from \( N^* \) by deleting duplicates of rows of \( N^* \),

\[
\Sigma_1, \ldots, \Sigma_v
\]

...
the rank of $N$ is equal to the rank of $N^*$. Noting that the rank of $N$ over $GF(q^{t+1})$ is equal to the rank of $N$ over $GF(q)$, we have the following theorem.

**Theorem 2.7.1.** Let $\Sigma_1, \ldots, \Sigma_\pi$ be a set of initial $d$-flats from which all $d$-flats of $PG(t,q)$ may be generated, and let $\theta_i(x)$, $i=1, \ldots, \pi$, be the corresponding incidence polynomials. Then the rank of the incidence matrix, $N$, of points and $d$-flats in $PG(t,q)$ is equal to $v$ minus the number of integers $m$, $0 \leq m \leq v-1$, such that $\theta_i(\beta^m) = 0$ for each $i=1, \ldots, \pi$.

Suppose $\Sigma$ is a $d$-flat generated from $\Sigma_i$, for some $i=1, \ldots, \pi$. Then, denoting the polynomial of $\Sigma$ by $\theta_\Sigma(x)$, we have

$$\theta_\Sigma(x) \equiv x^h \theta_i(x), \mod x^v-1,$$

for some integer $h$.

Hence, $\theta_\Sigma(\beta^m) = 0$ if and only if $\theta_i(\beta^m) = 0$, for any $m$. We therefore have the following corollary to Theorem 2.7.1.

**Corollary 2.7.1** The rank of $N$ over $GF(q)$ is equal to $v$ minus the number of integers $m$, $0 \leq m \leq v-1$, such that $\theta_\Sigma(\beta^m) = 0$ for every $d$-flat $\Sigma$ in $PG(t,q)$.

Let $\Sigma$ be a $d$-flat with defining points $(\alpha^0_0), (\alpha^1_0), \ldots, (\alpha^d_0)$, where $\alpha^0, \alpha^1, \ldots, \alpha^d$ are linearly independent elements of $GF(q^{t+1})$. Define the polynomial $S_\Sigma(x)$ by

$$S_\Sigma(x) = \sum_u x^u,$$  

where the summation is taken over all integers $u$ such that

$$\alpha^u = a_0^e \alpha^0 + a_1^e \alpha^1 + \ldots + a_d^e \alpha^d,$$

for some $a_0, \ldots, a_d$ of $GF(q)$, not all zero. Suppose, for a particular choice of $a_0, \ldots, a_d$,
(2.7.5) \[ a_0 \alpha^c + a_1 \alpha^{c+1} + \ldots + a_d \alpha^{c+j} = \alpha^{c+j}, 0 \leq c \leq v-1, 0 \leq j \leq q-2. \]

Then $\alpha^c$ is a point of $\Sigma$. Since $\alpha^v$ is a primitive element of $\text{GF}(q)$, the elements $\alpha^c, \alpha^{c+v}, \ldots, \alpha^{c+(q-2)v}$, which represent the same point of $\Sigma$, are also given by equation (2.7.5) for some choice of $a_0, \ldots, a_d$. Thus, each of the $q-1$ representations of a point of $\Sigma$ are given by equation (2.7.4). We may therefore write

\[
S_\Sigma(x) = a_0 \theta_\Sigma(x) + x^v \theta_\Sigma(x) + \ldots + x^{(q-2)v} \theta_\Sigma(x)
\]

\[
\equiv (q-1) \theta_\Sigma(x), \text{ mod } x^v - 1
\]

\[
\equiv - \theta_\Sigma(x), \text{ mod } x^v - 1, \text{ over } \text{GF}(q^{t+1}).
\]

We state this as a lemma.

**Lemma 2.7.1.** Let $\Sigma$ be a d-flat with incidence polynomial $\theta_\Sigma(x)$. For $S_\Sigma(x)$ defined by equation (2.7.3), then $\theta_\Sigma(x) \equiv -S_\Sigma(x), \text{ mod } x^v - 1, \text{ over } \text{GF}(q^{t+1})$.

The number of points on a d-flat is $(q^{d+1} - 1)/(q - 1) = 1 + q + \ldots + q^d$. Hence, $\theta_\Sigma(1) \equiv 1, \text{ mod } p$, for any d-flat $\Sigma$.

Let us consider $\theta_\Sigma(\beta^m)$, where $\Sigma$ is any d-flat and $1 \leq m \leq v-1$. Since $\beta^m$ is a root of $x^v - 1 = 0$, we have $\theta_\Sigma(\beta^m) = -S_\Sigma(\beta^m)$, from Lemma 2.7.1.

Now,

\[
S_\Sigma(\beta^m) = S_\Sigma(\alpha^{m(q-1)})
\]

\[
= \sum_u (\alpha^u)^{m(q-1)},
\]

where the summation is taken over all choices of $u$ such that

\[
\alpha^u = a_0 \alpha^0 + a_1 \alpha^1 + \ldots + a_d \alpha^d
\]

for some $a_0, \ldots, a_d$ of $\text{GF}(q)$, not all zero, and where $\alpha^0, \ldots, \alpha^d$ are defining points of the flat $\Sigma$. For $m > 0$, $0^{m(q-1)} = 0$. So we may write,
for \(1 \leq m \leq v-1\),
\[
S_\Sigma(\beta^m) = \sum_{s_0} \ldots \sum_{a_d} (a_0 \alpha_0^{e_{0+}} + \ldots + a_d \alpha_d^{e_{d}}) \ m(q-1),
\]
where each summation is taken over all elements of \(\mathbb{GF}(q)\). Expanding each term, we have
\[
(a_0 \alpha_0^{e_{0+}} + \ldots + a_d \alpha_d^{e_{d}}) \ m(q-1)
\]
\[
= \sum_j \left( \begin{array}{c} m(q-1) \\ j \end{array} \right) a_0^{j_0} a_1^{j_1} \ldots a_d^{j_d} \alpha_0^{e_{0+1}} \alpha_1^{e_{1+1}} \ldots \alpha_d^{e_{d+1}},
\]
where the summation is taken over all choices of \(j_0, j_1, \ldots, j_d\) such that \(j_0 + j_1 + \ldots + j_d = m(q-1)\) and \(0 \leq j_v \leq m(q-1), v=0,1,\ldots,d\).

Substituting into equation (2.7.6), and interchanging the order of summation, we obtain
\[
S_\Sigma(\beta^m)
\]
\[
= \sum_j \left( \begin{array}{c} m(q-1) \\ j \end{array} \right) \sum_{a_0} a_0^{j_0} \sum_{a_1} a_1^{j_1} \ldots \sum_{a_d} a_d^{j_d} \alpha_0^{e_{0+1}} \alpha_1^{e_{1+1}} \ldots \alpha_d^{e_{d+1}}.
\]

**Lemma 2.7.2** For any integer \(j \geq 0\),
\[
\sum_{a \in \mathbb{GF}(q)} a^j = \begin{cases} -1, & \text{if } j = k(q-1), \ k > 0, \\ 0, & \text{otherwise.} \end{cases}
\]

**Proof.** It is well known that for any integer \(j\),
\[
\sum_{a \in \mathbb{GF}(q)} a^j = \begin{cases} -1, & \text{if } j \equiv 0, \mod q-1 \\ 0, & \text{otherwise} \end{cases}
\]
If \(j = 0\), then \(a^0 = 1\) for all \(a \in \mathbb{GF}(q)\) and since \(q \equiv 0, \mod p\), the result is true. If \(j > 0\), then since \(0^j = 0\), the result follows from
the above.

It follows from Lemma 2.7.2 that, unless each $j_v$ in equation (2.7.6) is equal to $k_v(q-1)$, $k_v>0$, for $v=0,1,\ldots,d$, the corresponding term vanishes. Thus,

$$S_{\Sigma}(\beta^m) = (-1)^{d+1} \sum_{\alpha} \prod_{v}^{m(q-1)} k_0(q-1), \ldots, k_d(q-1)$$

where the summation is taken over all choices of $k_0(q-1), \ldots, k_d(q-1)$, such that

$$0 < k_v(q-1) \leq m(q-1), \quad v=0,1,\ldots,d, \text{ and } \sum_{v=0}^{d} k_v(q-1) = m(q-1).$$

Now, a sufficient condition that $S_{\Sigma}(\beta^m) = 0$ for every $d$-flat $\Sigma$ is that each of the multinomial coefficients in equation (2.7.7) is congruent to zero, mod $p$. We shall show this condition is also necessary.

A $d$-flat $\Sigma$ is determined by a set of $(d+1)$ linearly independent elements $\alpha^e_0, \ldots, \alpha^e_d$. We may regard $S_{\Sigma}(\beta^m)$ as a polynomial in $\alpha^e_0, \alpha^e_1, \ldots, \alpha^e_d$; in fact, we see from equations (2.7.7) and (2.7.8) that this is a homogeneous polynomial of degree $m(q-1) < q^{t+1}-1$.

Suppose $\alpha^e_0, \ldots, \alpha^e_d$ were chosen to be linearly dependent over $\mathbb{GF}(q)$, instead of linearly independent. Then, one of the $\alpha^e_i$'s is a linear combination of the others. We may assume that

$$\alpha^e_0 = b_1 \alpha^e_1 + \ldots + b_d \alpha^e_d$$

without loss of generality, for some $b_1, b_2, \ldots, b_d$ of $\mathbb{GF}(q)$, not all zero. Substituting this into equation (2.7.6), we have

$$S_{\Sigma}(\beta^m) = \sum_{\alpha^e_0} \sum_{\alpha^e_d} \left[ (a_0 b_1 + a_1) \alpha^e_1 + \ldots + (a_0 b_d + a_d) \alpha^e_d \right]^{m(q-1)}$$

where \( a'_i = a_0 b'_i + a_i, \) \( i = 1, \ldots, d. \) Since \( a_0 \) does not appear in the second term of this equation, we have

\[
S_{\Sigma}(\beta^m) = 0 \mod p
\]

Suppose \( S_{\Sigma}(\beta^m) = 0 \) for all \( d \)-flats \( \Sigma. \) Then it is zero for all choices of linearly independent elements \( \alpha^0, \alpha^1, \ldots, \alpha^d. \) It has just been shown that it is zero for all choices of linearly dependent elements \( \alpha^0, \alpha^1, \ldots, \alpha^d \) also. Hence, \( S_{\Sigma}(\beta^m) = 0 \) for all \( q^{t+l-1} \) choices of \( \alpha^i, \) \( i = 0, 1, \ldots, d. \) Since \( S_{\Sigma}(\beta^m) \) is a homogeneous polynomial in the \( \alpha^i \)'s, of degree less than \( q^{t+l-1}, \) this can happen only when each coefficient is zero, over \( GF(q^{t+l}). \)

We now investigate under what conditions each of the multinomial coefficients in equation (2.7.7) is congruent to zero, \( \mod p. \)

The following lemma is due to Dickson [8, p. 273].

**Lemma 2.7.3** If \( u_1 + \ldots + u_s = u, \) where \( 0 \leq u_i \leq u, \) \( i = 1, 2, \ldots, s, \) the multinomial coefficient

\[
\binom{u}{u_1, u_2, \ldots, u_s}
\]

is prime to \( p \) if and only if, when \( u \) and each of the \( u_i \) are written to the base \( p, \) in the form
the sum of the jth digits of each $u_i$ is equal to the jth digit of $u$, i.e.,

$$c_j = \sum_{i=1}^{s} c_j(i), \quad j=0,1,\ldots,n.$$ 

Moreover,

$$\left( u_1, u_2, \ldots, u_s \right) \equiv \prod_{j=0}^{n} \left( c_j(1), c_j(2), \ldots, c_j(s) \right), \mod p.$$

More insight is obtained as to the divisibility of a multinomial coefficient through the following lemma.

**Lemma 2.7.4** If $D_p(u)$ denotes the sum of the digits of $u$ to the base $p$, then the highest power of $p$ dividing the multinomial coefficient

$$\left( u_1, u_2, \ldots, u_s \right) = \frac{u!}{u_1! \cdot u_2! \cdots u_s!}$$

is equal to $D_p(u_1) + D_p(u_2) + \ldots + D_p(u_s) - D_p(u)$.

This lemma is a consequence of the well known result [8,p.263] that for any positive integer $u$, the highest power of $p$ dividing $u!$ is equal to

$$\frac{u - D_p(u)}{p-1}.$$

It follows from Lemma 2.7.4 that the multinomial coefficient

$$\left( \begin{array}{c} m(q-1) \\ k_0(q-1), \ldots, k_d(q-1) \end{array} \right) \not\equiv 0, \mod p,$$

i.e., is not divisible by $p$, if and only if

$$D_p(m(q-1)) = D_p(k_0(q-1)) + \ldots + D_p(k_d(q-1)).$$
otherwise, \[ D_p(m(q-1)) < D_p(k_0(q-1)) + \ldots + D_p(k_p(q-1)). \]

Let us, for the moment, restrict \( q \) such that \( q = p \), i.e., \( n = 1 \).

**Lemma 2.7.5** For any positive integers \( a \) and \( k \), \( D_a(k(a-1)) \equiv 0 \pmod{a-1} \).

**Proof.** Suppose the \( a \)-adic representation of \( k(a-1) \) is
\[ k(a-1) = b_0 + b_1 a + \ldots + b_N a^N. \]

Then, since \( a \equiv 1 \pmod{a-1} \), \( k(a-1) \equiv b_0 + b_1 + \ldots + b_N \pmod{a-1} \). But
\[ b_0 + b_1 + \ldots + b_N = D_a(k(a-1)). \] Since \( k(a-1) \equiv 0 \pmod{a-1} \), the result follows.

As a corollary, if \( k > 0 \), then \( D_a(k(a-1)) = r(a-1) \), where \( r \geq 1 \).

**Lemma 2.7.6** For \( q = p \), one of the multinomial coefficients in equation (2.7.7) is not divisible by \( p \) if and only if \( D_p(m(p-1)) = r(p-1) \), for some \( r \), \( d+1 \leq r \leq t+1 \).

**Proof.** Suppose one of the multinomial coefficients in equation (2.7.7) is not divisible by \( p \). Then, from Lemma 2.7.4,
\[ D_p(m(p-1)) = D_p(k_0(p-1)) + \ldots + D_p(k_d(p-1)), \]
where \( k_0, \ldots, k_d \) satisfy equation (2.7.8), in particular, \( k_v > 0, v=0, \ldots, d \). From Lemma 2.7.5, \( D_p(k_v(p-1)) \geq p-1, v=0, \ldots, d \). Hence,
\[ D_p(m(p-1)) \geq (d+1)(p-1). \] For \( 1 \leq m \leq v-1 \), the \( p \)-adic representation of \( m(p-1) \) is
\[ m(p-1) = c_0 + c_1 p + \ldots + c_t p^t. \]
Thus, \( D_p(m(p-1)) \leq (t+1)(p-1) \). We therefore must have \( D_p(m(p-1)) = r(p-1) \), where \( d+1 \leq r \leq t+1 \).

Conversely, suppose \( D_p(m(p-1)) = r(p-1) \), for some \( r \), \( d+1 \leq r \leq t+1 \). We shall show that there exist \( d+1 \) integers \( k_0(p-1), \ldots, k_d(p-1) \) such that \( 0 < k_v(p-1) \leq m(p-1), v=0,1, \ldots, d \), such that \( k_0(p-1) + \ldots + k_d(p-1) \)
= m(p-l) and \( D_p(m(p-l)) = D_p(k_0(p-l)) + \ldots + D_p(k_d(p-l)) \), by an induction argument through the following lemma.

**Lemma 2.7.7.** For \( m > 0 \), let \( D_p(m(p-l)) = s(p-l) \), where \( s \geq 1 \). Then for any \( 0 < \sigma \leq s \), there exist \( \sigma \) integers \( k_1(p-l), \ldots, k_\sigma(p-l) \) with \( 0 < k_v(p-l) \leq m(p-l) \), \( v=1, \ldots, \sigma \), and \( k_1(p-l) + \ldots + k_\sigma(p-l) = m(p-l) \) such that \( D_p(m(p-l)) = D_p(k_1(p-l)) + \ldots + D_p(k_\sigma(p-l)) \).

**Proof.** Let the \( p \)-adic representation of \( m(p-l) \) be

\[
m(p-l) = c_0 + c_1p + \ldots + c_tp^t.
\]

For \( s = 1 \), the lemma is trivially true.

For \( s = 2 \), let \( j \) be the smallest integer such that \( p-l < c_0 + \ldots + c_j \leq 2(p-l) \). Clearly \( 1 \leq j \leq t \) and \( 0 < c_0 + c_1 + \ldots + c_{j-1} \leq p-l \). Let

\[
 u_1 = c_0 + c_1p + \ldots + c_{j-1}p^{j-1} + [(p-l) - (c_0 + c_1 + \ldots + c_{j-1})]p^{j-1} \\
 u_2 = [c_0 + c_1 + \ldots + c_j - (p-l)]p^j + c_{j+1}p^{j+1} + \ldots + c_tp^t.
\]

Now \( u_1 \) and \( u_2 \) are both positive and the above are their respective \( p \)-adic representations. Moreover, \( D_p(u_1) = p-l \) and \( D_p(u_2) = D_p(m(p-l)) - (p-l) = (s-1)(p-l) = p-l \). Thus \( u_1 = k_1(p-l) \) and \( u_2 = k_2(p-l) \), for some positive \( k_1 \) and \( k_2 \). Furthermore, \( u_1 + u_2 = m(p-l) \) and the lemma is true for \( s = 2 \). Assume the lemma is true for \( s' = s-1 \).

We shall show it is true for \( s' = s \). Let \( u_1 \) and \( u_2 \) be as before. Then

\[
 D_p(u_2) = (s-1)(p-l), \text{ and } u_2 = k_2(p-l), \text{ where } k_2 > 0. \]

Applying the induction hypothesis to \( k_2(p-l) \), we may write

\[
k_2(p-l) = k'_1(p-l) + \ldots + k'_\sigma(p-l), \text{ with } 1 \leq \sigma \leq s-1,
\]

such that \( 0 < k'_v(p-l) \leq k_2(p-l) \), \( v=1, \ldots, \sigma \), and

\[
 D_p(k'_1(p-l)) + \ldots + D_p(k'_\sigma(p-l)) = D_p(k_2(p-l)).
\]

Letting \( u_1 = k'_0(p-l) \), the lemma follows.
Using this lemma, the required set of \( d+1 \leq r \) integers exists and, from Lemma 2.7.4, the corresponding multinomial coefficient in equation (2.7.7) is not divisible by \( p \). This completes the proof of Lemma 2.7.6.

Let \( \Sigma \) be a \( d \)-flat in \( \text{PG}(t,p) \). From Lemma 2.7.1, for any integer \( m, 1 \leq m \leq v-1 \), where \( v = (p^{t+1} - 1)/(p-1) \), \( \theta_\Sigma^\omega(\beta^m) = -s_\Sigma(\beta^m) \), where \( \beta = \alpha^{p-1} \) and \( \alpha \) is a primitive element of \( \text{GF}(p^{t+1}) \). We thus have the following theorem.

**Theorem 2.7.2** Let \( \Sigma \) be a \( d \)-flat in \( \text{PG}(t,p) \). For every \( d \)-flat \( \Sigma \),

(i) \( \theta_\Sigma^\omega(1) \neq 0 \);

(ii) For \( 1 \leq m \leq v-1 \), \( \theta_\Sigma^\omega(\beta^m) = 0 \), if and only if \( D_p(m(p-1)) = s(p-1) \), where \( 1 \leq s \leq d \), i.e., a necessary and sufficient condition that \( \theta_\Sigma^\omega(\beta^m) = 0 \) for every \( d \)-flat \( \Sigma \) is that \( D_p(m(p-1)) = s(p-1) \), where \( 1 \leq s \leq d \).

For \( 1 \leq m \leq v-1 \), we may write the \( p \)-adic representation of \( m(p-1) \) as \( m(p-1) = c_0 + c_1 p + \ldots + c_t p^t \). The number of integers \( m \), such that \( D_p(m(p-1)) = s(p-1) \) is equal to the number of ways of choosing \( t+1 \) integers \( c_0, \ldots, c_t \), \( 0 \leq c_i \leq p-1 \), with \( c_0 + \ldots + c_t = s(p-1) \). Let \( B_s(t,p) \) be this number. We observe that \( B_1(t,p) = B(t,p) \), defined in Section 2.6.

Now, \( B_s(t,p) \) is the coefficient of \( s(p-1) \) in the real expansion of \( (1+x+\ldots+x^{p-1})^{t+1} \). We may write, as in Lemma 2.6.4,

\[
(1+x+\ldots+x^{p-1})^{t+1} = \sum_{g=0}^{t+1} (-1)^g \binom{t+1}{g} x^p \sum_{h=0}^{\infty} \binom{t+h}{t} x^h.
\]

If we denote by \( L_s(p) \), the greatest integer in \( s(p-1)/p \), i.e.,

\[
L_s(p) = \left\lfloor \frac{s(p-1)}{p} \right\rfloor, \quad s = 1, \ldots, t+1,
\]
it may be verified that

\[
B_s(t, p) = \sum_{i=0}^{t} (-1)^i \binom{t+1}{i} \binom{t+s(p-1)-ip}{t}.
\]

Let

\[
R_d(t, p) = \sum_{s=1}^{d} B_s(t, p).
\]

The number of integers \( m, 1 \leq m \leq v-1 \), such that \( D_p(m(p-1)) = s(p-1) \), \( 1 \leq s \leq d \), is thus equal to \( R_d(t, p) \). From the corollary to Theorem 2.7.1, we have,

**Theorem 2.7.3** The rank of the incidence matrix of points and d-flats in \( \text{PG}(t, p) \) is equal to \( v \) minus \( R_d(t, p) \), where \( R_d(t, p) \) is given by equation (2.7.11).

Now \( B_s(t, p) \) is the number of ways of choosing \( t+1 \) integers \( c_0, c_1, \ldots, c_t \) such that \( 0 \leq c_i \leq p-1, i=0,1,\ldots, t \), and \( c_0 + c_1 + \cdots + c_t = s(p-1) \). Let \( d_i = p-1-c_i \). Then \( 0 \leq d_i \leq p-1, i=0,1,\ldots, t \), and \( d_0 + d_1 + \cdots + d_t = (t+1-s)(p-1) \). Hence \( B_s(t, p) = B_{t+1-s}(t, p) \) for \( s = 0,1,\ldots, t+1 \).

Also, \( R_t(t, p) = R_{t-1}(t, p) + B_t(t, p) = R_{t-1}(t, p) + B_1(t, p) \). Now \( R_t(t, p) \) is the number of integers \( m, 1 \leq m \leq v-1 \), such that \( D_p(m(p-1)) = s(p-1) \), where \( 1 \leq s \leq t \). But every integer \( m, 1 \leq m \leq v-1 \), has the property that \( D_p(m(p-1)) = s(p-1) \), where \( 1 \leq s \leq t \). Hence \( R_t(t, p) = v-1 \). We have, therefore,

\[ R_{t-1}(t, p) = v-1 - B_1(t, p), \]

and from equation (2.7.10),

\[ B_1(t, p) = \binom{t+p-1}{t}. \]

Thus

\[ R_{t-1}(t, p) = v-1 - \binom{t+p-1}{t}. \]
From Theorem 2.7.3, the rank of the incidence matrix of points and (t-1)-flats in PG(t,p) is equal to \( v - R_{t-1}(t,p) = \binom{t+p-1}{t} + 1 \), the result we obtained in Theorem 2.6.3 for the case n=1.

Returning to the general case, in which \( q = p^n \), \( n \geq 1 \), we shall obtain an upper bound on the rank of the incidence matrix of points and d-flats in PG(t,q).

For \( 0 \leq m \leq v-1 \), let the q-adic representation of \( m(q-1) \) be

\[
m(q-1) = A_0 + A_1 q + \ldots + A_t q^t,
\]

where \( 0 \leq A_i \leq q-1, i=0,1,\ldots,t \). We have \( D_q(m(q-1)) = A_0 + \ldots + A_t \equiv 0 \), mod q-1, for \( m(q-1) \equiv 0 \), mod q-1.

If one of the multinomial coefficients in equation (2.7.7) is not divisible by p, it is certainly not divisible by q. Replacing p by q in Lemma 2.7.4, the latter is true if and only if

\[
D_q(m(q-1)) = D_q(k_0(q-1)) + \ldots + D_q(k_d(q-1)).
\]

Since each \( k_i \) is positive, \( D_q(k_i(q-1)) \geq q-1, i=0,1,\ldots,d \). Thus, if one of the multinomial coefficients in equation (2.7.7) is not divisible by p, we must have

\[
D_q(m(q-1)) \geq (d+1)(q-1).
\]

Then, if \( D_q(m(q-1)) < (d+1)(q-1) \), each of the multinomial coefficients in equation (2.7.7) must be divisible by q and hence also by p. We therefore have the following theorem.

**Theorem 2.7.4** Let \( \Sigma \) be a d-flat in PG(t,p), where \( q=p^n \). Then,

(i) \( \theta_{\Sigma}(l) \neq 0 \);

(ii) For \( 1 \leq m \leq v-1 \), \( \theta_{\Sigma}(\mathbf{b}^m) = 0 \) for all d-flats \( \Sigma \) if \( D_q(m(q-1)) = s(q-1) \), where \( 1 \leq s \leq d \).

The functions \( B_s(t,q) \) and \( R_d(t,q) \) are defined by equations (2.7.10)
and (2.7.11), respectively. From part (ii) of the above theorem, the number of integers \( m, 1 \leq m \leq v-1 \), such that \( \Theta_\Sigma(\beta^m) = 0 \) for all \( d \)-flats \( \Sigma \) is at least equal to \( R_d(t,q) \). From the corollary 2.7.1, we have the following theorem.

**Theorem 2.7.5** The rank of the incidence matrix of points and \( d \)-flats in \( PG(t,q) \) is at most equal to \( v - R_d(t,q) \).

**Theorem 2.7.4** may be extended in the following manner. Since the coefficients of \( \Theta_\Sigma(x) \) are either 0 or 1, then, in \( GF(q^{t+1}) \),

\[
[\Theta_\Sigma(x)]^{p^j} = \Theta_\Sigma(x^{p^j}), \quad j = 0, 1, \ldots, n-1.
\]

Thus, if, for some \( j = 0, 1, \ldots, n-1 \), \( \Theta_\Sigma(B^{p^j}) = 0 \), then \( \Theta_\Sigma(B^m) = 0 \). We may apply Theorem 2.7.4 to \( p^j \), provided \( 1 \leq p^j \leq v-1 \).

Suppose

\[
(2.7.11) \quad m(q-1) = c_0 + c_1 p + \ldots + c_{n-1} p^{n-1} + c_n p^n + \ldots + c_1 t n^{p-1} + t^n
\]
is the \( p \)-adic representation of \( m(q-1) \). Let

\[
A_0 = c_0 + c_1 t + \ldots + c_n t^{n-1}
\]

\[
A_1 = c_1 + c_1 t + \ldots + c_1 t^{n-1}
\]

\[
\vdots
\]

\[
A_{n-1} = c_{n-1} t + \ldots + c_{n-1} t^{n-1}
\]

Then

\[
m(q-1) = A_0 + A_1 p + \ldots + A_{n-1} p^{n-1},
\]

where the terms \( A_i \) contain only powers of \( p^n = q \). Let

\[
a_0 = c_0 + c_1 t + \ldots + c_n t^{n-1}
\]

\[
a_1 = c_1 + c_1 t + \ldots + c_1 t^{n-1}
\]

\[
\vdots
\]

\[
a_{n-1} = c_{n-1} t + \ldots + c_{n-1} t^{n-1}
\]

\[
(2.7.13)
\]
Then
\[ D_q(m(q-1)) = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \]
\[ D_q(pm(q-1)) = a_{n-1} + a_0 p + \cdots + a_{n-2} p^{n-1} \]
\[ \cdots \]
\[ D_q(p^{n-1}m(q-1)) = a_1 + a_2 p + \cdots + a_{n-1} p^{n-2} + a_0 p^{n-1}. \]

We see from the above that if the residue of \( p^j m(q-1) \mod q^{t+1-1} \)
is \( u_j \), then \( D_q(p^j m(q-1)) = D_q(u_j) \). Since \( \theta_\Sigma(\alpha^{p^j m(q-1)}) = \theta_\Sigma(u_j) \),
then \( \theta_\Sigma(\beta^{p^j m}) = 0 \) if \( D_q(p^j m(q-1)) = s(q-1) \), where \( 1 \leq s \leq d \). Hence,
we have

**Lemma 2.7.8** If, for some \( j=0,1,\ldots,m-1 \), \( D_q(p^j m(q-1)) = s(q-1) \), where
\( 1 \leq s \leq d \), then \( \theta_\Sigma(\beta^m) = 0 \) for all \( d \)-flats in \( PG(t,q) \), for \( 1 \leq m \leq v-1 \).

The condition on \( m \) in this lemma is also necessary for \( \theta_\Sigma(\beta^m) \) to
be zero for all \( d \)-flats \( \Sigma \), as we shall now show. More precisely, we
shall show that if \( D_q(p^j m(q-1)) > d(q-1) \) for each \( j=0,1,\ldots,n-1 \), then
there exist integers \( k_0, k_1, \ldots, k_d \) such that \( 0 < k_0(q-1) \leq m(q-1) \),
\( v = 0,\ldots,d \), such that \( k_0(q-1) + \cdots + k_d(q-1) = m(q-1) \) and
\( D_p(m(q-1)) = D_p(k_0(q-1)) + \cdots + D_p(k_d(q-1)) \). It will follow from
Lemma 2.7.4 that the multinomial coefficient
\[ m(q-1) \]
\[ \binom{k_0(q-1), \ldots, k_d(q-1)}{v} \]
is not divisible by \( p \) and hence \( \theta(\beta^m) \neq 0 \) for some \( d \)-flat \( \Sigma \).

Suppose \( D_q(p^j m(q-1)) = b_j(q-1) \), where \( b_j \geq d+1, j=0,\ldots,n-1 \). Then,
recalling equations (2.7.11), (2.7.12) and (2.7.13),
\[ b_0(q-1) = D_q(m(q-1)) = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \]
\[ b_1(q-1) = D_q(pm(q-1)) = p b_0(q-1) - a_{n-1}(q-1) \]
$b_j(q-1) = pb_{j-1}(q-1) - a_{n-j}(q-1)$

...  

$b_{n-1}(q-1) = pb_{n-2}(q-1) - a_1(q-1)$,

from which

\begin{align*}
a_{n-1} &= pb_0 - b_1 \\
a_{n-2} &= pb_1 - b_2 \\
... \\
a_1 &= pb_{n-2} - b_{n-1} \\
a_0 &= pb_{n-1} - b_0
\end{align*}

Thus, $b_0, b_1, ..., b_{n-1}$ are restricted to values for which $a_0, a_1, ..., a_{n-1}$ lie between 0 and $(t+1)(p-1)$.

Taking subscripts mod $n$, for fixed $i$,

\[a_i = b_{n-i}^p - b_{n-i}^l\]

Since

\[a_i = c_i + c_{i+n} + ... + c_{i+tn}\]

we may write

\[c_i + c_{i+n} + ... + c_{i+tn} = pb_{n-i-1} - b_{n-i}\]

for which we obtain

\[c_i + c_{i+n} + ... + c_{i+tn} + b_{n-i} + b_{n-i-1} = b_{n-i-1}(p-1)\]

Let $s$ be the smallest integer such that

\[(b_{n-i-1-1}(p-1) < c_i + c_{i+n} + ... + c_{i+sn} + b_{n-i-1} \leq b_{n-i-1}(p-1)\]

Then

\[(b_{n-i-1-2}(p-1) < c_i + c_{i+n} + ... + c_{i+(s-1)n} + b_{n-i-1} - b_{n-i+1} \leq (b_{n-i-1-1}(p-1)\]

Let

\[A_i' = c_i + c_{i+n} + q + ... + c_{i+(s-1)n}^{s-1} + [(b_{n-i-1-1})(p-1)\]
\[-(c_i + c_{i+n} + \ldots + c_{i+(s-1)n} + b_{n-i} - b_{n-i-1})q^s ,\]

\[A_1' = [c_i + c_{i+n} + \ldots + c_{i+sn} + b_{n-i} - b_{n-i-1} - b_{n-i-1}(p-1)]q^s + c_{i+(s+1)n} q^{s+1} + \ldots + c_{i+tn} q^t .\]

Now, \(A_1'\) and \(A_1''\) contain only powers of \(p^n = q\) and both are positive integers, provided \(b_{n-i-1} \geq 2\), which will be the case for at least one \(i\). Moreover,

\[A_1 = A_1' + A_1''\]

and

\[D_q(A_1') = D_p(A_1') = (b_{n-i-1} - 1)(p-1)+b_{n-i} - b_{n-i-1} = a_1 - (p-1),\]

\[D_q(A_1'') = D_p(A_1'') = p-1.\]

Let \(W_0 = A_1' + A_1'p + \ldots + A_{n-i}'p^{n-1}\) and \(W_1 = A_1'' + A_1''p + \ldots + A_{n-i}'p^{n-1}\).

Taking residues mod \(q-1\),

\[W_0 \equiv q-1\] and \(W_1 \equiv a_0 + a_1p + \ldots + a_{n-1}p^{n-1} - (q-1) = (b_0 - 1)(q-1) .\]

Thus, there exist positive integers, \(k_0\) and \(k_1\) such that \(W_0 = k_0(q-1)\) and \(W_1 = k_1(q-1)\). It is easy to verify the following.

\[m(q-1) = k_0(q-1) + k_1(q-1)\]

and

\[D_p(m(q-1)) = D_p(k_0(q-1)) + D_p(k_1(q-1)).\]

We observe that

\[D_q(k_1(q-1)) = a_0 + a_1p + \ldots + a_{n-1}p^{n-1} - (q-1) = (b_0 - 1)(q-1)\]

\[D_q(pk_1(q-1)) = (b_1 - 1)(q-1)\]

\[\ldots\]

\[D_q(p^{n-1}k_1(q-1)) = (b_{n-1} - 1)(q-1)\]

We may thus repeat the above procedure, with \(k_1\) replacing \(m\), etc. At the \(d\)th stage, we have obtained \(d+1\) positive integers, \(k_0, k_1, \ldots, k_d\) with the required properties. Hence we have the following theorem.
Theorem 2.7.6.

Let $\Sigma$ be a $d$-flat in $FG(t,q)$, where $q=p^n$. Then

(i) $\theta_\Sigma(1) \neq 0$;

(ii) For $1 \leq m \leq v-1$, $\theta_\Sigma(p^m) = 0$ for every $d$-flat $\Sigma$ if and only if for some $j=0,1,\ldots,n-1$, $D_q(p^j m(q-1)) = s(q-1)$, where $1 \leq s \leq d$.

2.8 Incidence matrices of points and $d$-flats in $EG(t,q)$.

As in Section 2.6, we shall consider separately the incidence matrix of points and $d$-flats of $EG(t,q)$ which pass through the origin, and the incidence matrix of points and $d$-flats which do not pass through the origin in $EG(t,q)$. Here, $1 \leq d \leq t-1$. The affine case differs only slightly from the projective case, treated in Section 2.7.

Let $\Sigma$ be a $d$-flat in $EG(t,q)$ which passes through the origin. Let $\alpha$ be a primitive element of $GF(q^t)$. Then $\Sigma$ is given as the set of all those points, $\alpha^u$, of $GF(q^t)$ such that

$$(2.8.1) \quad \alpha^u = a_1 \alpha^{e_1} + a_2 \alpha^{e_2} + \ldots + a_d \alpha^{e_d},$$

where $\alpha^{e_1}, \ldots, \alpha^{e_d}$ are independent elements of $GF(q^t)$ and where $a_1, \ldots, a_d$ run independently over the elements of $GF(q)$, not all zero. $0$ is also on $\Sigma$.

In [24], it is shown that, starting with an initial $d$-flat $\Sigma$, passing through the origin, the transformation

$$ \alpha^u \rightarrow \alpha^{u+1} $$

$$ 0 \rightarrow 0 $$

on the points of $\Sigma$ yields another $d$-flat passing through the origin.

We may thus generate $d$-flats from $\Sigma$ by increasing the exponent of $\alpha$ by $1,2,\ldots$ in the representation of the points of $\Sigma$, other than the origin. The cycle of the flat $\Sigma$ is shown in [24] to be at most $v'=(q^t-1)/(q-1)$. 
If the points on Σ, other than the origin, are represented by $\alpha^1, ..., \alpha^{k-1}$, where the number of points on a d-flat is $k = q^d$, we define the incidence polynomial of Σ as
\[ \theta_\Sigma(x) = \sum_{i=1}^{u_1} x^1 + ... + x^{u_{k-1}}. \]
We observe that, over $\text{GF}(q^t)$, $\theta_\Sigma(1) = q^d - 1 \equiv -1, \text{ mod } p$. Hence, $\theta_\Sigma(1) \neq 0$.

Let $m$ be an integer such that $1 \leq m \leq q^t - 2$. Then
\[ \theta_\Sigma(\alpha^m) = \sum _{\alpha} (a_1 \alpha^1 + ... + a_d \alpha^d)^m. \]
Since $0^m = 0$, for $m > 0$, we may consider the summation to be taken over all possible choices of $a_1, a_2, ..., a_d$ as elements of $\text{GF}(q)$. In an analogous development of equation (2.7.7), we obtain
\[ (2.8.2) \quad \theta_\Sigma(\alpha^m) = (-1)^d \sum_k \binom{m}{k_1(q-1), ..., k_d(q-1)} \alpha^{k_1(q-1) + ... + k_d(q-1)}, \]
where the summation is taken over all choices of $k_1, ..., k_d$ such that
\[ 0 < k_v(q-1) \leq m, \quad v = 1, ..., d, \quad k_1(q-1) + ... + k_d(q-1) = m. \]
Thus, unless $m \equiv 0, \text{ mod } q-1$, $\theta_\Sigma(\alpha^m) = 0$. Moreover, as was argued in Section 2.7, as necessary and sufficient condition that $\theta_\Sigma(\alpha^m) = 0$, for all d-flats Σ passing through the origin in $\text{EG}(t,q)$, is that each of the multinomial coefficients in equation (2.8.2) is divisible by $p$, i.e., is congruent to zero mod $p$.

Replacing $m$ by $m'(q-1)$, we have an exactly analogous situation as in the case of $(d-1)$-flats in $\text{PG}(t-1,q)$ and the following two theorems may be similarly proved.

**Theorem 2.8.1** Let Σ be a d-flat passing through the origin in $\text{EG}(t,p)$:

(i) $\theta_\Sigma(1) \neq 0$;
(ii) For \(1 \leq m \leq q^t - 2\), if \(m \neq 0\), mod \(q-1\), \(\theta_\Sigma(\alpha^m) = 0\);

(iii) For \(m = m'(p-1)\), where \(1 \leq m' \leq v'-1\), \(\theta_\Sigma(\alpha^m) = 0\) for every \(d\)-flat \(\Sigma\) passing through the origin if and only if \(D_p(m'(p-1)) = r(p-1)\), where \(1 \leq r \leq d-1\). Here, \(v' = (p^t-1)(p-1)\).

**Theorem 2.8.2** Let \(\Sigma\) be a \(d\)-flat passing through the origin in \(EG(t,q)\), where \(q = p^n\). Then

(i) \(\theta_\Sigma(1) \neq 0\);

(ii) For \(1 \leq m \leq q^t - 2\), if \(m \neq 0\), mod \(q-1\), \(\theta_\Sigma(\alpha^m) = 0\).

(iii) For \(1 \leq m \leq q^t - 2\), if \(m = m'(q-1)\), where \(1 \leq m' \leq v'-1\), \(\theta_\Sigma(\alpha^m) = 0\) for every \(d\)-flat \(\Sigma\) passing through the origin if \(D_q(m'(q-1)) = r(q-1)\), where \(1 \leq r \leq d-1\). Here, \(v' = (q^t-1)/(q-1)\).

**Theorem 2.8.3** Let \(\Sigma\) be a \(d\)-flat in \(EG(t,q)\), passing through the origin, where \(q = p^n\). Then

(i) \(\theta_\Sigma(1) \neq 0\);

(ii) For \(1 \leq m \leq q^t - 2\), unless \(m \equiv 0\), mod \(q-1\), \(\theta_\Sigma(\alpha^m) = 0\).

(iii) For \(1 \leq m \leq q^t - 2\), let \(m = m'(q-1)\), where \(1 \leq m' \leq v'-1\). Then \(\theta_\Sigma(\alpha^m) = 0\) for every such \(d\)-flat \(\Sigma\) if and only if, for some \(j=0,1,\ldots,n-1\), \(D_q(p^j(m'(q-1))) = r(q-1)\), where \(1 \leq r \leq d-1\).

From Section 2.7, the number of integers \(m\), \(1 \leq m \leq v'-1\), such that \(D_q(m(q-1)) = r(q-1)\) where \(1 \leq r \leq d-1\) is equal to \(R_d(t-1,q)\), defined by equations (2.7.10) and (2.7.11). From the above theorems, it may be shown that the following theorem is true, in an analogous manner as that used in Section 2.7.

**Theorem 2.8.4** Over GF(q), the rank of the incidence matrix \(N\) of points other than the origin and \(d\)-flats passing through the origin in \(EG(t,q)\) is at most equal to \(v' - R_d(t-1,q)\). In the case \(q = p\), this is
exact, i.e., the rank of $N$ is equal to $v' - R_{d-1}(t-1, p)$.

The case of d-flats in $EG(t, q)$ which do not pass through the origin has been partially treated by Weldon [30]. For completeness, we shall repeat some of the results found in [30].

Suppose $\Sigma$ is a d-flat of $EG(t, q)$ which passes through the point $\alpha^c$ and which belongs to the same parallel bundle as the flat through the origin with defining points $\alpha^1, ..., \alpha^d$. Then the points on $\Sigma$ are given by those elements $\alpha^u$ of $GF(q^t)$ such that

$$\alpha^u = \alpha^c + a_1 \alpha^1 + ... + a_d \alpha^d,$$

where $a_1, ..., a_d$ run through the elements of $GF(q)$.

The incidence polynomial of $\Sigma$ is the polynomial $\theta_{\Sigma}(x)$, defined as

$$\theta_{\Sigma}(x) = \sum_u x^u$$

where the summation is taken over all integers $u$, $0 \leq u \leq q^t - 2$, such that $\alpha^u$ is given by equation (2.8.3).

Since there are $q^d$ points on $\Sigma$, $\theta_{\Sigma}(1) = 0$, over $GF(q^t)$.

For $1 \leq m \leq q^t - 2$,

$$\theta_{\Sigma}(\alpha^m) = \sum_u (\alpha^u)^m$$

$$= \sum_a \left( \alpha^a + a_1 \alpha^1 + ... + a_d \alpha^d \right)^m$$

$$= \sum_a \left\{ \sum_j a_1^{j_0} \cdots a_d^{j_d} \binom{m}{j_0, j_1, ..., j_d} \right\} c^{j_0} e_1^{j_1} \cdots e_d^{j_d} \alpha^{d'}.$$
where the inner summation is taken over all choices of \( j_0, j_1, \ldots, j_d \) such that \( j_0 + j_1 + \ldots + j_d = m \) and \( 0 \leq j_v \leq m, v=0,1,\ldots,d \)

Interchanging the order of summation and noting that, for \( v=1,\ldots,d \),

\[
\sum_{a, e \in \mathbb{F}(q)} a_{j_v} \overset{\text{def}}{=} \left\{ \begin{array}{ll} -1, & \text{if } j_v = k_v(q-1), k_v > 0, \\
0, & \text{otherwise}, \end{array} \right.
\]

we have

\[
(2.8.4) \quad \Theta_\Sigma (\alpha^m) = (-1)^d \sum_{j_0, k_1(q-1), \ldots, k_d(q-1)} \left( \begin{array}{c} m \\ j_0, k_1(q-1), \ldots, k_d(q-1) \end{array} \right) \\
\times c_{j_0 + k_1(q-1) + \ldots + k_d(q-1)},
\]

where the summation is taken over all choices of \( j_0, k_1(q-1), \ldots, k_d(q-1) \), such that \( 0 \leq j_0 \leq m, 0 < k_v(q-1) < m, v=1,\ldots,d \), and

\[
j_0 + k_1(q-1) + \ldots + k_d(q-1) = m.
\]

If each of the multinomial coefficients in equation (2.8.4) is divisible by \( p \), then \( \Theta_\Sigma (\alpha^m) = 0 \), for every \( d \)-flat \( \Sigma \) not passing through the origin in \( E\Gamma(t,q) \).

If one of these multinomial coefficients is not divisible by \( p \), it is not divisible by \( q = p^n \). This will hold if and only if

\[
(2.8.5) \quad D_q(m) = D_q(j_0) + D_q(k_1(q-1)) + \ldots + D_q(k_d(q-1)).
\]

Since \( D_q(j_0) \geq 0 \) for \( j_0 \geq 0 \) and for \( v=1,\ldots,d \), \( D_q(k_v(q-1)) \geq q-1 \), equation (2.8.5) holds only if \( D_q(m) \geq d(q-1) \). Thus, if \( D_q(m) < d(q-1) \), each of the multinomial coefficients must be divisible by \( q \) and hence by \( p \). We have the following theorem.

**Theorem 2.8.5** If \( \Sigma \) is a \( d \)-flat in \( E\Gamma(t,q) \) which does not pass through the origin, then

1. \( \Theta_\Sigma (1) = 0; \)
(ii) For \(1 \leq m \leq q^t-2\), if \(D_q(m) < d(q-1)\), then \(\theta_\Sigma(\alpha^m) = 0\) for all such \(d\)-flats \(\Sigma\).

Recall that the function \(B_s(t,q)\), defined by equation (2.7.10), is the number of ways of choosing \(t+1\) integers \(c_0, c_1, \ldots, c_t\) such that \(0 \leq c_i \leq q-1, i=0,1,\ldots,t\), and \(c_0 + c_1 + \ldots + c_t = s(q-1)\). For \(0 \leq m \leq q^t-2\), let the \(q\)-adic representation of \(m\) be

\[
m = A_0 + A_1 q + \ldots + A_{t-1} q^{t-1},
\]

where \(0 \leq A_i \leq q-1, i=0,1,\ldots,t-1\). Then

\[
D_q(m) = A_0 + A_1 + \ldots + A_{t-1}.
\]

Since the \(q\)-adic representation of \(m\) is unique, the number of integers \(m\), \(0 \leq m \leq q^t-2\), such that \(D_q(m) < d(q-1)\) is equal to the number of ways of choosing \(t\) integers \(A_0, A_1, \ldots, A_{t-1}\) such that \(0 \leq A_i \leq q-1, i=0,\ldots,t-1\), and \(A_0 + A_1 + \ldots + A_{t-1} < d(q-1)\). Let this number be \(K_d(t,q)\).

Let \(D_s(t,q)\) be the number of ways of choosing \(t\) integers \(A_0, \ldots, A_{t-1}\) such that \(0 \leq A_i \leq q-1\) and \((s-1)(q-1) \leq A_0 + \ldots + A_{t-1} < s(q-1)\). Then

\[
(2.8.6) \quad K_d(t,q) = \sum_{s=1}^d D_s(t,q).
\]

Suppose that \(A_0 + \ldots + A_{t-1} = s(q-1) - E_t\), where \(0 < E_t \leq q-1\). Then

\[
A_0 + A_1 + \ldots + A_{t-1} + E_t = s(q-1).
\]

The number of integral solutions \(A_0, \ldots, A_{t-1}, E_t\) of this equation such that \(0 \leq A_i \leq q-1, i=0,1,\ldots,t-1\) and \(0 \leq E_t \leq q-1\) is equal to \(B_s(t,q)\). But this number also includes those solutions \(A_0, \ldots, A_{t-1}, E_t\) such that \(E_t = 0\), i.e., such that \(A_0 + A_1 + \ldots + A_{t-1} = s(q-1)\). There are \(B_s(t-1,q)\) such solutions. Hence the required number of solutions is
D_s(t,q) = B_s(t,q) - B_s(t-1,q) .

Substituting this into equation (2.8.6), we obtain

\[ K_d(t,q) = \sum_{s=1}^{d} B_s(t,q) - \sum_{s=1}^{d} B_s(t-1,q) . \]

But

\[ R_d(t,q) = \sum_{s=1}^{d} B_s(t,q) . \]

Therefore,

(2.8.7) \[ K_d(t,q) = R_d(t,q) - R_d(t-1,q) . \]

Combining the above results with Theorem 2.8.5, we have

**Theorem 2.8.6** The number of integers m, 0 ≤ m ≤ \(q^t-2\), such that
\[ \theta_{\Sigma}(\alpha^m) = 0 \] for every d-flat \(\Sigma\) not passing through the origin in \(EG(t,q)\) is at least equal to \(K_d(t,q)\).

As a corollary, it may be shown that the rank of the corresponding incidence matrix of points other than the origin and d-flats not passing through the origin in \(EG(t,q)\) is at most equal to \(q^t-1-K_d(t,q)\).

Analogous to Theorem 2.8.3 is the following theorem.

**Theorem 2.8.7** Let \(\Sigma\) be a d-flat in \(EG(t,q)\) which does not pass through the origin. Then

(i) \[ \theta_{\Sigma}(1) = 0 \]

(ii) For \(1 ≤ m ≤ q^t-2\), if, for some \(j=0,1,\ldots,n-1\), \(D_q(p^j m) < d(q-1)\), then \(\theta_{\Sigma}(\alpha^m) = 0\) for all such d-flats \(\Sigma\).
CHAPTER III

GEOMETRIC CODES

3.1 Introduction

A number of classes of cyclic codes to which a majority decoding algorithm is applicable may be given a geometric interpretation. We shall call such codes geometric codes. Included in this grouping are the Reed-Muller codes and some of their generalizations. We shall define several new classes of geometric codes and investigate some of their properties, particularly as related to the BCH codes. A majority decoding algorithm for the geometric codes will also be given.

3.2 Cyclic codes

A familiarity with the theory of linear and cyclic codes will be assumed in this chapter. We state here a few of the specialized results on cyclic codes which are needed later. For a more complete description of cyclic codes, see Peterson [21], for example.

A q-ary linear code C is a vector subspace of the vector space $V_N$ of all N-vectors with elements from $GF(q)$; q being a prime power, say $q = p^n$. The dimension, k, of the subspace C is called the number of information symbols of the code C. The length of the code is N. C is referred to as an $(N,k)$ code. Denote the orthogonal or null space of C by $C_D$. If $r = N - k$, $C_D$ is an $(N,r)$ linear code called the dual code of C. The number r is the redundancy of the code C.
A matrix $G$ whose row vectors span or generate $C$ is called a **generator matrix** of $C$. A matrix $H$ whose row vectors span the dual code is called a **parity check matrix** of $C$. A vector $c'=(c_0,c_1,\ldots,c_{N-1})$ is a code vector of $C$ if and only if $c' \in C$, which is true if and only if

$$(3.2.1) \quad Hc = 0.$$ 

Each of the equations in (3.2.1) is a parity check equation. Indeed, if $h'=(h_0,h_1,\ldots,h_{N-1})$ is a vector of $C_D$, then $h'$ yields the parity check equation

$$h_0c_0 + h_1c_1 + \ldots + h_{N-1}c_{N-1} = 0$$

A linear code $C$ (a vector subspace of $V_N$) is cyclic if, for every code vector $c'=(c_0,c_1,\ldots,c_{N-1})$ of $C$, the vector $(c_{N-1},c_0,\ldots,c_{N-2})$, obtained from $c'$ by shifting each coordinate one unit to the right, is also a code vector of $C$. A convenient representation of cyclic codes may be made through the theory of ideals in the residue class ring $GF(q)[x]/(x^{N-1})$. 

In the residue class ring $GF(q)[x]/(x^{N-1})$, we correspond the (residue class of the) polynomial $c(x) = c_0 + c_1 x + \ldots + c_{N-1} x^{N-1}$ with the vector $c' = (c_0,c_1,\ldots,c_{N-1})$. $c(x)$ is called the polynomial of the vector $c'$, and $c'$, the vector of $c(x)$. Under this correspondence, it may be shown that a linear code is cyclic if and only if it is an ideal in the ring $GF(q)[x]/(x^{N-1})$. Each such ideal $C$ contains a unique monic **generator polynomial**, $g(x)$, of smallest degree less than $N$ such that (the residue class of) $c(x) \in C$ if and only if $g(x)$ divides $c(x)$. Moreover, $g(x)$ is a divisor of $x^{N-1}$ in $GF(q)$, say $x^{N-1} = g(x)h(x)$. If the degree of $h(x)$ is $k$, then $g(x)$ is of degree $r = N-k$ and the
code $C$ is an $(N,k)$ cyclic code. The polynomial $h(x)$ is called the parity check polynomial of $C$. The dual code of $C$ is also cyclic and its generator polynomial, denoted $g_D(x)$, is given by

$$g_D(x) = x^k h(x^{-1})$$

and is of degree $k$.

A cyclic code may be specified by the roots of its generator polynomial in an extension field of $\mathbb{GF}(q)$. Suppose $q^m - 1 = Nu$, where $u \geq 1$. (We assume $N$ and $q$ are relatively prime, so that $x^N - 1$ has no repeated roots.) Every root of $x^N - 1$ is an element of $\mathbb{GF}(q^m)$. Let $\alpha$ be an element of $\mathbb{GF}(q)$ of order $N$, i.e., $\alpha^N = 1$ and $1, \alpha, \alpha^2, \ldots, \alpha^{N-1}$ are all distinct. Then the roots of $x^N - 1$ are $1, \alpha, \alpha^2, \ldots, \alpha^{N-1}$. Any subset of these roots, say $\alpha_{u_1}, \alpha_{u_2}, \ldots, \alpha_{u_s}$, specifies a cyclic code $C$. The (residue class of the) polynomial $c(x)$ is a code polynomial of $C$ if and only if $\alpha_{u_1}, \ldots, \alpha_{u_s}$ are roots of $c(x)$. If $\phi_{u_i}(x)$ is the minimum function of $\alpha_{u_i}$, i.e., the monic polynomial of smallest degree less than $m$ in $\mathbb{GF}(q)[x]$ which has $\alpha_{u_i}$ as a root, then $c(x)$ is a code polynomial if and only if $\phi_{u_i}(x)$ divides $c(x)$, $i = 1, \ldots, s$. The generator polynomial is $g(x) = \text{L.C.M.}[\phi_{u_1}(x), \ldots, \phi_{u_s}(x)]$ and is of degree at most equal to $sm$; in general, some of the $\phi_{u_i}(x)$ may be identical, in which case the degree of $g(x)$ is less than $sm$. The degree of $g(x)$ is equal to the number of distinct elements in the sequence $\alpha_{u_1}, \alpha_{u_2}, \ldots, \alpha_{u_s}, \ldots$, i.e., the number of distinct residues, mod $N$, in the sequence $u_1, qu_1, \ldots, u_s, qu_s, \ldots$.

If $N = q^m - 1$, i.e., if $u = 1$, then $\alpha$ is a primitive element of $\mathbb{GF}(q^m)$.
and the code \( C \) is called a \textbf{primitive cyclic code}. If \( u > 1 \), then \( \alpha \) is not a primitive element and the code is a \textbf{non-primitive cyclic code}.

Every element of \( GF(q^m) \) may be represented as a power of a primitive element, \( \beta \), or as a polynomial in \( \beta \) of degree at most \( m-1 \) with coefficients in \( GF(q) \). Suppose \( \beta^u = b_0 + b_1 \beta + \ldots + b_{m-1} \beta^{m-1} \).

Corresponding each such element with the column vector of coefficients, it may be verified that the matrix \( H \), given by

\[
H = \begin{bmatrix}
1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{N-1} \\
1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{N-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha_s & \alpha_s^2 & \ldots & \alpha_s^{N-1}
\end{bmatrix},
\]

when regarded as a \( sm \times N \) matrix over \( GF(q) \), is a parity check matrix of the code \( C \), specified by \( \alpha_1^u, \ldots, \alpha_s^u \) as roots of every code polynomial.

Associated with the cyclic \((N,k)\) code \( C \) is an \textbf{extended cyclic code}, \( C_e \), which is not a cyclic code. If the generator polynomial of \( C \) does not have \( 1 \) as a root, then \( C_e \) is defined as the linear code with parity check matrix

\[
H_e = \begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
0 & 0 & 0 & \ldots & 0 \\
0 & H \\
0 & 0 & 0 & \ldots & 0
\end{bmatrix}.
\]

In this case, \( C_e \) is a \((N+1,k)\) code. If \( 1 \) is a root of \( g(x) \),
suppose \( \alpha^u = 1 \), then \( C_e \) is the linear code with parity check matrix

\[
H_e = \begin{bmatrix}
1 \\
0 \\
0 \\
\vdots \\
0
\end{bmatrix}
\]

in which case, \( C_e \) is a \((N+1,k+1)\) code. In either case, the generator polynomial of the code \( C \) will also be referred to as the generator polynomial of the extended code \( C_e \).

The best cyclic codes yet discovered are the well known Bose-Chaudhuri-Hocquenghem (BCH) codes [5], [6], [13], which are most easily defined in terms of the roots of the generator polynomial.

For any integer \( m \) and any prime power \( q \) let \( \alpha \) be a non-zero element of \( \text{GF}(q^m) \) of order \( N \). \( N \) must be a divisor of \( q^m - 1 \), say \( q^m - 1 = Nu \). Let \( c \) and \( d \) be integers, \( c \leq d \leq N - 2 \). The \( q \)-ary cyclic code whose generator polynomial, \( g(x) \), has roots

\[
(3.4.1) \quad \alpha^c, \alpha^{c+1}, \ldots, \alpha^{c+d-2}
\]

is a BCH code. Usually, \( c \) is taken as 1. In the case \( u=1 \), the code is a primitive BCH code; otherwise, it is a non-primitive BCH code.

The matrix

\[
H = \begin{bmatrix}
1 & \alpha^c & (\alpha^c)^2 & \ldots & (\alpha^c)^{N-1} \\
1 & \alpha^{c+1} & (\alpha^{c+1})^2 & \ldots & (\alpha^{c+1})^{N-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{c+d-2} & (\alpha^{c+d-2})^2 & \ldots & (\alpha^{c+d-2})^{N-1}
\end{bmatrix}
\]
when considered as a \((d-1) \times N\) matrix over \(\text{GF}(q^m)\), may be shown to have the property that no \(d-1\) columns of \(H\) are dependent over \(\text{GF}(q^m)\). Since \(H\) may also be regarded as a \(m(d-1) \times N\) parity check matrix over \(\text{GF}(q)\) and no \(d-1\) columns of \(H\) are dependent over \(\text{GF}(q)\), then the code has minimum distance at least \(d\). For this reason, the number \(d\) is often referred to as the designed distance of the \(\text{BCH}\) code specified by equation (3.4.1). If \(d=2t+1\), it is possible to correct up to \(t\) errors.

Since the rank of \(H\), over \(\text{GF}(q)\), is at most \(m(d-1)\), the redundancy of the \(\text{BCH}\) code is at most \(m(d-1)\) and the number of information symbols is at least \(N-m(d-1)\). The actual redundancy is equal to the degree of \(g(x)\), the generator polynomial, and may be less than \(m(d-1)\), depending on the degrees of the minimum functions of the roots in (3.4.1). An investigation of the number of information symbols in \(\text{BCH}\) codes may be found in [2] and in [17].

In some cases the true minimum distance of a \(\text{BCH}\) code may exceed the designed distance. For example, the Golay \((23,12)\) code is a non-primitive \(\text{BCH}\) code for which the designed distance is 5, but for which the actual distance is known to be 7 [19], [21]. Several authors have studied the distance properties of \(\text{BCH}\) codes for particular values of the parameters [14], [15], [19], [29]; most \(\text{BCH}\) codes are found to have their true minimum distances equal to the designed distance of the code.

The most important \(\text{BCH}\) codes are the primitive binary \(\text{BCH}\) codes, obtained by setting \(n=2\), \(u=1\), \(c=1\) and \(d=2t+1\). If \(\alpha\) is a primitive element of \(\text{GF}(2^m)\), the generator polynomial \(g(x)\) of the corresponding
A BCH code has roots $\alpha, \alpha^2, \ldots, \alpha^{2^t-1}$. If $\phi_i(x)$ is the minimum function of $\alpha^i$, then $\phi_{2i}(x) = \phi_i(x)$. $g(x)$ is given by

$$g(x) = \text{L.C.M.} \{\phi_1(x), \phi_2(x), \ldots, \phi_{2^t-1}(x)\}$$

and has degree at most equal to $mt$. The length of the code is $N=2^m-1$ and the number of information symbols is at least $2^m-1-mt$. The code will correct $t$ or fewer errors with certainty.

3.3 Majority decoding

A relatively simple decoding procedure, called majority decoding, is applicable to some linear codes. A comprehensive study of majority decoding and more generally, threshold decoding, particularly as applied to convolutional codes, is given by Massey [18]. We shall restrict our discussion to majority decoding of linear and cyclic codes.

The concept of majority decoding of linear codes is based on a certain 'orthogonality structure' the parity check equations may have. We first define this orthogonality structure and show how it relates to majority decoding.

Let $C$ be a $(N,k)$ linear code with symbols from $\mathbb{GF}(q)$. $C$ is completely specified by a set of parity check equations, which need not be linearly independent. Suppose a set of $r' \geq r=N-k$ parity check equations for $C$ is

$$h_{10^c \cdot \cdot \cdot h_{N-1}^c N-1} = 0$$

$$h_{20^c \cdot \cdot \cdot h_{2,N-1}^c N-1} = 0$$

$$\cdots \cdots$$

$$h_{r'0^c \cdot \cdot \cdot h_{r',N-1}^c N-1} = 0.$$
A vector \( c' = (c_0, c_1, \ldots, c_{N-1}) \) is a code vector of \( C \) if and only if the coordinates of \( c' \) satisfy the system of equations \((3.3.1)\). The \( j \)th equation is said to check the symbol \( d_i \) if \( h_{ji} \neq 0 \). A subset of \( J \) equations, say the first \( J \) equations in \((3.3.1)\), is said to be orthogonal on the symbol \( c_i \) \([18]\) if

1. \( h_{ji} = 1, j = 1, 2, \ldots, J, \) and
2. \( h_{ji} = 0 \) for all but at most one \( j = 1, 2, \ldots, J \) and for any fixed \( i' \neq i \).

That is, the first \( J \) equations are orthogonal on \( c_i \) if each of the first \( J \) equations checks \( c_i \) with coefficient 1 and no other symbol is checked by more than one of these \( J \) equations.

For example, in the system of equations

\[
\begin{align*}
c_0 + c_1 + c_3 &= 0 \\
c_1 + c_2 + c_4 &= 0 \\
c_2 + c_3 + c_5 &= 0 \\
c_3 + c_4 + c_6 &= 0 \\
c_0 + c_4 + c_5 &= 0 \\
c_1 + c_5 + c_6 &= 0 \\
c_0 + c_2 + c_6 &= 0,
\end{align*}
\]

the first, fifth and seventh equations are orthogonal on \( c_0 \); the first, second and sixth are orthogonal on \( c_1 \), etc.

Let us represent the system of equations \((3.3.1)\) in matrix form as

\[(3.3.2) \quad H \underline{c} = 0,\]

where \( H \) is a \( r' \times N \) parity check matrix of rank \( r \) over \( GF(q) \).
Suppose \( t' = (t_0, t_1, \ldots, t_{N-1}) \) is a transmitted code vector of \( C \) and the corresponding received vector is \( r' = (r_0, r_1, \ldots, r_{N-1}) \). The error vector is \( e' = (e_0, e_1, \ldots, e_{N-1}) \), where \( r' = t' + e' \). The syndrome of \( r' \) is \( s = H r \). Since \( t' \) satisfies equations (3.3.2), we have \( s = H e \), which we may write as

\[
\begin{align*}
    h_{10}e_0 + h_{11}e_1 + \cdots + h_{1,N-1}e_{N-1} &= s_1 \\
    h_{20}e_0 + h_{21}e_1 + \cdots + h_{2,N-1}e_{N-1} &= s_2 \\
    &\quad \cdots \\
    h_{r'0}e_0 + \cdots + h_{r',N-1}e_{N-1} &= s_{r'}.
\end{align*}
\]

(3.3.3)

It is desired to solve the system (3.3.3) for the (unknown) error vector, given the matrix \( H \) and the syndrome vector \( s' = (s_1, \ldots, s_{r'}) \). This is called the decoding of the code \( C \).

If it is possible to find a set of \( J \) parity check equations from (3.3.3) which are orthogonal on the symbol \( e_0 \), for example, then a majority decoding algorithm for determining \( e_0 \) is given by the following theorem, due to Massey [13].

**Theorem 3.3.1.** Suppose

\[
(3.3.4)
\]

is a system of \( J \) equations orthogonal on the symbol \( e_0 \). Provided that \( \lfloor J/2 \rfloor \) or fewer of the symbols checked by these \( J \) equations are non-zero, then \( e_0 \) is given correctly by the following rule:

1. \( e_0 \) is that value of \( GF(q) \) which is assumed by the greatest fraction of the \( \{s_j\} \), provided such a value exists.

\(^{1}\) The notation \([x]\) denotes the greatest integer less than or equal to \( x \).
In the case where no single value is assumed by a strict plurality of the \( s_j \), \( e_0 \) is zero.

This theorem is proved in [18]. An examination of the proof as given in [18] suggests that the condition of the orthogonality of the equations (3.3.4) on \( e_0 \) is not necessary, as we shall prove in the following theorem which is a generalization of the above; this next theorem appears also in Rudolph [26].

**Theorem 3.3.2** Suppose that each of the equations (3.3.4) checks the symbol \( e_0 \) and assume that, for any \( i \neq 0 \), \( e_i \) is checked by at most 5 of these \( J \) equations. Let \( A_j = s_j / h_j \). Then, provided at most \( [J/25] \) of the symbols checked by these \( J \) equations are non-zero, \( e_0 \) is given correctly by the following rule.

1. \( e_0 \) is that value of \( GF(q) \) which is assumed by the greatest fraction of the \( A_j \), if such a most frequent value exists.
2. In the case where no single value is assumed by a strict plurality of the \( A_j \), \( e_0 \) is zero.

**Proof.** Suppose at most \( t = [J/25] \) of the symbols checked by the equations (3.3.4) are non-zero. First, assume that all symbols other than \( e_0 \) are zero. Then

\[
A_j = s_j / h_j = e_0, \quad j=1,2,\ldots,J,
\]

and the decision rule of the theorem is correct. If one of the other symbols is non-zero, then at most 5 of the \( A_j \) of equations (3.3.5) are different from \( e_0 \). In general, if \( s \) other symbols are non-zero, at most \( s5 \) of the \( A_j \) of equations (3.3.5) are different from \( A_j \), since each such symbol can affect at most 5 of the \( A_j \).
If \( e_0 = 0 \), then if \( t \) or fewer of the symbols are non-zero, at most \( t \delta = \lfloor J/2 \rfloor \) of the \( A_j \) are non-zero and the decision rule of the theorem gives the correct value of \( e_0 \). If \( e_0 \neq 0 \), then at most \( (t-1) \delta < \lfloor J/2 \rfloor \) of the \( A_j \) are not equal to \( e_0 \) and the decision rule of the theorem is correct.

We observe that Theorem 3.3.1 is a particular case of Theorem 3.3.2 with \( \delta = 1 \). The decoding rule of Theorem 3.3.2 will be referred to as majority decoding. It should be remarked that a set of \( J \) equations satisfying the conditions of Theorem 3.3.2 must be available for each \( e_i \), \( i=0,1,\ldots,N-1 \) for complete decoding of an error vector. More accurately, only the information symbols in an error vector need be decoded if the encoding procedure is available to reconstruct the remaining symbols of the corresponding codeword.

For the case of a cyclic code, there is a 'symmetry' which ensures that if one symbol may be decoded by majority decoding, then all the other \( N-1 \) symbols in a codeword may also be so decoded.

The majority decoding algorithms of Theorems 3.3.2 and 3.3.1 are both one-step majority decoding procedures, i.e., only one determination of the majority of the \( A_j \) is necessary to decode a particular symbol. The algorithm may be used to decode certain sums of symbols, such as \( e_0 + e_1 \), provided \( J \) equations which check both \( e_0 \) and \( e_1 \) may be found. Suppose a number of sums involving \( e_0 \) may be decoded in this manner. These decoded sums may be treated as new parity checks and the majority decoding procedure could be applied to these new equations to decode \( e_0 \). Such a decoding procedure is referred to as 2-step majority decoding, or in general, \( L \)-step majority decoding. In [18], examples are given of particular codes.
which may be decoded in this manner. The well known binary Reed-Muller codes are such a class of codes. Many of the codes to which this majority decoding procedure is applicable may be given a geometric interpretation and are generalizations of the Reed-Muller codes. This will be discussed in the next sections.

3.4 Geometric codes

Underlying the (cyclic) Reed-Muller codes [20],[25], [15] and some of their generalizations is a geometric interpretation of the dual code. In this section we shall examine some of these codes in this light and in Section 3.5, indicate how such a geometric interpretation yields a majority decoding algorithm.

Let \( \alpha \) be a primitive element of \( \text{GF}(q^t) \) and let \( C \) be a primitive cyclic code of length \( q^t - 1 \) with symbols from \( \text{GF}(q) \). Denote the generator polynomial of \( C \) by \( g(x) \). If the degree of \( g(x) \) is \( r \), then \( C \) is a \( (q^t - 1, q^t - 1 - r) \) code. Let the dual code of \( C \) be \( C_d \), with generator polynomial \( g_d(x) \). If \( h(x) \) is given by

\[
    h(x) = (x^{q^t-1-1})/g(x),
\]

then \( g_d(x) \) is of degree \( k = q^t - 1 - r \) and is given by

\[
    g_d(x) = x^k h(x^{-1}).
\]

We may completely specify \( C \) by specifying the roots of \( g_d(x) \) in \( \text{GF}(q^t) \). Since the degree of \( g_d(x) \) is the number of information symbols of \( C \), it is desirable that \( g_d(x) \) have a relatively large number of roots.

Let \( \Sigma \) be a \( \mu \)-flat in \( EG(t,q) \) with incidence polynomial \( \theta_\Sigma(x) \), defined in Section 2.8. Unless otherwise specified, the origin will not be accounted for. The incidence vector of \( \Sigma \) is the \( (q^t-1) \)-vector
of coefficients of \( \theta_\Sigma(x) \). This incidence vector is a vector of the
dual code \( C_D \) if and only if \( \theta_\Sigma(x) \) is divisible by \( g_D(x) \). We observe
that if \( \alpha^0 = 1 \) is a root of \( g_D(x) \), then the dual code cannot contain
the incidence vector of any flat in \( \text{EG}(t,q) \) which passes through
the origin, for \( 1 \) is not a root of the corresponding incidence poly-
nomial, by Theorem 2.8.2.

We shall refer loosely to a primitive cyclic code of length
\( q^t-1 \) with symbols from \( \text{GF}(q) \) whose dual code contains the incidence
vectors of either all \( \mu \)-flats in \( \text{EG}(t,q) \) or all \( \mu \)-flats of \( \text{EG}(t,q) \)
which do not pass through the origin as a primitive geometric code
of order \( \mu \). In the case the dual contains the incidence vectors of
all \( \mu \)-flats, we shall refer to the code as a primitive geometric code
of type 0; otherwise, if the dual contains only the incidence vectors
of \( \mu \)-flats which do not pass through the origin, we shall refer to
the code as a primitive geometric code of type 1, as necessary.

For the non-primitive case, let \( \beta \) be an element of \( \text{GF}(q^{t+1}) \) of
order \( N=(q^{t+1}-1)/(q-1) \). We may take \( \beta = \alpha^{q-1} \), where \( \alpha \) is a primitive
element of \( \text{GF}(q^{t+1}) \). Let \( C \) be a non-primitive cyclic code of length
\( N \) with symbols from \( \text{GF}(q) \) and let the generator polynomial of the
dual code \( C_D \) be \( g_D(x) \). Then the dual code contains the incidence
vector of the \( \mu \)-flat \( \Sigma \) of \( \text{PG}(t,q) \) if and only if the incidence poly-
nomial \( \theta_\Sigma(x) \) of \( \Sigma \), defined in Section 2.7, is divisible by \( g_D(x) \).
We shall refer to a non-primitive cyclic code of length \( N \) whose dual
contains the incidence vectors of every \( \mu \)-flat in \( \text{PG}(t,q) \) as a non-
primitive geometric code of order \( \mu \).
Theorem 3.4.1

(1) A sufficient condition for a cyclic code of length $q^{t-1}$ to be a type 0 primitive geometric code of order $\mu$ is that every root $\alpha^h$ of the generator polynomial $g_\mathcal{D}(x)$ of the dual code satisfy

\begin{equation}
1 \leq h \leq q^{t-2} \quad \text{and} \quad 0 < D_q(p^jh) < \mu(q-1)
\end{equation}

for some $j = 0, 1, \ldots, n-1$.

(2) A sufficient condition for a cyclic code of length $q^{t-1}$ to be a type 1 primitive geometric code of order $\mu$ is that every root $\alpha^h$ of the generator polynomial of the dual code satisfy

\begin{equation}
0 \leq h \leq q^{t-2} \quad \text{and} \quad D_q(p^jh) < \mu(q-1) \quad \text{for some} \quad j = 0, 1, \ldots, n-1.
\end{equation}

Proof. If a root $\alpha^h$ of $g_\mathcal{D}(x)$ satisfies equation (3.4.1), then, from Theorem 2.8.3, $\alpha^h$ is also a root of the incidence polynomial of every $\mu$-flat in $\mathsf{EG}(t,q)$ which passes through the origin. From Theorem 2.8.4, $\alpha^h$ is also a root of the incidence polynomial of every $\mu$-flat which does not pass through the origin. Hence the dual code contains the incidence vectors of all $\mu$-flats in $\mathsf{EG}(t,q)$, i.e., the code is a type 0 primitive geometric code of order $\mu$.

If $\alpha^h$ satisfies equation (3.4.2), then $\alpha^h$ is also a root of the incidence polynomial of every $\mu$-flat in $\mathsf{EG}(t,q)$ which does not pass through the origin, from Theorem 2.8.7, and the code is a primitive geometric code of order $\mu$ and type 1.

Theorem 3.4.2 A necessary and sufficient condition for a non-primitive cyclic code of length $N = (q^{t+1}-1)/(q-1)$ with symbols from $\mathsf{GF}(q)$ to be a non-primitive geometric code of order $\mu$ is that every root $\beta^h$ of the generator polynomial $g_\mathcal{D}(x)$ of the dual code satisfy
\( (3.4.3) \quad 1 \leq h \leq N-1 \) and \( 0 < D_{q}(p^{j}h(q-1)) \leq \mu(q-1) \)

for some \( j = 0,1, \ldots, n-1. \)

**Proof.** From Theorem 2.7.6, \( \beta^{h} \) is a root of the incidence polynomial
of every \( \mu \)-flat in \( \text{PG}(t,q) \) if and only if \( h \) satisfies equation \( (3.4.3) \).

The most well known geometric codes are the (binary) Reed-Muller codes, of which the duals of the distance 3 and distance 4 Hamming codes are particular cases. The Generalized Reed-Muller codes of Kasami, Lin and Peterson [15] will be shown to be primitive geometric codes. Weldon's Difference-Set Cyclic codes [28] are examples of non-primitive geometric codes. We shall briefly describe these and other geometric codes here and then define new classes of both primitive and non-primitive geometric codes. A summary of these codes is given in Table 3.1.

With the exception of the Hamming codes, each of the above codes may be described conveniently in terms of the roots of the generator polynomial of the dual code.

**Definition 3.4.1** Let \( \alpha \) be a primitive element of \( \text{GF}(2^{t}) \). The binary distance 3 Hamming code is defined as the cyclic code of length \( N = 2^{t}-1 \) with symbols from \( \text{GF}(2) \) such that \( c(x) \) is a code polynomial if and only if \( \alpha \) is a root of \( c(x) \).

**Definition 3.4.2** Let \( \alpha \) be a primitive element of \( \text{GF}(2^{t}) \). The binary distance 4 Hamming code is defined as the cyclic code of length \( N = 2^{t}-1 \) with symbols from \( \text{GF}(2) \) such that \( c(x) \) is a code polynomial if and only if 1 and \( \alpha \) are roots of \( c(x) \).

The properties of the Hamming codes are well known and are
discussed in Peterson [21]. We mention here that the generator polynomial of the distance 3 Hamming code has roots precisely those elements $\alpha^h, 1 \leq h \leq 2^t -2$ such that $D_2(h) = 1$. The generator polynomial of the distance 4 Hamming code has as its roots precisely those elements $\alpha^h, 0 \leq h \leq 2^t -2$, such that $D_2(h) \leq 1$.

**Definition 3.4.3** [15] Let $\alpha$ be a primitive element of $GF(2^t)$. The $v$-th order Reed-Muller code is the cyclic code of length $N = 2^t -1$ with symbols from $GF(2)$ such that the generator polynomial $g_D(x)$ of the dual code has as roots precisely those elements $\alpha^h, 0 \leq h \leq 2^t -2$, such that $D_2(h) \leq v$.

This definition of the Reed-Muller codes is shown in [15] to be equivalent to that of the original Reed-Muller codes [20], [25], with the first coordinate deleted. We shall refer to the original Reed-Muller codes as the extended Reed-Muller codes, for it is shown in [15] that these codes are extended cyclic codes.

**Definition 3.4.4** The modified Reed-Muller code of order $v$ is the cyclic code of length $N=2^t -1$ whose dual code is obtained from the dual code of the $v$th order Reed-Muller code by deleting the element 1 as a root of the generator polynomial.

The generator polynomial of the dual code of the modified Reed-Muller code has as roots those elements $\alpha^h$ such that $1 \leq h \leq 2^t -2$ and $0 < D_2(h) \leq v$.

Let us denote the $v$th order Reed-Muller code by $C_v$ and the dual code by $C_D,v$. For $0 \leq h \leq 2^t -1$, write $h = c_0 + c_1 2^1 + \ldots + c_{t-1} 2^{t-1}$, where
the $c_i$ are 0 or 1. We see that the degree of $g_D(x)$ is
\[ k = 1 + t + \binom{t}{2} + \ldots + \binom{t}{v}. \]
So $C_v$ is a $(2^t-1,k)$ code. The generator polynomial of $C_v$ is
\[ g(x) = x^r h_D(x^{-1}) \]
where
\[ h_D(x) = \frac{x^{2^t-1}-1}{g_D(x)} \]
and is of degree $r = 2^t-1-k$. Now $h_D(x^{-1})$ has as roots those elements $\alpha^{-h}$ such that $0 \leq h \leq 2^t-2$ and $D_2(h) \geq v+1$. But $\alpha^{-h} = \alpha^{2^t-1-h}$ and $D_2(2^t-1-h) = t - D_2(h)$. Hence, $g(x)$ has as roots those elements $\alpha^{h'}$ such that $1 \leq h' \leq 2^t-2$ and $0 < D_2(h') \leq t-v-1$. From Definition 3.4.4, we see that the Reed-Muller code of order $v$ is the dual of the modified Reed-Muller code of order $t-v-1$.

It follows from Theorem 3.4.1 that the $v$th order Reed-Muller code is a type 1 primitive geometric code of order $v+1$ and that the modified $v$th order Reed-Muller code is a type 0 primitive geometric code of order $v+1$.

The preceding results on the Reed-Muller codes are well known, but not generally as a result of the notion of a primitive geometric code.

We may mention here that the distance 3 Hamming code is the dual code of the modified first order Reed-Muller code and the distance 4 Hamming code is the dual of the first order Reed-Muller code.

The following generalization of the Reed-Muller codes to the non-binary case is due to Kasami, Lin and Peterson [15].

**Definition 3.4.5** Let $\alpha$ be a primitive element of $\mathbb{GF}(q^t)$. The $v$th order Generalized Reed-Muller (GRM) code is the cyclic code of
length \( N = q^t - 1 \) with symbols from \( GF(q) \) such that the generator polynomial \( g_\nu(x) \) of the dual code has as roots those elements \( \alpha^h, 0 \leq h \leq q^t - 2 \), such that \( D_q(h) \leq \nu \).

It is shown in [15] that the generator polynomial \( g(x) \) of the \( \nu \)th order GRM code has as roots those elements \( \alpha^h, 1 \leq h \leq q^t - 2 \), such that \( 0 < D_q(h) < t(q - 1) - \nu - 1 \).

We may define a modified GRM code by deleting the root 1 as a root of the generator polynomial of the dual code. More precisely, we have

**Definition 3.4.6** Let \( \alpha \) be a primitive element of \( GF(q^t) \). The modified \( \nu \)th order GRM code is defined as the cyclic code of length \( q^t - 1 \) with symbols from \( GF(q) \) such that the generator polynomial of the dual code has as roots those elements \( \alpha^h, 1 \leq h \leq q^t - 2 \), such that \( 0 < D_q(h) \leq \nu \).

Thus the \( \nu \)th order GRM code is the dual of the \( \mu \)th order modified GRM code, where \( \mu = t(q - 1) - \nu - 1 \).

**Lemma 3.4.1** For \( \nu = \mu(q - 1) + s \), where \( 0 \leq s < q - 1 \), the \( \nu \)th order GRM code is a type 1 primitive geometric code of order \( \mu \) and the \( \nu \)th order modified GRM code is a type 0 primitive geometric code of order \( \mu + 1 \).

**Proof.** If \( D_q(h) \leq \nu \), then \( D_q(h) < \mu(q - 1) \) and the lemma is immediate from Theorem 3.4.1.

We now define a new class of primitive geometric codes, which we call the Affine Geometry codes. We use the term Affine Geometry...
because the term Euclidean Geometry has been applied to a class of
codes by Weldon [30]; we shall discuss these codes later.

**Definition 3.4.7** Let \( \alpha \) be a primitive element of \( \mathbb{GF}(q^t) \), where \( \alpha = p^n \).

The \( m \text{th order Affine Geometry code} \) is the primitive cyclic code of
length \( q^t - 1 \) with symbols from \( \mathbb{GF}(q) \) such that the generator poly­nomial \( g_D(x) \) of the dual code has \( \alpha^h \) as a root if and only if

\[
0 \leq h \leq q^t - 2 \quad \text{and} \quad D_q(p^j h) < \mu(q-1) \quad \text{for some } j=0,1,\ldots,n-1.
\]

This specification of the roots of the polynomial \( g_D(x) \) is
valid, for if \( \alpha^h \) satisfies \( D_q(p^j h) < \mu(q-1) \),
then \( D_q(p^j h) = D_q(p^j h) < \mu(q-1) \). Thus the conjugates \( \alpha^{qh}, \ldots, \alpha^h \)
are also included in the specification of the roots of \( g_D(x) \) if \( \alpha^h \)
is a root of \( g_D(x) \).

As an immediate consequence of Theorem 3.4.1, we have

**Lemma 3.4.2** The \( m \text{th order Affine Geometry code} \) is a type 1 primitive
geometric code of order \( \mu \).

**Definition 3.4.8** Let \( \alpha \) be a primitive element of \( \mathbb{GF}(q^t) \). The
modified \( m \text{th order Affine Geometry code} \) is the primitive cyclic code
of length \( q^t - 1 \) with symbols from \( \mathbb{GF}(q) \) such that the generator poly­nomial of the dual code has \( \alpha^h \) as a root if and only if

\[
1 \leq h \leq q^t - 2 \quad \text{and} \quad 0 < D_q(p^j h) < \mu(q-1) \quad \text{for some } j=0,1,\ldots,n-1.
\]
That is, the modified $\mu$th order Affine Geometry code is obtained from the $\mu$th order Affine Geometry code by deleting the element 1 as a root of the generator polynomial of the dual code. Again, from Theorem 3.4.1, we have

**Lemma 3.4.3** The modified $\mu$th order Affine Geometry code is a type 0 primitive geometric code of order $\mu$.

For the case $q = p$, the $\nu$th order Affine Geometry code is the $v = (\mu(p-1) - 1)$th order GRM code. In general, the $(\mu(q-1) - 1)$th order GRM codes are subcodes of the $\mu$th order Affine Geometry codes, as will follow from this next lemma.

**Lemma 3.4.4** Let $C_1$ and $C_2$ be cyclic codes of length $N$ with symbols from $GF(q)$ and let $g_{D1}(x)$ and $g_{D2}(x)$ be the generator polynomials of the dual codes, respectively. Then $C_1$ is a subcode of $C_2$ if and only if $g_{D1}(x)$ divides $g_{D2}(x)$.

**Proof.** Let the dual codes be $C_{D1}$ and $C_{D2}$, respectively. Then $C_1 \subseteq C_2$ if and only if $C_{D2} \subseteq C_{D1}$. It is thus sufficient to show that $C_{D2} \subseteq C_{D1}$ if and only if $g_{D1}(x)$ divides $g_{D2}(x)$.

Suppose $g_{D1}(x)$ divides $g_{D2}(x)$. Then every code polynomial of $C_{D2}$ is divisible by $g_{D2}(x)$ and $g_{D1}(x)$, i.e., $C_{D2} \subseteq C_{D1}$. Conversely, suppose that every code polynomial of $C_{D2}$ is also a code polynomial of $C_{D1}$. Since $g_{D2}(x)$ is a code polynomial of $C_{D2}$, then $g_{D1}(x)$ is also a code polynomial of $C_{D1}$ and hence is divisible by $g_{D1}$. This
completes the proof of the lemma.

Since every root of the generator polynomial of the dual code of the \((q-1)\)th order GRM code is also a root of the generator polynomial of the dual code of the \(q\)th order Affine Geometry code, the one polynomial divides the other. By Lemma 3.4.4, the \((q-1)\)th order GRM code is a subcode of the \(q\)th order Affine Geometry code. In general, the GRM code will be a proper subcode of the corresponding Affine Geometry code, for there will, in general, be integers \(h\) such that \(D_q(h) \geq (q-1)\) while \(D_q(p^h) < (q-1)\) for some positive \(j\).

For example, take the case \(t = 4\), \(q = 4 = 2^2\) and \(q = 2\). Let \(p = (2(4-1)-1) = 5\). For \(h = 43\), we may write \(43 = 3 + 2 \times 4 + 2 \times 4^2\) and thus \(D_q(43) = 7 > 6\). However, \(2 \times 43 = 86 = 2 + 4 + 4^2 + 4^3\) and \(D_q(86) = 5 < 6\). Thus, \(\alpha^{43}\) is a root of the generator polynomial of the dual of the 2nd order Affine Geometry code, but is not a root of the generator polynomial of the dual of the 5th order GRM code.

For the case \(q = 2^n\), the modified Affine Geometry codes are subcodes of Weldon's Euclidean Geometry codes [30], which we shall describe slightly differently than as given in [30].

\textbf{Definition 3.4.9} Let \(\alpha\) be a primitive element of \(GF(2^{nt})\). The \(v\)th order \textbf{Euclidean Geometry code} is defined as the cyclic code of length
$2^{n_t} - 1$ with symbols from $\mathbb{GF}(2^n)$ such that the roots of the generator polynomial of the dual code are precisely those elements $\alpha^h$ such that $\alpha^h$ is also a root of the incidence polynomial of every $v$-flat in $\text{EG}(t, 2^n)$.

In [30], the Euclidean Geometry codes are described in terms of the parity check polynomial, rather than the generator polynomial of the dual code; this merely reverses every vector in the dual code.

Because of the difficulties of determining exactly those elements $\alpha^h$ which are roots of the incidence polynomials of all $\mu$-flats in $\text{EG}(t, q)$, we have not defined the Affine Geometry codes as a natural extension of the Euclidean Geometry codes to the case $q = p^n$.

Before considering further properties of the $\mu$th order Affine Geometry codes, let us consider the dual codes. We shall show that the duals of Affine Geometry codes are subcodes of certain BCH codes.

Let
\[ h_0 = q^\mu - 1 = (q - 1) + (q - 1)q + \ldots + (q - 1)q^{\mu - 1}, \]
which we may write as
\[ h_0 = (p - 1) + (p - 1)q + \ldots + (p - 1)q^{\mu - 1} \]
\[ + [(p - 1) + (p - 1)q + \ldots + (p - 1)q^{\mu - 1}]p \]
\[ + \ldots \]
\[ + [(p - 1) + (p - 1)q + \ldots + (p - 1)q^{\mu - 1}]p^{n - 1}. \]

From the latter representation, we see that for each $j = 0, 1, \ldots, n - 1$,
\[ D_q(p^j h_0) = \mu(q - 1) \]
and for all $h < h_0$, $D_q(p^j h) < D_q(p^j h) = \mu(q - 1)$.

Thus, the generator polynomial of the dual code of the $\mu$th order Affine Geometry code of length $q^t - 1$ has at least the elements
1, \alpha, \alpha^2, ..., \alpha_{h_0-1}^{h_0-1}, but not \alpha_{h_0} as roots. Therefore, the dual code of a \mu-th order Affine Geometry code is a subcode of the BCH code of length \( q^t-1 \) with designed distance \( h_{0+1} = q^\mu \) and specified by the roots 1, \alpha, \alpha^2, ..., \alpha_{q^\mu-2}^{q^\mu-2}. Then the minimum distance of the dual of the \mu-th order Affine Geometry code is at least equal to \( q^\mu \). Since there are \((t-\mu-1) \cdot (t-1, \mu-1, q)\) \mu-flats in \( \text{EG}(t, q) \) not passing through the origin and the incidence vectors of each such flat have weight \( q^\mu \), there are at least \((q^{t-\mu-1}) \cdot (t-1, \mu-1, q)\) vectors of minimum weight \( q^\mu \) in the dual of the \mu-th order Affine Geometry code and hence also in the above BCH code.

For the modified \mu-th order Affine Geometry code, the generator polynomial of the dual code has at least the elements \alpha, \alpha^2, ..., \alpha_{q^\mu-2}^{q^\mu-2}, but not \alpha_{q^\mu-1}^{q^\mu-1}, as roots. Thus the dual code is a subcode of the BCH code with designed distance \( q^\mu-1 \) and specified by the roots \alpha, \alpha^2, ..., \alpha_{q^\mu-2}^{q^\mu-2}. Since there are \((t-1, \mu-1, q)\) \mu-flats in \( \text{EG}(t, q) \) passing through the origin and each of the corresponding incidence vectors has weight \( q^\mu-1 \), the dual of the modified \mu-th order Affine Geometry code and the above BCH code contain at least \((q^{t-\mu-1}) \cdot (t-1, \mu-1, q)\) vectors of minimum weight \( q^\mu-1 \) and at least \((q^{t-\mu-1}) \cdot (t-1, \mu-1, q)\) vectors of weight \( q^\mu \). We state these results as a lemma.

**Lemma 3.4.5.** The BCH code of length \( q^t-1 \) with designed distance \( q^\mu-1 \) and specified by the roots \alpha, \alpha^2, ..., \alpha_{q^\mu-2}^{q^\mu-2} \) has minimum distance exactly \( q^\mu-1 \). Moreover, there are at least \((t-1, \mu-1, q)\) vectors of weight \( q^\mu-1 \) and at least \((q^{t-\mu-1}) \cdot (t-1, \mu-1, q)\) vectors of weight \( q^\mu \) in the code.
The generator polynomial $g(x)$ of the $\mu$th order Affine Geometry code is given by $g(x) = x^r h_\mu(x^{-1})$, where

$$ h_\mu(x) = \frac{x^{t-1}-1}{g_D(x)} $$

and $r = N-k$, $k$ being the degree of $g_D(x)$. Since $g_D(x)$ has 1 as a root, $h_\mu(x)$ does not. The roots of $h_\mu(x)$ are those elements $\alpha^h$, $1 \leq h \leq q^t-2$, such that $D_q(p^j h) \geq \mu(q-1)$ for each $j=0,1,\ldots,n-1$.

Thus $h_\mu(x^{-1})$ has as roots those elements $\alpha^{q^t-1-h}$ such that $1 \leq h \leq q^t-2$ and $D_q(p^j h \cdot q^t-1-h) \geq (t-\mu)(q-1)$ for each $j=0,1,\ldots,n-1$. Let $h' = q^t-1-h$. Then $D_q(p^j h') = t(q-1) - D_q(p^j h)$, and $h_\mu(x^{-1})$ has as roots those elements $\alpha^{h'}$ such that $1 \leq h' \leq q^t-2$ and for each $j=0,1,\ldots,n-1$, $0 < D_q(p^j h') \leq (t-\mu)(q-1)$. This proves Lemma 3.4.6.

The generator polynomial $g(x)$ of the $\mu$th order Affine Geometry code of length $q^t-1$ has as roots those elements $\alpha^h$, $1 \leq h \leq q^t-2$, such that $0 < D_q(p^j h) \leq (t-\mu)(q-1)$ for each $j=0,1,\ldots,n-1$.

Let $h_1 = q^{t-\mu-1} = (q-1) + (q-1)q + \ldots + (q-1)q^{t-\mu-1}$, which we may write as

$$ h_1 = (p-1) + (p-1)q + \ldots + (p-1)q^{t-\mu-1} $$

$$ + [(p-1) + (p-1)q + \ldots + (p-1)q^{t-\mu-1}] p $$

$$ + \ldots $$

$$ + [(p-1) + (p-1)q + \ldots + (p-1)q^{t-\mu-1}] p^{n-1}. $$

From this representation, we see that for $0 < h \leq h_1$, $0 < D_q(p^j h) \leq D_q(p^j h_1) = (t-\mu)(q-1)$, for each $j=0,1,\ldots,n-1$. Thus the roots of $g(x)$ include the elements $\alpha, \alpha^2, \ldots, \alpha^{h_1}$, and by the BCH theorem, the minimum distance of the code is at least equal to
This bound on the minimum distance of a \( \mu \)th order Affine
Geometry code will be strengthened in Section 3.6.

Likewise, the generator polynomial of the modified \( \mu \)th order
Affine Geometry code has roots those elements \( \alpha^h \) such that
\( 0 \leq h \leq q^{t-2} \) and \( D_q(p^h) \leq (t-\mu)(q-1) \) for each \( j=0,1,\ldots,n-1 \). The
code is a subcode of the BCH code of length \( q^{t-1} \) specified by the
roots \( 1, \alpha, \alpha^2, \ldots, \alpha^{h_1} \) and has minimum distance at least \( h_1+2=q^{t-\mu}+1 \).

We now give a formula for the number of information symbols in
a \( \nu \)th order GRM code, where \( \nu = \mu(q-1)-1 \). Recall that the function
\( \tilde{R}_\mu(t,q) \) was defined in Section 2.7 as
\[
(3.4.4) \quad \tilde{R}_\mu(t,q) = \sum_{s=1}^{\mu} B_s(t,q),
\]
where
\[
(3.4.5) \quad B_s(t,q) = \sum_{i=0}^{L_s(q)} (-1)^i \binom{t+1}{i} \binom{t+s(q-1)-iq}{t}
\]
and where
\[
L_s(q) = \left\lfloor \frac{s(q-1)}{q} \right\rfloor.
\]
The function \( B_s(t,q) \) is the number of ways of choosing \( t+1 \)
integers \( c_0, c_1, \ldots, c_t \) such that \( 0 \leq c_i \leq q-1, i=0,1,\ldots,t, \) and
\( c_0 + \ldots + c_t = s(q-1) \).

**Theorem 3.4.2** The number of information symbols of a \( \nu \)th order
GRM code of length \( q^{t-1} \) with symbols from \( GF(q) \), when \( \nu = \mu(q-1)-1 \),
is equal to \( K_\mu(t,q) \), where
\[
(3.4.6) \quad K_\mu(t,q) = \tilde{R}_\mu(t,q) - \tilde{R}_\mu(t-1,q).
\]

**Proof.** From Definition 3.4.5, the number of information symbols
in a \( v \)th order GRM code is the number of integers \( h, 0 \leq h \leq q^t-2 \), such that \( D_q(h) \leq v \). For \( v = \mu(q-1)-1 \), this is equal to the number of integers \( h, 0 \leq h \leq q^t-2 \), such that \( D_q(h) < \mu(q-1) \). In the proof of Theorem 2.8.6, it was shown that the number of such integers \( h \) is equal to \( K_\mu(t,q) \). Hence the theorem is proved.

**Corollary 3.4.1** The number of information symbols of a \( \mu \)th order Affine Geometry code of length \( q^t-1 \) is at least equal to \( K_\mu(t,q) \). For \( q = p \), this is exact.

**Proof** We have already shown that the \( (v = \mu(q-1)-1) \)th order GRM code is a subcode of the \( \mu \)th order Affine Geometry code and hence the number of information symbols of the Affine Geometry code is at least equal to that of the corresponding GRM code. When \( q = p \), the two codes are identical.

The properties of the Affine Geometry codes discussed in this section are listed in Table 3.2 for various values of the parameters. For \( q = 2 \), these codes are identical to the cyclic Reed-Muller codes and are listed in Table 3.3.

### 3.5 Non-primitive geometric codes

We turn now to a consideration of non-primitive geometric codes. We shall define two new classes of such codes.

**Definition 3.5.1** Let \( \alpha \) be a primitive element of \( GF(q^{t+1}) \) and let \( \beta = \alpha^{q^t-1} \). The Non-Primitive Generalized Reed-Muller code of order \( \mu \) is defined as the cyclic code of length \( N = (q^{t+1}-1)/(q-1) \) with symbols from \( GF(q) \) such that the generator polynomial of the dual code has roots those elements \( \beta^h, 1 \leq h \leq N-1 \), such that
0 < D_q(h(q-1)) ≤ μ(q-1).

Definition 3.5.2 ² Let α be a primitive element of GF(q^t+1) and let β = α^{q-1}. The μth order Projective Geometry code is the cyclic code of length N = (q^t+1-1)/(q-1) with symbols from GF(q) such that the generator polynomial of the dual code has as roots those elements \( β^h, 1 ≤ h ≤ N-1 \), such that 0 < D_q(p^j h(q-1)) ≤ μ(q-1) for some j = 0, 1, ..., n-1. (Here, q = p^n).

The above specifications of the roots of the generator polynomials of the dual codes includes all roots, for if

0 < D_q(p^j h(q-1)) ≤ μ(q-1), then

0 < D_q(p^j h(q-1)) = D_q(p^j h(q-1)) ≤ μ(q-1), i.e., the conjugates of each root \( β^h \) are also included in the specification of the roots.

We observe that the generator polynomial of the dual code of the μth order Non-Primitive GRM code divides that of the dual code of the μth order Projective Geometry code. Hence the μth order Non-Primitive GRM code is a subcode of the μth order Projective Geometry code. One of the motivations for defining the μth order Non-Primitive GRM codes is that the degree of the generator polynomial of the dual code may be easily computed; in fact, an exact formula for it will be given later. However, the corresponding property of the μth order Projective Geometry code is more difficult to deal with, in general.

Lemma 3.5.1 Both the μth order Non-Primitive GRM codes and the μth order Projective Geometry codes are non-primitive geometric codes of...

² This is an explicit formulation of the projective geometry codes discussed by Rudolph [26].
Proof. This lemma is immediate from Theorem 3.4.2.

The \( \mu \)th order Projective Geometry code is optimum in the sense that, the number of information symbols of the code is the maximum possible for a non-primitive geometric code of order \( \mu \). This follows from Theorem 3.4.2, for a necessary condition that a code be a non-primitive geometric code of order \( \mu \) is that every root of the generator polynomial of the dual code be also a root of the generator polynomial of the dual code of the \( \mu \)th order Projective Geometry code. We state this as a lemma.

Lemma 3.5.2. Every non-primitive geometric code of order \( \mu \) and length \( \frac{q^{t+1}-1}{q-1} \) with symbols from \( GF(q) \) is a subcode of the corresponding \( \mu \)th order Projective Geometry code.

Let \( h_0 = \frac{q^{\mu+1}-1}{q-1} \). Then \( h_0(q-1) = (q-1) + (q-1)q + \ldots + (q-1)q^\mu \), which we may write as

\[
h_0(q-1) = (p-1) + (p-1)q + \ldots + (p-1)q^\mu \\
+ \left[ (p-1) + (p-1)q + \ldots + (p-1)q^\mu \right] p^n \\
+ \ldots \\
+ \left[ (p-1) + (p-1)q + \ldots + (p-1)q^\mu \right] p^{n-1}.
\]

From this, we observe that for each \( j = 0, 1, \ldots, n-1 \), \( D_q(p^j h_0(q-1)) = (\mu+1)(q-1) \), and for \( 1 \leq h \leq h_0 \), \( 0 < D_q(p^j h(q-1)) < D_q(p^j h_0(q-1)) = (\mu+1)(q-1) \), i.e., \( 0 < D_q(p^j h(q-1)) \leq \mu(q-1) \).

Let the generator polynomial of the dual code of the \( \mu \)th order Projective Geometry code by \( g_D(x) \). The \( g_D(x) \) has at least \( \beta, \beta^2, \ldots, \beta^{h_0-1} \) as roots, but not \( \beta^{h_0} \). The dual code of the \( \mu \)th
order Projective Geometry code is thus a subcode of the non-primitive
BCH code of length $N$ and designed distance $h_0$, specified by the roots
$\beta, \beta^2, \ldots, \beta^{h_0-1}$. The minimum distance of the dual code and the BCH
code is at least $h_0$. But the weight of the incidence vector of a
$\mu$-flat in $\text{PG}(t,q)$ is equal to $h_0$ and by Lemma 3.5.1, the dual of the
$\mu$th order Projective Geometry code contains at least $\phi(t,\mu,q)$ such
vectors. This proves the following lemma.

**Lemma 3.5.3** The non-primitive BCH code of length $(q^{t+1}-1)/(q-1)$
with designed distance $h_0 = (q^{\mu+1}-1)/(q-1)$ and specified by the
roots $\beta, \beta^2, \ldots, \beta^{h_0-1}$ has minimum distance exactly $h_0$. Moreover,
the code contains at least $\phi(t,\mu,q)$ vectors of minimum weight $h_0$.
Furthermore, for $\mu \leq \mu' \leq t-1$, there are at least $\phi(u,\mu',q)$ code
vectors of weight $(q^{\mu'+1}-1)/(q-1)$.

The number of information symbols of the $\mu$th order Non-Primitive GRM
code is equal to the degree of the generator polynomial of the dual
code, which in turn is equal to the number of integers $h$, $1 \leq h \leq N-1$, such that $0 < D_q(h(q-1)) \leq \mu(q-1)$, where $N = (q^{t+1}-1)/(q-1)$. Since
$h(q-1) \equiv 0 \pmod{q-1}$, then $D_q(h(q-1)) \equiv 0 \pmod{q-1}$. Recall from Section
2.7 that the number $R_{\mu}(t,q)$ is the number of integers $h$, $1 \leq h \leq N-1$
such that $D_q(h(q-1)) = s(q-1)$, $1 \leq s \leq \mu$. Hence, we have

**Lemma 3.5.4** The number of information symbols in a $\mu$th order Non-
Primitive GRM code of length $(q^{t+1}-1)/(q-1)$ is equal to $R_{\mu}(t,q)$, where
$R_{\mu}(t,q)$ is defined by equation (3.4.4).
Since the $\mu$th order Non-Primitive GRM code is a subcode of the $\mu$th order Projective Geometry code, and for $q = p$, the two codes are the same, we have

**Lemma 3.5.5** The number of information symbols in a $\mu$th order Projective Geometry code of length $(q^{t+1}-1)/(q-1)$ is at least $R_\mu(t,q)$; for $q = p$, this is the exact number of information symbols.

For the case $\mu = t-1$, we give the exact number of information symbols in a $(t-1)$th order Projective Geometry code as follows. For $1 \leq h \leq N-1$, the element $\beta^{-h}$ is not a root of the generator polynomial $g_D(x)$ of the dual code if and only if $\beta^{-h}$ is not a root of the incidence polynomial of some $(t-1)$-flat in $\text{PG}(t,q)$, because, by Definition 3.5.2 and Theorem 3.4.2, $\beta^{h'}$ is a root of $g_D(x)$ if and only if $\beta^{h'}$ is a root of the incidence polynomial of every $(t-1)$-flat in $\text{PG}(t,q)$. Also, $\beta^0 = 1$ is not a root of $g_D(x)$. From Section 2.6, $\beta^{-h}$ is not a root of $g_D(x)$ if and only if either $h=0$ or else $h(q-1) \in S_t$, where $0 \leq h \leq N-1$. The number of integers $h$, $0 \leq h \leq N-1$, such that $\beta^{-h}$ is not a root of $g_D(x)$ is thus $1 + |S_t|$, which is $1 + (p^{t+1}-1)^n$. We state this as a lemma.

**Lemma 3.5.6** The number of information symbols of a $(t-1)$th order Projective Geometry code of length $N=(q^{t+1}-1)/(q-1)$, where $q = p^n$, is equal to

This result has also been obtained independently by Goethals and Delsarte [10].
Let us now consider the generator polynomial \( g(x) \) of the \( \mu \)th order Projective Geometry code, given by

\[
g(x) = x^r h_D(x^{-1})
\]

where \( h_D(x) \) is of degree \( k = N-r \) and

\[
h_D(x) = (x^N - 1)/\beta_D(x).
\]

Since \( g_D(x) \) has as roots those elements \( \beta^h \) such that, for some \( j = 0, 1, ..., n-1 \), \( 0 < D_q(p^j h'(q-1)) \leq \mu(q-1), \ 1 \leq h \leq N-1, \)

then \( g(x) \) has as roots those elements \( \beta^h \) such that, for each \( j = 0, 1, ..., n-1, \) \( D_q(p^j h(q-1)) \geq (\mu+1)(q-1) \), and the element 1.

Now

\[
\beta^{-h} = \beta^{N-h}
\]

and for \( h' = N-h \), \( D_q(p^j h'(q-1)) = (t+1)(q-1) - D_q(p^j h(q-1)). \) So \( g(x) \) has as roots those elements \( \beta^h \) such that

\[
0 \leq D_q(p^j h(q-1)) \leq (t-\mu)(q-1) \text{ for each } j = 0, 1, ..., n-1, \text{ where }
\]

\[
0 \leq h \leq N-1.
\]

Let

\[
h_1 = (q^{y-\mu+1}-1)/(q-1).
\]

Then \( h_1(q-1) = (q-1) + (q-1)q + ... + (q-1)q^{t-\mu} \), which we may write as

\[
h_1(q-1) = [(p-1) + (p-1)q + ... + (p-1)q^{t-\mu}]p
\]

\[
+ ... + [(p-1) + (p-1)q + ... + (p-1)q^{t-\mu}]p^{n-1}.
\]

From this, we note that for each \( j = 0, 1, ..., n-1, \)

\[
D_q(p^j h_1(q-1)) = (t-\mu+1)(q-1) \text{ and that for } 0 \leq h < h_1, \text{ and }
\]

\[
N - 1 - \binom{p+t-1}{t}^n.
\]
for each $j = 0, 1, \ldots, n-1$,$$
 0 \leq D_q(p^j h(q-1)) < D_q(p^j h_1(q-1)),$$
i.e., $0 \leq D_q(p^j h(q-1)) \leq (t-\mu)(q-1)$ for each $j=0,1,\ldots,n-1$.

Thus $g(x)$ contains as roots at least the elements $1, \beta, \beta^2, \ldots, \beta^{h_1-1}$, but not $\beta^{h_1}$. From the BCH theorem, the $\mu$th order Projective Geometry code has minimum distance at least $h_1+1$.

We state this as a lemma.

**Lemma 3.5.7** The minimum distance of the $\mu$th order Projective Geometry code of length $(q^{t+1}-1)/(q-1)$ is at least equal to

$$(q^{\mu+1}-1)/(q-1) + 1.$$
\[(3.6.1) \quad \Phi(t,d,q) = \frac{(q^{t+1} - 1)(q^{t} - 1)\ldots(q^{d+1} - 1)}{(q - d - 1)(q - d)\ldots(q - 1)}.\]

By convention, \(\Phi(t, -1, q) = 1.\)

The number of \(\mu\)-flats in \(PG(t, q)\) is \(\Phi(t, \mu, q)\) and the number of \(\mu\)-flats which pass through, or contain, a given \(m\)-flat is \(\Phi(t-m-1, \mu-m-1, q)\). In particular, the number of \(\mu\)-flats which pass through a given point is \(\Phi(t-1, \mu-1, q)\) and the number of \(\mu\)-flats which pass through a given line or 1-flat is \(\Phi(t-2, \mu-2, q)\).

Every vector of \(C_D\) determines a parity check equation for \(C\).

In particular, the incidence vectors of each \(\mu\)-flat in \(PG(t, q)\) determine a parity check equation for \(C\), viz., if \(h' = (h_0, h_1, \ldots, h_{N-1})\) is the incidence vector of the \(\mu\)-flat \(\Sigma\), then, for every code vector \(c' = (c_0, c_1, \ldots, c_{N-1})\) of \(C\),

\[h_0 c_0 + h_1 c_1 + \ldots + h_{N-1} c_{N-1} = 0.\]

Let us label the points of \(PG(t, q)\) \(P_0, P_1, \ldots, P_{N-1}\) such that \(h_i = \begin{cases} 1, & \text{if } P_i \text{ is incident with } \Sigma \\ 0, & \text{otherwise} \end{cases}\)

where \(i = 0, 1, \ldots, N-1.\)

Corresponding to the transmitted code vector \(c'\), let \(r' = (r_0, \ldots, r_{N-1})\) be the corresponding received vector and let the error vector be \(e' = (e_0, e_1, \ldots, e_{N-1})\), where \(r' = c' + e'\).

Let \(s = h'r\). Then \(s = h'r = h'c + h'e = h'e\) since \(c'\) is a code vector. We may write this as

\[(3.6.2) \quad h_0 e_0 + h_1 e_1 + \ldots + h_{N-1} e_{N-1} = s.\]

We shall refer to equation \((3.6.2)\) as a parity check on \(e_0, e_1, \ldots, e_{N-1}\) corresponding to the flat \(\Sigma\). Each of the
\( J = \phi(t-1, \mu-1, q) \) \( \mu \)-flats in \( \text{PG}(t, q) \) which passes through the point \( P_0 \) determines a parity check equation which checks the symbol \( e_0 \) and the coefficient of \( e_0 \) in each such equation is 1. Suppose these \( J \) equations are

\[ e_0 + h_{j1}e_1 + \cdots + h_{jN-1}e_{N-1} = s_j, \quad j=1,2,\ldots,J. \]

Any two points, say \( P_0 \) and \( P_i, i \geq 1 \), determine a unique line, say \( L \). The symbol \( e_i \) is checked by only those equations in (3.6.3) corresponding to the \( \mu \)-flats in \( \text{PG}(t, q) \) which pass through the line \( L \). Since there are \( 5 = \phi(t-2, \mu-2, q) \) such \( \mu \)-flats, the symbol \( e_i \) is checked by exactly \( 5 \) of the equations (3.6.3). From Theorem 3.3.2, the following decoding rule gives \( e_0 \) correctly, provided at most \( [J/25] \) errors have occurred. Decode \( e_0 \) as that value of \( \text{GF}(q) \) which is assumed by the greatest fraction of the \( \{s_j\} \) of equations (3.6.3); in the event that no single value is assumed by a strict plurality of the \( \{s_j\} \), decode \( e_0 \) as zero.

The symbols \( e_1, e_2, \ldots, e_{N-1} \) may be decoded successively by choosing a different set of \( J \) equations which check \( e_1 \), etc. Having determined the error vector, \( \mathbf{e}' \), the transmitted vector, \( \mathbf{c}' \), may be recovered from the received vector, \( \mathbf{r}' \).

Now \( J/5 \) is equal to \( (q^{t-1})/(q^{\mu-1}) \), which, for large \( q \), is approximately equal to \( q^{t-\mu} \). We state the above as a theorem.

**Theorem 3.6.1.** Provided at most \( [(q^{t-1})/2(q^{\mu-1})] \) errors occur, a \( \mu \)th order non-primitive geometric code of length \( (q^{t+1}-1)/(q-1) \) may be correctly decoded using the one-step majority decoding algorithm as described above.
Alternatively, it is possible to use a \( \mu \)-step majority decoding procedure for a \( \mu \)th order non-primitive geometric code.

Two distinct \( \mu \)-flats in \( PG(t,q) \) intersect in at most a \( (\mu-1) \)-flat. There are \( J_1 = \binom{t-\mu+1}{0} \mu \)-flats which pass through a given \( (\mu-1) \)-flat, \( \Sigma \). Let the check sum of \( \Sigma \) be \( S \), i.e., if the points on \( \Sigma \) are \( P_0, \ldots, P_k \), then \( S = e_0 + e_1 + \ldots + e_k \). Take the parity check equations which correspond to the \( J_1 \) \( \mu \)-flats which intersect in \( \Sigma \). Each of these equations checks the sum \( S \), but no other symbol is checked by more than one of these equations. Let the equations be

\[
(3.6.4) \quad S + h_{j,k+1}e_{k+1} + \ldots + h_{j,N-1}e_{N-1} = s_j, \quad j=1, \ldots, J_1
\]

This set of \( J_1 \) equations is orthogonal on the sum \( S \). By Theorem 3.3.1, the following decoding rule gives \( S \) correctly, provided that at most \( \lfloor J_1/2 \rfloor \) errors have occurred. Decode \( S \) as that value of \( GF(q) \) which is assumed by the greatest fraction of the \( \{s_j\} \) in equations (3.6.4); in the event that no such value is assumed by a strict plurality of the \( \{s_j\} \), decode \( S \) as 0.

Likewise, the check sum of every \( (\mu-1) \)-flat in \( PG(t,q) \) may be decoded using a majority rule. These decoded sums may be treated as new parity check equations, and the check sums of the \( (\mu-2) \)-flats may be determined from these new equations by a majority procedure. Since two distinct \( (\mu-1) \)-flats intersect in at most a \( (\mu-2) \)-flat and there are \( J_2 = \binom{t-\mu}{0} \) \((\mu-1)\)-flats which intersect in a given \( (\mu-2) \)-flat, the check sum of each \( (\mu-2) \)-flat is given correctly by the majority procedure, provided at most \( \lfloor J_1/2 \rfloor \) and hence at most \( \lfloor J_2/2 \rfloor \) errors have occurred.
This is repeated until, at the \( \mu \)th stage, the check sums of each 0-flat, i.e., each of the symbols \( e_0, e_1, \ldots, e_{N-1} \), have been decoded. Provided at most \([J_1/2]\) errors have occurred, the check sum at each stage is decoded correctly. We state this in the following theorem.

**Theorem 3.6.2** Provided at most \([J_1/2]\) errors have occurred, a \( \mu \)th order non-primitive geometric code of length \((q^{t+1}-1)/(q-1)\) may be correctly decoded using the above \( \mu \)-step majority decoding procedure, where

\[
J_1 = \frac{q^{t-\mu+1}-1}{q-1}.
\]

We observe that for large \( q \), \( J_1 \) is approximately equal to \( q^{t-\mu} \), so that the \( \mu \)-step majority decoding procedure and the one-step majority decoding algorithm of Theorem 3.6.1 will correct approximately the same number of errors. Also, the one-step decoding procedure is easier and more economical to implement than the \( \mu \)-step procedure.

Since the minimum distance of the \( \mu \)th order Projective Geometry code is, from Lemma 3.5.7, equal to \( J_1 + 1 \), the number of errors correctable by the \( \mu \)-step majority decoding procedure is equal to that guaranteed correctable by the minimum distance property of the code. In Table 3.3, the number of errors correctable by one-step majority decoding is given for these codes. Except for small values of \( q \), there appears to be no appreciable advantage in using the \( \mu \)-step procedure for the Projective Geometry codes.

Similar majority decoding procedures may be used for primitive geometric codes.

Let \( C \) be a type 0 primitive geometric code of order \( \mu \) and length \( q^{t-1} \), i.e., the dual code contains the incidence vectors of all
\( \mu \)-flats in \( \text{EG}(t,q) \). As in the projective case, suppose the \( N = q^t - 1 \) points, other than the origin, in \( \text{EG}(t,q) \) are labelled \( P_0, P_1, \ldots, P_{N-1} \) such that if \( h' = (h_0, h_1, \ldots, h_{N-1}) \) is the incidence vector of the \( \mu \)-flat \( \Sigma \), then, for \( i = 0, 1, \ldots, N-1 \),

\[
h_i = \begin{cases} 
1, & \text{if } P_i \text{ is incident with } \Sigma \\
0, & \text{otherwise.}
\end{cases}
\]

The number of \( \mu \)-flats in \( \text{EG}(t,q) \) which pass through a given \( m \)-flat is \( \Phi(t-m-1, \mu-m-1, q) \). In particular, there are \( \Phi(t-1, \mu-1, q) \) \( \mu \)-flats which pass through a given point and \( \Phi(t-2, \mu-2, q) \) \( \mu \)-flats which pass through a given line or \( l \)-flat.

Each of the \( J = \Phi(t-1, \mu-1, q) \) \( \mu \)-flats in \( \text{EG}(t,q) \) which pass through a given point, say \( P_0 \), determines a parity check equation which checks the symbol \( e_0 \). Suppose these \( J \) equations are

\[
e_0 + h_{j1}e_1 + \ldots + h_{j,N-1}e_{N-1} = s_j, \quad j = 1, 2, \ldots, J.
\]

For \( i = 1, 2, \ldots, N-1 \), the points \( P_0 \) and \( P_i \) determine a unique line. Since there are \( S = \Phi(t-2, \mu-2, q) \) \( \mu \)-flats in \( \text{EG}(t,q) \) which pass through this line, the symbol \( e_i \) is checked by exactly \( S \) of these \( J \) equations. Hence, by Theorem 3.3.2, provided that at most \( \lfloor J/2 \rfloor \) errors have occurred, \( e_0 \) is given correctly as that value of \( GF(q) \) which is assumed by the greatest fraction of the \( \{ s_j \} \) in equations (3.6.5); in the case no value is assumed by a strict plurality of the \( \{ s_j \} \), \( e_0 \) is given correctly as 0.

The remaining symbols \( e_1, \ldots, e_{N-1} \) are similarly decoded.

Analogous to the \( \mu \)-step decoding procedure for the projective case, a \( \mu \)-step majority decoding procedure is available for the primitive geometric codes of type 0 and order \( \mu \).

For a type 1 primitive geometric code of order \( \mu \), the majority
decoding procedures are the same as the above, except that the only flats used are those which do not pass through the origin.

There are \( q^{t-\mu} \) \( (t-1, \mu-1, q) \) \( \mu \)-flats in \( EG(t, q) \), of which \( (t-1, \mu-1, q) \) pass through the origin and \( (q^{t-\mu-1}) \) \( (t-1, \mu-1, q) \) do not. Let \( P \) be any point of \( EG(t, q) \), other than the origin. The number of \( \mu \)-flats through \( P \) is \( \mu(t-1, \mu-1, q) \). Since \( P \) and the origin determine a unique line, say \( L \), and the number of \( \mu \)-flats passing through \( L \) is \( \mu(t-2, \mu-2, q) \), there are

\[
J_3 = \mu(t-1, \mu-1, q) - \mu(t-2, \mu-2, q)
\]

\( \mu \)-flats in \( EG(t, q) \) which pass through \( P \) but not the origin.

Suppose the parity check equations of all \( \mu \)-flats passing through the point \( P_0 \) but not the origin are

\[
(3.6.6) \quad e_0 + h_{j1} e_1 + \ldots + h_{jN-1} e_{N-1} = s_j, \quad j=1, 2, \ldots, J_3.
\]

For any \( i = 1, \ldots, N-1 \), either the origin, \( P_0 \) and \( P_i \) are collinear or they are not. If they are, then none of these \( J_3 \) equations check both the symbols \( e_0 \) and \( e_i \), for otherwise, the corresponding \( \mu \)-flat would pass through the unique line containing \( P_0 \) and \( P_i \), which also contains the origin, in this case; i.e., the \( \mu \)-flat would pass through the origin. If \( P_0 \), \( P_i \) and the origin are not collinear, then the three points determine a unique plane, \( \pi \). There are \( \mu(t-3, \mu-3, q) \) \( \mu \)-flats in \( EG(t, q) \) passing through \( \pi \). There are \( \mu(t-2, \mu-2, q) \) \( \mu \)-flats in \( EG(t, q) \) passing through the line determined by \( P_0 \) and \( P_i \), so there are

\[
\delta_3 = \mu(t-2, \mu-2, q) - \mu(t-3, \mu-3, q)
\]

\( \mu \)-flats passing through \( P_0 \) and \( P_i \) but not the origin. Consequently, at most \( \delta_3 \) of the \( J_3 \) equations (3.6.6) check both \( e_0 \) and \( e_i \), for any \( i = 1, \ldots, N-1 \).
The one-step majority decoding rule of Theorem 3.3.2 gives \( e_0 \) correctly, provided at most \( \left\lfloor J_3/2E_2 \right\rfloor \) errors have occurred. The remaining symbols \( e_1, e_2, \ldots, e_{N-1} \) may be decoded similarly.

The \( \mu \)-step majority decoding procedure for a type 1 primitive geometric code of order \( \mu \) is also similar to that for the non-primitive geometric codes.

Two \( \mu \)-flats which do not pass through the origin either do not intersect or else intersect in at most a \((\mu-1)\)-flat. Let \( \Sigma \) be such a \((\mu-1)\)-flat which does not pass through the origin. Then the origin and \( \Sigma \) determine a unique \( \mu \)-flat passing through the origin. There are \( \Phi(t-\mu,0,q) \) \( \mu \)-flats passing through \( \Sigma \), so there are

\[
J_4 = \Phi(t-\mu,0,q) - 1
\]

\( \mu \)-flats in \( \text{EG}(t,q) \) which pass through \( \Sigma \) but not the origin. Provided at most \( \left\lfloor J_4/2 \right\rfloor \) errors have occurred, the check sum of \( \Sigma \) is given correctly by a majority rule from the corresponding \( J_4 \) parity check equations. Having decoded the check sums of each \((\mu-1)\)-flat which does not pass through the origin, the procedure is repeated to give the check sums of each \((\mu-2)\)-flat which does not pass through the origin, etc. At the \( \mu \)th stage, the symbols \( e_0, e_1, \ldots, e_{N-1} \) are decoded correctly, provided at most \( \left\lfloor J_4/2 \right\rfloor \) errors have occurred.

Since a \( \mu \)th order Affine Geometry code is a primitive geometric code of type 1, we may apply the \( \mu \)-step majority decoding procedure described above. Since \( \left\lfloor J_4/2 \right\rfloor \) errors may be corrected, the minimum distance of the code is at least

\[
J_4 + 1 = \Phi(t-\mu,0,q) = \frac{q^{t-\mu+1}-1}{q-1} - 1.
\]
### TABLE 3.1

**SUMMARY OF GEOMETRIC CODES**

<table>
<thead>
<tr>
<th>Code</th>
<th>Length</th>
<th>Roots of $g_D(x)$ are</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRIMITIVE GEOMETRIC CODES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$v$th order Reed-Muller</td>
<td>$2^t - 1$</td>
<td>$\alpha^h$ such that $D_2(h) \leq v$</td>
</tr>
<tr>
<td>$v$th order GRM</td>
<td>$q^t - 1$</td>
<td>$D_q(h) \leq v$</td>
</tr>
<tr>
<td>$v$th order EG</td>
<td>$2^{nt} - 1$</td>
<td>$? \leq D_2(h)\leq v$</td>
</tr>
<tr>
<td>$\mu$th order Affine Geometry</td>
<td>$q^t - 1$</td>
<td>$D_q(p^j h) &lt; \mu(q-1)$ for some $j=0,..,n-1$</td>
</tr>
<tr>
<td><strong>NON-PRIMITIVE GEOMETRIC CODES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$v$th order Modified Reed-Muller</td>
<td>$(2^{t+1} - 1)/(2-1)$</td>
<td>$0 &lt; D_2(h) \leq v$</td>
</tr>
<tr>
<td>$\mu$th order Non-Primitive GRM</td>
<td>$(q^{t+1} - 1)/(q-1)$</td>
<td>$0 &lt; D_q(h(q-1)) \leq \mu(q-1)$</td>
</tr>
<tr>
<td>$\mu$th order Projective Geometry</td>
<td>$(q^{t+1} - 1)/(q-1)$</td>
<td>$0 &lt; D_q(p^j h(q-1)) \leq \mu(q-1)$</td>
</tr>
<tr>
<td>Difference-Set</td>
<td>$(q^3 - 1)/(q-1)$</td>
<td>$D_q(p^j h(q-1)) = (q-1)$.</td>
</tr>
<tr>
<td>$q$</td>
<td>$t$</td>
<td>$\mu$</td>
</tr>
<tr>
<td>----</td>
<td>----</td>
<td>------</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>63</td>
</tr>
<tr>
<td>2</td>
<td>63</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1023</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1023</td>
</tr>
<tr>
<td>3</td>
<td>1023</td>
<td>222</td>
</tr>
<tr>
<td>4</td>
<td>1023</td>
<td>968</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>511</td>
</tr>
<tr>
<td>2</td>
<td>511</td>
<td>392</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td>2</td>
<td>26</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>80</td>
</tr>
<tr>
<td>2</td>
<td>80</td>
<td>31</td>
</tr>
<tr>
<td>3</td>
<td>80</td>
<td>66</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>242</td>
</tr>
<tr>
<td>2</td>
<td>242</td>
<td>51</td>
</tr>
<tr>
<td>3</td>
<td>242</td>
<td>147</td>
</tr>
<tr>
<td>4</td>
<td>242</td>
<td>222</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>124</td>
</tr>
<tr>
<td>2</td>
<td>124</td>
<td>10</td>
</tr>
</tbody>
</table>
### TABLE 3.3
PARAMETERS OF PROJECTIVE GEOMETRY CODES

| q | t | μ | Length $q^{t+1}/(q-1)$ Info. Symbols $R_\mu(t,q)$ Minimum Distance $q^{t-\mu}/(q-1)$ Errors Corrected by 1-step Decoding $\frac{1}{3} (q^t-1)/(q^\mu-1)$ |
|---|---|---|---|---|---|---|
| 2* | 1 | 7 | 3 | 4 | 1 |
| 3 | 1 | 15 | 4 | 8 | 3 |
| | 2 | 15 | 10 | 4 | 1 |
| 4 | 1 | 31 | 5 | 16 | 7 |
| | 2 | 31 | 15 | 8 | 2 |
| | 3 | 31 | 25 | 4 | 1 |
| 5 | 1 | 63 | 6 | 32 | 15 |
| | 2 | 63 | 21 | 16 | 5 |
| | 3 | 63 | 41 | 8 | 2 |
| | 4 | 63 | 56 | 4 | 1 |
| 6 | 1 | 127 | 7 | 64 | 31 |
| | 2 | 127 | 28 | 32 | 10 |
| | 3 | 127 | 63 | 16 | 4 |
| | 4 | 127 | 98 | 8 | 2 |
| | 5 | 127 | 119 | 4 | 1 |
| 7 | 1 | 255 | 8 | 128 | 63 |
| | 2 | 255 | 36 | 64 | 21 |
| | 3 | 255 | 92 | 32 | 9 |
| | 4 | 255 | 162 | 16 | 4 |
| | 5 | 255 | 218 | 8 | 2 |
| | 6 | 255 | 246 | 4 | 1 |
| 8 | 1 | 511 | 9 | 256 | 127 |
| | 2 | 511 | 45 | 128 | 42 |
| | 3 | 511 | 129 | 64 | 18 |
| | 4 | 511 | 255 | 32 | 8 |
| | 5 | 511 | 381 | 16 | 4 |
| | 6 | 511 | 465 | 8 | 2 |
| | 7 | 511 | 501 | 4 | 1 |

* For q=2, the projective geometry codes are the cyclic Reed-Muller codes.
<table>
<thead>
<tr>
<th>q</th>
<th>t</th>
<th>μ</th>
<th>Length</th>
<th>Info. Symbols</th>
<th>Distance</th>
<th>1-step errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>21</td>
<td>10</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>85</td>
<td>20</td>
<td>22</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>85</td>
<td>64</td>
<td>6</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>341</td>
<td>35</td>
<td>86</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>341</td>
<td>170</td>
<td>22</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>341</td>
<td>305</td>
<td>6</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1365</td>
<td>56</td>
<td>342</td>
<td>170</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1365</td>
<td>392</td>
<td>86</td>
<td>34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1725</td>
<td>972</td>
<td>22</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1365</td>
<td>1308</td>
<td>6</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>1</td>
<td>73</td>
<td>36</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>585</td>
<td>120</td>
<td>74</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>585</td>
<td>464</td>
<td>10</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4681</td>
<td>330</td>
<td>586</td>
<td>292</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4681</td>
<td>2340</td>
<td>74</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4681</td>
<td>4350</td>
<td>10</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>1</td>
<td>273</td>
<td>136</td>
<td>18</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>4369</td>
<td>816</td>
<td>274</td>
<td>136</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4369</td>
<td>3552</td>
<td>18</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>1</td>
<td>1057</td>
<td>528</td>
<td>34</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>13</td>
<td>6</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>40</td>
<td>10</td>
<td>14</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>40</td>
<td>29</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>121</td>
<td>15</td>
<td>41</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>121</td>
<td>60</td>
<td>14</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>121</td>
<td>105</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>364</td>
<td>21</td>
<td>122</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>364</td>
<td>111</td>
<td>41</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>364</td>
<td>252</td>
<td>14</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>364</td>
<td>342</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>1</td>
<td>91</td>
<td>45</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>q</td>
<td>t</td>
<td>μ</td>
<td>Length</td>
<td>Info. Symbols</td>
<td>Distance</td>
<td>l-step errors</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>--------</td>
<td>--------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>1</td>
<td>820</td>
<td>165</td>
<td>92</td>
<td>45</td>
</tr>
<tr>
<td>2</td>
<td>820</td>
<td>654</td>
<td>11</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>2</td>
<td>1</td>
<td>757</td>
<td>378</td>
<td>29</td>
<td>14</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>1</td>
<td>31</td>
<td>15</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>156</td>
<td>35</td>
<td>32</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>156</td>
<td>120</td>
<td>7</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BIBLIOGRAPHY


107


