COUNTING ZEROS OF POLYNOMIALS OVER FINITE FIELDS

Thesis by

Daniel Edwin Erickson

In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California
1974
(Submitted September 20, 1973)

ACKNOWLEDGMENTS

I would like to take this opportunity to thank Robert J. McEliece who suggested the topic for this study, directed me to source material in this field and has been a continual source of guidance and review. My thanks also to Professor Robert P. Dilworth who has guided my graduate study and helped review this thesis, and to Professor Marshall Hall who suggested the material on blocking sets. I must thank my wife Vicky who has endured many inconveniences while I was engaged in writing this thesis. I am also grateful to Joyce Lundstedt who typed this work for me.

For financial assistance, I am indebted to the State of California for a partial fellowship, the California Institute of Technology for tuition fellowships and teaching assistantships, and to the Jet Propulsion Laboratory for part-time and summer employment.

ABSTRACT

The main results of this dissertation are described in the following theorem:

Theorem 5.1

If P is a polynomial of degree $r = s(q-1)+t$, with $0 < t \leq q-1$, in m variables over GF(q), and N(P) is the number of zeros of P, then:

1) $N(P) > q^m - q^{m-s} + tq^{m-s-1}$ implies that P is zero.
2) $N(P) < q^m - q^{m-s} + tq^{m-s-1}$ implies that $N(P) \leq q^m - q^{m-s} + tq^{m-s-1} - cq^{m-s-2}$ where

$$c = \begin{cases} q & \text{if } s = m-1 \text{ or if } t = 1 \text{ and either } s = 0 \text{ or } q \geq 4 \\ & \quad \text{or if } s = m-2 \text{ and } q = 2. \\ q-1 & \text{if } t = 1 \text{ and either } q = 3 \text{ and } 0 < s = m-2 \text{ or} \\ & \quad q < 4 \text{ and } 0 < s < m-2. \\ t-1 & \text{if } s < m-1 \text{ and either } 1 < t < (q+5)/2 \text{ or } 1 < t = q-1 \\ c_t & \text{if } q \geq 4,\ (q+5)/2 \leq t < q-1, \text{ and } s < m-1. \end{cases}$$

where $(q-t+3) \leq c_t \leq t-1$. Furthermore, there exists a polynomial Q in m variables over GF(q) of degree r such that $N(Q) = q^m - q^{m-s} + tq^{m-s-1} - cq^{m-s-2}$.

In the parlance of Coding Theory 5.1 states:

Theorem 5.1*

The next-to-minimum weight of the r^{th} order Generalized Reed-Muller Code of length q^m is $(q-t)q^{m-s-1} + cq^{m-s-2}$, where c, s, and t are defined above.

Chapter 4 deals with blocking sets of order n in finite planes. An attempt is made to find the minimum size for such sets.

TABLE OF CONTENTS

Page

ACKNOWLEDGMENTS ii

ABSTRACT iii

CHAPTER 1 1

CHAPTER 2 14

CHAPTER 3 39

CHAPTER 4 62

CHAPTER 5 80

REFERENCES 87

CHAPTER 1

This dissertation examines polynomials in several variables over finite fields. The general problem of exhibiting canonical forms for such polynomials being extremely difficult, this work concentrates on their sets of zeros. The specific goal of the first three chapters is to explore the restrictions on the number of zeros of polynomials of degree r in m variables over $GF(q)$, the field with q elements. Chapter one outlines the historical development in this area, the basic definitions, and the motivation for this particular specialization of the general problem. Chapters two and three contain the results of the author's research on zero-sets of polynomials. The fourth chapter deals with a related topic: blocking sets in affine planes. A discussion of the expected fruitfulness and difficulties of certain approaches to study in these areas occupies the fifth and final chapter.

The following notation will be used in discussing polynomials over finite fields:

Let $K = GF(q)$ be the field with q elements.

Let K^m be the vector space of dimension m over K consisting of all m-tuples $\bar{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$, $\alpha_i \in K$.

Let $P = P(x_1, x_2, \ldots, x_m)$ be a polynomial in m variables over K.

The <u>degree</u> or <u>total degree</u> of a term of P is the sum of the powers of all of the indeterminates in that term.

The <u>degree</u> or <u>total degree of P</u> is the degree of the maximum degree nonzero term of P. The degree of the zero polynomial is $-\infty$.

deg P will denote the degree of P.

The <u>x_i-degree of a term</u> of P is the power of the indeterminate x_i in the term.

The <u>x_i-degree of P</u> is the x_i-degree of the maximum x_i-degree nonzero term of P. The x_i-degree of the zero polynomial is $-\infty$.

$\deg_i$ P will denote the x_i-degree of P.

The <u>zero set</u> of P or set of zeros of P, Z(P), is the set of m-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ such that $P(\alpha_1, \alpha_2, \ldots, \alpha_m) = 0$.

$Z(P) = \{\overline{\alpha} \in K^m \,|\, P(\overline{\alpha}) = 0\}$.

The <u>nullity</u> of P, N(P), is the number of zeros of P.

$N(P) = ||Z(P)||$.

The first results establishing restrictions on N(P) were published by C. Chevalley [4] and E. Warning [13] in 1936. E. Artin had conjectured that if P is homogeneous of degree r with $r < m$, then P has a zero besides $\overline{0} = (0,0,\ldots,0)$. Chevalley showed that not only was Artin's conjecture true, but that it was still true if P was not homogeneous but had a zero constant term. Warning, using a lemma of Chevalley's, proved the theorem:

<u>Theorem 1.1</u>: Chevalley-Warning

If deg $P < m$ then the characteristic of K divides N(P).

Warning also showed that if $N(P) > 0$ and deg $P < m$, then $N(P) \geq q^{m-\deg P}$.

It was not until 1964 that these results were improved upon by James Ax [1]. He proved the following theorem:

Theorem 1.2: Ax Divisibility Condition

Let P be a polynomial in m variables over GF(q) with deg P = r. Let b = [(m-1)/r], the greatest integer less than or equal to (m-1)/r. Then q^b divides N(P).

He also exhibited a polynomial P of degree r in m variables over GF(q) such that q^b divides N(P), but pq^b does not divide N(P) where p is the characteristic of K = GF(q). In this sense, Theorem 1.2 is the best possible p-adic divisibility theorem.

More recently, results in this area have arisen from the study of Generalized Reed-Muller Codes in algebraic coding theory. It is not necessary, however to be familiar with coding theory to understand these results. The following discussion should suffice to illuminate these results.

Each polynomial $P(\overline{x}) = P(x_1, x_2, \ldots, x_m)$ in m variables over K generates a function $\overline{\alpha} \to P(\overline{\alpha})$ from K^m into K. But some different polynomials generate the same functions. For instance, $x_1^q - x_1$ maps every element of K^m into zero. Since every element of K satisfies $\alpha^q = \alpha$, any polynomial can be reduced modulo $(x_1^q - x_1), (x_2^q - x_2), \ldots,$ and $(x_m^q - x_m)$ to a new polynomial $P'(\overline{x})$ such that P and P′ agree on every point of K^m and $\deg_i P' \leq q-1$ for $i = 1, \ldots, m$. This observation leads to the definition:

A polynomial $P(x_1, \ldots, x_m)$ in m variables over K = GF(q) is called a reduced polynomial if $\deg_i P \leq q-1$ for $i = 1, 2, \ldots, m$.

There are q^{q^m} reduced polynomials in m variables over GF(q). There are the same number of mappings from K^m into K. That these are in one-to-one correspondence may be shown either by proving that no two reduced polynomials act identically on K^m, or by proving that for each function $f : K^m \rightarrow K$ there is a reduced polynomial $P(x_1, x_2, \ldots, x_m)$ such that $P(\sigma_1, \sigma_2, \ldots, \sigma_m) = f((\sigma_1, \sigma_2, \ldots, \sigma_m))$ for each $\overline{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_m) \in K^m$. The latter method provides some additional insights.

For each $\overline{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_m) \in K^m$ define

$$F_{\overline{\sigma}}(\overline{x}) = \prod_{i=1}^{m} (1 - (x_i - \sigma_i)^{q-1})$$

$F_{\overline{\sigma}}$ is a reduced polynomial. Considered as a function,

$$F_{\overline{\sigma}}(\overline{\tau}) = \begin{cases} 1 & \text{if } \overline{\tau} = \overline{\sigma} \\ 0 & \text{otherwise} \end{cases}$$

This can be seen from the fact that when $\lambda \in K$

$$\lambda^{q-1} = \begin{cases} 0 & \text{if } \lambda = 0 \\ 1 & \text{if } \lambda \neq 0 \end{cases}$$

Using the $F_{\overline{\sigma}}$ as a basis, a reduced polynomial which represents any given function $f : K^m \rightarrow K$ can be generated as follows:

Let $P(\overline{x}) = \sum_{\overline{\sigma} \in K^m} f(\overline{\sigma}) F_{\overline{\sigma}}(\overline{x})$. Then P represents f.

From this discussion the following theorem is obvious:

Theorem 1.3

The natural mapping $P \to (\bar{\sigma} \to P(\bar{\sigma}))$ is a vector space isomorphism from the space of reduced polynomials in m variables over GF(q) to the space of mappings from K^m into K.

For the remainder of this work, all polynomials referred to will be reduced polynomials unless a statement is made to the contrary. $\mathcal{P}(m,q)$ will denote the set of reduced polynomials in m variables over GF(q). The subset of $\mathcal{P}(m,q)$ consisting of those polynomials with degree less than or equal to r will be denoted $\mathcal{P}_r(m,q)$. Since $\deg(P+Q) \leq \max(\deg P, \deg Q)$ and $\deg(\alpha P) \leq \deg P$ for $\alpha \in K$, $\mathcal{P}_r(m,q)$ is a subspace of $\mathcal{P}(m,q)$.

If the elements of K^m are ordered $\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_{q^m}$, the value table of a polynomial $P \in \mathcal{P}(m,q)$ (with respect to this ordering) is the q^m-tuple $(P(\bar{\alpha}_1), P(\bar{\alpha}_2), \ldots, P(\bar{\alpha}_{q^m}))$.

The set of value tables for all polynomials of $\mathcal{P}(m,q)$ forms a vector space of dimension q^m over GF(q) which is isomorphic to $\mathcal{P}(m,q)$.

Definition

The set of value tables of polynomials in $\mathcal{P}_r(m,q)$ is called the r-th order Generalized Reed-Muller Code of length q^m, denoted $GRM_r(m,q)$.

Clearly $GRM_r(m,q)$ is a subspace of $GRM_{m(q-1)}(m,q)$ which is the space of all value tables. The dimension of $GRM_r(m,q)$ as a vector space over GF(q) can be computed by calculating the dimension of the isomorphic space $\mathcal{P}_r(m,q)$. As a basis for $\mathcal{P}_r(m,q)$ we can pick those polynomials of the form:

$$x_1^{i_1}x_2^{i_2}\ldots x_m^{i_m} \quad \text{where} \quad 0 \leqslant i_j \leqslant q\text{-}1 \quad \text{and} \quad \sum_{j=1}^{m} i_j \leqslant r \ .$$

If p(k, m, q) represents the number of distinct m-tuples $(a_1, a_2, \ldots, a_m)$ such that $0 < a_1 \leqslant q$ and $\sum_{j=1}^{m} a_j = k$, then

$$\dim \ \mathcal{P}_r(m,q) = \sum_{i=0}^{r} p(i+m, m, q) \ .$$

The GRM codes are examples of linear block codes. A <u>linear block code</u> is a subspace of the space of n-tuples of elements of a finite field. The <u>length of the code</u> is n and the <u>dimension of the code</u> is the dimension of the subspace. A linear block code of dimension k and length n is called an <u>(n, k) linear code</u>. Under this definition:

$$\mathrm{GRM}_r(m,q) \quad \text{is a} \quad (q^m, \ \sum_{i=0}^{r} p(i+m, m, q)) \quad \text{linear code} \quad .$$

The elements of a linear code are called <u>code vectors.</u> The <u>Hamming distance</u> between any two vectors $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $(\beta_1, \beta_2, \ldots, \beta_n)$ is defined as the number of positions in which they differ:

$$\langle\!\langle(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)\rangle\!\rangle = \|\{i \in \{1, \ldots, n\} \,|\alpha_i \neq \beta_i\}\| \ .$$

The <u>Hamming weight</u> of a vector $(\alpha_1, \ldots, \alpha_n)$ is defined as the number of positions in which it is nonzero:

$$|(\alpha_1, \ldots, \alpha_n)| = \|\{i \in \{1, \ldots, n\} \,|\, \alpha_i \neq 0\}\| \ .$$

The minimum distance of a linear block code C is the smallest distance between two distinct code vectors:

$$\text{minimum distance} = \min_{\substack{x, y \in C \\ x \neq y}} \langle x, y \rangle \ .$$

The minimum weight of a code C is the smallest nonzero weight of a code vector:

$$\text{minimum weight} = \min_{\substack{x \in C \\ x \neq 0}} |x| \ .$$

For a linear block code, the minimum weight and the minimum distance are equal. The natural isomorphism from $\mathcal{P}(m,q)$ onto K^{q^m} maps $\mathcal{P}_r(m,q)$ onto $GRM_r(m,q)$ and preserves weight if we define the weight of a polynomial P:

$$|P| = \|S(P)\| \quad \text{where } S(P) \text{ is the set of support points of } P:$$
$$S(P) = \{\bar{\alpha} \in K^m \,|\, P(\bar{\alpha}) \neq 0\} \ .$$

Thus, the notion of a minimum weight (nonzero) polynomial of $\mathcal{P}_r(m,q)$ is interchangable with that of a minimum weight code vector of $GRM_r(m,q)$. The weight of a polynomial is the dual of its nullity since $S(P) = K^m - Z(P)$ and $|P| = q^m - N(P)$. Many results of coding theory deal with constraints on the weights of code vectors of linear block codes. Some deal specifically with GRM codes. Through this duality, these results are directly applicable to the topic of this paper, restrictions on N(P).

The two concepts of coding theory which encompass such considerations of restrictions on weights are weight enumerators and weight spectra of linear codes. If A_i is the number of code vectors in a given (n,k) linear code which have weight i, then the generating function:

$$A(z) = \sum_{i=0}^{n} A_i z^i$$

is called the <u>weight enumerator</u> of the code. The <u>weight spectrum</u> of the code is just the set of i for which $A_i > 0$, (i.e., the set of weights which actually occur). The <u>gaps</u> in the spectrum are those i for which $A_i = 0$. The weight enumerator contains the complete information on the distribution of the weights of the code vectors in a form which is convenient for probability calculations. The weight spectrum records all of the restrictions on the weights of the code vectors (and hence on the number of zeros of polynomials in GRM codes).

The minimum weight of the r-th order Generalized Reed-Muller Code of length q^m ($GRM_r(m,q)$) was shown in 1968 by Kasami, Lin, and Peterson [6] to be $(q-t)q^{m-s-1}$ where $r = s(q-1) + t$ with $0 < t \leqslant q-1$. They also gave canonical forms for polynomials of this weight when $q = 2$. In 1970, Delsarte, Goethals, and MacWilliams [5] extended these results, giving canonical forms for minimum weight polynomials in the general q-ary case. (Proofs of the canonical forms and the minimum weight will be given in chapter two.) Once the canonical forms were found, A_i was calculated for i = minimum weight. The canonical forms are representatives of the equivalence classes under the equivalence described in the next paragraph.

A substitution of variables is made in a polynomial P by replacing each x_i by a linear polynomial, $a_{1i}x_1 + a_{2i}x_2 + \ldots + a_{mi}x_m + \omega_i$. This substitution defines a new polynomial $R(\bar{x}) = P(\bar{x}A + \bar{\omega})$ such that for any $\bar{\alpha} \in K^m$, $R(\bar{\alpha}) = P(\bar{\alpha}A + \bar{\omega})$. If A is non-singular, then $P(\bar{x}) = R(\bar{x}A^{-1} + (-\bar{\omega}A^{-1}))$. In this case, deg R = deg P and N(R) = N(P). Such a change of variables $T(\bar{x}) = \bar{x}A + \bar{\omega}$ is called an <u>invertible affine transformation of variables</u>. It is composed of an invertible homogeneous transformation $\bar{x} \rightarrow \bar{x}A$ and a translation $\bar{x} \rightarrow \bar{x} + \bar{\omega}$. The notation $[T(\bar{x})]_i$ will denote $a_{1i}x_1 + \ldots + a_{mi}x_m + \omega_i$. The homogeneous transformations all fix the origin and so are distinct from the nonzero translations. There are $(q^m-1)(q^m-q)\ldots(q^m-q^{m-1})$ invertible homogeneous transformations and q^m translations giving $q^m(q^m-1)(q^m-q)\ldots(q^m-q^{m-1})$ invertible affine transformation of variables. If $R(\bar{x}) = P(\bar{x}A + \bar{\omega})$ for some invertible A, then P and R are called equivalent. This is clearly an equivalence relation. Restating what was said above:

<u>Theorem 1.4</u>

If P and R are equivalent polynomials, then deg P = deg R, N(P) = N(R), and $|P| = |R|$.

In the special case, r = 2, Robert McEliece [9] has given canonical forms for the polynomials of $\mathcal{P}_2(m,q)$ and calculated the A_i for the second-order Generalized Reed-Muller Codes. The full result is quite complex and is presented in a series of tables, but the restrictions on the weight spectrum are simple enough to be given here:

Theorem 1.5: McEliece

If P is a polynomial of degree ≤ 2 over GF(q) in m variables, then the number of solutions to $P(\bar{x}) = a$ is of the form $q^{m-1} + \nu q^{m-j-1}$ where $\nu = 0, \pm 1$ or $\pm (q-1)$ and $0 < j \leq [m/2]$.

Another specialized case where significant results have been obtained is $q = 2$. The code $GRM_r(m, 2)$ is called the r-th order Reed-Muller Code of length 2^m denoted $RM(r, 2^m)$. In 1970, Tadao Kasami and Nobuki Tokura [7] characterized the polynomials of less than twice the minimum weight in $P_r(m, 2)$. This left coding theorists one equation short of a solution to a system of equations which would yield the weight enumerator for the code $RM(3, 2^8)$. In April of 1971 three mathematicians independently found this weight enumerator; namely, T. Kasami, R. Sarivate, and J. H. van Tilborg. To fully understand the nature of this problem and the motivation for this paper, one must understand dual codes and the MacWilliams identity.

Define a scalar product $\bar{c} \cdot \bar{d}$ of two n-tuples of elements of K. $\bar{c} = (c_1, c_2, \ldots, c_n)$; $\bar{d} = (d_1, d_2, \ldots, d_n)$

$$\bar{c} \cdot \bar{d} = \sum_{i=1}^{n} c_i d_i \quad .$$

Given an (n, k) code $\mathcal{A}$ (a subspace of dimension k), the dual of $\mathcal{A}$ is the set of vectors $\mathcal{B} = \{\bar{b} \mid \forall \bar{a} \in \mathcal{A}, \ \bar{a} \cdot \bar{b} = 0\}$. $\mathcal{B}$ is also a linear code, $\mathcal{A}$ is the dual of $\mathcal{B}$ and $\mathcal{B}$ has dimension n-k.

Theorem 1.6

The dual of $GRM_r(m,q)$ is $GRM_{(q-1)m-1-r}(m,q)$.

Proof:

If $P \in \mathcal{P}_r(m,q)$ and $Q \in \mathcal{P}_{(q-1)m-1-r}(m,q)$, then their product as polynomials PQ is in $\mathcal{P}_{(q-1)m-1}(m,q)$. If $\bar{a}$ is the value table of P and $\bar{b}$ is the value table of Q, then $\bar{a} \cdot \bar{b}$ is the value table of PQ, so $\bar{a} \cdot \bar{b} = \sum_{\bar{\sigma} \in K^m} PQ(\bar{\sigma})$. That $\sum_{\bar{\sigma} \in K^m} PQ(\bar{\sigma}) = 0$, follows from Lemma 1.7 below. If $Q \in \mathcal{P}(m,q)$ with $\deg Q \geqslant (q-1)m - r$, let one of the highest degree terms of Q be $ax_1^{i_1}x_2^{i_2} \ldots x_m^{i_m}$ where $0 \leqslant i_j \leqslant q-1$ for

$$j = 1,\ldots,m, \sum_{j=1}^{m} i_j \geqslant (q-1)m - r,$$

and $a \neq 0$. Let $P(\bar{x}) = x_1^{q-i_1-1}x_2^{q-i_2-1} \ldots x_m^{q-i_m-1}$. Then $\deg P = (q-1)m - \deg Q \leqslant r$ and $\deg PQ = (q-1)m$. By Lemma 1.7,

$$\bar{a} \cdot \bar{b} = \sum_{\bar{\sigma} \in K^m} PQ(\bar{\sigma}) \neq 0 \quad .$$

This completes the proof given Lemma 1.7.

Lemma 1.7

Let P be a polynomial in $\mathcal{P}(m,q)$, then $\deg P = m(q-1)$ if and only if $\sum_{\bar{\sigma} \in K^m} P(\bar{\sigma}) \neq 0$.

Proof of Lemma 1.7

For each $\overline{\sigma} \in K^m$, let $F_{\overline{\sigma}} = \prod_{i=1}^{m} (1 - (x_i - \sigma_i)^{q-1})$, then

$$F_{\overline{\sigma}}(\overline{\tau}) = \begin{cases} 1 & \text{if} \quad \overline{\tau} = \overline{\sigma} \\ 0 & \text{otherwise} \end{cases}$$

also $F_{\overline{\sigma}}(\overline{x}) = (-1)^m x_1^{q-1} x_2^{q-1} \dots x_m^{q-1}$ + terms of lower degree, so any $P \in \mathcal{P}(m,q)$ may be written:

$$P(\overline{x}) = \sum_{\overline{\sigma} \in K^m} P(\overline{\sigma}) F_{\overline{\sigma}}(\overline{x}) = (-1)^m \sum_{\overline{\sigma} \in K^m} P(\overline{\sigma})\ x_1^{q-1} x_2^{q-1} \dots x_m^{q-1}$$

+ lower degree terms, so deg $P < m(q-1)$ if and only if $\sum_{\overline{\sigma} \in K^m} P(\overline{\sigma}) = 0$.

This completes the proof of Lemma 1.7 and Theorem 1.6.

The MacWilliams identity relates the weight enumerator of a linear code to the weight enumerator of its dual.

Theorem 1.8: MacWilliams Identity

If A(z) is the weight enumerator of an (n, k) linear code, and B(z) is the weight enumerator of its dual, then

$$B(z) = q^{-k}(1 - (q-1)z)^n A\left(\frac{1 - z}{1 + (q-1)z}\right)$$

Most recent texts on coding theory contain proofs of this theorem. See Coding Theory by van Lint, pp. 120-121 [11] or Algebraic Coding Theory by Berlekamp, pp. 400-403 [2] for examples of proofs.

Intuitively, the MacWilliams identity is a tool which can be used to solve for the two weight enumerators completely if enough of the A_i and B_i are known. It has been found to be quite useful in this regard. When $r < m$, the Ax divisibility condition proves that many of the A_i are zero where $\mathcal{A} = GRM_r(m, q)$. The minimum weight results show that $A_i = 0$ for $0 < i < (q-t)q^{m-s-1}$. Warning's result on the minimum number of zeros when $r < m$ shows, in addition, that $A_i = 0$ for $q^m - q^{m-r} < i < q^m$.

Because in Reed-Muller Codes, $q = 2$, a polynomial of weight $|P|$ may be mapped into $P+1$ with weight $|P+1| = 2^m - |P|$. In $RM(3, 2^8)$ all of the gaps are either less than twice the minimum weight or more than 2^8-twice the minimum weight (in which cases they are predicted by the Kasami, Tokura paper), or they are predicted by the Ax divisibility condition. In 1971, van Tilborg [12] revealed four gaps of $RM(3, 2^9)$ which were not predicted by either paper: 132, 140 and their reflections 372 and 380. These gaps did fall under the scope of Kasami, Tokura and Azumi's 1973 publication [8] characterizing the code words with weight less than two-and-a-half times the minimum weight in a Reed-Muller Code.

This paper concentrates on low-weight gaps in non-binary GRM codes. One specific question which this dissertation seeks to answer is: What is the next-to-minimum weight in a Generalized Reed-Muller Code?

Theorem 2.1 gives a lower bound on the next-to-minimum weight. Theorem 3.1 improves this bound in some cases, shows that it cannot be improved for others, and for the rest of the cases, reduces the question of whether it can be improved upon to the case $m = 2$.

CHAPTER 2

The goal of this chapter is twofold; first, to prove Theorem 2.1, and secondly, to develop lemmas which will shed light on the structure of low-weight polynomials.

Theorem 2.1

Let $r = s(q-1) + t$ where $0 < t \leqslant q-1$, and let

$$c = \begin{cases} q-1 & \text{if } t = 1 \\ q-2 & \text{if } t = q-1 \neq 1 \\ \min(q-t, t-1) & \text{otherwise} \end{cases}$$

If P is a polynomial of degree r in m variables over GF(q) such that $|P| > (q-t)q^{m-s-1}$, then $|P| \geqslant (q-t)q^{m-s-1} + cq^{m-s-2}$.

The approach of this chapter is motivated by the work of Delsarte, Goethals, and MacWilliams [5]. In some cases, the lemmas are similar and will be cross-referenced to the D.G. and M. paper. The first lemma deals with linear factors, which will play an important role in this exposition.

Lemma 2.2 (D.G. and M. Lemma A1.1)

If $P(x_1, \ldots, x_m)$ is a nonzero polynomial such that $P(\overline{\alpha}) = 0$ whenever $\alpha_1 = a$, then $P(\overline{x}) = (x_1-a)\hat{P}(x)$ where $\deg \hat{P} = \deg P-1$ and $\deg_1\hat{P} = \deg_1 P-1$.

Proof:

$P(a, \alpha_2, \ldots, \alpha_m) = 0$ for all $\alpha_2, \ldots, \alpha_m$. Represent P $P(\overline{x}) = g_0 x_1^{q-1} + g_1 x_1^{q-2} + \ldots + g_{q-2} x_1 + g_{q-1}$ where $g_i = g_i(x_2, \ldots, x_m)$, then

$$P(\overline{x}) = P(\overline{x}) - P(a, x_2, \ldots, x_m) = g_0(x_1^{q-1} - a^{q-1}) + \ldots + g_{q-2}(x_1 - a)$$

$$= (x_1 - a)[g_0(x_1^{q-2} + \ldots + a^{q-2}) + \ldots + g_{q-2}] \ .$$

Lemma 2.3 (D.G. and M. Corollary A1.2)

If $P(\overline{x}) = 0$ unless $\alpha_1 = b$, then $P(\overline{x}) = (1 - (x_1 - b)^{q-1})\hat{P}(x_2, \ldots, x_m)$ where deg $\hat{P}$ = deg P - (q-1).

Proof:

$$\prod_{\substack{\alpha \in GF(q) \\ \alpha \neq b}} (x_1 - \alpha) = \left\{ \begin{matrix} \beta \text{ if } x_1 = b \\ 0 \text{ otherwise} \end{matrix} \right\} = \beta(1 - (x_1 - b)^{q-1})$$

where

$$\beta = \prod_{\gamma \neq 0} \gamma \neq 0 \ .$$

Lemma 2.4

If $y(\overline{x}) = \beta_1 x_1 + \ldots + \beta_m x_m + \eta$ and $y(\overline{\alpha}) = 0 \Rightarrow P(\overline{\alpha}) = 0$, then y divides P.

Proof:

Let $x \to xA + \overline{\omega}$ be an invertible affine transformation such that $\omega_1 = \eta$ and $a_{i1} = \beta_i$ for $i = 1, \ldots, m$. Let $R(\overline{x}) = P(\overline{x}A^{-1} - \overline{\omega}A^{-1})$ so that $P(\overline{x}) = R(\overline{x}A + \overline{\omega})$. And let $\overline{\alpha} = (0, \alpha_2, \ldots, \alpha_m)$ so that $R(\overline{\alpha}) = P(\overline{\alpha}A^{-1} - \overline{\omega}A^{-1})$.

Let $\bar{\gamma} = \bar{\alpha}A^{-1} - \bar{\omega}A^{-1}$. Then $\bar{\alpha} = \bar{\gamma}A + \bar{\omega}$ so

$$0 = \alpha_1 = \omega_1 + \sum_{i=1}^{m} a_{i1}\gamma_i = \eta + \sum_{i=1}^{m} \beta_i\gamma_i$$

so by the hypothesis, $P(\bar{\gamma}) = 0$. Thus $R(\bar{\alpha}) = 0$. Applying 2.2, $R(\bar{x}) = x_1\hat{R}(\bar{x})$. But invertible affine transformations preserve polynomial products, so $P(\bar{x}) = R(\bar{x}A + \bar{\omega}) = y \cdot \hat{R}(\bar{x}A + \bar{\omega})$.

Separation of a variable is an extremely useful technique which will be used heavily in chapters two and three. It is refined from a similar technique used by D.G. and M. and expounded upon in their Lemmas A1.6 and A1.7. The concept behind this technique is the isolation of the effect of the variable x_1. One may write:

$$P(\bar{x}) = P(x_1, x_2, \ldots, x_m) = P(x_1, \bar{x}') \qquad \text{where } \bar{x}' = (x_2, \ldots, x_m) \ .$$

For each $P \in \mathcal{P}(m, q)$, $m > 1$ and each $\lambda \in K = GF(q)$ define $P_\lambda(\bar{x}') = P(\lambda, \bar{x}') \in \mathcal{P}(m-1, q)$. Then

$$(201) \qquad |P|_m = \sum_{\lambda \in K} |P_\lambda|_{m-1}$$

where the subscripts on the weight serve only as reminders of the number of variables on which the polynomial depends.

Given any ordering of the elements of K, $\lambda_1, \lambda_2, \ldots, \lambda_q$, define polynomials $P^{(0)}, P^{(1)}, \ldots, P^{(q-1)}$ by:

$$(202) \qquad P^{(i)} = \begin{cases} P \text{ if } i = 0 \\ [P^{(i-1)} - P^{(i-1)}_{\lambda_i}]/(x_1 - \lambda_i) \qquad \text{for} \quad i = 1, 2, \ldots, q-1. \end{cases}$$

That $P^{(i)}$ is a polynomial follows from Lemma 2.2. It is also evident from 2.2 that

$$(203) \qquad \deg P^{(k)} \leqslant \deg P - k; \qquad \deg_1 P^{(k)} = \deg_1 P - k$$

with the convention that $\deg_1 P^{(k)} < 0$ means $P^{(k)} = 0$.

This, and the fact that P is a reduced polynomial imply that $\deg_1 P^{(q-1)} \leqslant 0$ so that $P^{(q-1)} = P^{(q-1)}_{\lambda_q}$. From (202),

$$P^{(i-1)} = P^{(i-1)}_{\lambda_i} + (x_1 - \lambda_i)P^{(i)} \qquad \text{for} \quad i = 1, \ldots, q-1 \quad .$$

By induction

$$(204) \qquad P^{(i)} = \sum_{j=i}^{q-1} \left[P^{(j)}_{\lambda_{j+1}} \prod_{k=i+1}^{j} (x_1 - \lambda_k) \right]$$

$$= P^{(i)}_{\lambda_{i+1}} + (x_1 - \lambda_{i+1})P^{(i+1)}_{\lambda_{j+1}} + \ldots + (x_1 - \lambda_{i+1})$$

$$\ldots (x_1 - \lambda_{q-1})P^{(q-1)}_{\lambda_q} \quad .$$

When i = 0 this becomes

$$(205) \qquad P = \sum_{j=0}^{q-1} \left[P^{(j)}_{\lambda_{j+1}} \prod_{k=1}^{j} (x_1 - \lambda_k) \right]$$

$$= P_{\lambda_1} + (x_1 - \lambda_1)P^{(i)}_{\lambda_2} + \ldots + (x_1 - \lambda_1) \ldots (x_1 - \lambda_{q-1})P^{(q-1)}_{\lambda_q} \quad .$$

From the definition of P_λ:

$$(206) \qquad P_{\lambda_i} = \sum_{j=0}^{i-1} \left[P^{(j)}_{\lambda_{j+1}} \prod_{k=1}^{j} (\lambda_i - \lambda_k) \right]$$

$$= P_{\lambda_1} + (\lambda_i - \lambda_1)P^{(1)}_{\lambda_2} + \ldots + (\lambda_i - \lambda_1) \ldots (\lambda_i - \lambda_{i-1})P^{(i-1)}_{\lambda_i} \quad .$$

Lemma 2.5

If $P \in \mathcal{P}(m, q)$ and $\lambda_1, \ldots, \lambda_q$ is an ordering of the elements of K such that $P_{\lambda_1} = \ldots = P_{\lambda_n} = 0$, then $\deg P_{\lambda_i} \leq \deg P - n$ for $i > n$.

Proof:

By induction from (206), $P^{(0)}_{\lambda_1} = \ldots = P^{(n-1)}_{\lambda_n} = 0$ so

$$\deg P_{\lambda_i} = \deg \sum_{j=n}^{i-1} P^{j}_{\lambda_{j+1}} \prod_{k=1}^{j} (\lambda_1 - \lambda_k) \quad \leq \deg P - n$$

from (203).

As an illustration of the use of this technique and also for the sake of completeness since this theorem will be used in future proofs, a proof is now given for Theorem 2.6.

Theorem 2.6: Bound on Minimum Weight

Let $r = s(q-1) + t$, $0 < t \leq q-1$ and let $d_r^m = (q-t)q^{m-s-1}$. If $P \in \mathcal{P}_r(m, q)$ such that $P \neq 0$, then $|P| \geq d_r^m$.

Many authors have given proofs of this result including Kasami, Lin, and Peterson [6].

Proof:

The theorem is trivially true for $m = 1$. Proceed by induction. Assume 2.6 is true for $m-1$. By (201) $|P|_m = \sum_{\lambda \in K} |P_\lambda|_{m-1}$. If $P_\lambda \neq 0$ for all $\lambda \in K$, then by the induction hypothesis $|P|_m \geqslant qd_r^{m-1} = d_r^m$. Otherwise, order the elements of K so that $P_{\lambda_1} = \ldots = P_{\lambda_n} = 0$, but $P_{\lambda_i} \neq 0$ for $i > n$. Since $P \neq 0$, $1 \leqslant n \leqslant q-1$. By Lemma 2.5, $\deg P_{\lambda_i} \leqslant r-n$ for $i > n$ so

$$|P|_m = \sum_{i=n+1}^{q} |P_{\lambda_i}|_{m-1} \geqslant (q-n)d_{r-n}^{m-1} = (q-n)\begin{cases}(q-t+n)q^{m-s-2} & \text{if } n < t\\ (1-t+n)q^{m-s-1} & \text{if } n \geqslant t\end{cases}$$

$$= \begin{cases}(q-t)q^{m-s-1} + n(t-n)q^{m-s-2} & \text{if } n < t\\ (q-t)q^{m-s-1} + (n-t)(q-1-n)q^{m-s-1} & \text{if } n \geqslant t\end{cases}$$

$$\geqslant (q-t)q^{m-s-1} \qquad \text{since } 0 < n \leqslant q-1 ,$$

completing the proof.

The parameter n plays a significant role in the above inequalities. It will be called the linear divisibility of P by x_1 and will be formalized by the following definitions.

A variable in $\mathcal{P}(m,q)$ is a polynomial $y \in \mathcal{P}(m,q)$ such that $\deg y = 1$.

The linear divisibility of a polynomial $P \in \mathcal{P}(m,q)$ by a variable y in $\mathcal{P}(m,q)$ is the number of distinct $\lambda \in K$ such that $y - \lambda$ divides P. This value is denoted $\ell d(P,y)$. Since polynomial products are preserved by invertible affine transformations, and we can always find an invertible affine transformation which takes y into x_1, there is a polynomial $\widetilde{P}_y$ such that $\widetilde{P}_y$ is equivalent to P and $\ell d(\widetilde{P}_y, x_1) = \ell d(P, y)$. With the same proof as 2.6 then:

Lemma 2.7

If $P \in \mathcal{P}_r(m, q)$ $P \neq 0$ and there is a variable y in $\mathcal{P}(m, q)$ such that $\ell d(P, y) = n$, then

$$|P| \geqslant d_r^m + \begin{cases} n(t-n)q^{m-s-2} & \text{if } n < t \\ (n-t)(q-1-n)q^{m-s-1} & \text{if } n \geqslant t \end{cases}$$

with equality if and only if $|Q_\lambda| > 0 \Rightarrow |Q_\lambda| = d_{r-n}^{m-1}$ for any $Q(\overline{x}) = P(T(\overline{x}))$ where T is an invertible affine transformation such that $T(x_1) = y$.

Proof:

$|P| = |\widetilde{P}_y|$ because equivalence preserves weight. Apply (201) and Lemma 2.5 as in the proof of 2.6.

This lemma provides the first step to a proof of Theorem 2.1 since it implies that

$$|P| \geqslant d_r^m + \begin{cases} q^{m-s-1} & \text{if } t = 1 \\ (t-1)q^{m-s-2} & \text{if } t > 1 \end{cases}$$

unless $\ell d(P, y) = 0$, t, or q-1 for all variables y. If, for some y, $\ell d(P, y) = q-1$, then by Corollary 2.3, $\widetilde{P}_y(x_1, \ldots, x_m) = (1 - (x_1 - b)^{q-1}) \cdot \hat{P}(x_2, \ldots, x_m)$ where $\hat{P} \in \mathcal{P}_{r-(q-1)}(m-1, q)$, and by (201), $|P|_m = |\hat{P}|_{m-1}$, so induction may be applied. If, for some y, $\ell d(P, y) = t$, then $|P| = |R|$ where $R = \widetilde{P}_y$, so that

$$|R| = \sum_{i=n+1}^{q} |R_{\lambda_i}|$$

where deg $R_{\lambda_i} \leq s(q-1)$. Later lemmas will examine this case more thoroughly.

If $\ell d(P, y) = 0$ for all y, then P has no linear factors. This case will be examined in greater detail in chapter three, but here a general lemma is given. The proof requires some knowledge of the relationships of affine subspaces of K^m.

An n-dimensional affine subspace of K^m is a set of vectors derived from a homogeneous n-dimensional subspace by the addition of a constant vector to each element. The zero set of a linear polynomial (variable) is an (m-1) dimensional affine subspace. Conversely, every (m-1) dimensional affine subspace is the zero-set of some variable. Thus, if a polynomial $P(\overline{x})$ is zero on every point of an (m-1) dimensional affine subspace, then there is a variable y such that $y(\overline{\alpha}) = 0 \Rightarrow P(\overline{\alpha}) = 0$ and, by Lemma 2.4, y divides P so that P has a linear factor.

If G is an n-dimensional affine subspace of K^m, a k-dimensional affine subspace of K^m which is contained in G will be called a k-dimensional affine subspace of G or, for brevity, a k-subspace of G. Given an (n-1)-subspace H_1 of G, there exist q-1 additional (n-1)-subspaces $H_2, \ldots, H_q$ of G such that $H_i \wedge H_j = \phi$ if $i \neq j$ and

$$\bigcup_{i=1}^{q} H_i = G \ .$$

The subspaces $H_1, H_2, \ldots, H_q$ will be called q parallel (n-1)-subspaces of G.

Given an (n-2)-subspace E of G, there exist q+1 (n-1)-subspaces $H_0, \ldots, H_q$ of G such that $H_i \cap H_j = E$ if $i \neq j$ and

$$\bigcup_{i=0}^{q} H_i = G \ .$$

In this case, the H_i will be called the q+1 (n-1)-subspaces of G containing E. D.G. and M. proved the following lemma in characterizing the minimum weight polynomials.

D.G. and M. Lemma A1.3

If S is a subset of K^m with the following properties:

1) $|S| \leq aq^b$, $0 < a \leq q-1$, $b \leq m-1$, a, b integers

2) For any (n-1)-subspace G of K^m such that $S \cap G \neq \phi$, $|S \cap G| \geq aq^{b-1}$;

then there is an (m-1)-subspace of K^m which does not meet S.

For the purposes of this paper, a stronger lemma is needed, namely:

Lemma 2.8

Given an n dimensional affine subspace B of K^m, if S is a subset of B with the properties:

1) $|S| < aq^b + aq^{b-1}$, a, b integers $0 < a \leq q-1$, $b \leq n-1$

2) For any k dimensional affine subspace G contained in B, either $|S \cap G| = 0$ or $|S \cap G| \geq aq^{b-n+k}$,

then there exists an (n-1)-subspace of B which does not meet S.

Proof:

If $n = 1$, then condition 1) implies $|S| \leq q-1$, so there exists a 0-subset (a point) of B which does not meet S. Proceeding by induction, assume 2.8 is true for all $n < N$. Let B be an N-dimensional affine subspace of K^m, S a subset of B satisfying 1) and 2). Examine q parallel (N-1) subspaces of B. One of these, call it H, has fewer than $aq^{b-1} + aq^{b-2}$ elements of S. By an application of the induction hypothesis to $S \cap H$ as a subset of H satisfying 1) and 2) with $n = N-1$, there exists an (N-2)-subspace L of H which does not meet S. Let $H_0, H_1, \ldots, H_q$ be the q+1 (N-1)-subspaces of B containing L. Then

$$|S| = \sum_{i=0}^{q} |H_i \cap S| - q|L \cap S| = \sum_{i=0}^{q} |H_i \cap S| .$$

Thus there is an i such that

$$|H_i \cap S| < (aq^b + aq^{b-1})/(q+1) = aq^{b-1} ,$$

but by condition 2) with $k = N-1$, $|H_i \cap S| = 0$, so H_i is the (N-1)-subspace we seek. This completes the proof of 2.8.

Corollary 2.8.1

If $P \in \mathcal{P}_r(m,q)$ and P has no linear factors, then $|P| \geq (q-t)a^{m-s-1} + (q-t)q^{m-s-2} = (1 + 1/q)d_r^m$ where $r = s(q-1) + t$ $0 < t \leq q-1$.

Proof:

Let $S = S(P)$, the support points of P, and let $a = (q-t)$, $b = m-s-1$. Then condition 2) is satisfied by Theorem 2.6. If $|P| < (q-t)q^{m-s-1} + (q-t)q^{m-s-2}$, then condition 1) is also satisfied and, by Lemma 2.8, P has a linear factor.

The next corollary is the first step toward characterizing low-weight, low-degree polynomials.

Corollary 2.8.2

If $P \in \mathcal{P}_r(m,q)$ with $r \leq q-1$ and $|P| < (1 + 1/q)d_r^m$, then P is the product of r linear factors.

Proof:

Certainly true for $r = 1$. Assume this corollary is true for $r \leq R-1$ and proceed by induction on r. If $P \in \mathcal{P}_R(m,q)$ and $|P| < (1 + 1/q)d_R^m$, then by 2.8.1, P has a linear factor, so

$$P = \ell\hat{P} \quad \text{where} \quad \deg \hat{P} \leq R-1 \quad .$$

But $|\hat{P}| \leq |P| + q^{m-1} < (q-R+1)q^{m-1} + (q-R)q^{m-2} < (1 + 1/q)d_{R-1}^m$ so by induction, $\hat{P}$ breaks into linear factors, completing the proof.

Corollary 2.8.1 establishes a lower bound for the weight of a polynomial without linear factors. We now turn our attention to low weight polynomials with linear factors.

Delsarte, Goethals, and MacWilliams [5] state the following theorem as 2.6.3 and prove it in their appendix:

Theorem 2.9 (D.G. and M, 2.6.3)

If $P \in \mathcal{P}_r(m,q)$ where $r = s(q-1) + t$, $0 < t \leq q-1$ and $|P| = d_r^m = (q-t)q^{m-s-1}$ then P is equivalent to a polynomial Q where

$$(207) \quad Q(\bar{x}) = \lambda \prod_{i=1}^{s} (1 - x_i^{q-1}) \prod_{j=1}^{t} (\lambda_j - x_{s+1}) \quad \lambda \neq 0 \quad \lambda_i \neq \lambda_j \quad \text{if } i \neq j \ .$$

A proof of this result will be given later in this chapter after several preparatory lemmas. It may be observed here, however, that for any r there exists such a Q, deg Q = r, $|Q| = d_r^m$, so that the bound given in Lemma 2.6 is, in fact, the minimum weight. This well-known result is stated as:

Theorem 2.10 Minimum Weight

The minimum weight of $GRM_r(m,q)$ is $d_r^m = (q-t)q^{m-s-1}$ where $r = s(q-1) + t$, $0 < t \leq q-1$.

Two other types of polynomials have low-weight and are closely related to (207). These are:

$$(208) \quad Q(\bar{x}) = \lambda x_{s+2} \prod_{i=1}^{s} (1 - x_i^{q-1}) \prod_{j=1}^{t-1} (\lambda_j - x_{s+1}) \quad \lambda \neq 0 \quad \lambda_i \neq \lambda_j \quad \text{if } i \neq j$$

$$(209) \quad Q(\bar{x}) = \lambda \prod_{i=1}^{s} (1 - x_i^{q-1}) \prod_{j=1}^{t} L_j(x_{s+1}, x_{s+2})$$

where $L_j(x_{s+1}, x_{s+2}) = \alpha_j x_{s+1} + \beta_j x_{s+2}$ and $\alpha_j \beta_i \neq \alpha_i \beta_j$ if $i \neq j$.

Both describe polynomials Q such that deg Q = r = s(q-1) + t $0 < t \leq q-1$ and if $t \neq 1$, then $|Q| = (q-t)q^{m-s-1} + (t-1)q^{m-s-2}$. In many cases, these are precisely the next-to-minimum weight polynomials, as will be shown.

The next two lemmas form a starting point for an induction proof of Theorem 2.9 and of Theorem 2.1. They deal with the case $r \leq q-1$ where $\ell d(P, y) > r$ implies $P = 0$.

Lemma 2.11 (D.G. and M., A1.5)

If $P \in \mathcal{P}_r(m,q)$ with $r \leq q-1$, and $|P| = d_r^m = (q-t)q^{m-1}$, then P is equivalent to a polynomial Q such that

$$Q(\overline{x}) = \lambda \prod_{j=1}^{r} (\lambda_j - x_1) \quad \lambda_i \neq \lambda_j \text{ if } i \neq j \quad \text{(i.e., form (207))} \ .$$

Proof:

Corollary 2.8.1 states that P has a linear factor $y(\overline{x})$. Let T be an invertible affine transformation such that $x_1 = T(y)$ and let $Q(\overline{x}) = P(T(\overline{x}))$. Then $\ell d(Q, x_1) > 0$, and $Q \neq 0$ so $\ell d(Q, x_1) \leq r$. Since $|Q| = d_r^m$, by Lemma 2.7, $\ell d(Q, x_1) = r$ so $Q = \hat{Q} \prod_{j=1}^{r} (\lambda_j - x_1)$, but $\deg \hat{Q} = 0$, so $\hat{Q} = \lambda$, and the proof is completed.

Lemma 2.12

If $P \in \mathcal{P}_r(m,q)$, $r \leq q-1$ and P has a linear factor, then $|P| > d_r^m = (q-r)q^{m-1}$ implies $|P| \geq d_r^m + (r-1)q^{m-2}$.

Proof:

Without loss of generality, assume x_1 divides P. Then $0 < \ell d(P, x_1) \leq r$. If $\ell d(P, x_1) = r$, then $|P| = d_r^m$ contradicting $|P| > d_r^m$. Otherwise, by Lemma 2.7, $|P| \geq d_r^m + n(r-n)q^{m-2} \geq d_r^m + (r-1)q^{m-2}$, where $n = \ell d(P, x_1)$.

Corollary 2.12.1

If $4 \leqslant 2r \leqslant q$, a next-to-minimum weight polynomial of degree r in m variables over GF(q) has weight $(q-r)q^{m-1} + (r-1)q^{m-2}$.

Proof:

From Corollary 2.8.1, if P has no linear factors, then $|P| \geqslant (q-r)q^{m-1} + (q-r)q^{m-2} \geqslant (q-r)q^{m-1} + rq^{m-2}$. From Lemma 2.12, if $|P| > d_r^m$ and P has a linear factor, then $|P| \geqslant (q-r)q^{m-1} + (r-1)q^{m-2}$. With $1 \leqslant r < q$, formulas (208) and (209) give polynomials with exactly this weight, so this is indeed the next-to-minimum weight.

It is, in fact, true that (208) and (209) characterize all of the polynomials of this weight with r in the given range, as will be proved in chapter three.

Corollary 2.12.1 is significant,in that given any $r \geqslant 2$ and any m, it establishes the next-to-minimum weight for all but a finite number of q.

The next lemma begins the study of another special class of r's: $r = s(q-1)$. Delsarte, Goethals and MacWilliams did not proceed by quite this route and so had no similar lemma.

Lemma 2.13

If P is a minimum-weight polynomial of $\mathcal{P}_r(m,q)$ where $r = s(q-1)$, then P is equivalent to:

$$\lambda \prod_{i=1}^{s} (1 - x_i^{q-1}) \qquad \text{(that is, (207))} \ .$$

Proof:

$d_r^m = q^{m-s}$. Let $P \in \mathcal{P}_r(m,q)$ such that $|P| = d_r^m$. By Corollary 2.8.1, P has a linear factor. Without loss of generality, assume x_1 divides P. Lemma 2.7 tells us that $\ell d(P, x_1) = q-1$ and thus $P \sim (1 - x_1^{q-1})\,\hat{P}(x')$ where $\hat{P}$ is minimum weight of degree (s-1)(q-1). With this argument as an induction step and Lemma 2.11 as a starting point, the proof is complete.

The next lemma deals with sums of minimum weight polynomials and polynomials of lesser degree.

Lemma 2.14

Let Q be a minimum weight polynomial in $\mathcal{P}_r(m,q)$ where $r = s(q-1)$, $0 < s \leq m$. Let R be a nonzero polynomial in $\mathcal{P}_{r-k}(m,q)$ where $0 < k \leq q-1$. If $P = Q+R$, then either $|P| = kq^{m-s}$ or $|P| \geq (k+1)q^{m-s}$.

Proof:

When $m = 1$, then $s = 1$. In this case $|Q| = 1$, $|R| \geq k+1$, and the conclusion $|P| = k$ or $|P| \geq k+1$ is obvious. Proceed by induction on m assuming 2.14 is true for m-1. By Lemma 2.13, it can be assumed that $Q = (1 - x_1^{q-1})Q_0(\overline{x}^1)$ where Q_0 is a minimum weight polynomial of degres (s-1)(q-1) in m-1 variables. Separating x_1 in P

1) $$|P|_m = \sum_{\lambda \in K} |P_\lambda|_{m-1} = |R_0 + Q_0|_{m-1} + \sum_{\lambda \neq 0} |R_\lambda|_{m-1} \qquad (201)$$

Order the elements of K, $\lambda_1, \ldots, \lambda_q$ so that: $\lambda_{n+1} = 0$, $|R_{\lambda_i}| = 0$ for $i \leqslant n$, $|R_{\lambda_i}| > 0$ for $i > n+1$. Since $R \neq 0$, $n \leqslant \deg R \leqslant r-k$, so if $s = 1$, $(n+k) \leqslant q-1$. If $n = q-1$, then $s > 1$ and $|P| = |R_0 + Q_0|_{m-1}$. In this case, the induction hypothesis proves the conclusion. Otherwise, write:

$$(2) \qquad R(x_1, \bar{x}') = \lambda \prod_{i=1}^{n} (x_1 - \lambda_i)[R_0(\bar{x}') + x_1\hat{R}(x_1, \bar{x}')]$$

where $\deg R_0 \leqslant r - (k+n)$ and $\deg \hat{R} \leqslant r - (k+n) - 1$.

If $P_0 \neq 0$, then $\deg P_0 = \deg(Q_0 + R_0) \leqslant \max(r - (q-1),\ r - (k+n))$ and $\deg P_{\lambda_i} \leqslant r - (k+n)$ for $i > n+1$ so $|P| \geqslant (q-n-1)d^{m-1}_{r-(k+n)} + d^{m-1}_{r-b}$ where $b = \min((q-1), (k+n))$.

$$(k+n) > (q-1) \quad \text{implies} \quad |P| \geqslant (q-n-1)(n+k+2-q)q^{m-s} + q^{m-s}$$
$$= [1 + k + (q-2-n)(n+k-(q-1))]q^{m-s} \geqslant (k+1)q^{m-s} \quad .$$

$$(k+n) \leqslant (q-1) \quad \text{implies} \quad |P| \geqslant (q-n)(1+k+n)q^{m-s-1}$$
$$= (1+k)q^{m-s} + n(q-1-(k+n))q^{m-s-1} \geqslant (k+1)q^{m-s} \quad .$$

If $P_0 = 0$, then $R_0 = -Q_0$ so $\deg R_0 = \deg Q_0 = r - (q-1)$. This implies $r - (k+n) \geqslant r - (q-1)$, so $(k+n) \leqslant (q-1)$.

$$(k+n) < (q-1) \quad \text{implies} \quad \deg P_{\lambda_i} = \deg R_{\lambda_i}$$
$$\leqslant \max(\deg R_0, \deg \hat{R}) = r - (k+n) - 1$$

$$\text{so} \quad |P| \geqslant (q-n-1)d^{m-1}_{r-(k+n)-1} = (q-n-1)(k+n+2)q^{m-s-1}$$
$$= (k+1)q^{m-s} + (1+n)(q-2-(n+k))q^{m-s-1} \geqslant (k+1)q^{m-s} \quad .$$

The only case left is $(k+n) = (q-1)$. Here $|P| \geqslant (q-n-1)d_{r-(k+n)}^{m-1} = kq^{m-s}$, but the equality holds if and only if $|R_{\lambda_i}| = d_{r-(q-1)}^{m-1}$ for $i > n+1$. Suppose for some $i > n+1$, $|R_{\lambda_i}| > d_{r-(q-1)}^{m-1}$, then from (2) $R_{\lambda_i}(\overline{x}') = \lambda'[R_0(\overline{x}') + \lambda_i\hat{R}_{\lambda_i}(\overline{x}')]$ where $\lambda' R_0$ is a minimum weight polynomial in $\mathcal{P}_{r-(q-1)}(m-1,q)$ and $\lambda'\lambda_i\hat{R}_{\lambda_i} \neq 0$, $\deg \lambda'\lambda_i\hat{R}_{\lambda_i} \leqslant r-(q-1)-1$. Applying the induction hypothesis, $|R_{\lambda_i}|_{m-1} > q^{m-s}$ implies $|R_{\lambda_i}|_{m-1} \geqslant 2q^{m-s}$. But this forces $|P| \geqslant (k+1)q^{m-s}$, completing the proof.

Notice that in the preceding proof, the only cases in which $|P| = kq^{m-s}$ could occur were $n = q-1$ and $(n+k) = (q-1)$ with $P_0 = 0$ and $|R_0|$ = minimum weight for $i > n+1$. This observation provides the basis for the next lemma.

Lemma 2.15

Let P be a polynomial of $\mathcal{P}_r(m,q)$ where $r = s(q-1)$, $0 < s < m$. If for some $\lambda_1, \lambda_2 \in K$ $\lambda_1 \neq \lambda_2$, $|P_{\lambda_1}| = |P_{\lambda_2}| = d_r^{m-1}$, then there is an invertible affine transformation T fixing x_1 such that if $R(\overline{x}) = P(T(x))$, then $R_{\lambda_1} = \sigma R_{\lambda_2}$ for some $\sigma \in K$.

By T fixing x_1 we mean $[T(\overline{x})]_1 = x_1$.

Proof:

If $m = 2$, then $s = 1$; $d_r^{m-1} = 1$ so $|P_{\lambda_1}| = |P_{\lambda_2}| = 1$. Thus, P has one support point such that $x_1 = \lambda_1$ and one support point such that $x_1 = \lambda_2$. Call these (λ_1, σ_1) and (λ_2, σ_2). Let

$$A = \begin{pmatrix} 1 & \dfrac{\sigma_2 - \sigma_1}{\lambda_2 - \lambda_1} \\ & \\ 0 & \dfrac{1}{\lambda_2 - \lambda_1} \end{pmatrix}$$

and let $T(\overline{x}) = \overline{x}A$.

$$R_{\lambda_1} = P((\lambda_1, x_2)A) = P(\lambda_1, \frac{(\sigma_2 - \sigma_1)\lambda_1 + x_2}{\lambda_2 - \lambda_1})$$

$$= P_{\lambda_1}(\frac{(\sigma_2 - \sigma_1)\lambda_1 + x_2}{\lambda_2 - \lambda_1})$$

similarly

$$R_{\lambda_2} = P_{\lambda_2}(\frac{(\sigma_2 - \sigma_2)\lambda_1 + x_2}{\lambda_2 - \lambda_1})$$

thus, $|R_{\lambda_1}| = |R_{\lambda_2}| = 1$, so if $S(R_{\lambda_1}) = S(R_{\lambda_2})$, then our conclusion $R_{\lambda_1} = \sigma R_{\lambda_2}$ is confirmed. But $R_{\lambda_1}(\sigma_1\lambda_2 - \sigma_2\lambda_1) = P_{\lambda_1}(\sigma_1) \neq 0$ and $R_{\lambda_2}(\sigma_1\lambda_2 - \sigma_2\lambda_1) = P_{\lambda_2}(\sigma_2) \neq 0$, so 2.15 is true for $m = 2$.

Now proceed by induction, assuming 2.15 is true for m-1.

Without loss of generality, assume

$$P_{\lambda_1} = \prod_{i=1}^{s} (1 - x_{i+1}^{q-1})$$

and write

$$P(x_1, \overline{x}') = P_{\lambda_1}(\overline{x}') + (x_1 - \lambda_1)\hat{P}(x_1, \overline{x}') \qquad \deg \hat{P} \leqslant r-1 \quad ,$$

then
$$P_{\lambda_2} = P_{\lambda_1} + (\lambda_2 - \lambda_1)\hat{P}_{\lambda_2}(\overline{x}') \qquad \deg \hat{P}_{\lambda_2} \leqslant r-1 \quad .$$

This is precisely the situation in Lemma 2.14 with $k = 1$.

$|P_{\lambda_2}| = kd_r^{m-1}$. Separating x_2, order the elements of K $\sigma_1, \sigma_2, \ldots, \sigma_q$ so that $\sigma_{n+1} = 0$, $|(P_{\lambda_2})_{\sigma_i}|_{m-2} = 0$ for $i \leq n$ and $|(P_{\lambda_2})_{\sigma_i}|_{m-2} > 0$ for $i > n+1$. As observed from the proof of 2.14, $n = q-1$ or ($n = q-2$, $(P_{\lambda_2})_0 = 0$ and $(P_{\lambda_2})_{\sigma_q}$ is minimum weight).

Define $P_{*,\sigma}(x_1, \bar{x}'') = P(x_1, \sigma, \bar{x}'')$ for $\sigma \in K$, and $P_{\lambda,\sigma}(\bar{x}'') = (P_{*,\sigma})_\lambda = (P_\lambda)_\sigma = P(\lambda, \sigma, \bar{x}'')$.

If $n = q-1$, then $|P_{\lambda_1,0}| = |P_{\lambda_2,0}|$, so applying the induction hypothesis to $P_{*,0}$, there is an invertible affine transformation $T''(x_1, \bar{x}'')$ fixing x_1 such that if $R'(x_1, \bar{x}'') = P_{*,0}(T''(x_1, \bar{x}''))$, then $R'_{\lambda_1} = \sigma R'_{\lambda_2}$.

Let $T(x_1, x_2, \bar{x}'') = (x_1, x_2, [T''(x_1, \bar{x}'')]_3, \ldots, [T''(x_1, \bar{x}'')]_m)$ and let $R(x) = P(T(\bar{x}))$. Then

$$\begin{aligned} R_{\lambda_1}(\bar{x}') &= P_{\lambda_1}(x_2, [T''(x_1, \bar{x}'')]_3, \ldots, [T''(x_1, \bar{x}'')]_m) \\ &= \begin{cases} 0 & \text{if } x_2 \neq 0 \\ R'_{\lambda_1} & \text{if } x_2 = 0 \end{cases} \\ &= \sigma R_{\lambda_2} \quad . \end{aligned}$$

If $n = q-2$, then $P_{\lambda_2} = (1 - (x_2 - \alpha)^{q-1})\tilde{P}(\bar{x}'')$ where $\tilde{P}$ is a minimum weight polynomial in $\mathcal{P}_{r-(q-1)}(m-2, q)$ and $\alpha \in K$ $\alpha \neq 0$. Define the transformation T_α as follows.

$$[T_\alpha(\bar{x})]_i = x_i \quad \text{for} \quad i \neq 2, \; [T_\alpha(\bar{x})]_2 = x_2 + \alpha \frac{x_1 - \lambda_1}{\lambda_2 - \lambda_1} \quad .$$

Then let $S(\bar{x}) = P(T_\alpha(\bar{x}))$

$$S_{\lambda_1} = P_{\lambda_1} \quad \text{and} \quad S_{\lambda_2} = (1 - x_2^{q-1})\tilde{P}(\bar{x}'') \quad .$$

Using the results of the previous case, $n = q-1$, there is an invertible affine transformation T' such that if $R(\overline{x}) = S(T'(\overline{x}))$, then $R_{\lambda_1} = \sigma R_{\lambda_2}$ and T' fixes x_1. $R(\overline{x}) = P(T_\alpha T'(\overline{x}))$ and $T_\alpha T'$ fixes x_1.

Corollary 2.15.1

Let P be a polynomial of $\mathcal{P}_r(m,q)$ where $r = s(q-1)$, $0 < s < m$. If for some $\lambda_1, \lambda_2 \in K$, $\lambda_1 \neq \lambda_2$, $|P_{\lambda_1}| = |P_{\lambda_2}| = d_r^{m-1}$, then there is an invertible affine transformation T fixing x_1 such that if $R(\overline{x}) = P(T(\overline{x}))$, then $R_{\lambda_1} = R_{\lambda_2}$.

Proof:

This strengthening of 2.15 is proved by observing that $\sigma R_{\lambda_2} = R_{\lambda_1}$ and

$$R_{\lambda_2} = R_{\lambda_1} + (\lambda_2-\lambda_1)\widetilde{R}(\overline{x}') \qquad \text{where} \qquad \deg \widetilde{R} \leq r-1$$

$$(\lambda_2-\lambda_1)\widetilde{R} = R_{\lambda_2} - R_{\lambda_1} = (1-\sigma)R_{\lambda_2}$$

but if $\sigma \neq 1$, this implies $|\widetilde{R}| = |R_{\lambda_2}| = d_r^{m-1} < d_{r-1}^{m-1}$ a contradiction!

The following proof of Delsarte, Goethals, and MacWilliams' Theorem 2.6.3 requires more lemmas than does theirs. It is not intended to be the most concise proof of the theorem, but to be illustrative of the techniques to be used in proving 2.1. Restating 2.9:

Theorem 2.9 Characterization of Minimum Weight Polynomials

If $P \in \mathcal{P}_r(m,q)$ where $r = s(q-1) + t$, $0 < t \leq q-1$ and $|P| = d_r^m = (q-t)q^{m-s-1}$, then P is equivalent to a polynomial Q where

(207) $Q(\bar{x}) = \lambda \prod_{i=1}^{s} (1 - x_i^{q-1}) \prod_{j=1}^{t} (\lambda_j - x_{s+1}) \quad \lambda \neq 0, \lambda_i \neq \lambda_j$ if $i \neq j$.

Proof:

When $m = 1$, $s = 0$ and Lemma 2.11 applies. Proceeding by induction, assume 2.9 is true for m-1. Corollary 2.8.1 states that P has a linear factor. Without loss of generality, assume x_1 divides P. By Lemma 2.7, $\ell d(P, x_1) = q-1$ or t. If $\ell d(P, x_1) = q-1$, our induction hypothesis completes the proof. If $\ell d(P, x_1) = t < q-1$, then $P(x_1, \bar{x}') \sim \prod_{j=1}^{t} (x_1 - \lambda_j) \hat{P}(x_1, \bar{x}')$.

Order the elements of K, $\lambda_1, \ldots, \lambda_q$. Then by 2.7, $|\hat{P}_{\lambda_i}|_{m-1} = d_{s(q-1)}^{m-1} = q^{m-s-1}$ for $i > t$. By Corollary 2.15.1 we may assume $\hat{P}_{\lambda_{t+1}} = \hat{P}_{\lambda_{t+2}}$, so $\hat{P}(x_1, \bar{x}') = \hat{P}_{\lambda_{t+1}} + (x_1 - \lambda_{t+1})(x_1 - \lambda_{t+2}) \tilde{P}(x_1, \bar{x}')$ where $\deg \tilde{P} \leq s(q-1) - 2$. This gives $\hat{P}_{\lambda_i} = \hat{P}_{\lambda_{t+1}} + (\lambda_i - \lambda_{t+1})(\lambda_i - \lambda_{t+2}) \tilde{P}_{\lambda_i}(\bar{x}')$ for $i > t+2$. By Lemma 2.14, $\tilde{P}_{\lambda_i} = 0$ for $i > t+2$ so $\hat{P}_{\lambda_i} = \hat{P}_{\lambda_{t+1}}$ for $i \geq t+2$ and $P \sim \prod_{j=1}^{t} (x_j - \lambda_j) \hat{P}_{\lambda_{t+1}}$ which is the correct form by induction.

It is helpful to prove one more lemma before beginning the proof of 2.1. This lemma is the restriction of 2.1 to the case $r = s(q-1)$.

Lemma 2.16

If $P \in \mathcal{P}_r(m, q)$, $r = s(q-1)$, and $|P| > d_r^m = q^{m-s}$, then $|P| \geq q^{m-s} + (q-2)q^{m-s-1}$.

Proof:

If $m = 1$, $s = 1$, and $q^{m-s} = 1$. $|P| > 1 \Rightarrow |P| \geq 2$. Proceeding by induction on m, assume 2.16 for m-1. If

$|P| < q^{m-s} + (q-2)q^{m-s-1}$, then by Lemma 2.7, $\ell d(P,x_1) = 0$ or $\ell d(P,x_1) = q-1$. If $\ell d(P,x_1) = q-1$, then $P = (1-x_1^{q-1})\hat{P}(\bar{x}')$ where $|\hat{P}| = |P| \leq q^{m-s} + (q-2)q^{m-s-1}$ and $\hat{P} \in \mathcal{P}_{r-(q-1)}(m-1,q)$, so, by the induction hypothesis, $|\hat{P}| = q^{m-s}$.

If $\ell d(P,x_1) = 0$, order the elements of K $\lambda_1,\ldots,\lambda_{k+1},\ldots,\lambda_q$, so that $|P_{\lambda_i}| = q^{m-s-1}$ for $i \leq k$ and $|P_{\lambda_i}| > q^{m-s-1}$ for $i > k$. If $k = q$, then $|P| = q^{m-s}$. If $k = 0$, then the induction completes the proof. If $k = 1$, then $|P_{\lambda_i}| \geq 2q^{m-s-1}$ by Lemma 2.14 so $|P| \geq q^{m-s-1} + 2(q-1)q^{m-s-1} = q^{m-s} + (q-1)q^{m-s-1}$. If $k > 1$, then by 2.15.1 we may assume that $P_{\lambda_1} = P_{\lambda_2}$ so that for $i > 2$

$$P_{\lambda_i}(\bar{x}') = P_{\lambda_1}(\bar{x}') + (\lambda_i-\lambda_1)(\lambda_i-\lambda_2)\tilde{P}_{\lambda_i}(\bar{x}')$$

where $$\deg \tilde{P} \leq r-2 .$$

If $|P_{\lambda_i}| = q^{m-s-1}$, by Lemma 2.14, $\tilde{P}_{\lambda_i} = 0$ so, in fact, $P_{\lambda_i} = P_{\lambda_1}$ and for $i > k$,

$$P_{\lambda_i}(\bar{x}') = P_{\lambda_1}(\bar{x}') + \prod_{j=1}^{k} (\lambda_i-\lambda_j)\hat{P}_{\lambda_i}(\bar{x}')$$

where $$\deg \hat{P} \leq r-k .$$

By Lemma 2.14, for $i > k$, $|P_{\lambda_i}| \geq kq^{m-s-1}$ so $|P| \geq kq^{m-s-1} + (q-k)kq^{m-s-1} = k(q-k+1)q^{m-s-1}$. But since $2 \leq k \leq q-1$, $|P| \geq 2(q-1)q^{m-s-1} = q^{m-s} + (q-2)q^{m-s-1}$. This completes the proof of 2.16.

The proof of Theorem 2.1 splits into a number of cases. The basic techniques used are the same as in the proof of 2.16. We begin by restating the theorem.

Theorem 2.1

Let $r = s(q-1)+t$ where $0 < t \leqslant q-1$, let $d_r^m = (q-t)q^{m-s-1}$, and let

$$c = \begin{cases} q-1 & \text{if } t = 1 \\ q-2 & \text{if } t = q-1 \neq 1 \\ \min(q-t, t-1) & \text{otherwise} \end{cases} .$$

If $P \in \mathcal{P}_r(m,q)$ such that $|P| > d_r^m$, then $|P| \geqslant d_r^m + cq^{m-s-2}$.

Proof:

Corollary 2.8.1 and Lemma 2.12 establish this result for $s = 0$. Lemma 2.16 proves the case $t = q-1$ if $q > 2$. If P has no linear factors, then Corollary 2.8.1 states that $|P| \geqslant d_r^m + (q-t)q^{m-s-2}$, which satisfies the theorem except when $t = q-1$ and $q > 2$ which is covered above.

To be a contradiction to the theorem, therefore, P must have a linear factor. Without loss of generality, assume x_1 divides P. If $\ell d(P, x_1) = q-1$, then $P \sim (1 - x_1^{q-1})\hat{P}$ and induction proves $|P| \geqslant d_r^m + cq^{m-s-2}$. This completes the proof when $q = 2$.

By Lemma 2.7, the only case left is when $\ell d(P, x_1) = t < q-1$. When this is true, $P = \prod_{j=1}^{t}(x_1 - \lambda_j)\hat{P}$ where $\dim \hat{P} \leqslant s(q-1)$.

Order the elements of K, $\lambda_1, \ldots, \lambda_q$, so that

$|P_{\lambda_i}| = |\hat{P}_{\lambda_i}|_{m-1} = d_{r-t}^{m-1}$ for $i = t+1, \ldots, t+k$ and $|P_{\lambda_i}| = |\hat{P}_{\lambda_i}| > d_{r-t}^{m-1}$ for $i > t+k$.

$$|P| = \sum_{i=t+1}^{q} |\hat{P}_{\lambda_i}|$$

by (201), so if $k = q-t$, then $|P| = (q-t)q^{m-s-1} = d_r^m$. If $k = 0$, then, by Lemma 2.16, $|\hat{P}_{\lambda_i}| \geqslant q^{m-s-1} + (q-2)q^{m-s-2}$

$$\begin{aligned} |P| &\geqslant (q-t)(q^{m-s-1} + (q-2)q^{m-s-2}) = d_r^m + (q-t)(q-2)q^{m-s-2} \\ &\geqslant d_r^m + cq^{m-s-2} \end{aligned}$$

when $q > 2$. If $k = 1$, then, by Lemma 2.14, $|\hat{P}_{\lambda_i}| \geqslant 2q^{m-s-1}$ for $i > t+1$ so

$$\begin{aligned} |P| &\geqslant q^{m-s-1} + (q-t-1)2q^{m-s-1} = d_r^m + (q-1-t)q^{m-s-1} \\ &\geqslant d_r^m + cq^{m-s-2} \end{aligned}$$

since $t < q-1$.

If $k \geqslant 2$, then, by Corollary 2.15.1, we may assume that $\hat{P}_{\lambda_{t+1}} = \hat{P}_{\lambda_{t+2}}$. If $|\hat{P}_{\lambda_i}| = q^{m-s-1}$ for $i > t+2$, write $\hat{P}_{\lambda_i} = \hat{P}_{\lambda_{t+1}} + (\lambda_i - \lambda_{t+1})(\lambda_i - \lambda_{t+2})\tilde{P}$ where $\deg \tilde{P} \leqslant s(q-1) - 2$ which by Lemma 2.14 implies $\tilde{P} = 0$. So $\hat{P}_{\lambda_i} = \hat{P}_{\lambda_{t+1}}$ for $i = t+1, \ldots, t+k$. For $i > t+k$, $\hat{P}_{\lambda_i} = \hat{P}_{\lambda_{t+1}} + \prod_{j=1}^{k} (\lambda_i - \lambda_{t+j})R$ where $\deg R \leqslant s(q-1) - k$, so by Lemma 2.14, $|\hat{P}_{\lambda_i}| \geqslant kq^{m-s-1}$ for $i > t+k$. Thus,

$$\begin{aligned} |P| &\geqslant kq^{m-s-1} + (q-t-k)kq^{m-s-1} = d_r^m + (k-1)(q-t-k)q^{m-s-1} \\ &\geqslant d_r^m + cq^{m-s-1} \end{aligned}$$

since $1 < k < q-t$. This completes the proof of Theorem 2.1.

The full power of this approach is not realized in Theorem 2.1. Chapter three attempts to discover when the bound given by 2.1 is the best possible, and to characterize next-to-minimum weight polynomials.

CHAPTER 3

This chapter deals with two questions which arise from the techniques and results of chapter two: When is the bound given in Theorem 2.1 the best possible; that is, when is it the next-to-minimum weight? What is the characterization of next-to-minimum weight polynomials?

Throughout this chapter, assume $P \in \mathcal{P}_r(m,q)$, where $r = s(q - 1) + t$, $0 < t \leqslant (q - 1)$ unless stated otherwise. Theorem 2.1 states that the next-to-minimum weight for $\mathcal{P}_r(m,q)$ is at least $d_r^m + c\, q^{m-s-2}$, where $d_r^m = (q-t)q^{m-s-1}$ is the minimum weight, and

$$c = \begin{cases} q - 1 \text{ if } t = 1 \\ q - 2 \text{ if } t = q - 1 \neq 1 \\ \min(t - 1,\ q - t) \text{ otherwise.} \end{cases}$$

The results of this chapter on the next-to-minimum weight are expressed in Theorem 3.1.

Theorem 3.1

The next-to-minimum weight of $\mathcal{P}_r(m,q)$ is $d_r^m + cq^{m-s-2}$, where $d_r^m = (q - t)\, q^{m-s-1}$ is the minimum weight, and

$$c = \begin{cases} q & \text{if } s = m - 1 \text{ (Lemma 3.2)} \\ t-1 & \text{if } s < m - 1 \text{ and } 1 < t \leqslant (q+1)/2 \text{ (Lemma 3.3)} \\ & \text{or } s < m - 1 \text{ and } t = q - 1 \neq 1 \\ q & \text{if } s = 0,\ t = 1 \text{ (trivial)} \\ \left.\begin{array}{ll} (q-1) & \text{if } q < 4,\ s < m - 2,\ t = 1 \\ (q-1) & \text{if } q = 3,\ s = m - 2,\ t = 1 \\ q & \text{if } q = 2,\ s = m - 2,\ t = 1 \end{array}\right\} & \text{(Lemma 3.4)} \\ q & \text{if } q \geqslant 4,\ 0 < s \leqslant m - 2,\ t = 1 \text{ (Theorem 3.8)} \\ c_t & \text{if } q \geqslant 4,\ s \leqslant m - 2,\ (q+1)/2 < t < q - 1 \text{ (Theorem 3.11)} \end{cases}$$

where c_t is defined to be the integer such that $d_t^2 + c_t$ is the next-to-minimum weight of $\mathcal{P}_t(2, q)$.

Proof:

Each of the possible cases is proved in the result given in parentheses. The case $s = 0,\ t = 1$ is trivial, merely stating that the next-to-minimum weight for linear polynomials is q^m.

Lemma 3.2

If $r = (m - 1)(q - 1) + t,\ 0 < t \leqslant q - 1$, the next-to-minimum weight of $\mathcal{P}_r(m, q)$ is $q - t + 1 = d_r^m + 1$.

Proof:

The next-to-minimum weight is at least $d_r^m + 1$, and the polynomial

$$Q(\overline{x}) = \prod_{i=1}^{m-1} (1 - x_i^{s-1}) \prod_{j=1}^{t-1} (x_m - \lambda_j) \text{ where } \lambda_j = \lambda_i \Rightarrow i = j$$

has weight $d^m_{r-1} = d^m_r + 1$.

Lemma 3.3

If $s \leq m - 2$ and either $1 < t \leq (q + 1)/2$ or $t = q - 1 \neq 1$, with $r = s(q - 1) + t$, then the next-to-minimum weight of $\mathcal{P}_r(m, q)$ is $d^m_r + (t - 1)q^{m-s-2}$.

Proof:

That the next-to-minimum weight is at least this value follows from Theorem 2.1. Formulas (208) and (209) give polynomials which have weight $d^m_r + (t - 1)q^{m-s-2}$ exactly.

$$Q(x) = \lambda\, x_{s+2} \prod_{i=1}^{s} (1 - x_i^{q-1}) \prod_{j=1}^{t-1} (\lambda_j - x_{s+1}),\ \lambda_i = \lambda_j \Rightarrow i = j$$

$$Q(x) = \lambda \prod_{i=1}^{s} (1 - x_i^{q-1}) \prod_{j=1}^{t} L_j(x_{s+1}, x_{s+2}), \text{ where}$$

$$L_j(x_{s+1}, x_{s+2}) = \alpha_j x_{s+1} + \beta_j\, x_{s+2} \text{ and } \alpha_i\beta_j = \alpha_j\beta_i \Rightarrow i = j.$$

The case $t = 1$, $1 \leq s \leq m - 2$ runs into some complexities. Theorem 2.1 states that the next-to-minimum weight in this case is at least $(q - 1)q^{m-s-1} + (q - 1)\, q^{m-s-2}$. In most cases, however, this is not the best possible lower bound, as will be shown later.

When $q = 2$, $1 \leq s \leq m - 3$, and $t = 1$, Kasami and Tokura [7] have found a polynomial, $x_1 x_2 \cdots x_{s-1}(x_s x_{s+1} + x_{s+2} x_{s+3})$, which has weight $2^{m-s-3}(6) = 2^{m-s-1} + 2^{m-s-2}$, showing that the bound from 2.1 is best possible. If $q = 2$, $s = m - 2$, $t = 1$, however, all polynomials must have even weight. This fact follows from the Ax divisibility condition. It can also be proved by observing that $r = (m - 2) + 1 = m - 1 < m(q - 1)$, so that, by Lemma 1.7,

$$\sum_{\sigma \in K^m} P(\overline{\sigma}) = 0,$$

which implies that $|P|$ is even, since $P(\overline{\sigma}) \in GF(2)$. Thus, the next-to-minimum weight cannot be 3, which is the bound given by 2.1. There is a polynomial, $x_1 x_2 \cdots x_{m-2}$, which has degree $m - 2$ and weight 4, so we can conclude that the next-to-minimum weight of $\mathcal{P}_{m-1}(m, 2)$ is 4.

When $q = 3$, $t = 1$, and $1 \leq s \leq m - 2$, Theorem 2.1 gives the lower bound $2.3^{m-s-1} + 2.3^{m-s-2}$ for the next-to-minimum weight. The polynomial

$$x_s x_{s+1} x_{s+2} \prod_{i=1}^{s-1} (1 - x_i^2)$$

has precisely this weight, so 2.1 does give the best bound in this case.

The preceeding discussion proves:

Lemma 3.4

The next-to-minimum weight of $\mathscr{P}_r(m,q)$ is:

$$\text{when } q = 2, \begin{cases} 2^m & \text{if } r = 1 \\ 2^{m-r} + 2^{m-r-1} & \text{if } 2 \leqslant r \leqslant m - 2 \\ 4 & \text{if } r = m - 1 \\ 2 & \text{if } r = m \end{cases}$$

$$\text{when } q = 3, \begin{cases} 3^m & \text{if } r = 1 \\ 3^{m-s-1} + 3^{m-s-2} & \text{if } r = 2s + 2 \quad 0 \leqslant s \leqslant m - 2 \\ 2 \cdot 3^{m-s-1} + 2 \cdot 3^{m-s-2} & \text{if } r = 2s + 1 \quad 1 \leqslant s \leqslant m - 2 \\ 3 & \text{if } r = 2m - 1 \\ 2 & \text{if } r = 2m \end{cases}$$

In the case $t = 1$, $1 \leqslant s \leqslant m - 2$, when $q \geqslant 4$, the situation is not as simple. From the proof of Theorem 2.1 it is evident that if $d_r^m < |P| < d_r^m + q^{m-s-1}$, then either P has no linear factors, or $P \sim (1 - x_1^{q-1})\,\hat{P}$, where $\deg \hat{P} = (s - 1)(q - 1) + 1$ and $|\hat{P}| = |P|$. Thus, to complete this case, a better understanding of polynomials without linear factors is needed.

Similarly, if $q \geqslant 4$, $s \leqslant m - 2$, and $1 < t < q - 1$, the proof of 2.1 reveals: $d_r^m < |P| < d_r^m + (t - 1)q^{m-s-2}$ implies that either P has no linear factors or $P \sim (1 - x_1^{q-1})\,\hat{P}$. Again, better bounds on the weight of polynomials without linear factors would be helpful.

In lemmas 2.14, 2.15, and 2.16 such bounds were developed for the case $t = q - 1$. Similar techniques will now be used to provide lemmas in the more general case.

Lemma 3.5

Let $Q \in \mathscr{P}_r(m, q)$, $r = s(q - 1) + t$, $0 < t < q - 1$, such that $Q = (1 - x_1^{q-1})\, Q_0(\overline{x}')$. And let $R \in \mathscr{P}_{r-k}(m, q)$, $0 < k \leqslant q - 1$, such that $(1 - x_1^{q-1})$ does not divide R. If $P = Q + R$, then either $|P|_m \geqslant (q - t + k)q^{m-s-1}$, or $k = 1$ and there exists a $\lambda \in K$ such that $(1 - (x_1 - \lambda)^{q-1})$ divides P.

Proof:

Separate the variable x_1, defining $R_\lambda(\overline{x}') = R(\lambda, \overline{x}')$ and $P_\lambda(\overline{x}') = P(\lambda, \overline{x}')$. By formula (201),

$$|P|_m = \sum_{\lambda \in K} |P_\lambda|_{m-1} = |Q_0 + R_0|_{m-1} + \sum_{\lambda \neq 0} |R_\lambda|_{m-1}.$$

Order the elements of K, $\lambda_1, \lambda_2 \cdots, \lambda_q$, so that $\lambda_{n+1} = 0$, $|R_{\lambda_i}| = 0$ for $i \leqslant n$, and $|R_{\lambda_i}| > 0$ for $i > n + 1$. By the hypothesis$(1 - x_1^{q-1}) \nmid R$, we know that $n < q - 1$. By Lemma 2.2,

$$R(x_1, \overline{x}') = \lambda(x_1 - \lambda_1)(x_1 - \lambda_2) \cdots (x_1 - \lambda_n)[R_0(\overline{x}') + x_1 \hat{R}(x_1, \overline{x}')],$$

where $\deg R_0 \leqslant r - (k + n)$ and $\deg \hat{R} \leqslant r - (k + n) - 1$.

If $P_0 \neq 0$, then deg P_0 = deg $(Q_0 + R_0) \leqslant \max\,(r - (q-1),\ r - (k+n))$, and deg $R_{\lambda_i} \leqslant r - (k+n)$ for $i > n+1$, so $|P| \geqslant (q-n-1)d^{m-1}_{r-(k+n)} + d^{m-1}_{r-b}$, where $b = \min((q-1),(k+n))$.

$$(k+n) > (q-1) \text{ implies } |P| \geqslant (q-n-1)d^{m-1}_{r-(k+n)} + d^{m-1}_{r-(q-1)}.$$

$$= \begin{cases} (q-n-1)((k+n) - (q+t-2))\, q^{m-s} + (q-t)\, q^{m-s-1} & \text{if } (k+n) \geqslant q+t-1 \\ (q-n-1)((k+n) - (t-1))q^{m-s-1} + (q-t)\, q^{m-s-1} & \text{if } (k+n) < q+t-1 \end{cases}$$

$$> \begin{cases} k\, q^{m-s} + (q-t)\, q^{m-s-1} & \text{if } (k+n) \geqslant q+t-1 \\ k\, q^{m-s-1} + (q-t)\, q^{m-s-1} & \text{if } (k+n) < q+t-1 \end{cases}$$

$$> (q-t+k)\, q^{m-s-1}.$$

$$(k+n) \leqslant (q-1) \text{ implies } |P| \geqslant (q-n)\, d_r - (k+n)$$

$$= (q-n) \begin{cases} (q-t+(k+n))q^{m-s-2} & \text{if } (k+n) < t \\ (1-t+(k+n))q^{m-s-1} & \text{if } (k+n) \geqslant t \end{cases}$$

$$= \begin{cases} (q-t+k)q^{m-s-1} + n(t-(n+k))q^{m-s-2} & \text{if } (k+n) < t \\ (q-t+k)q^{m-s-1} + (n+k-t)(q-1-n)q^{m-s-1} & \text{if } (k+n) \geqslant t \end{cases}$$

$$\geqslant (q-t+k)q^{m-s-1},$$

with equality only when $n + k = t$ and P_λ are all minimum weight or zero.

If $P_0 = 0$, then $R_0 = - Q_0$, so $\deg R_0 = \deg Q_0 = r - (q - 1)$. This implies $r - (k + n) \geqslant r - (q - 1)$, so $(k + n) \leqslant (q - 1)$. $(k + n) < q - 1$ implies $\deg R_{\lambda i} \leqslant r - (k + n) - 1$ for $i > n + 1$, so $|P| \geqslant (q - n - 1)\, d^{m-1}_{r-(k+n)-1}$

$$= (q - n - 1)\begin{cases}(q - t + k + n + 1)q^{m-s-2} & \text{if } (k + n) < t - 1\\ (1 - t + k + n + 1)q^{m-s-1} & \text{if } (k + n) \geqslant t - 1\end{cases}$$

$$= \begin{cases}(q - t + k)q^{m-s-1} + (n + 1)(t - 1 - (n + k))q^{m-s-2} & \text{if } (k + n) < t - 1\\ (q - t + k)q^{m-s-1} + (n+k-(t - 1))(q - 2 - n)q^{m-s-1} & \text{if } (k + n) \geqslant t - 1\end{cases}$$

$$\geqslant (q - t + k)q^{m-s-1},$$

with equality only when $n + k = t - 1$ and P_λ is minimum weight or zero for each λ. (Note: $n = q - 2$ implies $n + k \geqslant q - 1$).

$(k + n) = q - 1$ implies $|P| \geqslant (q - n - 1)\, d^{m-1}_{r-(q-1)} = k(q - t)q^{m-s-1}$

$$= (q - t + k - 1)q^{m-s-1} + (k - 1)(q - t - 1)q^{m-s-1}$$

$$\geqslant (q - t + k)q^{m-s-1} \text{ unless } k = 1, \text{ since } t < q - 1.$$

If $k = 1$, then $n = q - 2$, and this is the special case which the lemma allows.

Lemma 3.6

Let $P \in \mathcal{P}_r(m,q)$, $r = s(q-1)+t, 0<t<q-1$. If, for some $\lambda_1, \lambda_2 \in K$, $P_{\lambda_1} \neq 0$ and $(1 - x_2^{q-1}) | P_{\lambda_1}$, and $0 < |P_{\lambda_2}| < (q-t+1)q^{m-s-2}$, then there is an invertible affine transformation T, fixing x_i for $i \neq 2$, such that if $R(\overline{x}) = P(T(\overline{x}))$, then $(1 - x_2^{q-1}) | R_{\lambda_1}$ and $(1 - x_2^{q-1}) | R_{\lambda_2}$.

Proof:

$$P(\overline{x}) = P_{\lambda_1}(\overline{x}) + (x_1 - \lambda_1)\,\hat{P}(\overline{x}), \text{ where } \deg \hat{P} \leq r-1, \text{ so}$$

$$P_{\lambda_2}(\overline{x}') = P_{\lambda_1}(\overline{x}') + (\lambda_2 - \lambda_1)\,\hat{P}_{\lambda_2}(\overline{x}'), \ \deg \hat{P}_{\lambda_2} \leq r-1.$$

Lemma 3.5 asserts the existence of a λ such that $(1 - (x_2 - \lambda)^{q-1}) | P_{\lambda_2}$. Define $T(\overline{x})$ as follows:

$$[T(\overline{x})]_i = x_i \text{ for } i \neq 2, \ [T(\overline{x})]_2 = x_2 + \lambda \frac{(x_1 - \lambda_1)}{\lambda_2 - \lambda_1} .$$

Let $R(\overline{x}) = P(T(\overline{x}))$, then $R_{\lambda_1}(\overline{x}) = P_{\lambda_1}(\overline{x})$ and $R_{\lambda_2}(\overline{x}') = 0$ unless $x_2 = 0$, so, by Lemma 2.3, $(1 - x_2^{q-1}) | R_{\lambda_2}$, and the lemma is proved.

Lemma 3.7

Let $P \in \mathcal{P}_r(m,q)$ where $r = s(q-1)+t$, with $1 \leq s \leq m-2$, and $0 < t < q-1$. Let the elements of K, $\lambda_1, \cdots, \lambda_q$, be ordered so that $|P_{\lambda_1}| \leq \cdots \leq |P_{\lambda_q}|$.

If P has no linear factors, and P can be transformed $R(\overline{x}) = P(T(\overline{x}))$ by an invertible affine transformation T, fixing x_1, so that $(1 - x_2^{q-1}) | R_{\lambda_i}$ for $i = 1, \cdots, k$ but $(1 - x_2^{q-1}) \nmid R_{\lambda_{k+1}}$, then $|P| \geq d_r^m + k(q - k)q^{m-s-2}$.

Proof:

$|R| = |P|$, and since T fixes x_1, $|R_\lambda| = |P_\lambda|$ for $\lambda \in K$. R has no linear factors, so $k < q$. There is nothing to prove if $k = 0$, so assume $k > 0$. Then $(1 - x_2^{q-1}) | R_{\lambda_1}$. If $|R_{\lambda_{k+1}}| \geq (q - t + k)q^{m-s-2}$, then by (201),

$$|R| = \sum_{i=1}^{q} |R_{\lambda_i}| = \sum_{i=1}^{k} |R_{\lambda_i}| + \sum_{i=k+1}^{q} |R_{\lambda_i}|$$

$$\geq k(q - t)q^{m-s-2} + (q - k)(q - t + k)q^{m-s-2}$$

$$= d_r^m + (q - k)kq^{m-s-2}, \text{ and we are done.}$$

If $|R_{\lambda_{k+1}}| < (q - t + k)q^{m-s-2}$, write

$$R(x_1, x_2, \overline{x}'') = (1 - x_2^{q-1})\, \tilde{R}(x_1, \overline{x}'') + (x_1 - \lambda_1) \cdots (x_1 - \lambda_k)\, \hat{R}(x_1, x_2, \overline{x}''),$$

where $\deg \hat{R} \leq r - k$. Then

$$R_{\lambda_{k+1}}(x_2, \overline{x}'') = (1 - x_2^{q-1})\, \tilde{R}_{\lambda_{k+1}}(\overline{x}'') + (\lambda_{k+1} - \lambda_1) \cdots (\lambda_{k+1} - \lambda_n) \hat{R}_{\lambda_{k+1}}(x_2, \overline{x}'').$$

This is the situation of Lemma 3.5. If $(1 - x_2^{q-1}) \nmid R_{\lambda_{k+1}}$ and $|R_{k+1}| < (q - t + k)q^{m-s-2}$, then $k = 1$. But now, applying Lemma 3.6, there is a transformation T', fixing x_1, such that if $S(\bar{x}) = R(T'(\bar{x}))$, then $(1 - x_2^{q-1}) | S_{\lambda_1}$ and $(1 - x_2^{q-1}) | S_{\lambda_2}$. If $(1 - x_2^{q-1}) | S_{\lambda_i}$ for $i \leqslant k'$, but $(1 - x_2^{q-1}) \nmid S_{\lambda_{k'+1}}$, then since $2 \leqslant k' \leqslant q - 1$, $|S| \geqslant d_r^m + (q - 1)q^{m-s-2}$, which completes the proof.

Theorem 3.8

The next-to-minimum weight of $\mathscr{P}_r(m, q)$, where $r = s(q - 1) + 1$, $0 \leqslant s < m$, and $q \geqslant 4$, is q^{m-s}.

Proof:

The theorem is trivially true when $m = 1$, or $s = 0$ or $m - 1$. Assume now that $m \geqslant 2$ and $1 \leqslant s \leqslant m - 2$, and that 3.8 holds for smaller m and smaller s with the same m. The theorem will be proved for this m and s by contradiction. Assume $d_r^m < |P| < q^{m-s}$. Then as observed in the proof of Theorem 2.1, P has no linear factors. Order the elements of K, $\lambda_1, \cdots, \lambda_q$, so that $|P_{\lambda_1}| \leqslant \cdots \leqslant |P_{\lambda q}|$. Then

$$|P| = \sum_{i=1}^{q} |P_{\lambda i}| \leqslant q|P_{\lambda_1}|, \text{ so } |P_{\lambda_1}| < q^{m-s-1}.$$

This implies, by our induction hypothesis, that $|P_{\lambda_1}| = d_r^{m-1}$.

By Theorem 2.9, it may be assumed, without loss of generality, that $(1 - x_2^{q-1}) | P_{\lambda_1}$. Assume that $(1 - x_2^{q-1}) | P_{\lambda_i}$ for $i \leqslant k$, but

$(1 - x_2^{q-1}) \not| \, P_{\lambda_{k+1}}$. Then, by Lemma 3.7,

$$|P| \geqslant d_r^m + k(q - k)q^{m-s-2} = q^{m-s} - q^{m-s-1} + k(q - k)q^{m-s-2}.$$

Thus, $k = 1$, $q - 1$, or q.

If $k = q$, then P has a linear factor; a contradiction.

If $k = q - 1$, then

$$P(x_1, x_2, \overline{x}'') = (1 - x_2^{q-1})\, \tilde{P}(\overline{x}'') + (1 - (x_1 - \lambda_q)^{q-1})\, \hat{P}(x_2, \overline{x}''),$$

where $\deg \tilde{P} \leqslant r - (q - 1)$ and $\deg \hat{P} \leqslant r - (q - 1)$. Thus,

$$P_{\lambda_q}(\overline{x}') = (1 - x_2^{q-1})\, \tilde{P}(\overline{x}'') + \hat{P}(x_2, \overline{x}''). \text{ By (201),}$$

$$|P_{\lambda_q}|_{m-1} = \sum_{\sigma \in K} |P_{\lambda_q, \sigma}|_{m-2} = |P_{\lambda_q, 0}| + \sum_{\sigma \neq 0} |\hat{P}_\sigma| \geqslant (q-1) d_{r-(q-1)}^{m-2}$$

$$= (q - 1)\, d_r^{m-1}.$$

So $|P| = \sum_{i=1}^{q} |P_{\lambda_i}| \geqslant (q - 1)\, d_r^{m-1} + (q - 1)\, d_r^{m-1} = q^{m-s} +$

$$(q^2 - 4q + 2)q^{m-s-2} > q^{m-s}, \quad \text{when } q \geqslant 4 \quad .$$

Assume that $k = 1$.

If $|P_{\lambda_2}| < q^{m-s-1}$, then, by Lemma 3.6, there is an invertible affine transformation T, fixing x_1, such that if $R(\overline{x}) = P(T(\overline{x}))$, then $(1 - x_2^{q-1}) | R_{\lambda_1}$ and $(1 - x_2^{q-1}) | R_{\lambda_2}$. Since $|P| = |R|$, the above reasoning may be applied by R to complete the proof.

Similarly, if $(1 - (x_2 - \sigma)^{q-1}) | P_{\lambda_2}$, there is such a transformation, and $|P| \geqslant q^{m-s}$. Thus, $P_{\lambda_2, \sigma} \neq 0$, for at least two distinct $\sigma \in K$.

Let $R_\sigma(\bar{x}'') = P_{\lambda_2, \sigma}(\bar{x}'') = P_{\lambda_2}(\sigma, \bar{x}'') = P(\lambda_2, \sigma, \bar{x}'')$. Order the elements of K, $\sigma_1, \sigma_2, \cdots, \sigma_q$, so that $|R_{\sigma_1}| \leqslant \cdots \leqslant |R_{\sigma_q}|$. Suppose that $R_{\sigma_i} = 0$ for $i \leqslant n$, and $R_{\sigma_{n+1}} \neq 0$. By the above paragraph, $n < q - 1$.

Since $(1 - x_2^{q-1}) | P_{\lambda_1}$, write

$$(1) \quad P(x_1, x_2, \bar{x}'') = (1 - x_2^{q-1}) P_{\lambda_1, 0}(\bar{x}'') + (x_1 - \lambda_1) \hat{P}(x_1, x_2, \bar{x}''),$$

where $\deg \hat{P} \leqslant r - 1 = s(q - 1)$. Then

$$(2) \qquad R_\sigma(\bar{x}'') = (1 - \sigma^{q-1}) P_{\lambda_1, 0}(\bar{x}'') + (\lambda_2 - \lambda_1) \hat{P}(\lambda_2, \sigma, \bar{x}''),$$

so $\deg R_\sigma \leqslant \max(r - (q - 1), \deg \hat{P}(\lambda_2, \sigma, \bar{x}''))$. But $\deg \hat{P}(\lambda_2, \sigma, \bar{x}'') \leqslant (r - 1) - n$, by Lemma 2.7, so $\deg R_\sigma \leqslant r - 1 - n$, and $|R_{\sigma_i}| \geqslant (1 + n)q^{m-s-2}$ for $i > n$. Thus,

$$(3) \quad |P_{\lambda_2}| \geqslant (q - n)(1 + n)q^{m-s-2} = q^{m-s-1} + n(q - 1 - n)q^{m-s-2}.$$

But $|P| \geqslant |P_{\lambda_1}| + (q - 1)|P_{\lambda_2}|$, and, by assumption,

$$|P| < q^{m-s}, \text{ so}$$

$$(4) \quad |P_{\lambda_2}| < (q^{m-s} - (q - 1)q^{m-s-2})/(q - 1) < q^{m-s-1} + q^{m-s-2}.$$

This contradicts (3) unless $n = 0$. When $n = 0$, (4) implies $|R_{\sigma_1}| < q^{m-s-2} + q^{m-s-3}$, which, together with Lemma 2.16, forces $|R_{\sigma_1}| = d^{m-1}_{r-1} = q^{m-s-2}$. Suppose for $i \leq k'$, $|R_{\sigma_i}| = q^{m-s-2}$, and for $i > k'$, $|R_{\sigma_i}| > q^{m-s-2}$. Then, by 2.16, for $i > k'$, $|R_{\sigma_i}| \geq q^{m-s-2} + (q-2)q^{m-s-3}$. By (201),

$$|P_{\lambda_2}| \geq k' q^{m-s-2} + (q-k')[(q-2)q^{m-s-3} + q^{m-s-2}]$$

$$= q^{m-s-1} + (q-k')(q-2)q^{m-s-3}.$$

Together with (4) above, this forces $k' = q - 1$ or q. By arguments similar to those used in the proof of Lemma 2.16, there exists an i.a.t. $T'(\overline{x}')$, fixing x_2 such that if $R'(\overline{x}') = P_{\lambda_2}(T'(\overline{x}'))$, then $R'_{\sigma_i} = R'_{\sigma_1}$ for $i \leq k'$, where R'_{σ_1}, is a minimum weight polynomial. By making the transformation $T(\overline{x})$, defined by $[T(\overline{x})]_i = x_i$ for $i \neq 2$, $[T(\overline{x})]_2 = x_2 - \sigma \frac{x_1 - \lambda_1}{\lambda_2 - \lambda_1}$, it may be assumed that $\sigma_q = 0$. Now $R_\sigma = R_1$ for $\sigma \neq 0$, where $|R_1| = q^{m-s-2}$ and $\deg R_1 = r - 1 = s(q-1)$. From (1),

$$P(x_1, x_2, \overline{x}'') = (1 - x_2^{q-1})\, P_{\lambda_1, 0}(\overline{x}'') + (x_1 - \lambda_1)\, \hat{P}(x_1, x_2, \overline{x}''),$$

so

(5) $P_{\lambda_2}(x_2, \overline{x}'') = (1 - x_2^{q-1})\, P_{\lambda_1, 0}(\overline{x}'') + (\lambda_2 - \lambda_1)\, \hat{P}_{\lambda_2}(x_2, \overline{x}'')$, where

$$\deg P_{\lambda_1, 0} = r - (q-1) \text{ and } \deg \hat{P}_{\lambda_2} \leq r - 1.$$

Since $R_\sigma = R_1$ when $\sigma \neq 0$,

(6) $$P_{\lambda_2}(x_2, \bar{x}'') = R_1(\bar{x}'') + (1 - x_2^{q-1})\,\hat{R}(\bar{x}''), \text{ where}$$

$$\deg R_1 = r - 1 \text{ and } \deg \hat{R} \leqslant r - (q - 1).$$

Combining (5) and (6),

(7) $$(\lambda_2 - \lambda_1)\,\hat{P}(x_2, \bar{x}'') = R_1(\bar{x}'') + (1 - x_2^{q-1})[-P_{\lambda_1, 0}(\bar{x}'') + \hat{R}(\bar{x}'')].$$

If $\hat{R} = 0$, then deg $P_{\lambda_2} = r$. Since this is not true, $\hat{R} \neq 0$. Letting $x_2 = 0$ in (6), $R_0(x'') = R_1(\bar{x}'') + \hat{R}(\bar{x}'')$. By Lemma 2.14, $|R_0| \geqslant (q-2)q^{m-s-2}$, so $|P_{\lambda_2}| \geqslant q^{m-s-1} + (q - 3)q^{m-s-2}$, contradicting (4). This final contradiction completes the proof.

A similar proof could be given to establish the next-to-minimum weight in the case $r = s(q - 1) + t$, where $s \leqslant m - 2$ and $(q + 1)/2 < t < q - 1$, except that no starting point for the induction has been established. Such a point may be assumed as follows:

Define c_t for a fixed q and t, $0 < t \leqslant q - 1$, to be the difference between the next-to-minimum weight and the minimum weight of $\mathcal{P}_t(2, q)$. The minimum weight is $d_t^2 = (q - t)q$. The next-to-minimum weight, is, by this definition, $(q - t)q + c_t$. It has already been established that $c_1 = q$, and that $c_t = t - 1$ for $1 < t \leqslant (q + 1)/2$, by Lemma 3.3. For $t = q - 1$, $c_t = q - 2$, by Lemma 3.3. From Theorem 2.1, when $(q + 1)/2 < t < q - 1$, then $c_t \geqslant q - t$, and from the weights of polynomials (208) and (209), when $(q - 1)/2 < t < q - 1$, then $c_t \leqslant t - 1$.

The next lemma is analogous to Lemma 3.5 except that it deals with the case $s = 0$, which 3.5 does not cover.

Lemma 3.9

Let $P = Q + R$, where $Q \in \mathcal{P}_t(m, q)$, $0 < t \leqslant q - 1$; and $R \in \mathcal{P}_{t-k}(m, q)$, $0 < k \leqslant t$. If Q depends only on x_1, then either P depends only on x_1, or $|P| \geqslant d_t^m + k\, q^{m-1} = (q - t + k)q^{m-1}$.

Proof:

$$P = Q + R.$$

Order the elements of K, $\lambda_1, \cdots, \lambda_q$, so that $|P_{\lambda_1}| \leqslant \cdots \leqslant |P_{\lambda_q}|$. From the definition (202) of $P^{(i)}$, $P^{(i)} = Q^{(i)} + R^{(i)}$, $P^{(i)}_{\lambda_{i+1}} = Q^{(i)}_{\lambda_{i+1}} + R^{(i)}_{\lambda_{i+1}}$. In (206),

$$P_{\lambda_i} = \sum_{j=0}^{i-1} [Q^{(j)}_{\lambda_{j+1}} + R^{(j)}_{\lambda_{j+1}}] \prod_{k=1}^{j} (\lambda_i - \lambda_k), \text{ where}$$

$\deg R^{(j)}_{\lambda_{j+1}} \leqslant t - k - j$ and $Q^{(j)}_{\lambda_{j+1}}$ is a constant. Suppose $P_{\lambda_i} = 0$ if and only if $i \leqslant n$, then $P^{(i)}_{\lambda_{i+1}} = 0$ for $i < n$. This implies that

$$P_{\lambda_i} = \sum_{j=n}^{i-1} [Q^{(j)}_{\lambda_{j+1}} + R^{(j)}_{\lambda_{j+1}}] \prod_{k=1}^{j} (\lambda_i - \lambda_k), \text{ so}$$

deg $P_{\lambda_i} \leqslant \max(t - k - n, 0)$. If $n \geqslant t - k$, then $R^{(j)}_{\lambda_{j+1}}$ is a constant for $j \geqslant n$, so P_{λ_i} is a constant for each i. Thus P depends only on x_1.

If $n < t - k$, then deg $P_{\lambda_i} \leqslant t - k - n$, so

$$|P_{\lambda_{n+1}}| \geqslant d^{m-1}_{t-k-n} = (q + k + n - t)q^{m-2} \text{ and}$$

$$|P| \geqslant (q - n)(q + k + n - t)q^{m-2} = (q - t + k)q^{m-1} + n(t - k - n)q^{m-2}$$

$$\geqslant (q - t + k)q^{m-1}, \text{ proving the lemma.}$$

The next lemma proves a starting point for the induction proof of the following theorem.

Lemma 3.10

Let $P \in \mathscr{P}_t(m,q)$, $1 < t \leqslant q - 1$. If $|P| > d^m_t$, then $|P| \geqslant d_t + c_t\, q^{m-2}$.

Proof:

True for m = 1 and m = 2, by the definition of c_t. Assume that the lemma is true for fewer than m variables $m \geqslant 3$. Let P be a polynomial in m variables, with deg $P \leqslant t$ and $|P| > d^m_t$. Order the elements of K, $\lambda_1, \cdots, \lambda_q$, so that $|P_{\lambda_1}| \leqslant \cdots \leqslant |P_{\lambda_q}|$. Assume that $P_{\lambda_i} = 0$ for $i \leqslant n$ and $P_{\lambda_i} \neq 0$ for $i > n$. By Lemma 2.7,

$$|P| \geq d_t^m + n(t-n)q^{m-2} \geq d_t^m + (t-1)q^{m-2} \geq d_t^m + c_t\, q^{m-2}$$

unless n = 0 or n = t. If n = t, however, P is minimum weight. If n = 0,

$$|P_{\lambda_1}| \geq d_t^{m-1}.$$

If $|P_{\lambda_1}| > d_t^{m-1}$, then by the induction hypothesis, $|P_{\lambda_1}| \geq d_t^{m-1} + c_t\, q^{m-3}$, so

$$|P| \geq q\, |P_{\lambda_1}| \geq d_t^m + c_t\, q^{m-2}.$$

Without loss of generality, assume that P_{λ_1} depends only on x_2. Further assume that P_{λ_i} depends only on x_2 for $i \leq k$, but $P_{\lambda_{k+1}}$ does not depend only on x_2. If k = q, then P depends only on x_1 and x_2, and the lemma is true. Otherwise, $1 \leq k \leq q-1$. Write

$$P(x_1, x_2, \bar{x}'') = \tilde{P}(x_1, x_2) + (x_1 - \lambda_1) \cdots (x_1 - \lambda_k)\, \hat{P}(x_1, x_2, \bar{x}''),$$

where $\deg \hat{P} \leq t - k$.

$$P_{\lambda_{k+1}} = \tilde{P}_{\lambda_{k+1}}(x_2) + (\lambda_{k+1} - \lambda_1) \cdots (\lambda_{k+1} - \lambda_k)\, \hat{P}_{\lambda_{k+1}}(x_2, \bar{x}'')$$

By Lemma 2.9, $|P_{\lambda_{k+1}}| \geq d_t^{m-1} + kq^{m-2}$, so

$$|P| \geqslant k\, d_t^{m-1} + (q - k)(d_t^{m-1} + kq^{m-2})$$

$$= d_t^m + (q - k)\, k\, q^{m-2} \geqslant d_t^m + (q - 1)q^{m-2} \geqslant d_t^m + c_t\, q^{m-2}$$

Thus, in every case, $|P| > d_t^m \Rightarrow |P| \geqslant d_t^m + c_t\, q^{m-2}$.

Theorem 3.11

Let $P \in \mathcal{P}_r(m,q)$, where $r = s(q - 1) + t$, $1 < t < q - 1$, and $q \geqslant 4$. If $|P| > d_r^m = (q - t)\, q^{m-s-1}$, then $|P| \geqslant d_r^m + c_t\, q^{m-s-2}$.

Proof:

Lemma 3.10 proves this theorem for $s = 0$. The definition of c_t makes the theorem true for $m \leqslant 2$. Assume $m \geqslant 3$, $s \geqslant 1$, and assume that the theorem is true for smaller m and smaller s with the same m. Prove the theorem for this m and s by contradiction. Assume

$$\text{(1)} \qquad d_r^m < |P| < d_r^m + c_t\, q^{m-s-2} \leqslant d_r^m + (t - 1)q^{m-s-2}.$$

If P has a linear factor y, then by Lemma 2.7, $\ell d(P, y) = q - 1$ or t. If $\ell d(P, y) = q - 1$, then $P = (1 - x_1^{q-1})\, \tilde{P}$, where $\tilde{P} \in \mathcal{P}_{r-(q-1)}(m - 1, q)$ so, from (1), $d_{r-(q-1)}^{m-1} = d_r^m < |P| = |\hat{P}| < d_{r-(q-1)}^{m-1} + c_t\, q^{m-s-2}$, contradicting the induction hypothesis. If $n = t$, then as in the proof of 2.1, $|P| > d_r^m \Rightarrow |P| \geqslant d_r^m + q^{m-s-1}$.

Therefore, P has no linear factors. If $|P_{\lambda_1}| > d_r^{m-1}$, then, by the induction hypothesis, $|P_{\lambda_1}| \geqslant d_r^{m-1} + c_t\, q^{m-s-3}$, so $|P| \geqslant d_r^m + c_t\, q^{m-s-2}$. Therefore, $|P_{\lambda_1}| = d_r^{m-1}$. Assume without loss of generality, that $(1 - x_2^{q-1})$

divides P_{λ_i}. Then, by Lemma 3.7, $|P| \geq d_r^m + k(q-k)q^{m-s-2}$ for $1 \leq k \leq q$, so $|P| \geq d_r^m + (q-1)q^{m-s-2} > d_r^m + c_t\, q^{m-s-2}$. This completes the proof of 3.11.

Theorem 3.11 completes the proof of Theorem 3.1.

Theorem 3.1 reduces the area where the next-to-minimum weight of $\mathcal{P}_r(m,q)$ is not known, to the case $m = 2, (q+1)/2 < r < q-1$. In this case, if $c_r < (r-1)$, then the next-to-minimum weight polynomials of $\mathcal{P}_r(2,q)$ have no linear factors, by Lemma 2.12. Corollary 2.8.1 gives a lower bound of $(q-r) \leq c_r$. The next chapter discusses attempts to improve this bound by an examination of blocking sets in affine planes.

The remainder of this chapter characterizes next-to-minimum weight polynomials of $\mathcal{P}_r(m,q)$ when $0 < r < (q+1)/2$.

Lemma 3.12

Let $P \in \mathcal{P}_t(m,q)$, where $1 < t \leq q-1$, such that $|P| = d_t^m + (t-1)q^{m-2}$. If P is the product of t linear factors, then P is equivalent to a polynomial Q(x), such that either

(1) $$Q(x) = \lambda\, x_2 \prod_{i=1}^{t-1} (x_1 - \lambda_i), \text{ where } \lambda_i = \lambda_j \Rightarrow i = j\,,$$

or

(2) $$Q(x) = \lambda \prod_{i=1}^{t} L_i(x_1, x_2), \text{ where } L_i = \alpha_i x_1 + \beta_i x_2 \text{ and}$$

$$\alpha_i\beta_j = \alpha_j\beta_i \Rightarrow i = j.$$

That is, Q is of form (208) or (209).

Proof:

If y is any variable, then, by Lemma 2.7, $\ell d(P,y) = 0, 1, t-1$, or t. If $\ell d(P, y) = t$ for some y, then P is a minimum weight polynomial. If $\ell d(P,y) = t-1$ for some y, then P is of form (1) above. If $\ell d(P,y) = 0$ for all y, then P has no linear factors. But P has t linear factors. Assume that for each variable y, $\ell d(P,y) > 0 \Rightarrow \ell d(P,y) = 1$. Then P is equivalent to a polynomial Q such that $Q(\overline{x}) = L_1(\overline{x})\, L_2(\overline{x}) \cdots L_t(\overline{x})$, where $L_1(\overline{x}) = x_1$, $L_2(\overline{x}) = x_2$, the L_i are all independent linear polynomials.

$$Z(Q) = \bigcup_{i=1}^{t} [Z(L_i) - Z(L_i) \cap \bigcup_{j=1}^{i-1} Z(L_j)],$$

and this union is disjoint. Thus,

$$N(Q) = t\,q^{m-1} - \sum_{i=1}^{t} \left|\left|Z(L_i) \cap \bigcup_{j=1}^{i-1} Z(L_j)\right|\right|.$$

Let $N_i = \left|\left|Z(L_i) \cap \bigcup_{j=1}^{i-1} Z(L_j)\right|\right|$, and let $N = N(Q)$.

$$N_1 = 0,\ N_2 = q^{m-2},\ \text{and for } i > 2,\ N_i \geqslant q^{m-2}.$$

If, for some i, $N_i > q^{m-2}$, then

$$t\,q^{m-1} - (t-1)q^{m-2} = q^m - |P| = N = t\,q^{m-1} - \sum_{i=1}^{t} N_i > t\,q^{m-1} - (t-1)q^{m-2},$$

which is a contradiction. Thus $N_i = q^{m-2}$ for all $i > 2$.

$$q^{m-2} = N_i = \left|\left|Z(L_i) \wedge \sum_{j=1}^{i-1} Z(L_j)\right|\right| \geq \left|\left|Z(L_i) \wedge (Z(L_1) \vee Z(L_2))\right|\right|$$

$$= \left|\left|Z(L_i) \wedge Z(L_1)\right|\right| + \left|\left|Z(L_i) \wedge Z(L_2)\right|\right|$$

$$- \left|\left|Z(L_i) \wedge Z(L_1) \wedge Z(L_2)\right|\right|$$

$$= 2\,q^{m-2} - \left|\left|Z(L_i) \wedge Z(L_1) \wedge Z(L_2)\right|\right| \geq q^{m-2},$$

$$\text{so } \left|\left|Z(L_i) \wedge Z(L_1) \wedge Z(L_2)\right|\right| = q^{m-2}.$$

Thus $Z\ (L_i)$ contains the (m-2) dimensional subspace of K^m described by $x_1 = x_2 = 0$. But then $L_i(\overline{x}) = \alpha_i x_1 + \beta_i x_2$. The condition $\alpha_i\beta_j = \alpha_j\beta_i \Rightarrow i = j$ assures that the factors are distinct.

Theorem 3.13

If $1 < r < (q+1)/2$, then the next-to-minimum weight polynomials of $\mathcal{P}_r(m,q)$ are equivalent to either:

$$\text{(301)}\quad Q(\overline{x}) = \lambda\ x_2 \prod_{i=1}^{r-1} (x_1 - \lambda_1) \text{ where } \lambda_i = \lambda_j \Rightarrow i = j, \quad \text{or}$$

$$(302)\quad Q(\bar{x}) = \lambda \prod_{i=1}^{r} L_i(x_1, x_2) \text{ where } L_i = \alpha_i x_1 + \beta_i x_2 \text{ and}$$

$$\alpha_i \beta_j = \alpha_j \beta_i \Rightarrow i = j.$$

Proof:

The next-to-minimum weight is $d_r^m + (r - 1)q^{m-2}$. If $|P| = d_r^m + (r - 1)q^{m-2} < d_r^m + (q - r)q^{m-2}$, then, by Corollary 2.8.2, P is the product of r linear factors. Applying 3.12 completes the proof.

Given any $r > 1$, Theorem 3.13 characterizes the next-to-minimum weight polynomials for all but a finite number of q. The characterization of next-to-minimum weight polynomials in the general case requires better bounds on the weights of polynomials without linear factors. This subject will be dealt with in the next chapter.

CHAPTER 4

Using Theorem 3.1 and a complete knowledge of the next-to-minimum weights $d_t^2 + c_t$ of $\mathcal{P}_t(2,q)$ for each t such that $(q+1)/2 < t < q-1$, the next-to-minimum weights of all Generalized Reed-Muller Codes could be calculated. In Chapter 2 it was proved that when $(q+1)/2 < t < q-1$, then $q-t \leq c_t \leq t-1$, and further, that $c_t < t-1$ implies that a next-to-minimum weight polynomial of $\mathcal{P}_t(2,q)$ has no linear factors. The goal of this chapter is to improve the lower bound on c_t by improving the bound given by Corollary 2.8.1 for the weights of polynomials without linear factors. This will be done by exploring a related topic; blocking sets.

Blocking sets may be defined for either finite projective planes or finite affine planes. Much of the work of A. Bruen [3] concerning the former, can be extended to the latter. This chapter deals mainly with the affine plans K^2 where K = GF(q), but, where possible, more general results will be derived, with results for projective planes being given in square brackets. Bruen gave the following definition of a blocking set.

Given a finite projective plane Π, a subset S of Π is called a blocking set in Π if and only if each line of Π contains at least one point of S and at least one point of Π-S.

Clearly, this definition would still be meaningful if Π were an affine plane. For this study, a slightly more general concept is needed.

Let Π be a finite affine [projective] plane, and let S be a subset of Π. S is called a <u>blocking set of order n in Π</u> if and only if each line of Π contains at least n points of S and at least n points of Π-S.

The relationship between blocking sets and low-weight polynomials is expressed in the following lemmas.

Lemma 4.1

If $P \in \mathcal{P}_t(2,q)$, $0 < t \leqslant q-1$ such that $d_t^2 < |P| < d_t^2 + (t-1)$, then $S(P)$ is a blocking set of order $q-t$ in the affine plane K^2, $(K = GF(q))$.

Proof:

By Lemma 2.12, such a P has no linear factors. The rest follows from the following lemma.

Lemma 4.2

If $P \in \mathcal{P}_t(2,q)$, $0 < t \leqslant q-1$ such that P has no linear factors and $|P| \leqslant d_t^2 + (t-1)$, then $S(P)$ is a blocking set of order $q-t$ in K^2.

Proof:

Let ℓ be a line of K^2. Then ℓ corresponds to the zeros of a linear polynomial (a variable) y. $||\ell \cap S(P)|| \neq \phi$, for that would imply $y|P$. But P restricted to ℓ is a polynomial of degree at most t, so $||\ell \cap S(P)|| \geqslant q-t$. Finally, to show that $||\ell \cap S(P)|| \leqslant t$, use the next lemma.

Lemma 4.3

Let Π be an affine plane of order q. Let S be a subset of Π such that $||S|| = nq+b$, where $0 \leqslant b \leqslant q-1-n$. If, for each line ℓ of Π, $||S \cap \ell|| \geqslant n$, then S is a blocking set of order n in Π.

Proof:

Suppose that for some line ℓ of H, $||\ell \cap S|| = q$. Let $L_1 = \ell, L_2, \ldots, L_q$ be q parallel lines of Π.

$$nq+b = ||S|| = ||S \cap \Pi|| = \sum_{i=1}^{q} ||S \cap L_i|| = q + \sum_{i=2}^{q} ||S \cap L_i||$$

$$\geqslant q + (q-1)n = qn + (q-n) \quad ,$$

contradicting $b \leqslant q - 1 - n$.

Now, suppose that $||\ell \cap S|| > q - n$. Let x be a point of $\ell - S$, and let the $q+1$ lines through x be $L_0 = \ell, L_1, \ldots, L_q$.

$$nq+b = ||S|| = \sum_{i=0}^{q} ||L_i \cap S|| > q - n + qn > nq+b \quad ,$$

also a contradiction. This completes the proof of 4.1, 4.2, and 4.3.

Thus, it has been shown that, to each sufficiently low weight polynomial P of degree t without linear factors, there corresponds a blocking set of order $q - t$, the set S(P). Whether the converse is true is not wholly known. The blocking sets of order one constructed in the proof of a later theorem will indicate that a meaningful converse to this lemma may not be possible.

Many of the following lemmas concerning blocking sets were proved by A. Bruen [3] for blocking sets of order 1 in projective planes.

Lemma 4.4: (Generalization of Bruen, Lemma 3.2)

Let S be a blocking set of order n in a finite affine [projective] plane Π of order q, such that $||S|| = nq+b$. If ℓ is any line of Π, then $||\ell \cap S|| \leqslant b$.

Proof:

If $||\ell \cap S|| > b$, then let $x \in \ell - S$. Let $L_0 = \ell, L_1, \ldots, L_q$ be the $q+1$ lines of Π containing x. Then

$$||S|| = \sum_{i=0}^{q} ||L_i \cap S|| > b + qn \quad ,$$

contradicting $||S|| = nq+b$.

From Lemma 4.4, one can conclude that a blocking set of order n in a plane of order q has at least $nq+n$ elements. This conclusion is precisely the same as one may draw from Lemma 2.8.

The next lemma is a counting argument which will be used later.

Lemma 4.5: (Generalization of Bruen, Lemma 3.3)

Suppose that c objects are packed into a slots, at least n to a slot, and that $an < c < a(n+1)$. Define a function f on the objects x as follows:

$$f(x) = \begin{cases} 1 & \text{if the slot containing } x \text{ contains more than } n \text{ objects} \\ 0 & \text{if the slot containing } x \text{ contains exactly } n \text{ objects} \end{cases}$$

For each packing P, define $A(P) = \Sigma f(x)$, where the sum is taken over all the objects x. Then $A(P) \leqslant (c-an)(n+1)$.

Proof:

If, in the partition P, some slot contains more than $n+1$ objects, then, by the restriction $c < a(n+1)$, there is a slot with exactly n objects. If a new partition P' is derived from P by removing one object from the slot with more than $n+1$ objects, and placing it in a slot with exactly n objects, then $A(P') = A(P) + a$. Thus, $A(P)$ is maximized when P has only slots with at most $n+1$ objects. In this case $A(P) = (n+1)(c-an)$.

For the next portion of this discussion, let Π be an affine [projective] plane of order q. Let S be a blocking set of order n in Π such that $||S|| = nq+b$. Define $k = \max ||\ell \cap S||$, the maximum taken over all lines ℓ of Π. By Lemma 4.4, $k \leqslant b$. Let L be a specific line of Π such that $||L \cap S|| = k$.

Lemma 4.6: (Generalization of Bruen, Lemma 3.1)

With the above definitions, $k > n$. Furthermore, $k = n+1$ implies $b = n+1$.

Proof:

By definition, $k \geqslant n$. Thus, $b \geqslant n$. Let $L_0 = L, L_1, \ldots, L_q$ be the $q+1$ lines through a particular point $x \in L \cap S$, then

$$||S|| = \sum_{i=0}^{q} ||S \cap L_i|| - q \leqslant (q+1)k - q \quad .$$

If $k = n$, then $||S|| \leqslant qn + (n-q)$, contradicting $||S|| > qn$.

If $k = n+1$, then $||S|| \leqslant (q+1)(n+1) - q = qn + (n+1)$. So, $n+1 = k \leqslant b = ||S|| - qn \leqslant n+1$. Thus, $b = n+1$, and Lemma 4.6 is proved.

Now, define B, the set of lines of π other than L which intersect L - S and contain more than n points of S:

$$B = \{\ell \mid \ell \text{ is a line of } \Pi,\ \ell \neq L, \text{ such that}$$
$$\ell \cap (L-S) \neq \phi \text{ and } ||\ell \cap S|| > n\} \ .$$

Define the set of incidences I of points of S with lines of B:

$$I = \{(x, \ell) \mid \ell \in B \text{ and } x \in \ell \cap S\} \ .$$

The next two lemmas count I.

<u>Lemma 4.7</u>: (Generalization of Bruen, Lemma 3.4)

$||I|| \leqslant (n+1)(b-k)(q-k[+1])$, that is $||I|| \leqslant (n+1)(b-k)(q-k)$ for affine Π, [$||I|| \leqslant (n+1)(b-k)(q-k+1)$ for projective Π].

<u>Proof</u>:

For each point $y \in L-S$, the $nq+b-k$ points of $S-L$ are packed into q lines through y. By Lemma 4.5, these lines through y yield at most $(n+1)(b-k)$ incidences of I. Since there are $q-k$ such points $y \in L-S$ [$q-k+1$ if Π is projective], the lemma is proved.

For the next lemma, if $B \neq \phi$, define $d = \max\limits_{\ell \in B} ||\ell \cap S||$. Then $d > n$.

<u>Lemma 4.8:</u> (Generalization of Bruen, Lemma 3.5)

If $B \neq \phi$, then $||I|| \geqslant (qn+b-k)(nk+b-k^2-k+q[+k-n])(d-n)^{-1}$.

Proof:

Let x be any point of $S - L$. Then $||S|| - 1 = nq+b-1$ other points of S are partitioned into $q+1$ lines through x. Exactly k of these lines intersect $L \cap S$. Each of these contains at most $k-1$ points of $S - \{x\}$. In the affine case, there is exactly one line through x parallel to L. This line contains at most $k-1$ points of $S - \{x\}$. [In the projective case, no such line exists.] Thus, in the affine case, there remain at least $nq+b-1-(k+1)(k-1)$ points of $S - \{x\}$, partitioned among the remaining $q-k$ lines. [In the projective case, $nq+b-1-k(k-1)$ points; $q-k+1$ lines.] But, since no line of B contains more than d points of S, the number of incidences in I of the form (x, ℓ) is at least

$$(nq+b-k^2-(n-1)(q-k)[+k-n])(d-n)^{-1} = (nk+b-k^2-k+q[+k-n])(d-n)^{-1} \quad .$$

Since there are precisely $nq+b-k$ such points $x \in S - L$, the lemma is proved.

The next lemma is used to delete d from the inequality.

Lemma 4.9: (Generalization of Bruen, Lemma 3.6)

$$(d-n) \leqslant \tfrac{1}{2}(b-n).$$

Proof:

Some line of B, call it L_1, contains d points of S. Let $x = L \cap L_1$, then $x \notin S$. Let $L_0 = L$, and let $L_0, L_1, \ldots, L_q$ be the $q+1$ lines through x.

$$nq+b = ||S|| = \sum_{i=0}^{q} ||L_i \cap S|| \geqslant k+d+(q-1)n = qn+(d+k-n) \quad ,$$

so $b \geqslant d+k-n$.

Thus, $b - n \geq (d-n) + (k-n)$. By definition, $d \leq k$, so $(b-n) \geq 2(d-n)$, proving the lemma.

Combining Lemmas 4.7, 4.8, and 4.9:

$$(b-n)(n+1)(b-k)(q-k[+1]) \geq (b-n)\,||I|| \geq 2(qn+b-k)(nk+b-k^2-k+q[+k-n]) \quad ,$$

so when $B \neq \phi$, then

$$(401) \quad (b-n)(n+1)(b-k)(q-k[+1]) \geq 2(qn+b-k)(nk+b-k^2-k+q[+k-n]) \quad .$$

Furthermore, when $B = \phi$, then (401) still holds, since the right side must be non-positive, and the left side non-negative. Observing that

$$\begin{aligned} (n+1)(q-k[+1]) &= 2\left(nq - k[+ \tfrac{n+1}{2}] - \frac{(n-1)(q+k)}{2}\right) \\ &< 2(nq-k+b), \quad \text{since } n \geq 1 \; [\text{and } b > \tfrac{n+1}{2}] \; , \end{aligned}$$

simplify (401) to get

$$(402) \qquad (b-n)(b-k) \geq nk + b - k^2 - k + q[+k-n] \quad .$$

Let

$$(403) \qquad f(k) = (b-n)(b-k) + k^2 + k - nk - b - q[+n-k] \quad ,$$

then $f(k) \geq 0$.

Evaluating f at 0 and b,

$$f(0) = (b-n)b - b - q[+n] = b(b-n-1) - q[+n]$$

$$f(b) = b^2 + b - nb - b - q[+n-b] = b(b-n-1) - q + b[+n-b] \geq f(0) \quad .$$

Since f is concave upward, and $0 < k \leqslant b$, then $0 \leqslant f(k) \leqslant f(b) = b(b-n) - q[+n-b]$.

This proves the following theorem.

Theorem 4.10: (Generalization of Bruen, Theorem 3.8)

If S is a blocking set of order n in an affine [projective] plane of order q, such that $||S|| = nq+b$, then:

(404) $$b(b-n) - q[+n-b] \geqslant 0$$

or, in other words,

(405) $$b \geqslant \tfrac{1}{2}\left(n[+1] + \sqrt{(n[-1])^2 + 4q}\right) \quad .$$

In the projective case with $n = 1$, Theorem 4.10 reduces to Bruen's result, $||S|| \geqslant q + \sqrt{q} + 1$. When q is a square, Bruen points out that a subplane of order $\sqrt{q}$ is a blocking set of order one with exactly $q + \sqrt{q} + 1$ elelents. When q is not a square, however, this bound is not necessarily "tight". He improved the bound by "point chasing" in specific cases. For $q = 10$ and $q = 11$, he expressed his results in his Theorems 4.1 and 4.2.

Bruen's Theorem 4.1

Suppose there exists a projective plane Π of order 10. Assume that Π contains no projective subplane of order 2. Then if S is a blocking set (of order 1) in Π, we have $||S|| \geqslant 16$.

Bruen's Theorem 4.2

If Π is a (projective) plane of order 11, and S is a blocking set (of order 1) in Π, then $\|S\| \geq 17$. Further, the case $\|S\| = 18$ occurs.

Table 4.1 summarizes Bruen's results for blocking sets of order one in small projective planes. Besides the lower bounds which he obtained, he gave constructions of the smallest blocking sets which had been found for planes of small order. Bruen stated two theorems which deal with the existence of blocking sets.

Table 4.1

Lower Bound on the Size of a Blocking Set S of Order One in a Projective Plane of Order q*

q	Bound from Bruen Th. 3.8	Improved Bound	Improvement Technique	Smallest Known
3	$\|S\| \geq 6$	- - -	- - -	6
4	$\|S\| \geq 7$	- - -	- - -	7
5	$\|S\| \geq 9$	- - -	- - -	9
7	$\|S\| \geq 11$	$\|S\| \geq 12$	"point chasing"	12
8	$\|S\| \geq 12$	$\|S\| \geq 13$	"point chasing"	13
9	$\|S\| \geq 13$	- - -	- - -	13
10	$\|S\| \geq 15$	$\|S\| \geq 16$	Bruen Th. 4.1	20
		(if no subplanes of order 2)		
11	$\|S\| \geq 16$	$\|S\| \geq 17$	Bruen Th. 4.2	18

*A. Bruen [3].

Bruen's Theorem 2.1

If Π is the projective plane of order 2, then there does not exist a blocking set in Π.

Bruen's Theorem 2.2

If Π is (a projective plane) of order $n > 2$, then there exists a blocking set S (of order 1) in Π with $||S|| = 2n$.

Bruen also gave three, more specialized constructions of smaller blocking sets. His Theorems 5.1 to 5.3 deal with the projective planes $PG(2,q)$ where $q = p^t$, p prime, which may be derived from the affine planes $AG(2,q) = K^2$, $K = GF(q)$ by adding a line at infinity.

Bruen's Theorem 5.1

Let $\Pi = PG(2,q)$, $q = p^t$, p an odd prime. Then there exists a blocking set S in Π such that $||S|| = p^t + \frac{1}{2}(p^t+3)$.

Bruen's Theorem 5.2

Let $\Pi = PG(2,q^t)$, $t \geq 2$. Then there exists a blocking set S in Π with $||S|| = q^t + (q^t-1)(q-1)^{-1}$.

Bruen's Theorem 5.3: (Due to Ostram)

There exist blocking sets S in $\Pi = PG(2,q^t)$ such that $||S|| = q^t + q^{t-1} + 1$. (If $t \geq 2$.)

The constructions used in these last three theorems do not readily adapt to the affine case. The first two theorems are adaptable as follows.

Theorem 4.11

There are no blocking sets of order 1 in an affine plane of order q, when $q \leqslant 3$.

Proof:

By Theorem 4.10, if S is such a blocking set, then $||S|| \geqslant q + \frac{1}{2}(1 + \sqrt{4q+1})$. But, by the definition of blocking set, $\Pi - S$ is also a blocking set. Thus,

$$q + \tfrac{1}{2}(1 + \sqrt{4q+1}) \leqslant ||S|| \leqslant q^2 - q - \tfrac{1}{2}(1 + \sqrt{4q+1})$$

$$2q + 1 + \sqrt{4q+1} \leqslant q^2 \quad .$$

This implies $q > 3$.

Theorem 4.12

If Π is an affine plane of order q with $q > 4$, then there is a blocking set S of order 1 in Π such that $||S|| = 2q - 1$.

Proof:

Let xy_1zy_2 be a parallelogram in Π. That is, if $\overline{ab}$ denotes the line through a and b, then $\overline{xy_1} \,||\, \overline{zy_2}$ and $\overline{xy_2} \,||\, \overline{zy_1}$. Let w be any point of $\overline{y_1y_2}$ except y_1 or y_2. Let S be the set

$$S = \overline{xy_1} \cup \overline{xy_2} \cup \{z\} \cup \{w\} - \{y_1\} - \{y_2\} \quad .$$

The same construction would work for $q = 4$, except that $\overline{wz}$ might contain 4 points of S. We resolve this problem as follows.

Theorem 4.13

If Π is an affine plane of order 4, then there exists a blocking set S of order 1 in Π such that $||S|| = 7$, if and only if $\Pi \neq AG(2,4)$. There is, however, always a blocking set T of order 1 in Π such that $||T|| = 8$.

Proof:

Suppose that for some parallelogram xy_1zy_2 in Π, $\overline{xz} \cap \overline{y_1y_2} \neq \phi$. Then let $w = \overline{xz} \cap \overline{y_1y_2}$, and let $S = \overline{xy_1} \cup \overline{xy_2} \cup \{z\} \cup \{w\} - \{y_1\} - \{y_2\}$. Thus a blocking set S with $||S|| = 7$ exists if Π does not satisfy the parallelogram condition: the diagonals of every parallelogram are parallel. If S is any blocking set of Π such that $||S|| = 7$, then, by Lemma 4.6, there is a line L of Π such that $||L \cap S|| = 3$. Let $x \in L \cap S$. Consider the $q + 1$ lines through x, $L_0 = L, L_1, \ldots, L_q$.

$$7 = ||S|| = \sum_{i=0}^{4} ||L_i \cap S|| - 4$$

so $\sum_{i=1}^{4} ||L_i \cap S|| = 8$. If $||L_i \cap S|| \geq 2$ for each $i = 1, \ldots, 4$, then $S - \{x\}$ is a blocking set, and $||S - \{x\}|| = 6$, contradiction 4.10. Thus, there is an i′ such that $||L_{i'} \cap S|| = 3$. Let $L' = L_{i'}$. Let $y_1 \in L - S$, $y_2 \in L' - S$ and let z complete the parallelogram xy_1zy_2. We have that $\overline{xy_1} \cup \overline{xy_2} - \{y_1\} - \{y_2\} \leq S$. This accounts for 5 points, and leaves 3 lines unblocked; $\overline{y_1z}$, $\overline{y_2z}$, and $\overline{y_1y_2}$. Since $y_1, y_2 \notin S$, $z \in S$. We must also have some $w \in S \cap \overline{y_1y_2} - \{y_1\} - \{y_2\}$. The line $\overline{zw}$ intersects $\overline{xy_1}$ and $\overline{xy_2}$. If it intersects them in distinct points, it would contain four points of S. Thus $x \in \overline{zw}$ and $w \in \overline{xz} \cap \overline{y_1y_2}$ showing that Π does not satisfy the parallelogram condition. That AG(2,4) is the only affine plane of order 4 which satisfies the parallelogram condition can be established by point chasing.

To find T, let xy_1xy_2 be a parallelogram. $T = \overline{xy_1} \cup \overline{xy_2} \cup \overline{y_1z} - \{x\} - \{y_1\}$. This completes 4.13.

It is interesting to note that the blocking set $S = \overline{xy_1} \cup \overline{xy_2} \cup \{z\} \cup \{w\} - \{y_1\} - \{y_2\}$ from Theorem 4.12 is not the support set of a polynomial $P \in \mathcal{P}_{q-1}(2,q)$. If it were, then, by Theorem 1.6, if $R \in \mathcal{P}_3(2,q)$, then

$$\sum_{\overline{\sigma} \in K^2} P(\overline{\sigma})R(\overline{\sigma}) = 0 \quad , \tag{1}$$

since $q \geqslant 5$.

Let R be the product of three linear factors corresponding to the lines $\overline{xy_1}$, $\overline{xy_2}$, and $\overline{y_2z}$. Then $|PR| = 1$ contradicting (1).

This observation casts some doubt on the conjecture: Every blocking set S of order 1 in the plane AG(2,q) such that $||S|| < 2q-1$ is the support set of a polynomial of degree $q-1$. This conjecture, along with earlier results on polynomials would imply that no such blocking sets exist. The conjecture is vacuously true for $q \leqslant 9$, as established by a computer search. The hope of proving it in the general case as a means to establishing a lower bound of $2q-1$ on the number of elements in a blocking set, appears to be useless, however.

The following conjecture would establish that $c_t = t-1$ for $q \geqslant 4$.

Conjecture 4.14

Let Π be the affine plane $AG(2,q)$. If S is a blocking set of order n in Π, then $||S|| \geqslant nq + (q-n)$.

Actually, to prove that $c_t = t-1$, only $||S|| \geqslant nq + (q-1-n)$ is needed, but 4.14, together with Theorem 4.12, would give the size of the smallest blocking set of order one.

If $n \geqslant q/2$, then 4.14 is vacuously true. If $n < q/2$, then, by Theorem 4.10, $||S|| = nq + b$, where $b \geqslant \frac{1}{2}\left(n + \sqrt{n^2 - 4q}\right)$. Since $n < q-1$, $n^2 + 4q > n^2 + 4n + 4$. This proves Lemma 4.15.

Lemma 4.15

Let Π be an affine plane of order q. If S is a blocking set of order n in Π, then $||S|| \geqslant nq + n + 2$, (i.e., the case $k = b = n+1$ of Lemma 4.6 does not occur).

The next lemma is a bit more difficult to prove.

Lemma 4.16

Let Π be an affine plane of order q. Let S be a blocking set of order n in Π such that $||S|| = nq+b$. If $b = n+2$, then $n \geqslant q/2 - 1$.

Proof:

Let $k = \max ||\ell \cap S||$, where the max is taken over all lines ℓ of Π. Let L be a line such that $||L \cap S|| = k$. By Lemma 4.6, $k = b = n+2$. This being the case, every line except L which intersects $L - S$ contains exactly n points of S. Pick a point $x \in S - L$. Let L_0 be the line through x parallel to L. Let $L_1, \ldots, L_k$ be the lines through x which intersect

$L \wedge S$, and let $L_{k+1}, \ldots, L_q$ be the lines through x which intersect $L - S$. Then

$$nq + b = ||S|| = \sum_{i=0}^{q} ||L_i \wedge S|| - q = (q-k)n - q + \sum_{i=0}^{k} ||L_i \wedge S||$$

so, in using $k = b = n+2$,

$$\sum_{i=0}^{k} (k - ||L_i \wedge S||) = 2k - q \quad .$$

But, each term of the sum $k - ||L_i \wedge S||$ is non-negative. Suppose $2k - q \leqslant 1$, then $||L_0 \wedge S|| \geqslant k - 1 = n+1$, so each line of Π which is parallel to L would have at least $n+1$ points of S. This would imply $||S|| > qn + q \geqslant qn + n + 2$ a contradiction. Thus $2k - q \geqslant 2$. Substituting $k = n+2$, $2n+4 \geqslant q+2$ or $n \geqslant (q-2)/2$ which was to be proved.

Lemma 4.15 and Lemma 4.16 establish Conjecture 4.14 for $n \geqslant (q-3)/2$ and the weaker result for $n \geqslant (q-4)/2$. In addition to these two lemmas, another technique may be used to establish the truth of Conjecture 4.14 in certain cases. A computer program was written to run on the Xerox Data Systems 930 computer, which accepts as input, values for q, n, and b, along with information on how to build the finite field GF(q). The program builds tables which represent the affine plane $\Pi = AG(2,q)$. It then searches for blocking sets of order n in Π with at most b elements. If it locates such a blocking set S, the program resets the value of b to $||S|| - 1$ and continues the search. Thus, the program is intended to find a minimum size blocking set with at most b elements. The number of subsets of Π which must be tested, to determine whether they are indeed blocking sets, is large. The program uses the technique of backtracking to reduce the number of possibilities which must be tested. Negative results from such a program must be accepted with a degree of reserve, because the accuracy of the coding of the program, and indeed, the functioning of the computer hardware, cannot be verified. Therefore, the lower bounds on the sizes of blocking sets derived by the computer program are annotated by being followed by asterisks. The following results, not given by previous lemmas, were derived by the program.

Result 4.17

Let Π be the affine plane AG(2,q), and let S be a blocking set of order n in Π. Then

a) $q = 7,\ n = 1 \Rightarrow ||S|| \geq nq+q-n = 13^*$

b) $q = 8,\ n = 1 \Rightarrow ||S|| \geq nq+q-n = 15^*$

c) $q = 8,\ n = 2 \Rightarrow ||S|| \geq nq+q-n = 22^*$

d) $q = 9,\ n = 1 \Rightarrow ||S|| \geq nq+q-n = 17^*$.

A summary of the results concerning blocking sets of order one is given in Table 4.2.

Finally, these results on blocking sets of order n in affine planes may be applied to the prime objective of this paper, by Lemma 4.1.

Lemma 4.18

Let the next-to-minimum weight of $\mathcal{P}_t(2,q)$ be $(q-t)q+c_t$. If $(q+4)/2 < t < q-1$, then $c_t \geq q-t+3$. If $(q+1)/2 < t \leq (q+4)/2$, then $c_t = t-1$.

Table 4.2

Lower Bound on the Size of a Blocking Set S of Order One in an Affine Plane of Order q

q	Bound from Theorem 4.10	Improved Bound	Improvement Technique	Smallest Known
4	$\Vert S \Vert \geqslant 7$	Not AG(2,4)		7
		$\Vert S \Vert = 8$ for AG(2,4)		8
		Theorem 4.13		
5	$\Vert S \Vert \geqslant 8$	$\Vert S \Vert \geqslant 9$	Theorem 4.16	9
7	$\Vert S \Vert \geqslant 11$	$\Vert S \Vert \geqslant 13^*$	Computer search	13
8	$\Vert S \Vert \geqslant 12$	$\Vert S \Vert \geqslant 15^*$	Computer search	15
9	$\Vert S \Vert \geqslant 13$	$\Vert S \Vert \geqslant 17^*$	Computer search	17
11	$\Vert S \Vert \geqslant 15$			21

Proof:

Lemma 4.18 follows from Lemma 4.1 and the application of Lemmas 4.15 and 4.16.

This lemma will be integrated with Theorem 3.1, to form Theorem 5.1 in the next chapter.

CHAPTER 5

This chapter begins with a theorem summarizing much of the work of chapters two through four.

Theorem 5.1

If P is a polynomial of degree $r = s(q-1) + t$, with $0 < t \leqslant q-1$, in m variables over GF(q), and N(P) is the number of zeros of P, then:

1) $N(P) > q^m - q^{m-s} + tq^{m-s-1}$ implies that P is identically zero,

2) $N(P) < q^m - q^{m-s} + tq^{m-s-1}$ implies that $N(P) \leqslant q^m - q^{m-s} + tq^{m-s-1} - cq^{m-s-2}$ where

$$c = \begin{cases} q & \text{if } s = m-1 \text{ or if } t = 1 \text{ and either } s = 0 \text{ or} \\ & q \geqslant 4 \text{ or } s = m-2 \text{ and } q = 2 \\ q-1 & \text{if } t = 1 \text{ and either } q = 3 \text{ and } 0 < s = m-2 \text{ or} \\ & q < 4 \text{ and } 0 < s < m-2 \\ t-1 & \text{if } s < m-1 \text{ and either } 1 < t < (q+5)/2 \text{ or} \\ & 1 < t = q-1. \end{cases}$$

In the remaining case, $(q+5)/2 \leqslant t < q-1$, $s < m-1$, $q \geqslant 4$, $q-t+3 \leqslant c \leqslant t-1$. Furthermore, there exists a polynomial $P \in \mathcal{P}_r(m,q)$ with $N(P) = q^m - q^{m-s} + tq^{m-s-1} - cq^{m-s-2}$.

Proof: Theorem 3.1 and Lemma 4.18.

In the notation of coding theory, Theorem 5.1 might be stated:

Theorem 5.1*

The next-to-minimum weight of the r^{th} order Generalized Reed-Muller Code of length q^m, where $r = s(q-1)+t$, $0 < t \leq q-1$, is $(q-t)q^{m-s-1} + cq^{m-s-2}$. The restrictions on c are given in Theorem 5.1 and displayed in Table 5.1

The rest of this chapter concentrates on methods by which more knowledge about the weight spectra of Generalized Reed-Muller Codes might be obtained. Theorem 4.10 gives better results than Theorem 5.1 in the case $(q+5)/2 \leq t \leq q-1$ if

$$\frac{(q-t) + \sqrt{2q^2 - 2qt+t^2}}{2} > q-t+3 \quad ,$$

when the smaller of the former expression and $t-1$ is a lower bound for c. This improvement in 5.1 is miniscule compared to the improvement which could be derived from proving Conjecture 4.14. In that case, the lower bound of $t-1$ would stand, and it would be a tight bound. A backtracking search by computer might establish 4.14 in a few more specific cases. The smallest case not yet tested would be $q = 9$, $t = 2$. It would take an estimated fifty hours to complete this case with the currently implemented program on the XDS 930 computer. The program is equipped with a means of being interrupted and restarted so that it may be run during lulls in the computer's schedule. It is probably beyond the capacity of this program to complete the case $q = 11$ in a reasonable amount of time.

Table 5.1

Restrictions On Next-to-Minimum Weight of $GRM_r(m,q)$ Given by Theorem 5.1*, Where $r = s(q-1)+t,\ 0 < t \leqslant q-1$. Next-to-Minimum Weight $= (q-t)q^{m-s-1} + cq^{m-s-2}$.

	$t = 1$			$1 < t < (q+5)/2$ $t \neq q-1$	$(q+5)/2 \leqslant t < q-1$	$1 < t = q-1$	
	$q = 2$	$q = 3$	$q \geqslant 4$	$q \geqslant 4$	$q \geqslant 4$	$q = 3$	$q \geqslant 4$
$0 = s < m-1$	$c = q$	$c = q$	$c = q$	$c = t-1$	$q-t+3 \leqslant c$ $\leqslant t-1$	$c = q$	$c = t-1$
$0 < s < m-2$	$c = q-1$	$c = q-1$	$c = q$	$c = t-1$	$q-t+3 \leqslant c$ $\leqslant t-1$	$c = q$	$c = t-1$
$0 < s = m-2$	$c = q$	$c = q-1$	$c = q$	$c = t-1$	$q-t+3 \leqslant c$ $\leqslant t-1$	$c = q$	$c = t-1$
$s = m-1$	$c = q$	$c = q$	$c = q$	$c = q$	$c = q$	$c = q$	$c = q$

The computer might also be considered for use in an attempt to enumerate the equivalence classes of reduced polynomials of degree r in m variables over GF(q). Such an attempt does not seem to hold much promise for the following reason. The number of equivalence classes of $\mathcal{P}_r(m,q)$ must be at least as great as the quotient of the number of polynomials in $\mathcal{P}_r(m,q)$ by the number of invertible affine transformations. From Chapter 1, the number of invertible affine transformations is $q^m(q^m - 1)\cdots(q^m - q^{m-1})$. Also from Chapter 1, if $p(k,m,q)$ represents the number of m-tuples of integers $(a_1, a_2, \ldots, a_m)$ such that $0 < a_i \leq q$ and $\sum_{j=1}^{m} a_j = k$, then

(501) $$\dim \mathcal{P}_r(m,q) = \sum_{i=0}^{r} p(i+m,m,q) \quad .$$

And,. since

(502) $$\text{the number of i.a.t.'s} = q^m \prod_{i=0}^{m-1} (q^m - q^i) < q^{m^2+m} \quad ,$$

(503) the number of equivalence classes of $\mathcal{P}_r(m,q)$ is at least q^b where

$$b = \sum_{i=0}^{r} p(i+m,m,q) - m^2 - m \quad .$$

$$p(m,m,q) = 1$$

$$p(m+1,m,q) = m$$

$$p(m+2,m,q) = \begin{cases} m(m-1)/2 & \text{if } q = 2 \\ m(m+2)/2 & \text{if } q > 2 \end{cases}$$

$$p(m+3,m,q) = \begin{cases} m(m-1)(m-2)/6 & \text{if } q = 2 \\ m(m-1)(m+4)/6 & \text{if } q = 3 \\ m(m+1)(m+2)/6 & \text{if } q > 3 \quad . \end{cases}$$

Thus, from (503), the number of equivalence classes of $\mathcal{P}_3(m,q)$ is at least q^b where

$$b = \begin{cases} 1 + m(m^2-6m-1)/6 & \text{if } q = 2 \\ 1 + m(m^2-1)/6 & \text{if } q = 3 \\ 1 + m(m^2+5)/6 & \text{if } q > 3 \quad . \end{cases}$$

In either of these cases, the number of equivalence classes grows rapidly with m. Therefore, there seems to be little hope of finding canonical forms for polynomials of $\mathcal{P}_r(m,q)$ when $r \geqslant 3$ and m is even moderately large. Since canonical forms have been found for $r = 2$ (McEliece [9]), there is little new knowledge to be gained in this area without significant new techniques.

There is another way in which digital computers fail to obtain hoped-for results concerning weight spectra of GRM codes. One might hope to determine the weight spectrum of a GRM code empirically by a Monte Carlo method. That is, one might generate polynomials of $\mathcal{P}_r(m,q)$ with random coefficients in GF(q), determine their weight, and tabulate the results. This technique fails because the distribution of weights is so dense near $q^m - q^{m-1}$ and so sparse in low weight polynomials that the probability of a random polynomial having low weight is very small. Since we expect no gaps near the mean weight, $q^m - q^{m-1}$, other than those predicted by Ax, this process yields no interesting information.

There is one exception to these gloomy predictions of the uselessness of further computer applications in this area. A computer program may be able to determine, with a reasonable amount of computer time, the smallest subsets S of the plane K^2, $K = GF(q)$ which correspond to support sets of polynomials of $\mathcal{P}_r(2,q)$ without linear factors. Armed with these results and the results of chapters two and three, it might be possible to characterize the polynomials in $\mathcal{P}_r(m,q)$ of less than a certain weight for some specific $r > 2$ and $q > 2$. With enough results of this kind, conjectures and directions for further study might result.

Even without computer aid, the techniques and results developed in chapters two and three hold the promise of characterizing the low weight polynomials in certain cases, especially when $r = s(q-1) + t$, $0 < t < (q+1)/2$.

What types of theorems might we be able to prove once we have more data concerning weight spectra? We might hope to get results which generalize Kasami and Tokura's classification of all polynomials with weight less than $2\frac{1}{2}$ times the minimum weight when $q = 2$. In the general case, however, this bound may be $q/(q-1) + (q-1)/q$ times the minimum weight, or some similar expression. The McEliece results on second order GRM codes hint at the possibility of an extension of the divisibility condition of Ax. McEliece found that if $P \in \mathcal{P}_2(m,q)$, then

$N(P) = q^{m-1} + \nu q^{m-j-1}$, where $\nu = 0$, ± 1 or $\pm (q-1)$, and $0 \leqslant j \leqslant [\frac{m}{2}]$. Thus, not only does q^b divide N(P), where $b = [\frac{m-1}{2}] = m - [\frac{m}{2}] - 1$, as proved by Ax, but also $|N(P) - q^{m-1}| \geqslant q^a \Rightarrow q^a$ divides $|N(P) - q^{m-1}|$. These two divisibility conditions do not fully characterize McEliece's results. A condition similar to the second: $|N(P) - q^{m-1}| \geqslant$ bound $\Rightarrow q^a$ divides $|N(P) - q^{m-1}|$, where bound depends on a, q, m, and r; exists in the general case. Whether bound can be chosen to have a nice functional form remains to be seen.

In conclusion, more data are needed. Knowing the weight spectrum of $\mathcal{P}_r(m,q)$ for specific $q > 2$, $r > 2$, $m \geqslant 2$ could prove helpful. Using the results of chapters two and three, more data on low weight polynomials might be derived. It appears that the general problem of characterizing all polynomials in $\mathcal{P}_r(m,q)$ or even of finding the weight spectrum, is extremely difficult. More work on low-weight polynomials could probably improve the results obtained herein, however.

REFERENCES

[1] Ax, James. "Zeroes of Polynomials over Finite Fields," American Journal of Mathematics, Vol. 86, No. 2 (April 1964), pp. 255-261.

[2] Berlekamp E.R. Algebraic Coding Theory, San Francisco; McGraw-Hill, 1968.

[3] Bruen, A. "Blocking Sets in Finite Projective Planes," SIAM Journal on Applied Mathematics, Vol. 21, No. 3 (November 1971), pp. 380-392.

[4] Chevalley, C. "Demonstration d'une hypothèse de M. Artin," Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, Vol. 11 (1936), pp. 73-75.

[5] Delsarte, P., Goethals, J.M., and MacWilliams, F.J., "On Generalized Reed-Muller Codes and Their Relatives," Information and Control, Vol. 16 (1970), pp. 403-442.

[6] Kasami, T., Lin, S., and Peterson, W.W. "New Generalizations of the Reed-Muller Codes," IEEE Transactions on Information Theory, Vol. II-14 (1968), pp. 189-199.

[7] Kasami, T., and Tokura, N. "On the Weight Structure of Reed-Muller Codes," IEEE Transactions on Information Theory, Vol. II-16, No. 6 (November 1970), pp. 752-759.

[8] Kasami, T., Tokura, N., and Azumi, S. "Weight Enumerator Formulas of Reed-Muller Codes for $2d < w < 2.5d$," (January 1973), Faculty of Engineering, Osaka University (in Japanese).

[9] McEliece, Robert J. "Combinatorial Communication: Quadratic Forms Over Finite Fields and Second-Order Reed-Muller Codes," Space Program Summary 37-58, Vol. III; Jet Propulsion Laboratory, Pasadena, California, pp. 28-33.

[10] Sugino, M., Ienaga, Y., Tokura, N., and Kasami, T. "Weight Distribution of (128, 64) Reed-Muller Code," IEEE Transactions on Information Theory, Vol. IT-17, No. 5 (September 1971), pp. 627-628.

[11] van Lint, J.H. Coding Theory, New York; Springer-Verlag, 1971.

[12] van Tilborg, H. "Weights in the Third-Order Reed-Muller Codes," The Deep Space Network Progress Report for May and June 1971, Technical Report 32-1526, Vol. IV (August 1971); Jet Propulsion Laboratory, Pasadena, California; pp. 86-94.

[13] Warning, E. "Bemerkung zur vorstehenden Arbeit von Herrn Chevalley," Abhandlungen aus den Mathematischen Seminar der Universität Hamburg, Vol. 11 (1936), pp. 76-83.