On sumsets in $\mathbb{F}_2^n$

Chaohua Jia

Abstract. Let $\mathbb{F}_2$ be the finite field of two elements, $\mathbb{F}_2^n$ be the vector space of dimension $n$ over $\mathbb{F}_2$. For sets $A, B \subseteq \mathbb{F}_2^n$, their sumset is defined as the set of all pairwise sums $a + b$ with $a \in A, b \in B$.

Ben Green and Terence Tao proved that, let $K \geq 1$, if $A, B \subseteq \mathbb{F}_2^n$ and $|A + B| \leq K|A|^\frac{3}{2}|B|^\frac{1}{2}$, then there exists a subspace $H \subseteq \mathbb{F}_2^n$ with

$$|H| \gg \exp(-O(\sqrt{K} \log K))|A|$$

and $x, y \in \mathbb{F}_2^n$ such that

$$|A \cap (x + H)|^\frac{1}{2}|B \cap (y + H)|^\frac{1}{2} \geq \frac{1}{2K}|H|.$$ 

In this note, we shall use the method of Green and Tao with some modification to prove that if

$$|H| \gg \exp(-O(\sqrt{K})|A|),$$

then the above conclusion still holds true.

1. Introduction

Let $\mathbb{F}_2$ be the finite field of two elements, $\mathbb{F}_2^n$ be the vector space of dimension $n$ over $\mathbb{F}_2$. For sets $A, B \subseteq \mathbb{F}_2^n$, their sumset $A + B$ is defined as

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

In 1999, Ruzsa[4] proved the following theorem.

**Theorem 1** (Ruzsa). Let $K \geq 1$ be an integer, and suppose that set $A \subseteq \mathbb{F}_2^n$ with $|A + A| \leq K|A|$. Then $A$ is contained in a subspace $H \subseteq \mathbb{F}_2^n$ with $|H| \leq F(K)|A|$, where $F(K) = K^22^{K^4}$.

This result was improved by Sanders[5] to $F(K) = 2^{O(K^{\frac{3}{2}} \log K)}$ in 2008 and then improved by Green and Tao[2] to $F(K) = 2^{2K+O(\sqrt{K} \log K)}$ in 2009. The bound $F(K) = 2^{2K+O(\sqrt{K} \log K)}$ is almost best possible.

If we do not require that the subspace $H$ contains the set $A$ completely but contains a part of $A$, then related bounds can be further improved.
The following theorem was given in [1] and some explanations on it could be found in the introduction of [3].

**Theorem 2.** Suppose that $K \geq 1$ and that $A \subseteq \mathbb{F}_2^n$ with $|A + A| \leq K|A|$. Then there is a subspace $H \subseteq \mathbb{F}_2^n$ with $|H| \ll K^{O(1)}|A|$ such that

$$|A \cap H| \gg \exp(-K^{O(1)}|A|).$$

If we permit to replace the subspace $H$ by translates of it, then better bounds could be obtained. In 2009, Green and Tao[3] obtained the following result.

**Theorem 3 (Green-Tao).** Let $K \geq 1$, if $A, B \subseteq \mathbb{F}_2^n$ and $|A + B| \leq K|A|^\frac{1}{2}|B|^\frac{1}{2}$, then there exists a subspace $H \subseteq \mathbb{F}_2^n$ with

$$|H| \gg \exp(-O(\sqrt{K \log K})|A|)$$

and $x, y \in \mathbb{F}_2^n$ such that

$$|A \cap (x + H)|^\frac{1}{2}|B \cap (y + H)|^\frac{1}{2} \geq \frac{1}{2K}|H|.$$

In this note, we shall use the method of Green and Tao with some modification to prove the following theorem.

**Theorem 4.** Let $K \geq 1$, if $A, B \subseteq \mathbb{F}_2^n$ and $|A + B| \leq K|A|^\frac{1}{2}|B|^\frac{1}{2}$, then there exists a subspace $H \subseteq \mathbb{F}_2^n$ with

$$|H| \gg \exp(-O(\sqrt{K})|A|)$$

and $x, y \in \mathbb{F}_2^n$ such that

$$|A \cap (x + H)|^\frac{1}{2}|B \cap (y + H)|^\frac{1}{2} \geq \frac{1}{2K}|H|.$$

2. Definitions

In this section we shall introduce some definitions given in [3].

**Definition 1 (normalized energy).** For non-empty sets $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$, define the normalized energy

$$\omega(A_1, A_2, A_3, A_4) := \frac{1}{(|A_1||A_2||A_3||A_4|)^\frac{1}{2}} \left| \{(a_1, a_2, a_3, a_4) \in A_1 \times A_2 \times A_3 \times A_4 : a_1 + a_2 + a_3 + a_4 = 0\} \right|.$$
It was shown in [3] that
\[ 0 \leq \omega(A_1, A_2, A_3, A_4) \leq 1. \]  
\[ (1) \]

**Definition 2** (Fourier transform). For \( f : \mathbb{F}_2^n \to \mathbb{R} \), define the Fourier transform \( \hat{f} : \mathbb{F}_2^n \to \mathbb{R} \) by
\[ \hat{f}(\xi) := \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\xi \cdot x}, \]
where
\[ \xi \cdot x = (\xi_1, \ldots, \xi_n) \cdot (x_1, \ldots, x_n) = \xi_1 x_1 + \cdots + \xi_n x_n. \]

**Definition 3** (spectrum). If \( A \subseteq \mathbb{F}_2^n \) is non-empty and \( 0 < \alpha \leq 1 \), define the \( \alpha \)-spectrum
\[ \text{Spec}_\alpha(A) := \{ \xi \in \mathbb{F}_2^n : |\mathbf{1}_A(\xi)| \geq \alpha |A|/2^n \}, \]
where \( \mathbf{1}_A(x) \) is the indicator function of set \( A \).

**Definition 4** (coherently flat quadruples). Suppose that \( A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n \) are non-empty and \( \delta \in (0, 1/2) \) is a small parameter. If for each \( \xi \in \mathbb{F}_2^n \), one of the following conditions is satisfied:
1) \( \xi \in \text{Spec}_\frac{3}{10}(A_i) \) for all \( i = 1, 2, 3, 4 \);
2) \( \xi \not\in \text{Spec}_\delta(A_i) \) for all \( i = 1, 2, 3, 4 \),
we say that the quadruple \( (A_1, A_2, A_3, A_4) \) is coherently \( \delta \)-flat.

3. The proof of Theorem 4

**Lemma 1.** Let \( J \geq 1 \). Suppose that \( (A_1, A_2, A_3, A_4) \) is a coherently \( \frac{1}{\sqrt{2J}} \)-flat quadruple, the normalized energy of which satisfies
\[ \omega(A_1, A_2, A_3, A_4) \geq \frac{1}{J}. \]

Then there is a subspace \( H \subseteq \mathbb{F}_2^n \) with \( x_1, x_2, x_3, x_4 \in \mathbb{F}_2^n \) such that
\[ H \geq \frac{4}{5} (|A_1||A_2||A_3||A_4|)^{\frac{1}{4}}, \]
and
\[ \prod_{i=1}^{4} |A_i \cap (x_i + H)|^{\frac{1}{4}} \geq \frac{1}{2J} |H|. \]

(2)
This is Proposition 2.4 in [3].

Let
\[
\text{Dbl}(A, B) := \frac{|A + B|}{|A|^2 |B|^2}.
\]

Since
\[
|A + B| \geq \max(|A|, |B|),
\]
we have
\[
\text{Dbl}(A, B) \geq 1. \tag{4}
\]

**Lemma 2.** Suppose that \(A, B \subseteq \mathbb{F}_2^q\) are non-empty and that for \(J \geq 1\),
\[
\text{Dbl}(A, B) \leq J.
\]

If \((A, B, A, B)\) is not coherently \(\frac{1}{\sqrt{2J}}\)-flat, then there are \(A' \subseteq A, B' \subseteq B\) such that
\[
|A'| \geq \frac{1}{20} |A|, \quad |B'| \geq \frac{1}{20} |B| \tag{5}
\]
and
\[
\text{Dbl}(A', B') \leq \frac{J}{1 + \frac{1}{100\sqrt{J}}}. \tag{6}
\]

**Proof.** By the supposition, there is \(\xi \in \mathbb{F}_2^q\) such that
\[
\xi \notin \text{Spec}_{\frac{1}{\sqrt{2J}}} (A) \cap \text{Spec}_{\frac{1}{\sqrt{2J}}} (B) \tag{7}
\]
and
\[
\xi \in \text{Spec}_{\frac{1}{\sqrt{2J}}} (A) \cup \text{Spec}_{\frac{1}{\sqrt{2J}}} (B). \tag{8}
\]

By (7), \(\xi \neq 0\). Write
\[
A_0 := \{ x \in A : x \cdot \xi = 0 \}, \quad A_1 := \{ x \in A : x \cdot \xi = 1 \},
\]
\[
B_0 := \{ x \in B : x \cdot \xi = 0 \}, \quad B_1 := \{ x \in B : x \cdot \xi = 1 \}.
\]

If \(|A_0| \geq \frac{1}{2} |A|\), we write \(\alpha := \frac{|A_0|}{|A|}\). Otherwise, \(|A_0| < \frac{1}{2} |A| \Rightarrow |A_1| = |A| - |A_0| \geq |A| - \frac{1}{2} |A| = \frac{1}{2} |A|\). Then we write \(\alpha := \frac{|A_1|}{|A|}\). Without loss of generality, we can suppose that \(|A_0| \geq \frac{1}{2} |A|\) and write
\[
\alpha := \frac{|A_0|}{|A|},
\]
Similarly, we can also suppose that $|B_0| \geq \frac{1}{2}|B|$ and write

$$\beta := \frac{|B_0|}{|B|}.$$  

We have

$$\alpha \geq \frac{1}{2}, \quad \beta \geq \frac{1}{2} \quad (9)$$

By

$$|\hat{1}_A(\xi)| = \left| \frac{1}{2^n} \sum_{x \in A} (-1)^x \xi \right|$$

$$= \left| \frac{1}{2^n} \left( \sum_{x \in A_0} (-1)^x \xi + \sum_{x \in A_1} (-1)^x \xi \right) \right|$$

$$= \left| \frac{1}{2^n} \left( |A_0| - |A_1| \right) \right|$$

$$= \left| \frac{1}{2^n} \left( 2|A_0| - |A| \right) \right|$$

$$= (2\alpha - 1) \cdot \frac{|A|}{2^n}$$

and

$$|\hat{1}_B(\xi)| = (2\beta - 1) \cdot \frac{|B|}{2^n},$$

we know that the condition (7) is equivalent to

$$2\alpha - 1 < \frac{9}{10} \quad \text{or} \quad 2\beta - 1 < \frac{9}{10}. \quad (10)$$

and the condition (8) is equivalent to

$$2\alpha - 1 \geq \frac{1}{\sqrt{2J}} \quad \text{or} \quad 2\beta - 1 \geq \frac{1}{\sqrt{2J}}. \quad (11)$$

Without loss of generality, we suppose that

$$\beta \geq \alpha \quad (12)$$

and consider

$$|B_0 + A_0| + |B_0 + A_1|.$$  

If $\beta < \alpha$, we shall consider $|A_0 + B_0| + |A_0 + B_1|.$

It is easy to see that sets $B_0 + A_0$ and $B_0 + A_1$ are disjoint. Hence,

$$|B_0 + A_0| + |B_0 + A_1| \leq |B + A| \leq J|B|^{\frac{1}{2}}|A|^{\frac{1}{2}}.$$
or

\[
\frac{|B_0 + A_0|}{|B_0|^\frac{1}{2}|A_0|^\frac{1}{2}} \cdot \frac{|B_0|^\frac{1}{2}|A_0|^\frac{1}{2}}{\frac{1}{2}} + \frac{|B_0 + A_1|}{|B_0|^\frac{1}{2}|A_1|^\frac{1}{2}} \cdot \frac{|B_0|^\frac{1}{2}|A_1|^\frac{1}{2}}{\frac{1}{2}} \leq J. \tag{13}
\]

Let

\[
\Psi := \min\left(\frac{|B_0 + A_0|}{|B_0|^\frac{1}{2}|A_0|^\frac{1}{2}}, \frac{|B_0 + A_1|}{|B_0|^\frac{1}{2}|A_1|^\frac{1}{2}}\right).
\]

It follows from (13) that

\[
\Psi(\beta^\frac{1}{2} \alpha^\frac{1}{2} + \beta^\frac{1}{2}(1 - \alpha)^\frac{1}{2}) \leq J. \tag{14}
\]

Under the supposition (12), the condition (10) is equivalent to

\[
\alpha < \frac{19}{20}, \tag{15}
\]

and the condition (11) is equivalent to

\[
\beta \geq \frac{1}{2} + \frac{1}{2\sqrt{2J}}. \tag{16}
\]

We shall discuss in the following two cases.

Case 1. \(\frac{1}{2} + \frac{1}{2\sqrt{2J}} \leq \alpha < \frac{19}{20}\).

By (12),

\[
\beta^\frac{1}{2} \alpha^\frac{1}{2} + \beta^\frac{1}{2}(1 - \alpha)^\frac{1}{2} \geq \alpha + \alpha^\frac{1}{2}(1 - \alpha)^\frac{1}{2}.
\]

The discussion in [3] yields that

\[
\alpha + \alpha^\frac{1}{2}(1 - \alpha)^\frac{1}{2} \geq \alpha + 2\alpha(1 - \alpha)
\]

\[
= 1 + (2\alpha - 1)(1 - \alpha) \geq 1 + \frac{1}{20\sqrt{2J}}.
\]

Hence,

\[
\beta^\frac{1}{2} \alpha^\frac{1}{2} + \beta^\frac{1}{2}(1 - \alpha)^\frac{1}{2} \geq 1 + \frac{1}{20\sqrt{2J}}.
\]

Case 2. \(\frac{1}{2} \leq \alpha < \frac{1}{2} + \frac{1}{2\sqrt{2J}}\).

It follows from (16) that

\[
\beta^\frac{1}{2} \alpha^\frac{1}{2} + \beta^\frac{1}{2}(1 - \alpha)^\frac{1}{2} \geq \left(\frac{1}{2} + \frac{1}{2\sqrt{2J}}\right)^\frac{1}{2}(\alpha^\frac{1}{2} + (1 - \alpha)^\frac{1}{2}).
\]

Let

\[
f(\alpha) = \alpha^\frac{1}{2} + (1 - \alpha)^\frac{1}{2}.
\]
Since \( f'(\alpha) = \frac{1}{2\sqrt{\alpha}} - \frac{1}{2\sqrt{1-\alpha}} \leq 0 \),
the function \( f(\alpha) \) is decreasing monotonically. Thus,
\[
\alpha^{\frac{1}{2}} + (1 - \alpha)^{\frac{1}{2}} \geq \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right)^{\frac{1}{2}} + \left( 1 - \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right) \right)^{\frac{1}{2}}.
\]

Hence,
\[
\beta^{\frac{1}{2}} \alpha^{\frac{1}{2}} + \beta^{\frac{1}{2}}(1 - \alpha)^{\frac{1}{2}} 
\geq \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right)^{\frac{1}{2}} \left( \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right)^{\frac{1}{2}} + \left( 1 - \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right) \right)^{\frac{1}{2}} \right) 
= \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right) + \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right)^{\frac{1}{2}} \left( 1 - \left( \frac{1}{2} + \frac{1}{2\sqrt{2J}} \right) \right)^{\frac{1}{2}}
\]
which is the value of function \( \alpha + \alpha^{\frac{1}{2}}(1 - \alpha)^{\frac{1}{2}} \) at \( \alpha = \frac{1}{2} + \frac{1}{2\sqrt{2J}} \). By the discussion in Case 1, we have
\[
\beta^{\frac{1}{2}} \alpha^{\frac{1}{2}} + \beta^{\frac{1}{2}}(1 - \alpha)^{\frac{1}{2}} \geq 1 + \frac{1}{2\sqrt{2J}}.
\]
Combining the above two cases, we get
\[
\Psi \leq \frac{J}{1 + \frac{1}{20\sqrt{2J}}} \leq \frac{J}{1 + \frac{1}{100\sqrt{J}}}.
\]
Take \( B' = B_0, A' = A_0 \) or \( A_1 \) such that
\[
\Psi = \text{Dbl}(A', B').
\]
Then
\[
\text{Dbl}(A', B') \leq \frac{J}{1 + \frac{1}{100\sqrt{J}}}.
\]
Since
\[
|A_0| \geq \frac{1}{2} |A|, \quad |A_1| = |A| - |A_0| \geq |A| - \frac{19}{20} |A| = \frac{1}{20} |A|,
\]
we have
\[
|A'| \geq \frac{1}{20} |A|.
\]
We also have
\[
|B'| \geq \frac{1}{20} |B|.
\]
So far the proof of Lemma 2 is finished.

**Lemma 3.** Suppose that \( A, B \subseteq \mathbb{F}_2^n \) are non-empty and that for \( K \geq 1 \),
\[
\text{Dbl}(A, B) \leq K.
\]

Then there are \( A' \subseteq A, B' \subseteq B \) with
\[
|A'| \gg \exp(-O(\sqrt{K}))|A|, \quad |B'| \gg \exp(-O(\sqrt{K}))|B|
\]
such that for some \( J(1 \leq J \leq K) \),
\[
\text{Dbl}(A', B') \leq J \tag{17}
\]
and \((A', B', A', B')\) is coherently \( \frac{1}{\sqrt{2J}} \)-flat.

**Proof.** Take \( K_1 = K \). If \((A, B, A, B)\) is coherently \( \frac{1}{\sqrt{2K}} \)-flat, then the conclusion holds true.

If \((A, B, A, B)\) is not coherently \( \frac{1}{\sqrt{2K}} \)-flat, Lemma 2 produces that there are \( A'' \subseteq A \), \( B'' \subseteq B \) with
\[
|A''| \geq \frac{1}{20}|A|, \quad |B''| \geq \frac{1}{20}|B|
\]
such that
\[
\text{Dbl}(A'', B'') \leq \frac{K_1}{1 + \frac{1}{100\sqrt{K_1}}}.
\]
Then take
\[
K_2 = \frac{K_1}{1 + \frac{1}{100\sqrt{K_1}}},
\]
and for \( A'', B'' \) and \( K_2 \), repeat the above process.

Since \( \text{Dbl} \geq 1 \), this process has to stop after finite steps. We get a sequence \( K_1 = K, K_2, \ldots, K_m = J \) with
\[
K_{i+1} = \frac{K_i}{1 + \frac{1}{100\sqrt{K_i}}}, \quad i = 1, 2, \ldots, m - 1
\]
and \( A' \subseteq A, B' \subseteq B \) with
\[
|A'| \gg \frac{1}{(20)^m}|A|, \quad |B'| \gg \frac{1}{(20)^m}|B|
\]
such that
\[
\text{Dbl}(A', B') \leq J
\]
and \((A', B', A', B')\) is coherently \(\frac{1}{\sqrt{2}}\)-flat.

We distribute \(K_i\) into intervals

\[
\left(\frac{K}{e^{r+1}}, \frac{K}{e^r}\right), \left(\frac{K}{e^r}, \frac{K}{e^{r-1}}\right), \ldots, \left(\frac{K}{e^2}, \frac{K}{e}\right), \left(\frac{K}{e}, K\right), \quad r = [\log K].
\]

For the given interval \((\frac{K}{e^{s+1}}, \frac{K}{e^s})\)\((0 \leq s \leq r)\), if \(K_l\) and \(K_{l+j}(j \geq 1) \in (\frac{K}{e^{s+1}}, \frac{K}{e^s})\), we have

\[
\frac{K}{e^{s+1}} \leq K_{l+j} = \frac{K_{l+j-1}}{1 + \frac{1}{100\sqrt{K_{l+j-1}}}} \leq \frac{K_{l+j-1}}{1 + \frac{1}{100\sqrt{K_{l+j-1}}}} \leq \ldots
\]

\[
\leq \frac{K_l}{\left(1 + \frac{1}{100\sqrt{\frac{K}{e^s}}}\right)^j} \leq \frac{K_l}{\left(1 + \frac{1}{100\sqrt{\frac{K}{e^s}}}\right)^j} \leq \frac{1}{e^s} \cdot \left(1 + \frac{1}{100\sqrt{\frac{K}{e^s}}}\right)^j.
\]

Thus

\[
\left(1 + \frac{1}{100\sqrt{\frac{K}{e^s}}}\right)^j \leq e,
\]

\[
j \cdot \frac{1}{\sqrt{\frac{K}{e^s}}} \ll j \log\left(1 + \frac{1}{100\sqrt{\frac{K}{e^s}}}\right) \leq 1,
\]

\[
j \ll \sqrt{\frac{K}{e^s}}.
\]

Hence, the number of \(K_i\) dropping into the interval \((\frac{K}{e^{s+1}}, \frac{K}{e^s})\) is \(\ll \sqrt{\frac{K}{e^s}}\).

For the total number of \(K_i\), we have

\[
m \ll \sqrt{K} + \sqrt{\frac{K}{e}} + \sqrt{\frac{K}{e^2}} + \cdots + \sqrt{\frac{K}{e^s}}
\]

\[
\leq \sqrt{K}\left(1 + \frac{1}{\sqrt{e}} + \frac{1}{(\sqrt{e})^2} + \frac{1}{(\sqrt{e})^3} + \cdots\right)
\]

\[
\ll \sqrt{K}.
\]

Therefore

\[
|A'| \gg \exp(-O(\sqrt{K}))|A|, \quad |B'| \gg \exp(-O(\sqrt{K}))|B|.
\]

So far the proof of Lemma 3 is finished.

**The proof of Theorem 4.** We take \(A', B'\) in Lemma 3 with required properties. It is shown in [3] that

\[
\omega(A', B', A', B') \geq \frac{1}{\text{Dbl}(A', B')} \geq \frac{1}{J}.
\]
Lemma 1 claims that there is a subspace \( H \subseteq \mathbb{F}_2^n \) with \( x_1, x_2, x_3, x_4 \in \mathbb{F}_2^n \) such that
\[
H \geq \frac{4}{5} |A'| \frac{1}{2} |B'| \frac{1}{2} \gg \exp(-O(\sqrt{K})) |A| \frac{1}{2} |B| \frac{1}{2}
\]
and
\[
|A \cap (x_1 + H)| \frac{1}{2} |B \cap (x_2 + H)| \frac{1}{2} |A \cap (x_3 + H)| \frac{1}{2} |B \cap (x_4 + H)| \frac{1}{2} \\
\geq \frac{1}{2J} |H| \geq \frac{1}{2K} |H|.
\]
Since
\[
|A| \leq |A + B| \leq K |A| \frac{1}{2} |B| \frac{1}{2},
\]
we have
\[
K^{-2} |A| \leq |B|,
\]
hence
\[
H \gg \exp(-O(\sqrt{K})) |A|.
\]
Without loss of generality, we can suppose that
\[
|A \cap (x_1 + H)| \geq |A \cap (x_3 + H)|, \quad |B \cap (x_2 + H)| \geq |B \cap (x_4 + H)|,
\]
hence
\[
|A \cap (x_1 + H)| \frac{1}{2} |B \cap (x_2 + H)| \frac{1}{2} \geq \frac{1}{2K} |H|.
\]
So far the proof of Theorem 4 is finished.

**Acknowledgements**

In April 2012, Quanhui Yang of Nanjing Normal University gave a talk in “ergodic prime number theorem 2012” seminar in Morningside Mathematical Center of the Chinese Academy of Sciences in Beijing to introduce some results in the paper [3]. I would like to thank Quanhui Yang for his talk which attracts my interest to this topic. I also thank all my colleagues and friends in this seminar for helpful discussion.
References

[1] B. Green and T. Sanders, *Boolean functions with small spectral norm*, GAFA, **18**(2008), no.1, 144-162.

[2] B. Green and T. Tao, *Freiman’s theorem in finite fields via extremal set theory*, Combinatorics, Probability and Computing, **18**(2009), no.3, 335-355.

[3] B. Green and T. Tao, *A note on the Freiman and Balog-Szemerédi-Gowers theorems in finite fields*, J. Australian Math. Soc., **86**(2009), 61-74.

[4] I. Z. Ruzsa, *An analog of Freiman’s theorem in groups*, Structure theory of set addition, Astérisque, **258**(1999), 323-326.

[5] T. Sanders, *A note on Freiman’s theorem in vector spaces*, Combinatorics, Probability and Computing, **17**(2008), no.2, 297-305.

Institute of Mathematics, Academia Sinica, Beijing 100190, P. R. China
E-mail: jiach@math.ac.cn