Character Sums in Finite Fields [1] [2]

Mei-Chu Chang[3]

Let $\mathbb{F}_q$ be a finite field of order q with $q = p^n$, where p is a prime. A multiplicative character χ is a homomorphism from the multiplicative group $\langle \mathbb{F}_q^*, \cdot \rangle$ to the unit circle. In this note we will mostly give a survey of work on bounds for the character sum $\sum_x \chi(x)$ over a subset of $\mathbb{F}_q$. In Section 5 we give a nontrivial estimate of character sums over subspaces of finite fields.

§1. Burgess' method and the prime field case.

For a prime field $\mathbb{F}_p$ and when the subset is an interval, Polya and Vinogradov (Theorem 12.5 in [IK]) had the following estimate.

Theorem 1.1. (Polya-Vinogradov) *Let χ be a non-principal Dirichlet character modulo p. Then*

$$\Big| \sum_{m=a+1}^{a+b} \chi(m) \Big| < C p^{\frac{1}{2}} (\log p).$$

This bound is only nontrivial when $b > p^{\frac{1}{2}}(\log p)$. Forty four years later Burgess [B1] made the following improvement.

Theorem 1.2. (Burgess) *Let χ be a non-principal Dirichlet character modulo p. For any $\varepsilon > 0$, there exists $\delta > 0$ such that if $b > p^{\frac{1}{4}+\varepsilon}$, then*

$$\Big| \sum_{m=a+1}^{a+b} \chi(m) \Big| \ll p^{-\delta} b.$$

Applying the theorem to a quadratic character, one has the following corollary. (The power of $1/\sqrt{e}$ is gained by sieving.)

Corollary 1.3. *The smallest quadratic non-residue modulo p is at most $p^{\frac{1}{4\sqrt{e}}+\varepsilon}$ for $\varepsilon > 0$ and $p > c(\varepsilon)$.*

Note that we always assume $\varepsilon > 0$ and $p > c(\varepsilon)$.

The proof of the Burgess theorem is based on an amplification argument (due to Vinogradov), a bound on the multiplicative energy of two intervals (Lemma 1.4) and Weil's estimate (Theorem 1.5).

The multiplicative energy $E(A, B)$ of two sets A and B is a measure of the amount of common multiplicative structure between A and B.

$$E(A, B) = \Big| \big\{ (a_1, a_2, b_1, b_2) \in A \times A \times B \times B : a_1 b_1 = a_2 b_2 \big\} \Big|.$$

Similarly, we can define the multiplicative energy of multiple sets.

---

[1] 2000 *Mathematics Subject Classification.* Primary 11L40, 11L26; Secondary 11A07, 11B75.
[2] *Key words.* character sums, quadratic residues, Burgess
[3] Research partially financed by the National Science Foundation.

Friedlander and Iwaniec ([FI]) have an optimal bound on the multiplicative energy of two intervals.

Lemma 1.4. (Friedlander-Iwaniec) *If I, J are intervals with $|I|\,|J| < p$, then*

$$E(I,J) < c \log p\, |I|\,|J|.$$

The next estimate of the complete character sum of a polynomial is from the well-known Weil's bound on exponential sums. (See Theorem 11.23 in [IK]).

Theorem 1.5 (Weil) *Let χ be a non-principal multiplicative character of $\mathbb{F}_{p^n}$ of order $d > 1$. Suppose $f \in \mathbb{F}_{p^n}[x]$ has m distinct roots and f is not a d-th power. Then for $n \geq 1$ we have*

$$\sum_{x\in\mathbb{F}_{p^n}} \chi((f(x)) \leq (m-1)p^{\frac{n}{2}}.$$

Sketch of Burgess' Proof.

It suffices to give the proof for intervals of length $p^{\frac14+\varepsilon}$.

Let $I \subset [1,p)$ be an interval of length $|I| = [p^{\frac14+\varepsilon}]$, and let $J = [1, p^{\frac14}]$ and $T = [1, p^{\frac{\varepsilon}{2}}]$. For $y \in J$ and $t \in T$, we have

$$\Big|\sum_{x\in I}\chi(x) - \sum_{x\in I}\chi(x+yt)\Big| < \Big|I \setminus (I+yt)\Big| + \Big|(I+yt)\setminus I\Big| < 2p^{\frac14+\frac{\varepsilon}{2}}.$$

Hence,

$$\sum_{x\in I}\chi(x) = p^{-\frac14-\frac{\varepsilon}{2}} \sum_{\substack{x\in I, y\in J\\ t\in T}} \chi(x+yt) + O(p^{-\frac{\varepsilon}{2}}|I|).$$

Next, we estimate

$$\Big|\sum_{\substack{x\in I, y\in J\\ t\in T}} \chi(x+yt)\Big| \leq \sum_{x\in I, y\in J}\Big|\sum_{t\in T}\chi(xy^{-1}+t)\Big| = \sum_{u\in\mathbb{F}_p^*}\eta(u)\Big|\sum_{t\in T}\chi(u+t)\Big|,$$

where

$$\eta(u) = \Big|\{(x,y) : x\in I, y\in J,\ \ xy^{-1} = u \pmod p\}\Big|.$$

Next, apply Hölder's inequality with a suitably chosen large power $2r$.

$$\sum_{u\in\mathbb{F}_p^*}\eta(u)\Big|\sum_{t\in T}\chi(u+t)\Big| \leq \underbrace{\Big[\sum_u \eta(u)^{\frac{2r}{2r-1}}\Big]^{1-\frac{1}{2r}}}_{(A)} \underbrace{\Big[\sum_u \Big|\sum_{t\in T}\chi(u+t)\Big|^{2r}\Big]^{\frac{1}{2r}}}_{(B)}.$$

To estimate (A), we will use Lemma 1.4.

Since $1 < \frac{2r}{2r-1} < 2$, Hölder's inequality implies that

$$\begin{aligned}(A) &\leq \Big(\sum \eta(u)\Big)^{1-\frac1r}\ \Big(\sum \eta(u)^2\Big)^{\frac{1}{2r}}\\ &= (|I|\,|J|)^{1-\frac1r}\ E(I,J)^{\frac{1}{2r}}\\ &< \log p\ (|I|\,|J|)^{1-\frac{1}{2r}}.\end{aligned}$$

(The equality follows from the definitions of $\eta(u)$ and the multiplicative energy.)

Now we estimate (B)

$$(B) \le \Big\{ \sum_{t_1,\dots,t_{2r}\in T} \Big| \sum_{u\in\mathbb{F}_p} \chi\Big(\frac{(u+t_1)\cdots(u+t_r)}{(u+t_{r+1})\cdots(u+t_{2r})}\Big)\Big|\Big\}^{\frac{1}{2r}},$$

which by Weil's inequality, is bounded by

$$\Big\{ r^{2r}|T|^r p + |T|^{2r}(2r-1)p^{\frac12}\Big\}^{\frac{1}{2r}} < C_r\Big(|T|^{\frac12}p^{\frac{1}{2r}} + |T|p^{\frac{1}{4r}}\Big).$$

Therefore, up to an error of $O(p^{-\frac{\varepsilon}{2}}|I|)$, taking $r \sim \frac{1}{\varepsilon}$, our character sum is bounded by

$$\begin{aligned}\sum_{x\in I}\chi(x) \le& C_r \log p\, p^{-\frac14-\frac{\varepsilon}{2}}p^{(\frac12+\varepsilon)(1-\frac{1}{2r})}\Big[p^{\frac{\varepsilon}{4}+\frac{1}{2r}} + p^{\frac{\varepsilon}{2}+\frac{1}{4r}}\Big]\\ <& C_r\log p\, |I|\Big(p^{\frac{1}{4r}-\frac{\varepsilon}{4}-\frac{\varepsilon}{2r}} + p^{-\frac{\varepsilon}{2r}}\Big) \ll p^{-\frac{\varepsilon^2}{3}}|I|.\end{aligned}$$

§2. Extensions of Burgess method to a general finite field $\mathbb{F}_{p^n}$.

Let $\omega_1,\dots,\omega_n$ be an arbitrary basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Then for any $x\in\mathbb{F}_{p^n}$, there is a unique representation of x in terms of the basis.

$$x = x_1\omega_1 + \cdots + x_n\omega_n.$$

A *box* $B\subset\mathbb{F}_{p^n}$ is a set such that for each j, the coefficients x_j form an interval.

$$B = \Big\{\sum_{j=1}^n x_j\omega_j : x_j\in[N_j, N_j+H_j], \quad \forall j\Big\}. \tag{2.0}$$

Burgess, Friedlander, Karacuba, and Davenport-Lewis all contributed non-trivial estimates of the character sum

$$\sum_{x\in B}\chi(x).$$

Here by *non-trivial* we mean smaller than the trivial bound by a factor of q^ϵ for some $\epsilon>0$.

Let us recall their results.

The first theorem is about boxes defined by special bases. It was done by Burgess [Bu3] for $n=2$, and Karacuba [Kar2] for general n.

Theorem 2.1 (Burgess, Karacuba) *Let χ be a non-principal multiplicative character of $\mathbb{F}_{p^n}$, and let $\omega_1,\omega_2,\dots,\omega_n$ be a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ satisfying the condition that*

$$\omega_i\omega_j = \sum_{1\le r\le n} d_{ijr}\omega_r \qquad \text{with } |d_{ijr}| < C. \tag{2.1}$$

For a box B as defined in (2.0) by the basis $\omega_1,\omega_2,\dots,\omega_n$ with

$$H_j > p^{\frac14+\varepsilon}, \quad \forall j, \quad \text{for some } \varepsilon > 0, \tag{2.2}$$

we have

$$\Big|\sum_{x\in B}\chi(x)\Big| < p^{-\delta}|B|.$$

Remark 2.1.1. Let θ be an algebraic integer such that its minimal polynomial $\mathrm{irr}_{\mathbb{Z}}(\theta)$ is irreducible modulo p. The basis $\omega_1 = 1, \omega_2 = \theta, \ldots, \omega_n = \theta^{n-1}$ satisfies condition (2.1). Hence Theorem 2.1 applies.

For general bases, there is also the weaker result by Davenport and Lewis.

Theorem 2.2. (Davenport-Lewis [DL]) *Let χ be a non-principal multiplicative character of $\mathbb{F}_{p^n}$, and let $\omega_1, \ldots, \omega_n$ be an arbitrary basis, and let the box B be as defined in (2.0) with*

$$H_j = H > p^{\frac{n}{2(n+1)}+\varepsilon}, \quad \forall j.$$

Then for $p > p(\varepsilon)$, we have

$$\Big|\sum_{x\in B} \chi(x)\Big| < (p^{-\varepsilon_1} H)^n, \quad \textit{for some } \varepsilon_1(\varepsilon) > 0.$$

Remark 2.2.1. For $n = 1$, this is Burgess' result, but it becomes weaker for $n > 1$ and $\frac{n}{2(n+1)} \to \frac{1}{2}$ for n large.

In Karacuba's argument, the problem of estimating $E(B, B)$, B the given box in $\mathbb{F}_{p^n}$, is reduced to counting divisor in $\mathbb{Q}(\theta)$.

In Davenport-Lewis' argument, the amplification uses only an $\mathbb{F}_p$-parameter and this explains why their result is weaker. They raise the question of how to exploit a $\mathbb{F}_{p^n}$-parameter when the basis $\{\omega_1, \ldots, \omega_n\}$ is arbitrary.

For $n = 2$, we are able to have an estimate of Burgess' strength. (See Theorem 5 in [C2].)

Theorem 2.3. *Let Let χ be a non-principal multiplicative character of $\mathbb{F}_{p^2} = \mathbb{F}_p(\omega)$ and let B be a box*

$$B = \Big\{x_1 + x_2\omega : x_j \in [N_j, N_j + H], \quad \forall j\Big\},$$

where

$$H > p^{\frac{1}{4}+\varepsilon}.$$

Then

$$\Big|\sum_{x\in B} \chi(x)\Big| < p^{-\delta}|B|$$

with $\delta = \delta(\varepsilon)$ independent of ω.

As for the most essential ingredient of the proof, multiplicative energy, we have an optimal bound. (See Lemma 2' in [C2].)

Lemma 2.4. *Let $\omega \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$,*

$$B = \Big\{x + \omega y : x, y \in \Big[1, \frac{1}{10}p^{1/4}\Big]\Big\}.$$

Take $z_1, z_2 \in \mathbb{F}_{p^2}$ and $e_p = \exp\left(c\frac{\log p}{\log\log p}\right)$. Then

$$E(z_1 + B, z_2 + B) < e_p\, |B|^2,$$

where $z_i + B = \{z_i + b : b \in B\}$.

The proof of Lemma 2.4 uses the following estimate on divisor functions on a box.

Lemma 2.5. *Let B be a box defined as in the lemma above. Then*

$$\max_{\xi \in \mathbb{F}_{p^2}} \Big| \{(z_1, z_2) \in B \times B : \xi = z_1 z_2\} \Big| < \exp\Big(c \frac{\log p}{\log\log p}\Big).$$

To prove Lemma 2.5 we use the uniform bounds on divisor functions in algebraic number fields $\mathbb{Q}(\omega)$ of bounded degree.

As for general n, here is our improvement of Davenport and Lewis' result. (See Theorem 2 in [C1].)

Theorem 2.6. *Let B be a box as defined in (2.0) with $\omega_1, \dots, \omega_n$ being an arbitrary basis and*

$$\prod_{j=1}^{n} H_j > p^{(\frac{2}{5}+\varepsilon)n}$$

for some $\varepsilon > 0$.

Let $p > p(\varepsilon)$ and χ be a nontrivial multiplicative character of $\mathbb{F}_{p^n}$. Then

$$\Big| \sum_{x \in B} \chi(x) \Big| \ll n p^{-\frac{\varepsilon^2}{4}} |B|,$$

unless n is even and $\chi|_{F_2}$ is principal, F_2 = subfield of size $p^{n/2}$, in which case

$$\Big| \sum_{x \in B} \chi(x) \Big| \leq \max_{\xi} |B \cap \xi F_2| + O_n(p^{-\frac{\varepsilon^2}{4}} |B|).$$

As an application, we can estimate as follows the number of primitive roots of $\mathbb{F}_{p^n}$ in boxes. (See [DL], p131.)

Corollary 2.7 *Let $B \subset \mathbb{F}_{p^n}$ be as in Theorem 2.6 and satisfying $\max_\xi \big|B \cap \xi F_2\big| < p^{-\varepsilon}|B|$ if n even. Then the number of primitive roots of $\mathbb{F}_{p^n}$ belonging to B is*

$$\frac{\varphi(p^n - 1)}{p^n - 1} |B| (1 + o(p^{-\tau'})),$$

where $\tau' = \tau'(\varepsilon) > 0$ and assuming $n \ll \log\log p$.

The proof follows from the formula

$$\frac{\varphi(p^n-1)}{p^n-1} \left\{ 1 + \sum_{\substack{d | p^n - 1 \\ d > 1}} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}(\chi) = d} \chi(x) \right\} = \begin{cases} 1 & \text{if } x \text{ is primitive} \\ 0 & \text{otherwise.} \end{cases}$$

Recently, Konyagin [K] generalized Burgess' result to $n \geq 2$.

Theorem 2.8. (Konyagin) *Let χ be a nontrivial multiplicative character of $\mathbb{F}_{p^n}$ and $\varepsilon \in (0, 1/4]$ be given. If $n \geq 2$, $\{\omega_1, \dots, \omega_n\}$ is an arbitrary basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$,*

$$B = \{\sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j + 1, N_j + H_j] \cap \mathbb{Z}\}$$

is a box satisfying $H_j \geq p^{1/4+\varepsilon}$ $(j = 1, \dots, n)$, then we have

$$|\sum_{x \in B} \chi(x)| \ll_n p^{-\varepsilon^2/2} |B|,$$

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

Remark 2.8.1. Konyagin's proof is based on geometry of numbers and Minkowski's inequalities for successive minima.

Remark 2.8.2. At this point, Konyagin's argument requires each $H_j > p^{1/4+\epsilon}$, while Theorem 2.6 assumes only a condition on $\prod H_j$. Also, in Theorem 2.6, the dependence on n is better due to the fact that the multiplicative energy bound (Lemma 2.10 below) only involves a factor C^n.

The proof of Theorem 2.6 is divided into two cases, depending on whether $\max_j H_j < p^{\frac{1}{2}+\frac{\varepsilon}{10}}$.

If $H_j > p^{\frac{1}{2}+\frac{\varepsilon}{10}}$ for some $1 \leq j \leq n$, we use the following theorem by Perelmuter-Shparlinski [PS].

Theorem 2.9. (Perelmuter-Shparlinski) *Let χ be a non-principal multiplicative character of $\mathbb{F}_q$ and let $g \in \mathbb{F}_q$ be a generating element, i.e. $\mathbb{F}_q = \mathbb{F}_p(g)$. For any integral interval $I \subset [1, p]$,*

$$\Big|\sum_{t \in I} \chi(g + t)\Big| \leq c(n)\sqrt{p}\ \log p.$$

If $\max_j H_j < p^{\frac{1}{2}+\frac{\varepsilon}{10}}$, we apply Burgess' method. The bounding of the multiplicative energy is a variant of Garaev's argument ([G]) with later refinement due to Katz-Shen ([KS1], [KS2]) to obtain an explicit sum-product theorem in $\mathbb{F}_p$.

Lemma 2.10. *Let $\omega_1, \dots, \omega_n$ be an arbitrary basis, and let the box B be as defined in (2.0). Assume*

$$\max_j H_j < \frac{1}{2}(\sqrt{p} - 1).$$

Then

$$E(B, B) < C^n (\log p) |B|^{\frac{11}{4}}.$$

Remark 2.10.1. The lemma saves $\frac{1}{4}$ over the trivial bound $|B|^3$.

§3. Character sums with polynomial argument.

It follows from Weil's inequality that if χ is a multiplicative character modulo p of order d, and $f(x)$ is a polynomial that is not a d-th power modulo p, then

$$\Big|\sum_{x=N}^{N+H}\chi\big(f(x)\big)\Big| < Cp^{\frac{1}{2}}\log p,$$

where C depends on the degree of f. However, no analogue of Burgess' inequality is known. There is the following weaker variant by Burgess. [Bu5]

Theorem 3.1. (Burgess) *Let $f(x)$ be a non-linear polynomial that is a product of rational linear factors and not a perfect d-th power. Let $p \equiv 1 \mod d$ and χ a d-th order character mod p. Then if*

$$p^{\frac{1}{4}+\varepsilon} < H < p^{\frac{1}{2}},$$

we have

$$\Big|\sum_{N<x\le N+H}\chi\big(f(x)\big)\Big| < H - cH^2p^{-\frac{1}{2}},$$

where c depends on ε, d and f.

Corollary 3.2. *Let f, χ, and p be as in Theorem 3.1. Then there are $x_1, x_2 \in [N, N+H]$ such that*

$$f(x_i) \neq 0 \mod p, \quad \text{and } \chi\big(f(x_1)\big) \neq \chi\big(f(x_2)\big).$$

As for character sums over binary quadratic forms, Burgess has the following non-trivial uniform estimate. [Bu4]

Theorem 3.3. (Burgess) *Let χ be a nontrivial multiplicative character mod p. Suppose $x^2+axy+by^2 \in \mathbb{F}_p[x,y]$ is not a perfect square, and $I, J \subset [1, p-1]$ are intervals. If*

$$|I|, |J| > p^{\frac{1}{3}+\varepsilon}, \tag{3.1}$$

then

$$\Big|\sum_{x\in I, y\in J}\chi(x^2+axy+by^2)\Big| < p^{-\delta}|I||J|,$$

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

In the next theorem we improve Burgess' result from $\frac{1}{3}$ to $\frac{1}{4}$.

Theorem 3.4. *Under the assumption as in the theorem above, if $|I|, |J| > p^{\frac{1}{4}+\varepsilon}$, then there is a non-trivial bound.*

The proof has two cases.

Case 1. $x^2+axy+by^2$ is irreducible mod p. Let $\omega = \frac{1}{2}(-a+\sqrt{a^2-4b})$. Then $\omega \in \mathbb{F}_{p^2}\setminus\mathbb{F}_p$. Take B to be the box

$$B = \{x+\omega y : x \in I, y \in J\} \subset \mathbb{F}_{p^2}.$$

Now the theorem follows from the estimate in $\mathbb{F}_{p^2}$ on sum of the character χ_1

$$\sum_{x\in I, y\in J}\chi_1(x+\omega y) = \sum_{z\in B}\chi_1(z).$$

Case 2. $x^2+axy+by^2 = (x-\lambda_1 y)(x-\lambda_2 y)$ with $\lambda_1 \neq \lambda_2$ in $\mathbb{F}_p$. The argument is similar to Case 1 by replacing $\mathbb{F}_{p^2}$ with $\mathbb{F}_p \times \mathbb{F}_p$.

Assuming p large enough, there are applications of character sums to quadratic non-residues in sets with more structure. For example, we take a fixed nonzero integer k and let

$$f(x) = x^2 + k.$$

If $k = -r^2, r \in \mathbb{Z}$, then Corollary 1.3 implies that for some $j < p^{\frac{1}{4\sqrt{e}}+\varepsilon}$, jr and $(j+2)r$ do not have the same quadratic residuacity and $f(x)$ is quadratic non-residue mod p for some $x < p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.

In general, Burgess [Bu2] proved the following theorem.

Theorem 3.5. (Burgess)

$$\left(\frac{x^2+k}{p}\right) = -1$$

for some

$$x = O\big(p^{\frac{2}{3\sqrt{e}}+\varepsilon}\big).$$

We have the following improvement. $\big($[F],[C3]$\big)$

Theorem 3.6.

$$\left(\frac{x^2+k}{p}\right) = -1$$

for some

$$x = O\big(p^{\frac{1}{2\sqrt{e}}+\varepsilon}\big).$$

The argument has the same approach as Burgess', starting with

Lemma 3.7. (Burgess) *Let*

$$n = x^2 + ky^2.$$

Then there is a representation

$$n = u^2 \prod_{1\le i\le r} (v_i^2 + k)^{\alpha_i},$$

where $r, u, v_1, \dots, v_r \in \mathbb{Z}_+$*;* $u, v_1, \dots, v_r \le n$ *and* $\alpha_i = \pm 1$.

This reduces the problem to character estimates of binary forms.

Remark 3.8. One may be more specific about the role of k in Theorem 3.6. In view of Lemma 3.7, we gets $x \ll k^{1/\sqrt{e}} p^{1/2\sqrt{e}+\epsilon}$. See Problems 8 and 9.

§4. Other related character sums.

Definition 4.1. Let $q = p^n$ be a prime power such that $q \equiv 1 \bmod 4$. The undirected *Paley Graph of order* q, $G = (V, E)$ is defined by

$$V = \mathbb{F}_q$$

and

$$E = \big\{\{a, b\} \in \mathbb{F}_q \times \mathbb{F}_q : a - b \text{ is a square in } \mathbb{F}_q^*\big\}.$$

Problem 4.2. *What is the size of the largest clique in* G*?*

The problem asks for the size of the largest subset $S \subset \mathbb{F}_q$ such that for any $a, b \in S$, $a - b$ is a square. A. Blokhuis [Bl] proved that if $q = p^{2n}$ and $p \neq 2$, then the clique number is p^n. For $q = p$ prime, it is conjectured that the clique number is $\sim \log p$. A relevant character sum problem is the following.

Problem 4.3. *Let χ be the quadratic character mod p (or any non-trivial character). Prove that for some $\gamma = \gamma(\delta) > 0$*

$$\Big|\sum_{x\in A, y\in B} \chi(x+y)\Big| < p^{-\gamma}|A|\,|B|$$

holds, for arbitrary subsets $A, B \subset \mathbb{F}_p$ of size

$$|A| > p^{\delta}, |B| > p^{\delta}$$

and p large enough.

Karacuba has the following relevant results [Kar3].

Theorem 4.4. (Karacuba) *Let χ be a non-trivial multiplicative character mod p. If $|A| > p^{\frac{1}{2}+\delta}, |B| > p^{\delta}$, then*

$$\Big|\sum_{x\in A, y\in B} \chi(x+y)\Big| \ll p^{-0.05\delta^2}|A|\,|B|.$$

Remark. It is unknown if there is non-trivial bound on the character sum $\sum_{x\in A, y\in B} \chi(x+y)$ for $|A| = |B| \sim p^{\frac{1}{2}}$, not even for the special case when $A = B = H < \mathbb{F}_p^*$.

Considering special sets, Karacuba [Kar1] also proved

Theorem 4.5. (Karacuba) *Let χ be a non-trivial multiplicative character mod p, $I \subset [1, p)$ be an interval and $S \subset [1, p)$ an arbitrary set, such that*

$$|I|, |S| > p^{\frac{1}{3}+\varepsilon}.$$

Then

$$\sum_{y\in I}\Big|\sum_{x\in S} \chi(x+y)\Big| < p^{-\delta}|I|\,|S|$$

Remark 4.5.1. Related results were obtained by Friedlander and Iwaniec [FI] but under more restrictive assumptions on S that it is well-spaced.

We have the following slight improvement [C1].

Theorem 4.6. *Theorem 4.5 holds under the hypothesis that*

$$|I|, |S| > p^{\frac{7}{22}+\varepsilon}.$$

The proof uses the following estimate on multiplicative energy.

Proposition 4.7. *Take $k \in \mathbb{Z}, k \geq 2$ and $I = [0, p^{\frac{1}{k}}]$ an interval. Let $\mathcal{D} \subset \mathbb{F}_p$ be a $p^{\frac{1}{k}}$-separated set and $A = \mathcal{D} + I = \{d + i : d \in \mathcal{D}, i \in I\}$. Then*

$$E(A, I) < p^{\frac{4}{\log\log p}}|\mathcal{D}|^{\frac{1}{k-1}}\,|I|\,|A|.$$

There are more bounds on character sum over sets with more structures.

Theorem 4.8. (Karacuba) [Kar3] [Kar4] *Let* $\tau_k(n)$ *be the number of solutions of the equation* $n = n_1 \dots n_k$ *with* $n_i \in \mathbb{Z}_+$, $n_i \geq 2$, *and let*

$$T_N = \sum_{n \leq N} \tau_k(n)\ \chi(a+n), \qquad (a,p) = 1.$$

(*i*) *If* $N > p^{\frac{1}{2}+\varepsilon}$, *then* $|T_N| < N^{1-\delta}$.

(*ii*) *If* $0 < |a| \leq \sqrt{p}$, *and*

$$N > p^{\frac{1}{2} - \frac{1}{2(k+1)} + \varepsilon},$$

then

$$|T_N| < N^{1-\delta}.$$

The following is our result of type (ii) without restriction on a.

Theorem 4.9. *Let* T_N *be defined as in Theorem 4.8. Assume*

$$N > p^{\ \rho_k + \varepsilon}$$

with $\rho_k = \frac{3}{8} + \frac{k}{4} - \frac{1}{4}\sqrt{k^2 - k + \frac{9}{4}}$. *Then*

$$|T_N| < N^{1-\delta} \text{ for some } \delta = \delta(k, \varepsilon) > 0.$$

Theorem 4.9 follows from the following result in [C1].

Theorem 4.10. *Let* $I \subset \mathbb{F}_p$ *be an interval with* $|I| = p^\beta$ *and let* $\mathcal{D} \subset \mathbb{F}_p$ *be a* p^β*-spaced set with* $|\mathcal{D}| = p^\sigma$. *Assume*

$$2\beta + \sigma - \frac{\beta\sigma}{1-\beta} > \frac{1}{2} + \delta$$

for some $\delta > 0$. *Then*

$$\Big| \sum_{x \in I, y \in \mathcal{D}} \chi(x+y) \Big| < p^{-\frac{\delta^2}{12}}\ |I|\ |\mathcal{D}|$$

for a non-principal multiplicative character χ.

Corollary 4.11. *Let* $a \in \mathbb{Z}$ *be arbitrary such that* $(a,p) = 1$ *and let*

$$R_1 = \sum_{x^2+y^2 \leq N} \chi(x^2 + y^2 + a).$$

Assume

$$N > p^{\ \rho_2 + \varepsilon}, \quad \rho_2 = \frac{1}{8}(7 - \sqrt{17}) = 0.359...$$

Then

$$|R_1| < N^{1-\delta}.$$

§5. Character sums over subspaces.

Theorem 5.1. *Let $q = p^n$, and let V be a subspace of $\mathbb{F}_q$ over $\mathbb{F}_p$. Assume*

(1). *$dim V \geq \rho n$, where $\rho < \frac{1}{2}$ is a constant.*

(2). *$\max_{\xi \in \mathbb{F}_q^*} |V \cap \xi G| < |V|^{1-\epsilon}$, when n is even. Here G is the subfield of $\mathbb{F}_q$ with $|G| = \sqrt{q}$.*

(3). *$n < p\,(\log p)^{-4}$, where C is a sufficiently large constant.*

Then

$$\Big|\sum_{x\in V} \chi(x)\Big| < \big(\log p\big)^{-\delta}\,|V|$$

for some $\delta > 0$. In particular, V contains a quadratic non residue.

Lemma 5.2. *Let $q = p^n$, and let V be a subspace of $\mathbb{F}_q$ over $\mathbb{F}_p$ satisfying*

$$\max_{G} \max_{\xi \in \mathbb{F}_q^*} |V \cap \xi G| < |V|^{1-\epsilon}, \tag{5.1}$$

where $G < \mathbb{F}_q$ is a proper subfield. Then the multiplicative energy of V is bounded by

$$E(V, V) < c|V|^{3-\delta}, \tag{5.2}$$

where c, δ are absolute constants.

Proof. By the Balog-Szemerédi-Gowers Lemma and Theorem 4.3 in [BKT]. □

Let χ be a non-trivial multiplicative character of $\mathbb{F}_q$. Our goal is to estimate

$$\big|\sum_{x\in V} \chi(x)\big|. \tag{5.3}$$

Thus

$$\big|\sum_{x\in V} \chi(x)\big| = \frac{1}{p\,|V^*|}\Big|\sum_{\substack{x,\in V,\ y\in V^* \\ t\in\mathbb{F}_p}} \chi(x+yt)\Big| = \frac{1}{p\,|V^*|}\sum \eta(u)\Big|\sum_{t\in\mathbb{F}_p} \chi(u+t)\Big|, \tag{5.4}$$

where

$$\eta(u) = \big|\{(x,y) \in V \times V :\ xy^{-1} = u\big|.$$

It follows from the lemma and the definition of $\eta(u)$ that

$$\sum_u \eta(u)^2 = E(V,V) \leq |V|^{3-\delta}. \tag{5.5}$$

Applying Hölder's inequality twice, we have

$$\begin{aligned} &\big|\sum_{x\in V} \chi(x)\big| \\ \leq&\frac{1}{|V|p}\underbrace{\Big[\sum\ \eta(u)\Big]^{1-\frac{1}{r}}\ \Big[\sum\ \eta(u)^2\Big]^{\frac{1}{2r}}}_{A}\underbrace{\Big[\sum_{u\in\mathbb{F}_q}\ \Big|\sum_{t\in\mathbb{F}_p} \chi(u+t)\Big|^{2r}\Big]^{\frac{1}{2r}}}_{B}. \end{aligned}$$

By (5.5),

$$A \leq |V|^{2(1-\frac{1}{r})}|V|^{\frac{3-\delta}{2r}}. \tag{5.6}$$

For expression B, we write

$$\sum_{u\in\mathbb{F}_q} \Big|\sum_{t\in\mathbb{F}_p}\chi(u+t)\Big|^{2r}$$

$$\leq \sum_{t_1,\dots,t_{2r}\in\mathbb{F}_p} \Big|\sum_{u\in\mathbb{F}_q}\chi\Big(\frac{(u+t_1)\cdots(u+t_r)}{(u+t_{r+1})\cdots(u+t_{2r})}\Big)\Big|. \tag{5.7}$$

Case 1. One of the t_i is not repeated. By Weil's inequality, the contribution in (5.7) is bounded by

$$2rp^{2r}\sqrt{q}.$$

Case 2. Each t_i appears at least twice. We estimate the number of such $2r$-tuples $(t_1,\dots,t_{2r})$ as follows. By assumption, there exist $I\subset\{1,\dots,2r\}$, $|I|\leq r$, and a system $(t_i)_{i\in I}\in\mathbb{F}_p^I$ such that $t_j\in\{t_i : i\in I\}$. The corresponding count gives

$$\sum_{s\leq r}\binom{2r}{s}p^s s^{2r-s}\leq r^{2r}\Big[\sum_{s\leq r}\binom{2r}{s}\Big]\Big[\max_{s\leq r}\Big(\frac{p}{s}\Big)^s\Big]$$

$$\leq r^{2r}4^r\Big(\frac{p}{r}\Big)^r=(4rp)^r,$$

assuming

$$p>er. \tag{5.8}$$

Thus in Case 2, the contribution to (5.7) is at most

$$(4rp)^r\cdot q.$$

Hence

$$(B)<(2r)^{\frac{1}{2r}}p\, q^{\frac{1}{4r}}+(4rp)^{\frac12}\ q^{\frac{1}{2r}}. \tag{5.9}$$

From (5.6) and (5.9),

$$\Big|\sum_{x\in V}\chi(x)\Big|\leq\frac{1}{|V|\,p}|V|^{\,2(1-\frac1r)}|V|^{\frac{3-\delta}{2r}}\Big(p\,q^{\frac{1}{4r}}+2r^{\frac12}\ p^{\frac12}\ q^{\frac{1}{2r}}\Big)$$

$$=|V|\Big\{q^{\frac{1}{4r}}|V|^{-\frac{1+\delta}{2r}}+2\Big(\frac{r}{p}\Big)^{\frac12}|V|^{-\frac{1+\delta}{2r}}q^{\frac{1}{2r}}\Big\}. \tag{5.10}$$

Assume

$$\dim V>\Big(1-\frac{\delta}{4}\Big)\frac{n}{2}. \tag{5.11}$$

Thus $|V|>q^{\frac12\,(1-\frac{\delta}{4})}$ and from (5.10)

$$\Big|\sum_{x\in V}\chi(x)\Big|<\Big[p^{-\frac{n\delta}{8r}}+2\Big(\frac{r}{p}\Big)^{\frac12}p^{\frac{n}{4r}}\Big]\ |V|. \tag{5.12}$$

It remains to choose r optimally.

Take

$$r=n\ \frac{\log p}{\log\frac{p}{n}}.$$

Assume

$$n<\frac{p}{(\log p)^4} \tag{5.13}$$

and p large so that (5.8) holds in particular.

The first factor in (5.12) becomes

$$\Big(\frac{n}{p}\Big)^{\frac{\delta}{8}} + \Big(\frac{\log p}{\log \frac{p}{n}}\Big)^{\frac{1}{2}} \Big(\frac{n}{p}\Big)^{\frac{1}{4}} \lesssim \Big(\frac{n}{p}\Big)^{\frac{\delta}{4}} < \Big(\log p\Big)^{-\delta}$$

for $\delta \leq \frac{1}{2}$.

Thus we obtain that

$$\Big|\sum_{x\in V} \chi(x)\Big| < \big(\log p\big)^{-\delta} \, |V|$$

provided (5.11) and (5.13) hold.

§6. Problems.

Let $\mathbb{F}_{p^n}$ be a finite field and let θ be a generator of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Denote M the module over $\mathbb{F}_p$ generated by $1, \theta, \dots, \theta^{m-1}$.

Problem 1. *Estimate $S_m = \sum_{y\in M} \chi(y)$ nontrivially.*

By the bound of Katz [Ka] that $\Big|\sum_{t\in\mathbb{F}_p} \chi(\theta+t)\Big| \leq (n-1)\sqrt{p}$ implies

$$|S_m| < np^{m-\frac{1}{2}}.$$

However, their bound becomes trivial for $n > \sqrt{p}$. On the other hand, Burgess [Bu6] showed

$$S_m = O(p^{m(1-\delta)})$$

for $m > n(\frac{1}{4}+\epsilon)$, where $\delta = \delta(\epsilon)$.

One may hope to obtain an estimate S_m under weaker conditions on m.

To generalize Problem 1, we let $V < \mathbb{F}_{p^n}$ be an arbitrary m-dimensional subspace of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$.

Problem 2. *Obtain new estimate on $\sum_{y\in V} \chi(y)$.*

Theorem 5.1 is what we are able to prove.

Note that the Davenport-Lewis technique gives nothing here as one can not amplify by multiplication with the base field F_p. Also note that Perelmuter-Shparlinski' result requires $n > C\sqrt{p}\ \log p$.

As for character sums over sum sets, we have the following problems.

Problem 3. *Obtain a nontrivial estimate on*

$$\sum_{x\in A, y\in B} \chi(x+y)$$

for $A, B \subset \mathbb{F}_p$ arbitrary, and $|A|, |B| \sim \sqrt{p}$.

Problem 4. (Sarnak) *In Problem (3), consider $A = B = H < \mathbb{F}_p^*$ with $|H| \sim \sqrt{p}$.*

Problem 5. (Bourgain) *Obtain nontrivial bound on*

$$\sum_{x\in H} \chi(a+x)$$

for $H < \mathbb{F}_p^*$, $|H| \sim \sqrt{p}$, *and* $a \in \mathbb{F}_p^*$.

Consider the following sums

$$S_1 = \sum_{x\in I} \Big| \sum_{y\in A} \chi(x+y) \Big|$$

$$S_2 = \sum_{x\in I} \Big| \sum_{y\in A} \chi(1+xy) \Big|,$$

where I is the interval $[0, p^\alpha]$ and $A \subset [0, p^\beta]$ arbitrary with $|A| \sim p^\beta$.

If $\alpha + \beta > \frac{1}{2} + \epsilon$, one may obtain

$$|S_1|, |S_2| < p^{-\delta(\epsilon)} |I|\, |A|.$$

Problem 6. *Obtain estimate of* $|S_1|$ *and* $|S_2|$ *for* $\alpha + \beta = \frac{1}{2}$, $\alpha, \beta > \epsilon$.

An estimate for sums of the type S_2 is relevant to the following problem due to Vinogradov and Karacuba on the "shifted primes".

Problem 7. (Vinogradov) *Obtain nontrivial bounds on*

$$\sum_{q<N,\ q\ prime} \chi(a+q),$$

where $a \neq 0$ *is given,* $N \sim \sqrt{p}$.

A bound $Np^{-\delta}$ was obtained by Karacuba for $N > p^{\frac{1}{2}+\epsilon}$.

Problem 8. *Obtain nontrivial bound (uniform in a) for*

$$\sum_{x\in I} \chi(x^2 + a),$$

where $|I| \sim \sqrt{p}$.

Problem 9. *Prove that*

$$\min\{x \in [1,p] : a + x^2 \text{ is a quadratic nonresidue } \} < \sqrt{p}$$

for p large enough and $a \in \mathbb{F}_p^*$ *arbitrary (uniform in a).*

We note that Theorem 3.6 gives the bound $p^{\frac{1}{2\sqrt{e}}+\epsilon}$ with $a \neq 0$ given.

Problem 10. (Shparlinski) *Prove that*

$$\min\{x \in [1,p] : (x+a)(x+b) \text{ is a quadratic nonresidue } \} < p^{1/2-\eta}$$

for some fixed η *and uniformly over* $a \neq b$.

Acknowledgement. The author would also like to thank I. Shparlinski for many helpful comments, and the organizers for the opportunity to present this talk in F_q9.

References

[Bl] A. Blokhuis, *On subsets of GF(q2) with square differences*, Nederl. Akad. Wetensch. Indag. Math. 46 (1984), pp. 369372.

[BKT] J. Bourgain, N. Katz, T. Tao *A sum-product estimate in finite fields and their applications*, GAFA 14 (2004), n1, 27–57.

[Bu1] D.A. Burgess, *On character sums and primitive roots*, Proc LMS (3), 12, (1962), 179-192.

[Bu2] ______, *On the quadratic character of a polynomial*, JLMS, 42, (1967), 73-80.

[Bu3] ______, *Character sums and primitive roots in finite fields*, Proc. London Math. Soc (3) 37 (1967), 11-35.

[Bu4] ______, *A note on character sums of binary quadratic forms*, JLMS, 43 (1968), 271-274.

[Bu5] ______, *On Dirichlet characters of polynomials*, Proc. London Math. Soc. 13 (1963) 537-548.

[Bu6] ______, *A note on character sums over finite fields*, J. Reine Angew. Math. 255 (1972), 80-82.

[C1] M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*, Duke Math. J. 145 (2008), No. 3, 409–442.

[C2] ______, *Burgess inequality in* F_{p^2}, Geom. Funct. Anal (to appear).

[C3] ______, *On character sums of binary quadratic forms*, Journal of Number Theory, 129, No. 9 (2009), 2064-2071.

[DL] H. Davenport, D. Lewis, *Character sums and primitive roots in finite fields*, Rend. Circ. Matem. Palermo-Serie II-Tomo XII-Anno (1963), 129-136 .

[F] J. Friedlander, *On characters and polynomials*, Acta Arith., XXV, (1973), 31-37.

[FI] J. Friedlander, H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. 119, No 2, (1993), 265-372.

[G] M. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$, IMRN No.11 (2007).

[IK] H. Iwaniec, E. Kowalski, *Analytic number theory*, AMS Colloquium Publications, Vol 53 (2004).

[Kar1] A.A. Karacuba, *Distribution of values of Dirichlet characters on additive sequences*, Soviet Math. Dokl. 44 (1992), no. 1, 145–148.

[Kar2] ______, *Estimates of character sums*, Math. USSR-Izvestija Vol. 4 (1970), No. 1, 19-29.

[Kar3] ______, *A certain arithmetic sum*, Soviet Math Dokl, 12 (1971), No. 4, 1172-1174.

[Kar4] ______, *Character sums with weights*, Izv. Math. 64 (2) (2000), 249-263.

[KS1] Nets Katz, C-Y. Shen *A slight improvement of Garaev's sum product estimate*, Proc. Amerc. Math. Soc., 136 (2008), 2499–2504.

[KS2] ______, *Garaev's inequality in finite fields not of prime order*, J. Anal. Combin., 3, (2008), Article #3.

[Ka] Nick Katz, *An estimate for character sums*, JAMS Vol 2, No 2 (1989), 197-200.

[K] S.V. Konyagin, *Estimates of character sums in finite fields* Matematicheskie Zametki" to appear, (in Russian).

[PS] G.I. Perel'muter, I. Shparlinski, *Distribution of primitive roots in finite fields* Russian Math. Surveys 45 (1990), no. 1, 223–224 .

Department Of Mathematics, University Of California, Riverside, CA 92521

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