Weil Image Sums
(and some related problems)

Joshua E. Hill
Department of Mathematics
University of California, Irvine

Advancement to Candidacy Exam
2011-Sep-26 (rev. 1.04)

Talk Outline

1 Introduction
2 (Condensed) Literature Survey
3 Preliminary Results
4 Proposal
5 Conclusion
General Exponential Sums: Weyl Sums

Definition

A **Weyl Sum** is any sum of the form

\[ T = \sum_{j=1}^{N} e^{2\pi i P(j)} \]

where \( P(x) \) is a polynomial over the real numbers.

First approximations for bounds:

- Trivially: \( |T| \leq N \) (worst case)
- If \( P \) produced random outputs, then we would expect this to look like a 2-dimensional random walk: \( |T| = O(\sqrt{N}) \)
- Generally, there is some structure and we are stuck with \( |T| = o(N) \)
Applications

Exponential sums are a reoccurring tool

- Number Theory
  - Sums of Squares
  - Class field theory
- Discrete Fourier Transform
  - Implemented by some style of FFT: “If you speed up any nontrivial algorithm by a factor of a million or so, the world will beat a path toward finding useful applications for it.” – Numerical Recipes §13.0
- Paley graphs
- Computer Science
  - Graph theoretic applications
  - Random number generators

Characters

**Definition**

A character is a monoid homomorphism from a monoid $G$ to the units of a field $K^*$. 

- We will be principally working with finite fields, and our co-domain is $\mathbb{C}^*$.
- Fields have two obvious group structures we can use:
  - Additive
  - Multiplicative
- For this discussion, we are mainly concerned with additive characters.
Additive Characters

We can represent all additive characters of the form $\mathbb{F}_q \to \mathbb{C}^*$ nicely.

**Definition**

Let $\mathbb{F}_q$ be a finite field of $q = p^m$ elements (where $p$ is prime). The (absolute) trace of $\alpha \in \mathbb{F}_q$ is $\text{Tr}(\alpha) = \sum_{j=0}^{m-1} \alpha^p^j$.

**Theorem (Weber 1882)**

All additive characters of this type are of the form $\psi_\gamma(\alpha) = e^{\frac{2\pi i}{p^m} \text{Tr}(\gamma \alpha)}$ for some $\gamma \in \mathbb{F}_q$.

Weil Sums

**Definition**

A **Weil Sum** is any sum of the form

$$W_{f, \gamma} = \sum_{c \in \mathbb{F}_q} \psi_\gamma(f(c))$$

where $f(x)$ is a polynomial over $\mathbb{F}_q$ and $\psi_\gamma$ is an additive character.

Weil determined bounds:

**Theorem (Weil 1948)**

If $f(x) \in \mathbb{F}_q[x]$ is of degree $d > 1$ with $p \nmid d$ and $\psi_\gamma$ is a non-trivial additive character of $\mathbb{F}_q$, then $|W_{f, \gamma}| \leq (d - 1)\sqrt{q}$.
We adopt the notation $V_f = f(\overline{F_q})$

We examine incomplete Weil sums on the image set

$S_{f,\gamma} = \sum_{\alpha \in V_f} \psi_{\gamma}(\alpha)$

To remove the dependence on the choice of character, we look at the maximal such sum (over non-trivial additive characters)

$|S_f| = \max_{\gamma \in \overline{F_q}} |S_{f,\gamma}|$
Example

- In $\mathbb{F}_4$, we'll represent field elements as polynomials over $\mathbb{F}_2[t]$ mod the irreducible $t^2 + t + 1$.
- Examine $f(x) = x^3 + x$:

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$f(\alpha)$</th>
<th>$\text{Tr}(f(\alpha))$</th>
<th>$\text{Tr}(tf(\alpha))$</th>
<th>$\text{Tr}((t+1)f(\alpha))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$t$</td>
<td>$t+1$</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$t+1$</td>
<td>$t$</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

- $W_{f,1} = e^{\pi i 0} + e^{\pi i 0} + e^{\pi i 1} + e^{\pi i 1} = 0$
- $(V_f) = 3$
- $S_{f,1} = e^{\pi i 0} + e^{\pi i 1} + e^{\pi i 1} = -1$
- $|S_f| = 1$ (this is maximal)

Joshua E. Hill (UC Irvine)

Conjecture

Conjecture (Wan)

For all polynomials of degree $d$, with $p \nmid d$:

1. There is a real number $c_d$ such that $|S_f| \leq c_d \sqrt{q}$ for all $q$
2. $c_d \leq c \sqrt{d}$
3. $c \leq 1$

Some notes about conjecture (1):

- (1) is true when $q \gg d$ as a consequence of Cohen / Chebotarev / Lenstra-Wan (unpublished).
- If $d = o(q)$, then (1) isn’t very interesting.
What is Success?

Better information about $|S_f|$ or $\#(V_f)$:
- Better bounds
- An algorithm for computing or estimating
- Results that significantly refine the complexity class of these problems

Literature Survey Outline

1 Introduction

2 (Condensed) Literature Survey
   - Exponential Sums
   - Cardinality of Image Sets
   - $p$-adic Point Counting

3 Preliminary Results
   - Weil Image Sum Bounds
   - Image Set Cardinality

4 Proposal

5 Conclusion
Subsection 1

Exponential Sums

Gauss Sums

- Gauss sums were initially studied by... Gauss...
  Appeared in *Disquisitiones Arithmeticae*.
- If \( \psi \) is an additive character and \( \chi \) is a multiplicative character, then a Gauss sum is as sum of the form

\[
G(\psi, \chi) = \sum_{\alpha \in \mathbb{F}_q^*} \psi(\alpha) \chi(\alpha)
\]

- This is a finite-field analog to the \( \Gamma \) function.
- This sum is used extensively in number theory.
- Weil Image Sums are a variation of these sums (under the appropriate definitions of \( \chi(0) \)).
Weil Sums

Certain polynomial forms have special bounds for the associated Weil sum:

- $x^n + b$
- $p$-linear polynomials
- quadratics

Certain polynomials have explicit solutions for the associated Weil sum:

- $a x^{p^a+1} + bx$ [Carlitz 1980 for $a = 1$, Coulter 1998]

Some work for incomplete sums over alternate structures:

- Summed over quasi-projective varieties [Bombieri-Sperber, 1995]

Subsection 2

Cardinality of Image Sets
Cardinality of Image Sets

\[ \left\lceil \frac{q}{d} \right\rceil \leq \#(V_f) \leq q \]

- These bounds are sharp!
- If \( \#(V_f) = \left\lceil \frac{q}{d} \right\rceil \), then \( f \) is a polynomial with a **minimal value set**.
- If \( \#(V_f) = q \), then \( f \) is a **permutation polynomial**.

The Shape of the Problem (Average Results)

A vital companion function:

\[ f^*(u, v) = \frac{f(u) - f(v)}{u - v} \]

- If \( f^*(u, v) \) is absolutely irreducible then on average
  \[ \#(V_f) \sim \mu_d q + O_d(1) \] with \( \mu_d \) is the series \( 1 - e^{-1} \) truncated at \( d \) terms. [Uchiyama 1955]
Asymptotic Results I

\[ \#(V_f) = \mu q + O_d(\sqrt{q}) \]

First asymptotic results [Birch and Swinnerton-Dyer, 1959]

- \( \mu \) is dependent on some Galois groups induced by \( f \)
  
  \[ G(f) = \text{Gal} \left( f(x) - t/\mathbb{F}_q(t) \right) \quad \text{and} \quad G^+(f) = \text{Gal} \left( f(x) - t/\overline{\mathbb{F}_q}(t) \right) \]

  where \( G^+(f) \) is viewed as a subgroup of \( G(f) \).

- If \( G^+(f) \cong S_d \) (\( f \) is a “general polynomial”) then \( \mu = \mu_d \).
- Otherwise \( \mu \) depends only on \( G(f) \), \( G^+(f) \) and \( d \).

Asymptotic Results II

Cohen gave a way to explicitly calculate \( \mu \) [Cohen, 1970]

- Let \( K \) be the splitting field for \( f(x) - t \) over \( \mathbb{F}_q(t) \)
- Denote \( k' = K \cap \overline{\mathbb{F}_q} \)
- \( G^*(f) = \{ \sigma \in G(f) \mid K_\sigma \cap k' = \mathbb{F}_q \} \)
- \( G_1(f) = \{ \sigma \in G(f) \mid \sigma \text{ fixes at least one point} \} \)
- \( G_1^*(f) = G_1(f) \cap G^*(f) \)
- We then have \( \mu = \frac{\#(G_1^*)}{\#(G^*)} \).
- This provides a wonderful combinatorial explanation of \( \mu_d \) (proportion of non-derangements!)
Exact Results

Exact values for $\#(V_f)$ are known for very few classes of polynomials:

- Permutation polynomials (and exceptional polynomials)
- Polynomials with a minimal (or very small) value set
- Other

Permutation Polynomials

The class of polynomials where $\#(V_f) = q$

1. These polynomials are uncommon ($\sim e^{-q}$ for large $q$)
2. Dickson found all of the permutation polynomials $d \leq 6$ [Dickson 1896]
3. There is a ZPP algorithm to test to see if $f$ is a permutation polynomial. [Ma and von zur Gathen, 1995]
4. There is a deterministic algorithm to see if $f$ is a permutation polynomial that runs slightly sub-linear in $q$. [Shparlinski, 1992]
**Exceptional Polynomials**

Hayes harmonized these apparently disparate results by casting this into an Algo-Geometric setting [Hayes 1967]

### Definition

\( f(X) \in F_q[X] \) is an **exceptional polynomial** if when \( f^*(X, Y) \) is factored into irreducibles over \( F_q[X, Y] \) and all of these irreducible factors are not absolutely irreducible (that is, each irreducible factor cannot be irreducible over \( F_q[X, Y] \)).

- All exceptional polynomials are permutation polynomials [Cohen 1970], [Wan, 1993]
- If \( d > 1, p \nmid d \) and \( q > d^4 \), then all permutation polynomials are exceptional polynomials. (by Lang-Weil Bound)
- \( f \) is an exceptional polynomial if and only if \( \mu = 1 \).

**Small Image Set Polynomials**

- All polynomials with minimal value sets with \( d \leq \sqrt{q} \) were characterized in [Carlitz, Lewis, Mills, Straus 1961/1964]
- All polynomials with \( d^4 < q \) with \# \((V_f) < 2q/d \) were characterized in [Gomez-Calderon, 1986]
Other Cases

# \(V_f\) is known in a few other cases:
- Degree 0 and 1 cases are clear
- Degree 2,3 cases are due to [Kantor 1915] and [Uchiyama 1955]
- \(p\)-linear polynomials are known due to linearity
- Dickson Polynomials [Chou Gomez-Calderon, Mullen 1988]
- \(f(x) = x^k(1 + x)^{2^m-1}\) in \(\mathbb{F}_{2^m}\) (for \(k = \pm 1, \pm 2, 4\)) and \(f(x) = (x + 1)^d + x^d + 1\) for particular values of \(d\) [Cusick 2005]

An Important Note

- These results may seem to suggest that \(V_f\) can only be of certain forms. This is completely false.
- Lagrange interpolation can be used to build a polynomial with any image set.
- The restrictions discussed tell us that some of these image sets cannot be associated with polynomials of certain degrees.
- Note that we can always reduce mod \(X^q - X\) and get the same image set.
Subsection 3

$p$-adic Point Counting

The Zeta Function on Algebraic Sets

Consider the simultaneous zeros of a set of polynomials $f_1, \ldots, f_s \in \mathbb{F}_q[x_1, \ldots, x_n]$ over $\overline{\mathbb{F}}_q$; call this variety $X$.

- Let $X(\mathbb{F}_{q^k}) = X \cap \mathbb{F}_{q^k}$.

**Definition**

The zeta function of the algebraic set $X$ is defined to be

$$Z(X) = Z(X, T) = \exp \left( \sum_{k=1}^{\infty} \frac{\#(X(\mathbb{F}_{q^k}))}{k} T^k \right)$$
Curiouser and Curiouser

- Weil conjectured that the zeta function is rational.
- This conjecture was first proven by Dwork in 1960 using $p$-adic methods.
- This conjecture was again proven by Grothendieck in 1964 using $\ell$-adic cohomological methods.
- If it's rational, then intuitively there is only a fixed amount of information necessary to fully establish $Z(X)$. This is fundamentally what enables the $p$-adic approach to calculating $Z(X)$.
- Approaches to building up $Z(X)$ generally start by calculating $X(\mathbb{F}_q^k)$ up to a suitably large $k$.
- We only care about the number of points in $\mathbb{F}_q$, so we only need to look at $X(\mathbb{F}_q)$.

Point Counting Algorithm

The point counting algorithm of Lauder and Wan [Lauder-Wan 2008]:

**Lemma**

*If $f$ has total degree $d$ in $n$ variables and $p = O((d \log q)^C)$ for some constant $C$, then $\#(X(\mathbb{F}_q^k))$ can be calculated in polynomial time (polynomial in $p$, $m$, $k$, and $d$; exponential in $n$).*
Preliminary Results Outline

1. Introduction
2. (Condensed) Literature Survey
   - Exponential Sums
   - Cardinality of Image Sets
   - $p$-adic Point Counting
3. Preliminary Results
   - Weil Image Sum Bounds
   - Image Set Cardinality
4. Proposal
5. Conclusion

Joshua E. Hill (UC Irvine)
Weil Image Sums
Advancement Examination 33 / 61

Attribution

All of these results are taken from joint work with Daqing Wan.
Subsection 1

Weil Image Sum Bounds

Too Many Polynomials on the Dance Floor I

- Start with an arbitrary degree \( d \) polynomial
  \[
  f(x) = a_d x^d + \cdots + a_0, \quad a_i \in \mathbb{F}_q.
  \]
- \( f(x) \) and \( f(x - \lambda) \) have the same image set.
  - Setting \( \lambda = \frac{a_{d-1}}{a_d} \) removes \( x^{d-1} \) term.
  - Thus, WLOG we can examine \( f(x) = a_d x^d + a_{d-2} x^{d-2} + \cdots + a_0. \)
- We can do better: \( f(x) = x^d + a_{d-2} x^{d-2} + \cdots + a_1 x. \)
Too Many Polynomials on the Dance Floor II

Let \( I_f \) be some minimal preimage set that produces \( V_f \).

\[
|S_f| = \sum_{\beta \in I_f} \psi_{\gamma}(f(\beta)) \\
= \sum_{\beta \in I_f} \psi_{\gamma}\left(a_d \beta^d + a_{d-2} \beta^{d-2} + \cdots + a_1 \beta + a_0\right) \\
= \sum_{\beta \in I_f} \psi_{\gamma}\left(a_d \beta^d + a_{d-2} \beta^{d-2} + \cdots + a_1 \beta\right) \psi_{\gamma}(a_0) \\
= \left|\sum_{\beta \in I_f} \psi_{\gamma a_d} \left(\beta^d + \frac{a_{d-2}}{a_d} \beta^{d-2} + \cdots + \frac{a_1}{a_d} \beta\right)\right|
\]

Bounding \( |S_f| \)

We introduce two expressions to help us discuss bounds:

\[
\Phi_d = \max_{\substack{f \in \mathbb{F}_q[x] \\ \deg f = d}} \frac{|S_f|}{\sqrt{q}}
\]

- Examining \( \Phi_d \) gives us insight into the value \( c_d \): For all \( q \), \( c_d \geq \Phi_d \).
- A related question: for a given \( q \), what is the maximum \( |S_f| \) possible?

\[
|S_{A_q}| = \max_{A \subseteq \mathbb{F}_q} \left|\sum_{\alpha \in A} \psi_1(\alpha)\right|
\]
A Word of Warning

- At least one polynomial produces $A_q$ as an image set.
- This polynomial does not necessarily have degree relatively prime to $p$.
- Not every image set can be obtained as the image of a polynomial whose degree is relatively prime to $p$.

Example

- In $\mathbb{F}_4$ again.
- Examine $f(x) = x^2 + x$ ($p$-linear!):

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$f(\alpha)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$t$</td>
<td>1</td>
</tr>
<tr>
<td>$t+1$</td>
<td>1</td>
</tr>
</tbody>
</table>

  - Clearly no polynomial with degree 0 or 1 will have this image.
  - Idea: We don’t expect that degree 3 polynomials would be linear.
  - Actual Proof: Just evaluate all degree 3 polynomials in $\mathbb{F}_4[x]$ and note that none of them have this image.
Bounding Theorem Proof Outline I

**Theorem**

If \( q = p^m \) then

\[
|S_{A_q}| = \begin{cases} 
2^{m-1} & p = 2 \\
(p - 1) \csc \left( \frac{\pi}{2p} \right) & p > 2 
\end{cases}
\]

The “interesting part” of the proof:

- Trace is an \( \mathbb{F}_p \)-linear transform, and surjects onto \( \mathbb{F}_p \).
- \( \#(\ker Tr) = p^{m-1} \)
- Thus each element is hit \( p^{m-1} \) times.
- To find \( A_q \), find \( A_p \) and then choose all the elements in the same equivalence classes.

This reduces the question to the case where \( q = p \). The rest is “proof by calculus”.

Bounding Theorem Proof Outline II

- We are now summing distinct \( p \)th roots of unity, seeking the largest modulus possible.
- A proposed maximal sum must include all the roots of unity with angle \( \leq \pi/2 \) to the sum.
- \( p = 2 \) case is trivial. Assume \( p \) is odd.
- First stab: All of the \( p \)th roots of unity in quadrants I and IV?

\[
\sum_{j=-[p/4]}^{[p/4]} e^{2\pi ij/p} = \frac{1}{2} \csc \left( \frac{\pi}{2p} \right)
\]

- This is maximal, but obviously not unique.
Consequences of the Bounding Theorem

Corollary

As \( p \to \infty \) along the primes, \( |S_{A_q}| \sim \frac{q}{\pi} \)

![Graph showing the relationship between \( q \) and \( |S_{A_q}| \)]

Estimation of \( c_d \)

- Estimate \( \Phi_d \) by looking at all polynomials of that degree for various \( q \) or random sampling.
- We did both with fields up to 100 elements.
- The maximal value for each degree is plotted below.

![Graph showing the maximum values for each degree]
Estimation of $c$

- The same data, but additionally normalized by a factor of $\sqrt{d}$.

Subsection 2

Image Set Cardinality
Big-O and Soft-O Notation

- We have two eventually positive real valued functions
  \( A, B : \mathbb{N}^k \to \mathbb{R}^+ \). Take \( x \) as an \( n \)-tuple, with \( x = (x_1, \ldots, x_n) \).
- We’ll write \( |x|_{\min} = \min_i x_i \).

**Definition**

1. \( A(x) = O(B(x)) \) if there exists a positive real constant \( C \) and an integer \( N \) so that if \( |x|_{\min} > N \) then \( A(x) \leq CB(x) \).
2. \( A(x) = \tilde{O}(B(x)) \) if there exists a positive real constant \( C' \) so that \( A(x) = O(B(x) \log^{C'} (B(x) + 3)) \).

Naïve Algorithms

How to calculate \( \#(V_f) \)?

- Evaluate \( f \) at each point in \( \mathbb{F}_q \). Cost: \( \tilde{O}(qd) \) bit operations.
- For each \( a \in \mathbb{F}_q \), \( a \in V_f \iff \deg \gcd(f(x) - a, X^q - X) > 0 \). Cost: \( \tilde{O}(qd) \) bit operations.
Another connection between \( \#(V_f) \) and an algo-geometric structure:

**Theorem**

If \( f \in \mathbb{F}_q[x] \) of positive degree \( d \), then

\[
\#(V_f) = \sum_{i=1}^{d} (-1)^{i-1} N_i \sigma_i \left( \frac{1}{2}, \ldots, \frac{1}{d} \right)
\]

where \( N_k = \# \left \{ (x_1, \ldots, x_k) \in \mathbb{F}_q^k \mid f(x_1) = \cdots = f(x_k) \right \} \) and \( \sigma_i \) is the \( i \)th elementary symmetric function on \( d \) elements.

**Proof Outline I**

- \( V_{f,i} = \{ x \in V_f \mid \#(f^{-1}(x)) = i \} \) with \( 1 \leq i \leq d \) forms a partition of \( V_f \).
- Let \( m_i = \#(V_{f,i}) \). Thus \( m_1 + \cdots + m_d = \#(V_f) \). Introduce a new value \( \xi = -\#(V_f) \). We then have:
  \[
  m_1 + \cdots + m_d + \xi = 0 \tag{1}
  \]
- Define the space \( \tilde{N}_k = \left \{ (x_1, \ldots, x_k) \in \mathbb{F}_q^k \mid f(x_1) = \cdots = f(x_k) \right \} \).
  Then \( N_k = \#(\tilde{N}_k) \).
- By a counting argument,
  \[
  m_1 + 2^k m_2 + \cdots + d^k m_d = N_k \tag{2}
  \]
Proof Outline II

Arrange this into a system of equations:

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 & 1 \\
1 & 2 & \cdots & d & 0 \\
1 & 2^2 & \cdots & d^2 & 0 \\
\vdots & \vdots & \cdots & \vdots & \vdots \\
1 & 2^d & \cdots & d^d & 0
\end{pmatrix}
\begin{pmatrix}
m_1 \\
m_2 \\
m_3 \\
\vdots \\
m_d
\end{pmatrix}
= 
\begin{pmatrix}
0 \\
N_1 \\
N_2 \\
\vdots \\
N_d
\end{pmatrix}
\]

Solve for \( \xi \) using Cramer’s rule. There are some unfortunate details. See the paper. :-)

Variations on a Theme of Matrices

You can just as reasonably solve for \( m_j \) through the same process:

**Proposition**

\[
m_j = \binom{d}{j} \frac{1}{j} \sum_{i=1}^{d} (-1)^{j+i} N_i \sigma_{i-1}\left(1, \cdots, \frac{1}{j-1}, \frac{1}{j+1}, \cdots, \frac{1}{d}\right)
\]
Application of Lauder-Wan

- This equation is in terms of $N_k$, which we must establish.
- $\tilde{N}_k$ isn’t of any particularly desirable form: in particular, we can’t assume that it is non-singular projective or an abelian variety (if it were, faster algorithms would apply!)
- We’ll proceed through trickery.

Algorithm for finding $\#(V_f)$

**Theorem**

There is a an explicit polynomial $R$ and a deterministic algorithm which, for any $f \in \mathbb{F}_q[x]$ (with $q = p^m$, $p$ a prime, $f$ degree $d$), calculates $\#(V_f)$. This algorithm requires a number of bit operations bounded by $R(m^d d^d p^d)$.

More explicit performance: $\tilde{O} \left( 2^{8d+1} m^{6d+4} d^{12d-1} p^{4d+2} \right)$ bit operations.
Proof Outline

Define:

\[ F_k(x, z) = z_1 (f(x_1) - f(x_2)) + \cdots + z_{k-1} (f(x_1) - f(x_k)) \]

- If \( y \in \tilde{N}_k \) then \( F_k(y, z) = 0 \).
- If \( y \in \mathbb{P}_q^k \setminus \tilde{N}_k \) then the solutions to \( F_k(y, z) \) form a \((k-2)\)-dimensional subspace of \( \mathbb{P}_q^{k-1} \).
- If we denote the number of solutions to \( F_k(x, z) \) as \( #(F_k) \), then we have
  \[ #(F_k) = q^{k-1}N_k + q^{k-2}(q^k - N_k) \]
- So, we can solve:
  \[ N_k = \frac{#(F_k) - q^{2k-2}}{q^{k-2}(q - 1)} \]
- And that’s it!

Notes
Proposal: Goals

- A first step at understanding this style of sum is understanding $V_f$.
  - Calculating $V_f$.
  - Estimating $V_f$.
  - Refining bounds for or estimating $\mu$.
  - Refining the constant associated with the $O_d(\sqrt{q})$ term; current term is highly exponential in $d$; $d^{O(1)}$ may be possible.

- We seek to investigate incomplete exponential sums evaluated on image sets.
  - Work thus far has been with additive characters and Weil sums.
  - Many of the same approaches would work with Weil sums of multiplicative characters.
  - Other sum styles can also be investigated: incomplete Gauss and Jacobi sums may also yield results.

Proposal: Style of Results

We look for results of the following styles:
- Improved explicit bounds.
- Algorithms for explicitly calculating values.
- Algorithms for producing estimates.
- Refinements to the complexity class of these problems.
Conclusion

We outlined problems in finite fields concerning:
- incomplete Weil exponentials sums (Weil Image Sums)
- the image set of a polynomial

We surveyed literature relevant to these problems.

We discussed new findings related to these problems.

Proposed a course of investigation for further work.
The principal font is Evert Bloemsma’s 2004 humanist san-serif font Legato. This font is designed to be exquisitely readable, and is a significant departure from the highly geometric forms that dominate most san-serif fonts. Legato was Evert Bloemsma’s final font prior to his untimely death at the age of 46.

Equations are typeset using the MathTime Professional II (MTPro2) fonts, a font package released in 2006 by the great mathematical expositor Michael Spivak.

The serif text font (which appears mainly as text within mathematical expressions) is Jean-François Porchez’s wonderful 2002 Sabon Next typeface.

The URLs are typeset in Luc(as) de Groot’s 2005 Consolas, a monospace font with excellent readability.

Diagrams were produced in Mathematica.