Một bài toán cơ bản của tổ hợp cộng tính là đánh giá số phần tử của tập tổng $A+B$ theo số phần tử của A và B. Bài toán ngược tương ứng là mô tả các tập hợp đạt cận dưới. Trong nhiều trường hợp, dấu bằng buộc các tập ban đầu phải là những cấp số cộng có cùng công sai.

Chuyên đề trình bày các cận dưới cơ bản cùng điều kiện dấu bằng trong $\mathbb{R}$, định lý Cauchy–Davenport và định lý Vosper trong $\mathbb{Z}/p\mathbb{Z}$, sau đó giới thiệu phương pháp đa thức để xử lý tổng của hai phần tử phân biệt. Các chứng minh chỉ sử dụng thứ tự trên $\mathbb{R}$, phép đếm tập hợp và những tính chất sơ cấp của đa thức. Hai tài liệu tổng quan là [1, 2].

1 Ký hiệu và các khái niệm cơ bản

Trong toàn bộ chuyên đề, các tập hợp được xét đều hữu hạn. Ký hiệu $|X|$ chỉ số phần tử của tập hợp X. Với $G=\mathbb{R}$ hoặc $G=\mathbb{Z}/p\mathbb{Z}$ và hai tập con $A,B\subseteq G$, đặt

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

Với $t\in G$, ta viết

$$A+t=\{a+t : a\in A\},\qquad -A=\{-a : a\in A\}.$$

Ký hiệu $2A$ được hiểu là $A+A$, không phải tập $\{2a : a\in A\}$. Tương tự, $A_1+\cdots+A_r$ là tập tất cả các tổng $a_1+\cdots+a_r$ với $a_i\in A_i$.

Định nghĩa 1 (Tập tổng hạn chế)**.** Với $A,B\subseteq G$, đặt

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

Đặc biệt, $A\hat{+}A$ là tập các tổng của hai phần tử phân biệt thuộc A. Tổng quát hơn, với $1\le k\le |A|$, đặt

$$k^{\wedge}A=\{a_1+\cdots+a_k : a_1,\dots,a_k\in A \text{ đôi một phân biệt}\}.$$

Như vậy, $2^{\wedge}A=A\hat{+}A$.

Định nghĩa 2 (Cấp số cộng)**.** Một tập $X\subseteq\mathbb{R}$ gồm $m\ge 1$ phần tử là một cấp số cộng công sai $d>0$ nếu

$$X=\{x_0+id : 0\le i\le m-1\}.$$

Với p nguyên tố, một tập $X\subseteq\mathbb{Z}/p\mathbb{Z}$ gồm m phần tử, $1\le m\le p$, là một cấp số cộng công sai $d\neq 0$ nếu cũng có biểu diễn trên, với các phép toán thực hiện theo modulo p.

Một tập gồm một phần tử là cấp số cộng với mọi công sai được phép. Trong $\mathbb{Z}/p\mathbb{Z}$, một cấp số cộng công sai d cũng có thể viết thành cấp số cộng công sai $-d$ bằng cách đảo thứ tự các phần tử.

2 Cỡ của tập tổng trong $\mathbb{R}$

2.1 Tập tổng thông thường

Định lý 1. Cho A,B là hai tập con hữu hạn, khác rỗng của $\mathbb{R}$. Khi đó

$$|A+B|\ge |A|+|B|-1.$$

Dấu bằng xảy ra khi và chỉ khi $\min(|A|,|B|)=1$, hoặc A,B đều có ít nhất hai phần tử và là các cấp số cộng có cùng công sai.

https://nttuan.org/
Nguyễn Trung Tuân, 0915011235
T's Lab

Chứng minh. Viết

$$A = \{a_1 < \cdots < a_m\}, \qquad B = \{b_1 < \cdots < b_n\}.$$

Chuỗi tăng chặt

$$a_1 + b_1 < \cdots < a_1 + b_n < a_2 + b_n < \cdots < a_m + b_n$$

gồm $m + n - 1$ phần tử của $A + B$, nên $|A + B| \geq m + n - 1$.

Giả sử dấu bằng xảy ra và $m, n \geq 2$. Xếp các phần tử của $A + B$ là $s_1 < \cdots < s_{m+n-1}$. Với mỗi cặp (i, j), xét một dãy các cặp chỉ số từ $(1, 1)$ đến (m, n) đi qua (i, j), trong đó mỗi lần tăng đúng một chỉ số thêm 1. Dãy này có $m + n - 1$ cặp; các tổng tương ứng tăng chặt, nên phải lần lượt bằng $s_1, \ldots, s_{m+n-1}$. Cặp (i, j) đứng ở vị trí $i + j - 1$, do đó

$$a_i + b_j = s_{i+j-1}.$$

Suy ra, với $1 \leq i < m$ và $1 \leq j < n$,

$$a_{i+1} + b_j = a_i + b_{j+1}, \qquad a_{i+1} - a_i = b_{j+1} - b_j.$$

Vậy mọi khoảng cách giữa hai phần tử liên tiếp của A và của B đều bằng một số $d > 0$.

Ngược lại, nếu một tập chỉ có một phần tử thì dấu bằng hiển nhiên đúng. Nếu A, B là các cấp số cộng cùng công sai $d > 0$, thì

$$A + B = \{a_1 + b_1 + td : 0 \leq t \leq m + n - 2\},$$

nên $|A + B| = m + n - 1$. □

Hệ quả 1. (a) Cho $r \geq 1$ và các tập con hữu hạn, khác rỗng $A_1, \ldots, A_r \subseteq \mathbb{R}$. Khi đó

$$|A_1 + \cdots + A_r| \geq \sum_{i=1}^{r} |A_i| - r + 1.$$

Dấu bằng xảy ra khi và chỉ khi có nhiều nhất một tập có ít nhất hai phần tử, hoặc tất cả các tập có ít nhất hai phần tử đều là cấp số cộng với cùng một công sai.

(b) Với mọi tập con hữu hạn, khác rỗng $A \subseteq \mathbb{R}$,

$$|A - A| \geq 2|A| - 1.$$

Dấu bằng xảy ra khi và chỉ khi A là một cấp số cộng.

Chứng minh. (a) Áp dụng liên tiếp Định lý 1 thu được bất đẳng thức. Các tập một phần tử chỉ tạo ra phép tịnh tiến, nên có thể bỏ qua khi xét dấu bằng.

Giả sử còn lại $q \geq 2$ tập $B_1, \ldots, B_q$, mỗi tập có ít nhất hai phần tử. Nếu dấu bằng xảy ra thì mọi bất đẳng thức trong quá trình cộng lần lượt các tập đều phải là đẳng thức. Định lý 1 trước hết cho B_1, B_2 là các cấp số cộng cùng công sai d; tổng của chúng cũng là cấp số cộng công sai d. Tiếp tục áp dụng định lý cho tổng này và B_3, rồi cho các tập còn lại, ta được tất cả B_i là cấp số cộng cùng công sai d. Ở đây công sai dương của một cấp số cộng có ít nhất hai phần tử được xác định bởi hai phần tử nhỏ nhất. Chiều ngược lại suy ra trực tiếp từ công thức cộng các cấp số cộng.

(b) Áp dụng Định lý 1 cho A và $-A$. Nếu A là cấp số cộng công sai $d > 0$, thì $-A$, khi viết theo thứ tự tăng dần, cũng là cấp số cộng công sai d. □

2.2 Tổng của hai phần tử phân biệt

https://nttuan.org/
T's Lab
Nguyễn Trung Tuân, 0915011235

Định lý 2. Cho $A = \{a_1 < \cdots < a_n\} \subseteq \mathbb{R}$, $n \geq 2$. Khi đó

$$|A \hat{+} A| \geq 2n - 3.$$

Dấu bằng xảy ra khi và chỉ khi thuộc một trong các trường hợp sau:

(1) $n = 2$ hoặc $n = 3$;

(2) $n = 4$ và $a_1 + a_4 = a_2 + a_3$;

(3) $n \geq 5$ và A là một cấp số cộng.

Chứng minh. Chuỗi tăng chặt

$$a_1 + a_2 < \cdots < a_1 + a_n < a_2 + a_n < \cdots < a_{n-1} + a_n$$

gồm $2n - 3$ phần tử của $A \hat{+} A$, nên cho cận dưới cần chứng minh.

Giả sử $|A \hat{+} A| = 2n - 3$, và viết các phần tử của tập này là $s_1 < \cdots < s_{2n-3}$. Với $1 \leq i < j \leq n$, ta đi từ cặp $(1, 2)$ đến (i, j) bằng cách tăng chỉ số thứ hai đến j, rồi tăng chỉ số thứ nhất đến i. Sau đó tăng chỉ số thứ hai đến n, rồi tăng chỉ số thứ nhất đến $n - 1$. Mỗi lần chỉ tăng một chỉ số thêm 1, và chỉ số thứ nhất luôn nhỏ hơn chỉ số thứ hai.

Dãy các tổng tương ứng tăng chặt, có đúng $2n - 3$ phần tử, trong đó $a_i + a_j$ đứng ở vị trí $i + j - 2$. Bởi vậy

$$a_i + a_j = s_{i+j-2} \qquad (1 \leq i < j \leq n). \tag{1}$$

Nếu $n = 4$, áp dụng cho $(i, j) = (1, 4)$ và $(2, 3)$ được $a_1 + a_4 = a_2 + a_3$.

Nếu $n \geq 5$, đặt $d_i = a_{i+1} - a_i$ với $1 \leq i \leq n - 1$. Với $1 \leq i < j \leq n - 1$ và $j - i \geq 2$, công thức (1) cho

$$a_i + a_{j+1} = a_{i+1} + a_j, \qquad d_i = d_j.$$

Lấy $i = 1$, ta có $d_1 = d_3 = \cdots = d_{n-1}$; lấy $(i, j) = (2, 4)$, ta có thêm $d_2 = d_4 = d_1$. Vậy A là cấp số cộng.

Ngược lại, với $n = 2, 3$, các tổng của hai phần tử phân biệt tạo ra đúng $2n - 3$ giá trị. Với $n = 4$ và $a_1 + a_4 = a_2 + a_3$, các giá trị là

$$a_1 + a_2 < a_1 + a_3 < a_1 + a_4 = a_2 + a_3 < a_2 + a_4 < a_3 + a_4.$$

Nếu A là cấp số cộng công sai $d > 0$, thì

$$A \hat{+} A = \{2a_1 + td : 1 \leq t \leq 2n - 3\},$$

nên dấu bằng cũng xảy ra. □

Nhận xét. Điều kiện $n \geq 5$ trong kết luận về cấp số cộng là cần thiết. Chẳng hạn, $A = \{0, 1, 10, 11\}$ không phải cấp số cộng nhưng

$$A \hat{+} A = \{1, 10, 11, 12, 21\},$$

vẫn có đúng $2|A| - 3$ phần tử. Với bốn phần tử, điều kiện dấu bằng chỉ yêu cầu tập A đối xứng qua điểm $(a_1 + a_4)/2$.

2.3 Tổng của k phần tử phân biệt

https://nttuan.org/
T's Lab
Nguyễn Trung Tuân, 0915011235

Định lý 3. Cho $A = \{a_1 < \cdots < a_n\} \subseteq \mathbb{R}$ và số nguyên $1 \le k \le n$. Khi đó

$$|k^\wedge A| \ge k(n-k)+1.$$

Dấu bằng xảy ra khi và chỉ khi thuộc một trong các trường hợp sau:

(1) $k \in \{1, n-1, n\}$;

(2) $n = 4$, $k = 2$ và $a_1 + a_4 = a_2 + a_3$;

(3) $n \ge 5$, $2 \le k \le n-2$ và A là một cấp số cộng.

Chứng minh. Với $I = (i_1, \ldots, i_k)$, $1 \le i_1 < \cdots < i_k \le n$, đặt

$$\Sigma(I) = \sum_{t=1}^{k} a_{i_t}, \qquad r(I) = 1 + \sum_{t=1}^{k} (i_t - t).$$

Xét một dãy các bộ chỉ số từ $(1, \ldots, k)$ đến $(n-k+1, \ldots, n)$, đi qua I, trong đó mỗi lần tăng đúng một tọa độ thêm 1 và các tọa độ luôn tăng chặt. Dãy như vậy tồn tại: trước hết tăng lần lượt các tọa độ từ phải sang trái đến các giá trị $i_k, \ldots, i_1$; sau đó cũng theo thứ tự ấy tăng chúng đến $n, n-1, \ldots, n-k+1$.

Tổng số lần tăng là

$$\sum_{t=1}^{k} (i_t - t) + \sum_{t=1}^{k} (n - k + t - i_t) = k(n-k).$$

Các giá trị Σ tăng chặt dọc theo dãy, cho $k(n-k)+1$ phần tử phân biệt thuộc $k^\wedge A$. Điều này chứng minh cận dưới.

Nếu dấu bằng xảy ra, viết các phần tử của $k^\wedge A$ là $s_1 < \cdots < s_{k(n-k)+1}$. Dãy vừa dựng phải liệt kê toàn bộ tập này, nên

$$\Sigma(I) = s_{r(I)}. \tag{2}$$

Vì vậy, hai bộ k chỉ số có cùng tổng chỉ số thì cho cùng tổng các phần tử tương ứng của A.

Các trường hợp $k \in \{1, n-1, n\}$ là hiển nhiên; trường hợp $(n,k) = (4,2)$ đã được xét trong Định lý 2. Giả sử $n \ge 5$ và $2 \le k \le n-2$. Với $1 \le i < j \le n-1$, $j - i \ge 2$, bốn chỉ số $i, i+1, j, j+1$ đôi một phân biệt. Do $k - 2 \le n - 4$, chọn được một tập T gồm $k-2$ chỉ số khác bốn chỉ số này. Hai tập chỉ số

$$T \cup \{i, j+1\}, \qquad T \cup \{i+1, j\}$$

có cùng tổng. Áp dụng (2) rồi khử các số hạng có chỉ số thuộc T, ta được

$$a_i + a_{j+1} = a_{i+1} + a_j.$$

Đặt $d_i = a_{i+1} - a_i$. Như trong chứng minh Định lý 2, các đẳng thức $d_i = d_j$ khi $j - i \ge 2$ kéo theo $d_1 = \cdots = d_{n-1}$. Vậy A là cấp số cộng.

Ngược lại, khi $k = 1$ hoặc $k = n$, đẳng thức là hiển nhiên. Khi $k = n-1$, đặt $\sigma = \sum_{a \in A} a$; khi đó $(n-1)^\wedge A = \sigma - A$, có đúng n phần tử. Trường hợp $(n,k) = (4,2)$ suy ra từ Định lý 2. Cuối cùng, nếu $a_i = a_1 + (i-1)d$, $d > 0$, thì

$$\Sigma(I) = k a_1 + d\left(\sum_{t=1}^{k} i_t - k\right).$$

Tổng các chỉ số nằm trong đoạn nguyên từ $k(k+1)/2$ đến $k(2n-k+1)/2$, gồm $k(n-k)+1$ giá trị. Mặt khác, dãy chỉ số đã dựng đi qua tất cả các giá trị nguyên trong đoạn này vì mỗi lần tổng chỉ số tăng đúng 1. Do đó $|k^\wedge A| = k(n-k)+1$. □

Nhận xét. Ý tưởng chung của ba định lý trên là dựng một chuỗi tăng chặt có độ dài bằng cận dưới cần chứng minh. Khi dấu bằng xảy ra, mọi chuỗi như vậy đều phải liệt kê toàn bộ tập tổng theo đúng thứ tự. Vị trí của một tổng trong chuỗi khi đó được xác định bởi các chỉ số, dẫn đến những đẳng thức giữa các khoảng cách liên tiếp.

https://nttuan.org/
T's Lab
Nguyễn Trung Tuân, 0915011235

3 Cỡ của tập tổng trong $\mathbb{Z}/p\mathbb{Z}$

Trong mục này, p luôn là số nguyên tố. Ta viết $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; mọi phép toán giữa các phần tử của $\mathbb{F}_p$ đều được hiểu trong trường này.

3.1 Định lý Cauchy–Davenport

Định lý 4 (Cauchy–Davenport)**.** Với hai tập con khác rỗng $A, B \subseteq \mathbb{F}_p$, ta có

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Định lý được trình bày trong các tài liệu [3, 1]. Chứng minh dưới đây sử dụng biến đổi e của Dyson.

Chứng minh. Ta quy nạp theo $|B|$. Nếu $|B| = 1$ hoặc $A = \mathbb{F}_p$, kết quả hiển nhiên. Xét $|B| \geq 2$ và $1 \leq |A| < p$.

Chọn $b_1 \neq b_2$ thuộc B, đặt $d = b_2 - b_1 \neq 0$. Tồn tại $a \in A$ sao cho $a + d \notin A$. Thật vậy, nếu không thì $A + d = A$; từ một phần tử $a_0 \in A$, ta suy ra $a_0, a_0 + d, \ldots, a_0 + (p-1)d \in A$. Các phần tử này quét hết $\mathbb{F}_p$, trái với $|A| < p$.

Đặt $t = a - b_1$ và

$$A' = A \cup (B + t), \qquad B' = B \cap (A - t).$$

Vì $b_1 + t = a \in A$ còn $b_2 + t = a + d \notin A$, nên $1 \leq |B'| < |B|$. Công thức cộng lực lượng của hợp và giao cho

$$|A'| + |B'| = |A| + |B|.$$

Hơn nữa, $A' + B' \subseteq A + B$. Quả vậy, nếu $x \in A$, $y \in B'$ thì $x + y \in A + B$. Nếu $x \in B + t$, $y \in B'$, thì $x - t \in B$, $y + t \in A$ và

$$x + y = (y + t) + (x - t) \in A + B.$$

Áp dụng giả thiết quy nạp cho (A', B'), ta được

$$|A+B| \geq |A'+B'| \geq \min\{p, |A'|+|B'|-1\} = \min\{p, |A|+|B|-1\}. \qquad \square$$

Hệ quả 2. (a) Với $r \geq 1$ và các tập con khác rỗng $A_1, \ldots, A_r \subseteq \mathbb{F}_p$,

$$|A_1 + \cdots + A_r| \geq \min\left\{p, \sum_{i=1}^{r} |A_i| - r + 1\right\}.$$

(b) Cho $p-1$ số nguyên $x_1, \ldots, x_{p-1}$, không số nào chia hết cho p. Mỗi lớp thặng dư modulo p đều là tổng của một số các số đã cho, trong đó mỗi chỉ số được dùng nhiều nhất một lần và cho phép tổng rỗng.

Chứng minh. (a) Trường hợp $r = 1$ là hiển nhiên. Với $r \geq 2$, áp dụng liên tiếp Định lý 4, dùng đẳng thức

$$\min\{p, \min\{p, u\} + v\} = \min\{p, u + v\} \qquad (v \geq 0).$$

(b) Áp dụng (a) cho $A_i = \{0, \overline{x_i}\} \subseteq \mathbb{F}_p$, $1 \leq i \leq p-1$. Mỗi tập có hai phần tử, nên

$$|A_1 + \cdots + A_{p-1}| \geq \min\{p, 2(p-1) - (p-1) + 1\} = p.$$

Kết luận đúng cả khi $p = 2$, vì (a) cho phép $r = 1$. $\square$

Nhận xét. Trong chứng minh bằng biến đổi Dyson, tính nguyên tố của p bảo đảm rằng mỗi $d \neq 0$ sinh ra toàn bộ nhóm cộng $\mathbb{F}_p$. Không thể thay p bằng một hợp số tùy ý: trong $\mathbb{Z}/6\mathbb{Z}$, với $A = B = \{0, 2, 4\}$ ta có

$$|A + B| = 3 < \min\{6, 3 + 3 - 1\} = 5.$$

https://nttuan.org/
rTsLab
Nguyễn Trung Tuân, 0915011235

3.2 Định lý Vosper và các trường hợp dấu bằng

Bổ đề 1. Cho $\varnothing \neq X \subsetneq \mathbb{F}_p$ và $d \in \mathbb{F}_p \setminus \{0\}$. Khi đó

$$|X \cup (X+d)| = |X| + 1$$

khi và chỉ khi X là một cấp số cộng công sai d.

Chứng minh. Xếp các phần tử của $\mathbb{F}_p$ theo thứ tự vòng tròn

$$0, d, 2d, \ldots, (p-1)d.$$

Vì X khác rỗng và khác $\mathbb{F}_p$, các phần tử của X tạo thành một số đoạn liên tiếp cực đại trên vòng tròn này. Mỗi đoạn đóng góp đúng một phần tử cho $(X+d) \setminus X$, là phần tử đứng ngay sau đầu cuối của đoạn; các đoạn khác nhau cho các phần tử khác nhau. Do đó

$$|X \cup (X+d)| - |X| = \text{số đoạn liên tiếp cực đại của } X.$$

Hiệu này bằng 1 khi và chỉ khi X gồm đúng một đoạn, tức là một cấp số cộng công sai d. □

Định lý 5 (Vosper)**.** Cho $A, B \subseteq \mathbb{F}_p$ thỏa mãn $|A|, |B| \geq 2$ và $|A+B| \leq p-2$. Khi đó

$$|A+B| = |A| + |B| - 1$$

khi và chỉ khi A, B là hai cấp số cộng có cùng công sai khác 0.

Đây là trường hợp cấu trúc của dấu bằng trong định lý Cauchy–Davenport; xem [4, 1].

Chứng minh. Giả sử A, B là các cấp số cộng cùng công sai $d \neq 0$, với $|A| = m$, $|B| = n$. Khi đó

$$A + B = \{a_0 + b_0 + td : 0 \leq t \leq m+n-2\},$$

nên $|A+B| = \min\{p, m+n-1\}$. Do $|A+B| \leq p-2$, suy ra $|A+B| = m+n-1$.

Chiều còn lại, giả sử

$$|A+B| = |A| + |B| - 1 \leq p-2. \tag{3}$$

Trước hết, ta chứng minh A là một cấp số cộng bằng quy nạp theo $|B| \geq 2$. Nếu $B = \{b_1, b_2\}$, đặt $d = b_2 - b_1 \neq 0$. Khi đó

$$|A \cup (A+d)| = |A+B| = |A| + 1,$$

nên kết luận suy ra từ Bổ đề 1.

Giả sử $|B| \geq 3$ và kết luận đã đúng khi tập thứ hai có từ 2 đến $|B|-1$ phần tử. Tịnh tiến B để có $0 \in B$, rồi đặt

$$B^* = B \setminus \{0\}, \qquad E = (A+2B) \setminus (A+B).$$

Vì $0 \in B$, ta có $A + B \subseteq A + 2B$. Định lý 4 cho

$$|A+2B| \geq \min\{p, |A+B| + |B| - 1\} \geq |A+B| + 2,$$

trong đó bất đẳng thức cuối dùng $|A+B| \leq p-2$ và $|B| \geq 3$. Vậy $|E| \geq 2$.

Với mỗi $e \in E$, xét biến đổi Davenport

$$B_e = \{b \in B : e - b \notin A+B\}, \qquad C_e = B \setminus B_e.$$

Do $e \notin A+B$ nên $0 \in B_e$. Do $e \in A+2B$, có ít nhất một $b \in B$ sao cho $e - b \in A+B$. Bởi vậy

$$1 \leq |B_e| \leq |B| - 1.$$

https://nttuan.org/
T's Lab
Nguyễn Trung Tuân, 0915011235

Hai tập $A + B_e$ và $e - C_e$ đều nằm trong $A + B$ và rời nhau. Thật vậy, nếu $a + b = e - c$ với $a \in A$, $b \in B_e$, $c \in C_e$, thì $e - b = a + c \in A + B$, trái với định nghĩa B_e. Do đó

$$|A + B_e| + |C_e| \le |A + B| = |A| + |B| - 1,$$

tức $|A + B_e| \le |A| + |B_e| - 1$. Áp dụng Định lý 4 theo chiều ngược lại, chú ý $|A| + |B_e| - 1 < p$, ta được

$$|A + B_e| = |A| + |B_e| - 1. \tag{4}$$

Ta chứng minh có $e \in E$ sao cho $|B_e| \ge 2$. Nếu không thì $B_e = \{0\}$ và $C_e = B^*$ với mọi $e \in E$. Tính rời nhau ở trên khi đó cho $e - B^* \subseteq (A + B) \setminus A$. Lấy hợp theo e,

$$E - B^* \subseteq (A + B) \setminus A, \qquad |E - B^*| \le |B| - 1.$$

Nhưng Định lý 4 và $|E| \ge 2$ lại cho

$$|E - B^*| \ge \min\{p, |E| + |B^*| - 1\} \ge |B^*| + 1 = |B|,$$

mâu thuẫn. Vậy chọn được e với $2 \le |B_e| < |B|$. Từ (4) và giả thiết quy nạp áp dụng cho (A, B_e), suy ra A là một cấp số cộng.

Bây giờ viết $A = \{a_0, a_0 + d, \dots, a_0 + (m-1)d\}$, $d \ne 0$, và đặt

$$S_i = B + \{0, d, \dots, id\} \qquad (0 \le i \le m - 1).$$

Ta có $|S_0| = |B|$, $|S_{m-1}| = m + |B| - 1$, và $S_i = S_{i-1} \cup (S_{i-1} + d)$. Mỗi S_{i-1} là tập con khác rỗng, khác $\mathbb{F}_p$, nên $|S_i| \ge |S_{i-1}| + 1$. Tổng mức tăng qua $m - 1$ lần đúng bằng $m - 1$, do đó mỗi lần tăng đúng 1. Đặc biệt,

$$|B \cup (B + d)| = |B| + 1.$$

Bổ đề 1 cho B là cấp số cộng công sai d, hoàn tất chứng minh. □

Hệ quả 3. Cho $A, B \subseteq \mathbb{F}_p$ khác rỗng và $|A + B| < p$. Đẳng thức

$$|A + B| = |A| + |B| - 1$$

xảy ra khi và chỉ khi ít nhất một trong các điều kiện sau đúng:

(1) $\min(|A|, |B|) = 1$;

(2) tồn tại $c \in \mathbb{F}_p$ sao cho $B = \mathbb{F}_p \setminus (c - A)$;

(3) $|A|, |B| \ge 2$, $|A + B| \le p - 2$ và A, B là các cấp số cộng có cùng công sai khác 0.

Trong trường hợp (2), $A + B = \mathbb{F}_p \setminus \{c\}$.

Chứng minh. Trường hợp một tập có một phần tử là hiển nhiên. Khi $|A|, |B| \ge 2$ và $|A + B| \le p - 2$, áp dụng Định lý 5.

Nếu $|A+B| = p-1$ và dấu bằng xảy ra thì $|A|+|B| = p$. Gọi c là phần tử duy nhất không thuộc $A+B$. Khi đó $B \cap (c - A) = \varnothing$, nên $B \subseteq \mathbb{F}_p \setminus (c - A)$. Hai tập có cùng số phần tử, suy ra $B = \mathbb{F}_p \setminus (c - A)$.

Ngược lại, nếu $B = \mathbb{F}_p \setminus (c - A)$ thì $|A| + |B| = p$ và $c \notin A + B$. Định lý 4 cho $|A + B| \ge p - 1$, nên $A + B = \mathbb{F}_p \setminus \{c\}$ và dấu bằng xảy ra. □

Nhận xét. Không thể bỏ điều kiện $|A + B| \le p - 2$ trong Định lý 5. Chẳng hạn, trong $\mathbb{F}_7$, lấy

$$A = \{0, 1, 3\}, \qquad B = \{1, 2, 3, 5\} = \mathbb{F}_7 \setminus (-A).$$

Khi đó $A + B = \mathbb{F}_7 \setminus \{0\}$ và $|A + B| = 6 = |A| + |B| - 1$, nhưng A không phải cấp số cộng modulo 7. Nếu $|A + B| = p$, dấu bằng trong cận Cauchy–Davenport chỉ còn có nghĩa là $|A| + |B| \ge p + 1$; khi ấy không có kết luận cấp số cộng tương tự như trên.

https://nttuan.org/
T's Lab
Nguyễn Trung Tuân, 0915011235

3.3 Phương pháp đa thức và tổng hạn chế

Ràng buộc $a \neq b$ có thể được đưa vào đa thức bằng nhân tử $x - y$. Công cụ cần dùng là dạng hai biến của định lý sau của Alon [5].

Bổ đề 2 (Combinatorial Nullstellensatz, dạng hai biến)**.** Cho F là một trường, r, s là các số nguyên không âm và $P \in F[x, y]$ có tổng bậc không quá $r + s$. Giả sử hệ số của $x^r y^s$ trong P khác 0. Nếu $U, V \subseteq F$ thỏa mãn $|U| \geq r + 1$, $|V| \geq s + 1$, thì tồn tại $(u, v) \in U \times V$ sao cho $P(u, v) \neq 0$.

Chứng minh. Bỏ bớt phần tử nếu cần để $|U| = r + 1$, $|V| = s + 1$. Đặt

$$g(x) = \prod_{u \in U} (x - u), \qquad h(y) = \prod_{v \in V} (y - v).$$

Chia P cho g theo biến x, rồi chia phần dư cho h theo biến y, thu được đa thức R thỏa mãn

$$\deg_x R \leq r, \qquad \deg_y R \leq s, \qquad R(u, v) = P(u, v) \quad \text{trên } U \times V.$$

Trong mỗi phép chia, một đơn thức có số mũ quá lớn được thay bằng các đơn thức có tổng bậc nhỏ hơn. Vì tổng bậc ban đầu không vượt quá $r + s$, các phép thay này không làm thay đổi hệ số của $x^r y^s$. Do đó hệ số ấy trong R vẫn khác 0.

Nếu P triệt tiêu trên $U \times V$ thì R cũng vậy. Viết $R(x, y) = \sum_{j=0}^{s} r_j(x) y^j$, với $\deg r_j \leq r$. Với mỗi $u \in U$, đa thức $R(u, y)$ có bậc không quá s và có $s + 1$ nghiệm thuộc V, nên là đa thức không. Suy ra $r_j(u) = 0$ với mọi j và mọi $u \in U$. Mỗi r_j có bậc không quá r và có $r + 1$ nghiệm, nên cũng là đa thức không. Vậy $R = 0$, trái với hệ số khác 0 nói trên. □

Nhận xét (Một chứng minh khác của Cauchy–Davenport)**.** Đặt $m = |A|$, $n = |B|$. Nếu $m + n \geq p + 1$, thì với mỗi $c \in \mathbb{F}_p$, hai tập A và $c - B$ có giao khác rỗng, suy ra $c \in A + B$.

Xét $m + n \leq p$. Nếu $|A + B| \leq m + n - 2$, chọn $S \supseteq A + B$ với $|S| = m + n - 2$ và đặt

$$P(x, y) = \prod_{c \in S} (x + y - c).$$

Đa thức này triệt tiêu trên $A \times B$, nhưng hệ số của $x^{m-1} y^{n-1}$ bằng

$$\binom{m + n - 2}{m - 1} \neq 0 \quad \text{trong } \mathbb{F}_p,$$

vì $m + n - 2 < p$. Điều này mâu thuẫn với Bổ đề 2.

Định lý 6 (Alon–Nathanson–Ruzsa)**.** Cho $A, B \subseteq \mathbb{F}_p$ khác rỗng. Nếu $|A| \neq |B|$, thì

$$|A \hat{+} B| \geq \min\{p, |A| + |B| - 2\}.$$

Kết quả và phương pháp chứng minh dưới đây xuất phát từ [6].

Chứng minh. Do tính đối xứng, đặt $m = |A| > |B| = n$. Nếu $n = 1$, chỉ có thể phải loại đi một tổng trong $A + B$, nên $|A \hat{+} B| \geq m - 1 = m + n - 2$.

Giả sử $m > n \geq 2$; khi đó $p \geq 3$. Nếu $m + n \geq p + 2$, với mỗi $c \in \mathbb{F}_p$ ta có

$$|A \cap (c - B)| \geq m + n - p \geq 2.$$

Trong các phần tử a thuộc giao này, có nhiều nhất một phần tử thỏa $a = c - a$, vì p lẻ. Do đó tồn tại $a \in A$, $b = c - a \in B$ với $a \neq b$. Suy ra $A \hat{+} B = \mathbb{F}_p$.

https://nttuan.org/
T's Lab
Nguyễn Trung Tuân, 0915011235

Còn lại $m+n \le p+1$. Giả sử phản chứng $|A \hat{+} B| \le m+n-3$. Chọn $S \subseteq \mathbb{F}_p$ chứa $A \hat{+} B$ và có $|S| = m+n-3$. Xét

$$P(x,y) = (x-y)\prod_{c\in S}(x+y-c).$$

Nếu $a = b$ thì nhân tử $x-y$ triệt tiêu; nếu $a \neq b$ thì $a+b \in S$. Vì vậy P triệt tiêu trên $A \times B$.

Tổng bậc của P là $(m-1)+(n-1)$. Phần thuần nhất bậc cao nhất là $(x-y)(x+y)^{m+n-3}$, nên hệ số của $x^{m-1}y^{n-1}$ bằng

$$\binom{m+n-3}{m-2} - \binom{m+n-3}{m-1} = \frac{(m+n-3)!\,(m-n)}{(m-1)!\,(n-1)!}.$$

Hệ số này khác 0 trong $\mathbb{F}_p$: các giai thừa đều có chỉ số nhỏ hơn p, và $1 \le m-n < p$. Áp dụng Bổ đề 2 với $r = m-1$, $s = n-1$ thu được mâu thuẫn. □

Hệ quả 4 (Erdős–Heilbronn)**.** Cho $A \subseteq \mathbb{F}_p$ với $|A| \ge 2$. Khi đó

$$|A \hat{+} A| \ge \min\{p, 2|A|-3\}.$$

Chứng minh. Chọn $B \subset A$ với $|B| = |A|-1$. Vì $A \hat{+} B \subseteq A \hat{+} A$, Định lý 6 cho

$$|A \hat{+} A| \ge |A \hat{+} B| \ge \min\{p, |A|+|B|-2\} = \min\{p, 2|A|-3\}.$$ □

Nhận xét. Bất đẳng thức Erdős–Heilbronn được Dias da Silva và Hamidoune chứng minh trong [7]; Alon, Nathanson và Ruzsa đưa ra chứng minh bằng đa thức trong [6]. Cận dưới là tốt nhất: với $A = \{0,1,\dots,n-1\} \subseteq \mathbb{F}_p$, $2 \le n \le p$, ta có

$$A \hat{+} A = \{\overline{1}, \overline{2}, \dots, \overline{2n-3}\},$$

nên $|A \hat{+} A| = \min\{p, 2n-3\}$.

4 Đối chiếu các kết quả

Trong bảng sau, $m = |A|$, $n = |B|$ đối với $A+B$ và $A \hat{+} B$; riêng các dòng chỉ có tập A, ký hiệu $n = |A|$.

Không gian	Tập tổng	Cận dưới	Giả thiết và tham chiếu
$\mathbb{R}$	$A+B$	$m+n-1$	$m,n \ge 1$; Định lý 1.
$\mathbb{R}$	$A \hat{+} A$	$2n-3$	$n \ge 2$; Định lý 2.
$\mathbb{R}$	$k\hat{}A$	$k(n-k)+1$	$1 \le k \le n$; Định lý 3.
$\mathbb{F}_p$	$A+B$	$\min\{p, m+n-1\}$	$m,n \ge 1$; Định lý 4.
$\mathbb{F}_p$	$A \hat{+} B$	$\min\{p, m+n-2\}$	$m,n \ge 1$, $m \neq n$; Định lý 6.
$\mathbb{F}_p$	$A \hat{+} A$	$\min\{p, 2n-3\}$	$n \ge 2$; Hệ quả 4.

Trong $\mathbb{R}$, các Định lý 1–3 phân loại đầy đủ các trường hợp dấu bằng. Trong $\mathbb{F}_p$, dấu bằng cho tập tổng thông thường được mô tả bởi Định lý 5 và Hệ quả 3. Đối với tập tổng hạn chế trong $\mathbb{F}_p$, chuyên đề chỉ chứng minh cận dưới; không suy ra một phân loại dấu bằng tương tự từ các lập luận đã trình bày.

https://nttuan.org/
T's Lab
Nguyễn Trung Tuân, 0915011235

Tài liệu tham khảo

[1] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics, vol. 165, Springer, New York, 1996. Trang nhà xuất bản.

[2] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006. doi:10.1017/CBO9780511755149.

[3] H. Davenport, *On the addition of residue classes*, Journal of the London Mathematical Society **s1-10** (1935), no. 1, 30–32. doi:10.1112/jlms/s1-10.37.30.

[4] A. G. Vosper, *The critical pairs of subsets of a group of prime order*, Journal of the London Mathematical Society **s1-31** (1956), no. 2, 200–205. doi:10.1112/jlms/s1-31.2.200.

[5] N. Alon, *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing **8** (1999), nos. 1–2, 7–29. doi:10.1017/S0963548398003411.

[6] N. Alon, M. B. Nathanson and I. Ruzsa, *Adding distinct congruence classes modulo a prime*, The American Mathematical Monthly **102** (1995), no. 3, 250–255. doi:10.1080/00029890.1995.11990565. Bản toàn văn do tác giả cung cấp.

[7] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bulletin of the London Mathematical Society **26** (1994), no. 2, 140–146. doi:10.1112/blms/26.2.140.

https://nttuan.org/

T's Lab

Nguyễn Trung Tuân, 0915011235