ACTA ARITHMETICA
179.2 (2017)

Estimates for character sums with various convolutions

by

Brandon Hanson (University Park, PA)

1. Introduction. In analytic number theory, one is often concerned with estimating a bilinear sum of the form

$$S = \sum_{\substack{1\le m\le M\\ 1\le n\le N}} a_m b_n c_{m,n} \tag{1}$$

where a_m, b_n and $c_{m,n}$ are complex numbers. The standard way to handle this sum is to apply the Cauchy–Schwarz inequality so that

$$\begin{aligned}|S|^2 &\le \Big(\sum_{1\le m\le M} |a_m| \Big|\sum_{1\le n\le N} b_n c_{m,n}\Big|\Big)^2\\ &\le \Big(\sum_{1\le m\le M} |a_m|^2\Big)\Big(\sum_{1\le n_1,n_2\le N} b_{n_1}\overline{b_{n_2}} \sum_{1\le m\le M} c_{m,n_1}\overline{c_{m,n_2}}\Big).\end{aligned}$$

One usually knows that $\sum_{1\le m\le M} c_{m,n_1}\overline{c_{m,n_2}}$ is small when $n_1 \ne n_2$, so that the second factor is essentially dominated by the *diagonal terms* where $n_1 = n_2$.

For instance, suppose p is a prime number and denote by $\mathbb{F}_p$ the field with p elements. We write $e_p(u) = e^{2\pi i u/p}$ and we denote by χ a multiplicative (or Dirichlet) character modulo p. Two well-known sums of the form (1) are

$$S_\chi(A,B) = \sum_{a\in A}\sum_{b\in B} \chi(a+b), \tag{2}$$

$$T_x(A,B) = \sum_{a\in A}\sum_{b\in B} e_p(xab) \tag{3}$$

where A and B are subsets of $\mathbb{F}_p$.

By the triangle inequality, each of these sums is at most $|A|\,|B|$, but we expect an upper bound of the form $|A|\,|B|p^{-\varepsilon}$ for some positive ε. Indeed,

2010 *Mathematics Subject Classification*: Primary 11L40.
Key words and phrases: arithmetic combinatorics, sumsets, Sum-Product phenomenon.
Received 7 January 2016.
Published online 7 July 2017.

DOI: 10.4064/aa8404-5-2017

using the Cauchy–Schwarz inequality as above, and orthogonality of characters, one can prove that the sums (2) and (3) are at most $(p|A|\,|B|)^{1/2}$. Such an estimate is better than the trivial estimate when $|A|\,|B| > p$.

For the second sum, (3), the bound $(p|A|\,|B|)^{1/2}$ is quite sharp. Indeed, if $A = B = \{n : 1 \le n \le \delta p^{1/2}\}$ for a small number $\delta > 0$, then products ab with $a, b \in A$ are at most $\delta^2 p$ (here we are identifying residues modulo p with integers between 0 and $p-1$). It follows that $|e_p(ab) - 1| \ll \delta^2$, so the summands in (3) are essentially constant and there is little cancellation. On the other hand, it is conjectured that the first sum, (2), should exhibit cancellation even for small sets A and B. From now on, we will call (2) the *Paley sum*. The problem of obtaining good estimates for it beyond the range $|A|\,|B| > p$ appears to be quite hard.

In this article we investigate character sums which are related to the Paley sum. First, we motivate its study with the following question of Sárközy:

Problem (Sárközy). *Are the quadratic residues modulo p a sumset? That is, do there exist sets $A, B \subset \mathbb{F}_p$, each of size at least two, with $A + B$ equal to the set of quadratic residues?*

One expects that the answer to the above question is no. Heuristically, if B contains two elements b and b', we would require that $A + b$ and $A + b'$ are both subsets of the quadratic residues. But we expect that $a + b$ is a quadratic residue half of the time, and we expect that $a + b'$ also be a residue half of the time *independent* of whether or not $a + b$ is a quadratic residue. So if $A + B$ consisted entirely of quadratic residues, then many unlikely events must have occurred. For $A + B$ to consist of all the quadratic residues would be shocking. The difficulty in this problem is establishing the aforementioned independence.

In [Sh2], Shkredov showed the quadratic residues are never of the form $A + A$. In more recent work, [Sh1], he also ruled out the case that $Q = A + B$ when A is a multiplicative subgroup. By way of character sum estimates, Shparlinski [Shp], building on work of Sárközy [Sár], has proved that:

Theorem (Sárközy, Shparlinski). *If $A, B \subset \mathbb{F}_p$, each of size at least two, with $A + B$ equal to the set of quadratic residues, then $|A|$ and $|B|$ are within a constant factor of $\sqrt{p}$.*

As a consequence of this theorem and a combinatorial theorem of Ruzsa, one can deduce that the quadratic residues are not of the form $A + B + C$ with each set of size at least two.

Sárközy's question is settled by improved bounds for the Paley sum. Since each sum $a + b$ with $a \in A$ and $b \in B$ is a quadratic residue, we have

$$|A|\,|B| = \sum_{a \in A} \sum_{b \in B} \left(\frac{a+b}{p} \right) \le (p|A|\,|B|)^{1/2}.$$

So $|A|\,|B| \leq p$ and this estimate just fails to resolve Sárközy's problem. So even improving upon the bound $S_{(\frac{\cdot}{p})}(A,B) \leq (p|A|\,|B|)^{1/2}$ by a constant factor would be worthwhile.

Breaking past this barrier, often called the *square-root barrier*, is hard. In practice, the usual way we estimate character sums is via the method of completion. One way of doing so was outlined at the beginning of this article. With this method, we replace a short sum over a subset $A \subset \mathbb{F}_p$ with a complete sum over the whole of $\mathbb{F}_p$, which allows us to use orthogonality. However some terms, the diagonal terms, exhibit no cancellation at all and must be accounted for. By completing the sum we create more diagonal terms, and the resulting loss becomes worse than trivial when the set A is too small. One can dampen the loss from completion by using a higher moment (using Hölder's inequality as opposed to Cauchy–Schwarz's). This was the idea used by Burgess in his work on character sums [Bu1], [Bu2], and it is still one of the only manoeuvres we have for pushing past the square-root barrier. Still, with higher moments the off-diagonal terms become more complicated and we must settle for worse orthogonality estimates, which can be limiting.

In the case of the Paley sum, the square-root barrier is more than just a consequence of our methods. Suppose $q = p^2$ so that $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$ and each element in $\mathbb{F}_p$ is the square of an element in $\mathbb{F}_q$. Since $\mathbb{F}_p$ is closed under addition, any sum $a+b$ with $a, b \in \mathbb{F}_p$ is also a square in $\mathbb{F}_q$. So, if we take $A = B = \mathbb{F}_p$ and χ the quadratic character on $\mathbb{F}_q$, then there is no cancellation in $S_\chi(A,B)$. This shows that, for the Paley sum over $\mathbb{F}_q$, the bound $|S_\chi(A,B)| \leq (q|A|\,|B|)^{1/2}$ is essentially best possible. In order to improve the bound for the Paley sum past the square-root barrier, we need to use an argument which is sensitive to the fact that $\mathbb{F}_p$ has no subfields. Such arguments are hard to come by, and this is perhaps the greatest source of difficulty in the problem.

There have been improvements to estimates for the Paley sum when the sets A and B have a particularly nice structure. In [FI], Friedlander and Iwaniec improved the range in which one can obtain non-trivial estimates when the set A is an interval. This constraint was weakened by Mei-Chu Chang [C] to the case where $|A+A|$ is very small:

THEOREM (Chang). *Suppose $A, B \subset \mathbb{F}_p$ with $|A|, |B| \geq p^\alpha$ for some $\alpha > 4/9$ and such that $|A+A| \leq K|A|$. Then there is a constant $\tau = \tau(K,\alpha)$ such that for p sufficiently large and any non-trivial character χ, we have*

$$|S_\chi(A,B)| \leq |A|\,|B| p^{-\tau}.$$

We remark that in light of Freiman's Theorem, which we will recall shortly, the condition that $|A+A|$ has to be so small is still very restrictive.

Often problems involving a sum of two variables, called *binary additive problems*, are hard. Introducing a third variable gives rise to a *ternary additive problem*, which may be tractable. In this paper we establish non-trivial bounds beyond the square-root barrier for character sums with more than two variables. These results are different from those mentioned above since they hold for all sets which are sufficiently large—there are no further assumptions made about their structure. Our first theorem is the following.

THEOREM 1. *Given subsets* $A, B, C \subset \mathbb{F}_p$, *each of size* $|A|, |B|, |C| \geq \delta\sqrt{p}$ *for some* $\delta > 0$, *and a non-trivial character* χ, *we have*

$$\Big|\sum_{a\in A}\sum_{b\in B}\sum_{c\in C}\chi(a+b+c)\Big| = o_\delta(|A|\,|B|\,|C|).$$

There are analogous results for exponential sums. We have mentioned above that the sum $T_x(A,B)$ in (3) also obeys the bound $|T_x(A,B)| \leq (p|A|\,|B|)^{1/2}$. While this bound may be sharp, Bourgain [Bou] proved that with more variables one can extend the range in which the estimate is non-trivial.

THEOREM (Bourgain). *There is a constant* C *such that the following holds. Suppose* $\delta > 0$ *and* $k \geq C\delta^{-1}$; *then for* $A_1, \dots, A_k \subset \mathbb{F}_p$ *with* $|A_i| \geq p^\delta$ *and* $x \in \mathbb{F}_p^\times$, *we have*

$$\Big|\sum_{a_1\in A_i}\cdots\sum_{a_k\in A_k} e_p(xa_1\cdots a_k)\Big| < |A_1|\cdots|A_k|p^{-\tau}$$

where $\tau > C^{-k}$.

We cannot prove results of this strength. The reason is that one can play the additive and multiplicative structures of the frequencies appearing in such exponential sums and then leverage the Sum-Product Phenomenon to deduce some cancellation. The structure of multiplicative characters is not so nice and we rely on Burgess' method instead.

In Theorem 1, we would prefer a bound of the form $|S_\chi(A,B,C)| \leq |A|\,|B|\,|C|p^{-\tau}$ for some positive τ. However, the proof of Theorem 1 relies on Chang's Theorem, which only allows one to estimate $S_\chi(A,B)$ past the square-root barrier under the hypothesis that $|A+A| \leq K|A|$ for some constant K. This hypothesis plays a crucial part in the proof of her theorem because it allows for the use of Freiman's Classification Theorem:

THEOREM (Freiman). *Suppose* A *is a finite set of integers such that* $|A+A| \leq K|A|$. *Then there is a generalized arithmetic progression* P *containing* A *and such that* P *is of dimension at most* K *and* $\log(|P|/|A|) \ll K^c$ *for some absolute constant* c.

Using this classification theorem, one can make a change of variables $a \mapsto a + bc$, which is the first step in a Burgess-type argument. Freiman's Theorem is unable to accommodate the situation $|A + A| \leq |A|^{1+\delta}$, even for small values of $\delta > 0$, which is what is needed in order to get a power saving in our bound for ternary character sums. To circumvent the use of Freiman's Theorem, we can replace triple sums with sums of four variables. By incorporating both additive and multiplicative convolutions we arrive at sums of the form

$$H_\chi(A, B, C, D) = \sum_{a\in A} \sum_{b\in B} \sum_{c\in C} \sum_{d\in D} \chi(a + b + cd).$$

In this way we have essentially *forced* a scenario where we can make use of the Burgess argument. By introducing both arithmetic operations, we are able to weigh the additive structure in one of the variables against the multiplicative structure of that variable in order to use a Sum-Product estimate. Our second result is:

THEOREM 2. *Suppose $A, B, C, D \subset \mathbb{F}_p$ are sets with $|A|, |B|, |C|, |D| > p^\delta$, $|C| < \sqrt{p}$ and $|D|^4|A|^{56}|B|^{28}|C|^{33} \geq p^{60+\varepsilon}$ for some $\delta, \varepsilon > 0$. There is a constant $\tau > 0$ depending only on δ and ε such that*

$$|H_\chi(A, B, C, D)| \ll |A|\,|B|\,|C|\,|D|p^{-\tau}.$$

In the case that $|A|, |B|, |D| > p^\delta$, $|C| \geq \sqrt{p}$ and $|D|^8|A|^{112}|B|^{56} \geq p^{87+\varepsilon}$, there is a constant $\tau > 0$ depending only on δ and ε such that

$$|H_\chi(A, B, C, D)| \ll |A|\,|B|\,|C|\,|D|p^{-\tau}.$$

Theorem 2 is simplified greatly when all sets in question are assumed to have roughly the same size:

COROLLARY 1. *Suppose $A, B, C, D \subset \mathbb{F}_p$ are sets with $|A|, |B|, |C|, |D| > p^\delta$ and $\delta > 1/2 - 1/176$. Then $H_\chi(A, B, C, D) \leq |A|\,|B|\,|C|\,|D|p^{-\varepsilon}$ for some $\varepsilon > 0$ depending only on δ.*

2. Background. Here we recall facts concerning multiplicative characters over finite fields and additive combinatorics. For details concerning character sums, we refer to [IK, Chapters 11 and 12]. The reference [TV] is extremely helpful for all things additive combinatorial.

Multiplicative characters are the characters χ of the group $\mathbb{F}_q^\times$ which are extended to $\mathbb{F}_q$ by setting $\chi(0) = 0$. In order to carry out the proof of a Burgess-type estimate, we shall need Weil's bound for character sums with polynomial arguments.

THEOREM 3 (Weil). *Let $f \in \mathbb{F}_p[x]$ be a polynomial with r distinct roots over $\overline{\mathbb{F}}_p$. If χ has order l and f is not an lth power over $\overline{\mathbb{F}}_p[x]$, then*

$$\Big|\sum_{x\in\mathbb{F}_p} \chi(f(x))\Big| \le r\sqrt{p}.$$

LEMMA 1. *Let k be a positive integer and χ a non-trivial multiplicative character. Then for any subset $A \subset \mathbb{F}_p$,*

$$\sum_{x\in\mathbb{F}_q} \Big|\sum_{a\in A} \chi(a+x)\Big|^{2k} \le |A|^{2k} 2k\sqrt{p} + (2k|A|)^k p.$$

Proof. Expanding the $2k$th power and using $\overline{\chi}(y) = \chi(y^{p-2})$, we have

$$\sum_{a_1,\dots,a_{2k}\in A} \sum_x \chi((x-a_1)\cdots(x-a_k)(x-a_{k+1})^{p-2}\cdots(x-a_{2k})^{p-2}) = \sum_{\boldsymbol{a}\in A^{2k}} \sum_x \chi(f_{\boldsymbol{a}}(x)).$$

Here $f_{\boldsymbol{a}}$ is the polynomial

$$f_{\boldsymbol{a}}(X) = (X-a_1)\cdots(X-a_k)(X-a_{k+1})^{p-2}\cdots(X-a_{2k})^{p-2}.$$

By Weil's Theorem, $\sum_x \chi(f_{\boldsymbol{a}}(x)) \le 2k\sqrt{p}$ unless $f_{\boldsymbol{a}}$ is an lth power, where l is the order of χ. If any of the roots a_i of $f_{\boldsymbol{a}}$ is distinct from all other a_j then it occurs in the above expression with multiplicity 1 or $p-2$. Both 1 and $p-2$ are prime to l since l divides $p-1$. Hence $f_{\boldsymbol{a}}$ is an lth power only provided all of its roots can be grouped into pairs. So, for all but at most $(2k)!/(2^k k!) \le (2k|A|)^k$ vectors $\boldsymbol{a} \in A^{2k}$, we have the estimate $2k\sqrt{p}$ for the inner sum. For the remaining $\boldsymbol{a}$ we bound the sum trivially by p. Hence the upper bound

$$\sum_{x\in\mathbb{F}_q} \Big|\sum_{a\in A} \chi(a+x)\Big|^{2k} \le |A|^{2k} 2k\sqrt{p} + (2k|A|)^k p. \ \blacksquare$$

We now turn to results from additive combinatorics. Let A and B be finite subsets of an abelian group G. The *additive energy* between A and B is the quantity

$$E_+(A,B) = |\{(a,a',b,b') \in A\times A\times B\times B : a+b = a'+b'\}|.$$

One of the fundamental results on additive energy is the Balog–Szemerédi–Gowers Theorem, which we use in the following form.

THEOREM 4 (Balog–Szemerédi–Gowers). *Suppose A is a finite subset of an abelian group G and*

$$E_+(A,A) \ge |A|^3/K.$$

Then there is a subset $A' \subset A$ of size $|A'| \gg |A|/(K(\log(e|A|))^2)$ with

$$|A' - A'| \ll K^4 \frac{|A'|^3(\log(|A|))^8}{|A|^2}.$$

The implied constants are absolute.

This version of the theorem has very good explicit bounds, and is due to Bourgain and Garaev. The proof is essentially a combination of Lemmas 2.2 and 2.4 from [BG]. It was communicated to us by O. Roche-Newton. Since we prefer to work with sumsets rather than difference sets we have the following lemma, which is a well-known application of Ruzsa's triangle inequality.

LEMMA 2. *Suppose A is a finite subset of an abelian group G. Then*

$$|A - A| \le \left(\frac{|A + A|}{|A|}\right)^2 |A|.$$

We will prefer to work with the energy between a set and itself rather than between distinct sets, so we need the following fact, which is a simple consequence of the Cauchy–Schwarz inequality.

LEMMA 3. *For sets A and B,*

$$E_+(A, B)^2 \le E_+(A, A)E_+(B, B).$$

We now record a general version of Burgess' argument, which is an application of Hölder's inequality and Weil's bound. This proof is distilled from the proof of Burgess' estimate in [IK, Chapter 12].

LEMMA 4. *Let $A, B, C \subset \mathbb{F}_p$ and suppose χ is a non-trivial multiplicative character. Define*

$$r(x) = |\{(a, b) \in A \times B : ab = x\}|.$$

Then for any positive integer k,

$$\sum_{x\in\mathbb{F}_p} r(x)\Big|\sum_{c\in C}\chi(x + c)\Big| \le (|A|\,|B|)^{1-1/k} E_\times(A, A)^{1/(4k)} E_\times(B, B)^{1/(4k)} \cdot (|C|^{2k} 2k\sqrt{p} + (2k|C|)^k p)^{1/(2k)}.$$

Proof. Denote the left hand side above by S. Applying Hölder's inequality we get

$$|S| \le \Big(\sum_{x\in\mathbb{F}_p} r(x)\Big)^{1-1/k} \Big(\sum_{x\in\mathbb{F}_p} r(x)^2\Big)^{1/(2k)} \Big(\sum_{x\in\mathbb{F}_p}\Big|\sum_{c\in C}\chi(x + c)\Big|^{2k}\Big)^{1/(2k)} = T_1^{1-1/k} T_2^{1/2k} T_3^{1/2k}.$$

Now T_1 is precisely $|A|\,|B|$ and T_2 is the multiplicative energy $E_\times(A,B)$. By the inequality in Lemma 3, we have

$$E_\times(A,B) \le \sqrt{E_\times(A,A)E_\times(B,B)}.$$

The estimate for T_3 is immediate from Lemma 1. ∎

The last ingredient in the proofs of our main results is the most crucial. Sum-Product estimates are sensitive to prime fields and allow us to break the square-root barrier. We record the following estimate of Rudnev [R].

THEOREM 5 (Rudnev). *Let $A \subset \mathbb{F}_p$ satisfy $|A| < \sqrt{p}$. Then*

$$E_\times(A,A) \ll |A|\,|A+A|^{7/4}\log|A|.$$

This is not the state of the art for Sum-Product theory in $\mathbb{F}_p$, which at the time of this writing is found in [RNRS], but the above estimate is more readily applied to our situation. Moreover, the strength of the Sum-Product estimates is not the bottleneck for proving non-trivial character sum estimates in a wider range (avoiding completion is).

3. Ternary sums. We begin this section by giving a simple estimate which is non-trivial past the square-root barrier provided we can control certain additive energy.

LEMMA 5. *Given subsets $A, B, C \subset \mathbb{F}_p$ and a non-trivial character χ, we have*

$$|S_\chi(A,B,C)| \le \sqrt{p|A|E_+(B,C)}.$$

Proof. Let $r(x)$ be the number of ways in which $x \in \mathbb{F}_p$ is a sum $x = b+c$ with $b \in B$ and $c \in C$. Then

$$\begin{aligned}|S(A,B,C)| &\le \sum_{x\in\mathbb{F}_p} r(x)\Big|\sum_{a\in A}\chi(a+x)\Big| \\ &\le \Big(\sum_{x\in\mathbb{F}_p} r(x)^2\Big)^{1/2}\Big(\sum_{x\in\mathbb{F}_p}\Big|\sum_{a\in A}\chi(a+x)\Big|^2\Big)^{1/2}.\end{aligned}$$

It is straightforward to check that the first factor above is $(E_+(B,C))^{1/2}$ and, as before, the second factor is $(p|A|)^{1/2}$. ∎

LEMMA 6. *Let $z_1,\dots,z_n$ be complex numbers with $|\arg z_1 - \arg z_j| \le \delta$ for $j = 2,\dots,n$. Then*

$$|z_1+\cdots+z_n| \ge (1-\delta)(|z_1|+\cdots+|z_n|).$$

Proof. We have

$$\begin{aligned}|z_1|+\cdots+|z_n| &= \theta_1 z_1+\cdots+\theta_n z_n \\ &= \theta_1(z_1+\cdots+z_n)+(\theta_2-\theta_1)z_2+\cdots+(\theta_n-\theta_1)z_n\end{aligned}$$

for some complex numbers θ_k of modulus 1 with $|\theta_1 - \theta_j| \le \delta$. Thus by the triangle inequality

$$|z_1| + \cdots + |z_n| \le |z_1 + \cdots + z_n| + \delta(|z_2| + \cdots + |z_n|),$$

and the result follows. ∎

We are now able prove Theorem 1. Ignoring technical details for the moment, either we are in a situation where Lemma 5 improves upon the trivial estimate, or else we can appeal to the Balog–Szemerédi–Gowers Theorem and deduce that A has a subset with small sumset. In the latter case we can make use of Chang's Theorem and also arrive at a non-trivial estimate, even saving a power of p. Unfortunately, this second scenario does not come into play until one of the sets has a lot of additive energy. This means that the saving from Lemma 5 will become quite poor before we are rescued by Chang's estimate. We proceed with the proof proper.

Proof of Theorem 1. Suppose, by way of contradiction, that the theorem does not hold. This means that there is some positive constant $\varepsilon > 0$ such that for p arbitrarily large, we have sets $A, B, C \subset \mathbb{F}_p$ with $|A|, |B|, |C| \ge \delta\sqrt{p}$, and a non-trivial character χ of $\mathbb{F}_p^\times$ satisfying

$$|S_\chi(A, B, C)| \ge \varepsilon |A|\,|B|\,|C|.$$

It follows that

$$\varepsilon |A|\,|B|\,|C| \le \sum_{a \in A} |S_\chi(B, a + C)|.$$

If we let

$$A' = \left\{ a \in A : |S_\chi(B, a + C)| \ge \frac{\varepsilon}{2} |B|\,|C| \right\},$$

then

$$\frac{\varepsilon}{2} |A|\,|B|\,|C| \le \sum_{a \in A'} |S_\chi(B, a + C)|$$

and $|A'| \ge |A|\varepsilon/2$. Now by the same argument as in the proof of Lemma 5, we must have

$$\frac{\varepsilon^2}{4} |A|^2 |B|^2 |C|^2 \le p|C| E_+(A', B) \le p|C| E_+(A', A')^{1/2} E_+(B, B)^{1/2},$$

the last inequality being a consequence of Lemma 3. So, using the fact that $|A|, |B|, |C| \ge \delta\sqrt{p}$ and $E_+(B, B) \le |B|^3$, we get

$$E_+(A', A') \ge \frac{\varepsilon^4 \delta^4}{16} |A'|^3,$$

and so by Theorem 4 and Lemma 2 we can find a subset $A'' \subset A'$ with size at least $(\varepsilon\delta)^t \sqrt{p}$ and such that $|A'' + A''| \le (\varepsilon\delta)^{-t} |A''|$ for some $t = O(1)$.

Now since $A'' \subset A'$, we have

$$\frac{\varepsilon}{2}|A''|\,|B|\,|C| \leq \sum_{a\in A''} |S_\chi(B, a+C)|.$$

By the pigeon-hole principle, after passing to a subset of A''' of size $|A''|/16$, we can assume that the complex numbers $S_\chi(B, a+C)$ all have argument within $1/2$ of each other. Thus, by Lemma 6, we have

$$\frac{\varepsilon}{4}|A'''|\,|B|\,|C| \leq |S_\chi(A''', B, C)|,$$

we have $|A'''| \geq (\varepsilon\delta)^t\sqrt{p}/16$, and we have

$$|A''' + A'''| \leq |A'' + A''| \leq (\varepsilon\delta)^{-t}|A''| \leq 16(\varepsilon\delta)^{-t}|A'''|.$$

However, by the triangle inequality, this implies that

$$\frac{\varepsilon}{4}|A'''|\,|B+c| \leq \max_{c\in C} |S_\chi(A''', B+c)|.$$

This is in clear violation of Chang's Theorem provided p is sufficiently large in terms of δ and ε. Thus we have arrived at the desired contradiction. ∎

4. Mixed quaternary sums. We now turn to the estimation of the sums $H_\chi(A, B, C, D)$. First we consider an auxiliary ternary character sum with a multiplicative convolution:

$$M_\chi(A, B, C) = \sum_{a\in A}\sum_{b\in B}\sum_{c\in C} \chi(a+bc).$$

We can bound M_χ in terms of the *multiplicative energy*

$$E_\times(X, Y) = |\{(x_1, x_2, y_1, y_2) \in X\times X\times Y\times Y : x_1y_1 = x_2y_2\}|.$$

As before, this satisfies the bound

$$E_\times(X, Y)^2 \leq E_\times(X, X)E_\times(Y, Y).$$

Now, using Sum-Product estimates, if the sets had enough additive structure, we could bound the multiplicative energy non-trivially and make an improvement. This is essentially Burgess' argument, though he did not use Sum-Product theory; rather, since he was working with arithmetic progressions, the multiplicative energy could be bounded directly.

By fixing one element in the sum $H_\chi(A, B, C, D)$, we can view it as a ternary sum in two different ways. First,

$$H_\chi(A, B, C, D) = \sum_{d\in D} S_\chi(A, B, d\cdot C)$$

where $d\cdot C$ is the dilate of C by d. We can use Lemma 5 to bound this sum non-trivially whenever we can bound $E_+(C, C)$ non-trivially. If not, we can

write

$$H_\chi(A,B,C,D)=\sum_{a\in A} M_\chi(a+B,C,D)$$

instead and try to bound this non-trivially using Lemma 4, which we can do if $E_\times(C,C)$ is smaller than $|C|^3$. By making some simple manipulations to H_χ and using a Sum-Product estimate, we will be able to guarantee one of these facts holds.

Before presenting our proof, we mention that A. Balog has communicated to us that a similar result would follow from a theorem of his with Wooley (see [BW]):

THEOREM. *There is a positive δ such that any $X\subset\mathbb{F}_p$ can be decomposed as $X=Y\cup Z$ with $E_+(Y,Y)\le |Y|^{3-\delta}$ and $E_\times(Z,Z)\le |Z|^{3-\delta}$.*

The proof of this result uses ideas similar to those in our proof of Theorem 2, and implies a non-trivial estimate for H_χ. Indeed, decomposing $C=Y\cup Z$ as in the last theorem, we get

$$|H_\chi(A,B,C,D)|\le |H_\chi(A,B,X,D)|+|H_\chi(A,B,Y,D)|.$$

Estimating each of these sums as we mentioned above gives a non-trivial bound for $|H_\chi(A,B,C,D)|$.

Proof of Theorem 2. Let $2\le k\ll \log p$ be a (large) parameter. First we handle the case $|C|<\sqrt{p}$. Let us write

$$|H_\chi(A,B,C,D)|=\Delta|A|\,|B|\,|C|\,|D|$$

so that our purpose is to estimate Δ. Let

$$C_1=\{c\in C: |S_\chi(A,B,c\cdot D)|\ge \Delta|A|\,|B|\,|D|/2\}.$$

For any $C_2\subset C_1$,

$$\frac{|C_2|}{2|C|}|H_\chi(A,B,C,D)|=|C_2|\Delta|A|\,|B|\,|D|/2\le \sum_{c\in C_2}|S_\chi(A,B,c\cdot D)|,$$

and since the inner quantities are at most $|A|\,|B|\,|D|$, we also have

$$|C_1|\ge \frac{\Delta}{2}|C|.$$

Now, passing to a subset C_2 of C_1 of size at least

$$|C_2|\ge \frac{|C_1|}{16}\ge \frac{\Delta}{32}|C|,$$

we can assume that the complex numbers $S_\chi(A,B,c\cdot D)$ with $c\in C_2$ all have arguments within $1/2$ of each other, so that by Lemma 6,

$$\frac{|C_3|}{4|C|}|H_\chi(A,B,C,D)|\le \Big|\sum_{c\in C_3} S_\chi(A,B,c\cdot D)\Big| = |H_\chi(A,B,C_3,D)| \tag{4}$$

whenever C_3 is a subset of C_2. In particular, if $C_3 = C_2$ we have

$$\frac{\Delta^2}{128}|A|\,|B|\,|C|\,|D| \le \frac{|C_2|}{4|C|}|H_\chi(A,B,C,D)| \le \sum_{d\in D}|S_\chi(A,B,d\cdot C_2)|.$$

Now in view of Lemma 5, we see that

$$\begin{aligned}\frac{\Delta^2}{128}|A|\,|B|\,|C|\,|D| &\le |D|\max_{d\in D}\sqrt{p|A|E_+(B,d\cdot C_2)}\\ &\le \sqrt{p}\,|D|\,|A|^{1/2}|B|^{3/4}E_+(C_2,C_2)^{1/4},\end{aligned}$$

having bounded $E_+(B,B)$ trivially by $|B|^3$. Thus

$$E_+(C_2,C_2) \ge \frac{\Delta^8}{128^4}|A|^2|B|\,|C|^4p^{-2} \ge \left(\frac{\Delta^8}{128^4}|A|^2|B|\,|C|p^{-2}\right)|C_2|^3.$$

For convenience, write $K^{-1} = \frac{\Delta^8}{128^4}|A|^2|B|\,|C|p^{-2}$. By Theorem 4 there is a subset $C_3 \subset C_2$ of size at least $|C_2|/(K(\log p)^2)$ and such that

$$|C_3 - C_3| \ll K^4\frac{|C_3|^2(\log p)^8}{|C_2|^2}|C_3|.$$

In particular, by Theorem 5 we have

$$\begin{aligned}E_\times(C_3,C_3) &\ll |C_3|K^7\left(\frac{|C_3|^2(\log p)^8}{|C_2|^2}\right)^{7/4}|C_3|^{7/4}\log p\\ &= K^7|C_3|^{25/4}|C_2|^{-7/2}(\log p)^{15}.\end{aligned}$$

Inserting this into (4), we get

$$\begin{aligned}\frac{\Delta}{4}|A|\,|B|\,|C_3|\,|D| = \frac{|C_3|}{4|C|}|H_\chi(A,B,C,D)| &\le |H_\chi(A,B,C_3,D)|\\ &\le \sum_{a\in A}|M_\chi(a+B,C_3,D)|.\end{aligned}$$

Next we apply Lemma 4 to obtain

$$\begin{aligned}\frac{\Delta}{4}|A|\,|B|\,|C_3|\,|D| \ll |A|(|D|\,|C_3|)^{1-1/k}\big(E_\times(D,D)E_\times(C_3,C_3)\big)^{1/(4k)}\\ \times\big(|B|^{2k}2k\sqrt{p}+(2k|B|)^kp\big)^{1/(2k)},\end{aligned}$$

which implies (after bounding $E_\times(D,D)$ trivially by $|D|^3$)

$$\Delta^{4k} \ll |D|^{-1}|C_3|^{-4}E_\times(C_3,C_3)\big(2k\sqrt{p}+(2k|B|^{-1})^kp\big)^2.$$

Since $2 \le k \ll \log p$ and $|B| \ge p^\delta$, the final factor is at most $O(p(\log p)^{2k})$ as long as $k > 1/(2\delta)$, and after inserting the upper bound for $E_\times(C_3,C_3)$ we have

$$\Delta^{4k} \ll |D|^{-1}K^7|C_3|^{9/4}|C_2|^{-7/2}(\log p)^{2k+15}p.$$

Now we substitute $K^{-1} = \frac{\Delta^8}{128^4}|A|^2|B|\,|C|p^{-2}$ and see that

$$\Delta^{4k+56} \ll |D|^{-1}|A|^{-14}|B|^{-7}|C|^{-7}|C_3|^{9/4}|C_2|^{-7/2}(\log p)^{2k+15}p^{15}.$$

Bounding $|C_3| \le |C_2|$ and $|C_2| \gg \Delta|C|$ we get

$$\Delta^{4k+229/4} \ll |D|^{-1}|A|^{-14}|B|^{-7}|C|^{-33/4}(\log p)^{2k+15}p^{15}.$$

Upon taking $4k$th roots we have

$$\Delta^{1+229/(16k)} \ll (|D|^{-1}|A|^{-14}|B|^{-7}|C|^{-33/4}p^{15})^{1/(4k)}(\log p)^{1/2+15/(4k)}.$$

Since

$$|D|^4|A|^{56}|B|^{28}|C|^{33} \ge p^{60+\varepsilon},$$

the quantity in brackets on the right is at most $p^{-\varepsilon/4}$. This shows that we must have $\Delta < p^{-\tau}$ for some $\tau > 0$ depending only on ε and δ. This is because we only needed k to be sufficiently large in terms of δ.

If $|C| > \sqrt{p}$ then we can break C into a disjoint union of $m \approx |C|/\sqrt{p}$ sets $C_1, \dots, C_m$ of size at most $\sqrt{p}$. Then

$$|H_\chi(A,B,C,D)| \le \sum_j |H_\chi(A,B,C_j,D)|.$$

We obtain a saving of $p^{-\tau}$ for each $H_\chi(A,B,C_j,D)$ and hence also for $H_\chi(A,B,C,D)$ provided

$$|D|^4|A|^{56}|B|^{28}|C_j|^{33} \gg |D|^4|A|^{56}|B|^{28}p^{33/2} \ge p^{60+\varepsilon},$$

which is guaranteed by hypothesis (with 2ε in place of ε). ∎

Acknowledgments. The author is grateful to John Friedlander and Antal Balog for much fruitful discussion during the preparation of this article.

References

[BW] A. Balog and T. D. Wooley, *A low-energy decomposition theorem*, arXiv:1510.03309 (2015).

[Bou] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geom. Funct. Anal. 18 (2009), 1477–1502.

[BG] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Philos. Soc. 146 (2009), 1–21.

[Bu1] D. A. Burgess, *On character sums and L-series*, Proc. London Math. Soc. (3) 12 (1962), 193–206.

[Bu2] D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. (3) 13 (1963), 524–536.

[C] M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*, Duke Math. J. 145 (2008), 409–442.

[FI] J. Friedlander and H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. 119 (1993), 365–372.

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[RNRS] O. Roche-Newton, M. Rudnev and I. D. Shkredov, *New sum-product type estimates over finite fields*, Adv. Math. 293 (2016), 589–605.

[R] M. Rudnev, *An improved sum-product inequality in fields of prime order*, Int. Math. Res. Notices 2012, no. 16, 3693–3705.

[Sár] A. Sárközy, *On additive decompositions of the set of quadratic residues modulo p*, Acta Arith. 155 (2012), 41–51.

[Sh1] I. D. Shkredov, *Sumsets in quadratic residues*, Acta Arith. 164 (2014), 221–243.

[Sh2] I. D. Shkredov, *Differences of subgroups in subgroups*, arXiv:1508.03814 (2015).

[Shp] I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, SIAM J. Discrete Math. 27 (2013), 1870–1879, .

[TV] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math. 105, Cambridge Univ. Press, Cambridge, 2006.

Brandon Hanson
Mathematics Department
Pennsylvania State University
University Park, PA 16802, U.S.A.
E-mail: bwh5339@psu.edu