A Gauss sum estimate in arbitrary finite fields

Jean Bourgain\textsuperscript{a}, Mei-Chu Chang\textsuperscript{b}

\textsuperscript{a} Institute for Advanced Study, Olden Lane, Princeton, NJ 08540, USA
\textsuperscript{b} Mathematics Department, University of California, Riverside, CA 92521, USA

Received 7 September 2005; accepted after revision 23 January 2006
Available online 29 March 2006
Presented by Jean Bourgain

Abstract

We establish bounds on exponential sums \( \sum_{x \in \mathbb{F}_q} \psi(x^n) \) where \( q = p^m \), \( p \) prime, and \( \psi \) an additive character on \( \mathbb{F}_q \). They extend the earlier work of Bourgain, Glibichuk, and Konyagin to fields that are not of prime order \((m \geq 2)\). More precisely, a non-trivial estimate is obtained provided \( n \) satisfies \( \gcd(n, \frac{q-1}{p^\nu-1}) < p^{-\nu q^{1-\epsilon}} \) for all \( 1 \leq \nu < m \), \( \nu | m \), where \( \epsilon > 0 \) is arbitrary.

© 2006 Académie des sciences. Published by Elsevier SAS. All rights reserved.
où $\varepsilon > 0$ est fixé et arbitraire, on a l’estimée
\[
\left| \sum_{x \in \mathbb{F}_q} \psi (x^n) \right| < cq^{1-\delta}
\]
pour tout caractère additif non-trivial $\psi$ de $\mathbb{F}_q$ et où $\delta = \delta(\varepsilon) > 0$.

1.
Denote $q = p^m$ with $p$ prime, $m \in \mathbb{Z}$, $m \geq 1$.

Non-trivial subfields of $\mathbb{F}_q$ are of size $p^\nu$ where $1 \leq \nu < m$, $\nu | m$. Denote $\text{Tr}(x) = x + x^p + \cdots + x^{p^{m-1}}$ the trace of $x \in \mathbb{F}_q$.

Let $\psi(x) = e_p(\text{Tr}(\xi x))$, $\xi \in \mathbb{F}_q^*$ be a non-trivial additive character of $\mathbb{F}_q$. Our aim is to extend certain estimates on exponential sums of the type
\[
\left| \sum_{x \in \mathbb{F}_q} \psi(x^n) \right| < c q^{1-\delta} \tag{1}
\]
and
\[
\left| \sum_{j \leq t_1} \psi(g^j) \right| < t_1 q^{1-\delta} \tag{2}
\]
obtained in [2] for prime fields ($m = 1$) to the general case ($m \geq 2$) (in (2), we denoted $\text{ord}(g)$ the multiplicative order of $g \in \mathbb{F}_q^*$).

More precisely, it was shown in [2] that if $q = p$ and $\gcd(n, p-1) < p^{1-\varepsilon}$ ($\varepsilon > 0$ arbitrary) in (1) (resp. $t \geq t_1 > p^\varepsilon$ in (9)), then $\left| \sum_{x \in \mathbb{F}_q} \psi(x^n) \right| < p^{1-\delta}$ (resp. $\left| \sum_{j \leq t_1} \psi(g^j) \right| < t_1 p^{-\delta}$), where $\delta = \delta(\varepsilon) > 0$.

The method involved in [2] as well as here is the ‘sum-product’ approach, which permits us to establish non-trivial bounds in certain situations where ‘classical’ methods such as Stepanov’s do not seem to apply (see [4] for details).

Our main results are the following:

**Theorem 1.** Assume in (1) that $n| (p^m - 1)$ and satisfies the condition
\[
\gcd\left(n, \frac{p^m - 1}{p^\nu - 1}\right) < p^{-\nu} q^{1-\varepsilon} \quad \text{for all } 1 \leq \nu < m, \nu | m \tag{3}
\]
where $\varepsilon > 0$ is arbitrary and fixed. Then
\[
\max_{a \in \mathbb{F}_q^*} \left| \sum_{x \in \mathbb{F}_q} \psi(ax^n) \right| < c q^{1-\delta} \tag{4}
\]
where $\delta = \delta(\varepsilon) > 0$.

**Theorem 2.** Assume in (2) that $g \in \mathbb{F}_q^*$ and
\[
t \geq t_1 > q^\varepsilon \quad \text{and} \quad \max_{1 \leq \nu < m, \nu | m} \gcd(p^\nu - 1, t) < q^{-\varepsilon} t \tag{5}
\]
for some $\varepsilon > 0$. Then again
\[
\max_{a \in \mathbb{F}_q^*} \left| \sum_{j \leq t_1} \psi(ag^j) \right| < c q^{-\delta} t_1 \tag{6}
\]
where $\delta = \delta(\varepsilon) > 0$.

**Remark.** The classical bound
\[
\left| \sum_{x \in \mathbb{F}_q} \psi(x^n) \right| \leq (n - 1)q^{1/2} \tag{7}
\]
becomes trivial for $n > q^{1/2}$. The first non-trivial estimate when $n > q^{1/2}$ was obtained in [5], considering values of $n$ up to $p^{1/6}q^{1/2}$. Condition (3) (and similarly (5)) has clearly to do with the presence of non-trivial subfields of $\mathbb{F}_q$, which we do not want to contain most of the multiplicative group $\{x^n \mid x \in \mathbb{F}_q^*\}$ (and $\{g^j \mid j \leq t\}$ resp.). A condition of this form is obviously needed.

2.

As pointed out earlier, we rely on the same approach as in [2]. The proof of Theorem 2 (which implies Theorem 1) will be based on the following two results:

**Proposition 3.** Let $A \subset \mathbb{F}_q$ and $|A| > q^\varepsilon$. Let $\varepsilon > \kappa > 0$ and assume
\[ |A \cap (\eta + S)| < q^{-\varepsilon}|A| \] (8)
whenever $\eta \in \mathbb{F}_q$ and $S \subset \mathbb{F}_q$ satisfies the condition
\[ |S| < q^{1-\varepsilon/20} \] (9)
and
\[ |S + S| + |S.S| < q^\kappa|S|. \] (10)
Then for some $k = k(\kappa) \in \mathbb{Z}_+$ and $\delta = \delta(\kappa) > 0$
\[ \max_{a \in \mathbb{F}_q^*} \left| \sum_{x_1, \ldots, x_k \in A} \psi(ax_1 \cdots x_k) \right| < q^{-\delta}|A|^k. \] (11)

In (10), we denoted $S + S = \{x + y : x, y \in S\}$ (resp. $S.S = \{x.y : x, y \in S\}$) the sum-set (resp. the product-set). For small $\kappa > 0$, condition (10) expresses the property that both $S + S$ and $S.S$ are not much larger than $S$. Hence it is important to understand the structure of such sets.

The next result provides the required information:

**Proposition 4.** Assume $S \subset \mathbb{F}_q$, $|S| > q^\delta$ and $|S + S| + |S.S| < K|S|$. Then there is a subfield $G$ of $\mathbb{F}_q$ and $\xi \in \mathbb{F}_q^*$ such that
\[ |G| < K^C|S| \] (12)
and
\[ |S \setminus \xi G| < K^C \] (13)
where $C = C(\delta)$.

Proposition 3 is essentially Theorem 3.1 in [1]. The only difference is that in [1] we consider subsets of a ring $R = \prod Z_{g_j}$ instead of a field $\mathbb{F}_q$; but the essentially general argument carries over verbatim to the present situation (in fact it simplifies since the set $R \setminus R^*$ of non-invertible elements is trivial here). The proof of Theorem 3.1 in [1] uses only the additive Fourier transform.

We may again identify the set of additive characters of $\mathbb{F}_q$ with $\mathbb{F}_q$, letting
\[ \psi(x) = e_p(\text{Tr}(\xi x)); \quad e_p(y) = e^{2\pi i y/p} \]
where $\xi$ ranges in $\mathbb{F}_q$.

Proposition 4 appears in [3], as a byproduct of the proof of the sum-product theorem in prime fields.

3.

With Propositions 3 and 4 at hand, the proof of Theorem 2 is rather straightforward. For simplicity, take $t_1 = t$ (considering the complete sum), in which case $A = \{g^j : 0 \leq j < t\}$ is a multiplicative subgroup of $\mathbb{F}_q^*$. Assuming $A$ satisfies conditions (8)–(10) from Proposition 3, the conclusion (11) is then simply
\[ \max_{a \in \mathbb{F}_q^*} \left| \sum_{x \in A} \psi(ax) \right| < q^{-\delta}|A| \] (14)
which is (6).
(To treat incomplete sums, i.e. \(t_1 < t\), some minor additional technicalities are involved.)

Assume that for some \(\eta\) one has
\[
\left| A \cap (\eta + S) \right| \geq q^{-\kappa} |A|
\]  
(15)

with \(S\) satisfying (9), (10). Thus \(|S| > t q^{-\kappa} > q^{\varepsilon/2} \) if \(\kappa < \varepsilon/2\).

Apply Proposition 4 to the set \(S\) with \(\delta = \varepsilon/2, \quad K = q^{\kappa}\).

The subfield \(G\) satisfies by (12) and (9)
\[
|G| < q^{\kappa C} |S| < q^{1-\varepsilon/20 + \kappa C(\varepsilon)} < q
\]

taking \(\kappa\) small enough. Hence \(G\) is non-trivial and
\[
|G| = p^v \quad \text{for some } v < m, v|m.
\]  
(16)

From (13) and (15)
\[
\left| A \cap (\eta + \xi G) \right| > q^{-\kappa} |A| - q^{\kappa C(\varepsilon)} > \frac{1}{2} q^{-\kappa} |A|
\]  
(17)

implying that
\[
\left| \left\{ (s, s'): 0 \leq s, s' \leq t - 1, g^s - g^{s'} \in \xi G \right\} \right| > \frac{1}{4} q^{-2\kappa} t^2.
\]  
(18)

Equivalently, we may write
\[
\left| \left\{ (s, s'): 0 \leq s, s' \leq t - 1, g^s - g^{s'} \in \xi G \right\} \right| > \frac{1}{4} q^{-2\kappa} t^2.
\]

In particular there exist some \(s' \neq 0\) such that denoting \(\xi_1 = \xi(1 - g^{s'})^{-1}\)
\[
\left| \left\{ s: 0 \leq s \leq t - 1, g^s \in \xi_1 G \right\} \right| \gtrsim q^{-2\kappa} t.
\]  
(19)

Let \(g = g_0^{(q-1)/t}\), where \(g_0\) is a generator of \(\mathbb{F}_q^*\). Since by (16) \(x^{p^v-1} = 1\) for all \(x \in \mathbb{G}^*\), it follows from (19) that
\[
\left| \left\{ s: 0 \leq s \leq t - 1, g_0^{g_1^{-1}(p^v-1)s} = \xi_1^{p^v-1} \right\} \right| \gtrsim q^{-2\kappa} t.
\]

Therefore there is some \(0 < s \lesssim q^{2\kappa}\) such that \(g_0^{\frac{1}{p^v-1}(p^v-1)s} = 1\), or equivalently \(t | s(p^v - 1)\). But then \(\gcd(t, p^v - 1) > q^{-2\kappa} t\), violating assumption (5).

References

[1] J. Bourgain, M.-C. Chang, Exponential sum estimates over subgroups and almost subgroups of \(\mathbb{Z}_q^*\), where \(q\) is composite with few factors, GAFA, in press.


