EXPONENTIAL SUMS AND THE DISTRIBUTION OF SOLUTIONS OF CONGRUENCES

BY

TODD COCHRANE

R940606-2

INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
NANKANG, TAIPEI, TAIWAN
REPUBLIC OF CHINA
EXPONENTIAL SUMS AND THE DISTRIBUTION
OF SOLUTIONS OF CONGRUENCES

TODD COCHRANE
Kansas State University and Academia Sinica

ABSTRACT. In these notes we discuss the application of exponential sums to the problem of
determining the distribution of solutions of congruences. The notes are based in part on a
series of talks delivered at the Institute of Mathematics, Academia Sinica, Taipei, Taiwan
during the academic year 1993–94.

CONTENTS

1. Introduction
2. Method of finite fourier series
3. Zeta functions and the cardinality of algebraic sets
4. Exponential sums
   4.1. \( L \)-Functions
   4.2. The interplay between characteristic values and bounds on
        exponential sums
   4.3. Homogeneous exponential sums
   4.4. Hooley’s method of second moments and upper bounds on
        general exponential sums
   4.5. Exponential sums on tori
   4.6. Complete exponential sums
4.7. The sum \( S(V, y) \) and estimates for \(|V \cap B|\)
4.8. Upper bounds on \( S(V, y) \) for hypersurfaces
4.9. Algebraic sets defined over \( \mathbb{Z} \)
5. Weyl’s method and the work of Schmidt
6. The method of lattices for obtaining small solutions
7. Linear forms
8. Quadratic forms
9. Cubic forms
10. Diagonal congruences
11. Upper bounds on \(|V \cap B|\)

---

This research was partially funded by the United States National Security Agency and the National
Science Council of the Republic of China.

Typeset by \texttt{AMSTeX}
NOTATION

\( \mathbb{F}_p \) is the finite field in \( p \) elements, \( \mathbb{F}_q \) the finite field in \( q = p^r \) elements and \( \overline{\mathbb{F}}_q = \overline{\mathbb{F}}_p \) denotes its algebraic closure.

\( \mathbb{A}^n = \mathbb{F}_q^n = \) affine n-space, \( \mathbb{P}^n = \) projective n-space over \( \overline{\mathbb{F}}_q \).

Lower case \( \mathbf{x} = (x_1, \ldots, x_n) \) denotes a point in \( \mathbb{A}^n \), while capital \( X_1, \ldots, X_n \) denote indeterminates.

\( |\mathbf{x}| = \max |x_i| \)

\( |S| \) denotes the cardinality of a set \( S \)

\( \ll, \gg, \text{Big "Oh", and } c(n, s, ..) \) all denote constants depending only on \( n = \text{number of variables}, s = \text{number of polynomials}, \) and the degrees of the polynomials involved (and \( \epsilon \) if it appears).

We say that \( |V \cap B| \) is of the expected order if

\[
\frac{|B|}{p^n} |V| \ll |V \cap B| \ll \frac{|B|}{p^n} |V|.
\]

If \( \overline{V} \subset \mathbb{A}^n \) is an algebraic set defined by the polynomials \( f_1, \ldots, f_s \), over \( \mathbb{F}_q \) then we let \( V \) denote the points of \( \overline{V} \) with coordinates in \( \mathbb{F}_q \), \( \overline{V}_H \subset \mathbb{P}^n \) denote the algebraic set defined by the homogenizations of the polynomials \( f_1, \ldots, f_s \), and \( \overline{V}_\infty \subset \mathbb{P}^{n-1} \) denote the algebraic set defined by the maximal homogeneous parts of the polynomials \( f_1, \ldots, f_s \).

\[ e_p(x) = e^{2\pi i x/p} \text{ for } x \in \mathbb{F}_p, \quad \psi(x) = e_p(T\tau(x)) \text{ for } x \in \mathbb{F}_q, \text{ where } T\tau \text{ denotes the trace.} \]

\[ \mathbf{x} \in \mathbb{F}_p^n \]

\[ \sum_{\mathbf{x}} = \sum_{\mathbf{x} \in \mathbb{F}_p} \text{ or } = \sum_{\mathbf{x} \in \mathbb{F}_q} \]

\[ S(V, \mathbf{y}) = \sum_{\mathbf{x} \in V} e_p(\mathbf{x} \cdot \mathbf{y}) \text{ over } \mathbb{F}_p \text{ and } S(V, \mathbf{y}) = \sum_{\mathbf{x} \in V} \psi(\mathbf{x} \cdot \mathbf{y}) \text{ over } \mathbb{F}_q. \]

\[ \phi(V, \mathbf{y}) = \begin{cases} S(V, \mathbf{y}) & \text{for } \mathbf{y} \neq 0 \\ |V| - p^{n-s} & \text{if } \mathbf{y} = 0. \end{cases} \]

\[ \Phi(V) = \max_{\mathbf{y} \neq 0} |\phi(V, \mathbf{y})| \]

\[ H(\mathbf{y}) = \{ \mathbf{x} \in \mathbb{F}_p^n : \mathbf{x} \cdot \mathbf{y} = 0 \} \]
INTRODUCTION

Let \( f(x) = f(x_1, \ldots, x_n) \) be a polynomial with integer coefficients, \( p \) be a prime, \( Z_p(f) \) be the set of solutions in \( \mathbb{Z}^n \) of the congruence

\[
f(x) \equiv 0 \pmod{p},
\]

and

\[
B = \{ x \in \mathbb{Z}^n : a_i \leq x_i < a_i + b_i \}.
\]

Let \( |B| = \prod b_i \) denote the cardinality of the box \( B \). We call the box a cube of size \( b \) if \( b_i = b \) for all \( i \). In these notes we are interested in the following types of problems.

**Problem 1.** Find a small nonzero solution of (1.1), that is, a solution with \( \|x\| := \sup |x_i| \) small.

**Problem 2.** For a box \( B \) with sides of arbitrary lengths, how large must its cardinality be in order to guarantee that \( B \) contains a solution of (1.1).

**Problem 3.** Determine \( |Z_p(f) \cap B| \), the number of solutions of (1.1) contained in \( B \).

The point of view that interests us the most about these type of problems is given a particular polynomial \( f \) and prime \( p \), for instance a quadratic form in 4 variables or a nonsingular \( (\mod p) \) cubic form in 9 variables, what is the best we can say in answer to each of these problems. Of secondary interest, but also included in these notes, are results that are significant only if the number of variables is sufficiently large. We have also included results that hold for a general modulus but our primary interest is the case of prime moduli. The most powerful methods for addressing these problems entail the use of exponential sums and so a good portion of these notes are devoted purely to the study of exponential sums. There are two basic approaches here, one using Fourier series and leading to exponential sums over varieties of the type

\[
\sum_{x \in V} e_p(x \cdot y),
\]

where \( V \) is the set of points in \( \mathbb{F}_p^m \) satisfying (1.1), and the other making use of Weyl's method for bounding incomplete exponential sums of the type

\[
\sum_{x \in B} e_p(f(x)).
\]

The second method, developed primarily by W. M. Schmidt, has been discussed at length in the book of Baker (1986), *Diophantine Inequalities*, and so we only quote a few of the main results stemming from it in section 5.

We take up a detailed discussion of the method of finite Fourier series in section 2, a method that is primarily analytic in nature but which depends upon deep algebraic
results. Our point of view in this section is to work over the finite field $\mathbb{F}_p$, letting $V$ be the algebraic subset of $\mathbb{F}_p^n$ defined by (1.1) and viewing $B$ as a box of points imbedded in $\mathbb{F}_p^n$; here we require $b_i < p$ for all $i$. One could just as easily work over a more general finite field $\mathbb{F}_q = \mathbb{F}_{p^r}$ replacing $B$ with a box of points relative to a given basis for $\mathbb{F}_q$ over $\mathbb{F}_p$, and obtain the same results. But nothing new seems to be obtained by doing so and our final objective is that of congruences (mod $p$), so we have chosen not to do so. On the other hand we have found it advantageous to work with exponential sums over an arbitrary finite field and so we work over $\mathbb{F}_q$ in sections 3 and 4.

The success of the method of Fourier series depends upon determining the total number of points on the algebraic set $V$, a topic taken up in section 3 by means of the study of Zeta-functions, and upon determining good upper bounds on exponential sums of the type (1.3), a topic taken up in section 4. Generally such upper bounds are obtained by the study of the $L$-functions associated with the exponential sums. In particular one wishes to obtain upper bounds on the weights of the characteristic values associated with the $L$-functions. Our goal in sections 3 and 4 has been to make a thorough review on what is currently known about such issues and to include a number of new results and examples that cannot be found in the literature. Sections 3 and 4 can be read independently having much interest in their own right and having many applications beyond the problems of interest here.

In section 6 we discuss an elementary method using nothing more than Minkowski's theorem from the geometry of numbers for determining small solutions of homogeneous polynomial congruences. In sections 7, 8, 9, and 10 we discuss in turn linear, quadratic, cubic and diagonal congruences.

As one can see by browsing through the list of references, many papers have been published over the past 40 years dealing with the types of problems listed above and with the deep questions on exponential sums that arise from the study of these problems. Our goal here has been to summarize the methods and results of these investigations and whenever possible to push them a little further. We have tried to put together the many pieces that lie scattered throughout the literature. Whenever feasible, we have outlined proofs of the results stated here, but of course there are a number of fundamental theorems that we simply give references for, such as Deligne's proof of the Weil conjectures or Schmidt's very involved work on bounding incomplete exponential sums.

These notes are based in part on a series of talks delivered at The Institute of Mathematics, Academia Sinica, Taipei, Taiwan, during the academic year 1993–94, while the author was on sabbatical. The author wishes to thank Professor Jing Yu for sponsoring his visit to Academia Sinica and for suggesting and supporting this lecture series.
2. The Method of Finite Fourier Series

Fundamental Identities.
Let \( F = (f_1, \ldots, f_s) \) be an \( s \)-tuple of polynomials in \( \mathbb{F}_p[X_1, \ldots, X_n] \) and \( V = V(F) \) the algebraic subset of \( \mathbb{F}^n_p \) defined by

\[
f_1(x) = f_2(x) = \cdots = f_s(x) = 0.
\] (2.1)

Let \( B \) be the box of points in \( \mathbb{F}^n_p \) given by

\[
B = \{ x \in \mathbb{F}^n_p : a_i \leq x_i < a_i + b_i, 1 \leq i \leq n \}
\] (2.2)

for some integers \( a_i, b_i \) with \( 1 \leq b_i \leq p \); (the inequality in (2.2) is understood by identifying \( \mathbb{F}_p \) with an appropriate set of integer representatives). We say that \( B \) is a cube of size \( b \) if all of the \( b_i \) equal \( b \). Our interest is in determining the cardinality of the set \( V \cap B \) and in particular of determining how large \( |B| \) must be to guarantee that \( V \cap B \) is nonempty.

Let \( \alpha(x) \) be a real valued function defined on \( \mathbb{F}^n_p \) such that \( \alpha(x) \leq 0 \) for all \( x \) not in \( B \). In order to show \( V \cap B \) is nonempty it suffices to show \( \sum_{x \in V} \alpha(x) \) is positive. Now \( \alpha(x) \) has a finite Fourier expansion \( \alpha(x) = \sum_y a(y)e_p(x \cdot y) \) where \( a(y) = p^{-n} \sum_x \alpha(x)e_p(-x \cdot y) \), and we easily obtain the fundamental identity,

\[
\sum_{x \in V} \alpha(x) = p^{-n}|V| \sum_{x} \alpha(x) + \sum_{y \neq 0} a(y)S(V, y)
\] (2.3)

where

\[
S(V, y) = \sum_{x \in V} e_p(x \cdot y).
\]

This identity expresses the sum of \( \alpha(x) \) over \( V \) as a fraction of a complete sum over \( \mathbb{F}^n_p \) plus a certain error term. A variant of (2.3) that is sometimes more convenient to work with, especially if \( |V| \) is not apriori known, is

\[
\sum_{x \in V} \alpha(x) = p^{-s} \sum_{x} \alpha(x) + \sum_{y} a(y)\phi(V, y)
\] (2.4)

where

\[
\phi(V, y) = \begin{cases} 
S(V, y) & \text{for } y \neq 0 \\
|V| - p^{n-s} & \text{for } y = 0.
\end{cases}
\]

The reason (2.4) is sometimes more convenient is that we have the following formula: For any \( y \in \mathbb{F}^n_p \) (including \( y = 0 \))

\[
\phi(V, y) = p^{-s} \sum_{x \in \mathbb{F}^n_p} \sum_{\lambda \in \mathbb{F}^n_p} e_p(\lambda \cdot F(x) + x \cdot y).
\] (2.5)
Identities of the type (2.3) and (2.4) (in disguised forms) have appeared many places in the literature. In most of the early applications $\alpha$ was taken to be the characteristic function $\chi_B$ of the box $B$, whence (2.3) and (2.4) yield formulae for $|V \cap B|$. In this case, the first terms on the righthand sides of (2.3) and (2.4), $p^{-n}|B||V|$ and $p^{-s}|B|$ respectively, represent the expected value for $|V \cap B|$, the first being a more accurate representation if $|V|$ is not of the expected order $p^{n-s}$. Also, (2.4) in this case can be written

$$|V \cap B| = p^{-s}|B| + p^{-s} \sum_{\lambda \neq 0} \sum_{x \in B} e_p(\lambda \cdot F(x)).$$

(2.6)

Using the methods of Weyl one can attempt to bound the incomplete exponential sum appearing in (2.6) directly, without appeal to complete exponential sums. We take up a discussion of this mode of attack in section 5, but for now we shall focus on identities of the type (2.3).

**Basic Error Estimate.**

The simplest way to bound the error term

$$E(V) = \sum_{y \neq 0} a(y)S(V, y),$$

(2.7)

in (2.3) is to write

$$|E(V)| \leq \Phi(V) \sum_{y \neq 0} |a(y)|,$$

(2.8)

where $\Phi(V) = \max_{y \neq 0} |S(V, y)|$. Such a bound was used by Mordell (1957), Chalk (1963) and many others; see Chalk (1980) for further discussion. Now the Fourier coefficients of $\chi_B$ are given by

$$a_B(y) = p^{-n} \prod_{i=1}^{n} e_p \left( -\left( a_i + \frac{b_i}{2} - \frac{1}{2} \right) y_i \right) \frac{\sin(\pi b_i y_i / p)}{\sin(\pi y_i / p)}$$

where the term in the product is taken to be $b_i$ if $y_i = 0$. Thus, in order to estimate $\sum |a_B(y)|$ one needs to examine the Vinogradov sum $\sum |\sin \pi b y / p| / |\sin \pi y / p|$; see Vinogradov (1954, ex 12, chap. 15). In (1987, Theorem 1) we obtained the following sharp upper bounds:

$$\sum_{y=0}^{p-1} \frac{|\sin \pi b y / p|}{|\sin \pi y / p|} \leq \begin{cases} \frac{4}{\pi^2} p \log p + p, & \text{for all } p \\ p \log p, & \text{for } p > 3, \end{cases}$$

for any integer $b$; see also Peral (1990). It follows that for $p > 3$, $\sum_{y \neq 0} |a_B(y)| \leq (\log p)^n$, and so we obtain
Theorem 2.9. For any algebraic set $V$ defined by (2.1), with $p \neq 2, 3$, and any box $B$ of the type (2.2), we have
\[
|V \cap B| - \frac{|B|}{p^n} |V| \leq \Phi(V)(\log p)^n.
\] (2.10)

Many versions of this theorem are in the literature but usually they come with a big "Oh"; see the references above for a start.

If our goal is to simply show $V \cap B$ is nonempty for $|B|$ sufficiently large then $\chi_B$ is not the best choice for $\alpha$. It is better to let $\alpha$ be a weighted function such as
\[
\alpha(x) = \chi_{B_1} \ast \chi_{B_2}(x) = \sum_{u \in B_1} \sum_{v \in B_2} 1,
\] (2.11)
where $B_1 = \{0 \leq x_i < \left[ \frac{b_i + 1}{2} \right] \}$ and $B_2 = B_1 + (a_1, a_2, \cdots, a_n)$. By Parseval's identity, the Fourier coefficients $a(y)$ of $\alpha$ satisfy
\[
\sum_y |a(y)| = p^n \sum_y |a_{B_1}(y)|^2 = \sum_x |\chi_{B_1}(x)|^2 = |B_1|.
\]

Thus, by (2.3), (2.8) and the facts that $|B_1| \geq 2^{-n}|B|$ and $\sum_{x \in V} \alpha(x) \leq |B_1| |V \cap B|$, we obtain

Theorem 2.12. For any algebraic set $V$ and box $B$,
\[
|V \cap B| \geq 2^{-n} \frac{|B|}{p^n} |V| - \Phi(V).
\] (2.13)

In particular, $V \cap B$ is nonempty if
\[
|B| > 2^n p^n \Phi(V)/|V|,
\] (2.14)
and thus we have saved a factor of $(\log p)^n$ over (2.10). In fact (2.13) implies much more than just $V \cap B$ is nonempty. It says $V \cap B$ contains the expected number of points, up to the factor $2^{-n}$, for $|B|$ sufficiently large. To emphasize this fact we shall say that $|V \cap B|$ is of the expected order if upper and lower bounds of the type (2.15) hold with the constant $2^n$ replaced possibly by any constant depending only on $n, s$ and the degrees of the $f_i$.

Tietäväinen (1967) was perhaps the first to observe the savings obtained by using a weighted function of the type (2.11), (although his approach was somewhat different), and it has since been standard fare to use such functions.
The question then arises whether a better choice for $\alpha$ might yield a further savings when used in conjunction with an error estimate of type (2.8). In (1986, Lemma 5.1) we showed that the answer was no, except possibly for a savings of the factor $2^n$.

Our loss in using a weighted function instead of a characteristic function is that we no longer obtain an asymptotic estimate for $|V \cap B|$. However, we do obtain upper and lower bounds of the type

$$
(1 - \epsilon)2^{-n} \frac{|B|}{p^n} |V| < |V \cap B| < (1 + \epsilon)2^n \frac{|B|}{p^n} |V|
$$

(2.15)

for $|B| > \epsilon^{-1}2^n p^n \Phi(V)/|V|$. We can obtain the sharper bounds

$$
(1 - \epsilon) \frac{|B|}{p^n} |V| < |V \cap B| < (1 + \epsilon) \frac{|B|}{p^n} |V|
$$

(2.16)

for $|B|$ sufficiently large, and still save the $(\log p)^n$ factor in a couple of ways. One is to construct appropriate majorizing and minorizing functions for $\chi_B$, viewing $B$ as a solid box in $\mathbb{R}^n$ and using real Fourier series. In (1988) we constructed $n$-dimensional Fourier series for the Beurling and Selberg majorizing and minorizing functions and obtained the estimate (2.16) for $|B| > c(\epsilon,n) \Phi(V)p^n/|V|$. A second approach is due to Fujiwara (1988, Lemma 1). He proved a result of the following type: If bounds of the type

$$
(1 - \epsilon)p^{-n}|V| \sum_{x} \alpha(x) < \sum_{x \in V} \alpha(x) < (1 + \epsilon)p^{-n}|V| \sum_{x} \alpha(x)
$$

(2.17)

hold for all functions $\alpha$ of the type (2.11) with $B_1$, $B_2$ boxes (resp. cubes) with $|B_1| \geq c_1(n,\epsilon)p^n$ and $b_i \geq c_1(n,\epsilon)$, $1 \leq i \leq n$, then (2.16) holds for all boxes (resp. cubes) with $|B| \geq c_2(n,\epsilon)p^n$ and $b_i \geq c_2(n,\epsilon)$, $1 \leq i \leq n$. In practice, this is very useful since bounds of the type (2.17) generally are proven for arbitrary $\alpha$. The idea of his proof is to divide each edge of the box $B$ into $N$ equal length pieces, for some appropriately chosen $N$, and thus partition $B$ into $N^n$ smaller boxes to which (2.17) is applied.

**Refined Error Estimate.**

The error estimate in (2.8) is usually very wasteful, for as $y$ runs through $\mathbb{F}_p^n$, $|S(V,y)|$ is often less than its maximum value $\Phi(V)$ by a factor of $p^{1/2}$, or more. For instance, it was known by Carlitz (1953) that for a nonsingular quadratic form in an even number of variables, $|S(V,y)| \leq p^{-1} \Phi(V)$, unless $Q^*(y) = 0$, where $Q^*$ is the quadratic form associated with the inverse of the matrix for $Q$. Baker (1983) was perhaps the first to make use of this observation in improving the error estimate. He observed that for any nonsingular form $f$ there is a nonzero form $G$ such that $|S(V,y)| \leq p^{-1/2} \Phi(V)$ unless $G(y) = 0$. Thus we obtain

$$
|E(V)| \leq p^{-1/2} \Phi(V) \sum_{y} |a(y)| + \Phi(V) \sum_{G(y) = 0} |a(y)|
$$

(2.18)
and are left with studying sums of the type
\[ \sum_{G(\gamma) = 0} |a(\gamma)|. \]  
(2.19)

Heath-Brown (1985) presented a method using real Fourier series for bounding sums of the type (2.19) for quadratic forms \( G \) that can be easily adapted to finite Fourier series and generalized to arbitrary \( G \). Let \( \alpha(x) = \chi_{B_1} \cdots \chi_{B_k} \), where the \( B_i \) are cubes of size \( b \). Then
\[ |a(\gamma)| = p^{-n} \prod_{i=1}^{n} \frac{|\sin(\pi y_i/p)|^k}{|\sin(\pi y_i/p)|^k} \leq p^{-n} \min \left( b^{n+1}, \frac{p^{k} b^{k-n+1}}{2^k \|\gamma\|^k} \right), \]  
(2.20)
where we have identified \( \mathbb{F}_p \) with the set of integers from \(-\left[ \frac{p}{2} \right] \) to \( \left[ \frac{p}{2} \right] \). Thus
\[ \sum_{G(\gamma) = 0} |a(\gamma)| \leq p^{-n} \sum_{\|\gamma\| \leq \frac{p}{2}} b^{n+1} + p^{-n} \sum_{i=0}^{\infty} 2^{-i} b^{n+1} \]  
provided that \( k \geq n \). Using the upper bound of Theorem 11.3 for the number of points on a hypersurface contained in a cube we deduce that
\[ \sum_{G(\gamma) = 0} |a(\gamma)| \leq (\deg G)^{n+1} b^{n(k-1)+1} p^{-1}. \]  
(2.21)
In a similar manner we obtain for \( k > n \)
\[ \sum_{\mathcal{Y}} |a(\gamma)| \leq 4^{n+1} b^{n(k-1)}. \]
Thus, by taking \( k = n + 1 \) we have
\[ |E(V)| \leq (\deg G)^{n+1} |B_1|^n \Phi(V) \left( p^{-1/2} + \frac{b}{p} \right). \]  
(2.22)

Now let \( B \) be any cube of size \( b \) as given in (2.2), and set
\[ B_1 = \cdots = B_n = \left\{ 0 \leq x_i < \left[ \frac{b + n}{n + 1} \right] \right\}, \]
and \( B_{n+1} = B_1 + (a_1, \ldots, a_n) \). Then \( B_1 + \cdots + B_{n+1} \subset B \), \( |B_1| \geq \frac{1}{(n+1)^n} |B| \) and
\[ \sum_{x \in V} \alpha(x) \leq |V \cap B||B_1|^n, \]  
and so by (2.3) and (2.21) we obtain
Theorem 2.23. For any algebraic set \( V \) satisfying an inequality of the type (2.18), and any cube \( B \) of size \( b \), \(|V \cap B|\) is of the expected order if

\[
|B| > c(\deg G, n)p^n \left( \frac{\Phi(V)}{|V|} \right)^{\frac{n}{(n-1)}}.
\]  

(2.24)

In particular \( V \cap B \) is nonempty if \(|B|\) satisfies (2.24) with

\[
c(\deg G, n) = 4^n(n+1)^n(32 \deg G)^{n/(n-1)}.
\]

Since \( \Phi(V) \leq |V| \), the savings of (2.24) over (2.14) is apparent, but the shortcoming of this theorem is that it only holds for cubes, not for boxes with sides of arbitrary lengths.

The above method can be generalized to deal with arbitrary varieties \( V \) but before doing so let us consider how the values of \(|S(V, y)|\) might be distributed. It is easy to see that,

\[
\sum_y |S(V, y)|^2 = p^n|V| \leq Np^{n+e} + O(p^{n+e-\frac{1}{2}}),
\]

(2.25)

where \( e \) is the dimension of the algebraic set \( \overline{V} \), \( \overline{V} \) being the set of points satisfying (2.1) with coordinates in \( \mathbb{F}_p \), and \( N \) is the number of irreducible components of dimension \( e \). The first equality is just Parseval’s identity applied to the characteristic function of \( V \) while the second follows from (3.18). Thus, on average \(|S(V, y)| \ll p^{e/2} \). Moreover, it follows from (2.25) that \(|S(V, y)| \gg p^{e+\frac{1}{2}} \) for at most \( O(p^{n-1}) \) values of \( y \). Realizing that the analogous statements hold for any extension \( \mathbb{F}_q \) of \( \mathbb{F}_p \), one might ask whether this exceptional set of values of \( y \) is contained in some hypersurface. As we shall see, the answer is yes for many classes of varieties. In the same manner we see that for any positive integer \( r \), \(|S(V, y)| \) is of order \( p^{\frac{e}{2}+\frac{r}{2}} \) for at most \( O(p^{n-r}) \) values of \( y \) and so we might expect these values of \( y \) to be contained in an algebraic set of codimension \( r \). In any case we are lead to the following general set-up. Suppose that there is a positive integer \( M \) such that

(i) For all nonzero \( y \),

\[
|S(V, y)| \ll p^{M/2}, \quad \text{and}
\]

(ii) For \( r = e, e+1, \ldots, M-1 \) we have

\[
|S(V, y)| \ll p^{r/2} \quad \text{for all } y \notin S_r,
\]

(2.27)

where \( S_r \) is some subset of \( \mathbb{F}^n_p \).

Let \( w(r) \) be the dimension of the smallest algebraic set \( \overline{W}_r \) containing \( S_r \). In the same manner that (2.21) was obtained one can use the upper bound in Theorem 11.5 to show that

\[
\sum_{y \in \overline{W}_r} |a(y)| \ll b^{nk-w(r)}p^{w(r)-n}.
\]

(2.28)
Thus,

\[ |E(V)| \ll p^{c/2} \sum_{y} |a(y)| + \sum_{r=e+1}^{M} p^{r/2} \sum_{y \in S_{r-1} - S_r} |a(y)| \]

\[ \ll p^{c/2} b^{n(k-1)} + \sum_{r=e+1}^{M} p^{r/2} \sum_{y \in W_{r-1}} |a(y)| \]

\[ \ll^\dagger p^{c/2} b^{n(k-1)} + \frac{b^{nk}}{p^n} \sum_{r=e+1}^{M} p^{r/2} \left( \frac{p}{b} \right)^{w(r-1)} , \]

and so \( |V \cap B| \) is of the expected order if

\[ b \gg \max_{e \leq r \leq M} \{ p^{1-\frac{s}{2n}}, p^{1-\frac{s-r/2}{w(r-1)}} \} . \]  

(2.29)

Skorobogatov (1992) made use of such an approach but utilized real Fourier series.

In many cases we shall see that the value \( M \) appearing in (2.26) can be taken to be \( \ell + 1 \), that is

\[ |S(V, y)| \ll p^{\frac{\ell+1}{4}} , \quad \text{for all nonzero } y , \]  

(2.30)

where \( \ell \) is the dimension of the singular locus of \( \overline{V}_H \) viewed as a subset of \( \mathbb{P}^n \). If \( \overline{V}_H \) is nonsingular we take \( \ell = -1 \) and so in this case the upper bound in (2.30) is best possible.

With regard to the algebraic sets \( W_r \) appearing in (2.27), the heuristic argument given above suggests that we can take

\[ w(e) = n - 1, \quad w(e + 1) = n - 2, \quad w(e + 2) = n - 3, \quad \text{etc.} . \]  

(2.31)

Although it is premature to conjecture that (2.30) and (2.31) always hold true, we do not know of any counterexample. In section 4.8 we give many examples of varieties satisfying both of these conditions.

It follows from (2.29) that for any algebraic set \( V \) satisfying (2.30) and (2.31) and any cube \( B \) of size \( b \), \( |V \cap B| \) is of the expected order if

\[ b \gg \dagger p^{\frac{1}{2} + \frac{n-2}{2(n-1)}} . \]  

(2.32)

For hypersurfaces (2.32) simplifies to

\[ b \gg \dagger \begin{cases} 
  p^{\frac{1}{2} + \frac{1}{2n}} & \text{if } \overline{V}_H \text{ is nonsingular} \\
  p^{\frac{1}{2} + \frac{1}{2(n-1)}} & \text{if } \overline{V}_H \text{ has at most isolated singularities} \\
  p^{\frac{1}{2} + \frac{1}{2(n-1)}} & \text{in general.}
\end{cases} \]  

(2.33)

Baker (1983) established (2.33) for the case of hypersurfaces defined by a nonsingular form; in this case \( \overline{V}_H \) has an isolated singularity. Fujiwara (1985), (1988) and Shparlinskii and Skorobogatov (1990) generalized his work and established (2.32) for nonsingular homogeneous complete intersections; see section 4.7. Moreover, the big "Oh" constant appearing in the work of Baker and Fujiwara was shown to depend only on \( n, d \) and \( s \).

\[ \dagger \text{The constant here depends on the degrees of the polynomials defining the } \overline{W}_r \text{ as well as } n, s, \text{ and } d. \]
Best Possible Results.

One can sharpen the results above if better upper bounds are available for the number of points on the algebraic sets $W_r$ contained in a cube $B$ of small size, $b \ll p^{1/2}$. For instance, if the more optimistic upper bound

$$|W_r \cap B| \ll b^n / p^{(n-w(r))/2}$$

is available then we can replace the exponent on $p$ in (2.32) by $\frac{1}{2} + \frac{1}{2}(\frac{n-w}{n})$. Moreover, in general this is the best possible exponent obtainable by this method, for in bounding the error term $E(V)$ one will always have to contend with the term $p^{\frac{n}{2}} \sum_{y \neq 0} |a(y)|$. The only time one can do better is if the general term $S(V, y)$ is of order $\leq p^{\frac{n-1}{2}}$, such as in the case of a nonsingular quadratic form in an even number of variables. As we shall see, for most $V$ the general term will be of order $p^{\frac{n}{2}}$.

In order to push this method closer to the exponent $1/2$ (or better) one needs a novel way of bounding the error term $|E(V)|$ that takes into account all of the cancellation that one would expect from summing over the varying complex values $a(y)S(V, y)$.

Further Comments.

In closing this section we note that the method of using a convoluted function $\alpha$ to show that $V \cap B$ is nonempty can be applied just as readily to any convex set of lattice points in $\mathbb{R}^n$. For instance in (1986, Corollary 4.1) we showed that if $C$ is a convex subset of $\mathbb{R}^n$ symmetric about a point in $\mathbb{Z}^n$, of diameter $< 2p$, with $\text{Vol}(C) > 4^n \Phi(V)p^n / |V|$ then $C$ contains an integral solution of the congruence $F(x) \equiv 0 \pmod{p}$. See also (1986, Theorem 1.2) and Chalk (1989). Also the method adapts easily for obtaining a set of $n$ linearly independent points of $V$ in a box; see Cochrane (1986, Theorem 1.4).

Finally, we observe that for homogeneous algebraic sets the basic identity (2.3) takes on the following geometric form with $\alpha = \chi_B$; see Cochrane (1984, Proposition 7.2)

$$|B \cap V| = \frac{|B|}{p^n} |V| + \frac{1}{(p-1)^2} \frac{1}{p^n} \sum_{y \neq 0} (p|V \cap H(y)| - |V|)(p|B \cap H(y)| - |B|). \quad (2.34)$$

Indeed, the box $B$ in (2.34) can be replaced by any set of points. Similar identities are obtained for other choices of $\alpha$. Perhaps identities of this type can be used to improve on the error estimate.
3. Zeta Functions and the Cardinality of Algebraic Sets.

Definition of the Zeta Function.

In order to obtain precise information about the cardinality of an algebraic set we turn to a discussion of zeta functions. Let $\mathbb{F}_q$ be the finite field in $q = p^r$ elements, $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$, $A^n = \overline{\mathbb{F}}_q^n$ denote affine $n$-space and $\mathbb{P}^n$ denote projective $n$-space. Let $\overline{V} = \overline{V}(f_1, \ldots, f_s)$ be the algebraic subset of $A^n$ defined by polynomials $f_1, \ldots, f_s$ in $\mathbb{F}_q[X]$ of degrees $\leq d$. For any positive integer $j$ let $V_j$ denote the set of points in $\overline{V}$ with coordinates in $\mathbb{F}_{q^j}$. If the $f_i$ are homogeneous polynomials then they also define an algebraic subset of $\mathbb{P}^{n-1}$, which we shall again denote by $\overline{V}$, and we can define sets $V_j$ analogously. We set $N_j = |V_j|$, the number of affine points in $V_j$ or $N_j = |V_j|_P$, the number of projective points (if the $f_i$ are homogeneous) depending on the point of view we wish to take.

The zeta function for $\overline{V}$ is the formal power series in $t$ with rational coefficients given by

$$
\zeta(t) = e^{\sum_{j=1}^{\infty} \frac{N_j t^j}{j}} = \prod_{x \in \overline{V}} \left(1 - t^{\deg(x)}\right)^{-1},
$$

(3.1)

where $\deg(x)$ denotes the degree of the minimal extension of $\mathbb{F}_q$ containing the coordinates of $x$, and $\prod^*$ indicates that only one choice of $x$ is taken from its set of $\deg(x)$ conjugates. It is clear from the product form in (3.1) that $\zeta(t)$ is a series with integer coefficients.

The equality in (3.1) may be easily verified. Indeed, the logarithm of the right-hand side is equal to

$$
-\sum_{x \in \overline{V}}^* \log(1 - t^{\deg(x)}) = \sum_{x \in \overline{V}}^* \sum_{n=1}^{\infty} \frac{t^{n \deg(x)}}{n}
$$

$$
= \sum_{j=1}^{\infty} \left( \sum_{x \in \overline{V}, \deg(x) \equiv j}^* \deg(x) \right) \frac{t^j}{j},
$$

the latter equality obtained by setting $j = n \cdot \deg(x)$. Now $\deg(x) \equiv j$ if and only if $x$ has coordinates in $\mathbb{F}_{q^j}$, and so the latter sum is just the sum appearing in the exponent on the left-hand side of (3.1).

If the polynomials $f_i$ are all homogeneous then we may write $\zeta_A(t)$ or $\zeta_P(t)$ for the zeta function, depending on whether we are counting the points in affine or projective space. From the identity $(q^j - 1)|V_j|_P = |V_j| - 1$ it is easy to deduce that

$$
(1 - t)\zeta_A(t) = \zeta_P(qt)/\zeta_P(t).
$$

One motivation for defining the zeta function as above is the following. Suppose there exist complex numbers $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_m$, such that for all positive integers $j$ we have

$$
N_j = \alpha_1^j + \cdots + \alpha_s^j - \beta_1^j - \cdots - \beta_m^j.
$$

(3.2)

Then it is routine to verify that

$$
\zeta(t) = \prod_{i=1}^{m} \frac{1 - \beta_i t}{1 - \alpha_i t},
$$

(3.3)

a rational function in $t$, and visa-versa.
Example 3.4. Suppose that \( q \) is odd and that \( \overline{V} \) is a hypersurface defined by a nonsingular quadratic form \( Q \). If \( n \) is odd then \( |V_j| = (q^{n-1})^j \) and \( |V_j|_\mathbb{P} = (q^{(n-1)j} - 1)/(q^j - 1) \) and so the affine and projective zeta functions are given by

\[
\zeta_\mathbb{A}(t) = (1 - q^{n-1}t)^{-1} \quad \text{and} \quad \zeta_\mathbb{P}(t) = \prod_{i=0}^{n-2}(1 - q^i t)^{-1},
\]

respectively. If \( n \) is even then the number of affine points is given by

\[
N_j = (q^{n-1})^j + (\Delta q^{n/2})^j - (\Delta q^{3/2})^j
\]

where \( \Delta = 1 \) if \( (-1)^{n/2} \det(Q) \) is a square in \( \mathbb{F}_q \) and -1 otherwise, and so

\[
\zeta_\mathbb{A}(t) = \frac{(1 - q^{3/2} - 1\Delta t)}{(1 - q^{n-1}t)(1 - q^{3/2}t)}
\]

and

\[
\zeta_\mathbb{P}(t) = (1 - \Delta q^{3/2} - 1t)^{-1}\prod_{i=0}^{n-2}(1 - q^i t)^{-1}.
\]

It is of interest to note that the zeros and poles of the zeta functions in this example are all powers of \( q^{-1/2} \). This is an illustration of the Riemann Hypothesis discussed below.

Rationality of the Zeta Function and the Riemann Hypothesis.

We turn now to the cohomological interpretation of the zeta function. The key to this interpretation is the Lefschetz-Grothendieck fixed-point formula. Let \( F \) be the Frobenius morphism on \( \overline{V} \) given by

\[
F(x) = (x_1^q, \ldots, x_n^q).
\]

Since \( \overline{V} \) is defined by polynomials with coefficients in \( \mathbb{F}_q \), it follows that \( F \) maps points in \( \overline{V} \) to points in \( \overline{V} \). Moreover, letting \( F^j \) denote the composition of \( F \) with itself \( j \) times it follows that \( V_j \) is the set of fixed points of \( F^j \). Letting \( N_j \) denote the number of points in \( V_j \) it follows from the Lefschetz-Grothendieck fixed point (trace) formula that for any prime \( \ell \) different from \( p \),

\[
N_j = \sum_{i=0}^{2e} (-1)^i \text{Tr}(F^*; H^i(\overline{V}, \mathbb{Q}_\ell)),
\]

where \( \mathbb{Q}_\ell \) denotes the \( \ell \)-adic rationals, \( H^i \) denotes the \( i^{th} \) etale cohomology group, and \( F^* \) denotes the induced mapping of \( F \) on the cohomology group. Let \( H^i \) denote \( H^i(\overline{V}, \mathbb{Q}_\ell) \). It is well known that \( H^i \) is a finite dimensional vector space over \( \mathbb{Q}_\ell \). We denote its dimension by \( B_i \) and call \( B_i \) the \( i^{th} \) Betti number associated with \( \overline{V} \) (or associated with the zeta function for \( \overline{V} \)). It is known that the cohomology groups vanish for \( i > 2e \) and so the sum in (3.5) stops at \( i = 2e \). Inserting the expression for \( N_j \) in (3.5) into the definition of the zeta function we obtain,

\[
\zeta(t) = \prod_{i=0}^{2e} \left[ \exp \left( \sum_{j=1}^{\infty} \text{Tr}(F^*; H^i) \frac{t^j}{j} \right) \right] (-1)^i.
\]
\[ = \Pi_{i=0}^{2e} \det(1 - tF^*; H^i)^{(-1)^{i+1}}, \quad (3.6) \]

the last identity following from linear algebra. Let \( P_i(t) \) denote the polynomial \( \det(1 - tF^*; H^i) \), a polynomial with rational coefficients. Then \( B_i \) is the degree of \( P_i(t) \) and we see from (3.6) that the zeta function is a rational function of \( t \),

\[ \zeta(t) = \frac{P_1(t)P_2(t) \ldots P_{2e-1}(t)}{P_0(t)P_2(t) \ldots P_{2e}(t)}. \quad (3.7) \]

Let

\[ P_i(t) = \Pi_j(1 - \alpha_{ij}t) \]

denote the factorization of \( P_i(t) \) over the complex numbers. The values \( \alpha_{ij} \) are called the characteristic values of the Frobenius morphisms \( F^* \). In his celebrated proof of the Riemann Hypothesis for varieties over finite fields Deligne (1973, Weil-I) completed the proof of the Weil conjectures, stated by Weil in his (1949) paper, and established the following.

**Proposition 3.8. Deligne (1973).** Let \( \overline{V} \) be a smooth projective variety of dimension \( e \) in \( \mathbb{P}^n \). Then

(i) The polynomials \( P_i(t) \) in (3.7) have integer coefficients and are independent of the choice of the prime \( \ell \). Thus, the characteristic values \( \alpha_{ij} \) are algebraic integers. In particular, \( P_0(t) = (1 - t) \) and \( P_{2e}(t) = (1 - q^e t) \).

(ii) The Riemann Hypothesis: For any \( i, 0 \leq i \leq 2e, |\alpha_{ij}| = q^{i/2} \) for all \( j \). In particular, the conjugates (over \( \mathbb{Q} \)) of a given \( \alpha_{ij} \) all have the same absolute value.

(iii) Functional Equation: \( \zeta\left(\frac{1}{q^e t}\right) = q^{e}\chi(\overline{V})^{1/2}t^{\chi(\overline{V})}\zeta(t) \), where

\[ \chi(\overline{V}) = \sum_{i=0}^{2e} (-1)^i B_i \quad \text{and} \quad e = \begin{cases} 1 & \text{if } 2 \nmid e \\ (-1)^N & \text{if } 2|e, \end{cases} \quad (3.9) \]

where \( N \) is the multiplicity of the eigenvalue \( q^{e/2} \) of \( F^*H^e \).

(iv) If \( \overline{V} \) is obtained from a variety \( X \) defined over an algebraic number ring by reduction modulo a prime ideal, then \( B_i \) is the rank of the ordinary cohomology group \( H^i(X, \mathbb{Z}) \).

(v) If \( \overline{V} = \overline{V}(f_1, \ldots, f_s) \) is a smooth complete intersection of dimension \( e = n - s \), then

\[ \zeta(t) = P_e^*(t)^{(-1)^{e-1}} / \Pi_{j=0}^e (1 - q^j t), \quad (3.10) \]

where \( P_e^*(t) \) is the polynomial \( P_e(t) \) if \( e \) is odd and the polynomial \( P_e(t)/(1 - q^{e/2} t) \) if \( e \) is even.

The number \( \chi(\overline{V}) \) in (3.9) is called the **Euler-Poincaré** characteristic of \( \overline{V} \). It is the self-intersection number of the diagonal of \( V \times \overline{V} \). Also, from (3.7) it is plain that \( \chi(\overline{V}) \) is the degree of the zeta-function for \( \overline{V} \). A proof of Proposition 3.8, together with the requisite background material can be found in the book of Freitag and Kiehl (1988).

From Deligne's second major paper on the Weil conjectures (1980, Weil-II), we have the following version of the Riemann Hypothesis for more general algebraic sets.
Proposition 3.11. Deligne (1980). For any algebraic set $V$ (affine or projective) the characteristic roots of the zeta function are such that for any $i$ and $j$,

(i) $|\alpha_{ij}| = q^{w/2}$ for some nonnegative integer $w = w(i, j)$ called the weight of $\alpha_{ij}$,
(ii) $|\alpha_{ij}| \leq q^{i/2}$, that is $w(i, j) \leq i$ and
(iii) Again, the conjugates (over $\mathbb{Q}$) of $\alpha_{ij}$ all have the same absolute value.

Another important result due to Bombieri (1978) is an upper bound on the total number of characteristic values of the zeta function.

Proposition 3.12. Bombieri (1978, Theorem 2). Suppose that the zeta function is written as a ratio of relatively prime polynomials (that is all common linear factors have been cancelled out at the top and bottom in the expression (3.7)), then the total number of remaining characteristic values (that is, the total degree of the rational function) is bounded above by

$$ (4d + 9)^{n+s}, $$

where $n, d$ and $s$ are as defined at the beginning of this section.

The upper bound in (3.13) does not imply however an upper bound on the individual Betti numbers $B_i$. Bombieri noted that essentially the same upper bound could be deduced readily from the work of Dwork (1966). Adolphson and Sperber (1987b) obtained a related upper bound.

Curves.

Suppose that $\overline{V} \subseteq \mathbb{P}^2$ is a smooth curve. Then by Proposition 3.8 we have that

$$ \zeta(t) = \Pi_{j=1}^{B}(1 - \alpha_j t)/(1-t)(1-qt), $$

where $B = dim_{\mathbb{Q}} H^1(\overline{V}, \mathbb{Q}_2) = rank H^1(X, \mathbb{Z}) = 2g = (d-1)(d-2)$, $g$ is the genus of the curve, $d$ the degree, and $|\alpha_j| = q^{j/2}$ for all $j$. Putting $t = q^{-s}$ in the zeta function gives us the classical statement of the Riemann Hypothesis for curves over finite fields, namely that all the zeros of $\zeta(s)$ have real part $1/2$. From (3.2) we deduce the following estimate of Weil for the number of points on a smooth curve.

Theorem 3.14. Weil (1948a). (i) If $\overline{V} \subseteq \mathbb{P}^2$ is a smooth curve defined over $\mathbb{F}_q$ then

$$ ||V|_{\mathbb{F}_q} - (q+1) \leq 2gq^{1/2}. $$

(ii) More generally, if $f(X, Y)$ is an absolutely irreducible polynomial over $\mathbb{F}_q$ of degree $d$ and $\overline{V} = \overline{V}(f) \subseteq A^2$ then

$$ ||V| - q| \leq (d-1)(d-2)q^{1/2} + d^2. $$

Part (ii) follows by taking the projective closure of $V$ and using the fact that any projective curve is birationally equivalent to a nonsingular projective curve. Serre (1983) has pointed out that the upper bound in (3.15) can be sharpened slightly to the value $g[2q^{1/2}]$ where $[\cdot]$ denotes the greatest integer function; see also Lachaud (1991).
General Affine Varieties.

One can deduce from Theorem 3.14 the following general result.

**Theorem 3.17.** Lang and Weil (1954), Nisnevich (1954). Let \( \overline{V} = \overline{V}(f_1, \ldots, f_s) \subset \mathbb{A}^n \) be an absolutely irreducible variety of dimension \( e \). Then

\[
||V|| - q^e \leq c(d, n, s)q^{e-\frac{1}{2}}.
\]

Indeed, by Proposition 3.11 the constant in (3.18) can be taken to be the Bombieri constant (3.13). See also Schmidt (1976) for another proof of Theorem 3.17.

If \( \overline{V} \) is an arbitrary algebraic set (that is, not necessarily irreducible) of dimension \( e \), defined by a set of \( s \) polynomials of degrees \( \leq d \) then it follows from Proposition 3.11 and (3.13) that

\[
|V| \leq (4d + 9)^{n+s}q^e.
\]

If \( V \) is defined by the polynomials \( f_1, \ldots, f_s \) it is sometimes profitable to use the identity

\[
|V| = q^{n-s} + q^{-s} \sum_{\lambda \neq 0} \sum_{x} \psi \left( \sum_{i=1}^{s} \lambda_i f_i(x) \right),
\]

in conjunction with bounds on complete exponential sums (a topic discussed in section 4.6) for determining \( |V| \). Here \( \psi \) is a nontrivial additive character on \( \mathbb{F}_q \).

Smooth Complete Intersections.

Suppose that \( \overline{V} \) is a smooth irreducible complete intersection of dimension \( e = n - s \) in \( \mathbb{P}^n \). Then again from Proposition 3.8 and (3.2) it follows that

\[
||V||_P - (q^e + q^{e-1} + \ldots + 1) \leq B_e^*q^{e/2},
\]

where

\[
B_e^* = \begin{cases} B_e & \text{if } e \text{ is odd} \\ B_e - 1 & \text{if } e \text{ is even}. \end{cases}
\]

The values of the Betti numbers \( B_e \) are given in section XI of Grothendieck (1971).

The affine version of (3.21) is the following. If \( \overline{V} \subset \mathbb{A}^n \) is a complete intersection of homogeneous polynomials whose only singularity is at the origin, then it is immediate from (3.21) that

\[
||V|| - q^e \leq B_{e-1}^* q^{\frac{e+1}{2}},
\]

where \( B_{e-1} \) is the Betti number associated with the projective variety of dimension \( e - 1 \) in \( \mathbb{P}^{n-1} \) defined by the same polynomials defining \( \overline{V} \).

If \( \overline{V} \subset \mathbb{A}^n \) is defined by nonhomogeneous polynomials then we can still make use of (3.21) as follows. Let \( \overline{V}_H \) be the projective variety in \( \mathbb{P}^n \) defined by the homogenizations of the polynomials defining \( \overline{V} \), and \( \overline{V}_\infty \) be the projective algebraic subset of \( \mathbb{P}^{n-1} \) defined by the maximal homogeneous parts of the polynomials defining \( \overline{V} \). Then

\[
|V_H|_P = |V| + |V_\infty|_P,
\]

and so we deduce from (3.21) the following,
Theorem 3.24. If $\overline{V} \subset A^n$ is such that $\overline{V}_H$ and $\overline{V}_\infty$ are smooth irreducible complete intersections of dimensions $e$ and $e-1$ respectively, then
\[
||V|-q^e| \leq (B_e^* + B_{e-1}^*/\sqrt{q})q^{e/2},
\] (3.25)
where $B_e$ and $B_{e-1}$ are the Betti numbers associated with $\overline{V}_H$ and $\overline{V}_\infty$ respectively.

The estimate in (3.25) realizes an extra savings of $q^{1/2}$ over the estimate in (3.22). We note that Theorem 3.24 does not apply to homogeneous $\overline{V}$ for then $\overline{V}_H$ always has a singularity. Another result with less stringent hypotheses but consequently a weaker error estimate is

Theorem 3.26. Suppose that $\overline{V} = \overline{V}(f_1, \ldots, f_s) \subset A^n$, is such that every polynomial in the pencil $\lambda_1 f_1 + \cdots + \lambda_s f_s$, with $\lambda \neq 0 \in F_q^s$, is of degree $\geq 2$, not divisible by $p$, and nonsingular at $\infty$. Then
\[
||V|-q^{n-s}| \leq (d-1)^n q^{n/2}.
\] (3.27)

This theorem follows immediately from (3.20) and the upper bound (4.1.16) of Deligne for exponential sums. It is not surprising that the bound in (3.27) is weaker than the bounds given in (3.22) and (3.25) for $||V|-q^{n-s}|$. Indeed, the condition that $\overline{V}_\infty$ be a nonsingular projective variety of dimension $n-s$ implies in particular that every polynomial in the pencil $\lambda_1 f_1 + \cdots + \lambda_s f_s$, with $\lambda \neq 0 \in F_q^s$, is nonsingular at $\infty$. If $s = 1$ these two conditions are the same (and the bounds in (3.22) and (3.27) are the same), but for $s > 1$ the former is much stronger.

Complete Intersections with Singularities.

Hooley (1991) and Katz (1991) recently generalized (3.21) to account for varieties with singularities. If $\overline{V} \subset \mathbb{P}^n$ is defined by $f_1, \ldots, f_s$ we define the singular locus of $\overline{V}$ to be the set of points in $\overline{V}$ such that the rank of $[\partial f_i/\partial x_j]$ is less than $s$.

Theorem 3.28. Hooley (1991), Katz (1991). If $\overline{V} = \overline{V}(f_1, \ldots, f_s) \subset \mathbb{P}^n$ is a complete intersection of dimension $e = n-s$ with singular locus of dimension $\ell$, then
\[
||V||_p - (q^e + q^{e-1} + \cdots + 1) \leq (4d + 9)^{n-s+1}(\frac{q}{q-1})^{\frac{s+1}{4}}.
\] (3.29)

If $\overline{V}$ is nonsingular then we take $\ell = -1$ and so (3.29) in this case is the same as (3.21). To obtain the constant on the righthand side of (3.29) we use the affine cone over $\overline{V}$, (3.13), and the fact that $(q-1)||V||_p = ||V|| - 1$.

For affine varieties one can again use (3.23) to state the obvious generalization of Theorem 3.24.

Smooth Hypersurfaces.

When $\overline{V}$ is a smooth irreducible hypersurface in $\mathbb{P}^n$ of dimension $e = n-1$ and degree $d$, it is known that
\[
B_e^* = \frac{d-1}{d}[(d-1)^n + (-1)^{n+1}],
\] (3.30)
and so in particular the constants on the righthand sides of (3.22) and (3.25) can be taken as $(d-1)^{n-1}$ and $(d-1)^n$ respectively. The following example is an application of Theorem 3.24 and inequality (3.22).
Example 3.31. Let \( f(X) \) be a nonsingular form of degree \( d \) over \( \mathbb{F}_q \) and \( c \in \mathbb{F}_q \). Then the number \( N \) of solutions of \( f(x) = c \) over \( \mathbb{F}_q \) satisfies,

\[
|N - q^{n-1}| \leq \begin{cases} 
(d - 1)^n q^{\frac{n-1}{2}} & \text{if } c \neq 0, \\
(d - 1)^n q^{\frac{n}{2}} & \text{if } c = 0.
\end{cases}
\]

For nonhomogeneous polynomials we have the following application of Theorem 3.26.

Example 3.32. Let \( f(X) \) be any polynomial of degree \( d \) over \( \mathbb{F}_q \), \( p \nmid d \), nonsingular at infinity. Then for any \( c \in \mathbb{F}_q \), the number \( N \) of solutions of \( f(x) = c \) over \( \mathbb{F}_q \) satisfies

\[
|N - q^{n-1}| \leq (d - 1)^n q^{\frac{n}{2}}.
\]

Another case where a particularly good estimate for \( |V| \) is available is provided for in the following theorem of Adolphson and Sperber. They deduce it from their work on exponential sums over Tori, a topic we discuss in section 4.5. We state here a slightly refined version of their theorem that takes into account the recent work of Denef and Loeser (1991). The reader should refer to section 4.5 for the terminology used in the statement of the theorem.

Theorem 3.33. Adolphson and Sperber (1989, Theorem 6.8). Suppose that \( f \) is a polynomial over \( \mathbb{F}_q \) which is nondegenerate, commode and such that \( f, x_1 \frac{\partial f}{\partial x_1}, \ldots, x_n \frac{\partial f}{\partial x_n} \), have no common zero. Let \( V \) be the set of zeros of \( f \) over \( \mathbb{F}_q \). Then

\[
||V| - q^{n-1}| \leq \nu(f)q^{\frac{n-1}{2}},
\]

where \( \nu(f) \) is the value \( e_n \) given in Theorem 4.5.15.

It is of interest to note that if \( f \) is such that \( \overline{V}(f) \subset \mathbb{A}^n \) and \( \overline{V}_\infty(f) \subset \mathbb{P}^{n-1} \) are both smooth and irreducible then by a linear change of variables (over \( \overline{\mathbb{F}}_q \)) \( f \) can be put into a form satisfying the hypotheses of Theorem 3.33. Thus, for the case of hypersurfaces, Theorem 3.24 can be realized as a Corollary of Theorem 3.33.

Example 3.34. Let \( N \) be the number of solutions of the equation

\[
a_1 x_1^{d_1} + \ldots + a_n x_n^{d_n} = c,
\]

over \( \mathbb{F}_q \), with \( c \neq 0, a_i \neq 0 \) and \( d_i \geq 1 \) for all \( i \). It is clear that replacing \( d_i \) with \( \delta_i = (d_i, q - 1) \) does not change the number of solutions. Moreover, by doing so we may assume that the exponents are all relatively prime to \( p \). In this case Theorem 3.33 applies and we have \( \nu(f) = \Pi_{i=1}^n (\delta_i - 1) \). This proves the \( c \neq 0 \) part of the following theorem which is normally proved by the use of Jacobi sums; see for example Small (1991, 6.6).
Theorem 3.35. Weil (1949), Hua and Vandiver (1949). Let $N$ be the number of solutions of the equation $a_1x_1^{d_1} + \ldots + a_nx_n^{d_n} = c$ over $\mathbb{F}_q$, with $a_i \neq 0$ and $d_i \geq 1$ for all $i$. Set $\delta_i = (d_i, q - 1)$ for $1 \leq i \leq n$. Then

$$|N - q^{n-1}| \leq \begin{cases} (\delta_1 - 1) \cdots (\delta_n - 1)(1 - \frac{1}{q})q^{n/2} & \text{if } c = 0 \\ (\delta_1 - 1) \cdots (\delta_n - 1)q^{\frac{n-\sum \delta_i}{2}} & \text{if } c \neq 0. \end{cases}$$

The first part of this theorem follows immediately from (3.20) and the classical bound $\sum_{x_i} \psi(a_i x_i^{d_i}) \leq (\delta_i - 1)q^{1/2}$ for Gaussian sums; see Example 4.1.12. Another diagonal-type equation that enjoys a good bound on the error term is given in

Theorem 3.36. Schmidt (1976, p. 173) Let $F(X) = \sum_{i=2}^n f_i(x_1)X_i^{d_i}$ with the $f_i$ of degrees $\leq d$ and coprime in pairs. Suppose that whenever $a_j$, $2 \leq j \leq n$ are such that $0 < a_j < d_j$, $2 \leq j \leq n$ and $\sum_{i=2}^n a_i/d_i$ is integral then $\prod_{i=2}^n f_i(x_1)^{a_i/d_i}$ is not a $\delta$th power, where $\delta = \text{lcm}(d_2, \ldots, d_n)$. Then the number $N$ of solutions of the equation $F(x) = 0$ satisfies

$$|N - q^{n-1}| \ll q^{n/2}.$$

Schmidt’s Theorem generalizes a result of Perel’muter and Postnikov (1972).

Historical Comments.

For a discussion of the history of the Weil-Conjectures the reader is referred to the work of Dieudonné (1975), “On the history of the Weil Conjectures”, the paper of Katz (1976), “An overview of Deligne’s proof of the Riemann Hypothesis for varieties over finite fields” and the introduction to the book of Freitag and Kiehl (1988), “Etale Cohomology and the Weil Conjecture”. Gauss counted the number of solutions of the equation $y^2 = 1 - x^4$ over $\mathbb{F}_p$ and in so doing established an equivalent form of the Riemann hypothesis for this curve. Artin (1924) was the first person to consider zeta functions for curves, and established the Riemann Hypothesis for several special types of curves. Hasse (1933) proved the Riemann Hypothesis for all elliptic curves. Weil (1948a), (1949) proved the Riemann Hypothesis for all curves and general diagonal polynomials. At the same time he stated the Weil-Conjectures for more general algebraic sets. Dwork (1960) was the first to prove the rationality of the zeta function for general algebraic sets over finite fields. In (1972) Stepanov, Schmidt, and Bombieri gave an elementary proof of the Riemann Hypothesis for curves; see Bombieri (1973) and Schmidt (1976). Finally, Deligne (1973), (1980) proved the Weil conjectures for general algebraic sets.

One should see chapter 6 of Lidl and Neiderreiter (1983), in particular the notes at the end of the chapter, for a detailed account of the history of counting points on varieties over finite fields.
4. Exponential Sums

Our goal in this section is to obtain upper bounds on general exponential sums of the type

\[ S(V, \psi) = \sum_{x \in V} \psi(g(x)), \]

and then to apply the upper bounds for the particular sum

\[ S(V, y) = \sum_{x \in V} \psi(x \cdot y), \]

to the problem of estimating the number of points in \( V \cap B \). We turn first to a discussion of \( L \)-functions.

4.1 \( L \)-Functions

As in the previous section we again let \( f_1, \ldots, f_s \) be polynomials over \( \mathbb{F}_q \) in \( n \) variables and of degrees \( \leq d \), \( V = V(f_1, \ldots, f_s) \) be the algebraic subset of \( \mathbb{A}^n \) defined by \( f_1 = \cdots = f_s = 0 \), \( \epsilon \) its dimension, and for any positive integer \( j \) let \( V_j = V \cap \mathbb{F}_q^{\epsilon j} \). Let \( g(X) \) be any polynomial with coefficients in \( \mathbb{F}_q \). For \( j = 1, 2, \ldots \), set

\[ S_j = \sum_{x \in V_j} \psi_j(g(x)) \]

where \( \psi_j() = \epsilon_p(Tr_j()) \) and \( Tr_j \) is the trace mapping from \( \mathbb{F}_q^j \) to \( \mathbb{F}_p \). When \( j = 1 \) we write \( V = V_1 \), \( S = S_1 \), and \( \psi = \psi_1 \). Let \( L(t) \) be the formal power series in \( t \),

\[ L(t) = e^{\sum_{j=1}^{\infty} S_j t^j / j} = \prod_{x \in V}(1 - \psi_{\deg(x)}(x \cdot y) t^{\deg(x)})^{-1}, \tag{4.1.1} \]

where \( \mathbb{F}_q(x) \) denotes the minimal extension of \( \mathbb{F}_q \) containing the coordinates of \( x \), \( \deg(x) = [\mathbb{F}_q(x) : \mathbb{F}_q] \), and \( \prod^* \) indicates that only one choice of \( x \) is taken from its set of \( \deg(x) \) conjugates. \( L(t) \) is called the \( L \)-function associated with the algebraic set \( V \) and polynomial \( g \). Note that if \( g \) is taken to be the zero polynomial then the associated \( L \)-function is just equal to the zeta function for \( V \).

It is well known that \( L(t) \) is a rational function in \( t \). Indeed the cohomological interpretation given for the zeta function in section 3 is completely analogous here. By the Grothendieck trace formula we have

\[ S_j = \sum_{i=0}^{2\epsilon} (-1)^i Tr(F^{*j}; H^i(V, \mathcal{F}_\ell)), \tag{4.1.2} \]

where \( \mathcal{F}_\ell \) is a certain locally free \( \ell \)-adic sheaf associated with \( V \). \( H^i(V, \mathcal{F}_\ell) \) is a finite dimensional vector space over \( K_\ell = \mathbb{Q}_\ell(\zeta_p) \), say of dimension \( B_i \), where \( \zeta_p \) is a primitive \( p^{th} \) root of unity. Following the derivation in the previous section we obtain,
\[ L(t) = \frac{P_1(t)P_2(t) \cdots P_{2e-1}(t)}{P_0(t)P_2(t) \cdots P_{2e}(t)} \]  

(4.1.3)

where for \( i = 0, 1, \ldots, 2e \),

\[ P_i(t) = \text{det}(1 - tF^*, H^i(V, \mathcal{F})). \]

The \( i^{th} \) Betti number \( B_i \) is again the degree of the polynomial \( P_i(t) \).

Let

\[ P_i(t) = \prod_j (1 - \alpha_{ij} t) \]

denote the factorization of \( P_i(t) \) over the complex numbers. The values \( \alpha_{ij} \) are called the characteristic values associated with the \( L \)-function \( L(t) \). In (1980, Weil II) Deligne established the following more general version of Proposition 3.11.

**Proposition 4.1.4.** Deligne (1980). For any algebraic set \( V \) and polynomial \( g \) as given above we have for any \( i, j \),

(i) \( \alpha_{ij} \) and \( q^w/\alpha_{ij} \) are algebraic integers,

(ii) \( |\alpha_{ij}| = q^{w/2} \) for some nonnegative integer \( w = w(i, j) \) called the weight of \( \alpha_{ij} \),

(iii) \( |\alpha_{ij}| \leq q^{i/2} \), that is \( w(i, j) \leq i \), and

(iv) The conjugates (over \( \mathbb{Q} \)) of \( \alpha_{ij} \) all have the same absolute value.

Also, the upper bound of Bombieri (3.13) for the total number of characteristic values, after cancellation, is still valid. We need only replace \( d \) by the maximum of the degrees of the polynomials \( f_1, \ldots, f_s \), and \( g \). We can write \( L(t) \) in reduced form as

\[ L(t) = \frac{P(t)}{Q(t)} = \frac{\prod_{i=1}^{m}(1 - \beta_i t)}{\prod_{i=1}^{m}(1 - \alpha_i t)}, \]

for some relatively prime polynomials \( P(t) \), \( Q(t) \) having coefficients in \( \mathbb{Q}(\xi_p) \). As in (3.2) we have

\[ S_j = \alpha_1^j + \cdots + \alpha_s^j - \beta_1^j - \cdots - \beta_m^j, \]

for any positive integer \( j \). In particular we obtain,

**Proposition 4.1.5.** If \( M \) is the maximum weight of the characteristic values of \( L(t) \) then for \( j = 1, 2, \ldots, \)

\[ |S_j| \leq (4d^* + 9)^{n+s} q^{Mj/2}, \]

(4.1.6)

where \( d^* \) is the maximum of the degrees of the polynomials \( f_1, \ldots, f_s \) and \( g \).

Serre (1977) introduced the following terminology for a special class of \( L \)-functions of particular importance.
Definition 4.1.7. We say that the pair \((\overline{V}, g)\) is pure of weight \(e\) if

(i) All of the irreducible components of \(\overline{V}\) are of dimension \(e\),

(ii) \(H^i(\overline{V}, \mathcal{F}_\ell) = 0\) for all \(i \neq e\), and

(iii) All of the characteristic values of \(F^*\) on \(H^e(\overline{V}, \mathcal{F}_\ell)\) have weight \(e\), that is, \(|\alpha_{ej}| = q^{e/2}\) for all \(j\).

Equivalently, the pair \((\overline{V}, g)\) is pure of weight \(e\) if (i) holds and \(L(t)^{(e-1)^{e-1}}\) is a polynomial all of whose roots have modulus \(q^{-\frac{q}{2}}\). If the pair \((\overline{V}, g)\) is pure of weight \(e\) then in particular,

\[|S_j| \leq B_\ell q^{e_\ell/2},\]  

(4.1.8)

for any \(j\). Moreover the upper bound in (4.1.8), including the constant \(B_\ell\), is best possible in such a case; see the remark after (4.2.2). Serre (1977) discusses many important exponential sums having this type of purity property. We give a few examples here.

Example 4.1.9. Lidl and Niederreiter (1983, Theorem 5.15). Gauss established the following identity for quadratic Gauss sums.

\[
\sum_{x \in \mathbb{F}_q} \psi(x^2) = \begin{cases} 
(1)^{r-1} \sqrt{q} & \text{if } p \equiv 1 \pmod{4} \\
(1)^{r-1} i \sqrt{q} & \text{if } p \equiv -1 \pmod{4},
\end{cases}
\]  

(4.1.10)

where \(q = p^r\). Thus the \(L\)-function associated with the pair \((\mathbb{A}^1, X^2)\) is given by

\[
L(t) = \begin{cases} 
(1 + (1)^{r-1} \sqrt{q} \ t) & \text{if } p \equiv 1 \pmod{4} \\
(1 + (1)^{r-1} i \sqrt{q} \ t) & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]  

(4.1.11)

In particular, the pair \((\mathbb{A}^1, X^2)\) is pure of weight 1.

Example 4.1.12. Let \(g(X) = aX^d\) with \(a \neq 0\) and \(d|(q-1)\). For any multiplicative character \(\chi\) on \(\mathbb{F}_q^*\) and positive integer \(j\) let

\[
G_j(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi_j(x) \psi_j(x),
\]

where \(\chi_j = \chi(Norm_j)\) is the extension of \(\chi\) to \(\mathbb{F}_{q^j}\). Then

\[
S_j = \sum_{x \in \mathbb{F}_q} \psi_j(ax^d) = \sum_{x \in \mathbb{F}_q} \left( \sum_{\chi_j = 1} \chi_j(x) \right) \psi_j(ax) = \sum_{\chi_j = 1} \chi_j(a) G_j(\chi, \psi).
\]

Now by the Hasse-Davenport relationship \(G_j(\chi, \psi) = (-1)^{j+1} G_1(\chi, \psi)^j\), and the fact that \(\chi_j(a) = (\chi(a))^j\) for \(a \in \mathbb{F}_q\), we deduce that

\[
S_j = -\sum_{\chi_j = 1} (-\overline{\chi(a)} G_1(\chi, \psi))^j.
\]

It follows that the \(L\)-function associated with the pair \((\mathbb{A}^1, aX^d)\) is given by

\[
L(t) = \prod_{\chi_j \neq 1, \chi_j \neq 1} (1 + \overline{\chi(a)} G_1(\chi, \psi) t).
\]

Also, it is well known that \(|G_1(\chi, \psi)| = q^{1/2}\) for all nontrivial characters \(\chi\). Thus the pair \((\mathbb{A}^1, aX^d)\) is pure of weight 1 with \(B_1 = (d - 1)\).

Weil (1948b) obtained the following generalization of the previous two examples.
Example 4.1.13. Let \( g(X) \) be any polynomial over \( \mathbb{F}_q \) of degree \( d \) not divisible by \( p \). Then \( (\mathbb{A}^1, g(X)) \) is pure of weight 1 and \( B_1 = (d - 1) \). In particular,

\[
| \sum_{x \in \mathbb{F}_q} \psi(g(x)) | \leq (d - 1) q^{1/2}.
\]

Actually, in his (1948b) paper Weil only obtains \( B_1 \leq d - 1 \). Bombieri (1966, Lemma 4) proves that \( B_1 = d - 1 \). Serre (1977) deduces that \( B_1 = d - 1 \) from a more general result of Weil on exponential sums over curves.

Example 4.1.14. Kloosterman sums. Let \( \overline{V} \) be the hypersurface defined by \( x_1 x_2 \cdots x_n = c, n > 1, c \neq 0 \), and \( g(X) = \sum_{i=1}^{n} a_i X_i \) with \( a_i \neq 0 \) for all \( i \). Then \( (\overline{V}, g) \) is pure of weight (n-1), and \( B_{n-1} = n \). Thus

\[
|S_j| = \left| \sum_{x_1 \cdots x_n = c} \psi(\sum_{i=1}^{n} a_i x_i) \right| \leq nq^{\frac{n-1}{2}}.
\]

The case \( n = 2 \) was proven by Weil (1948b), and the general case by Deligne (1977, Theorem 7.4).

On the other hand, if exactly \( r \) of the \( a_i \) are 0 with \( r > 0 \), then it is elementary to show that

\[
S_j = (-1)^{n-r}(q^d - 1)^{r-1} = (-1)^{n-r} \sum_{i=0}^{r-1} \binom{r-1}{i} q^{j_i}.
\]

Thus for \( i = 0, 1, \ldots, (r - 1) \) there are \( \binom{r-1}{i} \) characteristic roots of weight 2i.

Theorem 4.1.15. Deligne (1973, Theorem 8.4). Let \( g \) be a polynomial in \( \mathbb{F}_q[X] \) of degree \( d \) not divisible by \( p \), and nonsingular at \( \infty \), (that is, the maximal homogeneous part of \( g \) is nonsingular). Then the pair \( (\mathbb{A}^n, g) \) is pure of weight \( n \) with \( B_n = (d - 1)^n \). Thus,

\[
\left| \sum_{x \in \mathbb{F}_q^n} \psi(g(x)) \right| \leq (d - 1)^n q^{n/2}.
\]

This theorem indicates that the upper bound of Bombieri (1978), \( (4d + 5)^n \), for the total number of characteristic values is of the correct order of magnitude. The case \( n = 1 \) of this theorem is just the result of Weil given in Example 4.1.13. Katz (1980) has indicated that Theorem 4.1.15 had been conjectured long ago by Mordell (no reference). More recently Bombieri (1966) conjectured the same result. He and Davenport (unpublished, but stated in Bombieri and Davenport (1966)) had established the result for cubic polynomials in 2 variables. To illustrate why it is natural to require the polynomial \( g \) to be nonsingular at infinity in the statement of the theorem we examine the case of quadratic polynomials.
Example 4.1.16. Quadratic polynomials. Let \( g(X) = \sum_{i=1}^{r} a_i X_i^2 + \sum_{i=1}^{n} b_i X_i + c \), with \( a_i \neq 0 \) for all \( i \) and \( r \leq n \). Then,

\[
| \sum_{x \in \mathbb{F}_q^n} \psi(g(x)) | = \begin{cases} 0 & \text{if some } b_i \neq 0, \ r + 1 \leq i \leq n, \\ q^{n - \frac{r}{2}} & \text{if } b_{r+1} = \ldots = b_n = 0. \end{cases}
\]

Thus \((\mathbb{A}^n, g)\) is pure of weight \( n \) if and only if \( r = n \), that is the maximal homogeneous part of \( g \) is nonsingular.

Katz (1980) gave the following generalization of Deligne's result.

Theorem 4.1.17. Katz (1980, Theorem 5.1.1). Suppose that \( \overline{V} \subset \mathbb{A}^n \) is such that \( \overline{V}_H \subset \mathbb{P}^n \) is a smooth, irreducible projective variety of dimension \( e \) over \( \mathbb{F}_q \) and that \( \overline{V}_\infty \in \mathbb{P}^{n-1} \) is also smooth. Let \( g \) be a polynomial of degree \( D \) over \( \mathbb{F}_q \) with \( p \nmid D \) such that the projective variety defined by the maximal homogenous part of \( g \) is transverse to \( \overline{V}_\infty \). Then the pair \((\overline{V}, g)\) is pure of weight \( e \).

Moreover, in the case that \( \overline{V} \) is a complete intersection Katz gives a formula for the Betti number \( B_e \) arising in Theorem 4.1.17. In particular if \( \overline{V} \) is a hypersurface of degree \( d \) and \( g \) a polynomial of degree \( D \) then,

\[
B_e = \left| \frac{d}{d - D} [(d - 1)^n - (D - 1)^n] \right|, \tag{4.1.18}
\]

for \( d \neq D \). If \( d = D \) then \( B_e = nd(d-1)^{n-1} \). Deligne's result, Theorem 4.1.15, is obtained by taking \( \overline{V} = \mathbb{A}^n \). Katz (1980) also gives several more general results of the nature of Theorem 4.1.17. A special case that Katz had already stated in (1977) is the following example which Hooley needed for his work on the Waring Problem.

Example 4.1.19. Let \( \overline{V} \) be the hypersurface defined by the polynomial \( f(X_1, X_2, X_3) \) of degree \( d \) and \( g \) be the linear polynomial \( g(X) = a_1 X_1 + a_2 X_2 + a_3 X_3 \). Then assuming the smoothness conditions of Theorem 4.1.17 we have,

\[
\left| \sum_{x \in \overline{V}} \psi(a_1 x_1 + a_2 x_2 + a_3 x_3) \right| \leq d(d - 1)^2 q.
\]

We note that \( \overline{V}_H \) is a smooth, irreducible projective variety if both \( \overline{V} \) and \( \overline{V}_\infty \) are smooth and the former is irreducible. However, it is not necessary that \( \overline{V}_\infty \) be smooth, as the following example illustrates.

Example 4.1.20. Let \( \overline{V} \subset \mathbb{A}^n \) be the hypersurface defined by the irreducible polynomial \( f = f_d + f_{d-1} + \ldots + f_0 \) where \( f_i \) indicates the homogeneous part of \( f \) of degree \( i \), \( 0 \leq i \leq d \). Then \( \overline{V}_H \) is the projective variety defined by \( F(X_0, X) = f_d(X) + X_0 f_{d-1}(X) + \ldots + X_0^d f_0 = \ldots \)
\( X^d f(X/X_0) \). Computing partial derivatives it is straightforward to check that \( \overline{V}_H \) is nonsingular if and only if \( \overline{V} \) is nonsingular and the system of equations

\[
\frac{\partial f_i}{\partial x_i}(x) = 0, \ 1 \leq i \leq n \quad \text{and} \quad f_{d-1}(x) = 0,
\]

has only the trivial solution \( x = 0 \). We see in particular that if \( \overline{V}_H \) is nonsingular then \( \overline{V}_\infty \) can have at most isolated singularities. For example if \( f = Q(X_1, \ldots, X_{n-1}) + X_n \), with \( Q \) a nonsingular quadratic form in \( n - 1 \) variables, then \( \overline{V} \) and \( \overline{V}_H \) are nonsingular, but \( \overline{V}_\infty \) has the singularity \( x_1 = x_2 = \ldots = x_{n-1} = 0 \).

Laumon (1983) obtained a result similar to Theorem 4.1.17 for diagonal polynomials satisfying sufficient nonsingularity conditions. Let \( f(X) = 1 + \sum_{i=1}^n c_i X_i^{d_i} \) be a diagonal polynomial over \( \mathbb{F}_q \) with \( d_i > 0 \) and \( c_i \neq 0 \) for all \( i \) and \( g(X) = \sum_{i=1}^n a_i X_i \), with the \( a_i \) not all zero. Let \( 1 \leq d_1 < d_2 < \cdots < d_N \) be the distinct values of the \( d_i \), and \( d \) be their least common multiple. For \( i = 1, 2, \ldots, n \) set \( r_i = d/d_i \) and for \( \nu = 1, 2, \ldots, N \) set \( r_\nu = d/d_\nu \),

\[
I_\nu = \{ i | d_i = d_\nu \} = \{ i | r_i = r_\nu \}, \quad I'_\nu = \{ i \in I_\nu | a_i \neq 0 \}, \quad \text{and}
\]

\[
I' = \bigcup_{\nu=1}^N I'_\nu = \{ i | a_i \neq 0 \}.
\]

**Theorem 4.1.22.** Laumon (1983). Let \( \overline{V} \subset \mathbb{A}^n \) be the hypersurface defined by the diagonal polynomial \( f(X) = 1 + \sum_{i=1}^n c_i X_i^{d_i} \) and suppose that

(i) \( p \nmid d \) and

(ii) for any value of \( \nu \) such that \( I'_\nu \) contains at least 2 elements the hypersurfaces

\[
\sum_{i \in I'_\nu} a_i x_i^{r_\nu} = 0 \quad \text{and} \quad \sum_{i \in I'_\nu} c_i x_i^d = 0,
\]

in \( \mathbb{A}^{\mid I'_\nu \mid} \) are transverse away from the origin. Then the pair \( (\overline{V}, \sum_{i=1}^n a_i X_i) \) is pure of weight \( n - 1 \) and

\[
B_{n-1} = \frac{d_{\nu_0}}{d_{\nu_0} - 1} \prod_{i=1}^n (d_i - 1)
\]

where \( \nu_0 \) is the smallest index such that \( I_{\nu_0} \neq \emptyset \).

A couple of remarks are in order. First, if \( p \mid d_i \) for some \( i \) then by writing \( d_i = p^{s_i} d'_i \) and replacing \( X_i \) with \( Y_i = X_i^{p^{s_i}} \), we can still apply the theorem. Second, if the exponents \( d_i \) are all distinct then hypothesis (ii) in the theorem holds automatically.

Another very general case where purity results are obtained derives from the results on exponential sums over Tori discussed in section 4.5. Indeed, most of the results mentioned in this section are corollaries of Theorem 4.5.15.
4.2. The Interplay between Characteristic Values and Bounds on Exponential Sums

In section 4.1 we saw that the exponential sums $S_j$ are given by

$$S_j = \alpha_1^j + \cdots + \alpha_k^j - \beta_1^j - \cdots - \beta_m^j, \quad (4.2.1)$$

where the $\alpha_i$, $\beta_i$ are the characteristic values of the associated $L$-function. We may assume that $\alpha_i \neq \beta_j$ for all $i, j$. Thus it is plain that an upper bound on the total number of characteristic values and on their weights yields a corresponding upper bound on the sums $S_j$; see (4.1.6) and (4.1.8). In particular if there are $B$ characteristic values of maximum weight $M$ then,

$$\limsup_{j \to \infty} \frac{|S_j|}{q_j^M} \leq B. \quad (4.2.2)$$

If the signs in (4.2.1) are all positive or all negative, we actually obtain equality in (4.2.2). This observation follows from the more general

**Lemma 4.2.3.** Katz (1980, Lemma 2.2.2.1). If $z_1, \ldots, z_k$ are complex numbers with $|z_i| \leq 1$, and $S_j = \sum_{i=1}^k z_i^j$, then

$$\limsup_{j \to \infty} |S_j| = |\{i : |z_i| = 1\}|.$$

**Proof.** We may assume that all of the $z_i$ have modulus 1. Let $C$ be the unit circle in the complex plane and let $\eta : \mathbb{Z} \to \mathbb{C}^k$ be the mapping $\eta(n) = (z_1^n, \ldots, z_k^n)$. If $\eta(\mathbb{Z})$ is discrete then for infinitely many $n$ we must have $\eta(n) = (1, 1, \ldots, 1)$, whence $S_j = k$ for all $j$. If $\eta(\mathbb{Z})$ is not discrete then $(1, 1, \ldots, 1)$ is a limit point and hence the sums $S_j$ get arbitrarily close to $k$. \qed

Going in the other direction we note that an upper bound on the $S_j$ for all sufficiently large $j$ implies in return an upper bound on both the weights of the characteristic values as well as the number of characteristic values of maximum weight, as indicated in the following theorem of Bombieri.

**Theorem 4.2.4.** Bombieri (1978, Theorem 3). Let the sums $S_j$ be as above. Then,

(i) If $|S_j| = O(q^{\theta j/2})$ for some positive real number $\theta$, then $|S_j| = O(q^{\theta j/2})$.

(ii) If $M$ is a positive integer such that $|S_j| \leq Cq^{M j/2}$ for all sufficiently large $j$, then the characteristic values have weight at most $M$ and there are at most $C^2$ characteristic values of weight $M$.

(iii) If $M$ is the maximum weight of the characteristic values and if there are $B$ values of weight $M$ then for any $\epsilon > 0$ and infinitely many $j$ we have $|S_j| > (B^{1/2} - \epsilon)q^{M j/2}$.

The theorem follows from
Lemma 4.2.5. Bombieri and Davenport (1966, Lemma 3). Let \( z_1, \ldots, z_m \) be distinct complex numbers of modulus 1 and \( b_1, \ldots, b_m \) be arbitrary complex numbers. Then

\[
\limsup_{n \to \infty} \left| \sum_{i=1}^{m} b_i z_i^n \right| \geq \left( \sum_{i=1}^{m} |b_i|^2 \right)^{1/2}.
\]

Proof. For any positive integer \( N \) we have

\[
\sum_{n=0}^{N} \left| \sum_{i=1}^{m} b_i z_i^n \right|^2 = \sum_{i,j} b_i \overline{b}_j \left( \sum_{n=0}^{N} (z_i \overline{z}_j)^n \right)
\]

\[
= (N + 1) \sum_{i=1}^{m} |b_i|^2 + O(\sum_{i \neq j} |b_i \overline{b}_j|) = (N + 1) \sum_{i=1}^{m} |b_i|^2 + O(1),
\]

and so

\[
\lim_{N \to \infty} \frac{1}{N + 1} \sum_{n=0}^{N} \left| \sum_{i=1}^{m} b_i z_i^n \right|^2 = \sum_{i=1}^{m} |b_i|^2,
\]

which implies the statement of the lemma. \( \square \)

Proof of Theorem 4.2.4. It is clear that (iii) implies (ii) and that by the Riemann Hypothesis (iii) implies (i). Thus it suffices to prove part (iii). Denote the distinct characteristic values of maximum weight \( M \) by \( \gamma_1, \ldots, \gamma_k \), and write

\[
S_j = \sum_{i=1}^{k} b_i \gamma_i^j + O(q^{M-1/2} j) = q^{M/2} \sum_{i=1}^{k} b_i z_i^j + O(q^{M-1/2} j),
\]

where \( |b_i| \) denotes the multiplicity of \( \gamma_i \) and \( z_i = e^{\frac{2\pi i}{|\gamma_i|}} \). Then for any \( \epsilon > 0 \) it follows from Lemma 4.2.5 that for infinitely many \( j \) we have

\[
|S_j| > q^{M/2} \left( \sum_{i=1}^{k} |b_i|^2 \right)^{1/2} - \epsilon \geq q^{M/2} [B^{1/2} - \epsilon],
\]

proving the theorem. \( \square \)

In particular, if there are \( B \) characteristic values of maximum weight \( M \) then

\[
\limsup_{j \to \infty} \left| \frac{S_j}{q^{M/2}} \right| \geq \left( \sum_{i=1}^{k} |b_i|^2 \right)^{1/2} \geq \sqrt{B},
\]

the values \( |b_i| \) being again the multiplicities of the characteristic values of maximal weight. This result is weaker than the equality obtained in (4.2.2) under the assumption that all of the signs in (4.2.1) are the same.

A generalization of Lemma 4.2.5 that one may have occasion to use is
Lemma 4.2.6. Let \( r \) and \( \ell \) be fixed positive integers. Let \( z_1, \ldots, z_m \) be distinct complex numbers of modulus 1 such that \( z_i^r \neq z_j^r \) for \( i \neq j \) and \( b_1, \ldots, b_m \) be arbitrary complex numbers. Then

\[
\limsup_{n \to \infty} \sum_{n \equiv \ell \pmod{r}} \left| \sum_{i=1}^{m} b_i z_i^n \right| \geq \left( \sum_{i=1}^{m} |b_i|^2 \right)^{1/2}.
\]

The same proof holds here as well. We note that the assumption that \( z_i^r \neq z_j^r \) for \( i \neq j \) is essential, the lemma being false otherwise. Hooley (1980, Lemma 10) made use of this generalization for the case \( n \equiv 1 \pmod{2} \).

The special case relevant to our study of \( L \)-functions is when the \( z_i \) are just the roots of a polynomial with coefficients in \( \mathbb{Q}(\xi_p) \). Suppose in this case that \( r \) is a prime not equal to \( p \) with \( r > [\mathbb{Q}(\xi_p, z_1, \ldots, z_m) : \mathbb{Q}(\xi_p)] \). Then we will never have \( z_i^r = z_j^r \) for \( i \neq j \). On the other hand, if we have \( z_i^r = z_j^r \) for some \( i \neq j \) and moreover that \( z_i, \xi r z_i, \ldots, \xi^{r-1} z_i \) are all roots of the polynomial then if \((\ell, r) = 1\) and \( n \equiv \ell \pmod{r} \) we have

\[
z_i^n + (\xi r z_i)^n + \cdots + (\xi^{r-1} z_i)^n = 0.
\]

In other words such values of \( z_i \) give no contribution to the sum in Lemma 4.2.6.

4.3. Homogeneous Exponential Sums

We call the exponential sum

\[
S_j = S_j(V_j, g) = \sum_{x \in V_j} \psi_j(g(x))
\]

homogeneous if both the polynomials defining \( V \) as well as the polynomial \( g \) are homogeneous. A simple trick allows one to express such sums in terms of the cardinalities of the sets \( V_j \) and \( V_j \cap H_j \), where \( H \) is the hypersurface defined by \( g \), whenever the degree \( D \) of \( g \) is relatively prime to \( q^j - 1 \). In this case for any nonzero \( \lambda \in \mathbb{F}_q^* \), \( S_j(V_j, \lambda g) = S_j(V_j, g) \).

Summing over \( \lambda \) we see that

\[
(q^j - 1) S_j = \sum_{\lambda \neq 0} \sum_{x \in V_j} \psi_j(g(x)) = \sum_{x \in V_j} \left( \sum_{\lambda} \psi_j(\lambda g(x)) - 1 \right)
\]

\[
= q^j |V_j \cap H_j| - |V_j| = q^j \left( (q^j - 1)|V_j \cap H_j|_{\mathfrak{p}} + 1 \right) - ((q^j - 1)|V_j|_{\mathfrak{p}} + 1).
\]

Thus, if \( D \) is relatively prime to \( q^j - 1 \) then

\[
S_j = (q^j - 1)^{-1} \left( q^j |V_j \cap H_j| - |V_j| \right) = q^j |V_j \cap H_j|_{\mathfrak{p}} - |V_j|_{\mathfrak{p}} + 1. \quad (4.3.1)
\]

In particular, \( S_j \) is an integer. Identities of this type have appeared many places in the literature, perhaps the first being in the work of Chalk and Williams (1965, Lemma 15).
Example 4.3.2. If $V$ is defined by a nonsingular quadratic form $Q$ over $\mathbb{F}_q$ with $q$ odd, and $g(X) = \sum_{i=1}^{n} y_i X_i$ is any linear form, then (4.3.1) provides a way of evaluating the exponential sum

$$S(V, y) = \sum_{x \in V} \psi(\sum_{i=1}^{n} y_i x_i),$$

(4.3.3)

without resorting to any knowledge of Gaussian sums. Suppose that $n$ is even. Let $H = H(y)$ be the hyperplane defined by $g$ and $H = H_1$. If $V \cap H$ is nonsingular then $|V \cap H| = q^{n-2}$. If the intersection has singularities then $|V \cap H| = q^{n-3} + \Delta(q-1)q^{n-2}$, where $\Delta$ is as given in Example 3.4. Moreover, one can easily see that the intersection is singular if and only if $Q^*(y) = 0$, where $Q^*$ is the quadratic form associated with the inverse of the matrix representing $Q$. Thus by (4.3.1), if $n$ is even and $y \neq 0$, then

$$S(V, y) = \begin{cases} -\Delta q^{\frac{n}{2}-1} & \text{if } Q^*(y) \neq 0 \\ \Delta q^{\frac{n}{2}-1}(q-1) & \text{if } Q^*(y) = 0 \end{cases}$$

One can argue similarly for odd $n$.

If $D$ is relatively prime to $q-1$ then there will be infinitely many values of $j$ for which $(D, q^j - 1) = 1$ and therefore (4.3.1) holds true. The question then arises whether (4.3.1) holds true for all values of $j$ in such a case. The answer is no, as the following example illustrates.

Example 4.3.4. Let $V = \mathbb{A}^n$ and $g(X) = X_1^3$. Then for any value of $j$ the righthand side of (4.3.1) is zero while the lefthand side is zero if and only if $3 \mid (q^j - 1)$. Indeed, if we suppose that $q$ is such that $3 \mid q(q-1)$ then for any $j$,

$$S_j = -q^{(n-1)j}((\sqrt{q})^j + (\sqrt{q})^{-j}),$$

where $G$ is the Gaussian sum in Example 4.1.12 with $q$ replaced by $q^3$, and $\chi$ is any multiplicative character on $\mathbb{F}_q^*$. Thus for any odd value of $j$, $S_j = 0$. On the otherhand for even $j$ we have $|S_j| = 2q^{(n-3)j}$.

More generally, if two polynomials $g_1$ and $g_2$ have the same set of absolutely irreducible factors but with different multiplicities then the righthand side of (4.3.1) will be the same for both polynomials but the exponential sum on the left will in general be different. However, it is perhaps nontrivial to observe that in the same case if the degrees of $g_1$ and $g_2$ are relatively prime to $q^j - 1$ then the exponential sums for $g_1$ and $g_2$ have the same value. If $g$ is absolutely irreducible is the answer to the question above still no?

Using the cardinality estimates of section 3 we deduce from (4.3.1) the following theorem.

Theorem 4.3.5. If $V \subset \mathbb{A}^n$ is a homogeneous algebraic set of dimension $e$ and $g$ a homogeneous polynomial such that none of the irreducible components of $V$ are contained in the hypersurface $H$ defined by $g$ then for any $j$ such that the degree $D$ of $g$ is relatively prime to $(q^j - 1)$ we have,

$$|S_j| \ll q^{(e-1)j}. \quad (4.3.6)$$

30
Proof. In this case $\overline{V} \cap \overline{H}$ is of dimension $e - 1$, viewed as a subset of affine space and dimension $e - 2$ viewed as a subset of projective space. Thus by (3.19), the righthand side of (4.3.1) is bounded above by $c(d, D, n, s)q^{(e-1)j}$. \hfill \square

Note that the bound in (4.3.6) is better than the analogous bound for nonhomogeneous sums, (4.4.9), by a factor of $q^{j/2}$. If $D$ and $q^j - 1$ have a common factor then the theorem does not apply. Indeed (4.3.6) may not hold true in this case as Example 4.3.4 illustrated. If $D$ is relatively prime to $q - 1$ then (4.3.6) holds for infinitely many $j$, but again Example 4.3.4 illustrates that one cannot conclude from this that (4.3.6) is then valid for all $j$. In particular, one cannot conclude that all of the characteristic values of the $L$-function associated with $\overline{V}$ and $g$ have weights $\leq 2(e - 1)$.

The upper bound in (4.3.6) is easily seen to be best possible if no further restrictions are placed on $V$.

Example 4.3.7. Let $V$ be defined by $x_1x_2\cdots x_{n-1} - x_n^{n-1} = 0$, with $n \geq 2$. Then $|V| = q^{n-1}$. If $H(y)$ is the hyperplane $x_n = 0$, then $|V \cap H(y)| = q^{n-1} - (q - 1)^{n-1}$, and so by (4.3.1) if $(n - 1, q - 1) = 1$ then

$$S(V, g) = q(q^{n-2} - (q - 1)^{n-2}) \geq (n - 2)(q - 1)^{n-2}.$$

The algebraic set $\overline{V}$ in the preceding example is absolutely irreducible and not contained in the hyperplane $H(y)$, but its intersection with $H(y)$ is reducible. We can sharpen the upper bound in (4.3.6) by a factor of $q^{1/2}$ if we impose the extra condition that $\overline{V} \cap \overline{H}$ be absolutely irreducible.

Theorem 4.3.8. If $\overline{V} \subset \mathbb{A}^n$ is a homogeneous algebraic set of dimension $e$ such that $\overline{V} \cap \overline{H}$ is irreducible, of dimension $e - 1$, then for $(D, q^j - 1) = 1$ we have

$$|S_j| \ll q^{(e-\frac{3}{2})j}. \quad (4.3.9)$$

The result of this theorem is simply obtained by inserting the cardinality estimate of (3.18) into (4.3.1). A sharper upper bound can be had if the singular locus of $\overline{V} \cap \overline{H}$ is of small enough dimension.

Theorem 4.3.10. Skorobogatov (1992, Theorem 3.2) Suppose that $\overline{V} \subset \mathbb{A}^n$ is an irreducible homogeneous algebraic set of dimension $e$ and that $g$ is a homogeneous polynomial of degree $D$ with $D$ relatively prime to $q - 1$. Suppose further that $\overline{V}$ is not contained in the hypersurface $\overline{H}$ defined by $g$ and that $\overline{V} \cap \overline{H} \subset \mathbb{P}^{n-1}$ has a singular locus of dimension $e^*$. Then for any $j$ such that $(D, q^j - 1) = 1$ we have

$$|S_j| \ll q^{(\frac{e+e^*+1}{2})j}. \quad (4.3.11)$$

Proof. Skorobogatov gives a cohomological proof of this theorem. Under the slightly stronger hypotheses that $\overline{V}$ and $\overline{V} \cap \overline{H}$ be irreducible complete intersections and that the
former have singular locus of dimension \( \leq (\ell^* + 1) \), it is easy to deduce (4.3.11) from (4.3.1) and (3.29). In this case we have

\[
|V_j|_p = (q^{(e-1)}j + q^{(e-2)}j + \ldots + 1) + \theta_1 q^{\left( \frac{e+\ell^*+1}{2} \right)}j,
\]

and

\[
|V_j \cap H_j|_p = (q^{(e-2)}j + q^{(e-3)}j + \ldots + 1) + \theta_2 q^{\left( \frac{e+\ell^*+1}{2} \right)}j,
\]

for some constants \( \theta_1, \theta_2 \ll 1 \).

Inequality (4.3.11) is sharper than (4.3.9) whenever \( \ell^* < e - 4 \).

4.4. Hooley's Method of Second Moments and Upper Bounds on General Exponential Sums

In his work on Waring type problems Hooley (1980, §9), (1981a, §10), and (1981b, §10) introduced a method for bounding the weights of the characteristic values of \( L \)-functions without resorting to further cohomology theory; his starting point being the results of Deligne (1980, Weil II) given in Proposition 4.1.4. He outlined the method in more generality in his (1982) work. His method cannot be used to prove "purity" type results as far as we know, but it can be applied to a number of \( L \)-functions that cohomological methods currently cannot address.

We shall use the same notation as in section 4.1. In particular \( d \) will denote the maximum of the degrees of the polynomials \( f_i \) defining \( V \) and the polynomial \( g \). For any nonzero value \( \lambda \in \mathbb{F}_{q^d} \) let

\[
S_j(\lambda) = \sum_{x \in V_j} \psi_j(\lambda g(x)),
\]

so that \( S_j(1) = S_j \), and let \( M_j \) denote the second moment,

\[
M_j = \sum_{\lambda \in \mathbb{F}_{q^d}, \lambda \neq 0} |S_j(\lambda)|^2. \tag{4.4.1}
\]

Let \( \gamma_1, \ldots, \gamma_k \) denote the distinct characteristic values associated with the sums \( S_j \) so that \( S_j = \sum_{i=1}^k e_i \gamma_i^j \), for some integers \( e_i \).

There are two key ingredients in Hooley's method. The first is that if \( \lambda \) is in the base field \( \mathbb{F}_p \), \( (q = p^r) \), then the coefficients of the \( L \)-function

\[
L_\lambda(t) = \exp \left\{ \sum_{j=1}^{\infty} \frac{S_j(\lambda)t^j}{j} \right\}.
\]

and of \( L(t) = L_1(t) \) are just conjugates, and therefore so are their characteristic values. Thus we can write

\[
S_j(\lambda) = \sum_{i=1}^k e_i \gamma_i^j \lambda.
\]
where \( \gamma_{i,\lambda}^j \) denotes the appropriate conjugate of \( \gamma_i \). The second key ingredient is the fact that the conjugates of a given characteristic value all have the same modulus, by Proposition 4.1.4. Let \( M \) denote the maximum weight of the characteristic values and \( B \) denote the number of values of maximum weight counted with multiplicity. Then for any nonzero \( \lambda \in \mathbb{F}_p \) we have

\[
S_j(\lambda) = q^{M_j} \sum_{i=1}^{K} e_{i} z_{i,\lambda}^j + O(q^{(M-1)j/2}),
\]

(4.4.2)

for some distinct complex numbers \( z_{i,\lambda} \) of modulus 1. Thus

\[
\limsup_{j \to \infty} \frac{|S_j(\lambda)|^2}{q^{M_j}} = \limsup_{j \to \infty} \left| \sum_{i=1}^{K} e_{i} z_{i,\lambda}^j \right|^2 \geq \left| \sum_{i=1}^{K} e_{i}^2 \right| \geq B,
\]

the first inequality following from Lemma 4.2.5. Summing over the \((p-1)\) nonzero values of \( \lambda \) in the base field we obtain

\[
\limsup_{j \to \infty} \frac{M_j}{q^{M_j}} \geq (p-1)B.
\]

(4.4.3)

This yields

**Proposition 4.4.4.** Suppose that \( N \) and \( C \) are positive real numbers such that \( M_j \leq C q^{Nj} \) for all \( j \) sufficiently large, and that \( p > \frac{C}{B} + 1 \). Then all of the characteristic values associated with the sums \( S_j \) have weights strictly less than \( N \).

Indeed, in the definition of the second moment \( M_j \) we could have restricted the sum to values of \( \lambda \) in the base field and the proposition would remain valid. However, it is more useful to work with the complete sum because of the nice geometric interpretation it permits.

For any nonzero \( \lambda \in \mathbb{F}_{q^j} \) we can write

\[
S_j(\lambda) = \sum_{\tau \in \mathbb{F}_{q^j}} N_j(\tau) \psi_j(\lambda \tau),
\]

where

\[
N_j(\tau) = |V_j \cap H_j(\tau)|,
\]

(4.4.5)

and \( H_j(\tau) \) is the set of points on the hypersurface \( \overline{H}(\tau) \) defined by \( g(x) = \tau \), with coordinates in \( \mathbb{F}_{q^j} \). In fact for any constant \( c \) (not depending on \( \tau \)) we have

\[
S_j(\lambda) = \sum_{\tau \in \mathbb{F}_{q^j}} (N_j(\tau) - c) \psi_j(\lambda \tau),
\]

(4.4.6)
for nonzero $\lambda$. Defining $S_j(0)$ formally by the expression in (4.4.6), we obtain
\[ M_j \leq \sum_{\lambda \in \mathbb{F}_{q^{j}}} |S_j(\lambda)|^2 = q^j \sum_{r \in \mathbb{F}_{q^{j}}} |N_j(r) - c|^2. \tag{4.4.7} \]

We note in passing that the moment $M_j$ can be expressed in the alternative manner,
\[ M_j = q^j \sum_{x,y \in V_j \atop g(x) = g(y)} 1 - |V_j|^2, \]

but we have found no special use for this manner of expression.

**Upper Bounds on General Exponential Sums.**

We start by remarking that for any $L$-function the characteristic values always have weights $\leq 2e$ where $e$ is the dimension of $\mathbb{V}$, by Proposition 4.1.4. The maximum weight will equal $2e$ if $g$ is constant on some irreducible component of $\mathbb{V}$. Indeed, in this case if $\mathbb{V}$ is irreducible and $g = \tau$ identically on $\mathbb{V}$, then $S_j = \psi_j(\tau)N_j$ for all $j$, and so the characteristic values of the $L$-function are just the characteristic values of the zeta function for $\mathbb{V}$ multiplied by a fixed $p^{th}$ root of unity. On the other hand we have

**Theorem 4.4.8.** Suppose that $p > (4d + 9)^{2(n+s+1)}$ and that $g$ is not constant on any irreducible component of $\mathbb{V}$. Then the characteristic values of the $L$-function associated with $\mathbb{V}$ and $g$ all have weights strictly less than $2e$, and so for all $j$,
\[ |\sum_{x \in V_j} \psi_j(g(x))| \leq (4d + 9)^{n+s}q^j(e^{-\frac{1}{2}}). \tag{4.4.9} \]

**Proof.** In this case $\mathbb{V} \cap \overline{H}(\tau)$ is of dimension $(e - 1)$ for all $\tau$ and so by (3.19) we have for all $j$,
\[ M_j \leq q^j \sum_{\tau} |N_j(\tau)|^2 \leq q^j(4d + 9)^{2(n+s+1)} \sum_{\tau} q^{(e-1)2j} \leq (4d + 9)^{2(n+s+1)}q^{2ej}. \]

The result now follows from Proposition 4.4.4. $\square$

If $\mathbb{V} \cap \overline{H}(\tau)$ is irreducible for almost all $\tau$ then we have the stronger result,

**Theorem 4.4.10.** Suppose that $p > (1+c^*)((d+9)^{2(n+s+1)}+1$, that $g$ is not constant on any irreducible component of $\mathbb{V}$ and that $\mathbb{V} \cap \overline{H}(\tau)$ is irreducible for all but $c^* = c^*(d,n,s)$ values of $\tau$. Then the characteristic values of the $L$-function associated with $\mathbb{V}$ and $g$ all have weights $\leq 2e - 2$. 

34
Proof. In this case we put \( c = q^{(e-1)j} \) in (4.4.7). Then by Theorem 3.17 (using the Bombieri constant (3.13)) we have

\[
M_j \leq q^j \sum_{\tau} (4d + 9)^{2(n+s+1)}q^{(2e-3)j} + c^*q^j (4d + 9)^{2(n+s+1)}q^{(2e-2)j} \\
\leq (1 + c^*) (4d + 9)^{2(n+s+1)}q^{(2e-1)j},
\]

for all \( j \) sufficiently large. \( \Box \)

The irreducibility conditions requisite for this theorem to apply will be satisfied if the generic algebraic set defined by

\[
f_1(x) = \cdots = f_s(x) = 0, \quad g(x) = t, \quad (4.4.11)
\]

where \( t \) is an indeterminate, is irreducible over \( \overline{F}_q(t) \). If such is the case then for \( p > c(d, n, s) \) and any \( j \) we have,

\[
| \sum_{x \in V_j} \psi_j(g(x)) | \leq (4d + 9)^{n+s}q^{j(e-1)}. \quad (4.4.12)
\]

We can make a more precise statement by utilizing the concept of the singular locus. Let \( \overline{H}(\tau) \) denote the hypersurfaces \( g = \tau \), and let \( \overline{V}_H \subset \mathbb{P}^n \) and \( \overline{V}_\infty \subset \mathbb{P}^{n-1} \) be as defined in section 3. In the same manner we let \( \overline{H}_H(\tau) \) and \( \overline{H}_\infty(\tau) \) denote the hypersurfaces defined by \( G = \tau X^n_{n+1} \) and \( g_D = 0 \) respectively, where \( G \) is the homogenization of \( g \) and \( g_D \) its maximal homogeneous part. Then by (3.23) we have

\[
N_j(\tau) = |V_{H,j} \cap H_{H,j}(\tau)|_P - |V_{\infty,j} \cap H_{\infty,j}(\tau)|_P. \quad (4.4.13)
\]

The important thing to notice here is that the second term on the righthand side of (4.4.13) is independent of \( \tau \) and so can be absorbed into the constant \( c \) in (4.4.7). Now, if \( \overline{V}_H \cap \overline{H}_H(\tau) \) is of dimension \( e - 1 \) then

\[
|V_{H,j} \cap H_{H,j}(\tau)|_P = q^{(e-1)j} + \theta(\tau)q^{\delta(\tau)j/2}, \quad (4.4.14)
\]

for some positive integer \( \delta(\tau) \leq 2(e-1) \) and constant \( |\theta(\tau)| < c(d, n, s) \). Setting

\[
c = q^{(e-1)j} - |V_{\infty,j} \cap H_{\infty,j}(0)|_P
\]

in (4.4.7) we see from (4.4.13) and (4.4.14) that

\[
M_j \leq q^j \sum_{\tau \in \mathbb{F}_q} \theta(\tau)^2 q^{\delta(\tau)j} \leq q^j \sum_{\tau \in \mathbb{F}_q} q^{\delta(\tau)j}. \quad (4.4.15)
\]
Proposition 4.4.16. Suppose that $\delta$ is a positive integer such that for all $j$ sufficiently large we can take $\delta(\tau) = \delta$ in (4.4.14) for all but $c^* = c^*(d, n, s)$ values of $\tau \in \mathbb{F}_q$, and that for the remaining values of $\tau$ we can take $\delta(\tau) = \delta + 1$. Suppose also that $p > \theta^2(1 + c^*) + 1$, where $\theta = \max_{\tau} |\theta(\tau)|$. Then the characteristic values of the $L$-function associated with $\overline{V}$ and $g$ all have weights $\leq \delta + 1$.

Proof. By (4.4.15) we have that for $j$ sufficiently large,

$$M_j \leq \theta^2 q^j \sum_{\tau} q^{o_j} + c^* \theta^2 q^j q^{(\delta + 1)j} \leq \theta^2 (1 + c^*) q^{(\delta + 2)j},$$

and so the result follows from Proposition 4.4.4. $\square$

Theorem 4.4.17. Suppose that for all $\tau \in \mathbb{F}_q$, $\overline{V}_H \cap \overline{H}_H(\tau)$ is a complete intersection of dimension $e - 1$. Moreover suppose that the singular locus of $\overline{V}_H \cap \overline{H}_H(\tau)$ is of dimension $\leq \ell$ for all but $c^* = c^*(d, n, s)$ values of $\tau$ and that for the remaining values of $\tau$ the dimension is $\leq \ell + 1$. Then if $p > (1 + c^*)(4d + 9)^2(n + s + 2)(\frac{q}{q-1})^2$ the characteristic values of the $L$-function associated with $\overline{V}$ and $g$ all have weights $\leq e + \ell + 1$.

Proof. By Theorem 3.28, under the given hypotheses we can take $\delta = e + \ell$ in Proposition 4.4.16 and $\theta = (4d + 9)^{n + s + 2}(\frac{q}{q-1})$. $\square$

In particular, under the assumptions of Theorem 4.4.17 we have

$$\left| \sum_{\mathbf{x} \in \mathcal{V}_j} \psi(g(\mathbf{x})) \right| \leq (4d + 9)^{n + s} q^j \frac{e + \ell + 1}{2}. \quad (4.4.18)$$

Example 4.4.19. Diagonal Hypersurfaces. Let $\overline{V}$ be the diagonal hypersurface

$$a_1 x_1^d + a_2 x_2^d + \cdots + a_n x_n^d = c$$

with $a_i \neq 0$ for all $i$, $d > 1$, $p \nmid d$, and $g(\mathbf{X}) = \mathbf{y} \cdot \mathbf{X}$ with $\mathbf{y} \neq 0$. Then a point $\mathbf{x} = (x_1, \ldots, x_{n+1}) \in \overline{V}_H \cap \overline{H}_H(\tau)$ is a singular point if and only if for some $\lambda \in \mathbb{F}_q$

$$d a_i x_i^{d-1} = \lambda y_i, \quad 1 \leq i \leq n \quad \text{and} \quad d c x_{n+1}^{d-1} = \lambda \tau. \quad (4.4.20)$$

Suppose first that $c \neq 0$. Then the intersection has a singularity only if $\tau$ satisfies

$$\sum_{i=1}^{n} y_i \left( \frac{y_i}{d a_i} \right)^{1/d-1} = \tau \left( \frac{\tau}{d c} \right)^{1/d-1}$$

for some choice of $(d - 1)^{th}$ roots. Hence there are at most $d(d - 1)^n$ values of $\tau$ that yield singularities. For any such value $\tau$ there are at most $(d - 1)^{n+1}$ isolated singularities determined by (4.4.20). Thus we may take $\ell = -1$ and $c^* = d(d - 1)^n$ in Theorem 4.4.17.
and conclude that all of the weights are \( \leq n - 1 \). In summary, if \( c \neq 0 \) and \( p \) is sufficiently large then for any nonzero \( y \in \mathbb{F}_q^n \),

\[
\sum_{\sum a_i x_i^d = c} \psi(x \cdot y) \leq (4d + 9)^{n+1} q^{n-1}. \tag{4.4.21}
\]

Hooley (1981a) had treated the special case \( x_1^3 + x_2^3 + x_3^3 = N \) in exactly this manner.

Suppose now that \( c = 0 \). Then the only value of \( \tau \) that yields a singularity is \( \tau = 0 \). In this case, however, the set of singularities is a union of one-dimensional linear subspaces. Thus Theorem 4.4.17 can only be applied with \( \ell = 0 \). One is better off in this case to simply write

\[
\sum_{\sum a_i x_i^d = 0} \psi(x \cdot y) = q^{-1} \sum_{\lambda \neq 0} \prod_i \left( \sum \psi(\lambda a_i x_i^d + y_i x_i) \right) \leq (d - 1)^n q^{n/2}.
\]

**Example 4.4.22.** \( \overline{V}_H \) and \( \overline{V}_\infty \) nonsingular. The previous example can be generalized. Suppose that \( f \) is a polynomial of degree \( d > 1 \), \( p \nmid d \), such that both \( \overline{V}_H \subset \mathbb{P}^n \) and \( \overline{V}_\infty \subset \mathbb{P}^{n-1} \) are nonsingular hypersurfaces, \( \overline{V}_\infty \) being defined by the maximal homogeneous part of \( f \). We claim that for \( p \) sufficiently large, for any nonzero \( y \in \mathbb{F}_q^n \) the characteristic values of the \( L \)-function associated with \( \overline{V} \) and \( y \cdot x \) all have weights \( \leq n - 1 \).

By virtue of Theorem 4.4.8 we may readily dispense with the case \( n = 2 \). Indeed, the fact that \( \overline{V}_H \) is nonsingular implies in particular that the polynomial \( f \) is absolutely irreducible and hence has no linear factor. Thus for \( p \) sufficiently large and \( y \neq 0 \), all of the weights are \( \leq 1 \).

Henceforth we suppose that \( n \geq 3 \). Let \( F \) denote the homogenization of \( f \) in the variables \( X_1, \ldots, X_{n+1}, y \), a fixed nonzero point in \( \mathbb{F}_q^n \), and for any \( \tau \) let \( H(\tau) \) be the hyperplane \( x \cdot y = \tau \). Since \( \overline{V}_H \) is nonsingular it follows that the intersection \( \overline{V}_H \cap \overline{H}_H(\tau) \) has at most isolated singularities. We claim that the intersection \( \overline{V}_H \cap \overline{H}_H(\tau) \) is nonsingular for all but finitely many values of \( \tau \). To begin, we note that \( (x_1, \ldots, x_{n+1}) \) is a singular point of \( \overline{V}_H \cap \overline{H}_H(\tau) \) if and only if there is some \( \lambda \) such that

\[
\frac{\partial F}{\partial x_i} = \lambda y_i, \quad 1 \leq i \leq n, \quad \frac{\partial F}{\partial x_{n+1}} = -\lambda \tau, \quad \text{and} \quad x \cdot y = \tau x_{n+1}. \tag{4.4.23}
\]

Since \( F \) is a nonsingular form, (4.4.23) has no solution (in \( \mathbb{P}^n \)) when \( \lambda = 0 \). Suppose that \( \lambda \neq 0 \) and let \( \lambda^{1/(d-1)} \) denote a \( (d-1)^{th} \) root of \( \lambda \). Then \( x_1, \ldots, x_{n+1} \) satisfies (4.4.23) if and only if \( x_i/\lambda^{1/(d-1)}, 1 \leq i \leq n+1, \) satisfies

\[
\frac{\partial F}{\partial x_i} = y_i, \quad 1 \leq i \leq n, \quad \frac{\partial F}{\partial x_{n+1}} = -\tau, \quad \text{and} \quad x \cdot y = \tau x_{n+1}. \tag{4.4.24}
\]

In particular, we must have

\[
\frac{\partial F}{\partial x_i} = y_i, \quad 1 \leq i \leq n, \quad \text{and} \quad x_{n+1} \frac{\partial F}{\partial x_{n+1}} = -x \cdot y. \tag{4.4.25}
\]
For fixed $y$ we claim that (4.4.25) can have at most finitely many solutions in the $x_i$, for otherwise the solution set is of dimension $\geq 1$. But then the homogenization of (4.4.25),

$$\frac{\partial F}{\partial x_i} = y_i x_{n+2}^{d-1}, \quad 1 \leq i \leq n, \quad \text{and} \quad x_{n+1} \frac{\partial F}{\partial x_{n+1}} = -(x \cdot y) x_{n+2}^{d-1},$$

has a solution set of dimension $\geq 1$ in $\mathbb{P}^{n+1}$ and so its intersection with the hyperplane $x_{n+2} = 0$ must therefore be nonempty, that is, there exists a nonzero solution of

$$\frac{\partial F}{\partial x_i} = 0, \quad 1 \leq i \leq n, \quad \text{and} \quad x_{n+1} \frac{\partial F}{\partial x_{n+1}} = 0.$$ 

Since $F$ is a nonsingular form, we must have

$$\frac{\partial F}{\partial x_i} = 0 \quad 1 \leq i \leq n, \quad \text{and} \quad x_{n+1} = 0,$$

for some nonzero $(x_1, \ldots, x_n)$. But this contradicts the nonsingularity of $V_\infty$.

Having established that (4.4.25) has at most finitely many solutions it follows from Bezout's theorem that there are at most $d(d-1)^n$ solutions. Given any such solution, there is exactly one value of $\tau$ satisfying (4.4.24). Thus there are at most $d(d-1)^n$ values of $\tau$ for which the intersection $V_H \cap \overline{H}_H(\tau)$ has a singularity.

Now, in order to apply Theorem 4.4.17 we need $V_H \cap \overline{H}_H(\tau)$ to be irreducible for all values of $\tau$. When $n \geq 4$ this follows from the fact that $V_H$ is nonsingular. Indeed, the intersection of $V_H$ with any hyperplane is irreducible. For suppose without loss of generality that $\overline{H}_H(\tau)$ is just the hyperplane $x_1 = 0$. If the intersection is reducible then we would have

$$F = X_1 G(X_1, \ldots, X_{n+1}) + H_1(X_2, \ldots, X_{n+1}) H_2(X_2, \ldots, X_{n+1})$$

for some nonconstant polynomials $H_1, H_2$ and polynomial $G$. Since $n \geq 4$ the polynomials $X_1, G, H_1$ and $H_2$ would have a common zero in projective space and this zero would be a singularity of $F$. Thus when $n \geq 4$ we can apply Theorem 4.4.17 with $\ell = -1$ and conclude that for $p$ sufficiently large all of the weights are $\leq n - 1$.

Finally, when $n = 3$ we make an appeal to Theorem 4.4.10. We need only observe that nonsingularity of $V_H \cap \overline{H}_H(\tau)$ implies irreducibility, for the intersection is just the set of zeros of a form in three variables. Therefore, by our result above, $V_H \cap \overline{H}_H(\tau)$ is irreducible for all but finitely many values of $\tau$. Thus, for $p$ sufficiently large, the characteristic values all have weights $\leq 2e - 2 = 2$.

**Remark 4.4.28.** (i) The assumption that $V_\infty$ be nonsingular cannot be dropped from the argument of the preceding example. For example, if $V$ is the hypersurface, $x_1^3 + x_2^2 + x_3^2 = 1$ and $H(\tau)$ the hyperplane $x_1 + x_2 = \tau$, then $V_H$ is nonsingular, but for any value of $\tau$, $V_H \cap \overline{H}_H(\tau)$ has a singularity at $x_1 = 1, x_2 = -1, x_3 = \sqrt{-3\tau}$, $x_4 = 0$. However, for this
example we can still conclude that all of the characteristic values have weights \( \leq 2 \). See Examples 4.8.15 and 4.8.20. In fact, it is conceivable that the result of Example 4.4.22 is true under just the assumption that \( \overline{V}_H \) be nonsingular. We take up a further discussion of this question in section 4.8.

(ii) A second note that we make is that when \( n = 3 \) it is possible to have a polynomial \( f \) such that both \( \overline{V}_H \) and \( \overline{V}_\infty \) are nonsingular and yet \( \overline{V}_H \cap \overline{H}_H(\tau) \) is reducible for some hyperplane \( \overline{H}_H(\tau) \). Take for instance, \( f = X_1^2 + X_2 X_3 + X_1 \), and \( \overline{H}_H(\tau) \) the hyperplane defined by \( x_1 = 0 \).

**Example 4.4.29.** Birch and Bombieri (1985) applied the method of Hooley to the sum

\[
S(a, b) = \sum_{x_1^a x_2^b x_3 x_4^1} \psi(x_1 + x_2 + x_3 + x_4),
\]

and obtained for \( p \) sufficiently large

\[
|S(a, b)| \ll q^{3/2}.
\]

We shall see further applications of Theorem 4.4.17 in sections 4.6 and 4.7.

**Historical Comments.**

Special cases of Theorem 4.4.8 were known much earlier. Bombieri (1966) obtained the upperbound,

\[
|\sum_{x \in \mathcal{V}} \psi(g(x))| \leq (d_1^2 + 2d_1 d_2 - 3d_1)q^{1/2} + d_1^2,
\]

for exponential sums over a curve \( \overline{V} = \overline{V}(f) \subset A^2 \), where \( d_1 \) and \( d_2 \) are the degrees of \( f \) and \( g \) respectively, provided that \( g \) is not of the form \( h^p - h \) on any irreducible component of \( \overline{V} \). In fact, Bombieri proved the result for rational functions \( g \). Chalk and Smith (1971) gave a different proof of (4.4.30) in the case \( q = p \) and used their result to prove a big "Oh" version of (4.4.9) for sums over hypersurfaces.

**4.5. Exponential Sums on Tori**

Adolphson and Sperber (1989), (1990) and Denef and Loeser (1991) obtained "purity" type results for exponential sums on Tori. The former used the \( p \)-adic methods of Dwork while the latter used \( \ell \)-adic methods and obtained slightly stronger results. Let

\[
\mathbb{T}^n = \{ \mathbf{x} \in A^n : x_i \neq 0, \ 1 \leq i \leq n \},
\]

denote the \( n \)-dimensional Torus, and \( \mathbb{T}_j^n \) denote those points of the Torus with coordinates in \( \mathbb{F}_q^j \). The regular functions \( f \) on \( \mathbb{T}^n \) are just the polynomials in \( X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1} \).
\[ S_j = \sum_{x \in \mathbb{T}^n_p} \psi_j(f(x)). \quad (4.5.1) \]

Deligne's general result on the Riemann Hypothesis, Proposition 4.1.4, still holds true in this setting and so it is natural to ask for the values of the Betti numbers and for conditions on \( f \) that will guarantee that the pair \( (\mathbb{T}^n, f) \) is pure of weight \( n \).

**Definition 4.5.2.** Let \( f = \sum_{i \in \mathbb{Z}^n} c_i X^i \) be a Laurent polynomial.

(i) The Newton polyhedron \( \Delta_\infty(f) \) of \( f \) at \( \infty \) is the convex hull in \( \mathbb{R}^n \) of \[ \{ i \in \mathbb{Z}^n : c_i \neq 0 \} \cup \{0\}. \]

(ii) For any face \( \sigma \) of \( \Delta_\infty(f) \) let \( f_\sigma = \sum_{i \in \sigma} c_i X^i \). We call \( f \) nondegenerate with respect to \( \Delta_\infty(f) \) if for every face \( \sigma \) (of any dimension) of \( \Delta_\infty(f) \) that does not contain the origin, the system
\[
\frac{\partial f_\sigma}{\partial x_1} = \ldots = \frac{\partial f_\sigma}{\partial x_n} = 0, \quad (4.5.3)
\]

has no solution in \( \mathbb{T}^n \).

**Theorem 4.5.4.** Denef and Loeser (1991, Theorem 1.3). Suppose that \( f \) is nondegenerate with respect to \( \Delta_\infty(f) \) and that \( \dim(\Delta_\infty(f)) = n \). Then \( B_i = 0 \) for \( i \neq n \) and \( B_n = n! Vol(\Delta_\infty(f)) \). In particular,
\[ |S_j| \leq n! Vol(\Delta_\infty(f)) q^{nj/2}. \]

If in addition the origin is an interior point of \( \Delta_\infty(f) \) then the pair \( (\mathbb{T}^n, f) \) is pure of weight \( n \).

This result was proved by Adolphson and Sperber for almost all \( p \).

**Example 4.5.5.** Let \( f(X, Y) = Y^7 + 4X^3Y^3 + 8X^{-6}Y^{-1} + XY^3 + X^3Y^{-1} - 5X^{-3} + 7 \). The Newton Polyhedron \( \Delta_\infty(f) \) is the quadrilateral drawn below.

If \( p \neq 2, 3, 7 \) it is easy to check that for each of the Laurent polynomials \( Y^7, 8X^{-6}Y^{-1}, X^3Y^{-1}, 4X^3Y^3, Y^7 + 4X^3Y^3, Y^7 + 8X^{-6}Y^{-1}, 4X^3Y^3 + X^3Y^{-1}, 8X^{-6}Y^{-1} + X^3Y^{-1} \), there is no point in \( \mathbb{T}^2 \) where both partial derivatives vanish. Therefore \( f \) is nondegenerate with respect to \( \Delta_\infty(f) \) and so the pair \( (\mathbb{T}^n, f) \) is pure of weight \( 2 \) with \( B_2 = 84 \).

**Example 4.5.6.** Kloosterman sums. We can write
\[ \sum_{x_1 \cdots x_n = 1} \psi \left( \sum_{i=1}^n y_i x_i \right) = \sum_{x \in \mathbb{T}^n-1} \psi \left( \sum_{i=1}^{n-1} y_i x_i + y_n(x_1 \cdots x_{n-1})^{-1} \right). \]

It is easy to check that the Laurent polynomial \( f(X) = \sum_{i=1}^{n-1} y_i X_i + y_n(X_1 \cdots X_{n-1})^{-1} \) is nondegenerate with respect to its Newton polyhedron \( \Delta_\infty(f) \) and that \( Vol(\Delta_\infty(f)) = \)
$n(n - 1)$. Also, it is clear that the origin is an interior point of $\Delta_\infty(f)$. Thus by Theorem 4.5.4 the Kloosterman sum is pure of weight $n - 1$ and $B_{n-1} = n$.

If the origin is not an interior point of $\Delta_\infty(f)$ then we would like to know the number of characteristic values of weight $w$ for $0 \leq w \leq n$. Set $e_w$ equal to this number. A formula for $e_w$ is given in Theorem 1.8 of Denef and Loeser (1991). A special case where the $e_w$ can be explicitly calculated is provided for in their Theorem 8.2 given below.

**Definition 4.5.7.** Suppose that $\sigma$ is a face of $\Delta_\infty(f)$ containing the origin. Let $L(\sigma)$ be the smallest linear subspace of $\mathbb{R}^n$ containing $\sigma$. We define the dimension $\dim(\sigma)$ of $\sigma$ to be the dimension of $L(\sigma)$ and we define $Vol_h(\sigma)$ to be the volume of $\sigma$ with respect to the Haar measure on $L(\sigma)$ so normalized that a fundamental domain for the lattice $L(\sigma) \cap \mathbb{Z}^n$ has volume 1. When the origin itself is a vertex, so that $\sigma_0 = (0, \ldots , 0)$ is a face of $\Delta_\infty(f)$, we set $Vol_h(\sigma_0) = 1$. The Haar measure can be computed as follows. Suppose that $\sigma$ is a $k$-simplex with one vertex at the origin and $k$ vertices in $\mathbb{Z}^n$. Let $M(\sigma)$ be the $(k \times n)$-matrix whose rows are the coordinates of the nontrivial vertices of $\sigma$. Then $k!Vol_h(\sigma)$ is the greatest common divisor of the $(k \times k)$-minors of $M(\sigma)$.

**Definition 4.5.8.** Let $\sigma_o$ be the smallest face of $\Delta_\infty(f)$ containing the origin. We say that $\Delta_\infty(f)$ is simple at the origin if $\dim(\Delta_\infty(f)) = n$ and $\sigma_o$ is contained in exactly $n - \dim(\sigma_o)$ faces of dimension $n - 1$ of $\Delta_\infty(f)$.

**Theorem 4.5.9.** Denef and Loeser (1991, Theorem 8.2). Suppose that $\Delta_\infty(f)$ is simple at the origin. Then for $w = 0, 1, \ldots , n$ we have

$$e_w = \sum_{i=0}^{w}(-1)^{w-i}i! \binom{n-i}{n-w} V_i,$$

(4.5.10)
where
\[ V_i = \sum_{0 \in \sigma, \dim(\sigma) = i} V(\sigma) \]  \hfill (4.5.11)

Example 4.5.12. One dimensional case. (Due to Weil (1948b)). When \( n = 1 \) then we can write \( f(X) = \sum_{i=d}^{D} c_i X^i \) for some integers \( d, D \) with \( c_d \neq 0 \) and \( c_D \neq 0 \). If \( d \) and \( D \) are of opposite signs then the origin is an interior point of \( \Delta_\infty(f) \) and so the sum is pure of weight 1 with \( B_1 = D - d \).

If \( d \) and \( D \) are both nonnegative then the origin is an endpoint of \( \Delta_\infty(f) \), and it is plain that \( \Delta_\infty(f) \) is simple at the origin. Thus by Theorem 4.5.9 we have \( e_0 = 1 \) and \( e_1 = D - 1 \). If we throw the origin into the original exponential sum then it becomes pure of weight 1 with \( B_1 = D - 1 \).

Example 4.5.13. Two dimensional case. When \( n = 2 \), \( \Delta_\infty(f) \) is always simple at the origin and so Theorem 4.5.9 applies. Adolphson and Sperber (1990) give the following example. Let \( f(X, Y) = X^2 + X^{-3} Y^5 + Y^8 \). Then \( \Delta_\infty(f) \) is the quadrilateral in \( \mathbb{R}^2 \) with vertices \((0,0), (2,4), (-3,6) \) and \((0,8)\). If \( p \neq 2, 3 \) then \( f \) is nondegenerate and \( B_2 = 2! V(\Delta_\infty(f)) = 40 \). Besides \( \Delta_\infty(f) \) there are three other faces containing the origin: \( \sigma_0 = (0,0), \sigma_1 = \text{line segment from } (0,0) \text{ to } (2,4), \) and \( \sigma_2 = \text{line segment from } (0,0) \text{ to } (-3,6) \). We have \( V(\sigma_0) = 1, V(\sigma_1) = 2 \) and \( V(\sigma_2) = 3 \) and so \( V_0 = 1, V_1 = 5 \) and \( V_2 = 40 \). Thus \( e_2 = 40 - 5 + 1 = 36, e_1 = -2 + 5 = 3, \) and \( e_0 = 1 \).

Complete Exponential Sums.

Complete sums can be partitioned into sums over tori as follows.
\[ \sum_{x} = \sum_{S} \sum_{x_i = 0 \text{ if } i \notin S} \sum_{x_i \neq 0 \text{ if } i \in S} \]  \hfill (4.5.14)
the sum being over all subsets \( S \) of \( \{1, 2, \ldots, n\} \). Thus if we wish to apply Theorem 4.5.4 to a complete exponential sum \( \sum_{x} \psi(f(x)) \), then the hypotheses must hold for each of the sums on the righthand side of (4.5.14). In particular, setting all but one variable equal to zero we see that \( f \) must contain a monomial of the form \( a_i X_i^{d_i}, a_i \neq 0, d_i > 0 \) for each value of \( i \), \( 1 \leq i \leq n \). Such polynomials are called commode. For such polynomials it is plain that the polynomial obtained from \( f \) by setting any subset of variables equal to zero will be nondegenerate provided that \( f \) itself is nondegenerate. Moreover it is plain that \( \Delta_\infty(f) \) is simple at the origin in this case. One can deduce the following

Theorem 4.5.15. Denef and Loeser (1991, Theorem 9.2). Suppose that \( f \) is commode and nondegenerate with respect to \( \Delta_\infty(f) \). Then the pair \((\mathbb{A}^n, f)\) is pure of weight \( n \) and \( B_n = e_n \) where \( e_n \) is the value given in (4.5.10) which can be written
\[ e_n = \sum_{0 \in \sigma} (-1)^{n-\dim(\sigma)} (\dim(\sigma))! V(\sigma), \]
the volume here being ordinary Lebesgue measure.
Example 4.5.16. Adolphson and Sperber (1989). Let
\[ f(X) = a_1X_1^{d_1} + \ldots + a_nX_n^{d_n} + g(X), \]  
(4.5.17)
where \( g \) is such that \( \Delta_\infty(f) \) is the simplex with vertices at the origin and at \((d_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, d_n)\), and \( f \) is nondegenerate with respect to \( \Delta_\infty(f) \). Then the hypotheses of Theorem 4.5.15 are satisfied and so the pair \((A^n, f)\) is pure of weight \( n \) with \( B_n = \Pi_{i=1}^n (d_i - 1) \).

In particular, if none of the exponents \( d_i \) in (4.5.17) are divisible by \( p \), and every nonzero monomial \( c_iX_1^{d_1}X_2^{d_2}\ldots X_n^{d_n} \) in \( g \) satisfies \( \sum_{j=1}^n \frac{d_j}{d_j} < 1 \), then \( f \) is nondegenerate with respect to \( \Delta_\infty(f) \).

If \( f \) is not commode to start with one can always make a linear change of variables to make \( f \) commode. This is a simple matter of choosing a basis of vectors for \( \mathbb{F}_q^n \) on which \( f \) never vanishes. Such bases will normally exist because \( f \) cannot be identically zero on the complement of any hyperplane provided that the degree in each variable is less than \( q - 1 \); one must avoid polynomials such as \( X_1^{q-1} - 1 \).

Polynomials of the type (4.5.17) can have bad singularities at infinity and thus Theorem 4.5.15 applies to many polynomials that Deligne’s result, Theorem 4.1.15, does not. On the other hand, if \( f \) is a polynomial of degree \( d \) prime to \( p \) and nonsingular at infinity then as Adolphson and Sperber pointed out, one can make a linear change of variables so that \( f \) is nondegenerate and of the form (4.5.17) with \( d_1 = \ldots = d_n = d \). The idea for making such a change of basis can be found in the work of Dwork (1962, section 4(c)). Thus Deligne’s result is a special case of the preceding example.

The Exponential Sum \( S(V, y) \).

If \( V \) is defined by a set of \( s \) polynomials \( f_1, \ldots, f_s \), then we can write
\[ S(V, y) = \sum_{x \in V} \psi(x \cdot y) = q^{-s} \sum_{\lambda} \sum_{x} \psi(\lambda_1 f_1(x) + \ldots + \lambda_s f_s(x) + x \cdot y), \]
and view the latter sum as a complete exponential sum over affine \((n + s)\)-space. In particular, the characteristic values associated with the sum \( S(V, y) \) are just those associated with the complete exponential sum multiplied by the factor \( q^{-s} \).

Example 4.5.18. Generalized Kloosterman Sums. Adolphson and Sperber (1989, section 6). Let \( V \) be the hyperplane defined by \( \Pi_{i=1}^n x_i^{d_i} = c \) with \( c \neq 0 \) and \( y \in \mathbb{F}_q^n \) be such that \( y_i \neq 0 \) for all \( i \). If the \( d_i \) are prime to \( p \) then it is straightforward to check that the polynomial \( \lambda(\Pi X_i^{d_i} - c) + \sum y_i X_i \) is commode and nondegenerate with respect to its Newton Polyhedron \( \Delta \) and so the sum is pure of weight \( n + 1 \). To find the volume of \( \Delta \) we view \( \lambda \) as the first coordinate and draw a line segment from the vertex point \((1, d_1, d_2, \ldots, d_n)\) to the origin. This partitions the polyhedron into \( n + 1 \) pyramids with bases on the coordinate planes and heights \( 1, d_1, \ldots, d_n \) respectively. Thus \((n + 1)!Vol(\Delta) = 1 + d_1 + \ldots + d_n \).
Also for \( i = 0, 1, \ldots, n \) it is obvious that \( V_i = \binom{n+1}{i} \binom{n}{i-1} \), in the notation of (4.5.11). Thus, using the formula for \( e_{n+1} \) in (4.5.10) we obtain \( B_{n+1} = \sum_{i=1}^{n} d_i \), and so if none of the \( y_i \) are zero then,

\[
| \psi(\sum_{i=1}^{n} x_i y_i) | \leq (\sum_{i=1}^{n} d_i)^{n-1}.
\]  

(4.5.19)

**General Exponential Sums over Hypersurfaces.**

In section 4.1 we stated the following theorem of Katz.

**Theorem 4.1.17.** Katz (1980, Theorem 5.1.1). Suppose that \( \overline{V} \subset \mathbb{A}^n \) is such that \( \overline{V}_H \subset \mathbb{P}^n \) is a smooth, irreducible projective variety of dimension \( e \) over \( \mathbb{F}_q \) and that \( \overline{V}_\infty \in \mathbb{P}^{n-1} \) is also smooth. Let \( g \) be a polynomial of degree \( D \) over \( \mathbb{F}_q \) with \( p \nmid D \) such that the projective variety defined by the maximal homogeneous part of \( g \) is transverse to \( \overline{V}_\infty \). Then the pair \((\overline{V}, g)\) is pure of weight \( e \).

Our intention here is to show that this is a corollary of Theorem 4.5.15 in the case when \( \overline{V} = \overline{V}(f) \) is a hypersurface. Let \( d \) denote the degree of \( f \), \( f_d \) the maximal homogeneous part of \( f \) and \( g_D \) the maximal homogeneous part of \( g \). By the assumptions of the theorem and a linear change of variables over a finite extension of \( \mathbb{F}_q \) if need be we may assume that,

1. \( f \) and \( g \) are of the types

\[
\begin{align*}
  f(X) &= a_1 X_1^d + \cdots + a_n X_n^d + h_1(X), \\
  g(X) &= c_1 X_1^D + \cdots + c_n X_n^D + h_2(X),
\end{align*}
\]  

(4.5.20)

with the \( a_i \) and \( c_i \) all nonzero,

2. \( \lambda f \), viewed as a polynomial in \((n + 1)\) variables is nondegenerate with respect to its Newton Polyhedron \( \Delta_\infty(\lambda f) \), and

3. \( \lambda f_d(X) + g_D(X) \) is nondegenerate with respect to its Newton Polyhedron at infinity.

The second assumption follows from the smoothness conditions on \( \overline{V} \) and the third from the transversality condition in the theorem. We also note that in order for \( \overline{V}_H \) to be smooth \( f \) cannot be homogeneous. If \( d < D \) it follows by assumption (i) above that the Newton Polyhedron \( \Delta \) for the polynomial \( \lambda f(X) + g(X) \), is a frustum of the right-pyramid having a base with with vertices \((0,0,\ldots,0), (0,D,0,\ldots,0), \ldots (0,0,\ldots,d)\), and a vertex at \((1 + \frac{d}{D-d}, 0, \ldots, 0)\), (as drawn below when \( n = 2 \), taking \( \lambda \) as the first coordinate).

The faces of \( \Delta \) not containing the origin are either faces of the top of the frustum determined by the polynomial \( \lambda f \) or faces of the skew side of the pyramid determined by the polynomial \( \lambda f_d + g_D \). By assumptions (ii) and (iii) we know that \( \lambda f(X) + g(X) \) is nondegenerate with respect to \( \Delta \). Thus the complete exponential sum is pure of weight \((n + 1)\) and the pair \((\overline{V}, g)\) is pure of weight \((n - 1)\). The values \( V_i \) in (4.5.11) are given by

\[
V_{n+1} = Vol(\Delta) = \frac{D^{n+1} - d^{n+1}}{(n+1)! (D-d)},
\]

44
\[ V_i = \binom{n}{i} \frac{D^i}{i!} + \binom{n}{i-1} \frac{D^i - d^i}{i!(D - d)}, \]

for \( i = 1, 2, ..., n \). Thus the Betti number \( B_{n-1} \) associated with the pair \((\overline{V}, g)\), (that is, \( B_{n+1} \) for the complete exponential sum), is given by

\[ B_{n-1} = (n + 1)!V_{n+1} + \sum_{i=0}^{n} (-1)^{n+1-i} i! V_i \]

\[ = \frac{D^{n+1} - d^{n+1}}{D - d} + \sum_{i=1}^{n} (-1)^{n+1-i} \binom{n}{i} D^i + \frac{1}{D - d} \sum_{i=1}^{n} (-1)^{n+1-i} \binom{n}{i-1} (D^i - d^i), \]

\[ = \frac{1}{D - d} \left[ D^{n+1} - d^{n+1} + \sum_{i=1}^{n} (-1)^{n+1-i} \binom{n}{i-1} (D^i - d^i) \right] + \sum_{i=0}^{n+1-i} \binom{n}{i} D^i, \]

\[ = \frac{D}{D - d} (D - 1)^n - \frac{d}{D - d} (d - 1)^n - (D - 1)^n \]

\[ = \frac{d}{D - d} [(D - 1)^n - (d - 1)^n], \quad (4.5.21) \]

which is the same value that Katz obtained, (4.1.18). Similar arguments hold when \( d > D \) and when \( d = D \).

It would be of interest to see whether Theorem 4.1.17 can be deduced from Theorem 4.5.15 for general varieties, and also whether the result of Laumon, Theorem 4.1.22 can be similarly deduced.
4.6. COMPLETE EXPONENTIAL SUMS

In this section we summarize the state of knowledge for complete exponential sums of the type

\[ S(g) = S(A^n, g) = \sum_{x \in \mathbb{F}_q^n} \psi(g(x)), \] (4.6.1)

where \( g \) is a polynomial of degree \( d \) over \( \mathbb{F}_q \). First suppose that \( g \) is any nonconstant polynomial with \( p \nmid d \). Then by a linear change of variables we may assume \( g \) is of the form

\[ g(X) = c_d X_n^d + c_{d-1}(X_1, \ldots, X_{n-1}) X_n^{d-1} + \cdots + c_0(X_1, \ldots, X_{n-1}) \]

for some nonzero constant \( c_d \) and polynomials \( c_0, \ldots, c_{d-1} \). Now, for any choice of the variables \( x_1, \ldots, x_{n-1} \) the sum over \( x_n \) in (4.6.1) is bounded above by \( (d - 1)q^{n-\frac{1}{2}} \) by the result of Weil, Example 4.1.14. Thus we obtain the upper bound,

\[ |S(g)| \leq (d - 1)q^{n-\frac{1}{2}}. \] (4.6.2)

Deligne (1977, Proposition 3.8), obtained the same upper bound (4.6.2) under the more natural hypothesis that \( g \) not be of the form \( f^p - f + c \) for any polynomial \( f \) over \( \mathbb{F}_q \) and constant \( c \in \mathbb{F}_q \). It is precisely the latter types of polynomials for which the sum in (4.6.1) blows up, that is, is of modulus \( q^n \).

If we impose the stronger conditions that the generic hypersurface \( g(x) = t \) is irreducible over \( \overline{\mathbb{F}_q}(t) \) and that \( p > c^*(d, n) \) then by (4.4.12) we obtain

\[ |S(g)| \leq (4d + 5)^n q^{n-1}. \] (4.6.3)

The constant \((4d+5)^n\) in (4.6.3) is again obtained from the result of Bombieri (1978). The size of the constant \( c^*(d, n) \) depends on the number of values of \( \tau \) for which the hypersurface \( g = \tau \) is reducible. From elimination theory and a theorem of Noether (1922), (see Schmidt (1976, pg 190)), it is known that this number is \( \leq k^{2k} \) where \( k = \binom{n+d-1}{n-1} \). Needless to say, a smaller value would be desirable. If the maximal homogeneous part of \( g \) is absolutely irreducible then the surface \( g = \tau \) is irreducible for all \( \tau \) and so by Theorem 4.4.10 we obtain

**Theorem 4.6.4.** Suppose that \( p > (4d + 9)^{2n+2} + 1 \). If the maximal homogeneous part of \( g \) is absolutely irreducible then (4.6.3) holds true.

We can make the upper bounds on \( S(g) \) more precise by utilizing the concept of the singular locus. Let \( G \) denote the homogenization of \( g \) in the variables \( X_1, \ldots, X_{n+1} \). Suppose that for any \( \tau \in \overline{\mathbb{F}_q} \) the polynomial \( g(x) - \tau \) is absolutely irreducible, that for all but \( c(n, d) \) values of \( \tau \) the hypersurface in \( \mathbb{P}^n \) defined by

\[ G(x_1, \ldots, x_{n+1}) = \tau x_{n+1}^d \] (4.6.5)
has a singular locus of dimension $\leq \ell$ and that for the remaining values of $\tau$ the singular locus is of dimension $\leq \ell + 1$. Then by Theorem 4.4.17, if $p > c^*(d, n)$ we have

$$|S(g)| \leq (4d + 5)^n q^{\frac{n+\ell+1}{2}}. \quad (4.6.6)$$

Now, the singular points of the hypersurface in (4.6.5) are of two types, those $(x, x_{n+1})$, with $x_{n+1} = 1$ and $x$ a singular point of the surface $g = \tau$ and those with $x_{n+1} = 0$ and $x$ satisfying,

$$\frac{\partial g_d}{\partial x_i}(x) = 0, \quad 1 \leq i \leq n \quad \text{and} \quad g_{d-1}(x) = g_d(x) = 0, \quad (4.6.7)$$

where $g_d$ and $g_{d-1}$ are the homogeneous parts of $g$ of degrees $d$ and $d - 1$ respectively. Let $\ell^*$ denote the dimension of the algebraic subset of $\mathbb{P}^{n-1}$ defined by

$$\frac{\partial g_d}{\partial x_i}(x) = 0, \quad 1 \leq i \leq n. \quad (4.6.8)$$

If $p \nmid d$ then $\ell^*$ is just the dimension of the singular locus of $g_d$. (When $p | d$ one needs to add the equation $g_d = 0$ to (4.6.8).) It is clear that the dimension of the set of points satisfying (4.6.7) is $\leq \ell^*$.

What can we say about the dimension of the set of singularities of $g = \tau$ relative to $\ell^*$? Let $\overline{W} \subset \mathbb{A}^n$ be the set of points satisfying

$$\frac{\partial g}{\partial x_i} = \frac{\partial g_d}{\partial x_i} + \frac{\partial g_{d-1}}{\partial x_i} + \cdots + \frac{\partial g_1}{\partial x_i} = 0, \quad 1 \leq i \leq n. \quad (4.6.9)$$

Then $\overline{W}_\infty$ is a subset of the set of points satisfying (4.6.8) (in fact, the sets are equal if none of the $\frac{\partial g_d}{\partial x_i}$ vanish identically), and so $\dim(\overline{W}_\infty) \leq \ell^*$. Since $\overline{W}_\infty$ is isomorphic to $\overline{W}_H \cap \{x_{n+1} = 0\}$ we have $\dim(\overline{W}) \leq \dim(\overline{W}_H) \leq \ell^* + 1$. Now, the set of singularities of $g = \tau$ is obtained by intersecting $\overline{W}$ with the surface $g = \tau$. If this intersection has the same dimension as $\overline{W}$ then the surface $g = \tau$ must contain one of the maximal irreducible components of $\overline{W}$. But given a maximal component, there is at most one value of $\tau$ such that the surface $g = \tau$ contains this component. Thus, for all but finitely many values of $\tau$ the set of singularities of $g = \tau$ is of dimension at most $\ell^*$, and so for such $\tau$ we conclude that the dimension of the set of singular points of the hypersurface in (4.6.5) is at most $\ell^*$. This proves

**Theorem 4.6.10.** Suppose that $p > c^*(d, n) > d$. Let $g$ be a polynomial of degree $d$ over $\mathbb{F}_q$ such that its maximal homogeneous part is absolutely irreducible and has a singular locus of dimension $\ell^*$. Then

$$|S(g)| \leq (4d + 5)^n q^{\frac{n+\ell^*+1}{2}}. \quad (4.6.11)$$
Thus when $\ell^* < n - 3$ we get an improvement on (4.6.3). If $n \geq 3$ and the maximal homogeneous part $g_d$ of $g$ is nonsingular, so that $\ell^* = -1$, then $g_d$ is necessarily absolutely irreducible and we obtain the best possible exponent $\frac{n}{2}$ in (4.6.11). This is the same exponent that Deligne obtained in Theorem 4.1.15, repeated below. Of course, Deligne obtained a “purity” type result with a sharper constant and only had the constraint $p \nmid d$ on $p$. If $n = 2$ then it is possible for $g_d$ to be reducible even when $g_d$ is nonsingular, and so Theorem 4.6.10 does not apply. In this case however, the surface $g = \tau$ is irreducible for all nonzero $\tau$ and so (4.6.3) yields the optimal exponent.

We note that it sometimes pays to examine the hypersurface in (4.6.5) directly rather than to apply (4.6.11). The dimension of the singular locus of the hypersurface in (4.6.6) is either equal to or one less than the dimension of the singular locus of $g_d$. For instance, if $g(X_1, X_2) = X_1^2 + X_2$ then the hypersurface in (4.6.6) is nonsingular but $g_d$ has an isolated singularity. In this case we would take $\ell = -1$ in (4.6.6) and obtain the best possible exponent $\frac{n}{2}$.

For homogeneous polynomials, (4.6.11) is essentially just a special case of (4.3.11), but we have replaced the hypothesis $(d, q - 1) = 1$ with the constraint $p > c^*(d, n)$.

In general the upper bound in (4.6.11) is best possible. For example, if we let $g = g(X_1, \ldots, X_r)$ be a polynomial in $r$ variables nonsingular at infinity, but view $g$ as a polynomial in $n$ variables, $n \geq r$, then $\ell^* = n - r - 1$ and $S(g)$ is of order $q^{n-r+\frac{r}{2}} = q^{n-\frac{r}{2}}$. Can one do better for nondegenerate polynomials?

**Purity Type Results.**

Many cases where the pair $(\mathbb{A}^n, g)$ is pure of weight $n$ were stated in section 4.1. They were all special cases of Theorem 4.1.15, which we repeat here.

**Theorem 4.1.15.** Deligne (1973, Theorem 8.4). Let $g$ be a polynomial in $\mathbb{F}_q[X]$ of degree $d$ not divisible by $p$, and nonsingular at infinity. Then the pair $(\mathbb{A}^n, g)$ is pure of weight $n$ with $B_n = (d - 1)^n$ and thus

$$\|S(g)\| \leq (d - 1)^n q^{n/2}. \quad (4.6.12)$$

As we have already observed, Theorem 4.1.15 in return is a special case of the more general Theorem 4.5.15.

**Theorem 4.5.15.** Denef and Loeser (1991, Theorem 9.2). Suppose that $f$ is commode and nondegenerate with respect to $\Delta_\infty(f)$. Then the pair $(\mathbb{A}^n, f)$ is pure of weight $n$ and $B_n = e_n$ where $e_n$ is the value given in (4.5.10) which can be written

$$e_n = \sum_{\sigma \in \Sigma} (-1)^{n - dim \sigma} (dim \sigma)! Vol(\sigma),$$

the volume here being ordinary Lebesgue measure.

**Historical Comments.**

Birch (1962) much earlier had proven the following weaker version of (4.6.11),

$$\|S(g)\| \ll p^{n-2^{1-d}(n-\ell^*)}, \quad (4.6.13)$$

48
where $\ell^*$ again is the dimension of the singular locus of $g$ at infinity.

An upper bound very similar to (4.6.13) can be given in terms of a factor called the $h$-invariant of $g$, the smallest positive integer $h$ such that $g_d$ may be written as

$$g_d = A_1B_1 + A_2B_2 + \cdots + A_hB_h$$

(4.6.14)

for some forms $A_i, B_i \in \mathbb{F}_q[X]$ of positive degree. Schmidt (1984, Theorem 1) gives the following upper bound on complete exponential sums.

$$|S(g)| \ll p^{n-2^1-d\lceil h/\Phi(d) \rceil},$$

(4.6.15)

where $\lceil \alpha \rceil$ denotes the smallest integer $> \alpha$, and one can take $\Phi(2) = \Phi(3) = 1, \Phi(4) = 3, \Phi(5) = 13$ and $\Phi(d) < (\log 2)^{-d}d!$ in general. This is better than the result of Birch (4.6.13) whenever $\lceil h/\Phi(d) \rceil > n - \ell^*$, where $\ell^*$ is the dimension of the singular locus of $g_d$. We always have $h > (n - \ell^* - 1)/2$ since any solution of $A_1 = B_1 = \cdots = A_h = B_h = 0$ is a singular point of $g_d$; here the $A_i$ and $B_i$ are as given in (4.6.14). Are there examples where the upper bound in (4.6.15) is sharper than the upper bound in (4.6.11)? For instance, when $d = 3$ such will be the case if $2\ell^* + h + 3 > 2n$.

4.7. Bounds on the Exponential Sum $S(V, y)$ and Estimates for $|V \cap B|$.

We turn now to the particular sum of interest in the study of the distribution of points on varieties, namely

$$S(V, y) = \sum_{x \in V} \psi(x \cdot y).$$

Let $\overline{V}$ be the algebraic set defined by the polynomials $f_1, \ldots, f_s$ over $\mathbb{F}_q$ of degrees $\leq d$ and for nonzero $y \in \mathbb{F}_q^n$ let $\overline{H}(y)$ be the hyperplane defined by $x \cdot y = 0$.

General Algebraic Sets.

If $\overline{V}$ is an arbitrary algebraic set of dimension $e$ such that none of its irreducible components are contained in a hyperplane of the type $x \cdot y = c$ and $p > (4d + 9)^{2(n+s+1)}$ then by (4.4.9)

$$|S(V, y)| \leq (4d + 9)^{n+s}q^{e-\frac{1}{2}}.$$  (4.7.1)

Thus by (2.14) we have

**Theorem 4.7.2.** If $\overline{V}$ is a variety defined over $\mathbb{F}_p$ not contained in any hyperplane defined over $\mathbb{F}_p$, then for any box $B$, $|V \cap B|$ is of the expected order if $|B| \gg p^{n-\frac{1}{2}}$.

In general the upper bound in (4.7.1) is best possible (up to the constant), even for nonsingular $\overline{V}$. Take for example the hypersurface $V$ defined by

$$x_1^2 + x_2 + \cdots + x_n = 0.$$
If \( y_2 = y_3 = \cdots = y_n \neq 0 \) then \(|S(V, y)| = q^{n-\frac{3}{2}}\). However, if we assume further that \( p > c(d, n, s) \) and that the generic algebraic set defined by

\[
f_1(x) = \cdots = f_s(x) = 0, \quad x \cdot y = t
\]

is irreducible over \( \overline{F}_q(t) \) then by (4.4.12) we obtain

\[
|S(V, y)| \leq (4d + 9)^{n+d-1}q^{e-1},
\]

and thus realize an extra savings of \( q^{1/2} \) over (4.7.1). In general this savings cannot be had for all nonzero \( y \). However, for irreducible hypersurfaces in \( n \geq 3 \) variables, it follows from a theorem of Noether (see Schmidt (1976, V Theorem 2A)) and Bertini’s Theorem (see Schmidt (1976, V Theorem 4B)) that there exists a nonzero polynomial \( G \in F_q[X_1, \ldots, X_{n+1}] \) of degree \( \leq m^{2n} \) with \( m = \binom{n+d-1}{n} \), such that the generic algebraic set in (4.7.3) is irreducible unless \( G(y, t) = 0 \). (This is false if \( n = 2 \).) In particular, since \( t \) is an indeterminate, there is at least one nonzero polynomial \( G_1 \in F_q[X_1, \ldots, X_n] \) such that (4.7.3) is irreducible unless \( G(y) = 0 \). Thus by (2.33) we obtain

**Theorem 4.7.4.** If \( f \) is an absolutely irreducible polynomial over \( \overline{F}_q \) of degree \( d \geq 2 \) in \( n \geq 2 \) variables and \( V = V(f) \), then for any cube \( B \) of size \( b \), \(|V \cap B| \) is of the expected order if

\[
b \gg \begin{cases} 
p^{3/4} & \text{if } n = 2 \\
p^{1-\frac{1}{\lfloor n(n-1)/2 \rfloor}} & \text{if } n \geq 3.
\end{cases}
\]

The case \( n = 2 \) is obtained from Theorem 4.7.2. It is interesting to note that the result of Theorem 4.7.4 becomes weaker as \( n \) gets larger. Thus, if our goal is simply to show that \( V \cap B \) is nonempty we might be able to do better by specializing a certain number of variables. To illustrate this let \( f \) be a polynomial in \( F_q[X] \). Write \( B = B_1 \times B_2 \) with \( B_1 \subset F_q^k \) and \( B_2 \subset F_q^{n-k} \) where \( 2 \leq k < n \), and \( x = (x_1, x_2) \) with \( x_1 \in F_q^k, x_2 \in F_q^{n-k} \). If for some \( x_2 \in B_2 \) the polynomial \( f_1(X_1) = f(X_1, x_2) \) is absolutely irreducible and nonlinear then we can apply the above results to \( f_1 \) and \( B_1 \). Some care needs to be taken. For example, the polynomial

\[
f(X) = f_1(X_3, \ldots, X_n)x_1^2 + f_2(X_3, \ldots, X_n)x_1x_2 + f_3(X_3, \ldots, X_n)x_2^2
\]

is reducible for all choices of \( X_3, \ldots, X_n \). This needs further investigation.

Does the result of Theorem 4.7.4 generalize to arbitrary varieties?

For varieties satisfying sufficient nonsingularity conditions we can utilize the result of Deligne, Theorem 4.1.15, to obtain good bounds on \(|S(V, y)|\).

**Theorem 4.7.5.** Let \( V = V(f_1, \ldots, f_s) \), and suppose that every polynomial in the pencil \( \lambda_1 f_1 + \cdots + \lambda_s f_s \), with \( \lambda \neq 0 \in F_q^s \), is of degree \( \geq 2 \), not divisible by \( p \), and nonsingular at \( \infty \). Then for any nonzero \( y \in F_q^n \),

\[
|S(V, y)| \leq (d - 1)nq^{\frac{n}{2}}
\]

(4.7.6)
Corollary 4.7.7. Suppose that $V$ is defined over $\mathbb{F}_p$ and satisfies the hypotheses of Theorem 4.7.5. Then for any box $B$, $|V \cap B|$ is of the expected order if $|B| > 2^n(d-1)^np^{\frac{n}{d}+d}$. Corollary 4.7.7 follows readily from (4.7.6) and (2.14). Myerson (1981) proved a very similar result under slightly different hypotheses.

For varieties with singularities one should be able to use Theorem 4.4.17 to prove a result analogous to the result for homogeneous varieties given below.

Homogeneous Varieties.

As a special case of Theorem 4.3.5 we have

**Theorem 4.7.8.** If $\overline{V} \subset \mathbb{A}^n$ is homogeneous, of dimension $e$, and such that none of its irreducible components are contained in the hyperplane $x \cdot y = 0$ then

$$|S(V, y)| \leq (4d + 9)^{n+s}q^{e-1}. \quad (4.7.9)$$

**Corollary 4.7.10.** Suppose that $\overline{V}$ is a homogeneous variety of dimension $e$ defined over $\mathbb{F}_p$ and not contained in a hyperplane defined over $\mathbb{F}_p$. Then for any box $B$, $|V \cap B|$ is of the expected order if $|B| \gg p^{n-1}$.

Corollary 4.7.10 realizes a savings of $p^{1/2}$ over the more general result of Theorem 4.7.2. Whenever the intersection of $\overline{V}$ with the hyperplane $x \cdot y = 0$ is absolutely irreducible we realize an extra savings of $q^{1/2}$ in (4.7.9) by (4.3.7). Thus, in the same manner that Theorem 4.7.4 was proved we obtain

**Theorem 4.7.11.** If $f$ is an absolutely irreducible form over $\mathbb{F}_p$ of degree $d \geq 2$ in $n \geq 3$ variables and $V = V(f)$, then for any cube $B$ of size $b$, $|V \cap B|$ is of the expected order if

$$b \gg \begin{cases} p^{2/3} & \text{if } n = 3 \\ p^{1-\frac{1}{n-1}} & \text{if } n \geq 4. \end{cases}$$

If $\overline{V}$ is a nonsingular homogeneous complete intersection, not contained in $\overline{H}(y)$ then as Shparlinskii and Skorobogatov (1990) observed, $\overline{V} \cap \overline{H}(y)$ can have at most isolated singularities. If the intersection is nonsingular then by (4.3.11) we have

$$|S(V, y)| \ll q^{e/2},$$

while if $\overline{V} \cap \overline{H}(y)$ has isolated singularities, then

$$|S(V, y)| \ll q^{\frac{e+1}{2}}. \quad (4.7.12)$$

Moreover, if $e \geq 3$ there exists a nonzero form $G$ defined over $\mathbb{F}_q$ of degree $D \leq c(d, n, s)$ such that the intersection is nonsingular unless $G(y) = 0$. That such a $G$ exists was observed by Baker (1983, (29)), in the case $s = 1$ and Fujiwara (1985, Lemma 1), (1988, Lemma 2) when $s \geq 1$. They used resultant theory to obtain the existence of $G$ and to show that its degree depends only on $d$, $n$ and $s$, and Bertini's Theorem to show that $G$ is not identically zero. Shparlinskii and Skorobogatov (1990) were the first to observe the upper bound (4.7.12) for $S(V, y)$ in the case of isolated singularities. The above mentioned authors then stated versions of the following theorem which can be deduced immediately from (2.32).
Theorem 4.7.13. If $\overline{V} \subset A^n$ is a nonsingular homogeneous complete intersection of dimension $e = n - s \geq 2$ defined over $\mathbb{F}_p$, and not contained in any hyperplane defined over $\mathbb{F}_p$, then for any cube $B$ of size $b$, $|V \cap B|$ is of the expected order if

$$b \gg \begin{cases} \frac{p^{\frac{3}{2} + \frac{e}{2(n-e)}}}{\frac{p^{1-e}}{b}} & \text{if } e \geq 3 \\ \frac{p^{1-e}}{b} & \text{if } e = 2. \end{cases} \quad (4.7.14)$$

The case $e = 2$ is a simple consequence of Corollary 4.7.10. When $s = 1$ Theorem 4.7.13 is essentially Theorem 2 of Baker (1983), while for $s > 1$ it is essentially Theorem 2 of Shparlinski and Skorobogatov (1990); both of their statements were for cubes centered at the origin.

What can be said if $\overline{V}$ has singularities? Henceforth we shall view $\overline{V}$ as a subset of $\mathbb{P}^{n-1}$ of dimension $e$ and let $\ell$ denote the dimension of the singular locus of $\overline{V}$. From (4.3.9) we have the upper bound

$$|S(V, y)| \ll q^{\frac{\ell^* + 1}{2}}, \quad (4.7.15)$$

where $\ell^*$ is the dimension of the singular locus of $\overline{V} \cap \overline{H}(y)$. Thus, (following Skorobogatov (1992)), we are interested in knowing

(i) How singular can the hyperplane section $\overline{V} \cap \overline{H}(y)$ be, and

(ii) What is the dimension of the set of hyperplanes $\overline{H}$ when the dimension of the singular locus of $\overline{V} \cap \overline{H}(y)$ is fixed?

Two results of Zak give answer to the first question. In (1987, 2, Corollary 5) he proves the general upper bound, $\ell^* \leq n + \ell - e - 1$. For complete intersections he has proven the sharper upper bound, $\ell^* \leq \ell + 1$; see Katz (1991, Appendix, Theorem 2).

To make sense of the second question we identify the hyperplane $\overline{H}(y)$ with the point $y$ in the dual projective space $\mathbb{P}^{n-1}$ and let $Z_i$ be the algebraic subset of $\mathbb{P}^{n-1}$ consisting of those $y$ for which the dimension of the singular locus of $\overline{V} \cap \overline{H}(y)$ is $\geq i$. Set $\delta_i = \text{dim}(Z_i)$. Skorobogatov proves the following lemmas.


(i) If $\overline{V}$ is smooth, then $\delta_i \leq n - i - 2$.

(ii) Assume that $\text{Sing } \overline{V} \neq \emptyset$. Then $\delta_i \leq \min\{n - 1, n + \ell - i - 2\}$.

Lemma 4.7.17. Skorobogatov (1992, Lemma 4.2). Suppose that $\overline{V}$ is smooth and that $\delta_0 = n - 2$. Then $\delta_i \leq n - i - 3$ for $i \geq 1$.

He also states a couple lemmas to deal with the case of varieties having only isolated singularities. The shortcoming of these lemmas is that we do not know the degrees of the algebraic sets $Z_i$. In particular we do not know if the degrees depend only on the degree of $\overline{V}$. To get around this difficulty, Skorobogatov starts with a complex variety $V(\mathbb{C})$ defined by a system of forms $f_1, \ldots, f_s$ with integer coefficients and shows (1992, Theorem 5.1) using a version of (2.29) that for $p > c_1(e, f_1, \ldots, f_s)$ and any cube $B$ of size $b$ with

$$p \geq b \geq c_2(e, f_1, \ldots, f_s)p^{1-\alpha},$$

52
\(|B \cap V_p|\) is of the expected order, where \(V_p\) denotes the solutions of the congruence
\[
f_1 \equiv \cdots \equiv f_s \equiv 0 \pmod{p},
\]
and
\[
\alpha = \alpha(V(C)) := \min_{-1 \leq i \leq \sigma} \frac{n-i}{2(\delta_i + 1)}.
\]
Here, \(\sigma\) is the maximal possible dimension of the singular locus of \(\overline{V} \cap H(y)\), and the \(\delta_i\) are defined with respect to the complex variety. Skorobogatov (1992, Corollary 4.7) gives lower bounds for \(\alpha\) depending on the nature of the variety \(V(C)\). For instance if \(V(C) \subset \mathbb{P}^{n-1}(C)\) is a singular complete intersection of dimension \(e\) with singular locus of dimension \(\ell\), then
\[
\alpha \geq \frac{e - \ell - 1}{2(n-2)},
\]
while if \(V(C)\) is a smooth complete intersection then
\[
\alpha \geq \frac{e}{2(n-1)}.
\]
The latter case was already accounted for in Theorem 4.7.13. Another special case of particular interest is when \(V(C)\) is a hypersurface with at most isolated singularities, such that it is not a cone. Then we have
\[
\alpha \geq \frac{n - 2}{2(n-1)},
\]
the same lower bound that one obtains for smooth hypersurfaces. Lower bounds on \(\alpha\) are also given for varieties that are not complete intersections but they appear to be fairly weak.

**Historical Comments.**

Smith (1970) proved a version of Theorem 4.7.2 for the case of hypersurfaces. Chalk and Smith (1971, Theorem 2) deduced from the result of Bombieri (4.4.30) a more precise version of (4.7.1) for the case of curves. If \(V\) is defined by a polynomial \(f(X_1, X_2)\) of degree \(d\) and no irreducible component of \(\overline{V}\) is a hyperplane of the type \(x \cdot y = c\) with \(c \in \mathbb{F}_p\), then they proved that \(|S(V, y)| \leq (d^2 - d)p^{1/2} + d^2\). Williams (1971) applied this result to the congruence
\[
a_1 x_1^{\ell_1} + a_2 x_2^{\ell_2} + a_0 \equiv 0 \pmod{p}
\]
and proved that there exists a solution with
\[
||x|| < 3(max(\ell_1, \ell_2) + 1)p^{3/4},
\]
a special case of Theorem 4.7.2.
Chalk and Williams (1965) observed (in the case \( s = 1 \)) that for homogeneous varieties one can save an extra factor of \( p^{1/2} \) in the estimate of \( S(V, y) \) whenever \( \overline{V} \not\subset \overline{H}(y) \) and \( \overline{V}, \overline{V} \cap \overline{H}(y) \) are both absolutely irreducible of dimensions \( n - 1 \) and \( n - 2 \) respectively. They also deduced from Chevalley's theorem that such was the case for all \( y \neq 0 \in \mathbb{F}_p^n \) if \( n \geq 2d + 1 \) and \( V \) is a hypersurface defined by a form \( f \) having no singularity over \( \mathbb{F}_p \) (that is, the system \( \partial f / \partial x_1 = \ldots = \partial f / \partial x_n = 0 \) has no common zero in \( \mathbb{F}_p^n \) other than \( 0 \)). Thus they concluded that if \( f \) is a form of degree \( d \geq 2 \) having no singularity over \( \mathbb{F}_p \) and \( n \geq 2d + 1 \), then

\[
|B \cap V(f)| = \frac{|B|}{p^n} |V(f)| + O(p^{n-\frac{5}{2}} \log^n p),
\]

using a version of (2.10).

Heath-Brown (1983, Lemma 12) made use of the fact that one saves an extra factor of \( q^{1/2} \) in the upper bound for \( |S(V, y)| \) whenever \( \overline{V} \cap \overline{H}(y) \) is nonsingular, in his work on nonsingular cubic forms in ten variables. He also proved using tools from algebraic geometry that there exists a nonzero form \( G \) of degree \( \geq 2 \) such that \( \overline{V} \cap \overline{H}(y) \) is nonsingular unless \( G(y) = 0 \).

### 4.8. Upper Bounds on \( S(V, y) \) for Hypersurfaces

Let \( \overline{V} = \overline{V}(f) \) be a hypersurface in \( \mathbb{A}^n \) defined by a polynomial \( f \) over \( \mathbb{F}_q \) of degree \( d \) and \( S(V, y) \) be the sum

\[
S(V, y) = \sum_{x \in V} \psi(x \cdot y),
\]

for nonzero \( y \in \mathbb{F}_q^n \). Let \( \ell \) denote the dimension of the singular locus of \( \overline{V}_H \subset \mathbb{P}^n \). In this section we give several examples of hypersurfaces satisfying the following two conditions. First,

\[
|S(V, y)| \ll q^{\frac{n+\ell}{2}} \quad \text{for all nonzero } y,
\]  

(4.8.1)

and second, for \( r = 0, 1, \ldots, \ell \) there is an algebraic set \( W_r \) of dimension \( \leq n - r - 1 \) and defined by polynomials of degrees \( \leq c(d,n) \) such that

\[
|S(V, y)| \ll q^{\frac{n-r\ell}{2}} \quad \text{for } y \notin W_r.
\]  

(4.8.2)

It is premature to conjecture that (4.8.1) and (4.8.2) hold for any hypersurface \( \overline{V}(f) \), but we do not know of any counterexample.

As we observed in section 2, (2.32), for any \( \overline{V} \) (over \( \mathbb{F}_p \)) satisfying (4.8.1) and (4.8.2) and any cube \( B \) of size \( b \), \( |V \cap B| \) is of the expected order if

\[
b \gg p^{\frac{1}{2} + \frac{\alpha}{2(n - \ell - 1)}}.
\]

If \( \overline{V}_H \) is nonsingular then \( \ell = -1 \) and so the second condition (4.8.2) is vacuous. In this case our task is to demonstrate that \( |S(V, y)| \ll q^{(n-1)/2} \) for all nonzero \( y \). If such is
the case (and V is defined over \( \mathbb{F}_p \)) then by (2.13), for any box \( B \), with sides of arbitrary lengths, \( |V \cap B| \) is of the expected order if

\[
|B| \gg p^{n+1}.
\]

If \( f \) is homogeneous then it is more natural to talk about the dimension of the singular locus of \( \bar{V}(f) \) viewed as a subset of \( \mathbb{P}^{n-1} \). If we let \( \ell' \) denote this dimension then \( \ell = \ell' + 1 \). In particular, if \( f \) is a nonsingular form then \( \ell = 0 \).

**Example 4.8.3. Degenerate polynomials.** We claim that whenever \( f(X_1, \ldots, X_n) = f_1(X_1, \ldots, X_m) \) with \( m < n \), where \( f_1 \) is such that the hypersurface \( \bar{V}_1 = \bar{V}(f_1) \subset A^m \) satisfies the conjecture then so does the hypersurface \( \bar{V}(f) \). Let \( \ell_1 \) denote the dimension of the singular locus of \( \bar{V}(f_1) \). Then \( \ell = \ell_1 + n - m \). Write \( y = (y_1, y_2) \) where \( y_1 = (y_1, \ldots, y_m) \) and \( y_2 = (y_{m+1}, \ldots, y_n) \). Then we have

\[
S(V, y) = \begin{cases} 
0 & \text{if } y_2 \neq 0 \\
q^{n-m}S(V_1, y_1) & \text{if } y_2 = 0,
\end{cases}
\]

and so for all nonzero \( y \),

\[
|S(V, y)| \ll q^{n-m+\frac{m+\ell_1}{2}} = q^{\frac{n+\ell}{2}}.
\]

Also, by assumption, for \( r_1 = 0, 1, \ldots, \ell_1 \), there is an algebraic subset \( U_{r_1} \subset A^m \) of dimension \( \leq m - r_1 - 1 \) such that

\[
|S(V_1, y_1)| \ll q^{\frac{m-1+r_1}{2}}
\]

for \( y_1 \notin U_{r_1}. \) Put \( r = n - m + r_1 \). Then for \( r = n - m, n - m + 1, \ldots, \ell \),

\[
|S(V, y)| \ll q^{n-m+\frac{m-1+r_1}{2}} = q^{\frac{n-1+r}{2}}
\]

unless \( y = (y_1, y_2) \in W_r \) where

\[
W_r = \{(y_1, 0) : y_1 \in U_{r_1}\} \subset A^n,
\]

an algebraic set of dimension \( \leq m - r_1 - 1 = n - r - 1 \). For \( r = 0, 1, \ldots, n - m - 1 \) we take \( W_r \) to be the hyperplane \( y_{m+1} = \cdots = y_n = 0 \) and (4.8.2) is satisfied.

**Example 4.8.4.** \( f(X_1, \ldots, X_n) = g(X_1, \ldots, X_m) + L(X_{m+1}, \ldots, X_n) \). Suppose that \( f \) is a polynomial of the type given in the title with \( n > m \), \( g \) of degree \( d \geq 2 \), \( p \nmid d \), and nonsingular at infinity, and \( L = \sum_{i=m+1}^{n} a_i X_i \) a nonzero linear form. We may assume that
\[ f \text{ is nondegenerate so that } a_i \neq 0 \text{ for all } i. \] Now
\[
\sum_{f=0}^{\psi(x \cdot y)} = q^{-1} \sum_{\lambda \neq 0} \sum_{x \neq 0} \psi(\lambda f(x) + x \cdot y)
= q^{-1} \sum_{\lambda \neq 0} \sum_{x_1} \cdots \sum_{x_m} \psi \left( \lambda g(x_1, \ldots, x_m) + \sum_{i=1}^{m} x_i y_i \right) \prod_{i=m+1}^{n} \sum_{x_i} \psi((\lambda a_i + y_i)x_i)
= \begin{cases} 
q^{n-m-1} \sum_{x_1, \ldots, x_m} & \psi \left( -\frac{y_n}{a_n} g(x_1, \ldots, x_m) + \sum_{i=1}^{m} x_i y_i \right) 
& \text{if } \frac{y_{m+1}}{a_{m+1}} = \ldots = \frac{y_n}{a_n} \\
0 & \text{otherwise} 
\end{cases}
\]
\[
\leq \begin{cases} 
q^{n-m-1} q^{m/2} = q^{\frac{n-1}{2} + \frac{n-m-1}{2}} & \text{if } \frac{y_{m+1}}{a_{m+1}} = \ldots = \frac{y_n}{a_n} \\
0 & \text{otherwise.} 
\end{cases}
(4.8.5)
\]

The hypersurface \( V_H \) is defined by the equation
\[ g_d + g_{d-1} x_{n+1} + \cdots + g_0 x_{n+1}^d + x_{n+1}^{d-1} L = 0 \]
and so it has singularities at those points where \( x_1 = \cdots = x_m = x_{n+1} = 0 \), and
\[ (d-1) x_{n+1}^{d-2} L(x_{m+1}, \ldots, x_n) = 0. \]

If \( d > 2 \) then the singular locus is of dimension \( n - m - 1 \) and so (4.8.5) is actually sharper than (4.8.1) by a factor of 1/2 in the exponent. If \( d = 2 \) then the singular locus has dimension \( n - m - 2 \) and so the upper bound in (4.8.5) agrees with the upper bound in (4.8.1).

**Example 4.8.6. Quadratic polynomials.** Any nondegenerate quadratic polynomial \( f \) over \( \mathbb{F}_q \) with \( q \) odd may be put in the form
\[ f(X) = \sum_{i=1}^{m} a_i X_i^2 + \sum_{i=m+1}^{n} a_i X_i + c, \]
with the \( a_i \) all nonzero, after a linear change of variables. If \( n > m \) then this is just a special case of the previous example. If \( n = m \) then the validity of (4.8.1) and (4.8.2) follow immediately from (A.6) and (A.7). In this case, if \( n \) is odd or \( n \) is even and \( c \neq 0 \) then for any nonzero \( y \),
\[ |S(V, y)| \leq q^{\frac{n-1}{2}}, \]
while if \( n \) is even and \( c = 0 \) then
\[ |S(V, y)| \leq \begin{cases} 
q^{n/2} & \text{if } \sum_i a_i y_i^2 = 0, \\
q^{n/2-1} & \text{otherwise.} 
\end{cases} \]

Thus any quadratic polynomial over \( \mathbb{F}_q \) with \( q \) odd satisfies the conjecture.
Example 4.8.7. Kloosterman Sums. Let \( \overline{V} \) be the hypersurface defined by \( x_1 x_2 \cdots x_n = c \), with \( n > 1 \) and \( c \neq 0 \). In Example 4.1.14 we saw that

\[
|S(V, y)| \leq \begin{cases} 
np^{\frac{n-1}{2}} & \text{if } y_i \neq 0 \text{ for all } i \\
2^{n-1} & \text{if exactly } r \text{ } y_i = 0, \text{ where } 1 \leq r \leq n - 1.
\end{cases}
\]

If \( p \nmid n \) then the set of singular points of \( \overline{V}_H \) is the set of points with \( x_{n+1} = 0 \) and \( x_i = 0 \) for at least two values of \( i \) with \( 1 \leq i \leq n \), and so \( \ell = n - 3 \). If \( p \mid n \) then \( \ell = n - 2 \). Thus (4.8.1) is always true. Observing that \( 2r - n - 1 \leq r \) for \( 1 \leq r \leq n - 1 \), we see that (4.8.2) holds as well.

Example 4.8.8. Generalized Kloosterman Sums. Suppose now that \( \overline{V} \) is defined by \( x_1^{d_1} \cdots x_n^{d_n} = c \) with \( c \) nonzero and \( p \nmid d_1 \cdot d_2 \cdots d_n \). If the \( y_i \) are all nonzero then as we saw in (4.5.19)

\[
|S(V, y)| \leq (\sum_{i=1}^{n} d_i)q^{\frac{n-1}{2}}.
\]

Suppose now that \( y_1 = y_2 = \ldots = y_r = 0 \), with \( 1 \leq r < n \). For \( 1 \leq i \leq n \) let \( \delta_i = (d_i, q - 1) \). We consider two cases. First, suppose that some \( \delta_i = 1 \), say without loss of generality \( \delta_1 = 1 \). Then it is easy to show that

\[
\sum_{x_1^{d_1}\cdots x_n^{d_n} = c} \psi\left(\sum_{i=1}^{n} x_i y_i\right) = (-1)^{n-r}(q - 1)^{r-1}.
\]

(4.8.9)

Thus we have the same situation that we saw for ordinary Kloosterman sums in the previous example.

Suppose next that \( \delta_i > 1 \) for \( 1 \leq i \leq n \), and that \( y_1 = y_2 = \ldots = y_r = 0 \) for some \( r \), \( 1 \leq r < n \). Then

\[
\sum_{x_1^{d_1}\cdots x_n^{d_n} = c} \psi\left(\sum_{i=1}^{n} x_i y_i\right) = \sum_{x_2 \neq 0} \cdots \sum_{x_n \neq 0} \psi\left(\sum_{i=2}^{n} x_i y_i\right) \sum_{x_1^{d_1} = 1} \chi\left(\frac{c}{x_2^{d_2} \cdots x_n^{d_n}}\right)
\]

(4.8.10)

\[
= \sum_{\chi^{d_1} = 1} \chi(c)\Pi_{i=2}^{n} \sum_{x_i \neq 0} \psi(x_i y_i)\chi^{-d_i}(x_i),
\]

where \( \chi \) runs through the multiplicative characters on \( \mathbb{F}_q^* \). Now \( \chi^{-d_i} \) is itself a multiplicative character and so the inner sum in (4.8.10) is just a Gaussian sum of modulus \( q^{1/2} \) provided that \( y_i \neq 0 \) and that the character \( \chi^{-d_i} \) is nontrivial. In general we have

\[
|\sum_{x_i \neq 0} \psi(x_i y_i)\chi^{-d_i}(x_i)| = \begin{cases} 
q^{\frac{1}{2}} & \text{for } y_i \neq 0, \chi^{-d_i} \neq 1 \\
1 & \text{for } y_i \neq 0, \chi^{-d_i} = 1 \\
0 & \text{for } y_i = 0, \chi^{-d_i} \neq 1 \\
q - 1 & \text{for } y_i = 0, \chi^{-d_i} = 1.
\end{cases}
\]

(4.8.11)
Thus
\[ | \sum_{x_1^{d_1} \cdots x_n^{d_n} = c} \psi(\sum_{i=1}^{n} x_i y_i) | \leq \delta_1 (q - 1)^{r - 1} q^{\frac{n-r}{2}} \leq \delta_1 q^{\frac{n+r-3}{2}}. \] (4.8.12)

In particular, \( |S(V, y)| \ll q^{\frac{2n-3}{2}} \) for all nonzero \( y \). Since \( \ell \geq n - 3 \) we see that (4.8.1) holds true. Also, (4.8.2) is implied by (4.8.12).

**Example 4.8.13. Nonsingular Forms.** Let \( f \) be a nonsingular form of degree \( d \geq 2 \) not divisible by \( p \). Then as we noted in section 4.7 there is a nonzero homogeneous polynomial \( G \) of degree \( \leq c(d, n) \) such that

\[ |S(V, y)| \ll \begin{cases} q^{\frac{n-1}{2}} & \text{if } G(y) \neq 0, \\ q^{n/2} & \text{if } G(y) = 0. \end{cases} \]

**Example 4.8.14. \( \bar{V}_H \) and \( \bar{V}_\infty \) nonsingular.** Suppose now that \( f \) is any polynomial of degree \( \geq 2 \) not divisible by \( p \) such that both \( \bar{V}_H \) and \( \bar{V}_\infty \) are nonsingular. If \( p \) is sufficiently large then as we saw in Example 4.4.2, \( |S(V, y)| \ll q^{\frac{n-1}{2}} \) for all nonzero \( y \). The result of Katz, Theorem 4.1.17, yields the same upper bound, but only when the hyperplane \( x \cdot y = 0 \) is transverse to \( \bar{V}_\infty \).

An important example satisfying these two conditions is any hypersurface of the form \( f = c \) with \( f \) a nonsingular form and \( c \neq 0 \).

**Example 4.8.15.** A simple example of a hypersurface of degree \( > 2 \) with \( \bar{V}_H \) nonsingular, but \( \bar{V}_\infty \) singular, is given by

\[ x_1^3 + x_2^3 - x_3^2 = 1, \] (4.8.16)

with \( p > 3 \). It is precisely this surface that was considered by Hooley (1980) in his work on representing numbers as the sum of two cubes. Using the method of section 4.4 he proved that if \( y = (y_1, y_2, 0) \) is such that \( y_1^3 \neq y_2^3 \) then \( |S(V, y)| \ll q \) for \( p \) sufficiently large; this is just an application of Theorem 4.4.17. The same result follows (without the constraint on \( p \)) from the theorem of Laumon, Theorem 4.1.22. But again, in order to apply Laumon’s theorem one needs to assume that \( y_1^3 \neq y_2^3 \). We will show here that the same upper bound holds even when \( y_1^3 = y_2^3 \neq 0 \), provided \( p > 3 \). Indeed, in this case \( S(V, y) \) can be evaluated.

Suppose that \( y_2 = \xi y_1 \), where \( \xi \) is any cube root of unity in \( \mathbb{F}_q \). Let \( \chi \) be the quadratic character on \( \mathbb{F}_q^* \) extending the Legendre symbol. For any \( \tau \in \mathbb{F}_q \) let \( N(\tau) \) denote the number of points on the hypersurface (4.8.16) satisfying \( y_1 x_1 + y_2 x_2 = \tau \). Put \( t = \tau/y_1 \). Then \( N(\tau) \) is just the number of points \( (x_2, x_3) \) satisfying,

\[ 3\xi^2 t \left( x_2 - \frac{t}{2\xi} \right)^2 - x_3^2 = 1 - \frac{t^3}{4}. \] (4.8.17)
The equation in 4.8.17 being a conic, it follows from (A.8) that for $p > 3$,

\[
N(\tau) = \begin{cases} 
(\chi(-1) + 1)q & \text{if } t = 0 \\
\chi(3t)q + q - \chi(3t) & \text{if } t^3 = 4 \\
q - \chi(3t) & \text{otherwise.}
\end{cases}
\]  

(4.8.18)

Thus

\[
S(V,y) = \sum_{\tau \in \mathbb{F}_q} N(\tau)\psi(\tau) = q\chi(-1) + q\chi(3/y_1) \sum_{\tau^3 = 4y_1^3} \chi(\tau)\psi(\tau) - \chi(3/y_1)G(\chi,\psi),
\]  

(4.8.19)

where $G(\chi,\psi)$ is the Gaussian sum $\sum \chi(\tau)\psi(\tau)$. In particular, $|S(V,y)| \leq 4q + \sqrt{q}$.

**Example 4.8.20.** We generalize the previous example and show that for any hypersurface $\overline{V}$ of the type

\[
a_1x_1^3 + a_2x_2^3 + a_3x_3^2 = 1,
\]  

(4.8.21)

with the $a_i$ all nonzero, and any nonzero $y$,

\[
|S(V,y)| \ll q,
\]

provided that $p > 20$. Let $N(\tau)$ denote as usual the number of points on $V \cap H(\tau)$, where $H(\tau)$ is the hyperplane $x \cdot y = \tau$. We claim that $\overline{V} \cap \overline{H}(\tau)$ is irreducible for all but possibly 4 values of $\tau$ in $\mathbb{F}_q$. For such $\tau$ we have by (3.16),

\[
|N(\tau) - q| \leq 2q^{1/2} + 9.
\]

If the intersection is reducible then at least we can say $N(\tau) \leq 3q$. Thus the moment $M = M_1$ in (4.4.7) is bounded above by

\[
M \leq 16q^3 + q \sum_{\tau} (2q^{1/2} + 9)^2 \leq 20q^3 + 18q^{5/2} + 81q^2.
\]

Realizing that the analogous upper bound holds for any extension of $\mathbb{F}_q$ we deduce from Proposition 4.4.4 that for $p > 20$ all of the characteristic values associated with the sum $S(V,y)$ have weights $\leq 2$.

We are left with proving the claim above. Suppose first that $y_3 = 0$, and that without loss of generality $y_2 = 1$. Then $N(\tau)$ is just the number of points $(x_1, x_3)$ satisfying

\[
a_1x_1^3 + a_2(\tau - y_1x_1)^3 + a_3x_3^2 = 1.
\]  

(4.8.22)

We claim that for all but possibly 4 choices of $\tau$ the polynomial in (4.8.22)

\[
a_1X_1^3 + a_2(\tau - y_1X_1)^3 + a_3X_3^2 - 1 = (a_1 - a_2y_1^3)X_1^3 + 3a_2y_1^2\tau X_1^2 + a_3X_3^2 - 3a_2\tau^2 y_1X_1 - a_2^2 \tau^3
\]

+ $a_2 \tau^3
\]

59
is absolutely irreducible. If $a_1 \neq a_2 y_1^3$ then the polynomial is in fact irreducible for all choices of $\tau$. Otherwise it would have to have a linear factor of the form $(X_1 - k)$ and thus vanish identically when we substitute $X_1 = k$ which is clearly impossible. If $a_1 = a_2 y_1^3$, then we are just left with a quadratic polynomial which will be nondegenerate for all but possibly 4 choices of $\tau$.

Suppose now that $y_3 \neq 0$, say without loss of generality $y_3 = 1$. Then we are left with showing that the polynomial

$$a_1 X_1^3 + a_2 X_2^3 + a_3(\tau - y_1 X_1 - y_2 X_2)^2 - 1,$$

(4.8.23)

is absolutely irreducible for almost all values of $\tau$. If the polynomial is reducible then it must have a linear factor of the form $X_1 - bX_2 - c$. Substituting $X_1 = bX_2 + c$ in (4.8.23) the resulting polynomial in the variable $X_2$ must be identically 0. This gives rise to the system of equations,

$$b^3 = -\frac{a_2}{a_1}, \quad c = -\frac{a_3(by_1 + y_2)^2}{3a_1 b^2}, \quad \tau = \frac{3a_1 c^2 b}{2a_3(by_1 + y_2)} + cy_1, \quad a_1 c^3 + a_3(\tau - cy_1)^2 = 1.$$

Clearly, the first three equations determine at most 3 values of $\tau$.

4.9. Algebraic Sets Defined Over $\mathbb{Z}$

A variant of the type of problem dealt with in these notes is to start with a fixed set of polynomials $f_1, \ldots, f_s$ (of degrees $\leq d$) with integer coefficients and let the prime modulus $p$ vary. Let $V(\mathbb{C})$ denote the complex algebraic set defined by the $f_i$ and for any given prime $p$ let $\overline{V}_p$ denote the algebraic subset of $\overline{\mathbb{F}}_p$ defined by the $f_i$ read $\pmod p$. In this case, we may seek bounds on exponential sums over $V_p$ in which the implied constants depend on the coefficients of the polynomials $f_1, \ldots, f_s$, or seek a small solution of the congruence

$$f_1(x) \equiv f_2(x) \equiv \cdots \equiv f_s(x) \equiv 0 \pmod p,$$

in which the implied constant depends again on the coefficients of the $f_i$. A couple of remarks are needed in order to apply the results of the previous sections. First, as Skorobogatov (1992, Section 5) has noted, if the polynomials $f_i$ are homogeneous then there is a constant $c_1$ depending on the polynomials $f_i$ such that for $p > c_1$, $\dim(V(\mathbb{C})) = \dim(\overline{V}_p)$, $\deg(V(\mathbb{C})) = \deg(\overline{V}_p)$, and $\dim \text{Sing}(V(\mathbb{C})) = \dim \text{Sing}(\overline{V}_p)$. Second, if the $f_i$ define an absolutely irreducible variety of dimension $e$ over $\mathbb{Q}$ then for $p > c_2(f_1, \ldots, f_s)$ they also define an absolutely irreducible variety of dimension $e$ over $\overline{\mathbb{F}}_p$. We note that the constants $c_1$ and $c_2$ will depend on the coefficients of the polynomials and not just on $n$, $d$, and $s$ as the following example illustrates.

Example 4.9.1. Suppose that the constant $c_2$ in the preceding paragraph depended only on $n$, $d$ and $s$. Then in particular there exists a constant $c$ such that for all absolutely irreducible polynomials $f$ of degree 2, if $p > c$ then $f$ is still absolutely irreducible when
read \hspace{1mm} (\text{mod} \ p). \text{ Let } p \text{ be any prime greater than } c \text{ and let } f = p(X_1^n + \cdots + X_n^n). \text{ Then for } n > 2 \text{ } f \text{ is absolutely irreducible over } \mathbb{Q}, \text{ but when read } \hspace{1mm} (\text{mod} \ p), \text{ } f \text{ vanishes.}

Let \( g \) be a polynomial over \( \mathbb{Z} \) in \( n \) variables. For any prime \( p \) we can form the exponential sum

\[ S_p(V_p, g) = \sum_{x \in V_p} e_p(g(x)), \]

and the associated \( L \)-function \( L_p(t) = L_p(\overline{V}_p, g, t) \). Katz (1979) established the following analogue of Theorem 4.4.10.

**Theorem 4.9.2.** Katz (1979, Théorème 2.3.1). Suppose that \( g \) is not constant on any irreducible component of \( V(\mathbb{C}) \) and that the generic intersection of \( V(\mathbb{C}) \) with the hypersurface \( g(x) = t \) is irreducible and of dimension \( e - 1 \). Then there exists a constant \( c = c(f_1, \ldots, f_s, g) \) such that for any prime \( p > c \), the characteristic values of \( L_p(t) \) all have weights \( \leq 2e - 2 \).

In lieu of the above comment it is clear that the constant appearing in the statement of Theorem 4.9.2 cannot depend on just the degrees of the polynomials \( f_1, \ldots, g \) and thus this result is slightly weaker than Theorem 4.4.10.

For the special case of linear forms \( g \) Katz and Laumon have proven the following.

**Theorem 4.9.3.** Katz and Laumon (1985, Théorème 5.7.0). If \( f_1, \ldots, f_s \in \mathbb{Z}[X] \) define an algebraic set \( \overline{V} \) over \( \mathbb{Q} \) of dimension \( e \), then there exists a constant \( c = c(f_1, \ldots, f_s) \) and a nonzero homogeneous polynomial \( G(X) \in \mathbb{Z}[X] \), both depending on \( f_1, \ldots, f_s \), such that for any prime \( p \)

\[ |S(V_p, y)| \leq cp^\frac{e}{2} \tag{4.9.4} \]

unless \( G(y) \equiv 0 \hspace{1mm} (\text{mod} \ p) \).

If the algebraic set \( \overline{V} \) in Theorem 4.9.3 is smooth then Katz and Laumon (1985, Théorème 5.2) proved even a stronger result. In this case they showed that for those \( y \) not satisfying \( G(y) \equiv 0 \hspace{1mm} (\text{mod} \ p) \), the exponential sum \( S(V_p, y) \) was "pure" of weight \( e \) and the Betti number \( B_e \) was independent of the choice of \( p \) and \( y \).

Katz (1989) took up the study of the average value of \( |S(V_p, y)| \) as \( y \) runs through \( \mathbb{F}_p^m \). Put

\[ M(p) := p^{-n} \sum_{y \in \mathbb{F}_p^m} |S(V_p, y)/p^{e/2}|. \tag{4.9.5} \]

As we noted in section 2, by (2.25) it follows easily that \( M(p) \ll 1 \). The terms in the sum \( M(p) \) satisfying (4.9.4) are referred to as the "general" terms. Using the theory of perversity, Katz showed that the total contribution to \( M(p) \) coming from the non-general terms is \( O(1/\sqrt{p}) \). He also established the following

**Theorem 4.9.6.** Katz (1989). Suppose that the complex variety \( V(\mathbb{C}) \) is reduced and irreducible, of dimension \( e \geq 1 \). Then there exists a nonnegative integer invariant \( A \) of \( V(\mathbb{C}) \) and constant \( C \) such that
(i) If $A = 0$, then for all primes $p$,

$$M(p) \leq C/\sqrt{p}.$$  

(ii) If $A = 1$, then for all primes $p$,

$$|M(p) - 1| \leq C/\sqrt{p}.$$  

(iii) If $A \geq 2$, then for all primes $p$,

$$M(p) \leq 1 + C/\sqrt{p},$$

and the inequality

$$M(p) \leq 1 - 1/4(1 + A^2) \quad (4.9.7)$$

holds for all $p$ in a set of primes of Dirichlet density $\geq 1/2A^4$. In fact, there exists a finite galois extension $K/Q$ such that (4.9.7) holds for any sufficiently large prime $p$ which splits completely in $K$.

Katz also indicates how one can calculate the $A$-number, and describes general classes of hypersurfaces having $A \geq 2$. The $A$-number is just the number of characteristic values of weight $e$ occuring in a general term $S(V_p,y)$.

5. WEYL’S METHOD AND THE WORK OF SCHMIDT

In this section we take up a study of incomplete exponential sums of the type

$$\sum_{x \in B} e_p(f(x)) \quad (5.1)$$

which as we saw in (2.6) arise in the determination of $|V \cap B|$. One can always use the method of section 2 to obtain an upper bound of the type

$$\sum_{x \in B} e_p(f(x)) \ll \max_{y \in \mathbb{Z}^d} \sum_{x} e_p((f(x) + x \cdot y)(\log p)^n) \quad (5.2)$$

by writing $\sum_{x \in B} = \sum_{x} a_B(x)$; Serre (1977, Théorème A.5) made just such an observation. All we need is the fact that $\sum_{y} |a_B(y)| \ll (\log p)^n$. But such upper bounds yield nothing new in our investigation of $|V \cap B|$. Thus our interest here is in a completely different mode of attack for bounding the sum in (5.1).

Schmidt (1984) obtained a Weyl-type inequality for sums of the type (5.1) and by doing so was able to obtain significant results on the distribution of solutions of congruences for cubes of size $p^{d+1/2}$, where $d$ is the minimum of the degrees of the polynomials involved. The method of Fourier series, as it stands, never yields a significant result for cubes of size $p^{1/2}$ even. Thus Schmidt’s method is a major breakthrough. The drawback is that often
the number of variables must be extremely large in order to obtain these good results. His work is very involved and we will not go into the method of proof any further here. It is discussed at length in Baker's book Diophantine Inequalities (1986).

Whereas in the method of Fourier series our concern is with conditions such as irreducibility or nonsingularity, in Schmidt's method our concern is with a factor called the \( h \)-invariant. Davenport and Lewis (1962) introduced the concept of the \( h \)-invariant of a cubic polynomial, and Schmidt (1984) generalized this to arbitrary polynomials. Let \( f \) be a polynomial of degree \( d \) over \( \mathbb{F}_p \) and \( f_d \) be its maximal homogeneous part. The \( h \)-invariant \( h = h(f) \) of \( f \) is the smallest positive integer \( h \) such that \( f_d \) may be written as

\[
f_d = A_1 B_1 + A_2 B_2 + \cdots + A_h B_h
\]

for some forms \( A_i, B_i \in \mathbb{F}_p[X] \) of positive degrees. If \( f_d \) is a cubic form then we can insist that all of the forms \( A_i \) be linear. In this case the \( h \)-invariant is just the codimension of the maximal linear subspace of \( \mathbb{F}_p^d \) on which \( f_d \) vanishes. It is of historical interest to note that Davenport and Lewis (1962) indicated that the concept of the \( h \)-invariant would not be useful for bounding exponential sums for polynomials of degree \( > 3 \) and even gave a counterexample to the effect, but it is clear that what they had in mind for the \( h \)-invariant was that all of the \( A_i \) should be linear forms. Schmidt's insight was to allow the \( A_i \) and \( B_i \) to be of arbitrary positive degrees.

If \( F = (f_1, f_2, \ldots, f_s) \) is an \( s \)-tuple of polynomials in \( \mathbb{F}_p[X] \), then we define the \( h \)-invariant of \( F \), \( h(F) \), to be the minimal \( h \)-invariant over all polynomials in the pencil \( \lambda_1 f_1 + \cdots + \lambda_s f_s \), with \( \lambda \neq 0 \in \mathbb{F}_p^s \).

Let \( f(X) \in \mathbb{F}_p[X] \) be a polynomial of degree \( d \) and \( B \) be any box of the type \((2.2)\) with all of the \( b_i \leq b = p^\delta \) with \( \frac{1}{d} < \delta \leq 1 \). Theorem 2 of Schmidt (1984) is the upper bound

\[
\left| \sum_{x \in B} e_p(f(x)) \right| \leq c(n, d, \delta, \epsilon) b^{n-\kappa+\epsilon}
\]

(5.4)

where \( \kappa = \kappa(\delta) = \frac{d-\delta+1}{d-1} 2^{1-d} \lceil h/\Phi(d) \rceil \), \( [\alpha] \) is the smallest integer > \( \alpha \), and \( \Phi(d) \) depends only on \( d \). One can take \( \Phi(2) = \Phi(3) = 1, \Phi(4) = 3, \Phi(5) = 13 \) and \( \Phi(d) < (\log 2)^{-d} d! \), in general. From (5.4) and (2.6), (repeated here)

\[
|V \cap B| = p^{-s}|B| + \sum_{\lambda \neq 0} \sum_{x \in B} e_{p}(\lambda \cdot F(x)),
\]

we immediately deduce asymptotic formulae for \( |V \cap B| \). In particular we have

**Theorem 5.5.** Let \( F \) be an \( s \)-tuple of polynomials in \( \mathbb{F}_p[X] \) with \( h \)-invariant \( h \) such that every polynomial in the pencil \( \lambda_1 f_1 + \cdots + \lambda_s f_s \) (\( \lambda \neq 0 \)) is of degree \( d' \) with \( 2 \leq d_2 \leq d' \leq d_1 \). Then for any \( \epsilon > 0 \) and for any cube \( B \) of size \( b \), \( |V(F) \cap B| \) is of the expected order if

\[
b \gg p^{\frac{1}{d_2}} + \frac{1}{(1-\frac{1}{d_2})^{2^{d_1-1}} \Phi(d_1)} + \epsilon.
\]

(5.6)
This is just a version of Schmidt (1984, Theorem 3). It is important to note that the larger \( h \) is the better the result is, and as \( h \to \infty \) while \( s \) and \( d \) are held fixed, the result becomes significant for cubes of size \( p^{\frac{1}{d_2} + \epsilon} \).

The \( h \)-invariant of a form \( f \) can lie anywhere from 1 to \( n \). By Chevalley's Theorem it follows that if \( n > d \) the degree of \( f \), then \( h < n \). More generally, if \( f \) vanishes on a linear subspace of dimension \( \ell \) then \( h \leq n - \ell \); see section 6 for a discussion of the size of \( \ell \). For quadratic and cubic forms the converse holds as well. If \( f \) is irreducible over \( \mathbb{F}_p \) then certainly \( h > 1 \) but not much more can be said. Even if \( f \) is absolutely irreducible and nondegenerate we can have \( h = 2 \); take for example \((x_2^2 + \cdots + x_n^2)x_1 - x_2^3\). For such forms one is much better off using the results obtained by the method of Fourier series. However, for nonsingular forms, \( h \geq n/2 \) (for otherwise the forms \( A_1, B_1, \ldots, A_h, B_h \) in (5.3) have a common nontrivial zero) and so (5.6) yields a very strong result.

**Corollary 5.7.** If every polynomial in the pencil \( \lambda_1 f_1 + \cdots + \lambda_s f_s, \lambda \neq 0 \), is nonsingular at \( \infty \) and of degree \( d' \) with \( 2 \leq d_2 \leq d' \leq d_1 \), then for any \( \epsilon > 0 \) and cube \( B \) of size \( b \), \( |V \cap B| \) is of the expected order if

\[
b \gg p^{\frac{1}{d_2} + \frac{s}{n}(1 - \frac{1}{d_2})2^{d_1 \Phi(d_1)} + \epsilon}.
\]

(5.8)

This is essentially Theorem 1 of Schmidt (1986a). This corollary should be compared with Corollary 4.7.7 which had the same hypotheses. The result of the Corollary 5.7 is stronger than that of Corollary 4.7.7 whenever

\[
\frac{1}{d_2} + \frac{s}{n}(1 - \frac{1}{d_2})2^{d_1 \Phi(d_1)} < \frac{1}{2} + \frac{s}{n}.
\]

More generally if the singular locus of a form is of dimension \( \ell \) then \( h \geq \frac{n - \ell}{2} \), and one can state the obvious analogue of Corollary 5.7.

It would be desirable to know more about the \( h \)-invariant of a polynomial. For instance what can be said about the \( h \)-invariant of a single diagonal form of degree \( d \)?

**Small Solutions of Congruences.**

For the case of homogeneous varieties and cubes centered at the origin Schmidt has obtained a number of additional results from his bounds on incomplete exponential sums. In Theorem 4 of Schmidt (1984) he proves that for any integers \( d, s \) and any \( \epsilon > 0 \), there exists an \( N = N(d, s, \epsilon) \) such that if \( n > N \), then any system of \( s \) forms of degrees \( \leq d \) in \( \mathbb{F}_p[X] \) have a nontrivial common zero with \( \|x\| \leq c(d, s, \epsilon)p^{\frac{1}{2} + \epsilon} \). The use of the \( h \)-invariant leads naturally to an inductive proof of this result but at the expense of requiring the number of variables to be extremely large and no attempt was made to estimate \( N(d, s, \epsilon) \) in this paper. In his paper (1985) Schmidt generalized this result to arbitrary moduli. In (1986a, Theorem 2) he returned to prime moduli and, arguing more carefully, was able to estimate \( N(d, s, \epsilon) \). We can state his result as follows:
Theorem 5.9. Let $f_1, \ldots, f_s$ be any system of forms in $\mathbb{F}_p[X]$ of degrees $\leq d$. Then for any $\epsilon > 0$ there is a nontrivial common zero $x$ with

\begin{align*}
\text{i)} \quad ||x|| &\ll p^{\frac{1}{2} + \frac{3 \sqrt{2}}{\sqrt{n}} + \epsilon}, \quad \text{for } d = 2 \\
\text{ii)} \quad ||x|| &\ll p^{\frac{1}{2} + \frac{\log 5 + \epsilon}{\sqrt{n}}}, \quad \text{for } d = 4 \\
\text{iii)} \quad ||x|| &\ll p^{\frac{1}{2} + \frac{\gamma(d) E d^{-1}}{\sqrt{n}} + \epsilon}, \quad \text{for } d \geq 3
\end{align*}

(5.10) \hspace{1cm} (5.11) \hspace{1cm} (5.12)

where $D = D(d)$ is the $(d - 1)^{st}$ element of the Fibonacci sequence $1, 1, 2, 3, \ldots$. (There are a few minor corrections that need to be made in the (1986) paper of Schmidt because the $p$ on the right-hand-side of (2.2) should have been $P = p^6$. We have incorporated these changes in (5.11).)

Little is known about the constant $\gamma(d)$ appearing in (5.12) other than $\log \log \gamma(d) \leq (d + o(d)) (\sqrt{5} - 1)/2$, and so (5.12) does not serve our interests here well. Even when $d = 4$ the statement in (5.11) is nontrivial only when $n > 64 \cdot 10^{10} s^6$, and so (5.11) does not give us information for forms in a small number of variables. On the other hand, for systems of linear and quadratic forms, (5.10) yields good information even when the number of variables is relatively small.

When all of the forms are of odd degrees Schmidt (1986, Theorem 3) was able to prove a stronger result, which we state as follows.

Theorem 5.13. Let $f_1, \ldots, f_s$ be any system of forms in $\mathbb{F}_p[X]$ of odd degrees $\leq d$ (with $d$ odd). Then for any $\epsilon > 0$ there is a nontrivial common zero $x$ with

\begin{align*}
\text{i)} \quad ||x|| &\ll p^{\frac{1}{3} + \frac{3 \sqrt{2}}{\sqrt{n}} + \epsilon}, \quad \text{for } d = 3 \\
\text{ii)} \quad ||x|| &\ll p^{\frac{1}{3} + \frac{o(d) E s^{-1}}{\sqrt{n}} + \epsilon}, \quad \text{for } d \geq 5,
\end{align*}

(5.14) \hspace{1cm} (5.15)

where $E = D(d - 2)$ for $d \geq 5$.

No information was given regarding the size of $o(d)$ in (5.15). It is remarkable that exponents smaller than $\frac{1}{3}$ were obtained in (5.14) and (5.15) but the value $\frac{1}{3}$ is by no means the final word. Indeed in (1980) Schmidt had already proven that for any $\epsilon > 0$, and $n$ sufficiently large, $n > N(\epsilon, s, d)$, any system of $s$ forms of odd degrees $\leq d$ have a nontrivial common zero with $||x|| \ll p^\epsilon$, but no estimate of $N(\epsilon, s, d)$ was given.

Improvements can sometimes be made by combining the results of Schmidt with the results of classical method of Fourier series and those of the geometric method discussed in the next section. Such examples are given in sections 8 and 9.

6. The Method of Lattices for Obtaining Small Solutions

This method applies strictly to homogeneous polynomials. Let $f_1, \ldots, f_s$ be forms in $\mathbb{F}_p[X]$ having some nontrivial common zero $z$; for instance if $n > \sum \deg(f_i)$ then Chevalley’s Theorem assures us that such a $z$ exists. Now, since the $f_i$ are homogeneous every multiple of $z$ is also a common zero and the set of all multiples of $z$ is a one-dimensional
subspace of \( \mathbb{F}_p^n \). This subspace corresponds to a lattice of points \( \mathcal{L} \) in \( \mathbb{Z}^n \) of determinant \( p^{n-1} \) satisfying the congruence

\[
f_1(x) \equiv \cdots \equiv f_s(x) \equiv 0 \pmod{p}.
\]

(6.1)

Then by Minkowski’s fundamental theorem there exists a nonzero point \( x \) in \( \mathcal{L} \) with \( ||x|| < p^{1-\frac{n}{s}} \). This result was perhaps first observed by Chalk and Williams (1965), but the idea is much older. (For instance, this idea has been used to show that every prime \( p \equiv 1 \pmod{4} \) is a sum of two squares and that every positive integer is a sum of four squares; see Cassels (1959, III.7).)

We obtain a better result if the forms \( f_1, \ldots, f_s \) vanish on an \( \ell \)-dimensional subspace of \( \mathbb{F}_p^n \) with \( \ell \geq 1 \). In this case, the lattice \( \mathcal{L} \) we obtain has determinant \( p^{n-\ell} \), and so we obtain a nontrivial solution of (6.1) with

\[
||x|| < p^{1-\frac{n}{s}}.
\]

(6.2)

Unfortunately, forms in general do not vanish on high dimensional linear subspaces. It can be shown by induction and successive applications of Chevalley’s Theorem that if

\[
n > \ell - 1 + \sum_{i=1}^{s} \left( \ell + d_i - 1 \right)
\]

(6.3)

then any set of forms \( f_1, \ldots, f_s \) of degrees \( d_1, \ldots, d_s \) vanish on an \( \ell \)-dimensional subspace. For a single form of degree \( d \) (6.3) simplifies to \( n > \frac{1}{(d-1)!} \ell^{d-1} + O(\ell^{d-2}) \). On the other hand, a counting argument reveals that if \( d < p \) and \( n < \frac{1}{d!} \ell^{d-1} \) then there exists a form of degree \( d \) over \( \mathbb{F}_p \) which does not vanish on any \( \ell \)-dimensional subspace. Thus in general for a form of degree \( d \geq 3 \) the best we can do is to set all but \( d+1 \) variables equal to zero and settle for a nontrivial zero of size \( < p^{d/(d+1)} \). For quadratic forms we can do much better since they vanish on relatively high dimensional subspaces. We discuss their case in section 8.

One nice feature of this geometric method is that it generalizes easily to composite moduli. Let \( F = (f_1, \ldots, f_s) \) be an \( s \)-tuple of forms in \( \mathbb{Z}[X] \) and \( m = p_1 p_2 \cdots p_k \), a product of distinct primes. Suppose that for each \( i \) there is a subspace \( W_i \) of \( \mathbb{F}_{p_i}^n \) of dimension \( \ell_i \) on which \( F(x) \equiv 0 \pmod{p_i} \), identically. Map \( \mathbb{Z}^n \) canonically onto \( \mathbb{F}_{p_1}^n \times \cdots \times \mathbb{F}_{p_k}^n \) via the Chinese Remainder Theorem, and let \( \mathcal{L} \) be the inverse image of \( W_1 \times \cdots \times W_k \) in \( \mathbb{Z}^n \). Then \( \mathcal{L} \) is a lattice of determinant \( \Pi_{i=1}^k p_i^{n-\ell_i} \), and each point of \( \mathcal{L} \) satisfies the congruence

\[
f_1(x) \equiv \cdots \equiv f_s(x) \equiv 0 \pmod{m}.
\]

(6.4)

Hence by Minkowski’s theorem we obtain a nontrivial solution of (6.4) with

\[
||x|| < \Pi_{i=1}^k p_i^{1-\ell_i}.
\]

(6.5)

If \( m = m_1 m_2 \) with \( m_2 \) square free, and all of the forms \( f_i \) are of degree \( \geq 2 \) then we obtain the small solution \( m_1 x \) where \( x \) is a solution of (6.4) \( \pmod{m_2} \) satisfying (6.5).

We note that in Cochrane (1987b) this method was generalized to algebraic number fields.
7. LINEAR FORMS

Let \( L_i(X) = \sum_{j=1}^{n} a_{ij}X_j \), \( 1 \leq i \leq s \), be a system of linear forms in \( \mathbb{F}_p[X] \) with \( [a_{ij}] \) of rank \( r < n \). Then the \( L_i \) vanish on a subspace of dimension \( n - r \) and so by (6.2) they have a common nontrivial zero with \( \|x\| < p^{r/n} \). Moreover, this is best possible, for given any \( r \) and \( n \) with \( r < n \) there exists a system of \( r \) linear forms in \( n \) variables such that any common nontrivial zero has \( \|x\| \geq \frac{1}{2}[p^{r/n}] \), as a counting argument will readily verify. For example if \( \beta = [p^{1/n}] \) then the congruence

\[
x_1 + \beta x_2 + \beta^2 x_3 + \cdots + \beta^{n-1} x_n \equiv 0 \pmod{p}
\]

has no nontrivial solution with \( \|x\| < [p^{1/n}] \), and the system of congruences

\[
x_{i+1} \equiv \beta^i x_1 \pmod{p}, \quad 1 \leq i \leq n - 1
\]

has no nontrivial solution with \( \|x\| < \beta^n/(\beta + 1) = (1 - \varepsilon)p^{n/(n-1)} \) say.

For general moduli, the geometric method of section 6 yields the following result. Let \( L_i(X) = \sum_{j=1}^{n} a_{ij}X_j \), \( 1 \leq i \leq s \), be forms in \( \mathbb{Z}[X] \), and \( m \) any positive integer. Then there is a nontrivial solution of the congruence

\[
L_1(x) \equiv \cdots \equiv L_s(x) \equiv 0 \pmod{m}
\]

with \( \|x\| \leq m^{r/n}/\Pi_{i=1}^{r}(m,d_i)^{1/n} \), where \( r \) is the rank of \([a_{ij}]\) over \( \mathbb{Q}\) and \( d_1,d_2,\ldots,d_r \) are the invariant factors of \([a_{ij}]\).

A more interesting problem is to ask how uniformly distributed the points of a linear surface are throughout all of \( \mathbb{F}_p^n \) (not just near the origin). Here we shall restrict our attention to a single hyperplane. Let \( B = B(a,b) \) be the cube \( \{a_i \leq x_i < a_i + b\} \) of size \( b < p \) and \( H = H(y,c) \) the hyperplane in \( \mathbb{F}_p^n \) defined by \( \sum_{i=1}^{n} y_i x_i = c \), with \( y \neq 0 \in \mathbb{F}_p^n \), \( c \in \mathbb{F}_p \).

We wish to investigate under what conditions on \( b \) and \( y \), \( B \cap H \) will be nonempty for all cubes of size \( b \). Our Euclidean notion of a plane can be misleading here for we do not expect the points on a plane to be very well distributed in an \( n \)-dimensional sense. Indeed, on hyperplanes such as \( x_1 = c \) or \( x_1 + x_2 + \cdots + x_n = 0 \), the points are not well distributed, that is, there are cubes of very large size (on the order of \( p \)) that completely miss these hyperplanes. On the other hand, there are some hyperplanes that hit every cube of size \( p^{1/n} \).

Example 7.3. Let \( \beta \) be a positive integer and \( p \) be a prime with \( \beta^n \leq p < \beta^n + \beta^{n-1} \); (for \( n > 2 \) and \( \beta \) sufficiently large we know that such a prime exists. We make this stipulation on \( \beta \) and \( p \) mainly for cosmetic reasons.) In particular \( \beta = [p^{1/n}] \). Let \( y = (1,\beta,\ldots,\beta^{n-1}) \) and \( H = H(y,c) \) with \( c \) arbitrary. We claim that any cube of size \( \beta + 1 \) has nonempty
intersection with $H$. By a translation of variables it suffices to consider the intersection $B(0, \beta + 1) \cap H(y, c')$, for arbitrary $c'$, $0 \leq c' < p$. If $c' < \beta^n$ then there exist positive integers $x_i$, with $0 \leq x_i < \beta$, $0 \leq i \leq n - 1$, such that $x_0 + x_1 \beta + \cdots + x_{n-1} \beta^{n-1} = c'$, and so $(x_0, \ldots, x_{n-1})$ is a point in the intersection. If $\beta^n \leq c' < p$, then $0 < c' - \beta^{n-1} < p - \beta^{n-1} < \beta^n$ and so $c' = x_0 + \cdots + (x_{n-1} + 1)\beta^{n-1}$ and again we obtain a nonempty intersection.

The best way to think about a hyperplane in $\mathbb{F}_p^n$ is as a lattice of points in $\mathbb{Z}^n$ of determinant $p$, or some translate thereof. To get a better understanding of what is going on in the preceding example we need the concept of a dual box and a dual lattice. If $B = B(a, b)$ is a cube as given above then we define its dual cube $B^*$ by

$$B^* = \{ x \in \mathbb{R}^n : ||x|| < p/b \},$$

a solid cube in $\mathbb{R}^n$ depending only on the size of $B$, not its position. We also define the dual lattice to $H(y, c)$ by

$$L_y = \{ x \in \mathbb{Z}^n : x \equiv \lambda y \pmod{p} \text{ for some } \lambda \in \mathbb{Z} \}.$$ 

$L_y$ is a lattice of determinant $p^{n-1}$ depending only on $y$, not on $c$. Define

$$\gamma_B(y) = \inf_{\gamma \in \mathbb{R}} \{ \gamma : \gamma B^* \cap L_y \neq \{0\} \}.$$ 

(Here, $\gamma B^* = \{ \gamma x : x \in B^* \}$. ) Minkowski’s theorem implies that $\gamma_B(y) \leq \frac{bp^{-1/n}}{\log p}$ for any $B$ and $y$, for if $\gamma^p(p/b)^n > p^{n-1}$ then $\gamma B^* \cap L_y \neq \{0\}$. On the other hand, for the value of $y$ in the preceding example, $\gamma_B(y) \geq (1 - \epsilon)bp^{-1/n}$, with $\epsilon$ the value appearing after (7.2), for $L_y$ is just the set of solutions of (7.2). Thus $L_y$ is an extremal lattice relative to the box $B^*$ in the sense that $\gamma_B(y)$ is as large as it can be. This is the underlying reason why the points of $H(y, c)$ are so well distributed.

The definition of $\gamma_B(y)$ can be generalized to an arbitrary box $B = \{ a_i \leq x_i < a_i + b_i \}$ where now the dual box is $B^* = \{ x \in \mathbb{R}^n : |x_i| < p/b_i, 1 \leq i \leq n \}$. We have been able to show that $B \cap H(y, c)$ is nonempty whenever $\gamma_B(z) \geq 2\log p$, but I suspect a stronger result is available, perhaps $\gamma_B(z) \geq \text{constant}$. Thus, whenever $L_y$ is an extremal lattice relative to $B^*$, say $\gamma_B(y) \geq c[B^{1/n}p^{-1/n}]$, then $H(y, c) \cap B$ is nonempty provided that $|B| > (2c^{-1}\log p)^n p$. We hope that this investigation might be useful for estimating the error term in identities of the type (2.34).

8. Quadratic Forms

Lattice Method.

Let $Q(X)$ be a quadratic form in $\mathbb{F}_p[X]$ with $p$ an odd prime. Set

$$\Delta_p(Q) = \begin{cases} \frac{(-1)^{n/2} \det Q}{p} & \text{if } n \text{ is even} \\ \frac{(-1)^{n-1/2} \det Q}{p} & \text{if } n \text{ is odd} \end{cases}$$

68
if det $Q \neq 0$, and let $\ell$ denote the dimension of a maximal isotropic subspace of $Q$, that is, a maximal linear subspace of $\mathbb{F}_p^\ell$ on which $Q$ is identically zero. If $n$ is even and $Q$ is nonsingular, then $\ell = \frac{n}{2}$ or $\frac{n}{2} - 1$ according as $\Delta_p(Q) = 1$ or $-1$, for in the former case $Q \sim X_1^2 + \cdots + X_{n-1}^2 + X_n^2$ while in the latter case $Q \sim X_1X_2 + \cdots + X_{n-3}X_{n-2} + X_{n-1}^2 - \alpha X_n^2$, with $\left( \frac{\alpha}{p} \right) = -1$. If $n \geq 3$ is odd and $Q$ is nonsingular then $\ell = \frac{n-1}{2}$. If $Q$ is singular then $\ell \geq n/2$. Thus by (6.2), $Q$ has a nontrivial zero of size

$$
\|x\| < \begin{cases} 
p^{1/2} & \text{if } n \text{ is even and } \Delta_p(Q) = 1 \\
p^{1/2} + \frac{1}{p^{n-1}} & \text{if } n \text{ is odd and } \Delta_p(Q) = 0 \\
p^{1/2} + \frac{1}{p^{n}} & \text{if } n \text{ is even and } \Delta_p(Q) = -1 \\
p^{1/2} + \frac{1}{p^{n}} & \text{if } n \text{ is odd and } \Delta_p(Q) \neq 0.
\end{cases}
$$

(8.1)

When $n$ is even and $\Delta_p(Q) = -1$, we set one variable equal to zero to obtain the result in (8.1). It is clear that the upper bound $p^{1/2}$ in (8.1) is best possible for quadratic forms by considering examples such as $X_1^2 + X_2^2 + \cdots + X_n^2$. For a discussion of some further cases where the geometric method leads to solutions of size $p^{1/2}$ see Cochrane (1988).

We can actually say much more following the method above. Let $C$ be any convex subset of $\mathbb{R}^n$ of diameter $p$ centered at $Q$, $W$ be any maximal isotropic subspace and $\mathcal{L}_W$ be the lattice of points in $\mathbb{Z}^n$ of volume $p^{n-\ell}$ corresponding to $W$. Then $C$ contains at least $2|\text{vol}(C)|/2^np^{n-\ell}$ distinct nonzero points of $\mathcal{L}_W$. Now there are $\Pi_{i=1}^{\ell}(p^{n-\ell-i} + 1)$ distinct maximal isotropic subspaces of $Q$ (this can be deduced from Proposition A2.14 of Andrianov (1980)) and each nonzero integral point in $C$ is contained in exactly $\Pi_{i=2}^{\ell}(p^{n-\ell-i} + 1)$ such subspaces. Hence $C$ contains at least $2^{-n}|\text{vol}(C)|/p$ distinct zeros of $Q(x) (\text{mod } p)$, provided that $\text{vol}(C) > 2np^{n-\ell}$. It is interesting to note that this is the same lower bound one obtains by using a convolution function in the exponential sum method.

Schinzel, Schlickewei and Schmidt (1980, Theorem 1) used the geometric method to prove that for any odd $n \geq 3$, any $Q(X) \in \mathbb{Z}[X]$ and any modulus $m$ there is a nonzero solution of the congruence

$$Q(x) \equiv 0 \pmod{m}$$

(8.2)

with $\|x\| < m^{1/2} + \frac{1}{m^{n-1}}$. This is an immediate consequence of (6.5) and the fact that for any prime $p$ (including $p = 2$) $Q$ vanishes on an $(n-1)/2$ dimensional subspace (mod $p$). If $n \geq 4$ is even one can always set one variable equal to zero and obtain a nontrivial solution of (8.2) with $\|x\| < m^{1/2} + \frac{1}{m^{n-1}}$.

One shortcoming of the above result is that it does not necessarily yield a solution of (8.2) with coordinates relatively prime to $m$. Indeed if $m = p^2$ with $p$ a prime, then the small solution we obtain is just $(p, p, \ldots, p)$, which in some sense is a trivial solution. Is it possible to use the lattice method to obtain nontrivial small solutions (mod $p^2$)?

**Exponential Sums.**

Inserting the values of $\phi(V, y)$ given in the Appendix, (A.6) and (A.7), into the fundamental identity (2.4) yields formulae for $|V \cap \mathcal{B}|$. For instance if $n$ is even, $Q$ is a nonsingular
quadratic form \( \mod p \), \( \Delta = \Delta_p(Q) \) and \( V = V(Q) \) then we obtain

\[
\sum_{x \in V} \alpha(x) = p^{-1} \sum_{x} \alpha(x) - \alpha(0) \Delta p^{\frac{n}{2} - 1} + \Delta p^{\frac{n}{2}} \sum_{Q^*(y) = 0} a(y),
\]

(8.3)

where \( Q^* \) is the quadratic form associated with the inverse of the matrix representing \( Q \). Heath-Brown (1985a) made use of such an identity (but using real Fourier series) to obtain the existence of a nontrivial zero of \( Q \) with \( \|x\| \ll p^{1/2} \log p \); (the only case he needed to concern himself with was when \( n = 4 \) and \( \Delta_p(Q) = -1 \), the others already being handled by the lattice method). The key step in his argument was to obtain a good upper bound on the sum \( \sum_{Q^*(y) = 0} a(y) \) which as we saw in section 2 requires in turn good upper bounds for \( |V(Q^*) \cap B_M| \), where \( B_M \) is a cube of size \( M \) centered at the origin. Combining Lemma 6 of Cochrane (1990) with Lemma 1 of Cochrane (1991) we have

\[
|V(Q) \cap B_M| \ll \begin{cases} 
M^n p + M p^{\frac{n}{2} - \frac{3}{2}} & \text{if } \Delta = -1 \\
M^n p^2 + M p^{\frac{n}{2}} & \text{if } \Delta = 1,
\end{cases}
\]

(8.4)

where \( Q \) is any nonsingular form in an even number of variables. Using the upper bound in (8.4) for the case \( \Delta = -1 \), (which is slightly sharper than the bound Heath-Brown used), we were able to prove the existence of a nontrivial zero of \( Q \) with \( \|x\| \ll p^{1/2} \), for any quadratic form in \( n \geq 4 \) variables; see (1991, Theorem 1). Wang (1989), (1993) generalized the result of Heath-Brown (1985) and then the result of Cochrane (1991) to arbitrary finite fields.

When \( n = 3 \), it follows from the lattice method that any quadratic form \( Q(x_1, x_2, x_3) \) has a nontrivial zero with \( \|x\| < p^{2/3} \) and that this is best possible in general; take for example \( Q(x) = L_1^2 - \alpha L_2^2 \) where \( \left( \frac{\alpha}{p} \right) = -1 \), and \( L_1, L_2 \) are linear forms having no nontrivial zero with \( \|x\| < \frac{1}{3} p^{2/3} \). However, this example is a degenerate form and so the question remains whether we can do better for nonsingular forms in three variables.

Extending the method of exponential sums to composite moduli has proven to be challenging. When the modulus \( m \) is a product of two distinct prime factors Heath-Brown (1991, Theorem 1) was able to obtain a nontrivial solution of (8.2) with \( \|x\| \ll m^{1/2 + \epsilon} \). We were able to remove the \( \epsilon \) and obtain the best possible upper bound \( m^{1/2} \) in Cochrane (1994). In fact both Heath-Brown’s result as well as our own extend to boxes with sides of arbitrary length, centered at the origin. Heath-Brown (1991, Theorem 2 and Theorem 3) also obtained the following result for arbitrary moduli. There is a nontrivial solution of (8.2) with

\[
\|x\| \ll \begin{cases} 
m^{(13/21) + \epsilon} & \text{if } n = 4, 5 \\
m^{(15/26) + \epsilon} & \text{if } n = 6, 7 \\
m^{(8/11) + \epsilon} & \text{if } n = 8, 9 \\
m^{(1/2) + (1/3n) + \epsilon} & \text{if } n \geq 10, n \text{ even} \\
m^{(1/2) + (1/3(n-1)) + \epsilon} & \text{if } n \geq 11, n \text{ odd},
\end{cases}
\]

(8.5)
and more generally,
\[
\|x\| \ll m^{(1/2)+(3/n^2)+\epsilon} \quad \text{if } n \geq 12, \text{ } n \text{ even.} \tag{8.6}
\]
This is an improvement of the general result of Schinzel, Schlickiwei and Schmidt (1980) obtained by the lattice method. Schinzel, Schlickiwei and Schmidt (1980), Baker (1986), Heath-Brown (1991) and Baker and Schäffer (1992) have all applied the "discrete" results on small solutions of congruences to the analogous problems in Diophantine Approximation.

In order to obtain a sharper result for a general modulus it is desirable to improve the upper bound on \(|V \cap B_m|\) in (8.4) in the case \(\Delta = 1\). The methods of Burgess (1963), (1986) for bounding incomplete character sums and of Friedlander and Iwaniec (1985) for bounding incomplete Kloosterman sums may be useful for addressing this problem. For forms of the type \(AX_1X_2 + BX_3X_4\) we have been able to use their ideas to get \(|V \cap B_M| \ll M^4/p + M^2(\log p)^2\) and this is almost best possible. Indeed, for the form \(X_2 - X_3X_4, M^4/p + M^2 \log p \ll |V \cap B_M| \ll M^4/p + M^2 \log p.\) A couple of other results that may be useful in this investigation are the bound on the incomplete Gauss sum \(\sum_{x=0}^b e(2\pi x^2/m) \ll m^{1/2}\), for \(1 \leq b \leq m\), due to Lehmer (1970), and a reciprocity formula of Sander (1987) for quadratic forms.

**Bounds on solutions of the type \(\|x\| < c(Q)m^{1/2}\).**

Let \(Q(X) \in \mathbb{Z}[X]\) be a quadratic form and \(m\) be any positive integer. In the last two sections we have been interested in finding a nontrivial solution of (8.2) with \(\|x\| < c(n)m^{1/2}\), where \(c(n)\) is a constant depending only on \(n\). Grant (1992) obtained a weaker type of result but of interest in its own right. He proved that for any positive definite \(Q\) with \(n \geq 4\) there is a nontrivial solution of (8.2) with
\[
\|x\| < c(Q)m^{1/2}, \tag{8.7}
\]
where \(c(Q)\) is a constant depending on the form \(Q\). This is a useful bound if we think of holding \(Q\) fixed and varying the modulus \(m\). His method was to use the theta function associated with \(Q\) and make use of the theory of modular forms. In Cochrane (1993) we were able to generalize the result of Grant to arbitrary quadratic forms in \(n \geq 3\) variables. The approach we took was to make use of classical results on the representations of integers by quadratic forms.

**Systems of Quadratic Forms.**

Baker (1980, Theorem 1) proved that for any positive integers \(s\) and \(m\), and any \(\epsilon > 0\) there is a number \(N(\epsilon, s)\) such that for any quadratic forms \(Q_1, \ldots, Q_s \in \mathbb{Z}[X]\) with \(n > N(\epsilon, s)\), the congruence
\[
Q_1(x) \equiv \cdots \equiv Q_s(x) \equiv 0 \pmod{m} \tag{8.8}
\]
holds for all \(x \in \mathbb{Z}^s\).

71
has a nontrivial solution with $||x|| < m^{1/2+\varepsilon}$. No estimate was given on the size of $N(\varepsilon,s)$. Wang (1992) generalized this result to algebraic number fields. For prime moduli Schmidt was able to obtain a good value for $N(\varepsilon,s)$. His result, given in Theorem 5.9, is that (8.8) has a nontrivial solution with

$$||x|| < c(n,s,\varepsilon)p^{\frac{1}{2} + \frac{3\varepsilon}{2n} + \varepsilon}$$

(8.9)

when $m = p$. For small values of $n$ one can do better using the geometric method. In this manner we are able to obtain a solution of (8.8) with

$$||x|| \leq m^{\frac{1}{2} + \frac{1}{n(r)}}$$

(8.10)

for any modulus $m$, where $r$ is the remainder on dividing $n - s$ by $s + 1$; see Cochrane (1987b, Theorem 2). We obtain (8.8) by first showing that any set of $s$ quadratic forms over $\mathbb{F}_p$ vanish on a subspace of dimension $\left\lfloor \frac{n-8}{s+1} \right\rfloor$. However this may fall short of the truth, and any improvement on this dimension will yield a sharper bound in (8.10). When $n = 2(s + 1)$ one can do no better than $m^{\frac{1}{2} + \frac{1}{2n}}$ as an example in the same paper (1987b) shows.

When $s = 2$ it follows from a theorem of Amer (1976, Satz 8) that any two quadratic forms over $\mathbb{F}_p$ vanish on a subspace of dimension $\left\lfloor \frac{n-3}{2} \right\rfloor$, and thus by (6.5) there is a nontrivial solution of (8.8) with $||x|| \leq m^{\frac{1}{2} + \frac{3}{2n}}$, when $n$ is odd, and $||x|| \leq m^{\frac{1}{2} + \frac{3}{2(n-1)}}$, when $n$ is even.

We can sometimes improve on (8.9) by combining the method of exponential sums with the geometric method. Suppose for example that $s = 3$ and that $(Q_1,Q_2,Q_3)$ is a 3-tuple of quadratic forms in $\mathbb{F}_p[X]$ with $h$-invariant $h$. Then every form in the pencil $\lambda_1Q_1 + \lambda_2Q_2 + \lambda_3Q_3$ with $\lambda \neq 0 \in \mathbb{F}_p^3$ is of rank $\geq 2h - 2$ and so $\Phi(V) \leq p^{n - \frac{3}{2}} \leq p^{n - h + 1}$, where $V$ is the algebraic set defined by $Q_1$, $Q_2$ and $Q_3$. It follows from (2.14) that there is a nontrivial solution of (8.8) with

$$||x|| \ll p^{1 - \frac{h}{2} + \frac{2}{n}}.$$  

(8.11)

At the same time the bound of Schmidt (5.6) in this case is

$$||x|| \ll p^{\frac{1}{2} + \frac{3}{2n} + \varepsilon}.$$  

(8.12)

These two bounds are good for large values of $h$. When $h$ is small we appeal to the lattice method. Without loss of generality we may assume that $h(Q_1) = h$ and that $Q_1$ vanishes on the subspace $x_1 = \cdots = x_h = 0$. Then $Q_2$ and $Q_3$, restricted to this subspace of dimension $n - h$, vanish on a subspace of dimension $\left\lfloor \frac{n - h - 3}{2} \right\rfloor$. Hence $Q_1$, $Q_2$ and $Q_3$ vanish on a subspace of the same dimension. It follows that there exists a nontrivial solution of (8.8) with

$$||x|| \leq p^{\frac{1}{2} + \frac{h}{2n} + \frac{2}{n}}.$$  

(8.13)
Combining (8.11), (8.12) and (8.13) we obtain a nontrivial solution of (8.8) with

\[ \|x\| \ll \begin{cases} p^{\frac{3}{2} + \frac{2}{n}} & \text{and} \\
p^{\frac{1}{2} + \frac{\sqrt{1+96/n} + 3}{2n}} + \varepsilon \end{cases} \]  

(8.14)

which is sharper than (8.9) and (8.10). Much more can be done in this direction. In particular one should consider how many forms in the pencil are of each possible rank.

9. CUBIC FORMS

We shall focus here on finding small zeros of a single cubic form $C(X)$ in $\mathbb{F}_p[X]$. We may assume that $C(X)$ is irreducible over $\mathbb{F}_p$. Then there are two possible factorizations over $\overline{\mathbb{F}}_p$. Either $C(X)$ splits into a product of linear forms with coefficients in $\mathbb{F}_p$ or $C(X)$ remains irreducible over $\overline{\mathbb{F}}_p$. Suppose the former happens. Let $\gamma_1, \gamma_2, \gamma_3$ be a basis for $\mathbb{F}_p$ over $\mathbb{F}_p$, and let $L(X)$ be a linear factor of $C(X)$. Then $L(X) = \gamma_1 L_1(X) + \gamma_2 L_2(X) + \gamma_3 L_3(X)$ for some linear forms $L_i(X) \in \mathbb{F}_p[X]$, $1 \leq i \leq 3$, and a point $x$ in $\mathbb{F}_p^n$ is a zero of $C$ if and only if it is a zero of $L_1$, $L_2$ and $L_3$. Thus, by the results of section 7, $C(X)$ has a nontrivial zero with $\|x\| < p^{3/n}$ and moreover there exist cubic forms for which one can do no better.

The second possibility is that $C(X)$ is absolutely irreducible. In this case, by Theorem 4.7.11 there is a nontrivial zero with

\[ \|x\| \ll \begin{cases} p^{2/3} & \text{for } n = 3, 4 \\
p^{1 - \frac{1}{n-1}} & \text{for } n \geq 5. \end{cases} \]  

(9.1)

But if $n \geq 5$, then the result of (9.1) is weaker than the bound $\|x\| < p^{3/4}$ that the geometric method yields. If we impose the stronger condition that $C(X)$ be nonsingular then we obtain bounds of the type $p^{\frac{1}{2} + \frac{\sqrt{n-1}}{n-1}}$, for $n \geq 3$, and $p^{\frac{1}{3} + \frac{h}{n} + \varepsilon}$, respectively from Theorems 4.7.13 and Corollary 5.7.

In Cochrane (1989), we observed that combining the results of Schmidt with the results of the lattice method sometimes leads to sharper bounds. On the one hand (5.6) yields a solution of size $p^{\frac{1}{2} + \frac{h}{n} + \varepsilon}$ where $h$ is the $h$-invariant of $C(X)$, while (6.2) yields a solution of size $p^{h/n}$. Combining these two results we have that for any $\varepsilon > 0$, and any cubic form $C(X)$, there is a nontrivial zero of $C(X)$ with

\[ \|x\| \ll p^{\frac{1}{3}(1 + \sqrt{1+96/n}) + \varepsilon}. \]  

(9.2)

We summarize the current state of knowledge for cubic forms in the chart below for a few values of $n$; (the entries represent the size of a nontrivial zero up to a constant factor.) There is much room for improvement and many questions to be asked. In particular, we need to determine just what the best possible result is we should be aiming for. It is probably overly optimistic to expect a nontrivial zero of size $p^{3/n}$ always.
10. DIAGONAL CONGRUENCES

Chalk (1963) showed that for a single diagonal equation of the type

\[ a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} = c \]  

over \( \mathbb{F}_p \) with \( a_i \neq 0 \) and \( 2 \leq d_i \leq d \) for all \( i \),

\[ \Phi(V) \ll p^{n/2}. \]  

This follows easily from the classical upper bound \( |\sum_x e_p(ax^d)| \leq (d - 1)p^{1/2} \). He then estimated \( |V \cap B| \) using a version of (2.10). If \( c = 0 \) then it is clear that the upper bound in (10.2) is best possible; take for instance a quadratic form in an even number of variables. When \( c \neq 0 \) is it possible to improve the upper bound in (10.2) by a factor of \( p^{1/2} \)? Or to be precise, when exactly can such an improvement be obtained? We have already seen several special cases when such an improvement can be had. If the exponents \( d_i \) are distinct and not divisible by \( p \) then it follows from the result of Laumon, Theorem 4.1.22, and Theorem 3.35 that such an improvement holds. If the exponents are all equal, and not divisible by \( p \), then it follows from Example 4.8.14, that such an improvement holds. In Example 4.8.20 we saw that such an improvement holds for the diagonal equation \( a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^2 = 1 \).

Spackman (1979), (1981) generalized the work of Chalk to systems of diagonal equations. Let \( V \) be the algebraic set defined by

\[ \sum_{j=1}^{n} a_{ij} x_j^{d_j} = c_j, \quad 1 \leq i \leq s < n \]  

with coefficients in \( \mathbb{F}_p \), and \( 2 \leq d_j \leq d \), for all \( j \). He proved that

\[ \Phi(V) \leq c(n, s, d)p^{n/2} \]  

if every \( s \)-by-\( s \) submatrix of \( [a_{ij}] \) is nonsingular, and that

\[ \Phi(V) \leq c(n, s, d)p^{\frac{n}{2} + (s-2)(s-1)} \]
if the matrix $[a_{ij}]$ is $\mu$-weakly nonsingular, $\mu \geq 2$, and $n > \mu(s - 1)$. By $\mu$-weakly nonsingular we mean that in any set of $\mu(k - 1) + 1$ column vectors of $[a_{ij}]$ with $1 \leq k \leq s$, at least $k$ vectors are linearly independent over $\mathbb{F}_p$; here $\mu$ is a positive integer. It is remarkable that when $\mu = 2$ the same bound holds in (10.5) as in (10.4). Spackman then used (10.4) and (10.5) to estimate $|V \cap B|$ using a version of (2.10), just as Chalk had done.

If $V$ is a homogeneous variety defined by the form $f(X) = a_1X_1^d + \cdots + a_nX_n^d$ of degree $d \geq 2$, $p \nmid d$, with all the $a_i \neq 0$, then $V$ is nonsingular, and so by (4.7.14) and (4.7.15) there is a nontrivial zero of $f$ with $\|x\| \ll p^{\frac{1}{2} + \frac{1}{2(n-1)}}$, for $n \geq 4$, $\|x\| \ll p^{2/3}$, for $n = 3$. Baker (1983, Theorem 1) not only noticed this but also generalized the result to arbitrary moduli using exponential sums. His result is that for any modulus $m$, any integers $a_1, \ldots, a_n$ and any $\varepsilon > 0$ the congruence

$$a_1x_1^d + a_2x_2^d + \cdots + a_nx_n^d \equiv 0 \pmod{m} \quad (10.6)$$

has a nontrivial solution with

$$\|x\| \ll m^{\frac{1}{2} + \frac{1}{2(n-1)} + \varepsilon} \quad (10.7)$$

if $n \geq 4$ and $\|x\| \ll m^{\frac{3}{2} + \varepsilon}$ if $n = 3$.

For odd $d$, the geometric method of section 6 can be applied to (10.6). In this manner we obtain a nontrivial solution of (10.6) with

$$\|x\| < m^{\frac{1}{2} + \frac{d-1}{2(n-1)}} \quad (10.8)$$

for arbitrary moduli $m$, and $\|x\| < p^{1/2}$ when $m$ is a prime $p$, provided $d$ is odd and $n > d$.

If we allow the number of variables to be sufficiently large then we can get smaller solutions yet of (10.6). Baker (1986, Lemma 10.1) showed that for $n > c(d, \varepsilon)$ there exist non-negative integers satisfying (10.6) with $\|x\| \leq m^{(1/d) + \varepsilon}$. It is clear, by considering a form such as $X_1^d + \cdots + X_n^d$ that when $d$ is even the exponent $1/d$ is best possible. However, for odd $d$, it follows from the work of Schmidt (1980) that one can get a solution of size $m^\varepsilon$ for $n$ sufficiently large. Baker (1986, Theorem 12.1) generalized his result to systems of diagonal forms. It would be desirable to have explicit and sharp estimates for the constant $c(d, \varepsilon)$ appearing in Baker's work.

We are still a long way from understanding just how small nontrivial solutions of diagonal congruences can be, even simple ones such as

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \equiv 0 \pmod{p}, \quad (10.9)$$

or

$$x_1^4 + x_2^4 + x_3^4 + \cdots + x_n^4 \equiv 0 \pmod{p}. \quad (10.10)$$

Is $p^{2/3}$ the best we can do for (10.9) in general? Computer evidence suggests that (10.9) will always have a nontrivial solution with $\|x\| \leq \sqrt{p} + 1$ with the exception of the congruence $x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod{p}$, but the latter always has a solution with $\|x\| \leq \sqrt{2p}$. Certainly $p^{1/4}$ is the best possible result for (10.10) but how close to this do we actually get? Schmidt's result (5.8) yields a solution of (10.10) with $\|x\| \ll p^{\frac{1}{4} + \frac{8\varepsilon}{n} + \varepsilon}$. It may be worth tracing through Schmidt's method to see if it can be refined for a particular form such as that in (10.10).
11. Upper Bounds on $|V \cap B|$  

Let $p$ be a prime, $\mathbb{F}_p$ the finite field in $p$ elements, $\mathbf{F}(\mathbf{X}) = (f_1(\mathbf{X}), \ldots, f_s(\mathbf{X}))$ an $s$-tuple of polynomials in $\mathbb{F}_p[X_1, \ldots, X_n]$, and $V = V(\mathbf{F})$ the algebraic subset of $\mathbb{F}_p^n$ defined by

$$f_1(x) = f_2(x) = \cdots = f_s(x) = 0. \quad (11.1)$$

Let $B$ be the box of points in $\mathbb{F}_p^n$ given by

$$B = \{ x \in \mathbb{F}_p^n : a_i \leq x_i < a_i + b_i, 1 \leq i \leq n \} \quad (11.2)$$

for some integers $a_i, b_i$ with $1 \leq b_i \leq p$; (the inequality in (10.2) is understood by identifying $\mathbb{F}_p$ with an appropriate set of integer representatives). We say that $B$ is a cube of size $b$ if all of the $b_i$ equal $b$. Our interest here is in determining an upper bound on the cardinality of the set $V \cap B$. The two theorems we state are valid for a more general cartesian product of sets.

**Theorem 11.3.** Let $f$ be a nonzero polynomial in $\mathbb{F}_p[X_1, \ldots, X_n]$ of degree $d$ and $S = S_1 \times S_2 \times \cdots \times S_n$ be a cartesian product of subsets $S_i$ of $\mathbb{F}_p$, with $|S_i| \leq b, 1 \leq i \leq n$. Then

$$|\overline{V}(f) \cap S| \leq db^{n-1} \quad (11.4)$$

**Proof.** The proof is by induction on $n$. When $n = 1$ the result is elementary. Suppose the result holds for polynomials in $n - 1$ variables and let $f$ be a polynomial in $n$ variables. Suppose first that $f$ is absolutely irreducible. Then for any choice of $x_n \in S_n$, $f(X_1, \ldots, X_{n-1}, x_n)$ is a nonzero polynomial in $n - 1$ variables, and hence has at most $db^{n-2}$ zeros in $S_1 \times S_2 \times \cdots \times S_{n-1}$. There being at most $b$ choices for $x_n$ we obtain the result of the theorem. If $f = g_1 \cdots g_r$ with the $g_i$ irreducible then applying the first case to each of the $g_i$ yields the result of the theorem. \( \square \)

If $f$ is a linear polynomial then the upper bound in (11.4) is best possible in general. Take for example a cube centered at the origin and $f = X_1$. (See section 7.2 for a further discussion in this case.) The same can be said for any polynomial having a linear factor with coefficients in $\mathbb{F}_p$. On the other hand, one would hope that for absolutely irreducible polynomials of degree greater than one the upper bound in (11.4) could be sharpened. In particular, our real interest is in sharpening the upper bound when $b$ is small, say $b \ll p^{1/2}$.

**Theorem 11.5.** Schmidt (1983, Appendix). Let $\overline{V}$ be an algebraic subset of $\mathbb{F}_p^n$ of dimension $e$, defined by a set of polynomials of degrees $\leq d$. Let $S$ be as in Theorem 11.3. Then

$$|\overline{V} \cap S| \leq c(n, d)b^e,$$

for some constant $c(n, d)$ depending only on $n$ and $d$.

**Proof.** Let $C(\ell)$ denote the class of algebraic sets defined by a set of $\ell$ polynomials of degrees $\leq \ell$. Note that any algebraic set is contained in some $C(\ell)$. Suppose that $\overline{V} \in C(\ell)$. Then

76
we can express $\overline{V}$ as a union of $m \leq \ell'$ irreducible varieties $\overline{V}_i \in C(\ell')$, for some $\ell' = \ell'(n, \ell)$; (see Seidenberg (1974) section 65). Thus we may assume that $\overline{V}$ is irreducible.

Suppose that $\overline{V} \in C(\ell)$ is irreducible and defined over the finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$. Let $(\xi, \eta) = (\xi_1, ..., \xi_e, \eta_1, ..., \eta_h)$ be a generic point of $\overline{V}$ over $\mathbb{F}_q$, where $e = \text{dim}(\overline{V}) = \text{trdeg}(\xi)$ over $\mathbb{F}_q$ and $\eta_1, ..., \eta_h$ are algebraic over $\mathbb{F}_q(\xi)$. Moreover, there exist nonzero polynomials $g_i(X_1, ..., X_e, Y_i) \in \mathbb{F}_q[X_1, ..., X_e, Y_i]$ of degrees $\leq \ell_2(n, \ell), 1 \leq i \leq h$, such that $g_i(\xi, \eta_i) = 0$.

Write $S = S' \times S'' \subset \overline{F}^e \times \overline{F}^h$. Suppose that $a \in S'$ is such that $g_i(a, Y_i)$ is not identically zero for $1 \leq i \leq r$. Then for any $i$ there are at most $\text{deg}(g_i)$ choices $y_i$ for $Y_i$ such that $g_i(a, y_i) = 0$, and so we obtain at most $b^e \ell_2^h$ points of $\overline{V} \cap S$ for such $a$.

If $e = 0$ then since the $g_i$ are not identically zero $\ell_2^h$ is an upper bound on the number of points in $\overline{V}$ and so apriori on the number of points in $\overline{V} \cap S$. If $e > 0$ then we have to consider points $(a, y)$ in $\overline{V} \cap S$ with

$$g_1(a, Y_1) \ldots g_h(a, Y_h) \equiv 0. \tag{11.6}$$

Let

$$G(X_1, ..., X_e, Y_1, ..., Y_h) = \prod_{i=1}^h g_i(X_1, ..., X_e, Y_i) = \sum_{r_1, ..., r_h} C_{r_1, ..., r_h}(X_1, ..., X_e) Y_1^{r_1} \ldots Y_h^{r_h}.$$ 

Now a point $a$ satisfies (11.6) if and only if it is a zero of all of the polynomials $C_{r_1, ..., r_h}(X_1, ..., X_e)$. Thus, those points $(a, y)$ of $\overline{V}$ satisfying (11.6) form an algebraic subset $\overline{W}$ of $\overline{V}$ of dimension $< e$. Moreover, $\overline{W}$ is defined by at most $\ell + \ell_2^h$ polynomials of degrees $\leq \max(\ell, \ell_2^h)$. Thus $\overline{W} \in C(\ell_3)$ with $\ell_3 = \ell + \ell_2^h$, a constant depending only on $n$ and $d$. Assuming inductively that the theorem is true for algebraic sets of dimension less than $e$ we infer that $|\overline{W} \cap S| \leq c(n, d)b^{e-1}$, and that

$$|\overline{V} \cap S| \leq b^e \ell_2^h + c(n, d)b^{e-1} \leq c_2(n, d)b^e.$$

□
APPENDIX. QUADRATIC GAUSS SUMS.

The results of this section can essentially be found in Carlitz (1953). Let \( \mathbb{F}_q \) be the finite field in \( q = p^r \) elements with \( p \) odd, \( \psi = e_p(T_{\gamma}(\cdot)) \) be an additive character on \( \mathbb{F}_q \), and \( \chi \) be the multiplicative character on \( \mathbb{F}_q^* \) extending the Legendre symbol. It is well known (see eg. Lidl and Niederreiter (1983, Theorem 5.15)) that

\[
G(\chi, \psi) := \sum_{x \in \mathbb{F}_q} \psi(x^2) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x) = \begin{cases} (-1)^{r-1} \sqrt{q} & \text{if } p \equiv 1 \pmod{4} \\ (-1)^{r-1} i^r \sqrt{q} & \text{if } p \equiv -1 \pmod{4}. \end{cases} \tag{A.1}
\]

In particular, \( G^2(\chi, \psi) = \chi(-1)q \). For any \( \alpha, \beta \in \mathbb{F}_q \) with \( \alpha \neq 0 \) we have

\[
G(\alpha) := \sum_{x \in \mathbb{F}_q} \psi(\alpha x^2) = \chi(\alpha)G(1) \tag{A.2}
\]

and

\[
\sum_{x \in \mathbb{F}_q} \psi(\alpha x^2 + \beta x) = \chi(\alpha)\psi(-\beta^2/4\alpha)G(1). \tag{A.3}
\]

Putting \( \alpha = -\lambda \) and \( \beta = 2 \) in (A.3) we have

\[
\sum_{x} \psi(-\lambda x^2 + 2x) = \chi(\lambda)\psi(1/\lambda)G(-1),
\]

and so summing over \( \lambda \) we obtain

\[
G(-1) \sum_{\lambda \neq 0} \chi(\lambda)\psi(\alpha \lambda + 1/\lambda) = \sum_{\lambda} \sum_{x} \psi(-\lambda x^2 + 2x + \alpha \lambda)
= \sum_{x} \sum_{\lambda} \psi(\lambda(\alpha - x^2))
= \begin{cases} (\psi(2\gamma) + \psi(-2\gamma))q & \text{if } \alpha = \gamma^2, \\ 0 & \text{if } \chi(\alpha) = -1. \end{cases}
\]

Thus for any nonzero \( \alpha \) and \( \beta \) we have

\[
\sum_{\lambda \neq 0} \chi(\lambda)\psi(\alpha \lambda + \beta / \lambda) = \begin{cases} \chi(\beta)(\psi(2\gamma) + \psi(-2\gamma))G(1) & \text{if } \alpha \beta = \gamma^2, \\ 0 & \text{if } \chi(\alpha \beta) = -1. \end{cases} \tag{A.4}
\]

The sum appearing in (A.4) is sometimes called a Salie sum.

Now let \( Q \) be any nonsingular quadratic form over \( \mathbb{F}_q \) in \( n \geq 2 \) variables, \( c \) be any element of \( \mathbb{F}_q \) and let \( V \) be the algebraic set defined by \( Q(x) = c. \) Put

\[
\Delta = \Delta(Q) = \begin{cases} \chi((-1)^{n/2} \det Q) & \text{if } n \text{ is even} \\ \chi((-1)^{(n-1)/2} \det Q) & \text{if } n \text{ is odd}. \end{cases}
\]

78
and for any \( y \in \mathbb{F}^n_q \),
\[
\phi(V, y) = \begin{cases} 
\sum_{x \in V} \psi(x \cdot y) & \text{if } y \neq 0 \\
|V| - q^{n-1} & \text{if } y = 0.
\end{cases}
\]

Recall, as we saw in (2.5), for any \( y \) (including \( y = 0 \)),
\[
\phi(V, y) = q^{-1} \sum_{\lambda \neq 0} \sum_x \psi(\lambda(Q(x) - c) + x \cdot y).
\]

By making a linear change of variables we may assume that \( Q \) is diagonal, say
\[
Q(X) = a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2,
\]
for some nonzero \( a_1, \ldots, a_n \) in \( \mathbb{F}_q \). Then for any \( y \),
\[
\phi(V, y) = q^{-1} \sum_{\lambda \neq 0} \sum_x \psi\left(\lambda\left(\sum a_ix_i^2 - c\right)\right)\psi(x \cdot y)
\]
\[
= q^{-1} \sum_{\lambda \neq 0} \psi(-\lambda c)\prod_{i=1}^n \sum_{x_i} \psi(\lambda a_i x_i^2 + x_i y_i)
\]
\[
= q^{-1} \sum_{\lambda \neq 0} \psi(-\lambda c)\prod_i \chi(\lambda a_i)\psi(-y_i^2/4\lambda a_i)G(1)
\]
\[
= q^{-1}G(1)^n\chi(a_1 \cdots a_n) \sum_{\lambda \neq 0} \chi(\lambda)^n\psi(-c\lambda - d/\lambda), \tag{A.5}
\]

where \( d = \frac{1}{4} \sum a_i^{-1} y_i^2 = \frac{1}{4}Q^*(y) \), where \( Q^* \) is the quadratic form associated with the inverse of the matrix representing \( Q \).

To evaluate the sum remaining in (A.5) we consider various cases. Suppose first that \( n \) is even so that \( \chi(\lambda)^n = 1 \). If \( c = d = 0 \) then the sum in (A.5) is equal to \((q-1)\). If exactly one of \( c, d \) is zero and the other nonzero then the sum is equal to -1. Finally, if \( c \) and \( d \) are both nonzero then we are just left with a Kloosterman sum
\[
K = \sum_{\lambda \neq 0} \psi(-c\lambda - Q^*(y)/4\lambda),
\]
which is bounded above by \( 2\sqrt{q} \).

Suppose next that \( n \) is odd, so that \( \chi(\lambda)^n = \chi(\lambda) \). If \( c = d = 0 \) then the sum in (A.5) is equal to -1. If \( c = 0 \) but \( d \) is nonzero then the sum is equal to \( \chi(-d)G(1) \), while if \( d = 0 \) but \( c \) is nonzero the sum equals \( \chi(-c)G(1) \). Finally, if both \( c \) and \( d \) are nonzero then we are just left with a Salie sum as in (A.4). In summary we have that for any nonzero \( y \in \mathbb{F}^n_q \),
i) If \( n \) is even,
\[
\phi(V, y) = \begin{cases} 
\Delta q^{n/2-1}(q - 1) & \text{if } c = 0, \; Q^*(y) = 0 \\
-\Delta q^{n/2-1} & \text{if } c = 0, \; Q^*(y) \neq 0 \\
-\Delta q^{n/2-1} & \text{if } c \neq 0, \; Q^*(y) = 0 \\
\Delta q^{n/2-1}K & \text{if } c \neq 0, \; Q^*(y) \neq 0
\end{cases} \tag{A.6}
\]
i) If $n$ is odd,

$$\phi(V, y) = \begin{cases} 
0 & \text{if } c = 0, \ Q^*(y) = 0 \\
\Delta \chi(Q^*(y)) q^{n-1} - \frac{1}{2} & \text{if } c = 0, \ Q^*(y) \neq 0 \\
\Delta \chi(c) q^{n-1} - \frac{1}{2} & \text{if } c \neq 0, \ Q^*(y) = 0 \\
\Delta \chi(Q^*(y)) (\psi(\gamma) + \psi(-\gamma)) q^{n-1} - \frac{1}{2} & \text{if } c \neq 0, \ Q^*(y) \neq 0 \text{ and } cQ^*(y) = \gamma^2 \\
0 & \text{if } c \neq 0, \ Q^*(y) \neq 0 \text{ and } \chi(cQ^*(y)) = -1.
\end{cases} \quad (A.7)$$

Putting $y = 0$ yields the following formulae for $|V|$, the number of solutions of the equation $Q(x) = c$.

i) If $n$ is even,

$$|V| = \begin{cases} 
q^{n-1} + \Delta q^{n-1} (q - 1) & \text{if } c = 0 \\
q^{n-1} - \Delta q^{n-1} & \text{if } c \neq 0
\end{cases} \quad (A.8)$$

ii) If $n$ is odd,

$$|V| = \begin{cases} 
q^{n-1} & \text{if } c = 0 \\
q^{n-1} + \Delta \chi(c) q^{n-1} & \text{if } c \neq 0.
\end{cases} \quad (A.9)$$
REFERENCES


—, Exponential sums on $(G_m)^n$, Invent. Math. 101 (1990), 63–79.

A.N. Andrianov, Quadratic forms and Hecke operators, Springer Verlag, New York, 1980.


—, Small solutions of congruences, Mathematika 30 (1983), 164–188.


—, Counting points on curves over finite fields (d’après S.A. Stepanov), Seminaire Bourbaki 25e année 1972/73, 1973.


Typeset by AMS-TeX


Small zeros of quadratic congruences modulo $pq$, Mathematika 37 (1990), 261–272.


On the number of points on a complete intersection over a finite field, J. of Number Theory 38 (1991), 338–358.


I.E. Shparlinskii and A.N. Skorobogatov, Rational points on complete intersections, Mathematika 37 (1990), 201–208.

A.N. Skorobogatov, Exponential sums, the geometry of hyperplane sections, and some diophantine problems, Israel J. of Math. 80 (1992), 359–379.


R.A. Smith, The distribution of rational points on hypersurfaces defined over a finite field, Mathematika 17 (1970), 328–332.


K. Williams, Small solutions of the congruence $a_1 x_1^2 + a_2 x_2^2 + a_0 \equiv 0 \pmod p$, Proc. Cambridge Philos. Soc. 70 (1971), 409–412.