Exponential Sums and Additive Combinatorics

Chun-Yen Shen
National Taiwan University

10th Cross-Strait Combinatorics Conference

Aug 22, 2019

Given a set A, we define its sum set to be the set

$$A + A := \{a + b : a, b \in A\}$$

and its product set to be

$$AA := \{ab : a, b \in A\}.$$

Erdös and Szemerédi (1983) conjectured that at least one of these two sets has near-quadratic growth. Precisely, it was conjectured

$$\max\{|A + A|, |AA|\} \geq C_\epsilon |A|^{2-\epsilon},$$

for any $\epsilon > 0$. (i.e. $\frac{|A|^2}{(\log |A|)^b}$)

Why did they come up with this lower bound ?
Consider A as

$$A = \{1, 2, 3, \cdots, N\},$$

in other words, A is an arithmetic progression and so $A + A$ is small, but AA is quadratically large.
On the other hand, consider

$$A = \{2, 2^2, 2^3, \cdots, 2^N\},$$

a geometric progression, then AA is small, but $A + A$ is quadratically large.

There have been some important progress for this problem, but it is still widely open. On the other hand, the same problem in prime fields was proved by Bourgain, Katz and Tao in 2004 that

$$\max\{|A+A|, |AA|\} \geq |A|^{1+\epsilon},$$

for any $A \subset F_p$ with $|A| < p^{1-\delta}$. The result has been found extremely useful in various research problems.

The breakthrough work of H. A. Helfgott asserts that if E is a subset of $SL_2(\mathbb{F}_p)$ and not contained in any proper subgroup with $|E| < p^{3-\delta}$, then $|E \cdot E \cdot E| > c|E|^{1+\epsilon}$ for some $\epsilon = \epsilon(\delta) > 0$. This result confirms a longstanding conjecture of Babai.

Another important application of the BKT sum-product theorem is the following (resolved a longstanding open problem in analytic number theory).

Theorem (Bourgain-Konyagin)

Let H be a multiplicative subgroup of $\mathbb{F}_p^*$ with size of p^δ. Then uniformly for all $a \neq 0$, we have

$$|\sum_{x \in H} \exp(ax)| \leq \frac{|H|}{p^\epsilon},$$

for some $\epsilon = \epsilon(\delta) > 0$.

Exponential sum estimates have applications to Fourier transform.

Recall: Given a set $A \subset F_p$, we define the Fourier transform of the set A by

$$\widehat{\chi_A}(\xi) = \frac{1}{p} \sum_{x \in A} \exp(-\xi \cdot x)$$

Take an example. Consider $A = \{a^2 : a \in F_p\}$, then Gauss exponential sum estimate will tell us that when $\xi \neq 0$ the set A has large Fourier decay. In other words.

$$|\widehat{\chi_A}(\xi)| \text{is small when } \xi \neq 0.$$

We actually can directly compute the value.

$|\sum_{a\in F}\exp(-\xi\cdot a^2)|^2 = \sum_{a,b\in F}\exp(-\xi(a^2-b^2)) =$
$\sum_{a,h\in F}\exp(-\xi(a^2-(a+h)^2))$

$= \sum_{h\in F}\exp(-\xi h^2)\sum_{a\in F}\exp(-\xi 2ah)$.
However, if $h\neq 0$, the sum $\sum_{a\in F}\exp(-\xi 2ah) = 0$ because of the orthogonal property. Thus we can conclude that

$$|\sum_{a\in F}\exp(-\xi\cdot a^2)|^2 = |F|.$$

This gives $|\hat{\chi_A}(\xi)| \leq \frac{1}{|F|^{1/2}}$

Above example shows that exponential sum estimate helps Fourier transform. Let us look at an example that shows Fourier transform helps additive combinatorics.

Theorem (J. Bourgain)

Let $A \subset \mathbb{F}_p$ with $|A| > |F|^{3/4}$. Then $AA + AA + AA = F$.

$$AA + AA + AA = F$$

Look at this expression in analytic number theory way, it says :

The equation $a_1 a_2 + a_3 a_4 + a_5 a_6 = c$ is always solvable in A for any $c \in F$ as long as the size of the set A is large enough.

Define $f(x) = \frac{1}{|A|} \sum_{a \in A} \chi_{a \cdot A}(x)$. Clearly the support of f is AA. If we take Fourier transform and use Cauchy-Schwartz inequality and use previous Fourier decay estimate, we obtain for $\xi \neq 0$,

$$|\widehat{f}(\xi)| \leq \frac{1}{|F|^{1/2}}.$$

$f * f * f(x) = \sum_{\xi \in F} \widehat{f}(\xi)^3 \exp(\xi x) \geq |\hat{f}(0)|^3 - \sum_{\xi \neq 0} |\hat{f}(\xi)|^3 > 0$. Since the support of $f * f * f$ is $AA + AA + AA$, it is done.

Summary: Exponential sum estimates $\rightarrow$ Fourier transform $\rightarrow$ Additive combinatorics.

Our below results show the converse direction. Using techniques in Additive combinatorics to obtain some nontrivial estimate for some certain exponential sums.

Let $\mathbb{F}_p$ be a prime field, χ be a non-trivial multiplicative character of $\mathbb{F}_p^*$.
The well-known graph Paley conjecture: any two sets $A, B \subset \mathbb{F}_p$ with $|A|, |B| > p^\delta$, there exists $\gamma = \gamma(\delta)$ such that the following estimate holds:

$$\left| \sum_{a \in A, b \in B} \chi(a+b) \right| < p^{-\gamma} |A||B|.$$

The conjecture remains widely open. There have been some progress if we make some assumptions on the size of $|A|, |B|$ or some additional structures on the sets A, B. For example, It was showed by M-C Chang that if we have

$$|A| > p^{\frac{4}{9}+\delta},$$

$$|B| > p^{\frac{4}{9}+\delta},$$

$$|B+B| < K|B|.$$

Then

$$\left|\sum_{a\in A, b\in B} \chi(a+b)\right| < p^{-\gamma}|A||B|.$$

Later Shkredov and Volostnov , using Croot-Sisask lemma on almost periodicity of convolutions of characteristic functions of sets, further improved this theorem with an additional assumption on additive sets.
Suppose that

$$|A| > p^{\frac{12}{31}+\delta},$$

$$|B| > p^{\frac{12}{31}+\delta},$$

$$|A+A| < K|A|,$$

$$|A+B| < L|B|.$$

Then we have

$$\left|\sum_{a\in A, b\in B} \chi(a+b)\right| < \sqrt{\frac{L\log 2K}{\delta \log p}}|A||B|.$$

Inspired by the structures of the sets A, B, we may make some more progress on the exponential sums estimates if we find more techniques from additive combinatorics and the connections between these problems.

This is the goal of our result. We did not make any progress for the graph Paley conjecture, but we find an interesting connection if we consider the following exponential sums.

Given four sets T, U, V, W and two sequences of weights $\alpha = (\alpha_t)$, $\beta = (\beta_{u,v,w})$ with

$$\max_{t \in T} |\alpha_t| \leq 1, \quad \max_{(u,v,w) \in U \times V \times W} |\beta_{u,v,w}| \leq 1,$$

We consider the following exponential sum

$$S = \sum_{t \in T, u \in U, v \in V, w \in W} \alpha_t \beta_{uvw} \chi(t + f(u, v, w)), \qquad (1)$$

where f is a polynomial in three variables in $\mathbb{F}_p[x, y, z]$.

Our results include several previous results obtained by analytic number theory techniques. In particular, the cases $f(x, y, z) = x + yz$ or $f(x, y, z) = x(y + z)$.

Theorem

Let $M = \max\{U, V, W\}$. *then for any fixed integer* $n \geq 1$, *we have*

$$S \ll \left((UVW)^{1-\frac{1}{4n}} + M^{1/2n}(UVW)^{1-\frac{1}{2n}}\right) \cdot$$

$$T^{1/2}p^{1/2} \;\; \text{if} \;\; n = 1$$

$$Tp^{\frac{1}{4n}} + T^{\frac{1}{2}}p^{\frac{1}{2n}} \;\; \text{if} \;\; n \geq 2.$$

For example,

1. If $U \sim V \sim W \sim T \sim N$, then by setting $n = 1$, we have
$$S \ll N^{11/4} p^{1/2},$$
which is non-trivial whenever $N \geq p^{\frac{2}{5}+\epsilon}$ for some $\epsilon > 0$.
2. Suppose that $T \geq p^{\epsilon}$ for some $\epsilon > 0$ and $U \sim V \sim W$. Taking $n = \lfloor \frac{2}{\epsilon} \rfloor + 1$, we have
$$S \ll UVWT \left(\frac{p}{UVW} \right)^{1/4n},$$
which is non-trivial as long as $UVW > p^{1+\epsilon}$ for some $\epsilon > 0$.

For two variables polynomials, we also have similar results. In other words, we can consider:

$$S = \sum_{t \in T, u \in U, v \in V} \alpha_t \beta_{uv} \chi(t + f(u, v)).$$

and obtain

$$S \lesssim \frac{TUV}{p^{\delta}},$$

for some $\delta > 0$,

One of the key ingredients in our proofs is the energy estimate for polynomials for which we use point-plane incidences estimate and some combinatorial arguments.

Energy estimate is one of the most important topics in the area of additive combinatorics.

Energy estimates:

Given two sets A, B. The energy, denoted by $E(A, B)$, is the quantity

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

A trivial but sharp upper bound is $|A||B|^2$ or $|A|^2|B|$.

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

On the other hand, if we have some structures information for A, B, we can expect to get a better upper bound. For example:

If we know A, B have lots of multiplicative structures, how can we get a better upper bound ?

Remark: If we know the information of the energy estimate, there is a famous theorem by Balog-Szemeredi-Gowers which gives some information for the structures of the sets A, B.

Various energy estimates:

Given a two (or three) variables polynomial $f(x, y)$, what can we say about the energy:

$$E = |\{(a, b, a', b') : f(a, b) = f(a', b')\}|,$$

and

$$E = |\{(a, b, c, a', b', c') : f(a, b, c) = f(a', b', c')\}|$$

For three variables polynomials, we have the following estimate:

$$E \ll (UVW)^{3/2} + MUVW + V^2W^2,$$

where $M = \max\{U, V, W\}$.

After some reductions, we can assume that $f(x, y, z) = axy + bxz + cyz + r(x) + s(y) + t(z)$ where one of $a, b, c \in \mathbb{F}_p$ is not zero, and r, s, t are polynomials in one variable with degree at most two. Furthermore, from the symmetric property of $f(x, y, z)$ we only need to consider the following three cases:

(Case 1) $f(x, y, z) = axy + bxz + r(x) + s(y) + t(z)$ with $a \neq 0$ and $\deg(t) = 2$.
(Case 2) $f(x, y, z) = axy + bxz + r(x) + s(y) + t(z)$ with $a \neq 0$ and $\deg(t) = 1$.
(Case 3) $f(x, y, z) = axy + bxz + cyz + r(x) + s(y) + t(z)$ with $a, b, c \neq 0$.

Our proofs use the followings:
The first one is the point-plane incidences estimate by Rudnev.

Theorem (2015 Adv in Math)

Let P denote a set of points in $\mathbb{F}_p^3$ and S a set of planes in $\mathbb{F}_p^3$. Assume that there is no line that contains k points of P and is contained in k planes of S. Then we have

$$I(P,S) := |\{(p,s) : p \in P, s \in S\}| \ll |P|^{1/2}|S| + k|S|.$$

Second, we also use the following theorem.

Lemma (Kővari–Sós–Turán)

Let $G = (A \cup B, E(G))$ be a $K_{2,t}$-free bipartite graph. Then the number of edges between A and B is bounded by

$$|E(G)| \ll t^{1/2}|A||B|^{1/2} + |B|.$$

Let E be the number of tuples (x, y, z, x', y', z') such that $f(x, y, z) = f(x', y', z')$, where the polynomial f takes the form in **Case 1.** This implies that

$$ayx - ax'y' + (bxz + r(x) + t(z) - s(y')) = bx'z' + r(x') + t(z') - s(y).$$

We can view this relationship as an incidence between a point set and a plane set in $\mathbb{F}_p^3$.

Let P be the following point set:

$$\{(x, y', bxz + r(x) + t(z) - s(y')) : (x, y', z) \in U \times V \times W\} \subset \mathbb{F}_p^3,$$

and S be the following plane set

$$\{ayX - ax'Y + Z = bx'z' + r(x') + t(z') - s(y) : (x', y, z') \in U \times V \times W\}.$$

Something that we need to be careful is the multiplicity of the point set and plan set. We need to make sure these sets are not degenerate.

For each fixed $(u, v, w) \in P$, at most two elements (x, y', z) in $U \times V \times W$ reproduce (u, v, w), because $\deg(t) = 2$. In fact, we can take $x = u, y' = v$, and z values are solutions to

$$t(z) + buz + r(u) - s(v) = w.$$

Similarly, we can check each fixed plane in S can be determined by at most two elements (x', y, z'), and each element in $U \times V \times W$ determines a point in P and a plane in S. All of this gives us

$$|P| \sim |S| \sim UVW \quad \text{and} \quad E \sim I(P, S).$$

To bound $I(P.S)$, we apply Rudnev's point-plane incidence theorem. Again, we need to check the assumptions.

First we count the number of collinear points in P. Let P' be the projection of P onto the first two coordinates, i.e. $P' = U \times V$. Thus any line contains at most $\max\{U, V\}$ points unless it is vertical. In the case of vertical lines, we can see that no plane in S contains such lines, because the z-coordinate of normal vectors of planes in S is one. Therefore, we can apply the incidence Theorem with $k = \max\{U, V\}$ to get

$$E \ll (UVW)^{3/2} + U^2VW + UV^2W.$$

Remark: Case 1 is simple.

Case 2: $\deg(t) = 1$. In other words, $f(x, y, z) = axy + bxz + r(x) + s(y) + mz$ for some $m \in \mathbb{F}_p^*$. Still, we define the set P of points and the set S of planes as follows:

$$P = \{(x, y', bxz + r(x) + mz - s(y'))\}$$

$$S = \{ayX - ax'Y + Z = bx'z' + r(x') + mz' - s(y)\}.$$

The reason that Case 2 is more difficult is that if $u = -m/b \in U$, then the triples $(-m/b, v, w) \in P$ can be determined by many triples $(x, y', z) \in U \times V \times W$. For this case, we need to do some more technical steps. So If $-m/b \notin U$, previous arguments can be applied.

Thus we now assume that $u = -m/b \in U$. As above, we first need to estimate the sizes of P and S. For $(u, v, w) \in P$ and $(x, y', z) \in U \times V \times W$, we consider the following system of three equations:

$$u = x,\ v = y',\ w = buz + r(u) + mz - s(v).$$

Since $u = -m/b \in U$, then we have

$$u = x,\ v = y',\ w = r(u) - s(v) \quad \text{for all } \ z \in W. \tag{2}$$

Let P_1 be the set of points $(u, v, w) \in P$ with $u = -m/b$. Then P_1 is a set with V points, since for any $v = y' \in V$, w is determined uniquely. Above equation and the definition of $P1$, we have that each point in P_1 is determined by W triples $(x, y', z) \in U \times V \times W$. Let $P_2 = P \setminus P_1$. Now notice that each point in P_2 is determined by exactly one triple $(x, y', z) \in U \times V \times W$.

Using the same arguments, we also partition the set of planes S into two sets S_1 and S_2 with $S_2 = S \setminus S_1$ so that $|S_1| = V$, each plane in S_1 is determined by W triples $(x', y, z') \in U \times V \times W$, and each plane in S_2 is determined by exactly one triple $(x', y, z') \in U \times V \times W$.

It now follows that each incidence between P_1 and S_2, or between P_2 and S_1 contributes to E by W, each incidence between P_1 and S_1 contributes to E by W^2, and each incidence between P_2 and S_2 contributes to E by one. Namely we have

$$E \ll W^2 \cdot I(P_1, S_1) + W \cdot I(P_1, S_2) + W \cdot I(P_2, S_1) + I(P_2, S_2).$$

It is not hard to show

$$I(P_1, S_1) \ll V^2.$$

To bound $I(P_2, S_2)$, recall that each element of P_2 and S_2 is determined by exactly one element $(x, y, z) \in U \times V \times W$ with $x \neq -m/b$. Hence, using the same arguments, we can show

$$I(P_2, S_2) \ll (UVW)^{3/2} + U^2VW + UV^2W.$$

To bound $I(P_1, S_2)$, we will use graph Lemma.

Lemma (Kővari–Sós–Turán)

Let $G = (A \cup B, E(G))$ be a $K_{2,t}$-free bipartite graph. Then the number of edges between A and B is bounded by

$$|E(G)| \ll t^{1/2}|A||B|^{1/2} + |B|.$$

Thus if we let $A := P_1$ and $B := S_2$, it can be directly checked that the graph $(A \cup B, E(G))$ is $K_{2,V}$ free, it follows that

$$I(P_1, S_2) = E(G) \ll V^{1/2}V(UVW)^{1/2} + UVW = U^{1/2}W^{1/2}V^2 + UVW.$$

Similarly, we also have

$$I(P_2, S_1) \ll U^{1/2}W^{1/2}V^2 + UVW.$$

Combining everything, we have proved that

$$E \ll (UVW)^{3/2} + UV^2W + U^2VW + UVW^2 + V^2W^2 + U^{1/2}V^2W^{3/2}$$
$$\ll (UVW)^{3/2} + UV^2W + U^2VW + UVW^2 + V^2W^2.$$

Case 3:
Recall, we aim to estimate E : the number of tuples (x, y, z, x', y', z') satisfying the equation

$$f(x, y, z) = f(x', y', z'), \tag{3}$$

$$f(x, y, z) = axy + bxz + cyz + dx^2 + ey^2 + gz^2 + hx + iy + jz,$$

where $a, b, c \neq 0$ and $d, e, g, h, i, j \in \mathbb{F}_p$.

After some reductions, we can assume that one of the equations $ib = ja$ and $4eg = c^2$ is not satisfied. The equation (3) can be rewritten as

$$(ay + bz)x - x'(ay' + bz') + dx^2 - e(y')^2 - cy'z' - g(z')^2 + hx - iy'$$

$$= d(x')^2 - ey^2 - cyz - gz^2 + hx' - iy - jz.$$

Let us view it as an incidence between a point set and a plane set as following:

$$P = \{(x, ay' + bz', dx^2 - e(y')^2 - cy'z' - g(z')^2 + hx - iy' - jz')\},$$

where $(x, y', z') \in U \times V \times W$.

$$S = \{(ay+bz)X - x'Y + Z = d(x')^2 - ey^2 - cyz - gz^2 + hx' - iy - jz\},$$

where $(x', y, z) \in U \times V \times W$.

Again, we estimate the sizes of P and S. For a given point $(u, v, w) \in P$, we now count the number of triples $(x, y', z') \in U \times V \times W$ such that

$$u = x, \quad v = ay' + bz', \quad w = dx^2 - e(y')^2 - cy'z' - g(z')^2 + hx - iy' - jz'.$$

These equations yield that

$$\left(b^2 e - abc + a^2 g\right)(y')^2 + \left(bcv - 2agv + ib^2 - jab\right) y'$$

$$+\left(b^2 w - b^2 du^2 + gv^2 - b^2 hx + bjv\right) = 0.$$

We now fall into the following two cases:

Case 1**:** If either $b^2e - abc + a^2g$ or $bcv - 2agv + ib^2 - jab$ is non-zero.
Case 2**:** If both $b^2e - abc + a^2g$ and $bcv - 2agv + ib^2 - jab$ are zero.
These cases actually make some steps very technical. But after all, we still get what we want that:

$$E \ll (UVW)^{3/2} + (V + W + U)(UVW).$$

Putting everything together. Sketch of the proof of the result. Since $\max_{(u,v,w)\in U\times V\times W} |\beta_{uvw}| \le 1$, we have

$$|S| \le \sum_{u\in,v\in,w\in} \left| \sum_{t\in} \alpha_t \chi(t + f(u,v,w)) \right|.$$

For $\lambda \in \mathbb{F}_p$, let $N(U,V,W,\lambda)$ be the number of solutions of the equation

$$f(u,v,w) = \lambda,$$

with $(u,v,w) \in U \times V \times W$.

It is clear that we have

$$\sum_{\lambda \in \mathbb{F}_p} N(U, V, W, \lambda) = UVW,$$

and

$$\sum_{\lambda \in \mathbb{F}_p} N(U, V, W, \lambda)^2 = E,$$

where E is the number of tuples $(u, v, w, u', v', w') \in (U \times V \times W)^2$ such that

$$f(u, v, w) = f(u', v', w').$$

Thus we have

$$|S| \leq \sum_{\lambda \in \mathbb{F}_p} N(U, V, W, \lambda) \left| \sum_{t \in T} \alpha_t \chi(t + \lambda) \right|.$$

Using the Hölder inequality, we have

$$|S|^{2n} \leq \left(\sum_{\lambda \in \mathbb{F}_p} \left| \sum_{t \in T} \alpha_t \chi(t + \lambda) \right|^{2n} \right) \cdot \left(\sum_{\lambda \in \mathbb{F}_p} N(U, V, W, \lambda)^{\frac{2n}{2n-1}} \right)^{2n-1}$$

$$\ll \left(\sum_{\lambda \in \mathbb{F}_p} N(U, V, W, \lambda) \right)^{2n-2} \left(\sum_{\lambda \in \mathbb{F}_p} N(U, V, W, \lambda)^2 \right)$$

$$\cdot \left(\sum_{\lambda \in \mathbb{F}_p} \left| \sum_{t \in T} \alpha_t \chi(t + \lambda) \right|^{2n} \right)$$

$$= (UVW)^{2n-2} \cdot E \cdot \left(\sum_{\lambda \in \mathbb{F}_p} \left| \sum_{t \in T} \alpha_t \chi(t + \lambda) \right|^{2n} \right).$$

Finally, the estimate is reduced to the estimate of

$$\left(\sum_{\lambda \in \mathbb{F}_p} \left| \sum_{t \in T} \alpha_t \chi(t+\lambda) \right|^{2n} \right).$$

Theorem (Iwaniec and Kowsalski)

For $T \subset \mathbb{F}_p^*$ *and a sequence of weights* $\alpha = (\alpha_t)_{t \in}$ *with* $\max_{t \in} |\alpha_t| \leq 1$, *and for any fixed integer* $n \geq 1$, *we have*

$$\sum_{\lambda \in \mathbb{F}_p} \left| \sum_{t \in} \alpha_t \chi(\lambda + t) \right|^{2n} \ll \begin{cases} Tp \;\; \text{if} \;\; n = 1 \\ T^{2n} p^{1/2} + T^n p \;\; \text{if} \;\; n \geq 2. \end{cases}$$

Therefore, we have

$$|S| \leq \left((UVW)^{1-\frac{1}{4n}} + M^{1/2n}(UVW)^{1-\frac{1}{2n}} + \frac{UVW}{U^{1/n}} \right) \cdot \begin{cases} T^{1/2}p^{1/2} & \text{if } n = 1 \\ Tp^{1/4n} + T^{1/2}p^{1/2n}. \end{cases}$$

It is joint work with Thang Pham, a postdoctoral fellow at UCSD.

Thank you for your attention.