arXiv:2303.00828v1 [math.CO] 1 Mar 2023

# 自然数集中的大型无和集的结构

LEO VERSTEEGEN

Abstract. 若集合 $A \subset \mathbb{F}_p^n$ 与 $A+A$ 不相交，则称其为无和集。若 $p \equiv 2$ 模 3，则 $\mathbb{F}_p^n$ 中无和集的最大大小已知为 $(p^n+p^{n-1})/3$。我们证明，若无和集 $A \subset \mathbb{F}_p^n$ 的大小至少为 $p^n/3 - p^{n-1}/6 + p^{n-2}$，则存在一个余维 1 子空间 $V < \mathbb{F}_p^n$，使得 $A$ 包含于 $V$的 $(p+1)/3$ 个陪集中。特别地，对于 $p = 5$，我们证明了更强的结论：每个大小大于 $1.2 \cdot 5^{n-1}$ 的无和集都具有这一性质，从而改进了 Lev 最近的一项定理。

## 1. 引言

设 $G$ 是一个有限阿贝尔群。给定子集 $A$、$B \subset G$，我们用 $A+B$ 表示它们的和集$\{a+b : a \in A$、$b \in B\}$。若集合 $A \subset G$ 满足 $(A+A) \cap A = \emptyset$，则称其为无和集；也就是说，不存在 $a$、$b$、$c \in A$ 使得 $a+b=c$。早在 1969年，Yap [13] 就研究了 $G$中最大无和集的大小，记作 $\lambda(G)$。尽管这一问题在许多群类中早期已有一些进展 [3, 8, 11, 12], ，但直到 Green 和 Rusza [4], 确定了所有有限阿贝尔群的 $\lambda(G)$，这一问题才得到彻底解决。我们仅陈述这项历时 35 年以上研究的最终结果，并请读者参阅 [4] 以了解更详细的论述。

定理 1.1。 $N = |G|$, $\lambda(G)$的写法由以下情况确定。

- 若 $N$ 可被一个模 3 同余于 $p \equiv 2$ 的素数整除，则 $\lambda(G) = N(p+1)/3p$，其中 $p$ 是满足条件的最小素数。
- 若 $N$ 不能被任何模 3 同余于 $p \equiv 2$ 的素数整除，但 $3|n$，则 $\lambda(G) = N/3$。
- 若 $N$只能被模 3 同余于 $p \equiv 1$ 的素数整除，则 $\lambda(G) = (1-1/m)N/3$，其中 $m$ 是 $G$中任一元素的最大阶。

早在 [4], 之前，人们就已对一个相关研究方向产生兴趣，即探究一个较大的无和集可能具有何种结构。早在 [13], ，Yap 就指出，若 $|G|$ 的最小素因子 $p$ 模 3 同余于 2，且 $A$ 是无和集，并满足 $|A| = \lambda(G) = |G|(p+1)/3p$，那么$A$ 是子群 $H \subset G$ 的若干陪集之并，且 $A/H$ 构成等差数列。另一个例子是，受编码理论应用的启发，Davydov 和 Tombak [2] 以及独立地，Clark 和 Pedersen [1] 证明了以下结果。

定理1.2. 如果 $A \subset \mathbb{F}_2^n$是无和的且 $|A| > 5 \cdot 2^{n-4}$，那么存在一个真子空间$V < \mathbb{F}_2^n$，使得 $A$ 包含在 $V$的一个陪集中。

集合 $A = \{(1,0,0,0)$、$(0,1,0,0)$、$(0,0,1,0)$、$(0,0,0,1)$、$(1,1,1,1)\}$ 表明界 $5 \cdot 2^{n-4}$ 是紧的。后来，Lev [6] 证明了关于 $p=3$的类似结论。

作者感谢剑桥大学三一学院通过三一学院外部研究人员奖学金提供资助。

本文研究 $\mathbb{F}_p^n$ 中模 $p \equiv 2$ 为 3 的奇素数情形下，大型无和子集的结构。根据定理 1.1，$\lambda(\mathbb{F}_p^n) = (p+1)p^{n-1}/3$，而且不难找到一个达到此界的无和集。事实上，令 $m_p = (p+1)/3$，并取一个余维 1 的子空间$V < \mathbb{F}_p^n$以及一个元素 $w \in \mathbb{F}_p^n \setminus V$。那么集合 $A(V,w) = \{m_p \cdot w, \dots, (2m_p - 1) \cdot w\} + V$是无和集，其大小为 $\lambda(\mathbb{F}_p^n)$。当然，$A(V,w)$ 的任意子集也都是无和集；我们称无和集 $A$ 是正规的，如果 $A$ 包含于某个形如 $A(V,w)$ 的集合中。用这一术语，Lev [7] 最近的一个结果可以表述如下。

定理 1.3：如果 $A \subset \mathbb{F}_5^n$ 是无和集且 $|A| > 1.5 \cdot 5^{n-1}$，那么 $A$ 是正规的。

注意到，$\mathbb{F}_5^n$ 中无和集可能达到的最大大小为 $2 \cdot 5^{n-1}$。Lev认为定理 1.3 并非最佳。我们的第一个主要结果证实了这一点。

定理 1.4：如果 $A \subset \mathbb{F}_5^n$ 是无和集且 $|A| > 1.2 \cdot 5^{n-1}$，那么 $A$ 是正规的 *al.*

我们将在第 3 节末尾简要比较定理 1.3 和定理 1.4 的证明。

作为定理 1.4 证明的一部分，我们将证明，对于 $n = 2$，界 $6 \cdot 5^{n-2} = 6$ 可以替换为 5；由 $A = \{$(0, 1)、(1, 2)、(2, 2)、(3, 2)、(4, 3)$\}$ 可知，这是最佳可能的结果。对于更大的 $n$，下面的例子表明，定理 1.4 中的界不可能改进到超过 $1.12 \cdot 5^{n-1}$。

例 1.5。考虑集合

$$X = \{(1,x,y) \in \mathbb{F}_5^3 : x \in \{1,2\} \vee (x = 0 \wedge y \in \{1,2\})\} \cup \{(2,0,0),(2,0,1)\}.$$

容易看出，$X$ 与 $X + X$、$X - X$或 $-(X + X)$均不相交，因此$Y = X \cup (-X)$是无和集。另一方面，$Y$ 并不包含在二维子空间的两个陪集中，因为这样的子空间必须包含 (0, 0, 1) 和 (0, 1, 0)。对于任意 $n \geq 3$，取 $A = Y \times \mathbb{F}_5^{n-3}$，即可得到一个含有 $28 \cdot 5^{n-3} = 1.12 \cdot 5^{n-1}$ 个元素的无和集，但它不是正规集。

我们没有特别的理由相信 $1.2 \cdot 5^{n-1}$和 $1.12 \cdot 5^{n-1}$这两个界限中的任何一个是正确的。甚至可以设想，数列 $(\lambda(\mathbb{F}_5^n))_{n \in \mathbb{N}}$ 根本无法达到其上确界。

对于较大的素数 $p$，我们得到以下结果。

定理 1.6. 设 $p \equiv 2$ 模 3 且 $n \in \mathbb{N}$。若 $A \subset \mathbb{F}_p^n$ 是无和集且 $|A| \geq (m_p - 1/2 + 1/p)p^{n-1}$，则 $A$ 是正规集。

界 $(m_p - 1/2 + 1/p)p^{n-1}$ 应与 $\lambda(\mathbb{F}_p^n) = m_p p^{n-1}$进行比较。据我们所知，此类问题此前最好的界归功于 Green 和 Rusza；他们证明了一个引理，该引理意味着，若无和集 $A \subset \mathbb{F}_p^n$ 满足 $|A| \geq (m_p - 1/(3p^2 + 3p))p^{n-1}$，则它必为正规集（见 [4]中的引理 5.6.）。定理 1.6 中的界不可能是紧的，因为 $(m_p - 1/2 + 1/p)p^{n-1}$ 不是整数，而且似乎有可能将其提高一个与 $p^{n-1}$成正比例的量。然而，下面的例子表明，该界无法改进到优于 $(m_p - 1)p^{n-1}$。

例 1.7。设 $p \geq 11$ 为素数，$p \equiv 2$ 模 3，并设

$$A_2 = \{(m_p - 1, 0), (2m_p - 1, p - 1)\} \cup \{m_p\} \times (\mathbb{F}_p \setminus \{p-1\}) \cup \{2m_p - 2\} \times (\mathbb{F}_p \setminus \{0\}) \cup \{m_p + 1, \dots, 2m_p - 3\} \times \mathbb{F}_p \subset \mathbb{F}_p^2.$$

集合 $A_2 \times \mathbb{F}_p^{n-2} \subset \mathbb{F}_p^n$是无和的，大小为 $(m_p - 1)p^{n-1}$，且不是正规集合。

我们以如下评论结束引言：对于模3余1的素数，情况似乎更加复杂。事实上，即使对于 $p = 7$，也存在大小为 $\lambda(\mathbb{F}_7^n)$的无和集，但它们不是正规无和集。

例1.8。在 $\mathbb{F}_7^2$中，集合

$A = \{(3, 0), (4, 0), (3, 1), (4, 1), (3, 2), (4, 2), (2, 3), (3, 3), (4, 3), (3, 4), (4, 4), (3, 5), (4, 5), (3, 6)\}$

是无和集，大小为 $\lambda(\mathbb{F}_7^2) = 14$，但不包含于三个陪集中。

## 2. Preliminaries

在陈述一些关键要素之前，我们先约定一些术语。在本节中，设 $G$ 为有限阿贝尔群，$p$ 为一个模 3 同余于 2 的素数，且 $n \in \mathbb{N}$。对于集合 $A \subset \mathbb{F}_p^n$，我们用 $\langle A\rangle$ 表示 $A$ 的线性张成；按惯例，将 $\langle\{v_1, \ldots, v_k\}\rangle$ 简写为 $\langle v_1, \ldots..., v_k\rangle$，其中 $v_1, \ldots..., v_k \in \mathbb{F}_p^n$。集合 $I_p$ 是中心区间 $\{m_p + 1, \ldots, 2m_p - 1\} \subset \mathbb{F}_p$；对于元素 $v \in \mathbb{F}_p^n$ 和集合 $J \subset \mathbb{F}_p$，我们用 $J(v)$ 表示 $\{xv\colon\ x \in J\} \subset \mathbb{F}_p^n$。

如果存在 $\mathbb{F}_p^n$ 的一个自同构，也就是一个可逆线性映射 $\phi\colon\ \mathbb{F}_p^n \to \mathbb{F}_p^n$，使得 $\phi(A) = B$，我们就称集合 $A$、$B \subset \mathbb{F}_p^n$ 同构。注意，若 $A$ 与 $B$ 同构，且 $A$ 是无和集，那么 $B$ 也必定是无和集，反之亦然。我们将反复利用这一观察来简化证明步骤：假设某些线性无关向量 $v_1, \ldots..., v_k$ 是标准单位向量 $e_1, \ldots..., e_k$。

给定一个集合 $X \subset G$，$X$ 的对称群 $\mathrm{Sym}(X)$ 定义为 $\{g \in G\colon\ g + X = X\}$。注意，$\mathrm{Sym}(X)$ 实际上是一个群。我们将多次使用 Kneser 的一个定理[5]（英文参考资料见 [9]）。

引理 2.1（Kneser定理）。对于有限阿贝尔群 $G$ 及非空集合 $A$、$B \subset G$，有

$$|A + B| \geq |A + \mathrm{Sym}(A + B)| + |B + \mathrm{Sym}(A + B)| - |\mathrm{Sym}(A + B)|.$$

Kneser定理的一个重要特例如下，我们将经常不加说明地使用它。

引理 2.2。设 $G$ 是一个有限阿贝尔群，其子集为 $A$、$B \subset G$。假设存在一个子群 $H \leq G$ 及 $a$、$b \in G$，使得 $A \subset a + H$ 且 $B \subset b + H$。若 $|A| + |B| > |H|$，则 $A + B = a + b + H$。

证明。不失一般性，$a = b = 0$，此时显然有 $A + B \subseteq H$。现在假设 $C = H \setminus (A + B)$非空。我们必有$(C - A) = C + (-A)$与$B$不相交，但这与 $|C - A| + |B| \geq |A| + |B| > |H|$矛盾。□

下一个引理将使我们能够通过考察无和集与一个子空间的交集，深入了解无和集的结构。

引理 2.3. 设 $n \geq 3$，令 $A \subset \mathbb{F}_p^n$ 为无和集，并设 $u \in \mathbb{F}_p^n \setminus \{0\}$ 使得 $I_p(u) \subset A$。那么存在两个不同的余维 1 子空间 $W_1$、$W_2 < \mathbb{F}_p^n$，使得 $I_p(u) \subset W_1 \cap W_2$，且 $|W_i \cap A| \geq |A|/p$ 对于 $i \in \{1, 2\}$。

证明. 令 $\mathfrak{W}$ 为 $\mathbb{F}_p^n$ 中包含 $u$ 的余维 1 子空间集合。这样的子空间有 $K := (p^{n-1}-1)/(p-1)$ 个。我们断言，其中至少有两个与 $A$ 的交集包含多于 $|A|/p$ 个元素。为此，我们先求 $\mathfrak{W}$ 中的子空间与 $A$ 的交集的平均大小。我们有

$$\sum_{W\in\mathfrak{W}} |A\cap W| = \sum_{w\in A} |\{W\in\mathfrak{W} : w\in W\}| = Km_p + \sum_{w\in A\setminus\langle u\rangle} |\{W\in\mathfrak{W} : w\in W\}|. \tag{2.1}$$

$\mathbb{F}_p^n \setminus \langle u\rangle$ 中的所有元素，在 $\mathfrak{W}$中的子空间里出现的次数都相同。由于 $\mathbb{F}_p^n \setminus \langle u\rangle$ 有$p^n - p$ 个元素，而每个 $W\in\mathfrak{W}$ 包含其中的 $p^{n-1}-p$ 个，因此这个次数必定是

$$\frac{p^{n-1}-p}{p^n-p}K = \frac{p^{n-2}-1}{p^{n-1}-1}K.$$

将此代入（2.1）得

$$\begin{aligned}\sum_{W\in\mathfrak{W}} |A\cap W| &= Km_p + \frac{p^{n-2}-1}{p^{n-1}-1}K(|A|-m_p)\\ &= \frac{p^{n-1}-p^{n-2}}{p^{n-1}-1}Km_p + \frac{K|A|}{p} - \frac{p-1}{p(p^{n-1}-1)}K|A|\\ &= m_p p^{n-2} + \frac{K|A|}{p} - \frac{|A|}{p}.\end{aligned} \tag{2.2}$$

现在反设，除一个例外 $W_1$外， $\mathfrak{W}$中的所有子空间与 $A$ 的交集都严格少于 $|A|/p$ 个点。由于 $A$ 是无和集，我们有 $|A\cap W_1| \le \lambda(\mathbb{F}_p^{n-1}) = m_p p^{n-2}$；又由于对所有 $W\in\mathfrak{W}$， $|A|$ 和 $|A\cap W|$ 都是整数，因此对所有 $W\in\mathfrak{W}\setminus\{W_1\}$，我们有$|A\cap W| \le (|A|-1)/p$。因此，

$$\sum_{W\in\mathfrak{W}} |A\cap W| \le m_p p^{n-2} + \frac{(K-1)(|A|-1)}{p} = m_p p^{n-2} + \frac{K|A|}{p} - \frac{|A|}{p} + \frac{1-K}{p}.$$

由于 $K>1$ 如 $n\ge 3$，这与（2.2）矛盾。 □

最后，下面这个由 Vosper 得出的结果（另见 [9]）是定理 1.6 的基例。

引理 2.4（Vosper 定理）。设 $p$ 为素数，且 $A$、$B\subset\mathbb{F}_p$ 满足 $|A|$、$|B|\ge 2$ 和 $|A+B|\le p-2$。那么， $|A+B| = |A|+|B|-1$ 当且仅当 $A$ 和 $B$ 是具有相同公差的等差数列。

## 3. 定理 1.4 的证明

定理 1.4 的证明涉及相当多的技术步骤，但其核心可以在一个归纳框架下分成两个主要部分。简要来说，考虑一个无和集 $A\subset\mathbb{F}_5^n$。利用引理 2.3 和归纳假设，我们将找到一个子空间 $V<\mathbb{F}_5^n$，使得 $A\cap V$ 是正规的，也就是说，它包含在某个 $(n-2)$ 维子空间 $U<V$ 的两个陪集中。

在归纳步骤的第一部分，我们将证明，如果 $A$ 在 $\mathbb{F}_5^n$ 中的 $U$ 的其他陪集上分布得不够均匀，那么就可以将 $A$ 缩减为一个同样无和的集合 $A'\subset\mathbb{F}_5^2$。基于对二维情形的充分理解，我们便能推断出 $A'$ 的结构性质，并据此得出 $A$ 必定是正规的。在归纳步骤的第二部分，我们将利用 $A$ 是无和集这一事实，在

一系列线性不等式中证明， $A$ 在 $U$ 的各陪集上的分布实际上必定高度不规则，从而完成证明。

尽管两部分之间的划分并不完全清晰，第一部分大致对应于引理 3.1、引理 3.5、断言 3.6 和断言 3.7，而定理 1.4 的证明其余部分则涵盖第二部分。

引理 3.1。设 $A \subset \mathbb{F}_5^2$ 是一个大小至少为 5 的无和集。则 $A$ 同构于一个包含 (1, 0)、(1, 1) 和 (1, 2) 的集合。

证明。只需证明存在一个一维子空间 $W < \mathbb{F}_5^2$ 和 $u \in \mathbb{F}_5^2$，使得 $|A \cap (u + W)| \geq 3$。假设并非如此。由于 $A$ 是无和的，我们必有$A \cap (A - A) = \emptyset$。因此，我们必有 $|A - A| \leq 20$，这意味着必存在$a$、$b$、$c$、$d \in A$，使得 $a \neq b$、$c$ 以及 $a-b = c-d$。我们也不可能有 $a = d$ 或 $b = c$，因为那样就会有三个点构成等差数列。剩下需要验证的是，不存在 $f \in \mathbb{F}_5^2 \setminus \{a, b, c, d\}$，使得 $\{a, b, c, d, f\}$ 是无和的，且 $\{a, b, c, d\}$ 中没有两个点与 $f$ 共线。为简化这一过程，我们可假设 $a-b = c-d = e_1$ 且 $a-c = e_2$。将$d$写成 $(x, y)$，其中 $x$、$y \in \mathbb{F}_5$，我们有 $c = (x+1, y)$ $a = (x+1, y+1)$ 以及 $b = (x, y+1)$。由对称性，我们可假设，当将它们视为 $\{0, \ldots, 4\}$ 中的元素时 $x \geq y$，并且由于 $A$ 是无和的，我们必有 $(x, y) \notin \{(0, 0), (1, 0), (3, 0), (4, 0), (1, 1), (4, 1), (3, 3), (4, 3), (4, 4)\}$。这就留下了六种可能的 $(x, y)$ 选择，需要手工检验；这一任务留给读者。□

以下两个引理是上述内容的直接推论。

引理 3.2. 若无和集 $A \subset \mathbb{F}_5^2$ 的大小至少为 5，则存在一个一维子空间 $V < \mathbb{F}_5^2$，使得 $(A + A) \cup (A - A)$ 包含 $V$ 的两个陪集。

证明。拜引理 3.1，可不失一般性地假设 $(1,0),(1,1),(1,2) \in A$，由此 $\langle e_2 \rangle \subset A - A$ 和 $2e_1 + \langle e_2 \rangle \subset A + A$。□

引理 3.3. 定理 1.4 对 $n = 1$ 和 $n = 2$ 成立。

证明。对于 $n = 1$，结论显然；对于 $n = 2$，则可由引理 3 直接推出。 2. □

下一个引理将引理 2.3 应用于情形 $p = 5$，使我们能够通过归纳法证明定理 1.4。

引理 3.4. 对于 $n \geq 2$ 和任意满足 $|A| > 1.2 \cdot 5^{n-1}$ 的无和集 $A \subset \mathbb{F}_5^n$，存在一个余维 1 的子空间 $W < \mathbb{F}_5^n$，使得 $|A \cap W| \geq |A|/5$。

证明。首先假设 $n = 2$。根据假设， $|A| \geq 6$，因此由引理 3.3 可知， $A$ 必须是正规的。不失一般性， $A \subset \{e_1, -e_1\} + \langle e_2 \rangle$，并且必定存在 $y \in \mathbb{F}_5$，使得 $(1, y)$、$(-1, -y) \in A$。

现在假设 $n \geq 3$。根据引理 2.3，只需找到 $u \neq 0$ 使得 $I_p(u) \subset A$。运用上述论证，只需找到一个二维子空间 $V < \mathbb{F}_5^n$ 使得$|A \cap V| \geq 6$。为此，设 $K$ 为 $\mathbb{F}_5^n$的二维子空间数。 $A$ 中的每个元素都出现在其中的 $K(5^2 - 1)/(5^n - 1)$ 个子空间中。因此，一个二维子空间平均包含

$$\frac{|A|(5^2 - 1)}{5^n - 1} > \frac{28.8}{5}$$

$A$中的元素，这意味着其中一个至少包含六个元素，正如所需。 □

我们指出，只需再多费些工夫，就能将引理 3.4 中的界 $1.2 \cdot 5^{n-1}$ 改进为 $5^n/6$。

引理 3.5. 设 $n \geq 2$ 和 $A \subset \mathbb{F}_5^n$ 为无和集。若存在一个余维 1 子空间 $W < \mathbb{F}_5^n$ ， $v \in \mathbb{F}_5^n$ 和 $x_1$、 $x_2$、 $x_3 \in \mathbb{F}_5$，使得 $|A \cap （\{x_1v, x_2v, x_3v\} + W）| > 26 \cdot 5^{n-3}$，则 $A$ 是正规的。

证明. 不妨设 $W$ 是坐标平面 $\{w： w_1 = 0\}$ 和 $v = e_1$。对于 $x \in \mathbb{F}_5$，令 $C_x = xe_1 + W$ 和 $A_x = A \cap C_x$。先假设 $A_{x_1}$、 $A_{x_2}$ 和 $A_{x_3}$、 $A_{x_3}$ 中有一个（例如）为空。在这种情况下，我们有 $|A_{x_1}| + |A_{x_2}| > 5^{n-1}$，因此必有 $A_{x_1} - A_{x_2} = C_{x_1-x_2}$、 $A_{x_2} - A_{x_1} = C_{x_2-x_1}$ 且 $（A_{x_1} - A_{x_1}）\cup（A_{x_2} - A_{x_2}）= C_0$。因此， $A$ 是正规的。

现在假设 $A_{x_1}$、 $A_{x_2}$ 和 $A_{x_3}$ 均非空，且不失一般性地，$x_1 + x_2 = x_3$。我们有 $|A_{x_1}| + |A_{x_2}| + |A_{x_3}| > 26 \cdot 5^{n-3}$，但要使 $A$ 成为无和集，必须有 $|A_{x_1} + A_{x_2}| + |A_{x_3}| \leq 5^{n-1}$。根据 Kneser定理，这只有在对称群 $U :=$ Sym$(A_{x_1} + A_{x_2})$ 的阶为 $5^{n-2}$ 时才可能。由于 $A_{x_1} + A_{x_2} \subset C_{x_3}$，我们必须有 $U \subset W$。

同样不失一般性地， $e_2 \notin U$，并考虑集合 $S = \{(x, y) \in F_5^2： x \in \{x_1, x_2, x_3\}$ 和 $A \cap (U + xe_1 + ye_2) \neq \emptyset\}$。我们知道 $|S|$ 至少为 6，因为 $U$ 的五个陪集至多能容纳 $25 \cdot 5^{n-3}$ 个元素。另一方面， $U$ 的任何陪集都不可能同时包含 $A_{x_1} + A_{x_2}$ 和 $A_{x_3}$ 中的元素，因此很容易看出 $|S| = 6$。

假设 $S$ 是正规的。在这种情况下，必然存在 $a \in \mathbb{F}_5^2$，使得 $S$ 包含于 $\langle a \rangle$ 的两个陪集中。令 $V = \langle U、 a_1e_1 + a_2e_2 \rangle$，我们看到，包含超过 $26 \cdot 5^{n-3}$ 个元素的 $A_{x_1} \cup A_{x_2} \cup A_{x_3}$ 包含于 $V$ 的两个陪集中。重复证明的第一步，我们看到 $A$ 必须是正规的。

如果 $S$ 不是正规的，引理 3.3 告诉我们， $S$ 不可能是无和的。令 $a$、 $b$、 $c \in S$ 使得 $a + b = c$。由于我们可以假设三个点 $a$、 $b$ 和 $c$ 中至多有两个相等，并且所有坐标属于 $S$ 的 $U$ 的陪集之并与 $A$ 的交至少包含 $26 \cdot 5^{n-3}$ 个元素，因此必有 $\sum_{(x,\ y) \in \{a,b,c\}} |A \cap （U + xe_1 + ye_2）| > 7 \cdot 5^{n-3}$，从而 $A$ 不可能是无和的。□

现在我们可以完整地证明定理 1.4 了。

定理 1.4 的证明。我们对 $n$ 采用归纳法来证明该结论。因此，假设该结论对 $n - 1$ 成立，并设 $A \subset \mathbb{F}_5^n$ 是一个满足 $|A| > 6 \cdot 5^{n-2}$ 但不是正规的无和集。

对于子空间 $V \leq \mathbb{F}_5^n$和元素 $v \in \mathbb{F}_5^n$，我们将 $d_{V,v}$定义为 $5|A \cap (v + V)|/|V|$。我们声称，存在一个 $(n - 2)$ 维子空间 $U$和元素 $u \in \mathbb{F}_5^n$，使得 $d_{U,u} > 3$。事实上，注意到根据引理 3.4，存在一个余维 1 的子空间 $V < \mathbb{F}_5^n$ ，使得$d_{V,0} > 1.2$；又因为 $A \cap V$是无和集，我们可以由归纳假设得出，$V$必有一个维数为 $n-2$的子空间 $U \leq V$，使得 $A \cap V$包含在 $U$的两个陪集中。这两个陪集中至少有一个与 $A$的交集包含多于 $3 \cdot 5^{n-3}$个元素，证毕。

现在我们选取维数为 $n-2$ 的 $U$ 和 $v \in \mathbb{F}_5^n$，使得 $d_{U,v}$ 最大。由于 $A$ 是无和集，且 $d_{U,v} > 3$，因此必有 $v \neq 0$，从而 $V = \langle U \cup \{v\} \rangle$ 的维数为 $n-1$。不失一般性，$v = e_1$ 且 $e_2 \notin V$。接下来，我们将 $U$ 的陪集看作排列成一个二维网格，并称它们为单元格；将 $V$ 的陪集称为行。对于 $x, y \in \mathbb{F}_5$，我们定义 $U_{x,y} := U + xe_1 + ye_2$, $A_{x,y} = A \cap U_{x,y}$ 以及 $f(x,y) = |A_{x,y}|/5^{n-3}$。对于集合 $S \subset \mathbb{F}_5^2$，我们定义 $f(S) = \sum_{(x,y)\in S} f(x,y)$。

断言 3.6. 集合 $S = \{(x,y) : f(x,y) > 2\}$ 的大小至多为 5。

断言 3.6 的证明。反设 $|S| \geq 6$。由 Kneser定理，$S$ 必为无和集，因此由引理 3.3，$S$ 必为正规。我们不妨假设 $S \subset (e_1 + \langle e_2 \rangle) \cup (-e_1 + \langle e_2 \rangle)$，同时保持 $f(1,0) > 3$。令 $T = \{(x,y) \notin (e_1 + \langle e_2 \rangle) \cup (-e_1 + \langle e_2 \rangle) : f(x,y) > 0\}$。因为 $f(1,0) > 3$，对所有 $(x,y) \in S$，必有 $f(x+1,y) = f(x-1,y) = 0$，因此不难看出 $|T|$ 至多为 6。我们还知道 $T \subset (S+S) \cup (S-S)$，并且对于所有 $(x_1,y_1)$、$(x_2,y_2) \in S$，由 Kneser定理可得 $|A_{x_1,y_1} \pm A_{x_2,y_2}| > 4 \cdot 5^{n-3}$，从而对所有 $(x,y) \in T$，必有 $f(x,y) < 1$。

由于 $f(\mathbb{F}_5^2) > 30$ 且 $f(T) < 6$，因此必定存在 $x \in \{-2,0,2\}$ 使得 $f(\{e_1, -e_1, xe_1\} + W) > 26$，而这与引理 3.5 矛盾。□

断言 3.7. 不存在大小至少为 5 的集合 $|S| \subset \mathbb{F}_5^2$，使得对所有 $(x,y) \in S$，都有 $f(x,y) > 1$；并且对所有互不相同的 $(x_1,y_1)$、$(x_2,y_2) \in S$，都有 $f(x_1,y_1) + f(x_2,y_2) > 5$。

断言 3.7 的证明。反设存在满足断言条件的集合 $S$。由Kneser定理，$S$ 必为无和集；因此，由引理 3.1，不妨设 $S$ 包含点 (1, 0)、(1, 1) 和 (1, 2)。取 $y_0 \in \{0,1,2\}$，使得 $f(1,y_0)$ 最小。根据断言中关于 $S$的第二个假设，对 $y \in \{0,1,2\} \setminus \{y_0\}$必有$f(1,y) > 2.5$。由Kneser定理可知，对所有$y \in \mathbb{F}_5$，都有 $f(0,y) = 0$；对所有 $y \in \mathbb{F}_5 \setminus \{2y_0\}$，都有 $f(2,y) = 0$；并且 $f(2,2y_0) < 3$。因此，$f(\{e_1, 3e_1, 4e_1\} + \langle e_2 \rangle) > 27$，与引理 3.5 矛盾。□

若一行 $ye_2 + V$中至少有四个包含在 $ye_2 + V$内且与 $A$交集非空的单元格，我们就称该行为分散行。同理，若这类单元格恰有三个或至多两个，则分别称该行为半分散行或聚焦行。

断言 3.8. 假设 $f(1,0) > 4$。每个分散行 $ye_2 + V$都满足 $f(ye_2 + \langle e_1 \rangle) \leq 2.5$；若 $ye_2 + V$是半分散的，则可找到 $(x_1,y)$、$(x_2,y)$，使得 $f(x_1,y)\, f(x_2,y) > 0$且 $f(x_1,y) + f(x_2,y) \leq 1$。

断言 3.8 的证明。假设存在一个分散行 $ye_2 + V$，满足 $f(ye_2 + \langle e_1 \rangle) > 2.5$。由平均论证，必存在 $x \in \mathbb{F}_5$，使得 $f(x,y) + f(x+1,y) > 1$。$A_{x,\,y}$ 和 $A_{x+1,\,y}$ 中必有一个为空；否则，根据Kneser定理，

$$|A_{x,y} + A_{1,0}| + |A_{x+1,y}| > |A_{x,y}| + |A_{x+1,y}| + 4 \cdot 5^{n-3} > 5^{n-2},$$

这将与假设 $A$ 是无和集相矛盾。但此时我们可以不失一般性地假设 $f(x,y) > 1$，并用同样的论证得出 $A_{x-1,\,y}$ 也必为空，从而与假设 $ye_2 + V$ 是离散的相矛盾。

为了证明该断言的第二部分，我们只需在这三个单元格中找出两个：它们与 $A$ 在 $ye_2+V$ 中的交集非空，且其 $x$ 坐标相差 1，然后对它们应用 Kneser 定理。□

断言 3.9。每个分散行 $ye_2+V$都满足 $f(ye_2+\langle e_1\rangle)\le 5$；若 $ye_2+V$是半分散的，则可找到 $(x_1,y)$、$(x_2,y)$，使得 $f(x_1,y)\ f(x_2,y)>0$，且 $f(x_1,y)+f(x_2,y)\le 2$。

断言3.9的证明。同断言 3.8，注意到 $f(1,0)>3$。 □

断言 3.10。分散行至多有两行。

断言3.10的证明。单个单元格至多包含 $5\cdot 5^{n-2}$ 个 $A$ 的元素，因此聚焦行至多包含 $10\cdot 5^{n-2}$ 个 $A$ 的元素；根据断言 3.9，半分散行至多包含 $7\cdot 5^{n-2}$ 个 $A$ 的元素。由于每个分散行与 $A$ 的交集至多包含 $5\cdot 5^{n-3}$ 个元素，且 $|A|>30\cdot 5^{n-3}$，我们知道分散行至多有三行；若确有三行，则其余行中至少有一行必须是聚焦行。此外，$V$绝不可能是分散行，因为 $f(0,0)=f(2,0)=0$。现在反设仅有两行非分散行，即对于某个 $y\in\mathbb{F}_5$，它们是 $V$ 和 $ye_2+V$。

我们首先假设 $V$和 $ye_2+V$都聚焦。在 $V\cup(ye_2+V)$ 中，与 $A$有非空交集的单元格至多有四个；又由于 $|A\setminus(V\cup(ye_2+V))|\le 15\cdot 5^{n-3}$，这意味着 $V\cup(ye_2+V)$ 中至少有三个单元格与 $A$ 的交集大于 $2.5\cdot 5^{n-3}$。我们固定坐标 $x_1$、$x_2$、$x_3$、$y_1$和 $y_2$，使得 $x_1\neq x_2$、$y_1\neq y_2$，以及$|A_{x_1,\ y_1}|$、$|A_{x_2,\ y_1}|$、$|A_{x_3,\ y_2}|\ge 2.5\cdot 5^{n-3}$。不失一般性地，$y_1-y_2\notin\{y_1,y_2\}$，因此$A_{y_1-y_2,\ x_1-x_3}=A_{y_1-y_2,\ x_2-x_3}=\emptyset$，这意味着 $(y_1-y_2)e_2+V$不是散布的。

如果 $V$或 $ye_2+V$中有一个是半散布的，不妨设后者是半散布的。根据断言 3.9，存在一个元素 $x\in\mathbb{F}_5$，使得 $|A\cap(ye_2+V)\setminus A_{x,\ y}|\le 2\cdot 5^{n-3}$。这意味着$|A_{x,\ y}\cup(A\cap V)|>13\cdot 5^{n-3}$，因此 $V\cup(yw+V)$ 中必定有三个单元格与$A$ 相交，且至少有 $3\cdot 5^{n-3}$ 个元素，我们可以像之前一样继续。□

现在我们将通过把 $\mathbb{F}_5^2$ 划分为合适的集合来分析 $f$。首先，我们用 $R$表示位于分散行内的单元格的坐标对。其次，我们取一个集合 $S\subset\mathbb{F}_5^2$，其中每个半分散行 $ye_2+V$都对应两对坐标 $(x_1,y)$ 和 $(x_2,y)$，使得 $f(x_1,y)\ f(x_2,y)>0$，并且 $f(x_1,y)+f(x_2,y)\le 1$，若 $f(1,0)>4$；或者 $f(x_1,y)+f(x_2,y)\le 2$，若$f(1,0)\le 4$。根据断言 3.8 和断言 3.9，这样的集合存在。我们用 $r$和 $s$分别表示分散行和半分散行的数量。

现在，令 $T=\{(x,y)\in\mathbb{F}_5^2\setminus(R\cup S):\ f(x,y)>0\}$。每条聚焦直线最多包含两个坐标位于 $T$ 中的单元格，因此我们有 $|T|\le 10-2r-s$。假设存在 $\varepsilon\ge 0$和一个集合 $E\subset T$，使得 $f(E)\le\varepsilon$，并且对于 $c>0$，令 $K_c=\{(x,y)\in T:\ f(x,y)>c\}$。对于所有 $c>0$，我们有

$$f(\mathbb{F}_5^2)=f(R)+f(S)+f(E)+f(K_c\setminus E)+f(T\setminus K_c\setminus E)$$

回想一下，$f(1,0)$使 $f$ 取得最大值，且 $f(\mathbb{F}_5^2)>30$，由此得到

$$f(R)+f(S)+\varepsilon+f(1,0)|K_c\setminus E|+c(10-2r-s-|E|-|K_c\setminus E|)>30. \tag{3.1}$$

断言 3.11. 我们必有 $f(1,0)>4$。

证明。首先注意，根据断言 3.9，$f(R) \le 5r$ 且 $f(S) \le 2s$。为导出矛盾，假设 $f(1,0) \le 4$。将此代入 (3.1) 中的 $c=2$、$E=\emptyset$ 和 $\varepsilon=0$，得到

$$r+2|K_2|+20>30.$$

根据断言 3.10，$r$ 至多为 2，这意味着 $|K_2|$ 大于 4，因此至少为 5。根据断言 3.7，必定存在两点 $(x_1,y_1)$、$(x_2,y_2)\in K_2$，使得 $f(x_1,y_1)+f(x_2,y_2)\le 5$。取 $E=\{(x_1,y_1)、(x_2,y_2)\}$ 和 $\varepsilon=5$，我们可以再次应用 (3.1)，令 $c=2$，得到

$$r+5+2|K_2\setminus E|+16>30,$$

由此可得，$|K_2\setminus E|$ 至少为 4。将断言 3.6 应用于 $K_2$，便可得出矛盾。□

为了完成定理 1.4 的证明，现在来分析 $f(1,0)>4$时会发生什么。根据断言 3.8，我们知道 $f(R)\le 2.5r$ 且 $f(S)\le s$。首先假设不存在满足 $f(x,y)\in[1.5,3]$ 的 $(x,y)\in T$。那么我们可以令 $c=1.5$、$E=\emptyset$和$\varepsilon=0$，应用 (3.1)，得到

$$3.5|K_{1.5}|+15>30,$$

这意味着 $|K_{1.5}|\ge 5$。然而，由于 $K_{1.5}=K_3$，根据断言 3.7 可得矛盾。

接下来，假设存在 $(x,y)\in T$，使得 $f(x,y)\in(2,3]$。我们可以对 $E=\{(x,y)\}$、$\varepsilon=3$ 和 $c=2$ 应用 (3.1)，得到

$$3+3|K_2\setminus E|+18>30,$$

这意味着 $|K_2\setminus E|\ge 4$。根据断言 3.7，必定存在 $(x_1,y_1)$、$(x_2,y_2)\in K_2$，使得$f(x_1,y_1)+f(x_2,y_2)\le 5$。再次对 $E=\{(x_1,y_1)、(x_2,y_2)\}$、$\varepsilon=5$ 和$c=2$ 应用 (3.1)，得到

$$5+3|K_2\setminus E|+16>30, \tag{3.2}$$

这意味着 $|K_2\setminus E|\ge 4$。对 $K_2$ 应用断言 3.6，即可得到矛盾。

This l排除了 $f$ 取值于 $[1.5,2]$ 但不取值于 $(2,3]$的可能性。我们定义

$$\alpha=\max\{f(x,y):(x,y)\in T\setminus K_2\} \qquad \text{and} \qquad \beta=\min\{f(x,y):(x,y)\in K_2\}.$$

若 $\alpha+\beta\le 5$，我们固定 $(x_1,y_1)$ 和 $(x_2,y_2)$，使得 $f(x_1,y_1)=\alpha$ 且 $f(x_2,y_2)=\beta$。取$E=\{(x_1,y_1),(x_2,y_2)\}$，我们再次得到 (3.2)，从而有 $|K_2\setminus E|\ge 4$，这使我们能够将断言 3.7 应用于 $K_2=K_3$。

因此我们可以假设 $\alpha+\beta>5$。最后一次应用 (3.1)，取 $E=\emptyset,\varepsilon=0$ 和 $c=2$，得到

$$3|K_2\setminus E|+20>30,$$

这意味着 $|K_2|\ge 4$。这里，我们将断言 3.7 应用于 $K_2\cup\{(x_1,y_1)\}$，由此再次导出矛盾。□

在讨论更大的素数之前，我们先简要说明定理 1.4 的证明与 Lev 在 [7] 中给出的定理 1.3 的证明有何关联。Lev 的证明可以分为与我们在本节开头概述的相同两个主要部分：一部分是找出一个较大的子空间，使得 $A$ 在其陪集中分布不均；另一部分则利用这一性质证明 $A$ 是正规的。

Lev 的证明与我们的证明之间的关键区别在于，在 [7], 中，那个较大的子空间是 $(n-1)$ 维的，并且是通过傅里叶论证得到的；而我们则采用归纳论证来找出一个 $(n-2)$ 维子空间。后者在证明的两个部分都带来了改进。首先，即使 $A$ 很小，归纳论证也能提供关于 $A$ 的强结构信息。相比之下，随着 $A$ 的规模减小，从傅里叶系数中提取的定量信息会迅速减少。其次，考虑一个 $(n-2)$ 维子空间，使我们能够利用诸如引理 3.1 这类关于二维无和集结构的洞见。

通过分析 $\mathbb{F}_5^k$ 中固定较小 $k \geq 3$ 下非正规无和集的结构，定理 1.4 似乎很可能得到进一步改进。然而，这种分析在 $k$ 中的复杂性会迅速增加，而且尚不清楚这种方法是否最终能够为 $\mathbb{F}_5^n$ 中对所有 $n$ 而言的最大非正规无和子集的大小给出精确界。

## 4. The proof of Theorem 1.6

在本节始终设 $p \geq 11$ 是一个模 3 同余于 2 的素数， $I = I_p$、 $m = m_p$ 和 $\alpha = 1/2 - 1/p$。我们不直接证明定理 1.6，而是证明以下命题，这对我们的归纳法证明更加方便。

命题 4.1. 设 $A \subset \mathbb{F}_p^n$ 是无和集，且 $u \in A$ 满足 $I(u) \subset A$ ，以及 $|A| \geq (m-\alpha)p^{n-1}$。则存在一个余维 1 的子空间 $V$，使得 $A \subset I(u) + V$。

由命题 4.1 证明定理 1.6。令 $n \in \mathbb{N}$ ，并令 $A \subset \mathbb{F}_p^n$ 为无和集，且其大小至少为 $(m-1/2+1/p)p^{n-1}$。显然，只需找到 $u \in \mathbb{F}_p^n$ ，使得 $I(u) \subset A$。 $\mathbb{F}_p^n$中有 $(p^n-1)/(p-1)$ 个一维子空间，并且我们注意到，每个 $v \in A$ 恰好包含在其中一个子空间中。因此， $\mathbb{F}_p^n$ 中的平均一维子空间包含

$$\frac{(p-1)|A|}{p^n-1} > \frac{(p-1)(p-1/2+1/p)}{3p} > \frac{p-2}{3}$$

$A$ 个元素。于是我们可以找到 $v \in \mathbb{F}_p^n$ ，使得 $A' = A \cap \langle v \rangle$ 满足 $|A'| = m$。由于 $(A'+A') \cap A' = \emptyset$，我们有 $|A'+A'| \leq 2m-1$。另一方面，根据 Kneser定理， $|A'+A'| \geq 2m-1$，因此由 Vosper 定理（引理 2.4）， $A'$ 必须是 $\langle v \rangle$ 中的等差数列。将 $v$ 乘以适当的因子后，我们得到 $u$ ，使得 $I(u) = A' \subset A$。□

为了证明命题 4.1，我们需要以下初等引理。

引理 4.2. 设 $d \in \{0, \ldots, m-1\}$ and $J \subset \{m-d, \ldots, 2m-1+d\}$ 是 $\mathbb{F}_p$ 的一个子集，其大小至少为 $d+1$，且包含在 $I$ 的某个平移中。那么 $\mathbb{F}_p \backslash (I+J) \subset \{|J|-d, \ldots, d-|J|\}$。

证明。由于 $J$ 包含在 $I$ 的某个平移中， $I+J$ 是一个区间。设 $x$ 是将 $J$ 视为 $\{0, \ldots, p-1\}$ 的子集时的最小元素。我们知道 $x \geq m-d > 0$ and$x \leq 2m+d-|J| \leq 2m-1$。因此， $I+J$ 包含

$$\{2m+d-|J|+m, \ldots, 0, \ldots, m-d+|J|-1+2m-1\} = \{d-|J|+1, \ldots, |J|-d-1\},$$

而取补集即可得到该引理。 □

命题 4.1 的证明。我们对 $n$ 使用归纳法来证明该断言，其中基例 $n=1$ 显然成立。因此，假设 $n \geq 2$， $A \subset \mathbb{F}_p^n$ 是无和的，并且不失一般性，

有 $I(e_1) \subset A$。对于一个元素 $v \in \mathbb{F}_p^n$，我们定义 $A_v$ 为 $\mathbb{F}_p$ 的唯一子集，使得$A_v(e_1) = (A - v) \cap \langle e_1 \rangle$。特别地， $A_0 = I$，并且对所有 $v \in \mathbb{F}_p^n$，$(A_0 + A_v) \cap A_v = \emptyset$。根据 Kneser定理，这意味着对所有 $v$， $|A_v| \leq m$；但与此同时， $A_v$ 的平均大小至少为 $m - \alpha$。这使我们能够得出结论：对大多数$v$， $|A_v| \geq m$。我们将这样的 $v$ 称为好的，而将 $v$ 称为坏的。

注意，如果 $v$ 是良好的，那么根据 Kneser定理和 Vosper 定理， $A_v$ 必须是区间 $I$ 的一个平移，即对于某个 $t_v \in \mathbb{F}_p$，有 $A_v = t_v + I$。此外，不同 $v$ 对应的这些偏移量 $t_v$ 之间存在某些关系，下面的命题刻画了这些关系。

命题 4.3. 对所有良好的 $v$、$w$，我们有

$$A_{v+w} \subset t_v + t_w + I \tag{4.1}$$

*and*

$$A_{v-w} \subset t_v - t_w + I. \tag{4.2}$$

证明。注意到 $I + I = I - I = \mathbb{F}_p \setminus I$，我们有

$$A_{v+w} \subset \mathbb{F}_p \setminus (A_v + A_w) = t_v + t_w + (\mathbb{F}_p \setminus (I + I)) = t_v + t_w + I$$

and

$$A_{v-w} \subset \mathbb{F}_p \setminus (A_v - A_w) = t_v - t_w + (\mathbb{F}_p \setminus (I - I)) = t_v - t_w + I.$$

□

由于良好的 $v$ 很多，我们将能够得出结论：即使对于不好的 $v$，集合 $A_v$ 也包含在某个 $I$ 的平移中。证明的其余部分旨在确保这些平移确实相对于某个余维 1 子空间 $V$ 对齐。为此，我们首先构造一个合适的候选 $V$；而这一任务的处理方法取决于 $n$ 是 2 还是大于 2。我们先讨论前一种情况。

命题 4.4. 假设 $n = 2$。存在一个维数为 1 的子空间 $V \subset \mathbb{F}_p^2$，使得$A \cap V = A \cap (e_1 + V) = A \cap (-e_1 + V) = \emptyset$。

命题 4.4 的证明。取任意一个元素 $v \in \mathbb{F}_p^2 \setminus \langle e_1 \rangle$，并考虑集合 $G = \{x \in \mathbb{F}_p : |A_{xv}| = m\}$。通过简单的计数论证， $G$ 的大小至少为 $p/2 + 1$，因此必定存在一个非零的 $x$，使得 $A_{xv}$ 和 $A_{2xv}$ 都属于 $G$。不妨假设 $x = 1$ 且 $t_v = 0$；这总可以通过先对 $v$ 进行缩放，再将其平移一个适当的 $e_1$ 倍来实现。根据 (4.1)，这也意味着 $t_{2v} = 2t_v = 0$。

我们将 $\mathbb{F}_p^*$划分为 $H = \{2, 4, \ldots, p-1\}$ 和 $H-1$。假设$\sum_{x \in H} |A_{xv}| \geq \sum_{x \in (H-1)} |A_{xv}|$。特别地，我们必有

$$\sum_{x \in H} m - |A_{xv}| \leq \frac{(p-1)m}{2} - \frac{(m-\alpha)p - m}{2} = \frac{\alpha p}{2} < m - 1,$$

由于左侧的和是一个整数，因此它必定不超过 $m-2$。将$H$ 视为 $\mathbb{N}$的子集，我们定义

$$f \colon H \to \mathbb{N}_0 \qquad x \mapsto \sum_{\substack{z \in H \\ z < x}} m - |A_{zv}|.$$

注意，对于所有 $x \in H$，我们都有 $f(x) \leq m - 2 - (m - |A_{xv}|) = |A_{xv}| - 2$；并且由于 $|G| > p/2$，根据 (4.1) 和引理 2.2， $A_{xv}$ 对所有 $x \in \mathbb{F}_p$ 都必须包含在 $I$ 的某个平移中。

利用引理 4.2 以及 $A_{2v} = I$ 这一事实，我们因此可以归纳证明，对于所有 $x \in H$， $A_{xv} \subset \{m - f(x)....., 2m - 1 + f(x)\}$。最后，利用 $A_v = I$，我们可以再次对所有 $x \in H$ 应用引理 4.2 于 $A_{xv}$，从而得到 $A_{x-1} \subset \{2, \dots, 3m-3\}$。取 $V = \langle v \rangle$ 即可得到所需的子空间。若 $\sum_{x \in (H-1)} |A_{xv}| > \sum_{x \in H} |A_{xv}|$，我们可以交换 $H$ 和 $H-1$ 的角色，并以类似方式论证。□

对于 $n \geq 3$，论证稍长一些，但大部分内容归结为相当简单的线性代数。

断言 4.5。假设 $n \geq 3$。存在一个余维 1 子空间 $V \subset \mathbb{F}_p^n$，使得$A \cap V = A \cap (e_1 + V) = A \cap (-e_1 + V) = \emptyset$。

断言 4.5 的证明。由引理 2.3，存在两个不同的余维 1 子空间 $W_1$ 和 $W_2$，使得 $\langle e_1 \rangle \subset W_1 \cap W_2$ 和 $|A \cap W_1|, |A \cap W_2| \geq |A|/p$。对于 $i \in \{1, 2\}$，我们可以对 $A \cap W_i$ 应用归纳假设，从而得到存在一个 $(n-2)$ 维子空间 $V_i < W_i$，使得 $A \cap W_i$ 包含于 $I(e_1) + V_i$。注意， $|A \cap W_i|$ 大于 $|V_i|$，因此 $e_1$ 不可能包含于 $V_i$；又由于 $e_1 \in W_1 \cap W_2$，我们可以得出 $\dim V_1 \neq V_2$。

现在假设 $e_1 \in V_1 + V_2$。由此可得 $W_1$、$W_2 \subset V_1 + V_2$，进而对于所有 $x_1$、$x_2 \in \mathbb{F}_p$，有 $(x_1 e_1 + V_1) + (x_2 e_1 + V_2) = \mathbb{F}_p^n$。根据平均论证，必存在 $x_1$、$x_2 \in \mathbb{F}_p$，使得对于 $i \in \{1, 2\}$，

$$|A \cap (x_i e_1 + V_i)| \geq \frac{|A|}{mp} \geq p^{n-2}(1 - \alpha/m).$$

同时，$V_1 + V_2 = \mathbb{F}_p^n$ 也意味着 $\dim V_1 \cap V_2 = n - 4$，因此 t

$$|A \cap (x_1 e_1 + V_1)||A \cap (x_2 e_1 + V_2)| \leq |V_1 \cap V_2||A + A| = p^{n-4}|A + A|.$$

由此可得 $|A + A| \geq (1 - \alpha/m)^2 p^n > 3p^n/4$，但这不可能成立，因为 $A$ 是无和的，且 $|A| > p^n/4$。因此，必有 $e_1 \notin V_1 + V_2$，从而 $\dim V_1 \cap V_2 = n - 3$。令 $V = V_1 + V_2$，我们得出 $\dim V = n - 1$。

对于 $v \in V$，令 $v^{(1)} \in V_1$、$v^{(2)} \in V_2$ 满足条件，使得 $|A_{v^{(1)}}| + |A_{v^{(2)}}|$ 在满足 $v^{(1)} + v^{(2)} = v$ 的情况下取最大值。显然，最大值至少不小于平均值，因此

$$|A_{v^{(1)}}| + |A_{v^{(2)}}| \geq p^{-(n-3)} \sum_{\substack{w^{(1)} \in V_1, w^{(2)} \in V_2 \\ w^{(1)} + w^{(2)} = v}} |A_{w^{(1)}}| + |A_{w^{(2)}}|. \tag{4.3}$$

另一方面，我们知道 $A_v \subset \mathbb{F}_p \backslash (A_{v^{(1)}} + A_{v^{(2)}})$，并且对所有 $w \in V_1 \cup V_2$ 都有 $A_w \subset I$，由此可得（根据 $\mathbb{F}_p$ 的 Kneser定理）

$$|A_v \cap I| \geq |A_v| - (2m - 1 - |A_{v^{(1)}} + A_{v^{(2)}}|) \geq |A_v| + |A_{v^{(1)}}| + |A_{v^{(2)}}| - 2m.$$

对所有 $v \in V$ 求该不等式的和，并代入 (4.3)，得到

$$\begin{aligned}
\sum_{v \in V} |A_v \cap I| &\geq \sum_{v \in V} \Big( |A_v| - 2m + p^{-(n-3)} \sum_{\substack{w^{(1)} \in V_1, w^{(2)} \in V_2 \\ w^{(1)} + w^{(2)} = v}} |A_{w^{(1)}}| + |A_{w^{(2)}}| \Big) \\
&= |A| - 2mp^{n-1} + p^{-(n-3)} \sum_{w^{(1)} \in V_1, w^{(2)} \in V_2} |w^{(1)} + A_{w^{(1)}}(e_1)| + |w^{(2)} + A_{w^{(2)}}(e_1)| \\
&= |A| - 2mp^{n-1} + p|A \cap W_1| + p|A \cap W_2|.
\end{aligned}$$

结合上述结果以及 $|A| \geq (m-\alpha)p^{n-1}$ 和 $|A \cap W_i| \geq (m-\alpha)p^{n-2}$ 在 $i \in \{1,2\}$ 时的界，我们得到

$$|A \cap (I(e_1)+V)| = \sum_{v \in V} |A_v \cap I| \geq (m-3\alpha)p^{n-1}.$$

我们有 $(m-3\alpha)/m > 1/2$，因此通过抽屉原理论证，存在 $x \in \mathbb{F}_p$使得 $|A \cap (\{xe_1,(x+1)e_1\}+V)| > p^{n-1}$。根据引理 2.2,

$$e_1 + V \subset (A \cap ((x+1)e_1+V)) - (A \cap (xe_1+V))$$

and

$$-e_1 + V \subset (A \cap (xe_1+V)) - (A \cap ((x+1)e_1+V)),$$

于是 $A \cap (\{\pm e_1\}+V) = \emptyset$。此外，我们必有 $|A \cap (xe_1+V)| > 1/2$或 $|A \cap ((x+1)e_1+V)| > 1/2$，从而得到 $A \cap V = \emptyset$，如所需。□

为完成命题 4.1 的证明，设 $V \subset \mathbb{F}_p^n$ 是一个余维 1 的子空间，使得 $A \cap V = A \cap (e_1+V) = A \cap (-e_1+V)) = \emptyset$。还需证明 $V$ 满足 $A \subset I(e_1)+V$。令 $G$ 为 $V$ 中好元素的集合。注意到 $e_1 \notin V$，我们看到集合族 $(v+\langle e_1\rangle)_{v \in V}$ 是 $\mathbb{F}_p^n$ 的一个划分，并且可以利用界 $|A_v| \leq m$ 证明 $G$ 必须很大。具体而言，我们有

$$(m-\alpha)p^{n-1} \leq |A| \leq m|G| + (m-1)(p^{n-1}-|G|) = mp^{n-1} + |G| - p^{n-1},$$

因此

$$|G| \geq (1-\alpha)p^{n-1} \geq p^{n-1}/2 + p^{n-2}, \tag{4.4}$$

这意味着 $G+G=V$。注意，由 (4.1) 可知，只要证明对所有好的 $v$ 都有 $t_v = 0$，证明便告完成。事实上，由于 $G+G=V$，对每个 $v \in V$，都存在元素 $v^{(1)}$、$v^{(2)} \in G$，使得 $v = v^{(1)} + v^{(2)}$，因此 $A_v \subset t_{v^{(1)}} + t_{v^{(2)}} + I = I$。

为此，我们先定义 $L = \{v \in G : t_v \in \{-(m-1)\ldots,0\}\}$, $R = \{v \in G : t_v \in \{0,\ldots,m-1\}\}$, $C = L \cap R$, $L^+ = L \setminus C$，以及 $R^+ = R \setminus C$。注意，$L^+ \cup R = L \cup R^+ = G$，因为 $t_v \notin \{-(m-1)\ldots,m-1\}$ 意味着 $A_v$ 包含 0，从而 $v \in A \cap V$，这与我们的假设 $A \cap V = \emptyset$ 矛盾。不妨将 $C$ 中的元素视为对应于处在所需“中心”位置的行的指标，而 $L^+$ 和 $R^+$ 则表示处于该中心位置“左侧”或“右侧”的行。这些集合的用处在于，它们在加法下封闭，即

$$(L^+ + L) \cap G \subset L^+ \qquad \text{and} \qquad (R^+ + R) \cap G \subset R^+. \tag{4.5}$$

例如，考虑 $v^{(1)} \in L^+$ 和 $v^{(2)} \in L$，使得 $v^{(1)} + v^{(2)} \in G$。由 (4.1)，$t_{v^{(1)}+v^{(2)}}$ 属于集合 $\{-2(m-1)\ldots,-1\} \subset G \setminus R$，因此实际上属于 $L^+$，因为 $G = L^+ \cup R$。

通过类似的论证，我们还可以得出

$$(L^+ - R) \cap G \subset L^+ \qquad \text{and} \qquad (R^+ - L) \cap G \subset R^+. \tag{4.6}$$

我们要证明 $C = G$，因此反设 $L^+$ 或 $R^+$至少有一个非空；不失一般性，设 $L^+$非空。

我们首先假设 $R^+$ 为空，因此 $L = G$。记 $V$中的坏元素集合为 $B = V \setminus G$，由 (4.5) 可推得 $L^+ + L \subset L^+ \cup B$。我们知道 $L^+$ 是一个真

子集 $G$，因为 $0 \in C$，因此 $L^+ \cup B \neq V$ 且 $|\mathrm{Sym}(L^+ + L)| \leq p^{n-2}$。由此，根据Kneser定理，我们得到

$$|L^+| + |B| \geq |L^+ + L| \geq |L^+| + |G| - p^{n-2}.$$

但这意味着 $|G| \leq |B| + p^{n-2} \leq \alpha p^{n-1} + p^{n-2} = p^{n-1}/2$，与 (4.4) 矛盾。

如果 $R^+$ 非空，我们则改为考虑集合 $L^+ - R$ 和 $R^+ - L$。由 (4.6) 可知，前者包含于 $L^+ \cup B$，后者包含于 $R^+ \cup B$。遗憾的是，这不足以完全按照之前的方式进行论证，但我们可以利用以下观察。每当有 $v \in (L^+ - R) \cap (R^+ - L)$ 时，$v$ 不仅是坏的，而且是双重坏的，也就是说，$|A_v| \leq m - 2$。事实上，必定存在 $v^{(1)} \in L^+$、$v^{(2)} \in R$、$w^{(1)} \in R^+$ 和 $w^{(2)} \in L$，使得 $v = v^{(1)} - v^{(2)} = w^{(1)} - w^{(2)}$。由 (4.2)，这意味着

$$A_v \subset (t_{v^{(1)}} - t_{v^{(2)}} + I) \cap (t_{w^{(1)}} - t_{w^{(2)}} + I). \tag{4.7}$$

我们有 $s_L := t_{v^{(1)}} - t_{v^{(2)}} \in \{-2(m-1), \ldots, -1\}$ 以及 $s_R := t_{w^{(1)}} - t_{w^{(2)}} \in \{1, \ldots, 2(m-1)\}$。如果 $s_L \in \{-2(m-1), \ldots, -m\}$，那么 $(s_L + I)$ 至少包含 $-1$、0 和 1 中的两个。但 $A_v$ 不可能包含这三个点中的任何一个，因为这样 $A$ 就会包含 $v - e_1$、$v$ 或 $v + e_1$，这与假设不符。因此，在这种情况下，我们可以得出 $|A_v| \leq m - 2$。

因此，我们不妨假设 $s_L \in \{-(m-1), \ldots, -1\}$，同样地假设 $s_R \in \{1, \ldots, (m-1)\}$。根据 (4.7)，我们有

$$\begin{aligned} A_v &\subset (\{-(m-1), \ldots, -1\} + I) \cap (\{1, \ldots, (m-1)\} + I) \\ &= \{1, \ldots, 2m-2\} \cap \{m+1, \ldots, 3m-2\} \\ &= \{m+1, \ldots, 2m-2\}. \end{aligned}$$

后一个集合本身的大小仅为 $m - 2$，因此 $|A_v| \leq m - 2$。

既然我们已经证明每个 $v \in (L^+ - R) \cap (R^+ - L)$ 都是双重坏的，便可得出

$$|A| = \sum_{v \in V} |A_v| \leq mp^{n-1} - |B| - |(L^+ - R) \cap (R^+ - L)|.$$

结合 $|A| \geq (m - \alpha)p^{n-1}$，可得 $|B| + |(L^+ - R) \cap (R^+ - L)| \leq \alpha p^{n-1}$；由容斥原理和 (4.6)，我们有

$$\begin{aligned} |L^+ - R| + |R^+ - L| &= |(L^+ - R) \cup (R^+ - L)| + |(L^+ - R) \cap (R^+ - L)| \\ &= |L^+ \cup R^+ \cup B| + |(L^+ - R) \cap (R^+ - L)| \\ &= |L^+| + |R^+| + |B| + |(L^+ - R) \cap (R^+ - L)| \\ &< |G| + \alpha p^{n-1}, \end{aligned} \tag{4.8}$$

最后一个不等式之所以严格，是因为 $0 \in C$。出于同样的原因，我们可以断言 $|\mathrm{Sym}(L^+ - R)|, |\mathrm{Sym}(R^+ - L)| \leq p^{n-2}$，因此由Kneser定理，

$$|L^+ - R| + |R^+ - L| \geq 2(|G| - p^{n-2}). \tag{4.9}$$

结合 (4.8) 和 (4.9)，我们得到 $|G| < \alpha p^{n-1} + 2p^{n-2} = p^{n-1}/2 + p^{n-2}$，这与 (4.4) 矛盾。命题 4.1 的证明至此完成。□

致谢。作者感谢其导师 Julia Wolf 对本文早期版本提出的宝贵意见。他还要感谢 Vsevolod Lev 与他进行了一次有趣的交流，并由此发现了例 1.5。

## References

[1] W. E. Clark 和 J. Pedersen。“GF(2) 上向量空间中的无和集”。组合理论杂志 A 辑 61(2) (1992)，第 222–229 页。 DOI：10.1016/0097-3165(92)90019-Q。[2] A. A. Davydov 和 L. M. Tombak。“具有距离 4 的准完美线性二元码与射影几何中的完全弧”。信息传输问题 25(4) (1989)，第 11–23 页。[3] P. H. Diananda 和 H. P. Yap。“有限群元素的极大无和集”。日本学士院院刊 45 (1969年)，第 1–5 页。 DOI：10.3792/pja/1195520891。[4] B. Green 和 I. Z. Ruzsa。“阿贝尔群中的无和集”。以色列数学杂志 147 (2005)，第 157–188 页。 DOI：10.1007/BF02785363。[5] M. Kneser。“和集渐近密度的估计”。数学杂志 58 (1953)，第 459–484 页。 DOI：10.1007/BF01174162。[6] V. F. Lev。“三元空间中的大型无和集”。组合理论杂志 A 辑 111(2) (2005)，第 337–346 页。 DOI：10.1016/j.jcta.2005.01.004。[7] V. F. Lev。“ $Z_5^n$中的无和集”（2023）。arXiv：1910.06436。[8] A. H. Rhemtulla 和 A. P. Street。“有限阿贝尔群中的极大无和集”。澳大利亚数学会通报 2 (1970)，第 289–297 页。 DOI：10.1017/S000497270004199X。[9] T. Tao 和 V. Vu。《加法组合学》。剑桥高等数学研究丛书 105。剑桥大学出版社，剑桥，2006。 DOI：10.1017/CBO9780511755149。[10] A. G. Vosper。“素数阶群子集的临界对”。伦敦数学会杂志 31 (1956)，第 200–205 页。 DOI：10.1112/jlms/s1-31.2.200。[11] H. P. Yap。“有限阿贝尔群中的极大无和集 IV”。南塔数学 5(3) (1972)，第 70–75 页。[12] H. P. Yap。“有限阿贝尔群中的极大无和集 V”。澳大利亚数学会通报 13(3) (1975)，第 337–342 页。 DOI：10.1017/S0004972700024588。[13] H. P. Yap。“群元素的极大无和集”。伦敦数学会杂志 44 (1969年)，第 131–136 页。 DOI：10.1112/jlms/s1-44.1.131。

Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, United Kingdom*Email address*: lvv23@dpmms.cam.ac.uk