Three Constructions of Cap Sets in $\mathbb{Z}_4^n$

presented by Hein Thant AUNG (1155173220)

April 18, 2023

Let $r_3(\mathbb{Z}_4^n)$ be the largest size of a subset $A \subseteq \mathbb{Z}_4^n$ that does not contain a proper arithmetic progression of length 3. That is, whenever $x, y, z \in A$ satisfy $x + z = 2y$, at least two of x, y, z must be equal. A recent paper of Elsholtz and Pach (2020) deeply explores the lower bounds for $r_3(\mathbb{Z}_4^n)$ by extending the well-known constructions for $\mathbb{Z}$, and gives the exact value of $r_3(\mathbb{Z}_4^n)$ for $n \leq 5$. The result that we are interested in today is the following asymptotic bound.

Theorem 1. There exists a constant C such that

$$r_3(\mathbb{Z}_4^n) \geq Cn^{-1/2}3^n.$$

We will explore three different constructions giving us three proofs to theorem 1.

1 The First Proof

This proof is the simplest one we are going to see today. Let

$$S = \{(x_1, \dots, x_n) \in \{0, 1, 2\}^n : x_i = 1 \text{ for } m = \lfloor n/3 \rfloor \text{ values } i\} \subseteq \mathbb{Z}_4^n.$$

We claim that S has desired number of elements and in fact it does not even contain three collinear points. Indeed,

$$\begin{aligned} |S| &\sim 2^{2n/3}\binom{n}{n/3} \\ &\sim 2^{2n/3}\frac{\sqrt{2\pi n}n^n}{e^n}\frac{e^{n/3}}{\sqrt{2\pi n/3}(n/3)^{n/3}}\frac{e^{2n/3}}{\sqrt{2\pi 2n/3}(2n/3)^{2n/3}} \\ &= \Omega(n^{-1/2}3^n). \end{aligned}$$

Now, suppose to the contrary that S contains three points x, y, z forming a non-trivial arithmetic progression. Then,

$$x_i = y_i = z_i \quad \text{or} \quad (x_i, y_i, z_i) = (0, 1, 2) \text{ or } (2, 1, 0) \text{ or } (2, 0, 2) \text{ or } (0, 2, 0)$$

for each coordinate x_i, y_i, z_i of x, y, z. Since the number of 1s in each vector is constant, it follows that $(x_i, y_i, z_i) = (0, 1, 2)$ or $(2, 1, 0)$ is impossible. Therefore, we must have $x = z$.

2 Second Proof

This construction will make use of binary codes with certain minimum distances. For positive integers m and d with $m \geq d$, let $A(m,d)$ denote the largest possible size of a code in $\mathbb{F}_2^m$ with minimum hamming distance at least d. Note that

$$A(m,1) = 2^m \quad \text{and} \quad A(m,2) = 2^{m-1}.$$

The main observation is the following:

Theorem 2. For $n > 1$, we have $r_3(\mathbb{Z}_4^n) \geq \max_{0 \leq t \leq n} \sum_{i=t+1}^{n} \binom{n}{i} A(i, i-t)$.

Proof. For each $a \in \mathbb{Z}_4^n$, let $T(a) = \{i \in [n] : a_i \in \{0,2\}\}$ i.e. $T(a)$ records the positions of 0s and 1s. If $a, b, c \in \{0,1,2\}^n$ form an arithmetic progression, as we have seen in section 1, we must have

$$(a_i, b_i, c_i) \in \{(0,0,0), (1,1,1), (2,2,2), (0,1,2), (2,1,0), (2,0,2), (0,2,0)\}.$$

Therefore, a and c only differ at positions $i \in T(a) \setminus T(b)$ and $T(a) = T(c) \subseteq T(b)$.

Fix any t and $S \subseteq \{0,1,2\}^n$ be such that

- $|T(a)| \geq t$ for all $a \in S$, and
- for all T with $|T| \geq t$, the set $\{a \in S : T(a) = T\}$ has minimum hamming distance at least $|T| - t + 1$.

Then, if $a, b, c \in S$ were to form a proper arithmetic progression, then

$$d(a,c) \leq |T(a) \setminus T(b)| = |T(a)| - |T(b)| \leq |T(a)| - t$$

which implies that $a = c$.

We may construct an explicit example of the set S as follows. For every $T \subseteq [n]$ of size at least $i \geq t$, take a binary code in $\{0,2\}^T$ of size $A(i, i-t)$ of minimum distance $i-t$ and put 1s in other entries $[n] \setminus T$ to get a code A_T. Then, let $S = \sqcup_{|T| \geq t} A_T$ satisfies the desired properties and its size meets the stated lower bound. □

We can easily obtain a bound for $r_3(\mathbb{Z}_4^n)$ by substituting a value of t in theorem 2 so that $A(i, i-t)$ are easy for calculation. One may do this by setting $t = \lceil (2n-5)/3 \rceil$ and get

$$\sum_{i=t+1}^{n} \binom{n}{i} A(i, i-t) \geq \binom{n}{t+1} 2^{t+1} + \binom{n}{t+2} 2^{t+1} \sim \frac{3}{2} \cdot 2^{2n/3} \binom{n}{2n/3} \sim \frac{9}{4\sqrt{\pi}} \cdot \frac{3^n}{\sqrt{n}}.$$

3 The Third Proof

This construction mimics Behrend's construction of projecting a sphere into $\mathbb{Z}$. In fact, we have a stronger result.

Theorem 3. Let $m \geq 4$ be even. There exists some constant $C_m > 0$ such that

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+2}{2}\right)^n.$$

With $\sigma_m = \sqrt{\frac{m^4+8m^3+4m^2-48m}{2880}}$, one can choose $C_m = \frac{1}{3\sqrt{3}\sigma_m}$. For large m, one has that $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}m^2}$.

Proof. Define

$$S_R = \{(a_1, \dots, a_n) : a_i \in \{0, 1, \dots, m/2\}, \sum_{i=1}^n \left(a_i - \frac{m}{4}\right)^2 = R\}.$$

Then, each S_R does not contain a proper 3-term arithmetic progression. Suppose P_1, P_2, P_3 are points forming an arithmetic progression in S_R. For illustration purposes, suppose for now that the i-th coordinates of P_1, P_2, P_3 have the form $a_i - d_i, a_i, a_i + d_i$. Then, we have

$$\sum_{i=1}^n \left(\left(a_i + d_i - \frac{m-1}{4}\right)^2 + \left(a_i - d_i - \frac{m-1}{4}\right)^2 - 2\left(a_i - \frac{m-1}{4}\right)^2\right) = 0$$

and thus $\sum_{i=1}^n 2d_i^2 = 0$. So, the three points are identical. However, in $\mathbb{Z}_m^n$ for even m, the i-th coordinates may also have the form $0, m/2, 0$ or $m/2, 0, m/2$. The rest of the coordinates have the form $a_i - d_i, a_i, a_i + d_i$. Then, arguing as before, we can show that $d_i = 0$ for all i with coordinates not of the form $m/2, 0, m/2$ or $0, m/2, 0$. Hence, P_1 and P_3 are identical, contradiction.

We wish to find a S_R with many points. We may do so by first using Chebyshev's inequality to determine a range of radii in which majority of the points lie in, then use pigeonhole principle to pick one of these highly populated spheres. Consider $a_1, \dots, a_n$ to be independent random variables distributed uniformly over the set $\{0, 1, \dots, m/2\}$. Define the random variables

$$Y_i = a_i - \frac{m}{4}, \quad Z_i = Y_i^2, \quad Z = Z_1 + \cdots + Z_n$$

for $i \in \{1, \dots, n\}$. Then, calculations show that

$$\mathbb{E}(Z_i) = \frac{1}{48}m^2 + \frac{1}{12}m$$
$$\mathbb{E}(Z) = n\mathbb{E}(Z_i)$$
$$\sqrt{\text{Var}\,(Z_i)} = \sqrt{\frac{m^4 + 8m^3 + 4m^2 - 48m}{2880}}$$
$$\sqrt{\text{Var}\,(Z)} = \sqrt{n} \cdot \sqrt{\text{Var}\,(Z_i)}$$

Write $\mu = \mathbb{E}(Z)$ and $\sigma = \sqrt{\text{Var}\,(Z)}$. By Chebyshev's inequality, we can see that for at least two-thirds of all elements in $[0, m/2]^n$, sum of the digit squares-distances from the center $(m/4, \dots, m/4)$ is in the interval $[\mu n - \sqrt{3}\sigma, \mu n + \sqrt{3}\sigma]$. So, by pigeonhole principle, there exist a squared radius R such that

$$|S_R| \geq \frac{1}{\sqrt{3}\sigma}\left(\frac{m+2}{2}\right)^n = \frac{C_m}{\sqrt{n}}\left(\frac{m+2}{2}\right)^n$$

where $C_m = 1/(3\sqrt{3}\sigma_m)$ where $\sigma_m = \frac{m^4+8m^3+4m^2-48m}{2880}$. □

The same proof (in fact easier) can be done for odd $m \geq 5$.

Theorem 4. Let $m \geq 5$ be odd. There exists some $C_m > 0$ such that

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+1}{2} \right)^n .$$

Moreover, with $\sigma_m = \sqrt{\frac{m^4+4m^3-14m^2-36m+45}{2880}}$, we may take $C_m = \frac{1}{3\sqrt{3}\sigma_m}$. For increasing odd m, we asymptotically have $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}m^2}$.