



关于 $\mathbb{F}_2^n$ 中的和集

贾朝华^{①②}

① 中国科学院数学与系统科学研究院数学研究所, 北京 100190;

② 中国科学院华罗庚数学重点实验室, 北京 100190

E-mail: jiach@math.ac.cn

收稿日期: 2012-06-02; 接受日期: 2012-11-15

国家自然科学基金 (批准号: 11071235) 和国家重点基础研究发展计划 (973 计划) (批准号: 2013CB834202) 资助项目

摘要 设 $\mathbb{F}_2$ 为两个元素组成的有限域, $\mathbb{F}_2^n$ 为 $\mathbb{F}_2$ 上的 n 维向量空间. 对于集合 $A, B \subseteq \mathbb{F}_2^n$, 它们的和集定义为所有两两互异的和 $a+b$ 所组成的集合, 其中 $a \in A, b \in B$. Green 和 Tao 证明了: 设 $K \geq 1$, 如果 $A, B \subseteq \mathbb{F}_2^n$ 且 $|A+B| \leq K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$, 则存在一个子空间 $H \subseteq \mathbb{F}_2^n$ 满足

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

以及 $x, y \in \mathbb{F}_2^n$, 使得

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

本文我们将使用 Green 和 Tao 的方法并作一些修改, 证明如果

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

则以上的结论仍然成立.

关键词 和集 正规化能量 协同平坦四元组**MSC (2010) 主题分类** 11T30

1 引言

设 $\mathbb{F}_2$ 为两个元素组成的有限域, $\mathbb{F}_2^n$ 为 $\mathbb{F}_2$ 上的 n 维向量空间. 对于集合 $A, B \subseteq \mathbb{F}_2^n$, 它们的和集 $A+B$ 定义为

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

1999 年, Ruzsa^[1] 证明了如下的定理.

定理 1^[1] 令 $K \geq 1$ 为整数. 假设集合 $A \subseteq \mathbb{F}_2^n$ 满足 $|A+A| \leq K|A|$, 则 A 包含在一个子空间 $H \subseteq \mathbb{F}_2^n$ 中, 这里 $|H| \leq F(K)|A|$, 而 $F(K) = K^2 2^{K^4}$.

这个结果被 Sanders^[2] 改进为 $F(K) = 2^{O(K^{\frac{3}{2}} \log K)}$, 又被 Green 和 Tao^[3] 改进为 $F(K) = 2^{2K+O(\sqrt{K} \log K)}$. 界 $F(K) = 2^{2K+O(\sqrt{K} \log K)}$ 几乎是最佳可能的.

如果我们不要求子空间 H 完全包含集合 A , 而只是包含 A 的一部分, 则相关的界可以进一步改进. 下面的定理在文献 [4] 中给出, 关于它的一些说明可见文献 [5] 的引言.

定理 2 假设 $K \geq 1$, $A \subseteq \mathbb{F}_2^n$ 满足 $|A+A| \leq K|A|$, 则有一个子空间 $H \subseteq \mathbb{F}_2^n$ 满足 $|H| \ll K^{O(1)}|A|$, 使得

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

如果我们允许将子空间 H 用它的平移来代替, 则可得到更好的界. 2009 年, Green 和 Tao [5] 得到了下面的结果.

定理 3 [5] 设 $K \geq 1$, 如果 $A, B \subseteq \mathbb{F}_2^n$ 且 $|A+B| \leq K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$, 则存在一个子空间 $H \subseteq \mathbb{F}_2^n$ 满足

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

以及 $x, y \in \mathbb{F}_2^n$, 使得

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

本文我们将使用 Green 和 Tao 的方法并作一些修改, 证明如下的定理.

定理 4 设 $K \geq 1$, 如果 $A, B \subseteq \mathbb{F}_2^n$ 且 $|A+B| \leq K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$, 则存在一个子空间 $H \subseteq \mathbb{F}_2^n$ 满足

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

以及 $x, y \in \mathbb{F}_2^n$, 使得

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

2 一些定义

本节我们将引入文献 [5] 中给出的一些定义.

定义 5 (正规化能量) 对于非空集合 $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$, 定义正规化能量

$$\omega(A_1, A_2, A_3, A_4) := \frac{1}{(|A_1||A_2||A_3||A_4|)^{\frac{3}{4}}} |\{(a_1, a_2, a_3, a_4) \in A_1 \times A_2 \times A_3 \times A_4 : a_1 + a_2 + a_3 + a_4 = 0\}|.$$

如文献 [5] 中所示,

$$0 \leq \omega(A_1, A_2, A_3, A_4) \leq 1. \quad (1)$$

定义 6 (Fourier 变换) 对于 $f: \mathbb{F}_2^n \rightarrow \mathbb{R}$, 定义 Fourier 变换 $\hat{f}: \mathbb{F}_2^n \rightarrow \mathbb{R}$ 为

$$\hat{f}(\xi) := \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\xi \cdot x},$$

其中 $\xi \cdot x = (\xi_1, \dots, \xi_n) \cdot (x_1, \dots, x_n) = \xi_1 x_1 + \dots + \xi_n x_n$.

定义 7 (谱) 如果 $A \subseteq \mathbb{F}_2^n$ 是非空的, 而 $0 < \alpha \leq 1$, 定义 α -谱

$$\text{Spec}_\alpha(A) := \left\{ \xi \in \mathbb{F}_2^n : |\hat{\mathbf{1}}_A(\xi)| \geq \alpha \frac{|A|}{2^n} \right\},$$

其中 $\mathbf{1}_A(x)$ 是集合 A 的指示函数.

定义 8 (协同平坦四元组) 假设 $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$ 均为非空的, 而 $\delta \in (0, \frac{1}{2})$ 是一个小的参数. 如果对于每个 $\xi \in \mathbb{F}_2^n$, 下面的条件总有一个满足:

- 1) $\xi \in \text{Spec}_{\frac{\delta}{10}}(A_i)$, 对于所有的 $i = 1, 2, 3, 4$;
- 2) $\xi \notin \text{Spec}_\delta(A_i)$, 对于所有的 $i = 1, 2, 3, 4$,

我们称四元组 (A_1, A_2, A_3, A_4) 是协同 δ -平坦的.

3 定理 4 的证明

引理 9 设 $J \geq 1$. 假设 (A_1, A_2, A_3, A_4) 是一个协同 $\frac{1}{\sqrt{2J}}$ -平坦四元组, 它的正规化能量满足

$$\omega(A_1, A_2, A_3, A_4) \geq \frac{1}{J},$$

则有一个子空间 $H \subseteq \mathbb{F}_2^n$ 以及 $x_1, x_2, x_3, x_4 \in \mathbb{F}_2^n$, 使得

$$H \geq \frac{4}{5}(|A_1||A_2||A_3||A_4|)^{\frac{1}{4}} \quad (2)$$

并且

$$\prod_{i=1}^4 |A_i \cap (x_i + H)|^{\frac{1}{4}} \geq \frac{1}{2J} |H|. \quad (3)$$

证明 这是文献 [5] 中的命题 2.4. □

令

$$\text{Dbl}(A, B) := \frac{|A+B|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}.$$

因为

$$|A+B| \geq \max(|A|, |B|),$$

所以我们有

$$\text{Dbl}(A, B) \geq 1. \quad (4)$$

引理 10 假设 $A, B \subseteq \mathbb{F}_2^n$ 均为非空的, 并且对于 $J \geq 1$, 有

$$\text{Dbl}(A, B) \leq J.$$

如果 (A, B, A, B) 不是协同 $\frac{1}{\sqrt{2J}}$ -平坦的, 则有 $A' \subseteq A, B' \subseteq B$ 使得

$$|A'| \geq \frac{1}{20}|A|, \quad |B'| \geq \frac{1}{20}|B| \quad (5)$$

并且

$$\text{Dbl}(A', B') \leq \frac{J}{1 + \frac{1}{100\sqrt{J}}}. \quad (6)$$

证明 根据假设, 有 $\xi \in \mathbb{F}_2^n$ 使得

$$\xi \notin \text{Spec}_{\frac{9}{10}}(A) \cap \text{Spec}_{\frac{9}{10}}(B), \quad (7)$$

并且

$$\xi \in \text{Spec}_{\frac{1}{\sqrt{2J}}}(A) \cup \text{Spec}_{\frac{1}{\sqrt{2J}}}(B). \quad (8)$$

由 (7) 知, $\xi \neq 0$. 记

$$\begin{aligned} A_0 &:= \{x \in A : x \cdot \xi = 0\}, & A_1 &:= \{x \in A : x \cdot \xi = 1\}, \\ B_0 &:= \{x \in B : x \cdot \xi = 0\}, & B_1 &:= \{x \in B : x \cdot \xi = 1\}. \end{aligned}$$

如果 $|A_0| \geq \frac{1}{2}|A|$, 我们记 $\alpha := \frac{|A_0|}{|A|}$. 不然的话, $|A_0| < \frac{1}{2}|A| \Rightarrow |A_1| = |A| - |A_0| \geq |A| - \frac{1}{2}|A| = \frac{1}{2}|A|$. 则记 $\alpha := \frac{|A_1|}{|A|}$. 不失一般性, 我们可设 $|A_0| \geq \frac{1}{2}|A|$ 且记 $\alpha := \frac{|A_0|}{|A|}$. 相似地, 我们也可设 $|B_0| \geq \frac{1}{2}|B|$ 且记 $\beta := \frac{|B_0|}{|B|}$. 我们有

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

由

$$\begin{aligned} |\hat{1}_A(\xi)| &= \left| \frac{1}{2^n} \sum_{x \in A} (-1)^{x \cdot \xi} \right| = \left| \frac{1}{2^n} \left(\sum_{x \in A_0} (-1)^{x \cdot \xi} + \sum_{x \in A_1} (-1)^{x \cdot \xi} \right) \right| \\ &= \left| \frac{1}{2^n} (|A_0| - |A_1|) \right| = \left| \frac{1}{2^n} (2|A_0| - |A|) \right| = (2\alpha - 1) \cdot \frac{|A|}{2^n} \end{aligned}$$

和

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

我们知条件 (7) 等价于

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

而条件 (8) 等价于

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

不失一般性, 我们假设

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

并且考虑

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

如果 $\beta < \alpha$, 我们将考虑 $|A_0 + B_0| + |A_0 + B_1|$.

易见集合 $B_0 + A_0$ 与 $B_0 + A_1$ 是不相交的, 因此,

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

或

$$\frac{|B_0 + A_0|}{|B_0|^{\frac{1}{2}}|A_0|^{\frac{1}{2}}} \cdot \frac{|B_0|^{\frac{1}{2}}|A_0|^{\frac{1}{2}}}{|B|^{\frac{1}{2}}|A|^{\frac{1}{2}}} + \frac{|B_0 + A_1|}{|B_0|^{\frac{1}{2}}|A_1|^{\frac{1}{2}}} \cdot \frac{|B_0|^{\frac{1}{2}}|A_1|^{\frac{1}{2}}}{|B|^{\frac{1}{2}}|A|^{\frac{1}{2}}} \leq J. \quad (13)$$

令

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

由 (13) 可得

$$\Psi(\beta^{\frac{1}{2}}\alpha^{\frac{1}{2}} + \beta^{\frac{1}{2}}(1 - \alpha)^{\frac{1}{2}}) \leq J. \quad (14)$$

在假设 (12) 之下, 条件 (10) 等价于

$$\alpha < \frac{19}{20}, \quad (15)$$

而条件 (11) 等价于

$$\beta \geq \frac{1}{2} + \frac{1}{2\sqrt{2J}}. \quad (16)$$

我们将在以下两种情形中讨论.

情形 1 $\frac{1}{2} + \frac{1}{2\sqrt{2J}} \leq \alpha < \frac{19}{20}$.

由 (12) 知,

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

由文献 [5] 中的讨论可得

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

因此,

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

情形 2 $\frac{1}{2} \leq \alpha < \frac{1}{2} + \frac{1}{2\sqrt{2J}}$.

由 (16) 可得

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

令 $f(\alpha) = \alpha^{\frac{1}{2}} + (1-\alpha)^{\frac{1}{2}}$. 因为

$$f'(\alpha) = \frac{1}{2\sqrt{\alpha}} - \frac{1}{2\sqrt{1-\alpha}} \leq 0,$$

所以函数 $f(\alpha)$ 是单调递减的. 因此,

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

从而有

$$\begin{aligned} \beta^{\frac{1}{2}}\alpha^{\frac{1}{2}} + \beta^{\frac{1}{2}}(1-\alpha)^{\frac{1}{2}} &\geq \left(\frac{1}{2} + \frac{1}{2\sqrt{2J}}\right)^{\frac{1}{2}} \left(\left(\frac{1}{2} + \frac{1}{2\sqrt{2J}}\right)^{\frac{1}{2}} + \left(1 - \left(\frac{1}{2} + \frac{1}{2\sqrt{2J}}\right)\right)^{\frac{1}{2}} \right) \\ &= \left(\frac{1}{2} + \frac{1}{2\sqrt{2J}}\right) + \left(\frac{1}{2} + \frac{1}{2\sqrt{2J}}\right)^{\frac{1}{2}} \left(1 - \left(\frac{1}{2} + \frac{1}{2\sqrt{2J}}\right)\right)^{\frac{1}{2}}, \end{aligned}$$

而这正是函数 $\alpha + \alpha^{\frac{1}{2}}(1-\alpha)^{\frac{1}{2}}$ 在 $\alpha = \frac{1}{2} + \frac{1}{2\sqrt{2J}}$ 处的值. 用情形 1 中的讨论, 我们有

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

综合以上两种情形, 我们得到

$$\Psi \leq \frac{J}{1 + \frac{1}{20\sqrt{2J}}} \leq \frac{J}{1 + \frac{1}{100\sqrt{J}}}.$$

取 $B' = B_0$, $A' = A_0$ 或者 A_1 , 使得 $\Psi = \text{Dbl}(A', B')$. 则

$$\text{Dbl}(A', B') \leq \frac{J}{1 + \frac{1}{100\sqrt{J}}}.$$

因为

$$|A_0| \geq \frac{1}{2}|A|, \quad |A_1| = |A| - |A_0| \geq |A| - \frac{19}{20}|A| = \frac{1}{20}|A|,$$

所以 $|A'| \geq \frac{1}{20}|A|$. 我们也有 $|B'| \geq \frac{1}{20}|B|$. 至此, 引理 10 证毕. $\square$

引理 11 假设 $A, B \subseteq \mathbb{F}_2^n$ 均为非空的, 并且对于 $K \geq 1$, 有 $\text{Dbl}(A, B) \leq K$. 则有 $A' \subseteq A, B' \subseteq B$ 满足

$$|A'| \gg \exp(-O(\sqrt{K}))|A|, \quad |B'| \gg \exp(-O(\sqrt{K}))|B|, \quad (17)$$

使得对于某个 J ($1 \leq J \leq K$), 有

$$\text{Dbl}(A', B') \leq J \quad (18)$$

且 (A', B', A', B') 是协同 $\frac{1}{\sqrt{2J}}$ -平坦的.

证明 取 $K_1 = K$. 如果 (A, B, A, B) 是协同 $\frac{1}{\sqrt{2K}}$ -平坦的, 则结论成立.

如果 (A, B, A, B) 不是协同 $\frac{1}{\sqrt{2K}}$ -平坦的, 根据引理 10, 有 $A'' \subseteq A, B'' \subseteq B$ 满足

$$|A''| \geq \frac{1}{20}|A|, \quad |B''| \geq \frac{1}{20}|B|,$$

使得

$$\text{Dbl}(A'', B'') \leq \frac{K_1}{1 + \frac{1}{100\sqrt{K_1}}}.$$

然后, 取

$$K_2 = \frac{K_1}{1 + \frac{1}{100\sqrt{K_1}}},$$

并对 A'', B'' 和 K_2 , 重复以上的过程.

因为 $\text{Dbl} \geq 1$, 所以这个过程一定在有限步之后停止. 我们得到一个序列 $K_1 = K, K_2, \dots, K_m = J$ 满足

$$K_{i+1} = \frac{K_i}{1 + \frac{1}{100\sqrt{K_i}}}, \quad i = 1, 2, \dots, m-1,$$

以及 $A' \subseteq A, B' \subseteq B$ 满足

$$|A'| \gg \frac{1}{20^m}|A|, \quad |B'| \gg \frac{1}{20^m}|B|,$$

使得

$$\text{Dbl}(A', B') \leq J$$

且 (A', B', A', B') 是协同 $\frac{1}{\sqrt{2J}}$ -平坦的.

我们将 K_i 分配到区间

$$\left(\frac{K}{e^{r+1}}, \frac{K}{e^r}\right], \left(\frac{K}{e^r}, \frac{K}{e^{r-1}}\right], \dots, \left(\frac{K}{e^2}, \frac{K}{e}\right], \left(\frac{K}{e}, K\right], \quad r = \lfloor \log K \rfloor$$

中. 对于给定的区间 $(\frac{K}{e^{s+1}}, \frac{K}{e^s}]$ ($0 \leq s \leq r$), 如果 K_l 和 K_{l+j} ($j \geq 1$) $\in (\frac{K}{e^{s+1}}, \frac{K}{e^s}]$, 我们有

$$\begin{aligned} \frac{K}{e^{s+1}} &\leq K_{l+j} = \frac{K_{l+j-1}}{1 + \frac{1}{100\sqrt{K_{l+j-1}}}} \leq \frac{K_{l+j-1}}{1 + \frac{1}{100\sqrt{\frac{K}{e^s}}}} \leq \dots \\ &\leq \frac{K_l}{(1 + \frac{1}{100\sqrt{\frac{K}{e^s}}})^j} \leq \frac{K}{e^s} \cdot \frac{1}{(1 + \frac{1}{100\sqrt{\frac{K}{e^s}}})^j}. \end{aligned}$$

因此,

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

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

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

于是, 落入区间 $(\frac{K}{e^{s+1}}, \frac{K}{e^s}]$ 中的 K_i 的个数 $\ll \sqrt{\frac{K}{e^s}}$. 关于 K_i 的总数, 我们有

$$\begin{aligned} m &\ll \sqrt{K} + \sqrt{\frac{K}{e}} + \sqrt{\frac{K}{e^2}} + \cdots + \sqrt{\frac{K}{e^r}} \\ &\leq \sqrt{K} \left(1 + \frac{1}{\sqrt{e}} + \frac{1}{(\sqrt{e})^2} + \frac{1}{(\sqrt{e})^3} + \cdots \right) \\ &\ll \sqrt{K}. \end{aligned}$$

所以,

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

至此, 引理 11 证毕. □

定理 4 的证明 取引理 11 中的 A' 和 B' , 它们具有我们所需要的性质. 文献 [5] 中证明了

$$\omega(A', B', A', B') \geq \frac{1}{\text{Dbl}(A', B')} \geq \frac{1}{J}.$$

于是, 根据引理 9, 存在一个子空间 $H \subseteq \mathbb{F}_2^n$ 以及 $x_1, x_2, x_3, x_4 \in \mathbb{F}_2^n$, 使得

$$|H| \geq \frac{4}{5} |A'|^{\frac{1}{2}} |B'|^{\frac{1}{2}} \gg \exp(-O(\sqrt{K})) |A|^{\frac{1}{2}} |B|^{\frac{1}{2}},$$

并且

$$|A \cap (x_1 + H)|^{\frac{1}{4}} |B \cap (x_2 + H)|^{\frac{1}{4}} |A \cap (x_3 + H)|^{\frac{1}{4}} |B \cap (x_4 + H)|^{\frac{1}{4}} \geq \frac{1}{2J} |H| \geq \frac{1}{2K} |H|.$$

因为

$$|A| \leq |A + B| \leq K |A|^{\frac{1}{2}} |B|^{\frac{1}{2}},$$

所以有

$$K^{-2} |A| \leq |B|,$$

因而,

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

不失一般性, 我们可以假设

$$|A \cap (x_1 + H)| \geq |A \cap (x_3 + H)|, \quad |B \cap (x_2 + H)| \geq |B \cap (x_4 + H)|,$$

因此,

$$|A \cap (x_1 + H)|^{\frac{1}{2}} |B \cap (x_2 + H)|^{\frac{1}{2}} \geq \frac{1}{2K} |H|.$$

至此, 定理 4 证毕. □

致谢 2012 年 4 月, 南京师范大学杨全会在中国科学院晨兴数学中心“遍历型素数定理 2012”讨论班上作报告, 介绍了文献 [5] 中的一些结果. 感谢杨全会, 正是他的报告将我的兴趣吸引到这个课题上来. 感谢中国科学院晨兴数学中心给予“遍历型素数定理”讨论班的长期支持, 以及讨论班的同事和朋友们的有益探讨.

参考文献

- 1 Ruzsa I Z. An analog of Freiman's theorem in groups. *Astérisque*, 1999, 258: 323–326
- 2 Sanders T. A note on Freiman's theorem in vector spaces. *Combin Probab Comput*, 2008, 17: 297–305
- 3 Green B, Tao T. Freiman's theorem in finite fields via extremal set theory. *Combin Probab Comput*, 2009, 18: 335–355
- 4 Green B, Sanders T. Boolean functions with small spectral norm. *Geom Funct Anal*, 2008, 18: 144–162
- 5 Green B, Tao T. A note on the Freiman and Balog-Szemerédi-Gowers theorems in finite fields. *J Aust Math Soc*, 2009, 86: 61–74

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

JIA ChaoHua

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 $a \in A, b \in B$.

Green and Tao proved that, 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 that if

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

then the above conclusion still holds true.

Keywords sumset, normalized energy, coherently flat quadruple

MSC(2010) 11T30

doi: 10.1360/012012-572