A GAUSS SUM ESTIMATE IN ARBITRARY FINITE FIELDS

Jean Bourgain   Mei-Chu Chang

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

UNE ESTIMÉE DES SOMMES DE GAUSS DANS DES CORPS FINIS ARBITRAIRES

Resumé. On etabli des bornes sur les sommes d'exponentielles $\sum_{x\in\mathbb{F}_q}\ \psi(x^n)$ où $q=p^m$, p est premier et ψ est un caractère additif de $\mathbb{F}_q$. Il s'agit d'une extension des résultats de [BGK] pour un corps qui n'est pas d'ordre premier, c.a.d. $m\geq 2$. On obtient une estimée non-triviale pour tout n satisfaisant la condition pgcd$\,(n, \frac{q-1}{p^\nu-1}) <$ $p^{-\nu}q^{1-\varepsilon}$ pour tout $1\leq\nu<m, \nu|m$ et où $\varepsilon>0$ est arbitraire.

Version fransaise abrégée

Dans cette note nous démontrons une extension des résultats obtenus dans [BGK] pour des sommes de Gauss $\sum_{x\in\mathbb{F}_q}\psi(x^n)$ et plus generalement $\sum_{j=1}^{t_1}\psi(g^j)$, où ψ est un caractère additif de $\mathbb{F}_q$, $g\in\mathbb{F}_q^*$ d'ordre multiplicatif $t\geq t_1$. Les résultats de [BGK] traitent le cas où $q=p$ est premier alors qu'ici on considère le cas général $q=p^m$. En usant de la même approche basée sur des propriétés combinatoires des ensembles 'sommes' et 'produits', nous établissons des estimées non-triviales sous des hypothèses très faibles (et essentiellement optimales). Si n satisfait la condition

$$\text{pgcd}\left(n, \frac{q-1}{p^\nu-1}\right) < p^{-\nu}q^{1-\varepsilon} \text{ pour tout } 1\leq\nu<m, \nu|m$$

où $\varepsilon > 0$ est fixé et arbitraire, on a l'estimée

$$\Big|\sum_{x\in\mathbb{F}_q}\psi(x^n)\Big| < cq^{1-\delta}$$

pour tout caractère additif non-trivial ψ 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^ν where $1 \leq \nu < m, \nu|m$. Denote $Tr(x) = x + x^p + \ldots + x^{p^{m-1}}$ the trace of $x \in \mathbb{F}_q$.

Let $\psi(x) = e_p\big(Tr(\xi x)\big), \xi \in \mathbb{F}_q^*$ be a nontrivial additive character of $\mathbb{F}_q$. Our aim is to extend certain estimates on exponential sums of the type

$$\sum_{x\in\mathbb{F}_q}\psi(x^n) \tag{1.1}$$

and

$$\sum_{j\leq t_1}\psi(g^j) \qquad t_1 \leq t = \mathrm{ord}(g) \tag{1.2}$$

obtained in [BGK] for prime fields ($m = 1$) to the general case ($m \geq 2$) (in (1.2), we denoted $\mathrm{ord}(g)$ the multiplicative order of $g \in \mathbb{F}_q^*$).

More precisely, it was shown in [BGK] that if $q = p$ and $\gcd(n, p-1) < p^{1-\varepsilon}$ ($\varepsilon > 0$ arbitrary) in (1.1) $\big($resp. $t \geq t_1 > p^\varepsilon$ in (2.2)$\big)$, then $|\sum_{x\in\mathbb{F}_q}\psi(x^n)| < p^{1-\delta}$ (resp. $|\sum_{j\leq t_1}\psi(g^j)| < t_1 p^{-\delta}$), where $\delta = \delta(\varepsilon) > 0$.

The method involved in [BGK] 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 [KS] for details).

Our main results are the following

Theorem 1. *Assume in (1.1) that $n|(p^m - 1)$ and satisfies the condition*

$$\gcd\Big(n, \frac{p^m-1}{p^\nu-1}\Big) < p^{-\nu}q^{1-\varepsilon} \text{ for all } 1 \leq \nu < m, \nu|m \tag{1.3}$$

where $\varepsilon > 0$ is arbitrary and fixed. Then

$$\max_{a\in\mathbb{F}_q^*}\Big|\sum_{x\in\mathbb{F}_q}\psi(ax^n)\Big| < cq^{1-\delta} \tag{1.4}$$

where $\delta = \delta(\varepsilon) > 0$.

and

Theorem 2. *Assume in (1.2) that $g \in \mathbb{F}_q^*$ and*

$$t \geq t_1 > q^\varepsilon \text{ and } \max_{\substack{1 \leq \nu < m \\ \nu | m}} gcd(p^\nu - 1, t) < q^{-\varepsilon} t \tag{1.5}$$

for some $\varepsilon > 0$. Then again

$$\max_{a \in \mathbb{F}_q^*} \Big| \sum_{j \leq t_1} \psi(ag^j) \Big| < cq^{-\delta} t_1 \tag{1.6}$$

where $\delta = \delta(\varepsilon) > 0$.

Remark. The classical bound

$$\Big| \sum_{x \in \mathbb{F}_q} \psi(x^n) \Big| \leq (n-1) q^{1/2} \tag{1.7}$$

becomes trivial for $n > q^{1/2}$. The first nontrivial estimate when $n > q^{1/2}$ was obtained in [S], considering values of n up to $p^{\frac{1}{6}} q^{\frac{1}{2}}$. Condition (1.3) (and similarly (1.5)) has clearly to do with the presence of nontrivial subfields of $\mathbb{F}_q$, which we do not want to contain most of the multiplicative group $\{x^n | x \in \mathbb{F}_q^*\}$ (and $\{g^j | j \leq t\}$ resp.). A condition of this form is obviously needed.

2. As pointed out earlier, we rely on the same approach as in [BGK]. 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*

$$|A \cap (\eta + S)| < q^{-\kappa} |A| \tag{2.1}$$

whenever $\eta \in \mathbb{F}_q$ and $S \subset \mathbb{F}_q$ satisfies the condition

$$|S| < q^{1 - \frac{\varepsilon}{20}} \tag{2.2}$$

and

$$|S + S| + |S.S| < q^\kappa |S|. \tag{2.3}$$

Then for some $k = k(\kappa) \in \mathbb{Z}_+$ and $\delta = \delta(\kappa) > 0$

$$\max_{a \in \mathbb{F}_q^*} \Big| \sum_{x_1, \dots, x_k \in A} \psi(a x_1 \dots x_k) \Big| < q^{-\delta} |A|^k. \tag{2.4}$$

In (2.3), 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 (2.3) 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*

$$|G| < K^C|S| \tag{2.5}$$

and

$$|S \backslash \xi G| < K^C \tag{2.6}$$

where $C = C(\delta)$.

Proposition 3 is essentially Theorem 3.1 in [BC]. The only difference is that in [BC] we consider subsets of a ring $R = \prod \mathbb{Z}_{g_j}$ 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 $R\backslash R^*$ of non-invertible elements is trivial here). The proof of Theorem 3.1 in [BC] uses only the additive Fourier transform.

We may again identify the set of additive characters of $\mathbb{F}_q$ with $\mathbb{F}_q$, letting

$$\psi(x) = e_p\big(Tr(\xi x)\big); \quad e_p(y) = e^{\frac{2\pi i y}{p}}$$

where ξ ranges in $\mathbb{F}_q$.

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

3. With Proposition 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 (2.1)-(2.3) from Proposition 3, the conclusion (2.4) is then simply

$$\max_{a \in \mathbb{F}_q^*} \Big| \sum_{x \in A} \psi(ax) \Big| < q^{-\delta}|A| \tag{3.1}$$

which is (1.6).

(To treat incomplete sums, i.e. $t_1 < t$, some minor additional technicalities are involved).

Assume that for some η one has

$$|A \cap (\eta + S)| \geq q^{-\kappa}|A| \tag{3.2}$$

with S satisfying (2.2), (2.3). Thus $|S| > tq^{-\kappa} > q^{\varepsilon - \kappa} > q^{\frac{\varepsilon}{2}}$ if $\kappa < \frac{\varepsilon}{2}$.

Apply Proposition 4 to the set S with $\delta = \frac{\varepsilon}{2}, K = q^\kappa$.

The subfield G satisfies by (2.5) and (2.2)

$$|G| < q^{\kappa C}|S| < q^{1-\frac{\varepsilon}{20}+\kappa C(\varepsilon)} < q$$

taking κ small enough. Hence G is nontrivial and

$$|G| = p^\nu \text{ for some } \nu < m, \nu | m. \tag{3.3}$$

From (2.6) and (3.2)

$$|A \cap (\eta + \xi G)| > q^{-\kappa}|A| - q^{\kappa C(\varepsilon)} > \frac{1}{2} q^{-\kappa}|A| \tag{3.4}$$

implying that

$$|\{(s, s') : 0 \leq s, s' \leq t-1, g^s - g^{s'} \in \xi G\}| > \frac{1}{4} q^{-2\kappa} t^2. \tag{3.5}$$

Equivalently, we may write

$$|\{(s, s') : 0 \leq s, s' \leq t-1, g^s - g^{s'+s} \in \xi G\}| > \frac{1}{4} q^{-2\kappa} t^2.$$

In particular there exist some $s' \neq 0$ such that denoting $\xi_1 = \xi(1 - g^{s'})^{-1}$

$$|\{s : 0 \leq s \leq t-1, g^s \in \xi_1 G\}| \gtrsim q^{-2\kappa} t. \tag{3.6}$$

Let $g = g_0^{\frac{q-1}{t}}$, where g_0 is a generator of $\mathbb{F}_q^*$. Since by (3.3) $x^{p^\nu - 1} = 1$ for all $x \in G^*$, it follows from (3.6) that

$$|\{s : 0 \leq s \leq t-1, g_0^{\frac{q-1}{t}(p^\nu-1)s} = \xi_1^{p^\nu - 1}\}| \gtrsim q^{-2\kappa} t.$$

Therefore there is some $0 < s \lesssim q^{2\kappa}$ such that $g_0^{\frac{q-1}{t}(p^\nu-1)s} = 1$, or equivalently $t | s(p^\nu - 1)$. But then $\gcd(t, p^\nu - 1) > q^{-2\kappa} t$, violating assumption (1.5).

References

[BGK]. J. Bourgain, A. Glibichuk, S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, to appear in J. London Math. Soc.

[BKT]. J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and their applications*, GAFA 14 (2004), no. 1, 27–57.

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

[KS]. S. Konyagin, I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge UP, Cambridge, 1999.

[S]. I. Shparlinski, *Bounds on Gauss sums in finite fields*, Proc. AMS, Vol. 132, no 10, 2817–2824.

Institute for Advanced Study, Olden Lane, Princeton, N.J. 08540, U.S.A.

E-mail address: `bourgain@math.ias.edu`

Mathematics Department, University of California, Riverside, CA 92521

E-mail address: `mcc@math.ucr.edu`