

Định lý Bruck – Ryser – Chowla về design đối xứng

Trương Phước Nhân, 07/02/2016

Định lý Bruck – Ryser – Chowla : Nếu tồn tại một (v, k, λ) - design và v lẻ thì phương trình

$$z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}} \lambda y^2 \text{ có một nghiệm nguyên không tầm thường } (x, y, z) \neq (0, 0, 0).$$

Chứng minh : Để chứng minh định lý trên ta sẽ chứng minh lại một kết quả kinh điển của lý thuyết số học cổ điển sau :

Định lý Lagrange: Mọi số nguyên dương đều có thể biểu diễn dưới dạng tổng của bốn số chính phương

$$\text{Dễ dàng nhận thấy rằng : } (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

trong đó

$$z_1 = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4,$$

$$z_2 = x_2 y_1 - x_1 y_2 + x_4 y_3 - x_3 y_4,$$

$$z_3 = x_3 y_1 - x_4 y_2 - x_1 y_3 + x_2 y_4,$$

$$z_4 = x_4 y_1 + x_3 y_2 - x_2 y_3 - x_1 y_4$$

Thật vậy, với các số phức a, b, c, d bất kì,

$$\begin{aligned} |\overline{ac} + \overline{bd}|^2 + |bc - ad|^2 &= (\overline{ac} + \overline{bd})(\overline{ac} + \overline{bd}) + (bc - ad)(\overline{bc} - \overline{ad}) \\ &= a\overline{a}c\overline{c} + b\overline{b}d\overline{d} + b\overline{b}c\overline{c} + a\overline{a}d\overline{d} \\ &= |a|^2 |c|^2 + |b|^2 |d|^2 + |b|^2 |c|^2 + |a|^2 |d|^2 \\ &= (|a|^2 + |b|^2)(|c|^2 + |d|^2) \end{aligned}$$

để thu được kết quả cần chứng minh ta đặt $a = x_1 + x_2 i$, $b = x_3 + x_4 i$, $c = y_1 + y_2 i$, $d = y_3 + y_4 i$, bởi vì

$$\overline{ac} + \overline{bd} = z_1 + z_2 i \text{ và } bc - ad = z_3 + z_4 i.$$

Nhận xét trên kéo theo rằng nếu m và n có thể biểu diễn thành tổng của bốn số chính phương thì mn cũng như vậy. Bởi vì $2 = 1^2 + 1^2 + 0^2 + 0^2$ nên ta chỉ cần chứng minh khẳng định của bổ đề cho trường hợp p là một số nguyên tố lẻ. Ta cần kết khẳng định quan trọng sau trong quá trình lập luận :

Khẳng định : Nếu p là một số nguyên tố lẻ thì ta luôn tìm được các số nguyên dương x, y và m sao cho $1 + x^2 + y^2 = mp$ và $0 < m < p$

Chứng minh khẳng định : Tất cả các phần tử của tập $A = \left\{ x^2 \mid 0 \leq x \leq \frac{p-1}{2} \right\}$ nằm trong các lớp thặng dư

khác nhau theo modulo p . Thật vậy, với hai phần tử phân biệt a^2 và b^2 thì hiệu $a^2 - b^2 = (a-b)(a+b)$ chia hết cho p khi và chỉ khi $a-b$ hoặc $a+b$ chia hết cho p , điều đó là không thể xảy ra được.

Lập luận tương tự, tất cả các phần tử của tập $B = \left\{ -1 - y^2 \mid 0 \leq y \leq \frac{p-1}{2} \right\}$ nằm trong các lớp thặng dư khác

nhau theo mod p . Nhận xét rằng cả hai tập này đều có $\frac{p+1}{2}$ phần tử, và do đó ta có thể tìm được $x^2 \in A$

và $-1 - y^2 \in B$ cùng nằm trong một lớp thặng dư. Nói cách khác ta tìm được một số nguyên m sao cho

$$1 + x^2 + y^2 = x^2 - (-1 - y^2) = mp \text{ và do } 0 < 1 + x^2 + y^2 < 1 + 2\left(\frac{p}{2}\right)^2 < p^2 \text{ nên } 0 < m < p.$$

Chứng minh bổ đề :

Giả sử p là một số nguyên tố lẻ. Áp dụng các khẳng định ta suy ra được sự tồn tại của các số nguyên x_1, x_2, x_3, x_4 và một số nguyên dương $m < p$ sao cho $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. (lưu ý rằng $1 = 1^2 + 0^2$)

Gọi m_0 là số nguyên nhỏ nhất trong các số nguyên m như vậy. Theo khẳng định ta suy ra $m_0 < p$. Ta sẽ chỉ ra rằng $m_0 = 1$, giả sử phản chứng $m_0 > 1$.

Nếu m_0 là số chẵn thì $x_1^2 + x_2^2 + x_3^2 + x_4^2$ là số chẵn và các số nguyên x_1, x_2, x_3, x_4 hoặc tất cả đều chẵn hoặc tất cả đều lẻ hoặc có chính xác hai số chẵn và hai số lẻ, ta tạm giả sử trong trường hợp này x_1, x_2 chẵn còn x_3, x_4 lẻ; trong bất kì trường hợp nào ta đều nhận thấy rằng các số $x_1 + x_2, x_1 - x_2, x_3 + x_4$ và $x_3 - x_4$ đều

là các số chẵn và $\frac{m_0}{2}p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$. Do đó $\frac{m_0}{2}p$ có thể được biểu diễn thành tổng của bốn số chính phương, mâu thuẫn với tính nhỏ nhất của m_0 .

Do đó m_0 là số lẻ và do vậy $m_0 \geq 3$.

Các số nguyên x_1, x_2, x_3, x_4 không thể cùng đồng thời chia hết cho m_0 ; nếu ngược lại m_0^2 sẽ là ước của $m_0p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ và do đó m_0 là ước của p , điều này không thể xảy ra được vì $1 < m_0 < p$. Ta chọn các số nguyên b_1, b_2, b_3, b_4 sao cho $y_i = x_i - b_i m_0$ và $|y_i| < \frac{m_0}{2}$ với $i = 1, 2, 3, 4$. Theo nhận định trên thì có ít

nhất một trong các số nguyên y_1, y_2, y_3, y_4 khác không, nên $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{m_0}{2}\right)^2 = m_0^2$

Bởi vì $x_1^2 + x_2^2 + x_3^2 + x_4^2$ và tất cả các hiệu $y_i^2 - x_i^2 = b_i^2 m_0^2 - 2x_i b_i m_0$ đều chia hết cho m_0 nên $y_1^2 + y_2^2 + y_3^2 + y_4^2$ cũng như vậy. Do đó ta có thể tìm được số nguyên m_1 sao cho

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1, \text{ trong đó } 0 < m_1 < m_0$$

Khi đó $m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2$, trong đó z_1, z_2, z_3, z_4 được xác định như ở phần đầu của phân tích.

Nhận xét: $z_1 = \sum_{i=1}^4 x_i y_i = \sum_{i=1}^4 x_i (x_i - b_i m_0) \equiv \sum_{i=1}^4 x_i^2 \equiv 0 \pmod{m_0}$, bằng phương pháp tương tự z_2, z_3, z_4 đều chia hết cho m_0 . Do đó ta có thể tìm được các số nguyên t_i sao cho $z_i = m_0 t_i$ ($i = 1, 2, 3, 4$), và ta suy ra

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2$$

Nhưng $0 < m_1 < m_0 < p$, mâu thuẫn với tính cực tiểu của m_0 . Điều này suy ra rằng $m_0 = 1$

Chứng minh định lý Bruck – Ryser – Chowla :

Sử dụng định lý Langrange ta sẽ tìm được các số nguyên a, b, c, d sao cho $n = k - \lambda = a^2 + b^2 + c^2 + d^2$.

Bằng cách đặt $H = \begin{pmatrix} -a & b & c & d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$, ta dễ dàng chứng minh được các hệ thức $HH^T = H^T H = nI_4$.

Giả sử A là ma trận liên thuộc của (v, k, λ) - design. Sử dụng hệ thức cơ bản của lý thuyết cấu hình, $A^T A = nI_v + \lambda J_v$. Do v lẻ nên ta cần xét hai trường hợp sau :

Trường hợp 1: $v \equiv 3 \pmod{4}$.

Đặt $B = \begin{pmatrix} & & 0 \\ & A & \dots \\ & & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$, $K = \begin{pmatrix} H & 0 & \dots & 0 \\ 0 & H & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & H \end{pmatrix}$ là các ma trận kích thước $(v+1) \times (v+1)$. Bằng các phép

tính toán trên các ma trận khối ta có các hệ thức sau : $B^T B = \begin{pmatrix} k & \lambda & \dots & \lambda & 0 \\ \lambda & k & \dots & \lambda & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \lambda & \lambda & \dots & k & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$, $K^T K = nI_{v+1}$.

Dễ dàng nhận thấy rằng B là một ma trận khả nghịch, bằng cách tính định thức hoặc biến đổi ma trận để tính hạng của $B^T B$. Đặt $P = B^{-1}K$, hiển nhiên tất cả các phần tử của ma trận P là các số hữu tỉ. Nếu

$x = (x_1, x_2, \dots, x_{v+1})^T \in \mathbb{Q}^{v+1}$ và $y = (y_1, y_2, \dots, y_{v+1})^T \in \mathbb{Q}^{v+1}$ thỏa mãn phương trình $x = Py$ thì $Bx = Ky$ và

$$y^T K^T Ky = x^T B^T Bx$$

$$\Rightarrow n(y_1^2 + y_2^2 + \dots + y_{v+1}^2) = k(x_1^2 + x_2^2 + \dots + x_v^2) + x_{v+1}^2 + \lambda \sum_{1 \leq i, j \leq v, i \neq j} x_i x_j$$

$$\Rightarrow n(y_1^2 + y_2^2 + \dots + y_{v+1}^2) = \lambda(x_1 + x_2 + \dots + x_v)^2 + x_{v+1}^2 + n(x_1^2 + x_2^2 + \dots + x_v^2) \quad (*)$$

Bây giờ ta sẽ chỉ ra rằng hệ phương trình $x = Py$ theo $2(v+1)$ ẩn x_i và y_i có một nghiệm trong $\mathbb{Q}$ sao cho $y_{v+1} = 1$ và $x_i^2 = y_i^2$ với $1 \leq i \leq v$. Bằng cách đặt $y_{v+1} = 1$, khi đó ta nhận thấy v phương trình đầu của hệ có dạng :

$$\begin{pmatrix} x_1 \\ \dots \\ x_v \end{pmatrix} = R \begin{pmatrix} y_1 \\ \dots \\ y_v \end{pmatrix} + \begin{pmatrix} p_{1,v+1} \\ \dots \\ p_{v,v+1} \end{pmatrix},$$

trong đó ma trận R là ma trận con được tạo thành từ r cột và r hàng đầu tiên của ma trận P . Không quá khó để ta có thể chứng minh được rằng : với mọi ma trận R cấp $v \times v$ trên $\mathbb{Q}$ thì ta luôn có thể tìm được ma trận $E = \text{diag}\{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_v\}$ để cho ma trận $R - E$ khả nghịch, trong đó $\varepsilon_i \in \{-1; 1\}$. Bằng cách đặt $x_i := \varepsilon_i y_i$, ta thu được một hệ phương trình tuyến tính theo các biến y_i với ma trận hệ số là $R - E$ khả nghịch, nên ta luôn tìm được các bộ x_i và y_i với $1 \leq i \leq v$. Thay các giá trị vừa tìm được vào phương trình cuối cùng ta tìm được giá trị x_{v+1} .

Thay nghiệm này vào (*) ta thu được hệ thức :

$$n = ny_{v+1}^2 = \lambda(x_1 + \dots + x_v)^2 + x_{v+1}^2, \text{ trong đó } x_1, x_2, \dots, x_{v+1} \in \mathbb{Q}.$$

Do đó, tồn tại các số nguyên $x \neq 0, y$ và z sao cho $n = \lambda\left(\frac{y}{x}\right)^2 + \left(\frac{z}{x}\right)^2$, và do đó phương trình

$z^2 = nx^2 - \lambda y^2$ có nghiệm không tầm thường.

Trường hợp 2: $v \equiv 1 \pmod{4}$

$$\text{Đặt } K = \begin{pmatrix} H & & & 0 \\ & H & & 0 \\ & & \dots & \dots \\ & & & H & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \text{ là ma trận cấp } v \times v, \text{ khi đó } K^T K = \begin{pmatrix} n & & & 0 \\ & n & & 0 \\ & & \dots & \dots \\ & & & n & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \text{ Bằng cách áp dụng}$$

lại lỗi lập luận đã sử dụng trong trường hợp 1), nếu $x = (x_1, x_2, \dots, x_v)^T$ và $y = (y_1, y_2, \dots, y_v)^T$ thỏa

$$x = A^{-1}Ky \text{ thì } n(y_1^2 + \dots + y_{v-1}^2) + y_v^2 = n(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2.$$

Như trong trường hợp $v \equiv 3 \pmod{4}$, ta có thể tìm được các số $x_1, \dots, x_v \in \mathbb{Q}$ sao cho

$$1 = nx_v^2 + \lambda(x_1 + \dots + x_v)^2. \text{ Do đó, tồn tại các số nguyên } x, y, z \text{ không đồng thời bằng không sao cho}$$

$$z^2 = nx^2 + \lambda y^2$$

Tài liệu tham khảo :

- [1]. Ian Anderson, Ashort Course in Combinatorial Designs, ??/??/2012
- [2]. Trương Phước Nhân, Lý thuyết cấu hình tổ hợp, 02/02/2018
- [3]. Trương Phước Nhân, Cấu hình đối xứng, 06/02/2018

