J. Number Theory 129(2009), no. 2, 434–438

A Variant of Tao's Method with Application to Restricted Sumsets

Song Guo[1] and Zhi-Wei Sun[2]

[1]Department of Mathematics, Huaiyin Teachers College
Huaian 223300, People's Republic of China
guosong77@hytc.edu.cn

[2]Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Abstract

In this paper, we develop Terence Tao's harmonic analysis method and apply it to restricted sumsets. The well known Cauchy-Davenport theorem asserts that if $\emptyset \neq A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ with p a prime, then $|A+B| \geqslant \min\{p, |A|+|B|-1\}$, where $A+B = \{a+b:\ a \in A,\ b \in B\}$. In 2005, Terence Tao gave a harmonic analysis proof of the Cauchy-Davenport theorem, by applying a new form of the uncertainty principle on Fourier transform. We modify Tao's method so that it can be used to prove the following extension of the Erdős-Heilbronn conjecture: If A, B, S are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ with p a prime, then $\big|\{a+b:\ a \in A,\ b \in B,\ a-b \notin S\}\big| \geqslant \min\{p, |A|+|B|-2|S|-1\}$.

1 Introduction

Let p be a prime, and let A and B be two subsets of the finite field

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{r} = r + p\mathbb{Z}:\ r \in \mathbb{Z}\}.$$

Set

$$A+B = \{a+b:\ a \in A,\ b \in B\} \tag{1}$$

and

$$A \dot{+} B = \{a+b:\ a \in A,\ b \in B,\ a \neq b\}. \tag{2}$$

Keywords: Restricted sumsets; uncertainty principle; Erdős-Heilbronn conjecture.
2000 *Mathematics Subject Classifications:* Primary 11B75; Secondary 05A05, 11P99, 11T99.
The second author is supported by the National Natural Science Foundation of People's Republic of China.

The well-known Cauchy-Davenport theorem asserts that

$$|A+B| \geqslant \min\{p,\, |A|+|B|-1\}. \tag{3}$$

In 1964 P. Erdős and H. Heilbronn [5] conjectured that

$$|A\dot{+}A| \geqslant \min\{p,\, 2|A|-3\}; \tag{4}$$

this was confirmed by J. A. Dias da Silva and Y. O. Hamidoune [4] in 1994. In 1995-1996 N. Alon, M. B. Nathanson and I. Z. Ruzsa [2] proposed the so-called polynomial method to handle similar problems. By the powerful polynomial method (cf. [1] and [2]), many interesting results on restricted sumsets have been obtained (see, e.g., [7], [8], [10], [11], [12]).

In 2005, Terence Tao [13] developed a harmonic analysis method in this area, applying a new form of the uncertainty principle on Fourier transform. Let p be a prime. For a complex-valued function $f : \mathbb{Z}_p \to \mathbb{C}$, we define its support $\mathrm{supp}(f)$ and its Fourier transform $\hat{f} : \mathbb{Z}_p \to \mathbb{C}$ as follows:

$$\mathrm{supp}(f) = \{x \in \mathbb{Z}_p :\ f(x) \neq 0\} \tag{5}$$

and

$$\hat{f}(x) = \sum_{a\in\mathbb{Z}_p} f(a)e_p(ax) \quad \text{for all } x \in \mathbb{Z}_p, \tag{6}$$

where $e_p(\bar{r}) = e^{-2\pi i r/p}$ for any $r \in \mathbb{Z}$.

Here is the main result of the paper [13].

Theorem 1. (T. Tao [13]) *Let p be an odd prime. If $f : \mathbb{Z}_p \to \mathbb{C}$ is not identically zero, then*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geqslant p+1. \tag{7}$$

Moreover, given two non-empty subsets A and B of $\mathbb{Z}_p$ with $|A|+|B| \geqslant p+1$, we can find a function $f : \mathbb{Z}_p \to \mathbb{C}$ such that $\mathrm{supp}(f) = A$ and $\mathrm{supp}(\hat{f}) = B$.

Using this theorem Tao [13] gave a new proof of Cauchy-Davenport theorem. Note that the inequality (7) was also discovered independently by Andráas Biró (cf. [6] and [13]). In this article we adapt the method further and use the refined method to deduce the following result.

Theorem 2. *Let A and B be non-empty subsets of $\mathbb{Z}_p$ with p a prime, and let*

$$C = \{a+b :\ a \in A,\, b \in B,\, a-b \notin S\} \tag{8}$$

with $S \subseteq \mathbb{Z}_p$. Then we have

$$|C| \geqslant \min\{p,\, |A|+|B|-2|S|-1\}. \tag{9}$$

Theorem 2 in the case $S = \emptyset$ reduces to the Cauchy-Davenport theorem. When $A = B$ and $S = \{0\}$, Theorem 2 yields the Erdős-Heilbronn conjecture. In the case $p \neq 2$ and $\emptyset \neq S \subset \mathbb{Z}_p$, Pan and Sun [10, Corollary 2] obtained the stronger inequality

$$|C| \geqslant \min\{p,\, |A| + |B| - |S| - 2\} \tag{10}$$

via the polynomial method. The second author (cf. [7]) ever conjectured that 2 in (10) can be replaced by 1 if $|S|$ is even. We conjecture that when $A \neq B$ we can also substitute 1 for 2 in (10).

2 Proof of Theorem 2

Without loss of generality, we let $|A| \leqslant |B|$. When $|A| + |B| \leqslant 2|S| + 1$ or $|A| = 1$, (9) holds trivially. Below we suppose that $|A| + |B| > 2|S| + 1$ and $|A| \geqslant 2$.

In the case $p = 2$, we have $A = B = \mathbb{Z}_2$ and $C = (A + B) \setminus S = \mathbb{Z}_2 \setminus S$, thus

$$|C| = 2 - |S| \geqslant \min\{2,\, |A| + |B| - 2|S| - 1\} = \min\{2,\, 3 - 2|S|\}.$$

Below we assume that p is an odd prime. Set $k = p - |A| + 1 \in [1, p-1]$ and $l = p - |B| + 1 \in [1, p-1]$. Then $k + l \leqslant 2p - 2|S|$ and $l \leqslant p - |S|$ since $2|B| \geqslant |A| + |B| \geqslant 2|S| + 2$. Define

$$\hat{A} = \{\bar{0}, \ldots, \overline{k-1}\} = \{\bar{0}, \ldots, \overline{p - |A|}\} \tag{11}$$

and

$$\hat{B} = \{\overline{p - |S| - l + 1}, \ldots, \overline{p - |S|}\} = \{\overline{|B| - |S|}, \ldots, \overline{p - |S|}\}. \tag{12}$$

Clearly, $|\hat{A}| = p + 1 - |A|$ and $|\hat{B}| = p + 1 - |B|$. By Theorem 1 there are functions $f, g : \mathbb{Z}_p \to \mathbb{C}$ such that

$$\mathrm{supp}(f) = A,\ \mathrm{supp}(\hat{f}) = \hat{A},\ \mathrm{supp}(g) = B,\ \mathrm{supp}(\hat{g}) = \hat{B}. \tag{13}$$

Now we define a function $F : \mathbb{Z}_p \to \mathbb{C}$ by

$$F(x) = \sum_{a \in \mathbb{Z}_p} f(a) g(x - a) \prod_{d \in S} (e_p(x - a) - e_p(a - d)). \tag{14}$$

For each $x \in \mathrm{supp}(F)$, there exists $a \in \mathrm{supp}(f)$ with $x - a \in \mathrm{supp}(g)$ and $d := a - (x - a) \notin S$, hence $x = a + (x - a) \in C$. Therefore

$$\mathrm{supp}(F) \subseteq C. \tag{15}$$

For any $x \in \mathbb{Z}$ we have

$$\hat{F}(x) = \sum_{b \in \mathbb{Z}_p} F(b) e_p(bx) = \sum_{a \in \mathbb{Z}_p} \sum_{b \in \mathbb{Z}_p} f(a) g(b-a) e_p(bx) P(a,b),$$

where

$$\begin{aligned} P(a,b) &= \prod_{d \in S} (e_p(b-a) - e_p(a-d)) \\ &= \sum_{T \subseteq S} (-1)^{|T|} e_p\left((|S|-|T|)(b-a)\right) e_p\left(|T|a - \sum_{d \in T} d\right). \end{aligned}$$

Therefore

$$\begin{aligned} \hat{F}(x) = &\sum_{T \subseteq S} (-1)^{|T|} e_p\left(-\sum_{d \in T} d\right) \sum_{a \in \mathbb{Z}_p} f(a) e_p(ax + |T|a) \\ &\times \sum_{b \in \mathbb{Z}_p} g(b-a) e_p\left((b-a)x + (|S|-|T|)(b-a)\right) \\ = &\sum_{T \subseteq S} (-1)^{|T|} e_p\left(-\sum_{d \in T} d\right) \hat{f}\left(x + \overline{|T|}\right) \hat{g}\left(x + \overline{|S|-|T|}\right). \end{aligned}$$

For $T \subseteq S$, if $\overline{p-|S|} + \overline{|S|-|T|} \in \mathrm{supp}(\hat{g}) = \hat{B}$, then we must have $|T| = |S|$ (i.e., $T = S$) by the definition of $\hat{B}$. It follows that

$$\hat{F}\left(\overline{p-|S|}\right) = (-1)^{|S|} e_p\left(-\sum_{d \in S} d\right) \hat{f}\left(\overline{0}\right) \hat{g}\left(\overline{p-|S|}\right) \neq 0$$

since $\overline{0} \in \hat{A} = \mathrm{supp}(\hat{f})$ and $\overline{p-|S|} \in \hat{B} = \mathrm{supp}(\hat{g})$. With the helps of (15) and Theorem 1, we get

$$|C| \geqslant |\mathrm{supp}(F)| \geqslant p + 1 - |\mathrm{supp}(\hat{F})|.$$

Suppose that $x \in \mathrm{supp}(\hat{F})$. By the above, there is a subset T of S such that $x + \overline{|T|} \in \mathrm{supp}(\hat{f}) = \hat{A}$ and $x + \overline{|S|-|T|} \in \mathrm{supp}(\hat{g}) = \hat{B}$. As $0 \leqslant |T| \leqslant |S|$,

$$x + \overline{|T|} \in \hat{A} \Longrightarrow x \in \{\overline{p-|S|}, \ldots, \overline{p-1}, \overline{0}, \ldots, \overline{k-1}\}$$

and

$$x + \overline{|S|-|T|} \in \hat{B} \Longrightarrow x \in \{\overline{|B|-2|S|}, \ldots, \overline{p-|S|}\}.$$

Therefore $x = \overline{p-|S|}$, or $x = \overline{r}$ for some $r \in [|B|-2|S|, \, k-1]$.

If $|A| + |B| \geqslant p + 2|S| + 1$, then $k - 1 = p - |A| < |B| - 2|S|$, hence $\mathrm{supp}(\hat{F}) = \{\overline{p-|S|}\}$ and thus $|C| \geqslant p$. If $|A| + |B| < p + 2|S| + 1$, then

$$|\mathrm{supp}(\hat{F})| \leqslant 1 + k - (|B| - 2|S|) = k + l - p + 2|S|$$

and hence

$$|C| \geqslant p + 1 - k - l + p - 2|S| = |A| + |B| - 2|S| - 1.$$

So (9) always holds. We are done.

Acknowledgment. The authors are grateful to the referee for his/her helpful comments.

References

[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Prob. Comput. **8**(1999), 7–29.

[2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, J. Number Theory **56**(1996), 404–417.

[3] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. **10**(1935), 30–32.

[4] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. **26**(1994), 140–146.

[5] P. Erdős and H. Heilbronn, *On the addition of residue classes modulo p*, Acta Arith. **9**(1964), 149–159.

[6] P. E. Frenkel, *Simple proof of Chebotarëv's theorem on roots of unity*, preprint, `arXiv:math.AC/0312398` (version 3), 2004.

[7] Q. H. Hou and Z. W. Sun, *Restricted sums in a field*, Acta Arith. **102**(2002), 239–249.

[8] J. X. Liu and Z. W. Sun, *Sums of subsets with polynomial restrictions*, J. Number Theory **97**(2002), 301–304.

[9] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math., 165, Springer, New York, 1996.

[10] H. Pan and Z. W. Sun, *A lower bound for* $|\{a+b:\ a \in A,\ b \in B,\ P(a,b) \neq 0\}|$, J. Combin. Theory Ser. A **100**(2002), 387–393.

[11] H. Pan and Z. W. Sun, *Restricted sumsets and a conjecture of Lev*, Israel J. Math. **154**(2006), 21–28.

[12] Z. W. Sun, *On Snevily's conjecture and restricted sumsets*, J. Combin. Theory Ser. A **103**(2003), 291–304.

[13] Terence Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. **12**(2005), 121–127.