1956

Sums of Irreducible Polynomials With Coefficients in Gf(q).

Ray Paul Authement
Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation
Authement, Ray Paul, "Sums of Irreducible Polynomials With Coefficients in Gf(q)." (1956). LSU Historical Dissertations and Theses. 163.
https://digitalcommons.lsu.edu/gradschool_disstheses/163

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
SUMS OF IRREDUCIBLE POLYNOMIALS WITH COEFFICIENTS IN GF(q).

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

Ray Paul Authement
M.S., Louisiana State University, 1952
August, 1956
ACKNOWLEDGMENT

My sincere thanks to Dr. L. I. Wade for introducing me to analytic number theory and for his assistance in the preparation of this dissertation.
# TABLE OF CONTENTS

ABSTRACT ........................................ iv

INTRODUCTION ..................................... 1

CHAPTER I
  Density of Sets of Primary Polynomials .......... 2

CHAPTER II
  Sets of Irreducible Polynomials ................. 8
  Algebraic Theorems of Viggo Brun ............... 12
  Method of Viggo Brun .......................... 17
  Number of Polynomials in $P(n)+P(n-1)$ ........ 23

CHAPTER III
  Sums of Irreducible Polynomials ............... 31
  List of Constants ................................ 33

BIBLIOGRAPHY .................................... 35

AUTOBIOGRAPHY ................................... 36
ABSTRACT

In 1742 Goldbach conjectured that every even number greater than six can be written as the sum of two odd primes, and every odd number greater than nine can be written as the sum of three odd primes. As recently as 1931, a Russian mathematician, Schnirelman was able to make the first contribution towards the solution of this problem. By using the methods of Viggo Brun he was able to show that every number can be written as the sum of not more than 300,000 primes. In 1937, another Russian mathematician, Vinogradoff, was able to show by different methods that all sufficiently large numbers can be written as the sum of not more than four primes.

In this dissertation we consider an analog to this problem. Namely, that any primary polynomial $f$ with coefficients in $GF(q)$ can be written as

$$f = p + p'$$

where $p$ and $p'$ are irreducibles and $\deg p \neq \deg p'$.

By the use of methods similar to those of Schnirelman we show that every primary polynomial with coefficients in $GF(q)$ can be written as the sum of at most a finite number of irreducibles.

iv
INTRODUCTION

In this dissertation we consider sets of polynomials with coefficients in $\text{GF}(q), (q=\prod^n, \forall \text{any prime}).$

In the first chapter we define the density of a set of primary polynomials (polynomials with leading coefficient 1) as the greatest lower bound of the number of primary polynomials of degree $n$ in the set divided by the total number of primary polynomials of degree $n$. We show that a set of polynomials satisfying certain conditions is a basis for the entire set of primary polynomials.

In the second chapter, we show that the number of polynomials of degree $n$ with coefficients in $\text{GF}(q)(q \neq 2)$ which can be written as

$$p + p'$$

where $p$ and $p'$ are irreducibles and $\deg p \neq \deg p'$ is $>C_{18}q^n$.

Using the results of the first two chapters we show in chapter three that the number of irreducibles needed to write any polynomial $f$ with coefficients in $\text{GF}(q)(q \neq 2)$ as

$$f = p + \sum p' (\deg p' < \deg p)$$

is at most $C_{20}$ ($C_{20}$ depends only on $q$).

We wish to acknowledge the use we have made of the Bruns, Landau, and Schnirelmann material in order to obtain our results.
CHAPTER I

A. Density of Sets of Primary Polynomials.

Let A be a set of polynomials with coefficients in GF(q), and A' the set of primary polynomials contained in A. Denote by A(n) the set of polynomials of degree n contained in A, and by \([A(n)]\) the number of polynomials in \(A(n)\). We see that the inequality,

\[0 \leq \frac{[A'\,(n)]}{q^n} \leq 1\]

holds. Analogous to the "Schnirelmann Density" for the sequence of natural numbers we define the greatest lower bound of all values of the above fraction to be the density of the set \(A'\), i.e.

\[d(a) = \text{g.l.b.} \frac{[A(n)]}{q^n}\]

Let \(B' \subset B\) be defined as above and \(C'(n)\) be the set of primary polynomials of the form \(A'(n) + \hat{B}(n-1)\) where \(\hat{B}(n-1)\) is the set of polynomials of degree \(\leq n-1\) contained in \(B\), \((\hat{B}(n-1) = \emptyset\) for \(n=0\)). Our first objective is to develop a tool for estimating the density of \(C'\) from the density of \(A'\) and \(B'\).

In order to proceed in this direction we assume \(A'(n)\) is not empty, and

---

1) If $fcB$, $afB$ where $a \in GF(q), (a=0 \Rightarrow 0 \in B)$. Under these assumptions we are able to arrive at a crude but useful tool for estimating the density of $C$ from the density of $A'$ and $B'$. This device in the classical case is commonly referred to as the "Schnirelmann Inequality".²

**THEOREM 1.1:** $d(C) \geq d(A') + d(B') - d(A) d(B')$.

**Proof.** For simplicity we let $d(A') = \alpha, d(B') = \beta$. We assume $\alpha, \beta > 0$ (otherwise the theorem is trivial, so that $[A'(n)] \geq \alpha q^n, [B'(n)] \geq \beta q^n$.

We denote $x^n + a_1 x^{n-1} + \ldots + a_n \in A(n)$ by the $n+1$ tuples $(1, a_1, a_2, \ldots, a_n)$. Now all polynomials contained in $A'(n)$ are also in $C'(n)$, since zero is contained in $B$.

Let $A'(n)[1, a_1, \ldots, a_{i-1}]$ be the subset of $A'(n)$ with the first $i$ tuples having fixed values $1, a_1, \ldots, a_{i-1}$, i.e. $A'(n)[1, a_1, \ldots, a_{i-1}]$ consists of all $n+1$ tuples in $A'(n)$ of the form $(1, a_1, \ldots, a_{i-1}, a_1', \ldots, a_n')$. Now let $s_i, (s_i \leq q)$ be the number of different sets $A(n)[1, a_1, \ldots, a_{i-1}, a_1'] \in A(n)$. We let $q-s_i = e[1, a_1, \ldots, a_{i-1}]$, so that we can adjoin to $A(n), e[1, a_1, \ldots, a_{i-1}]$ sets of $[B(n-1)]$ polynomials since

²Ibid., p. 652.
B satisfies 1). Hence the total number of different polynomials not in $A(n)$ that can be adjoined to $A(n)$ in this way is given by

$$\sum_{i=1}^{q} \sum_{[l,a_1,\ldots,a_{l-1}]} e[1,a_1,\ldots,a_{l-1}] [B(n-1)]$$

so that $[C(n)] \geq [A'(n)] + \sum_{i=1}^{q} \sum_{[l,a_1,\ldots,a_{l-1}]} e[1,a_1,\ldots,a_{l-1}] [B(n-1)]$.

But by definition of density,

$$[B(n-1)] \geq \beta q^{n-1}$$

so that $[C(n)] \geq [A'(n)] + \sum_{[l,a_1,\ldots,a_{l-1}]} e[1,a_1,\ldots,a_{l-1}] \beta q^{n-1}$.

But $\sum_{[l,a_1,\ldots,a_{l-1}]} e[1,a_1,\ldots,a_{l-1}] q^{n-1} = q^n [A(n)],$ so our inequality can be written as,

$$[C(n)] \geq [A'(n)] + \beta (q^n - [A(n)])$$

$$\geq [A'(n)] + \beta q^n - \beta [A(n)]$$

$$= (1-\beta) [A'(n)] + \beta q^n.$$

Now since $[A'(n)] \geq \alpha q^n$ and $(1-\beta) \geq 0$ we have

$$[C(n)] \geq (1-\beta) \alpha q^n + \beta q^n$$

$$\geq \alpha q^n + \beta q^n - \alpha \beta q^n$$

or $\frac{[C(n)]}{q^n} \geq \alpha + \beta - \alpha \beta$
But since the above inequality holds for all $n$, we have

$$d(C') \geq d(A') + d(B') - d(A) d(B).$$

We write the inequality $d(C') \geq d(A') + d(B') - d(A) d(B)$ in the form,

$$\text{i}) \quad 1 - d(C') \leq \left\{1 - d(A')\right\} \left\{1 - d(B')\right\}.$$

We let $C_k'$ be the set of primary polynomials of form $A_1'(n) + A_2'(n-1) + \cdots + A_k'(n-1)$, where $0 < n < \infty$ and $A_1$ satisfies assumption 1), so that we are able to make the following useful extension of the above inequality:

$$1 - d(C_k') \leq \prod_{i=1}^{k} \left\{1 - d(A_i')\right\}.$$

(We show this by induction on $k$.) The inequality holds for $k=2$, (by i). Assume,

$$1 - d(C_{k-1}') \leq \prod_{i=1}^{k-1} \left\{1 - d(A_i')\right\}.$$

Now,

$$1 - d(C_k') \leq \left\{1 - d(C_{k-1}')\right\} \left\{1 - d(A_k')\right\}.$$

$$\leq \prod_{i=1}^{k-1} \left\{1 - d(A_i')\right\} \left\{1 - d(A_k')\right\} \text{ by induction hyp,}$$

$$\leq \prod_{i=1}^{k} \left\{1 - d(A_i')\right\}.$$

From this inequality we are able to arrive at the following theorem.

**THEOREM 2.1:** Every set $A$, with $d(A') = \infty > 0$, and satisfying 1) is a basis for the set of all primary polynomials.
We first prove the following lemma:

**Lemma 1.1.** If \([A'(n)] + [\hat{B}(n-1)] > q^n\), then
\[ [C'(n)] = q^n. \]

**Proof.** Let \(f_1, \ldots, f_r\) and \(g_1, \ldots, g_s\) \((r+s>q^n)\) be the different polynomials contained in \(A'(n)\) and \(\hat{B}(n-1)\) respectively. Now if \(h\) is any primary polynomial of degree \(n\), all of the polynomials
\[
f_1, f_2, \ldots, f_r
\]
\[
h-g_1, h-g_2, \ldots, h-g_s
\]
are primary of degree \(n\). But there are \(r+s>q^n\) polynomials in the above two rows, so that
\[ f_i = h-g_k \text{ for some } i \leq r \text{ and } k \leq s. \]
Hence \(h=f_1+g_k\), so that \(C'(n)=A'(n)+\hat{B}(n-1)=q^n\) since \(h\) was arbitrary.

We are now able to prove our theorem. If we write the inequality
\[
1-d(C'_k) \leq \prod_{i=1}^{k} \left\{ 1-d(A'_i) \right\}
\]
as
\[
d(C'_k) \geq 1-\prod_{i=1}^{k} \left\{ 1-d(A'_i) \right\}
\]
and set \(A'_i=A\) for \(i=1, \ldots, k\) we have
\[
d(C'_k) \geq 1-(1-\alpha)^k \text{ where } \alpha = d(A').
\]
Hence for \(\alpha > 0\), and \(k\) sufficiently large we have
\[
d(C'_k) \geq 1-(1-\alpha)^k > \frac{1}{2}.
\]
Now the above arguments hold not only for sets of primary polynomials, but for sets with any fixed leading coefficient. Hence since $A$ satisfies 1) we have

$$[\hat{C}_k(n-1)] > \frac{(q-1)}{2} \sum_{k=0}^{q^l} q^k + 1 > \frac{q^n}{2}.$$  

Thus by Lemma 1.1,

$$C_k'(n) + \hat{C}_k(n-1) = q^n.$$
CHAPTER II

A. Sets of Irreducible Polynomials.

We denote by $P$ the set of all irreducibles with coefficients in $GF(q)$, ($q\neq 2$) and by $P'$ the set of all primary irreducibles contained in $P$. It is well known that the number of primary irreducibles of degree $n$ is given by

$$2) \ [P(n)] = \frac{1}{n} \left\{ \sum_{d|n} \mu(d) q^{n/d} \right\}.$$

From this identity we are able to arrive at a series of lemmas which are fundamental in what follows.

Lemma 2.1. $[P(n)] > \left(\frac{q-2}{q-1}\right) \frac{q^n}{n} = c_1 \frac{q^n}{n}$.

Proof. From 2) we see that

$$[P'(n)] = \frac{1}{n} \left\{ q^{n-1} \sum_{d|n} \mu(d) q^{n/d} \right\},$$

$$> \frac{1}{n} \left\{ q^{n-1} \sum_{k=0}^{n-1} q^k \right\} = \frac{1}{n} \left\{ q^n \frac{q^{n-1} - 1}{q-1} \right\},$$

$$> \frac{q^n}{n} \left[ 1 - \frac{1}{q-1} \right] = \left(\frac{q-2}{q-1}\right) \frac{q^n}{n}.$$

Lemma 2.2. $[\hat{P}(n-1)] > \left(\frac{q-2}{q-1}\right) \frac{q^n}{n} = c_2 \frac{q^n}{n}$.

Proof. (We note that $\hat{P}(n-1) = \emptyset$, for $n<2$, and for $n=2$ the lemma is trivial.) For $n \geq 3$ we have

$$[\hat{P}(n-1)] > \left(\frac{q-2}{q-1}\right) (q-1) \sum_{j=1}^{n-1} \frac{q^j}{j} = (q-2) \sum_{j=1}^{n-1} \frac{q^j}{j}.$$
We let
\[ \sigma_{n-1} = \sum_{j=1}^{n-1} \frac{q^j}{j}, \] so that
\[(q-1) \sigma_{n-1} = \sum_{j=1}^{n-1} \frac{q^{j+1}}{j} - \sum_{j=1}^{n-1} \frac{q^j}{j}, \]
\[= \frac{q^n}{n-1} + \sum_{j=2}^{n-1} \left( \frac{1}{j-1} - \frac{1}{j} \right) q^j - q, \]
\[= \frac{q^n}{n-1} + \sum_{j=3}^{n-1} \frac{1}{j(j-1)} q^j + \left( \frac{q^2}{2} - q \right), \]
\[> \frac{q^n}{n-1} > \frac{q^n}{n}. \]

Hence
\[ [\hat{P}(n-1)] > (q-2) \sigma_{n-1} > \left( \frac{q-2}{q-1} \right) \frac{q^n}{n}. \]

**Lemma 2.3.** Let \( p_1, p_2, \ldots, p_w, \ldots \) be any ordering of the elements \( p \in P \) so that \( \deg p_1 \leq \deg p_1+1 \). Then
\[ \log_q 2w \leq C_3 \deg p_w. \]

**Proof.** We show first that \([\hat{P}(n)] \leq q^n\). For \( n=1 \), equality holds, so we let \( n \geq 2 \). From 2) we see that
\[ [\hat{P}(n)] < \frac{q^n}{n} + \frac{q^{n-1}}{n-1} + \ldots + q, \]
\[< q^n \left[ \frac{1}{n} + \frac{1}{(n-1)q} + \ldots + \frac{1}{q^{n-1}} \right], \]
\[< q^n \left[ \frac{1}{n} + \sum_{j=1}^{\infty} \frac{1}{q^j} \right]. \]
\[ \leq q^n \left( \frac{1}{2} + \frac{1}{q-1} \right) \leq q^n. \]

Hence
\[ 2w \leq 2q^{\deg p_w}, \]
and
\[ \log_q 2w \leq \deg p_w + \log_q 2 \leq C_3 \deg p_w, \]
where
\[ C_3 = 1 + \log_q 2. \]

**Lemma 2.4.** Let \( p \in P' \) and \( |p| = q^{\deg p} \). Then
\[
\left| \frac{\sum_{d \geq p \in N} \frac{1}{|p|} - \log n}{|p|} \right| \leq 1.
\]

**Proof.** We consider \( \sum_{j=1}^{n} \frac{1}{j} - \log n \). If we set \( s_n = \sum_{j=1}^{n} \frac{1}{j} - \log n \),
we see that \( s_{n-1} - s_n = - \frac{1}{n} - \log (n-1) + \log n \)
\[ = - \frac{1}{n} - \log (1 - \frac{1}{n}) = \frac{1}{2n^2} + \frac{1}{3n^3} + \ldots > 0, \]
so that \( \sum_{j=1}^{n} \frac{1}{j} - \log n \) decreases monotonically as \( n \) increases.

It is well known that
\[ \lim_{n \to \infty} \left( \sum_{j=1}^{n} \frac{1}{j} - \log n \right) = \gamma, \ (\gamma = \text{Euler Constant}), \]
so that
\[ 3) \ o \leq \gamma < \sum_{j=1}^{n} \frac{1}{j} - \log n \leq 1. \]

Thus, from 2) and 3) it follows that
\[
\sum_{d \geq p \in N} \frac{1}{|p|} - \log n \leq \sum_{j=1}^{n} \frac{1}{q^j} - \log n = \frac{q}{q^j} - \frac{1}{j} - \log n \leq 1,
\]
and since $[P'(n)] \geq \frac{1}{n} [q^n - \sum \frac{q^k}{k}] > \frac{q^n}{n} - \frac{q^\frac{n}{2}}{(q-1)n} > \frac{q^n}{n} - \frac{q^\frac{n}{2}}{q-1}$,

$$\sum_{\text{deg } p \neq n} \frac{1}{|p|} - \log n > \frac{n}{q} \sum_{j=1}^\infty \frac{q^j}{j} \left( \frac{1}{q^j} \right) - \log n - \frac{\sum q^j}{\sum_{j=1}^\infty (q-1)q^j} > -\frac{1}{(q-1)^2} > -1.$$  

Hence \[ \left| \sum_{\text{deg } p \neq n} \frac{1}{|p|} - \log n \right| \leq 1. \]

Lemma 2.5. \[ \sum_{\text{deg } p \neq n} \frac{1}{|p|} \left( 1 - \frac{1}{|p|} \right) \left\{ \begin{array}{c} \frac{1}{C_5 n} \\ \frac{1}{C_5 n} \end{array} \right\}, \] where \( C_5 = C_4 \).

Proof. We have

$$\left| \sum_{\text{deg } p \neq n} \log \left( 1 - \frac{1}{|p|} \right) + \sum_{\text{deg } p \neq n} \frac{1}{|p|} \right| = \left| \sum_{\text{deg } p \neq n} \log \left( 1 - \frac{1}{|p|} \right) + \frac{1}{|p|} \right|,$$

$$= \sum_{\text{deg } p \neq n} \sum_{m=2}^\infty \frac{1}{m|p|^m} \leq \sum_{\text{deg } p \neq n} \sum_{m=2}^\infty \frac{1}{|p|^m} \leq \sum_{\text{deg } p \neq n} \frac{1}{(|p|-1)|p|},$$

$$\leq \sum_{j=1}^n \frac{q^j}{(q^j-1)q^j} = \sum_{j=1}^n \frac{1}{(q^j-1)} \leq \sum_{j=1}^\infty \frac{1}{(q^j-1)} = \frac{1}{q-2}.$$

Thus \[ \log \prod_{\text{deg } p \neq n} \left( 1 - \frac{1}{|p|} \right) + \log n \leq \frac{1}{q-2} + 1 = \frac{q-1}{q-2} = C_4, \]
and \[ \log n \prod_{\text{deg } p \neq n} \left(1 - \frac{1}{|p|}\right) < C_4. \]

Hence
\[ \prod_{\text{deg } p \neq n} \left(1 - \frac{1}{|p|}\right) \leq \left(\frac{e}{n}\right)^{C_4}. \]

B. **Algebraic Theorems of Viggo Brun.**

**THEOREM 2.1:** Let 1) \( t > 0, \)

\[ k_0 > k_1 > \ldots > k_t, \]

\( T_s \) be given for \( k_t < s < k_0. \)

1) \( N_i^{(m)} = \begin{cases} 1 & \text{for } i = 0 \\ \prod_{k > s_1 > s_2 > \ldots > s_l > k_m} T_{s_1} \ldots T_{s_l} & \text{for } i > 0 \end{cases} \]

(For \( i > k_{m-1} - k_m \), we set \( N_i^{(m)} = 0; \) and for \( 1 \leq i \leq k_{m-1} - k_m \).

\( N_i^{(m)} \) is the \( i \)th elementary symmetric function of \( T_s \) with \( k_m < s < k_{m-1}. \))

---

111) $M_i^{(m)} = \begin{cases} 1 & \text{for } i = 0 \\ S_i > s^>_k T_s \cdots T_s_i & \text{for } 0 \leq i \leq t \end{cases}$

$s_j \leq k_{\left[ \frac{j-1}{2} \right]}$ for $1 \leq j \leq i$

(For $2m < i \leq t$, we set $M_{i}^{(m)} = 0$ since $\frac{i-1}{2} \geq m$ and $s_j \leq k_{\left[ \frac{i-1}{2} \right]} \leq k_m$.)

Then

$$\sum_{n=0}^{i} M_{n}^{(m-1)} N_{i-n}^{(m)} = M_{i}^{(m)}.$$  

**Proof.** For $1 \leq m \leq t$, $0 \leq n \leq i \leq 2m$ we have

$$N_{i-n}^{(m)} = \begin{cases} 1 & \text{for } n = i, \\ \Sigma T_{s} \cdots T_{s-i} & \text{for } n < i. \end{cases}$$

Now if $n+1 \leq j \leq i$, $j \leq 2m$ by hypothesis, so that

$$\left[ \frac{j-1}{2} \right] \leq m - 1,$$

$$s_j \leq k_{m-1}$$

and

$$s_j \leq k_{\left[ \frac{j-1}{2} \right]}.$$  

For $i = 0$, our theorem is trivial ($1 = 1$), and for $1 \leq m \leq t$, $0 \leq i \leq 2m$ we have

$$\sum_{n=0}^{i} M_{n}^{(m-1)} N_{i-n}^{(m)} = \sum_{n=0}^{i} \Sigma T_{s} \cdots T_{s-n} \Sigma T_{s} \cdots T_{s-n}$$

$s_j \leq k_{\left[ \frac{j-1}{2} \right]} \quad s_j \leq k_{\left[ \frac{j-1}{2} \right]}$
where for $n=0$ the first, and for $n=1$ the second factor under $\sum_{n=0}^{i} M(n-1) N_{i-n} = \sum_{s_{i} \leq k_{m-1}} T_{s_{i}} ... T_{s_{i}} = M_{1}$ has value 1. Therefore

$$\sum_{n=0}^{i} M(n-1) N_{i-n} = \sum_{s_{i} \leq k_{m-1}} T_{s_{i}} ... T_{s_{i}} = M_{1}$$

since for every system $s_{1}, ..., s_{i}$ with $s_{1} > ... > s_{i} > k_{m}$,

either $k_{m-1} > s_{1}$ ($n=0$), or $s_{n} > k_{m-1} > s_{n+1}$ where $0 < n < i, s_{i} < k_{m-1}$.

**THEOREM 2.2:** If under the hypothesis of Theorem 2.1 we set

$$M(m) = \sum_{i=0}^{2m} (-1)^{i} M_{1}$$

we have for $1 \leq m \leq t$

$$M(m-1) \prod_{k_{m} < s_{i} < k_{m-1}} (1 - T_{s}) = M(m) = \sum_{n=0}^{2m-2} (-1)^{n} M(m-1) \sum_{u=2m-n+1}^{\infty} (-1)^{u} N_{u}.$$

**Proof.** Since $2m > 2m-1 > 2(m-1)$,

$$M(2m-1) = M(2m) = 0.$$

Now according to Theorem 2.1, we have

$$M(m) = \sum_{i=0}^{2m} (-1)^{i} M_{1} = \sum_{i=0}^{2m} (-1)^{i} \sum_{n=0}^{\infty} M(m-1) N_{i-n},$$

$$= \sum_{n=0}^{2m} (-1)^{n} M(m-1) \sum_{i=n}^{2m} (-1)^{i-n} N_{i-n}.$$
$M(m-1) = \sum_{n=0}^{2m-2} (-1)^n M_n^{(m-1)} \sum_{i=n}^{2m} (-1)^{i-n} N_{i-n}^{(m)}$.

Now

$M(m-1) = \sum_{n=0}^{2m-2} (-1)^n M_n^{(m-1)}$,

and

$\prod_{k_m \leq s \leq k_{m-1}} (1-T_s) = \sum_{u=0}^{\infty} (-1)^u N_u^{(m)}$

so that

$M(m-1) \prod_{k_m \leq s \leq k_{m-1}} (1-T_s) = \sum_{n=0}^{2m-2} (-1)^n M_n^{(m-1)} \sum_{u=0}^{\infty} (-1)^u N_u^{(m)}$

$= \sum_{n=0}^{2m-2} (-1)^n M_n^{(m-1)} \sum_{u=0}^{2m-2} (-1)^u N_u^{(m)} + \sum_{n=0}^{2m-2} (-1)^n M_n^{(m-1)} \sum_{u=2m-n+1}^{\infty} (-1)^u N_u^{(m)}$

$= M(m) + \sum_{n=0}^{2m-2} (-1)^n M_n^{(m-1)} \sum_{u=2m-n+1}^{\infty} (-1)^u N_u^{(m)}$.

**Theorem 2.3:** Let $t > 0$

$k_0 > k_1 > \ldots > k_t$

$0 < T_s < 1$ for $k_t < s \leq k_0$

$L_m = \prod (1-T_s) \geq \frac{1}{2}$ for $1 \leq m \leq t$.

Let $M(t)$ be defined as in Theorem 2.2. Then

$|M(t)| < 2 \sum_{i=1}^{t} L_i$.

**Proof.** Under the hypothesis of our preceding Theorem,
we have for \(1 \leq m \leq t\)

\[
\alpha \left( N^{(m)} \right) = \sum_{k_{n_{j+1}}^{<k_{m-1}}} T_{s} \leq - \sum_{k_{n_{j+1}}^{<k_{m-1}}} \log(1-T_s) = - \log L_{m} \log(1+\frac{1}{t}) < \frac{1}{t}.
\]

Thus for \(u>0\)

\[
u! N^{(m)} = u! \sum_{k_{n_{j+1}}^{<k_{m-1}}} T_{s} \leq \left( \sum_{k_{n_{j+1}}^{<k_{m-1}}} T_{s} \right)^{u} < \frac{1}{4^{u}}.
\]

Furthermore, for \(1 \leq m \leq t\)

\[
\sum_{k_{n_{j+1}}^{<k_{m-1}}} T_{s} = \sum_{n=1}^{m-1} N^{(1)} < \frac{m-1}{4}.
\]

We have, therefore, for \(0 \leq n \leq 2m-2\)

\[
\left| \sum_{n=2m-n+1}^{\infty} (-1)^{u} N^{(m)}_{n} \right| < \sum_{n=2m-n+1}^{\infty} \frac{1}{u!} \frac{1}{4^{u}} < \frac{1}{(2m-n)!} \sum_{n=1}^{(2m-n)+1} \frac{1}{4^{n}}
\]

\[
= \frac{1}{(2m-n)!} \left( \frac{1}{3} \frac{1}{4^{2m-n+1}} < \frac{1}{(2m-n)!} \frac{1}{4^{2m-n}} \right)
\]

and for \(0 \leq n \leq 2m-2\)

\[
n! M^{(m-1)}_{n} \leq n! \sum_{k_{n_{j+1}}^{<k_{m-1}}} T_{s} \leq \left( (m-1)^{n} \right).
\]

Hence \(n! M^{(m-1)}_{n} \leq \sum_{k_{n_{j+1}}^{<k_{m-1}}} T_{s} \leq (m-1)^{n} \)

From Theorem 2.2 we have

\[
\left| M^{(m-1)} - M^{(m)} \right| = \left| \sum_{n=0}^{2m-2} (-1)^{n} M^{(m-1)} \sum_{n=2m-n+1}^{\infty} (-1)^{u} N^{(m)}_{n} \right|
\]

\[
\leq \sum_{n=0}^{2m-2} \frac{(m-1)^{n}}{n!} \frac{1}{4^{2m-n}} \leq \frac{1}{4^{2m}} \sum_{n=0}^{2m} \frac{(m-1)^{n}}{n!(2m-n)!}
\]
\[ V_2 \sum_{n=0}^{2m} \binom{2m}{n} (m-1)^n = \frac{1}{(2m)!} \left( \frac{4}{(2m)^2} \right)^{2m} \]

\[ = \frac{1}{(2m)!} \frac{m^{2m}}{4^{2m}} < \frac{e^{2m}}{(2m)^{2m}} \frac{m^{2m}}{4^{2m}} = \left( \frac{e}{8} \right)^{2m} < \left( \frac{1}{2} \right)^{2m} = \frac{1}{4^m}. \]

Hence for \( 1 \leq m \leq t \), it follows that

\[ |M(m)| < |M(m-1)| L_m + \frac{1}{4^m} \]

and

\[ \frac{|M(m)|}{\prod_{i=1}^{t} L_i} - \frac{|M(m-1)|}{\prod_{i=1}^{t-1} L_i} < \frac{1}{4^m \prod_{i=1}^{t-1} L_i} \leq \frac{1}{4^m} \left( \frac{5}{16} \right)^m < \frac{1}{2^m}. \]

Summation over \( m \) from 1 to \( t \) gives

\[ \prod_{i=1}^{t} \frac{|M(t)|}{L_i} - 1 < \sum_{m=1}^{t} \frac{1}{2^m} < 1 \]

\[ |M(t)| < 2 \prod_{i=1}^{t} L_i. \]

C. Method of Viggo Brun.\(^2\)

Let \( n > 0 \)

\( f \) be a primary polynomial of degree \( n \),

\( |f| = q^n \) (The number of different residue classes (mod \( f \))),

\( d \) be any primary polynomial,

\(^2\)Ibid., p. 47.
$h$ be a polynomial of degree $< \text{degree } d$,

$k \geq 0$.

In case $k>0$, let $p_1, p_2, \ldots, p_k$ be different primary irreducibles prime to $d$. Let $F(d; p_1, \ldots, p_k)$, $(F(d)$ for $k=0)$ be the number of polynomials $g$ with

$0 \leq \deg g \leq n$, $g \equiv h \pmod{d}$, $g(f-g) \not\equiv 0 \pmod{p_r}$ for $1 \leq r \leq k$,

and with $g$ of degree $n$ primary.

We do not include $h$ and $f$ in our notation since $f$ is fixed and $h$ plays a minor role in our arguments. The expression $uF(d; p_1, \ldots, p_k)$, $(uF(d)$ for $k=0$ denotes the sum of $u$ functions $F(d; p_1, \ldots, p_k)$, $(F(d))$ with the same $f$ but not necessarily the same $h$. If $d=1$, $F$ is independent of $h$.

Let

\[ v_r = \begin{cases} 
2 & \text{if } p_r \nmid f, \\
1 & \text{if } p_r \mid f,
\end{cases} \]

which in each case is exactly equal to the number of residue classes $\pmod{dp_r}$ with

$g \equiv h \pmod{d}$, $g(f-g) \equiv 0 \pmod{p_r}$.

We show this as follows:

1) If $p_r \mid f$ and $g(f-g) \equiv 0 \pmod{p_r}$, $p_r \mid g$. But $(d, p_r)=1$ so that the set of congruences $g \equiv h \pmod{d}$, $g \equiv 0 \pmod{p_r}$ has a unique solution $\pmod{dp_r}$ by the Chinese Remainder Theorem.
ii) If \( p_r \mid f \) and \( g(f-g) \equiv o(\text{mod } p_r) \), \( p_r \mid g \) or \( p_r \mid f-g \).

But as above, each set of congruences \( g \equiv h(\text{mod } d) \), \( g \equiv o(\text{mod } p_r) \) and \( g \equiv o(\text{mod } d) \), \( g \equiv f(\text{mod } d) \) have solutions (mod \( dp_r \)).

**THEOREM 2.4:** \[
\left| F(d) - \frac{2^{\lfloor \frac{n}{d} \rfloor}}{1} \right| < 1.
\]

**Proof.** Since \( g = h + td \), deg \( d > \text{deg } h \), \( d \) and all \( g \) of degree \( n \) are primary, we have for

i) deg \( d = n \), \( F(d) = 2 \) so that \( F(d) - \frac{2^{\lfloor f \rfloor}}{\lfloor d \rfloor} = 0 \),

ii) deg \( d < n \), \( F(d) = 2q^{n - \text{deg } d} \) so that \( F(d) - \frac{2^{\lfloor f \rfloor}}{\lfloor d \rfloor} = 0 \),

iii) deg \( d > n \), \( F(d) = 1 \) or \( 0 \), so that \( F(d) - \frac{2^{\lfloor f \rfloor}}{q^{\text{deg } d - n}} < 1 \).

**THEOREM 2.5:** For \( k > 0 \),

\[
F(d; p_1, \ldots, p_k) = F(d; p_1, \ldots, p_{k-1}) - v_k F(d; p_1, \ldots, p_{k-1}).
\]

**Proof.** \( F(d; p_1, \ldots, p_k) \) is equal to the number of \( g \)'s with \( 0 \leq \text{deg } g \leq n \), \( g \) of degree \( n \) primary, \( g \equiv h(\text{mod } d) \), and \( g(g-f) \not\equiv o(\text{mod } p_r) \) for \( 1 \leq r < k \) decreased by the number of the above \( g \)'s with \( g(g-f) \equiv o(\text{mod } p_k) \)

(The number of \( g \) s to be subtracted is exactly \( v_k F(d; p_1, \ldots, p_{k-1}) \)).
THEOREM 2.6: \( F(d; p_1, \ldots, p_k) = F(d) - \sum_{i \leq \eta \leq k} v_{\eta} F(dp_{\eta}; p_1, \ldots, p_{\eta-1}) \).

Proof. If \( k = 0 \), the theorem is trivial (\( F(d) = F(d) \)). We assume the theorem true for \( k-1 \), and prove it true by \( k \). By Theorem 2.5
\[ F(d; p_1, \ldots, p_k) = F(d; p_1, p_2, \ldots, p_{k-1}) - v_k F(dp_k; p_1, \ldots, p_{k-1}) \]
But \( F(d; p_1, p_2, \ldots, p_{k-1}) = F(d) - \sum_{i \leq \eta \leq k-1} v_{\eta} F(dp_\eta; p_1, \ldots, p_{\eta-1}) \) by induction hypothesis, so that the theorem follows.

THEOREM 2.7: \( F(d; p_1, \ldots, p_k) = F(d) - \sum_{i \leq \eta \leq k} v_{\eta} F(dp_{\eta}) \)

+ \( \sum_{1 \leq \eta' < \eta \leq k} v_{\eta'} v_\eta F(dp_{\eta'}; p_1, \ldots, p_{\eta'-1}) \).

Proof. Application of Theorem 2.6 gives
\[ F(d; p_1, \ldots, p_k) = F(d) - \sum_{i \leq \eta \leq k} v_{\eta} F(dp_{\eta}) \]
- \( \sum_{1 \leq \eta' < \eta \leq k} v_{\eta'} v_\eta F(dp_{\eta'}; p_1, \ldots, p_{\eta'-1}) \).

THEOREM 2.8: Let \( t > 0 \)
\[ k = k_0 > k_1 > \ldots > k_{t-1} > k_t > 0 \]
then \( F(1; p_1, \ldots, p_k) \leq F(1) + \frac{2^{k-1}}{2} \sum_{i=1}^{k-1} (-1)^i \sum_{1 \leq \eta' \leq \eta \leq k} v_{\eta'} v_\eta v_{r_{k_t}} \cdots v_{r_{k_t}} F(p_{r_{k_t}} \cdots p_{r_{k_t}}) \]
+ \( \sum_{1 \leq \eta' \leq \eta \leq k} v_{\eta'} v_\eta F(p_{r_{k_t}} \cdots p_{r_{k_t}}; p_1, \ldots, p_{\min(r_{k_t} - 1, k_t)}) \)

where the \( r_j \)'s satisfy the following conditions
\[ r_1 > r_2 \cdots > r_{2t} > 0 \]

4) \[ r_j \leq k \left[ \frac{r_{j-1}}{2} \right] \text{ for } 1 \leq j \leq 2t. \]

**Proof.** (By induction on \( t \)). We let \( d = 1 \), so by Theorem 2.7 we have

\[
F(1; p_1, p_2, \ldots, p_k) = F(1) - \sum_{1 \leq r_i \leq k} v_i F(p_i) + \sum_{1 \leq r_i \leq k} v_i v_{r_i} F(p_{r_i} p_{r_i} p_1, \ldots, p_{r_i-1})
\]

and certainly

\[
F(p_{r_1} p_{r_2} p_1, \ldots, p_{r_i-1}) \leq F(p_{r_1} p_{r_2} p_1, \ldots, p_{\min(r_{r_i-1}, k_i)})
\]

so that theorem is true for \( t = 1 \). Now if the theorem is true for \( t \), it follows for \( t+1 \), since from Theorem 2.7 we have

\[
F(p_{r_1} \cdots p_{r_{2t}}, p_1, \ldots, p_{\min(r_{2t-1}, k_t)})
\]

\[
= F(p_{r_1} \cdots p_{r_{2t}}) - \sum_{r_{2t+1}} v_{r_{2t+1}} F(p_{r_1} \cdots p_{r_{2t+1}}) + \sum_{r_{2t+1}, r_{2t+2}} v_{r_{2t+1}} v_{r_{2t+2}} F(p_{r_1} \cdots p_{r_{2t+2}}, p_1, \ldots, p_{r_{2t+1}})
\]

where case \( r_{2t+1} \) and \( r_{2t+2} \) take on all integral values in the ranges:

\[ 1 \leq r_{2t+1} \leq \min(r_{2t-1}, k_t) \]

\[ 1 \leq r_{2t+2} \leq r_{2t+1} - 1 = \min(r_{2t+1} - 1, k_t). \]

Now we can replace \( p_{r_{2t+2}} \) by \( p_{\min(r_{2t+1} - 1, k_t)} \) behind the last
comma in 5) without decreasing $F$, so that theorem follows.

**THEOREM 2.9:** Under the hypothesis of Theorem 2.8

$$F(1;p_1,\ldots,p_k) \leq F(1) + \sum_{i=1}^{\frac{2t}{2}} (-1)^i \sum_{\eta_1,\ldots,\eta_t} v_{r_1} \cdots v_{r_t} F(p_{r_1} \cdots p_{r_t})$$

where the $r_i$'s satisfy conditions 4).

**Proof.** $F(p_{r_1} \cdots p_{r_t}) \geq F(p_{r_1} \cdots p_{r_t}; p_1,\ldots,p_{\min(r_t-1,k_i)})$ so that the proof follows from Theorem 2.8.

**THEOREM 2.10:** Let the hypothesis of Theorem 2.8 be satisfied, and the $r_i$'s satisfy conditions 4). Set

$$S = 1 + \sum_{i=1}^{\frac{2t}{2}} (-1)^i \sum_{\eta_1,\ldots,\eta_t} v_{r_1} \cdots v_{r_t} \left(\frac{v_{r_1}}{|p_{r_1}|} \cdots \frac{v_{r_t}}{|p_{r_t}|}\right)$$

then $F(1,p_1,\ldots,p_k) \leq 2q^n S + 2 \Pi_{m=0}^{t-1} (2k_m)^2$.

**Proof.** From Theorems 2.3 and 2.9 we have

$$F(1;p_1,\ldots,p_k) \leq 2q^n S + \sum_{i=1}^{\frac{2t}{2}} (-1)^i \sum_{\eta_1,\ldots,\eta_t} v_{r_1} \cdots v_{r_t} \left(\frac{2q^n}{|p_{r_1}|} \cdots \frac{2q^n}{|p_{r_t}|}\right)$$

$$= 2q^n S + \sum_{i=1}^{\frac{2t}{2}} \sum_{\eta_1,\ldots,\eta_t} v_{r_1} \cdots v_{r_t} \leq 2q^n S + \sum_{i=1}^{\frac{2t}{2}} 2^i$$

$$\leq 2q^n S + \sum_{i=1}^{\frac{2t}{2}} k_0 k_1 k_2 \cdots k_{t-1} k_t$$

by conditions 4),
\[ < 2q^n + 2^{2t+1} \prod_{m=0}^{t-1} k_m^2 \]

\[ = 2q^n + 2 \prod_{m=0}^{t-1} (2k_m)^2 \]

D. **Number of Polynomials in** \( P(n) + \hat{P}(n-1), (n>2) \).

**THEOREM 2.11:** Let \( \deg f > 2 \), and \( p_1, \ldots, p_k \) be an ordering of the set of primary irreducibles \( (\deg p_i < \deg p_{i+1}) \) with

\[ 1 \leq |p| \leq q^{n/C_7} \]

for a given constant \( C_7 > 1 \). Then

\[ F(1; p_1, \ldots, p_k) < C_13 \frac{q^n}{n^2} \sum_{g \in f} \frac{1}{|g|}. \]

**Remark.** If \( C_7 \) decreases, \( q^{n/C_7} \) increases so that \( F(1; p_1, \ldots, p_k) \) does not increase.

**Proof.** i) For \( 2 \leq \deg f < 3C_7 \), we set

\[ F(1; p_1, \ldots, p_k) < C_9 < C_{10} \frac{q^n}{n^2} \sum_{g \in f} \frac{1}{|g|}. \]

ii) For \( \deg f \geq 3C_7, k > 0 \), so for \( 1 \leq i < k \) we set

\[ \frac{v_i}{|p_i|} = T_i \]
so that \(1-T_1 \geq 1 - \frac{2}{11} > \frac{4}{5}\). We now set \(k=k_0\) and let \(k_1\) be the smallest number \(\geq 0\) with

\[
L_1 = \prod_{k_1 \leq s \leq k_0} (1-T_s) \geq \frac{4}{5}.
\]

According to this \(k_1 < k_0\), so if \(k_1 > 0\) let \(k_2(<k_1)\) be the smallest number \(\geq 0\) with

\[
L_2 = \prod_{k_2 \leq s \leq k_1} (1-T_s) \geq \frac{4}{5}.
\]

If we continue this process we arrive at the following set of numbers,

\[
t > 0
\]

\[
k_0 > k_1 > \ldots > k_t > 0
\]

with \(L_m = \prod_{k_m \leq s \leq k_{m-1}} (1-T_s) \geq \frac{4}{5}\) for \(1 \leq m \leq t\).

We see, therefore, that the hypotheses of Theorem 2.8 are satisfied. Besides we have for \(1 \leq m \leq t-1\)

\[
(1-T_{k_m}) L_m = \prod_{k_m \leq s \leq k_{m-1}} (1-T_s) < \frac{4}{5}.
\]

and \(L_m < \frac{\frac{4}{5}}{1-T_{k_m}} < \frac{\frac{4}{5}}{9/11} = \frac{\frac{4}{5}}{1} = (1- \frac{3}{135}) < (1- \frac{1}{135})^3\).

Now from Theorem 2.10 we see that \(S=M(t)\), (Since for \(M(t)\), the notation \(s_i > k_t \Rightarrow s_i > 0\)), and Theorem 2.3 gives

\[
|S| < 2 \prod_{i=1}^{t} L_i.
\]
It follows from Theorem 2.10 that

\[ F(1; p_1, \ldots, p_k) < 4q^n \prod_{i=1}^t L_i + 2 \prod_{m=0}^{t-1} (2k_m)^2. \]

We now proceed to find upper bounds for

\[ 4q^n \prod_{i=1}^t L_i \text{ and } 2 \prod_{m=0}^{t-1} (2k_m)^2. \]

**Lemma 2.6.** \( 2 \prod_{m=0}^{t-1} (2k_m)^2 < C_8 \frac{q^n}{n^2} \)

**Proof.** From Lemma 2.5, we have

\[ \frac{1}{C_7^n} < \prod_{\|P\| \leq q^m} (1 - \frac{1}{|P|}) < \frac{C'_7}{m} \]

and from Lemma 2.3, \( C_3 \deg p_w > \log_2 w \), so that

\[ \prod_{\|P\| \leq q^m} (1 - \frac{1}{|P|}) < \frac{C'_7}{\deg p_w} < \frac{C_6}{\log_2 2^{-w}}, \text{ where } (C_6 = C_3 C'_7). \]

If we set \( \prod_{s=1}^\infty (1 - \frac{1}{|P_s|}) = \lambda \), we see that

\[ \log_q (2k_m) < \frac{C_6}{\prod_{s=1}^m (1 - \frac{1}{|P_s|})} = \frac{C_6}{\lambda} \prod_{j=1}^m \prod_{k_j \leq k_{j+1}} (1 - \frac{1}{|P_j|}). \]

On the other hand, \( (1 - \frac{1}{|P_s|})^3 < 1 - \frac{3}{|P_s|^2} + \frac{3}{|P_s|^3} < 1 - \frac{3}{|P_s|^2} - \frac{1}{|P_s|} \)

\[ = 1 - \frac{2}{|P_s|} < 1 - \frac{V_s}{|P_s|} = 1 - T_s, \]

so for \( 0 < m < t - 1 \),
\[
\log_q(2k_m) < \frac{C_6}{\lambda} \left( \prod_{j=1}^{\Pi} I_j \right) \leq \frac{C_6}{\lambda} \left( 1 - \frac{1}{135} \right)^m.
\]

Hence \[
\log_q \prod_{m=0}^{t-1} (2k_m)^2 < \frac{2C_6}{\lambda} \sum_{m=0}^{\infty} \left( 1 - \frac{1}{135} \right)^m = \frac{270C_6}{\lambda}
\]

and \[
2 \prod_{m=0}^{t-1} (2k_m)^2 < 2q \frac{270C_6}{\lambda}.
\]

From Lemma 2.5, we have
\[
\frac{1}{\lambda} = \frac{1}{\prod_{|p| \leq q^{C_7}} (1 - \frac{1}{|p|})} = \frac{C_7}{C_6 n}
\]

so if we set \( C_7 = 1 + 270C_6^2 \) we have
\[
2 \prod_{m=0}^{t-1} (2k_m)^2 < 2q \frac{270C_6^2}{(1 + 270C_6^2)} \leq C_8 \frac{q^n}{n^2},
\]

where \( C_8 = 2(1 + 270C_6^2)^2 \), since for \( n \geq 3(1 + 270C_6^2) \)
\[
\frac{n}{1 + 270C_6^2} \geq \left( \frac{n}{1 + 270C_6^2} \right)^2.
\]

**Lemma 2.7.** \( n! q^n \prod_{i=1}^{t} I_i < C_{13} \frac{q^n}{n^2} \sum_{g|f} \frac{1}{|g|}. \)

**Proof.** \[
\prod_{i=1}^{t} I_i = \prod_{s=i}^{n} \left( 1 - \frac{v_s}{|p_s|} \right) \leq \prod_{s=i}^{n} \left( 1 - \frac{1}{|p_s|} \right)^{v_s} = \frac{\prod_{s=i}^{n} \left( 1 - \frac{1}{|p_s|} \right)^{v_s}}{\prod_{1 \leq |p| \leq q^{C_7}} \left( 1 - \frac{1}{|p|} \right)^{v_s}} \leq \frac{\lambda^2}{\prod_{p|f} \left( 1 - \frac{1}{|p|} \right)}.
\]
Now from above

\[ \lambda^2 = \left( \prod_{|p| \neq 0} \frac{1}{|p|} \left(1 - \frac{1}{|p|}\right)^2 \right) < \frac{C_6^2}{n^2/C_7^2} = \frac{C_{11}}{n^2} \]

and

\[ \frac{1}{\prod \frac{1}{|p|} \left(1 - \frac{1}{|p|} \right)^2} = \prod \frac{1}{|p|} \left(1 - \frac{1}{|p|} \right)^2 \left(1 + \frac{1}{|p|} \right) \]

But

\[ \prod \frac{1}{|p|} \left(1 - \frac{1}{|p|^2} \right) \leq \sum \frac{1}{|g|^2} = \sum q^j \frac{q^j}{q^{2j}} \leq \frac{q}{q-1} \]

and

\[ \prod \frac{1}{|p|} \left(1 + \frac{1}{|p|} \right) \leq \sum \frac{1}{|g|} \]

We see therefore, that

\[ 4q^n \prod_{i=1}^{n} L_i < 4q^n \frac{C_{11}}{n^2} \left(\frac{q}{q-1}\right) \sum_{g \mid f} \frac{1}{|g|} = C_{12} \frac{q^n}{n^2} \sum_{g \mid f} \frac{1}{|g|} \]

where \( C_{12} = 4(C_7C_6)^2 \left(\frac{q}{q-1}\right) \)

and

\[ F(1, p_1, \ldots, p_k) < C_{12} \frac{q^n}{n^2} \sum_{g \mid f} \frac{1}{|g|} + C_8 \frac{q^n}{n^2} \]

\[ < (C_{12} + C_8) \frac{q^n}{n^2} \sum_{g \mid f} \frac{1}{|g|} = C_{13} \frac{q^n}{n^2} \sum_{g \mid f} \frac{1}{|g|} \]

Since \( \sum_{g \mid f} \frac{1}{|g|} > 1 \), and \( C_{10} < C_{12} \).

**THEOREM 2.12.** Let \( N(f) \) be the number of solutions of

\[ f = p + p' \] where \( \deg p \neq \deg p' \).

Then for \( \deg f \geq 2 \)

\[ N(f) \leq C_{13} \frac{q^n}{n^2} \sum_{g \mid f} \frac{1}{|g|} \]
Proof. We now let $C_7 = 2$ and consider the following cases:

i) If $\deg f < 6 = 3C_7$, then

$$N(f) < \frac{q^6}{6} < C_{13} \frac{q^n}{n^2} \sum_{g|f} \frac{1}{|g|}$$

ii) If $\deg f \geq 6$, $f = p + p'$ where $\deg p$ or $p' \leq \frac{n}{2}$,

$$N(f) < 2q^{n/2} < C_{14} \frac{q^n}{n^2} \sum_{g|f} \frac{1}{|g|}$$

($C_{13} > C_{14}$ since $\frac{q^n}{n^2} > q^{n/2}$ for $n \geq 8$).

iii) If $\deg f \geq 6$, $f = p + p'$ where $\deg p$ and $p' > \frac{n}{2}$,

$$N(f) \leq F(1, p_1, \ldots, p_k) < C_{13} \frac{q^n}{n^2} \sum_{g|f} \frac{1}{|g|}$$

since $p_1, p_2, \ldots, p_k$ consists of all primary irreducibles such that $1 \leq |p_i| \leq q^{n/2}$, and $p_i \nmid p$, $p_i \nmid f - p = p'$.

Lemma 2.8. $\sum_{\deg f = n} N^2(f) < C_{16} \frac{q^{3n}}{n^4}$

Proof. Since $N(f) < C_{13} \frac{q^n}{n^2} \sum_{g|f} \frac{1}{|g|}$, we have

$$\sum_{\deg f = n} N^2(f) < \sum_{\deg f = n} C_{13} \frac{q^n}{n^2} \sum_{g|f} \frac{1}{|g|} \sum_{h|f} \frac{1}{|h|}$$
We let \( \{g, h\} \) be the least common multiple of \( g \) and \( h \) and observe that \( \deg \{g, h\} \geq \deg g, \geq \deg h \). Hence

\[
\deg \{g, h\} \geq \frac{1}{2} \deg (g \cdot h).
\]

It follows that

\[
\sum_{f \atop \deg f = n} \sum_{g | f} \frac{1}{|g|} \sum_{h \atop \deg h = n} \frac{1}{|h|} = \sum_{f \atop \deg f = n} \sum_{g | f} \frac{1}{|g|} \sum_{h \atop \deg h = n} \frac{1}{|h|} \sum_{f \mod \{g, h\}} \frac{1}{|\{g, h\}|} \cdot q^n
\]

\[
\leq \sum_{f \atop \deg f = n} \sum_{g | f} \frac{1}{|g|} \sum_{h \atop \deg h = n} \frac{1}{|h|} \cdot \frac{q^n}{|\{g, h\}|} \cdot \frac{1}{|g \cdot h|^{1/2}}
\]

\[
< q^n \sum_{f \atop \deg f = n} \frac{1}{|g|^{1/2}} \sum_{h \atop \deg h = n} \frac{1}{|h|^{1/2}} = C_{15} q^n
\]

where \( C_{15} = \left( \frac{q^{1/2}}{q^{1/2} - 1} \right)^2 = \frac{q}{(q^{1/2} - 1)^2} \).

Hence

\[
\sum_{f \atop \deg f = n} N^2(f) < C_{13} C_{15} \frac{3n}{n^4} = C_{16} \frac{3n}{n^4}.
\]

**Theorem 2.13**: Let \([\mathcal{P}(n)]\) be the number of primary polynomials contained in \( P(n) + \mathcal{P}(n-1) \). Then

\[
[\mathcal{P}(n)] \geq C_{18} q^n.
\]

**Proof.** From Lemma 2.1 and 2.2 we see that
\[
\sum_{f \in \mathcal{P}(n)} N(f) = \sum_{\deg(p) = n} \frac{q^n}{n} C_1 \frac{q^n}{C_2 n} = C_{17} \frac{q^{2n}}{n^2}
\]

where \( C_{17} = 2C_1 C_2 \).

Now by Lemma 2.8 and Schwartz's Inequality we have

\[
\frac{C_{17}^2 q^{4n}}{n^4} \leq \left( \sum_{f \in \mathcal{P}(n)} N(f) \right)^2 \leq [\mathcal{P}(n)] \sum_{f \in \mathcal{P}(n)} N^2(f) \leq [\mathcal{P}(n)] C_{16} \frac{q^{3n}}{n^4}
\]

so that

\[
\mathcal{P}(n) > \frac{C_{17}^2}{C_{16}} q^n = c_{18} q^n.
\]
CHAPTER III

A. Sums of Irreducible Polynomials.

We adjoin to the $P$ of irreducible polynomials the set $P(0) = \{a | a \in \text{GF}(q)\}$, (i.e. To the set $P'$ of primary irreducibles we adjoin $P(0)=1$.) From 2) we have

$$[P'(n)] \leq \frac{q^n}{n},$$

so that

$$d(P') = \text{g.l.b.} \frac{[P'(n)]}{q^n} \leq \text{g.l.b.} \frac{1}{n} = 0.\]

We have shown, however, that

$$d(P') = \text{g.l.b.} \frac{[P'(n)]}{q^n} \geq \text{g.l.b.} \frac{C_{18}q^n}{q^n} = C_{18}$$

where $P'(n) = P(n) + \hat{P}(n-1)$ so that we are able to prove the following important theorem.

**THEOREM 3.1:** The number of irreducibles needed to represent any polynomial $g$, ($\text{deg } g \geq 1$) in the form

$$g = p + \sum_{a < \text{deg } p' \leq \text{deg } p} p'$$

is at most $C_{20}(q)$.

**Proof.** The results of Theorem 2.14 hold not only for
primary irreducibles but for polynomials with any fixed leading coefficient so that \( \hat{P} \) satisfies condition 1).

If we let \( \hat{P}_k(n) = \hat{P}_1(n) + \hat{P}_2(n-1) + \cdots + \hat{P}_k(n-1) \) we have for \( k \) sufficiently large

\[
d(\hat{P}_k) \geq 1 - (1 - c_{18})^k > \frac{1}{2}.
\]

Hence by Lemma 1.1 we have that the number of irreducibles needed to represent \( g \) in the form

\[
g = p + \sum_{\text{deg } p' \leq \text{deg } p} (p' \text{or constant})
\]

is \( 2k = C_{19} \). Now if

\[
g = p + \sum_{\text{deg } p' \leq \text{deg } p} (p' + c),
\]

we write \( g = p + \sum_{\text{deg } p' \leq \text{deg } p} (x+c) + (-x) = p + \sum_{\text{deg } p' \leq \text{deg } p} p' \)

so that \( g \) can be written as the sum of \( C_{19} + 1 = C_{20} \) irreducibles.
B. List of Constants.

\[ C_1 = C_2 = \frac{q-2}{q-1} \]

\[ C_3 = 1 + \log q^2 \]

\[ C_4 = \frac{q-1}{q-2} \]

\[ C_5 = e^{C_4} \]

\[ C_5^* = \begin{cases} C_5 & \text{for } q \geq 11 \\ C_5 \prod_{|p| \leq 11} \left(1 - \frac{1}{1 - \frac{1}{|p|}}\right) & \text{for } q < 11 \end{cases} \]

\[ C_6 = C_3 \cdot C_5 \]

\[ C_7 = 1 + 270C_6^2 \]

\[ C_8 = 2(1 + 270C_6^2)^2 \]

\[ C_9 < C_{10} \frac{q^n}{n^2} \sum_{g | f} \frac{1}{|g|} \]

\[ C_{10} < C_{12} \]
\[ c_{11} = (c_6 \cdot c_7)^2 = \begin{cases} 
\left(1 + 270c_6^2(1 + \log q^2) \frac{q-1}{e^{q-2}}\right)^2 & \text{for } q \geq 11 \\
\left(1 + 270c_6^2(1 + \log q^2) \frac{q-1}{e^{q-2}} \frac{1}{|p|} \left(1 - \frac{1}{|p|}\right)\right)^2 & \text{for } q \leq 11 
\end{cases} \]

\[ c_{12} = \frac{4q}{q-1} c_{11} \]

\[ c_{13} = c_8 + c_{12} = \begin{cases} 
\left(1 + 270c_6^2\right)^2 \left(2 - \frac{4q}{q-1} \left(1 + \log q^2 \frac{q-1}{e^{q-2}}\right)^2\right) & \text{for } q \leq 11 \\
\left(1 + 270c_6^2\right)^2 \left(2 - \frac{4q}{q-1} \left(1 + \log q^2 \frac{q-1}{e^{q-2}} \frac{1}{|p|} \left(1 - \frac{1}{|p|}\right)\right)^2\right) & \text{for } q \leq 11 
\end{cases} \]

\[ c_{14} < c_{13} \]

\[ c_{15} = \frac{q}{(q^{1/2} - 1)^2} \]

\[ c_{16} = c_{13} \cdot c_{15} \]

\[ c_{17} = 2c_1c_2 \]

\[ c_{18} = \frac{c_{17}^2}{c_{16}} = \frac{2(q-4)^4 (q^{1/2} - 1)^2}{q(q-1)^4 \cdot c_{13}^2} \quad \text{As } q \text{ increases } c_{13} \text{ obviously decreases so that } c_{13}^2 \text{ decreases.} \]

\[ c_{19} = 2k > -2 \left[\frac{\log 2}{\log (1 - c_{18})}\right] \]

\[ c_{20} = c_{19} + 1 \]


Ray Paul Authement was born in Chauvin, Louisiana on November 19, 1928. He attended the public schools of Terrebonne Parish and was graduated from Terrebonne High School in 1946. He attended Southwestern Louisiana Institute, receiving his B.S. in 1950. During the academic year of 1950-51 he held an instructorship in Physics at Southwestern. He enrolled in the Graduate School at Louisiana State University in the summer of 1951, and received his M.S. in the summer of 1952. He is at present an instructor of mathematics at Louisiana State University.
Candidate: Ray Authement

Major Field: Mathematics

Title of Thesis: Sums of Irreducible Polynomials with Coefficients in GF(q).

Approved:

[Signatures of Major Professor and Chairman, Dean of the Graduate School]

EXAMINING COMMITTEE:

[Signatures of committee members]

Date of Examination: August 1, 1956,