arXiv:2304.01777v1 [math.CO] 4 Apr 2023

关于 $\mathbb{Z}_p^2$ 中某些集合的子集和分布

´诺伯特·海吉瓦里

Abstract. 若给定的自然数子集 A 满足其中每个元素都能表示为从 A 中取出的互不相同的项之和，则称该子集为完备的。这个课题与背包问题密切相关，而背包问题是一个已知的 NP 完全问题。

有趣的是，若 A 和 B 是完备数列，则 $A \times B$ 在 $\mathbb{N}^2$ 中未必是完备的。本文考虑这一问题的模版本，其动机来自 [2] 的通信复杂度问题。

2010 年 AMS 分类：主分类 11B30、11B39；次分类 11B75

关键词：子集和、加法组合学、特殊图中的匹配

1. Introduction

令 $\mathbb{S}$ 为任意加法半群。对于集合 A、$B \subset \mathbb{S}$，其和定义为 $A \pm B := \{a \pm b : a \in A; \quad b \in B\}$。对于任意 $X \subseteq \mathbb{S}$，令

$$FS(X) := \{\sum_{i=1}^{\infty} \varepsilon_i x_i : \ x_i \in X, \ \varepsilon_i \in \{0,1\}, \ \sum_{i=1}^{\infty} \varepsilon_i < \infty\},$$

并且可以将子集和的概念 $FS(X)$ 扩展到更高维的情形，即当$X \subseteq \mathbb{S}^k; k \geq 1$时。若集合 $X \subseteq \mathbb{S}$ 中的每个元素都能表示为从 X 中取出的若干互不相同项之和，则称 $X \subseteq \mathbb{S}$ 关于 $\mathbb{S}$ 是完备的。如果 $\mathbb{S} = \mathbb{N}$，关于这一主题已有大量文献（例如，可参见 [6], [10] 和 [12] 中的综述）。

这类问题与背包问题或子集和问题密切相关。问题是给定正整数 $a_1, a_2, \ldots, a_n$ 和一个整数 m，判断集合 $\{a_j\}$ 是否存在一个子集，其元素之和为 m。这通常被称为1

NP完全问题。这个主题也与一些通信复杂度问题有关（例如参见 [2]），这正是本研究的动机。

高维中的完备性与一维情形大不相同。例如，一个经典结果是，如果一个级数在 $n > n_0$ 以内包含超过 $c\sqrt{n}$ 个元素，那么它就是完备的（见 [12]）。而在二维情形中，可以给出一个稠密集 A，使得 $FS(A)$ 甚至不包含算术级数（见 [8] 和 [9]）。更多结果可见 [1] 和 [4]。

令 F_n 为 n^{th} 斐波那契数，即令 $F_0 = 0$； $F_1 = 1$，且对于 $n \geq 0$ $F_{n+2} = F_{n+1} + F_n$。对于负整数，令 $F_{-n} = (-1)^{n-1}F_n$，使递归公式同样成立。第 2 节将考察 $\mathbb{Z}_p^2$ 中三个集合的子集和分布。

更确切地说，令 $A_1 = \{2^n\}_{n=0}^{\infty} \times \{F_n\}_{n=0}^{\infty}$、 $A_2 = \{2^n\}_{n=0}^{\infty} \times \{2^n\}_{n=0}^{\infty}$ 和 $A_3 =\{F_n\}_{n=0}^{\infty} \times \{F_n\}_{n=0}^{\infty}$。我们将证明，对于几乎所有的 prim p， $FS(A_i)$ (mod p) $= \mathbb{Z}_p^2 (i = 1, 2, 3)$。对于 $X \subseteq \mathbb{N}^2$ X (mod p) $= \{(v_1, v_2) \in \mathbb{Z}_p^2 : \exists (x_1, x_2) \in X;\ v_i \equiv x_i (\text{mod } p);\ i = 1, 2\}$。

此外，我们将分析扩展到类型为 $A_4 = \{b^n\}_{n=0}^{\infty} \times \{F_n\}_{n=0}^{\infty}$ and $A_5 = \{b^n\}_{n=0}^{\infty} \times \{2^n\}_{n=0}^{\infty}$ 的集合，其中 $b > 2$ integer。尽管集合 $\{b^n\}_{n=0}^{\infty}$ 对于 $b > 2$ 并不完整，但请注意， b^n 可以作为集合 A_4 和 A_5 中的一个坐标出现无界多次。因此，由于所有正整数都可以用 b 进制表示，这个问题便与前面的问题相契合。

在 [2] 中，我们也在 $\mathbb{N}^2$中研究上述问题。有趣的是，上述集合的分布与 $\mathbb{Z}_p^2$中的分布不同。例如，对于 $i = 1$、2 和 3，我们描述了满足 $\mathbb{N}^2 \setminus E_i \subseteq FS(A_i)$的集合 E_i。此外，我们证明 E_i 包含任意“大的”正方形，其中不含来自 $FS(A_i)$的元素；还包含大小为 $k \times k$的正方形，其中含有来自 $FS(A_i)$的 $k \log k$ 个元素。

2. Modular case

本节将证明以下定理:

定理 2.1。存在一个 $\delta > 0$ ，使得除至多 $O(x/(\log x)^{1+\delta})$ 个素数$p \leq x$ 外，对所有 $|FS(A_4)$（模 $p)| \geq \frac{p^2}{b}$.

当 $b = 2$ 时，前一个定理说明 $|FS(A_1) \pmod p| \geq \frac{p^2}{2}$. 但在这种情况下，我们还能得到更强的结论:

定理 2.2. 存在一个 $\delta > 0$ ，使得除至多 $O(x/(\log x)^{1+\delta})$ 个素数$p \leq x$外，对于所有 $FS(A_1)$ (模 $p) = \mathbb{Z}_p^2$。

下述定理可用与定理 2.2 类似的方法证明。

定理 2.3. 存在一个 $\delta > 0$ ，使得除去至多 $O(x/(\log x)^{1+\delta})$ 个素数$p \leq x$外，对于所有 FS，都有 $A_i \pmod p = \mathbb{Z}_p^2 (i = 2, 3)$。

定理 2.2 的证明。令 $\mathcal{P}_1$ 为所有不超过 x 且满足 $|\pmod p\{2^n\}_{n=0}^{\infty}| > 2\sqrt{p}$ 的素数集合，令 $\mathcal{P}_2$ 为所有不超过 x 且满足 $|\pmod p\{F_n\}_{n=0}^{\infty}| > 2\sqrt{p}$ 的素数集合。记为 $\mathcal{P} = \mathcal{P}_1 \cap \mathcal{P}_2$。我们将验证，除去至多 $O(x/(\log x)^{1+\delta})$ 个素数 $p \leq x$外，所有 $p \leq x$都属于 $\mathcal{P}$。

我们需要以下引理

引理 2.4. 存在一个 $\delta > 0$，使得除去至多 $O(\frac{x}{(\log x)^{1+\delta}})$ 个素数 $p \leq x$ 外，我们有

$$|\{F_n\}_{n=0}^{\infty} \pmod p| > 3\sqrt{p}, \tag{1}$$

其中，当 x 足够大时， $\delta > 0.086072$ 是可容许的。

这是 [7, 引理 3.1] 的一个小改动。

引理 2.5. 存在一个 $\delta > 0$，使得

$$|\{b^n\}_{n=0}^{\infty} \pmod p| > 2\sqrt{p} \tag{2}$$

除去至多 $O(x/(\log x)^{1+\delta})$ 个素数 $p \le x$ 外。可以像前一个引理中那样选取 δ。

这个引理是定理 3（见 [5]）的直接推论。

利用这些引理可知，除去至多 $O(x/(\log x)^{1+\delta})$ 个素数 $p \le x$ 外，(2) 和 (1) 均成立。将这些素数构成的集合记为 $\mathcal{P}$，于是对每个 $p \in \mathcal{P}$，$T := |\{b^n\}_{n=0}^{\infty} \pmod p| > 2\sqrt{p}$ 和 $R := |\{F_n\}_{n=0}^{\infty} \pmod p| > 2\sqrt{p}$ 均成立。（仅当假设 $b > 2$ 时，我们才需要引理 2.4 中的因子 3，见第 2.1 节。）证明的第三个要素如下:

引理 2.6（Olson）。设 $A = \{a_1, \ldots, a_k\}$ 是模素数 p 的互不相同的非零剩余类。若 $k > 2\sqrt{p}$，则 $FS(A) = \mathbb{Z}_p$。

参见 [11] 中的证明。从现在起，在本节中我们假设 $b = 2$。记 $\{F_n\}_{n=0}^{\infty} = \{F_{j_1}, F_{j_2}, \ldots, F_{j_R}\} \pmod p$ 和 $\{2^n\}_{n=0}^{\infty} = \{2^{i_1}, 2^{i_2}, \ldots, 2^{i_T}\} \pmod p$。取 $\mathbb{Z}_p^2$ 中任意一点 (v_1, v_2)。由引理 2.6，可将 v_1 写成 $v_1 = \sum_{m=1}^{T} \varepsilon_m 2^{i_m}$；$\varepsilon_m \in \{0, 1\}$ 的形式，并将 v_2 写成 $v_2 = \sum_{k=1}^{R} \eta_k F_{j_k}$；$\eta_k \in \{0, 1\}$ 的形式。

首先假设 $\sum_{m=1}^{T} \varepsilon_m > \sum_{k=1}^{R} \eta_k$。我们将找出一个子集 $\{F'_{j_n}\}$，使得 $\sum_{n=1}^{V} \zeta_n F'_{j_n} = v_2$、$\zeta_n > 0$ 和 $\sum_n \zeta_n = T$。注意，我们允许 ζ_n 大于一，也就是说，我们允许某些 F'_j 重复出现。于是，元素 $(2^{i_1}, F'_{j_1})$、$(2^{i_2}, F'_{j_2})$、.....、$(2^{i_T}, F'_{j_T})$ 两两不同（因为它们的第一坐标两两不同），并且 $\sum_{t=1}^{T} (2^{i_t}, F'_{j_t}) = (v_1, v_2)$，正如我们所希望的。

因此取 F_{i_1}，并找到一个元素 F_r，使得 $r > \sum_{m=1}^{T} \varepsilon_m$ 且 $F_r \equiv F_{i_1} \pmod p$。由于序列 F_n 是周期性的（模 p），这样的 r必定存在。现在将F_r 改为 $F_{r-1} + F_{r-2}$。总共重复这一更改过程 $\sum_{m=1}^{T} \varepsilon_m - \sum_{k=1}^{R} \eta_k$次（即将 F_{r-1} 改为 $F_{r-2} + F_{r-3}$，等等）。由于 $r > \sum_{m=1}^{T} \varepsilon_m$ 这一过程

已经终止。然后，我们可以将二的幂的各项与相应的斐波那契数（可能重复出现）相匹配。

当 $\sum_{m=1}^{T}\varepsilon_m < \sum_{k=1}^{R}\eta_k$ 时，过程相同；只需注意，我们将一项 2^m 替换为 $2^{m-1}+2^{m-1}$。□

2.1. 当 $b>2$ 时的情形。在一般情形下，我们给出 $FS(A_4)$（模 p）基数的一个上界，其中 $A_4=\{b^n\}_{n=0}^{\infty}\times\{F_n\}_{n=0}^{\infty}$

定理 2.1 的证明。设 $p\in\mathcal{P}$。将（模 p）$\{F_n\}_{n=0}^{\infty}=\{F_{j_1},F_{j_2},\dots,\}$ 拆分为两个不相交的部分 $G_1\cup G_2$，其中 $|G_2|=b-1$。记（模 p）$\{b^n\}_{n=0}^{\infty}=\{b^{i_1},b^{i_2},\dots,b^{i_T}\}$、$G_1=\{Fi_1,F_{i_2},\dots,F_{i_V}\}$ 和 $G_2=\{F_{s_1},F_{s_2},\dots,F_{s_{b-1}}\}$。根据假设和引理 2.5，我们得到 $V=|G_1|>2\sqrt{p}$。由引理 2.6 可知，对于任意 (v_1,v_2)，$\in\mathbb{Z}_p^2$ v_1 可写为 $\sum_{k=1}^{T}\varepsilon_k b^{i_k}$；$\varepsilon_k\in\{0,1\}$，而 v_2 可写成 $v_2=\sum_{k=1}^{V}\eta_k F_{j_k}$；$\eta_k\in\{0,1\}$。

假设 $\sum_{m=1}^{T}\varepsilon_m>\sum_{k=1}^{V}\eta_k$。然后按照前面的过程 s.

因此，假设 $\sum_{m=1}^{T}\varepsilon_m<\sum_{k=1}^{V}\eta_k$。然后取一个足够大的 m，使得$b^m\equiv b^{i_1}$（模 p），并改变 $b^m=b^{m-1}+b^{m-1}+\cdots+b^{m-1}$（$m$ 次）。重复这一过程，每一步将项数增加 b 个元素。如果某一步的项数恰好为 $\sum_{k=1}^{V}\eta_k$，则我们就完成了。否则，某次重复会使项数超过 $\sum_{k=1}^{V}\eta_k$，超出 r 个元素，并且显然 $\min r\le b-1$。然后用项 F_{s_1}、F_{s_2}、.....、F_{s_r} 补全和 $\sum_{k=1}^{V}\eta_k F_{j_k}$，我们便能在 FS（A_4）模 p 下表示（v_1，$v_2+\sum_{t=1}^{r}F_{s_t}$）。

考虑一种对 $\mathbb{Z}_p^2$ 按照 $\sum_{t=1}^{r}F_{s_t}$ 的值着色的方式；$(r=0,1,\dots b-1)$，即若 $(v_1,v_2+\sum_{t=1}^{r}F_{s_t})$ 属于 $FS(A_4)$（模 p），则令 (v_1,v_2) 的颜色为 r。注意，这种着色并不唯一；(v_1,v_2) 和 (v_1',v_2') 可以具有相同的颜色。为清楚起见，取颜色 r 为最小值。记 L_r 为颜色为 r 的点集。现在选择使$|L_{r_0}|$ 最大的 $L_{r_0}\subseteq\mathbb{Z}_p^2$。我们有 $|L_{r_0}|\ge\frac{p^2}{b}$。于是 $L_{r_0}+\sum_{t=1}^{r_0}F_{s_t}\subseteq FS$（$A_4$）（模 p），且 $|L_{r_0}+\sum_{t=1}^{r_0}F_{s_t}|=|L_{r_0}|\ge\frac{p^2}{b}$。

□

Acknowledgment

本研究由国家研究、发展与创新办公室 NKFIH 的 K-129335 号资助项目支持。

References

[1] B. Bakos, P´alfy, 《关于使用伪递归数列子集和的一种加密方法的一些结果》, 《离散数学快报》5：1，第 63–67 页，5 页（2021）[2] B. Bakos, N. Hegyv´ari and M. P´alfy, 《组合数论中的一个通信复杂度问题》, 《莫斯科组合学杂志》, 第 10 卷（2021），第 4 期，297–302, DOI：10.2140/moscow.2021.10.297[3] B. Bakos, N. Hegyv´ari and M. P´alfy, 《关于 Z $\mathbb{N}^2$ 中某些集合的子集和的分布》, 进行中[4] Chen, YG；Fang, JH；Hegyv´ari, N, 《Z $\mathbb{N}^r$ 中的 Erd˝os–Birch 型问题》, 《数论杂志》187，第 233–249 页，17 页（2018）[5] P. Erd˝os 和 M. R. Murty, 《关于模 p 的阶》, 载于: 《数论》（加拿大安大略省渥太华，1996），《CR M 会议论文集与讲义》19（美国数学会，罗得岛州普罗维登斯，1999），第 87–97 页。[6] P. Erd˝os，R.L. Graham, 《组合数论中的新旧问题与结果》, 《数学教学论专著》´ematique[7] Garcia V, Luca F 和 Mejia J., 《模 p 的斐波那契数之和》, 《澳大利亚数学会通报》83(03):413–419，DOI：10.1017/S0004972710001693[8] Hegyv´ari, N., 《Z $\mathbb{N}^2$ 中的完备数列》, 《欧洲组合学杂志》（17）（1996）741–749。[9] Hegyv´ari, N, 《子集和》, 《组合学、概率与计算》（5）（1996）393–402。[10] N.B. Nathanson, 《加法数论》, 施普林格出版社，纽约，1996[11] J. E. Olson, 《模 p 加法定理》, 《组合学理论杂志》5（1968），45–52[12] T. Tao, V. Vu, 《加法组合学》, 剑桥大学出版社，剑桥，2006

Norbert Hegyvári, ELTE TTK, Eötvös University, Institute of Mathematics, H-1117 Pázmány st. 1/c, Budapest, Hungary and Alfréd Rényi Institute of Mathematics, H-1364 Budapest, P.O.Box 127.

电子邮件地址：hegyvari@renyi.hu