

Cấu hình tổ hợp

Trương Phước Nhân, 16/07/2018

1. Hình vuông Latin

1.1. Hình vuông Latin và các ánh xạ discordant

Hai ánh xạ $\varphi: X \rightarrow Y$ và $\psi: X \rightarrow Y$ được gọi là discordant trên tập $X_1 \subseteq X$ nếu $\varphi(x) \neq \psi(x)$ với mọi $x \in X_1$. Các ánh xạ φ và ψ được gọi là discordant nếu chúng là discordant trên tập X . Nếu φ và ψ là các hoán vị discordant thì φ^{-1} và ψ^{-1} cũng là các hoán vị discordant.

Sử dụng lối ký hiệu vừa trình bày ở trên ta tiến hành xây dựng cấu trúc metric ρ trên nhóm đối xứng S_n :

Với mọi $s, s' \in S_n$, ta đặt $\rho(s, s') = |X_1|$, trong đó X_1 là tập con lớn nhất của X sao cho hai hoán vị s, s' là discordant trên đó. Hàm ρ thỏa mãn tất cả các yêu cầu của một metric:

(1) $\rho(s, s') \geq 0$ với mọi $s, s' \in S_n$ và $\rho(s, s') = 0$ khi và chỉ khi $s = s'$.

(2) $\rho(s, s') = \rho(s', s)$ với mọi $s, s' \in S_n$.

(3) $\rho(s, s'') \leq \rho(s, s') + \rho(s', s'')$ với mọi $s, s', s'' \in S_n$.

Tính chất (1) và (2) là hiển nhiên nên ta sẽ chỉ chứng minh tính chất (3):

Từ định nghĩa của hàm ρ ta nhận ra rằng $\rho(s, s') = \rho(e, s^{-1}s')$, trong đó e là hoán vị đồng nhất. Với điều kiện như vậy ta thấy rằng $\rho(e, s) = n - \gamma$, trong đó γ là số các chu trình độ dài đơn vị của hoán vị s .

Đặt $\gamma_1, \gamma_2, \gamma_3$ lần lượt là số các chu trình độ dài đơn vị của các hoán vị $s^{-1}s'', s^{-1}s', (s')^{-1}s''$.

Nhận thấy rằng nếu $s^{-1}s''(x) \neq x$ với một $x \in X$ thì hoặc $s^{-1}s'(x) \neq x$ hoặc $(s')^{-1}s''(x) \neq x$.

Do đó, $n - \gamma_1 \leq (n - \gamma_2) + (n - \gamma_3)$, điều này tương đương với việc $\rho(e, s^{-1}s'') \leq \rho(e, s^{-1}s') + \rho(e, (s')^{-1}s'')$.

Từ định nghĩa của hàm của metric ρ ta nhận thấy rằng hai hoán vị $s, s' \in S_n$ là discordant nếu $\rho(s, s') = n$.

Cho $s_1, \dots, s_k$ là các hoán vị bậc n discordant từng đôi một trên tập $X = \{1, \dots, n\}$. Một họ các hoán vị như vậy giúp ta xây dựng nên một mô hình đơn giản về một hình chữ nhật Latin cấp $k \times n$.

Thật vậy, từ họ $s_1, \dots, s_k$ ta dựng nên một ma trận L_{kn} cấp $k \times n$ với $L_{kn} = (s_i(j))_{i=1, \dots, k; j=1, \dots, n}$, thông thường ta có thể ký hiệu gọn lại là $L_{kn} = [s_1, \dots, s_k]_n$. Nếu $k = n$ thì một hình chữ nhật Latin sẽ được gọi là hình vuông Latin và được ký hiệu là $L_n = [s_1, \dots, s_n]$. Một hình vuông Latin tương ứng với một ma trận vuông cấp n , $L_n = (s_i(j))_{i,j=1, \dots, n}$. Do các hoán vị $s_1, \dots, s_n$ là discordant từng đôi một nên tất cả các hàng và tất cả các cột của hình vuông Latin là phân biệt. Các hàng và các cột của một hình vuông Latin là các hoán vị của các số $1, \dots, n$.

Ký hiệu bộ ba (i, j, l) có nghĩa là số l nằm ở vị trí giao giữa hàng thứ i và cột thứ j của một hình vuông Latin. Để xác định một hình vuông Latin cần tương ứng n^2 bộ ba. Khẳng định này được suy ra từ sự kiện hai phần tử bất kỳ trong một bộ ba xác định duy nhất phần tử còn lại. Dễ dàng nhận thấy rằng phần tử l được xác định duy nhất bởi phần tử i và j . Giả sử rằng tồn tại hai phần tử j và j' phân biệt cùng tương ứng với phần tử i và l . Khi đó, $s_i(j) = s_i(j')$, $j \neq j'$, mâu thuẫn với giả thiết s_i là một hoán vị. Nếu tồn tại hai phần tử phân biệt i và i' cùng tương ứng với phần tử j và l , nên ta có $s_i(j) = s_{i'}(j)$, điều này mâu thuẫn với giả thiết các hoán vị s_i và $s_{i'}$ là discordant với $i \neq i'$. Luôn tồn tại các hình chữ nhật Latin và các hình vuông Latin với mọi n, k ($n \leq k$). Thật vậy, xét hoán vị $c = (1, 2, \dots, n)$ của các số $1, 2, \dots, n$. Khi đó, các hoán vị $c, c^2, \dots, c^k$ xác định một hình chữ nhật Latin cấp $k \times n$ còn các hoán vị $c, c^2, \dots, c^n$ xác định một hình vuông Latin cấp n .

Dễ dàng nhận thấy rằng sau khi hoán đổi vị trí các hàng và các cột của một hình chữ nhật hoặc hình vuông Latin thì ta vẫn thu được một hình chữ nhật hoặc một hình vuông Latin. Do đó bằng cách hoán đổi vị trí các hàng và các cột (nếu cần) từ một hình vuông Latin bất kỳ ta luôn đưa nó về dạng đặc biệt, dạng chuẩn, trong đó hàng đầu tiên và cột đầu tiên bằng với vector $(1, 2, \dots, n)$.

1.2. Các hình vuông Latin trực giao

Các hình vuông Latin $L_n = [s_1, \dots, s_n]$, $L'_n = [s'_1, \dots, s'_n]$ được gọi là trực giao nếu

$$(s_i(j), s'_i(j)) \neq (s_k(l), s'_k(l)) \text{ với mọi } (i, j) \neq (k, l).$$

Nếu các hình vuông Latin L_n và L'_n là trực giao thì ta ký hiệu $L_n \perp L'_n$.

Nếu $L_n = (s_i(j))_{i,j=1,\dots,n}$ và $L'_n = (s'_i(j))_{i,j=1,\dots,n}$ trực giao thì ma trận $((s_i(j), s'_i(j)))_{i,j=1,\dots,n}$ sẽ có tất cả các phần tử phân biệt với nhau.

Sau đây ta xem xét một số tính chất cơ bản của các cặp hình vuông Latin trực giao

Kết quả 1. Các hình vuông Latin $L_n = [s_1, \dots, s_n]$, $L'_n = [s'_1, \dots, s'_n]$ trực giao khi và chỉ khi các hoán vị $s_1^{-1}s'_1, \dots, s_n^{-1}s'_n$ lập thành một hình vuông Latin.

Chứng minh. Giả sử $L_n \perp L'_n$ nhưng các hoán vị $s_1^{-1}s'_1, \dots, s_n^{-1}s'_n$ không lập thành một hình vuông Latin, có nghĩa là tồn tại v sao cho $s_i^{-1}s'_i(v) = s_k^{-1}s'_k(v)$ với i, k ($i \neq k$) nào đó. Đặt $s_i^{-1}(v) = j$, $s_k^{-1}(v) = l$, khi đó ta thu được $s_i(j) = s_k(l)$ và $s'_i(j) = s'_k(l)$, điều này mâu thuẫn với giả thiết trực giao của L_n và L'_n .

Bây giờ ta giả sử các hoán vị $s_1^{-1}s'_1, \dots, s_n^{-1}s'_n$ lập thành một hình vuông Latin, tức là $s_i^{-1}s'_i(v) \neq s_k^{-1}s'_k(v)$ với mọi v, i, k ($i \neq k$). Giả sử thêm rằng L_n không trực giao với L'_n , tức là $(s_i(j), s'_i(j)) = (s_k(l), s'_k(l))$ với $(i, j) \neq (k, l)$ nào đó. Do đó $s_i(j) = s_k(l)$, $s'_i(j) = s'_k(l)$. Từ hệ thức thứ nhất ta suy ra rằng tồn tại một phần tử v sao cho $s_i^{-1}(v) = j$, $s_k^{-1}(v) = l$. Kết hợp với hệ thức thứ hai ta suy ra $s_i^{-1}s'_i(v) = s_k^{-1}s'_k(v)$, $i \neq k$, mâu thuẫn.

Ta tiến hành định nghĩa phép nhân giữa một hoán vị bậc n với một hình vuông Latin cấp n như sau:

Nếu $L_n = [s_1, \dots, s_n]$ là một ma trận Latin ta định nghĩa $\varphi L_n = [\varphi s_1, \dots, \varphi s_n]$ và $L_n \psi = [s_1 \psi, \dots, s_n \psi]$,

trong đó φ và ψ là các hoán vị nào đó.

Kết quả 2. Nếu $L_n \perp L'_n$ thì $L_n \varphi \perp L'_n \psi$ với mọi hoán vị φ và ψ thuộc S_n .

Chứng minh. Từ Kết quả 1, ta nhận ra rằng các hình vuông Latin $L_n \varphi$ và $L'_n \psi$ trực giao với nhau khi và chỉ khi các hoán vị $\varphi^{-1}s_1^{-1}s'_1\psi, \dots, \varphi^{-1}s_n^{-1}s'_n\psi$ lập thành một hình vuông Latin.

Giả sử tồn tại phần tử v sao cho $\varphi^{-1}s_i^{-1}s'_i\psi(v) = \varphi^{-1}s_k^{-1}s'_k\psi(v)$ với i, k ($i \neq k$) nào đó.

Do đó $s_i^{-1}s'_i(\mu) = s_k^{-1}s'_k(\mu)$, $i \neq k$, điều này mâu thuẫn với giả thiết về tính trực giao của L_n và L'_n , nên ta cũng suy ra điều phải chứng minh.

Một hình vuông Latin L_n được gọi là nửa chuẩn hóa nếu nó có dạng $L_n = [e, s_2, \dots, s_n]$, trong đó e là hoán vị đồng nhất. Kết quả 2 chỉ ra rằng luôn có thể chuyển một cặp hình vuông Latin trực giao bất kỳ về dạng nửa chuẩn hóa. Thật vậy, nếu $L_n = [s_1, \dots, s_n]$ và $L'_n = [s'_1, \dots, s'_n]$ là các hình vuông Latin trực giao với nhau thì các hình vuông Latin $L_n s_1^{-1}$ và $L'_n (s'_1)^{-1}$ cũng trực giao với nhau và đều có dạng nửa chuẩn hóa.

Tiếp theo ta sẽ định nghĩa tích của hai hình vuông Latin bậc n . Nếu $L_n = [s_1, \dots, s_n]$ và $L'_n = [s'_1, \dots, s'_n]$ là các hình vuông Latin thì ta định nghĩa tích L''_n của chúng bởi $L''_n = L_n \circ L'_n = [s_1 s'_1, \dots, s_n s'_n]$.

Kết quả 3. Các hình vuông Latin L_n và L'_n trực giao với nhau khi và chỉ khi tồn tại một hình vuông Latin L''_n sao cho $L'_n = L_n \circ L''_n$.

Chứng minh. Thật vậy, nếu $L_n \perp L'_n$ thì từ Kết quả 1 ta suy ra dãy các hoán vị $s_1^{-1}s'_1, \dots, s_n^{-1}s'_n$ lập thành một hình vuông Latin. Bằng cách đặt $L''_n = [s_1^{-1}s'_1, \dots, s_n^{-1}s'_n]$ ta nhận thấy rằng $L'_n = L_n \circ L''_n$. Ngược lại, nếu tồn tại một hình vuông Latin L''_n sao cho $L'_n = L_n \circ L''_n$ thì bằng cách đảo lại các lập luận vừa trình bày ta cũng nhận ra rằng $L_n \perp L'_n$.

Nhận xét: Bằng cùng một phương pháp lập luận như vừa được trình bày ở trên ta cũng thu được kết quả sau

Kết quả 4. Các hình vuông Latin $L_n^{(1)}, \dots, L_n^{(r)}$ trực giao nhau từng đôi một khi và chỉ khi tồn tại $\frac{r(r-1)}{2}$ hình vuông Latin $L_n^{(i,j)}$ sao cho $L_n^{(i)} = L_n^{(j)} \circ L_n^{(i,j)}$.

Bây giờ ta sẽ xét một lớp đặc biệt các hình vuông Latin.

Một hình vuông Latin $L_n = [s_1, \dots, s_n]$ gọi là được dựng trên nhóm các hoán vị G nếu $G = \{s_1, \dots, s_n\}$.

Kết quả 5. Nếu các hình vuông Latin L_n và L'_n được dựng trên nhóm G trực giao với nhau thì hình vuông Latin được xác định bởi điều kiện $L'_n = L_n \circ L''_n$ cũng được dựng trên nhóm G .

Chứng minh. Thật vậy, $L''_n = [s_1^{-1}s'_1, \dots, s_n^{-1}s'_n]$ và $G = \{s_1^{-1}s'_1, \dots, s_n^{-1}s'_n\}$, tính không bị lặp lại của các phần tử được suy ra từ việc L''_n là một hình vuông Latin.

Một tập cực đại các hình vuông Latin bậc n trực giao nhau từng đôi một được gọi là một tập đầy đủ.

Kết quả 6. Một tập đầy đủ các hình vuông Latin bậc n chứa không quá $n-1$ phần tử.

Chứng minh. Xét một tập đầy đủ gồm các hình vuông Latin bậc n là $L_n^{(1)}, \dots, L_n^{(r)}$. Không mất tính tổng quát ta có thể giả sử rằng tất cả các hình vuông Latin này đều có dạng nửa chuẩn hóa, bởi vì phép nửa chuẩn hóa một hình vuông Latin bảo toàn tính trực giao. Khi đó, phần tử ở vị trí $(2,1)$ của các hình vuông Latin này phải chứa các phần tử khác nhau, trong trường hợp ngược lại sẽ mâu thuẫn với tính trực giao của các hình vuông Latin. Đồng thời các phần tử ở vị trí $(2,1)$ không thể bị trùng với phần tử của vị trí $(1,1)$ nên số các phần tử như vậy không thể lớn hơn $n-1$. Do đó, $r \leq n-1$.

1.3. Phương pháp Bose – Stevens

Sau đây ta sẽ trình bày phương pháp Bose – Stevens để xây dựng một tập đầy đủ các hình vuông Latin bậc n trực giao nhau từng đôi một với số phần tử bằng $n-1$ mà cơ sở của nó chính là kết quả sau

Kết quả 7. Cho $n = p^\alpha$, trong đó p là một số nguyên tố và α là một số tự nhiên nào đó.

Khi đó, với mọi $n \geq 3$, luôn tồn tại một tập đầy đủ gồm $n-1$ hình vuông Latin bậc n trực giao nhau từng đôi một.

Chứng minh. Đặt $GF(p^\alpha) = \{a_0 = 0, a_1 = 1, a_2, \dots, a_n\}$.

Xét $n-1$ ma trận $L_n^{(l)} = (a_{ij}^{(l)})_{i,j=0,1,\dots,n-1}$, $l = 1, \dots, n-1$, trong đó $a_{ij}^{(l)} = a_i a_l + a_j$. Mỗi ma trận này xác định cho ta một hình vuông Latin. Thật vậy, hệ thức $a_{ij}^{(l)} = a_{ij'}^{(l)}$ với $j \neq j'$ kéo theo $a_j = a_{j'}$, mâu thuẫn. Tương tự, hệ thức $a_{ij}^{(l)} = a_{i'j}^{(l)}$ với $i \neq i'$ kéo theo $(a_i - a_{i'})a_l = 0$, do $a_l \neq 0$ nên ta thu được $a_i = a_{i'}$, mâu thuẫn.

Tiếp theo, ta sẽ chứng minh rằng hai hình vuông Latin $L_n^{(k)}$ và $L_n^{(l)}$ trực giao nhau với $k \neq l$.

Giả sử $(a_{ij}^{(k)}, a_{ij}^{(l)}) = (a_{i'j'}^{(k)}, a_{i'j'}^{(l)})$ với $(i, j) \neq (i', j')$.

Do đó, ta thu được hệ phương trình sau

$$a_i a_k + a_j = a_{i'} a_k + a_{j'},$$

$$a_i a_l + a_j = a_{i'} a_l + a_{j'}.$$

Trừ phương trình thứ nhất cho phương trình thứ hai ta nhận được $a_i(a_k - a_l) = a_{i'}(a_k - a_l)$, do $a_k - a_l \neq 0$ nên ta thu được $a_i = a_{i'}$, tức là $i = i'$. Từ phương trình thứ nhất ta suy ra $a_j = a_{j'}$, tức là $j = j'$, điều này mâu thuẫn với điều kiện $(i, j) \neq (i', j')$.

2. (v, b, k) -cấu hình

2.1. Định nghĩa và các tính chất cơ bản của (v, b, k) -cấu hình

Một họ các tập con $X_1, \dots, X_v$ của tập $X = \{x_1, \dots, x_n\}$ được gọi là một (v, b, k) -cấu hình nếu

$$0 < \lambda < k < v-1 \text{ và } |X_i \cap X_j| = \begin{cases} k, & i = j, \\ \lambda, & i \neq j. \end{cases}$$

Các tập con $X_1, \dots, X_v$ được gọi là các khối. Ma trận liên thuộc của một (v, b, k) -cấu hình là một $(0, 1)$ -ma

$$\text{trận } A = (a_{ij})_{i,j=1,\dots,v} \text{ trong đó } a_{ij} = \begin{cases} 1, & x_j \in X_i, \\ 0, & x_j \notin X_i. \end{cases}$$

Ký hiệu I là ma trận vuông đơn vị cấp v còn J là ma trận vuông với tất cả các phần tử đều bằng 1.

Sau đây ta sẽ trình bày một số tính chất của ma trận liên thuộc của một (v, b, k) -cấu hình:

$$(1) \quad AJ = kJ.$$

Tính chất này biểu diễn cho điều kiện $\sum_{j=1}^v a_{ij} = k, i=1, \dots, v$, điều này thì tương đương với

$$|X_i| = k, i=1, \dots, v.$$

$$(2) \quad AA^T = \lambda J + (k - \lambda)I.$$

Tính chất này biểu diễn cho điều kiện $\sum_{i=1}^v a_{il}a_{jl} = |X_i \cap X_j| = \begin{cases} k, & i = j, \\ \lambda, & i \neq j. \end{cases}$

$$(3) \quad \det(AA^T) = (\det A)^2 = (k + \lambda(v-1))(k - \lambda)^{v-1}.$$

Từ tính chất vừa trình bày ta suy ra $AA^T = \lambda J + (k - \lambda)I = \begin{pmatrix} k & \lambda & \dots & \lambda \\ \lambda & k & \dots & \lambda \\ \dots & \dots & \dots & \dots \\ \lambda & \lambda & \dots & k \end{pmatrix}$ và từ đây bằng một số phép

biến đổi định thức đơn giản ta suy ra khẳng định trên.

(4) Các tham số của một (v, b, k) -cấu hình liên hệ với nhau theo hệ thức $k(k-1) = \lambda(v-1)$.

Bằng cách nhân phải hai vế của (2) cho J , ta thu được $AA^T J = (k + \lambda(v-1))J$.

Do $\lambda < k$ nên từ hệ thức (3) ta suy ra ma trận A không suy biến nên từ (1) ta có $A^{-1}J = \frac{1}{k}J$.

Bây giờ từ hệ thức $AA^T J = (k + \lambda(v-1))J$ ta tính được $A^T J = \frac{1}{k}(k + \lambda(v-1))J$.

Chuyển vị hai vế của biểu thức vừa nhận được và thực hiện nhân phải hai vế cho J , ta được

$$JAJ = \frac{v}{k}(k + \lambda(v-1))J.$$

Mặt khác, từ (1) ta suy ra rằng $JAJ = kvJ$.

Kết hợp hai kết quả trên ta nhận được $\frac{v}{k}(k + \lambda(v-1)) = kv$, thực hiện các phép biến đổi đơn giản ta thu được $k(k-1) = \lambda(v-1)$.

$$(5) \quad JA = kJ.$$

Tính chất này nói lên rằng số các tập con của họ $X_1, \dots, X_v$ cùng chứa một phần tử x_j luôn bằng k , tức là

$$\sum_{i=1}^v a_{ij} = k, j=1, \dots, v.$$

Tính đúng đắn của (5) được suy ra từ việc $A^T J = \frac{1}{k}(k + \lambda(v-1))J$ và $\frac{v}{k}(k + \lambda(v-1)) = kv$.

$$(6) \quad AA^T = A^T A.$$

Một ma trận thỏa mãn tính chất này thường được gọi là một ma trận chuẩn.

Tính đúng đắn của (6) được suy ra như sau:

$$A^T A = A^{-1}AA^T A = A^{-1}(\lambda J + (k - \lambda)I)A = \frac{\lambda}{k}JAJ + (k - \lambda)I = \lambda J + (k - \lambda)I = AA^T.$$

Từ tính chất này ta suy ra $\sum_{i=1}^v a_{il}a_{ij} = \begin{cases} k, & i = j, \\ \lambda, & i \neq j, \end{cases}$ tức là một cặp phần tử phân biệt x_i và x_j cùng thuộc chính

xác λ khối của họ $X_1, \dots, X_v$.

Các tính chất vừa xét ở trên của một (v, b, k) -cấu hình cung cấp cho ta một cách định nghĩa một (v, b, k) -cấu hình theo hướng tổ hợp:

Một họ các tập con $X_1, \dots, X_v$ của một tập $X = \{1, \dots, v\}$ có dạng một (v, b, k) -cấu hình với $0 < \lambda < k < v-1$ nếu mỗi phần tử của tập X được chứa trong chính xác k tập con của họ này và mỗi cặp phần tử phân biệt của tập X cùng thuộc chính xác λ tập con của họ này.

Định nghĩa vừa trình bày thể hiện nhiều sự liên kết giữa (v, b, k) -cấu hình và cấu trúc (b, v, r, k, λ) -cấu hình sẽ được trình bày trong phần 4 của bài viết.

2.2. Định lý Bruck-Chowla-Ryser

Cho $A = (a_{ij})_{i,j=1,\dots,v}$ là ma trận liên thuộc của một (v, b, k) -cấu hình. Mỗi khối X_i được cho tương ứng với

một dạng tuyến tính $F_i = F_i(u_1, \dots, u_v) = \sum_{j=1}^v a_{ij} u_j, i = 1, \dots, v$.

$$\text{Đặt } Q_v = \sum_{i=1}^v F_i^2 = \sum_{j=1}^v u_j^2 \sum_{i=1}^v a_{ij} + \sum_{j \neq l} u_j u_l \sum_{i=1}^v a_{ij} a_{il}.$$

Từ hai hệ thức $\sum_{i=1}^v a_{ij} = k, j = 1, \dots, v$, và $\sum_{i=1}^v a_{ij} a_{il} = \begin{cases} k, & i = j, \\ \lambda, & i \neq j, \end{cases}$ ta thu được

$$Q_v = \sum_{i=1}^v F_i^2 = (k - \lambda) \sum_{j=1}^v u_j^2 + \lambda \left(\sum_{j=1}^v u_j \right)^2.$$

Sau đây ta sẽ trình bày định lý Bruck-Chowla-Ryser. Định lý này cung cấp một điều kiện cần để biết được khi nào thì tồn tại một (v, b, k) -cấu hình. Để phục vụ cho mục đích này ta cần đến hai kết quả phụ sau

Bổ đề 1. Cho c_1, c_2, c_3, c_4 là các số hữu tỷ sao cho $c_1^2 + c_2^2 + c_3^2 + c_4^2 \neq 0$ còn u_1, u_2, u_3, u_4 và w_1, w_2, w_3, w_4 là các biến số thỏa mãn điều kiện

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = \begin{pmatrix} c_1 & -c_2 & -c_3 & -c_4 \\ c_2 & c_1 & -c_4 & c_3 \\ c_3 & c_4 & c_1 & -c_2 \\ c_4 & -c_3 & c_2 & c_1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix}.$$

Khi đó, $w_1^2 + w_2^2 + w_3^2 + w_4^2 = (c_1^2 + c_2^2 + c_3^2 + c_4^2)(u_1^2 + u_2^2 + u_3^2 + u_4^2)$ và các biến u_1, u_2, u_3, u_4 được biểu diễn như các tổ hợp tuyến tính của các biến w_1, w_2, w_3, w_4 với các hệ số hữu tỷ.

Chứng minh. Điều kiện cho trong khẳng định có thể được viết lại dưới dạng vector như sau:

$$w = Cu,$$

trong đó w và u là các vector tương ứng với các biến w_1, w_2, w_3, w_4 và u_1, u_2, u_3, u_4 còn C là ma trận tương ứng trong điều kiện.

Do đó ta suy ra rằng $w^T w = u^T C^T C u$.

Dễ dàng kiểm tra được rằng $C^T C = \left(\sum_{i=1}^4 c_i^2 \right) I$, trong đó I là ma trận đơn vị cấp 4.

$$\text{Do đó, } \sum_{i=1}^4 w_i^2 = \sum_{i=1}^4 c_i^2 \sum_{i=1}^4 u_i^2.$$

Từ hệ thức $C^T C = \left(\sum_{i=1}^4 c_i^2 \right) I$ ta suy ra được rằng $\det C = (c_1^2 + c_2^2 + c_3^2 + c_4^2)^2$.

Điều này có nghĩa là các hệ số trong biểu diễn tuyến tính của các biến u_1, u_2, u_3, u_4 qua các biến w_1, w_2, w_3, w_4 là các số hữu tỷ.

Tiếp theo, ta nhắc lại một kết quả đã quá quen thuộc đến từ lý thuyết số của tác giả Lagrange.

Bổ đề 2. Mọi số tự nhiên n đều có thể được biểu diễn dưới dạng tổng bình phương của bốn số nguyên khác không, tức là $n = c_1^2 + c_2^2 + c_3^2 + c_4^2$.

Sau đây ta sẽ trình bày kết quả của Bruck-Chowla-Ryser

Kết quả 8. Điều kiện cần để tồn tại một (v, k, λ) - cấu hình là

a) $k - \lambda$ là bình phương của một số tự nhiên nếu v chẵn;

b) phương trình $z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}} \lambda y^2$ có một nghiệm nguyên không tầm thường, tức là $x^2 + y^2 + z^2 \neq 0$ nếu v lẻ.

Chứng minh. Từ các hệ thức $\det(AA^T) = (k + \lambda(v-1))(k - \lambda)^{v-1}$ và $k(k-1) = \lambda(v-1)$ ta suy ra được

$$(\det A)^2 = k^2 (k - \lambda)^{v-1}.$$

Do đó, ta suy ra $(k - \lambda)^{v-1}$ là bình phương của một số tự nhiên nào đó, nếu v chẵn thì $k - \lambda$ sẽ phải là bình phương của một số tự nhiên.

Tiếp theo ta khảo sát trường hợp khi v lẻ.

Đầu tiên ta giả sử rằng $v \equiv 1 \pmod{4}$. Thực hiện chia các biến $u_1, \dots, u_{v-1}$ thành các nhóm liên tiếp nhau sao cho mỗi nhóm gồm bốn phần tử và đưa vào các biến $w_1, \dots, w_{v-1}$ được xác định bởi các hệ thức

$$W_j = CU_j, j = 1, 5, 9, \dots, v-4,$$

$$\text{trong đó } W_j^T = (w_j, w_{j+1}, w_{j+2}, w_{j+3}) \text{ và } U_j^T = (u_j, u_{j+1}, u_{j+2}, u_{j+3}) \text{ còn } C = \begin{pmatrix} c_1 & -c_2 & -c_3 & -c_4 \\ c_2 & c_1 & -c_4 & c_3 \\ c_3 & c_4 & c_1 & -c_2 \\ c_4 & -c_3 & c_2 & c_1 \end{pmatrix} \text{ với}$$

c_1, c_2, c_3, c_4 được xác định từ hệ thức $k - \lambda = c_1^2 + c_2^2 + c_3^2 + c_4^2$.

Áp dụng Bổ đề 1 ta suy ra rằng $w_j^2 + w_{j+1}^2 + w_{j+2}^2 + w_{j+3}^2 = (k - \lambda)(u_j^2 + u_{j+1}^2 + u_{j+2}^2 + u_{j+3}^2)$, $j = 1, 5, \dots, v-4$, và các biến $u_j, u_{j+1}, u_{j+2}, u_{j+3}$ là các tổ hợp tuyến tính của $w_j, w_{j+1}, w_{j+2}, w_{j+3}$ với các hệ số hữu tỷ.

Đặt $w_v = u_v$ và $w = u_1 + \dots + u_v$, ta thu được $\sum_{i=1}^v F_i^2 = \sum_{j=1}^{v-1} w_j^2 + (k - \lambda)w_v^2 + \lambda w^2$.

Chú ý rằng do $u_1, \dots, u_v, w$ là các tổ hợp tuyến tính của $w_1, \dots, w_v$ với các hệ số hữu tỷ nên hệ thức vừa thu được là một đồng nhất thức theo các biến $w_1, \dots, w_v$.

Từ phân tích trên ta nhận thấy rằng $F_1 = d_{11}w_1 + \dots + d_{1v}w_v$, trong đó $d_{11}, \dots, d_{1v}$ là các số hữu tỷ.

Đặt $F_1 = -w_1$ nếu $d_{11} = 1$ và $F_1 = w_1$ nếu $d_{11} \neq 1$. Trong cả hai trường hợp ta nhận thấy rằng w_1 luôn là một tổ hợp tuyến tính của $w_2, \dots, w_v$ và $F_1^2 = w_1^2$.

Bây giờ từ hệ thức $\sum_{i=1}^v F_i^2 = \sum_{j=1}^{v-1} w_j^2 + (k - \lambda)w_v^2 + \lambda w^2$ ta thu được một đồng nhất thức mới theo các biến độc lập là $w_2, \dots, w_v$:

$$\sum_{i=2}^v F_i^2 = \sum_{j=2}^{v-1} w_j^2 + (k - \lambda)w_v^2 + \lambda w^2.$$

Bằng cách làm tương tự, tức là các phép đặt $F_2 = \pm w_2, \dots, F_{v-1} = \pm w_{v-1}$ ta thu được kết quả sau

$$F_v^2 = (k - \lambda)w_v^2 + \lambda w^2,$$

trong đó F_v và w đều tỉ lệ với w_v với các hệ số là các số hữu tỷ còn w_v là một biến độc lập.

Bằng cách chọn cho w_v một giá trị nguyên khác không và thực hiện quy đồng mẫu F_v và w ta sẽ tìm được các số nguyên x, y, z sao cho $z^2 = (k - \lambda)x^2 + \lambda y^2$ trong đó $x \neq 0$.

Kế tiếp ta xét trường hợp $v \equiv 3 \pmod{4}$.

Ta đưa vào biến mới là u_{v+1} và cộng hai vế của hệ thức $\sum_{i=1}^v F_i^2 = (k - \lambda) \sum_{j=1}^v u_j^2 + \lambda \left(\sum_{j=1}^v u_j \right)^2$ cho $(k - \lambda)u_{v+1}^2$

thu được hệ thức sau $\sum_{i=1}^v F_i^2 + (k - \lambda)u_{v+1}^2 = (k - \lambda) \sum_{j=1}^{v+1} u_j^2 + \lambda \left(\sum_{j=1}^{v+1} u_j \right)^2$.

Thực hiện chia các biến $u_1, \dots, u_{v+1}$ thành các nhóm liên tiếp nhau sao cho mỗi nhóm gồm bốn phần tử và áp dụng phép biến đổi tương tự như đã làm khi khảo sát trường hợp $v \equiv 1 \pmod{4}$, ta thu được một đồng nhất thức theo các biến $w_1, \dots, w_{v+1}$:

$$\sum_{i=1}^v F_i^2 + (k - \lambda) u_{v+1}^2 = \sum_{j=1}^{v+1} w_j^2 + \lambda w^2,$$

trong đó $w = u_1 + \dots + u_v$.

Bằng kỹ thuật tương tự như trong trường hợp $v \equiv 1 \pmod{4}$, ta thu được đồng nhất thức chỉ phụ thuộc vào một biến là w_{v+1} :

$$(k - \lambda) u_{v+1}^2 = w_{v+1}^2 + \lambda w^2,$$

trong đó u_{v+1} và w đều tỉ lệ với w_{v+1} với các hệ số hữu tỷ.

Bằng cách chọn cho w_{v+1} một giá trị nguyên khác không và thực hiện quy đồng mẫu u_{v+1} và w ta sẽ tìm được các số nguyên x, y, z sao cho $z^2 = (k - \lambda)x^2 - \lambda y^2$ trong đó $x \neq 0$.

Tiếp theo ta sẽ xét một số trường hợp riêng của (v, k, λ) - cấu hình.

2.3. Perfect difference set

Cho $D = \{d_1, \dots, d_k\}$ là một tập nhỏ nhất các thặng dư khác không theo modulo v thỏa mãn điều kiện với mọi $a \not\equiv 0 \pmod{v}$ có chính xác λ cặp $(d_i, d_j), i \neq j$, sao cho $d_i - d_j \equiv a \pmod{v}$, trong đó $0 < \lambda < k < v - 1$.

Một tập D thỏa mãn các tính chất vừa nêu được gọi là một perfect difference set.

Đặt $D_l = \{d_1 + l, \dots, d_k + l\}, l = 0, 1, \dots, v - 1$, trong đó phép cộng được thực hiện theo modulo v .

Ta sẽ chỉ ra rằng $D_0, D_1, \dots, D_{v-1}$ là một họ các tập con của $D = \{0, 1, \dots, v - 1\}$ có dạng một (v, k, λ) - cấu hình.

Để thực hiện điều vừa nói ở trên ta chỉ cần chỉ ra rằng $|D_i \cap D_j| = \begin{cases} k, & i = j, \\ \lambda, & i \neq j. \end{cases}$

Với $i \neq j$,

$$\begin{aligned} |D_i \cap D_j| &= |\{d_1 + i, \dots, d_k + i\} \cap \{d_1 + j, \dots, d_k + j\}| \\ &= |\{(d_s, d_l) \mid d_s + i \equiv d_l + j \pmod{v}\}| \\ &= |\{(d_s, d_l) \mid d_s - d_l \equiv a \pmod{v}, a = j - i\}| \\ &= \lambda. \end{aligned}$$

Điều ta vừa nói ở trên đã chứng tỏ $D_0, D_1, \dots, D_{v-1}$ là một (v, k, λ) - cấu hình nên các tham số của một perfect difference set liên hệ với nhau theo hệ thức $k(k - 1) = \lambda(v - 1)$.

Một ma trận $A = (a_{ij})_{i, j=1, \dots, n}$ được gọi là circulant nếu một hàng bất kỳ của nó có thể thu được từ hàng trước bằng cách hoán vị vòng quanh các phần tử trong hàng theo chiều từ trái sang phải, tức là $a_{i+1, j+1} = a_{ij}$ trong đó phép cộng được thực hiện theo modulo n . Không quá khó khăn để ta có thể nhận ra rằng ma trận liên thuộc của một (v, k, λ) - cấu hình tương ứng với một perfect difference set là một ma trận circulant.

2.4. Ma trận Hadamard và Cấu hình Hadamard

Một ma trận vuông H cấp n được gọi là ma trận Hadamard nếu tất cả các phần tử của nó nhận các giá trị 1 hoặc -1 và $HH^T = nI$, trong đó I là ma trận đơn vị.

Nếu ta ký hiệu $H_1, \dots, H_n$ là các vector hàng của ma trận H thì điều kiện trong định nghĩa nói lên rằng tích vô hướng của hai hàng bất kỳ bằng $(H_i, H_j) = \begin{cases} n, & i = j, \\ 0, & i \neq j, \end{cases}$ tức là các hàng của ma trận H trực giao với

nhau. Đồng thời từ điều kiện nêu trong định nghĩa ta cũng suy ra ma trận H không suy biến, bởi vì $\det(HH^T) = (\det H)^2 = n^2$.

Ma trận H là ma trận chuẩn; thật vậy, $H^T H = H^{-1} H H^T H = H^{-1} (nI) H = nI = H H^T$.

Từ một ma trận Hadamard bằng cách nhân một hàng hoặc một cột bất kỳ cho -1 thì ta cũng thu được một ma trận Hadamard mới; thật vậy, nếu $H = (h_{ij})_{i,j=1,\dots,n}$ thì từ điều kiện trong định nghĩa tương đương với

$$\sum_{l=1}^n h_{il} h_{jl} = \begin{cases} n, & i = j, \\ 0, & i \neq j, \end{cases} \text{ và hiển nhiên rằng các hệ thức này vẫn được bảo toàn khi ta thực hiện phép biến đổi.}$$

Do đó, từ một ma trận Hadamard cho trước ta luôn có thể chuẩn hóa nó sao cho hàng đầu tiên và cột đầu tiên có tất cả các phần tử đều bằng 1.

Kết quả 9. Một ma trận Hadamard bậc n chỉ có thể có nếu $n=1, 2$ hoặc $n \equiv 0 \pmod{4}$.

Chứng minh.

Với $n=1, 2$ các ma trận Hadamard lần lượt là (1) và $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, khẳng định là hiển nhiên.

Xét một ma trận Hadamard đã chuẩn hóa với $n \geq 3$. Khi đó các cột của ba hàng đầu tiên của ma trận này có thể có một trong các dạng sau:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}.$$

Giả sử số lượng của các loại cột vừa đề cập ở trên lần lượt bằng x, y, z, w . Do tổng số các cột là n và từ tính trực giao của các hàng, ta thu được hệ phương trình sau

$$\begin{aligned} x + y + z + w &= n, \\ x + y - z - w &= 0, \\ x - y + z - w &= 0, \\ x - y - z + w &= 0. \end{aligned}$$

Giải hệ phương trình trên ta thu được $x = y = z = w = \frac{n}{4}$.

Do đó, $n = 4\mu$, trong đó μ là một số tự nhiên nào đó.

Bây giờ ta sẽ tiến hành định nghĩa tích Kronecker của hai ma trận vuông. Nếu cho trước hai ma trận vuông $A = (a_{ij})_{i,j=1,\dots,n}$ và $B = (b_{ij})_{i,j=1,\dots,m}$ thì tích Kronecker $A \otimes B$ của ma trận A và B là một ma trận

vuông cấp mn xác định bởi công thức $A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \dots & \dots & \dots & \dots \\ a_{n1}B & a_{n2}B & \dots & a_{nn}B \end{pmatrix}.$

Nói cách khác, $C = A \otimes B = (c_{s_i s_j})_{i,j=1,\dots,mn}$, trong đó $c_{s_i s_j} = a_{i_1 j_1} b_{i_2 j_2}$, $s_i = (i_1, j_1)$, $s_j = (i_2, j_2)$ và $s_1, s_2, \dots, s_{mn}$ là các cặp (i, j) với $i=1, \dots, n$, $j=1, \dots, m$, được sắp xếp theo thứ tự:

$$((1,1), \dots, (1,m), (2,1), \dots, (2,m), \dots, (n,1), \dots, (n,m)).$$

Tích Kronecker của các ma trận thỏa mãn một số tính chất cơ bản sau:

(1) $(A \otimes B)^T = A^T \otimes B^T$.

(2) Nếu A và B là các ma trận cấp n còn C là một ma trận cấp m thì $(A+B) \otimes C = A \otimes C + B \otimes C$.

Các tính chất trên được suy ra trực tiếp từ định nghĩa của tích Kronecker.

(3) Nếu A và B là các ma trận vuông cấp n còn C và D là các ma trận vuông cấp m thì

$$(AB) \otimes (CD) = (A \otimes C)(B \otimes D).$$

Tính đúng đắn của tính chất này được suy ra từ hệ thức $\sum_{\mu} a_{i\mu} b_{\mu j_1} \sum_{\nu} c_{i_2 \nu} d_{\nu j_2} = \sum_{\mu, \nu} a_{i\mu} c_{i_2 \nu} b_{\mu j_1} d_{\nu j_2}.$

(4) Tích Kronecker của hai ma trận Hadamard cũng là một ma trận Hadamard.

Thật vậy, nếu H và H' lần lượt là các ma trận Hadamard bậc n và m thì

$$(H \otimes H')(H \otimes H')^T = (H \otimes H')(H^T \otimes H'^T) = HH^T \otimes H'H'^T = nI_n \otimes mI_m = mnI_{mn}.$$

Kết quả 10. Với mọi số nguyên dương α luôn tồn tại một ma trận Hadamard bậc $n = 2^\alpha$.

Chứng minh.

Với $n = 2$, $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ là một ma trận Hadamard.

Với $n = 4$, $H_4 = H_2 \otimes H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$ cũng là một ma trận Hadamard.

Với $n = 8$, $H_8 = H_2 \otimes H_2 \otimes H_2$ cũng là một ma trận Hadamard.

Bằng lập luận tương tự ta nhận ra rằng, trong trường hợp tổng quát, $H_{2^\alpha} = \underbrace{H_2 \otimes \dots \otimes H_2}_{\alpha \text{ nhân tử } H_2}$ là một ma trận

Hadamard.

Kết quả 11. Một ma trận Hadamard chuẩn bậc n với $n = 4\mu$ tương đương với một (v, b, k) -cấu hình với các tham số $v = 4\mu, k = 2\mu - 1, \lambda = \mu - 1$ tương ứng.

Chứng minh. Đầu tiên loại bỏ đi hàng đầu tiên và cột đầu tiên khỏi ma trận Hadamard chuẩn H và thay các số -1 bởi các số 0 . Khi đó ta thu được một $(0, 1)$ -ma trận A cấp $v \times v$ trong đó mỗi hàng chứa chính xác $2\mu - 1$ số 1 , bởi vì trong ma trận Hadamard H ban đầu thì mỗi hàng chứa chính xác 2μ số 1 . Hai hàng bất kỳ của ma trận A chứa chính xác $\mu - 1$ số 1 nằm trên cùng cột. Các tính chất này chỉ ra rằng A là ma trận liên thuộc của một (v, b, k) -cấu hình với $v = 4\mu, k = 2\mu - 1, \lambda = \mu - 1$.

Ngược lại, bắt đầu từ ma trận liên thuộc của một (v, b, k) -cấu hình với các tham số được xác định như trên và bằng cách đảo lại thứ tự các lập luận ta có thể xây dựng lại được một ma trận Hadamard chuẩn có bậc $n = 4\mu$.

Nhận xét: (v, b, k) -cấu hình tương ứng với ma trận Hadamard như trình bày ở trên được gọi là một cấu hình Hadamard.

2.5. Mặt phẳng xạ ảnh hữu hạn

2.5.1. Một số tính chất cơ bản của mặt phẳng xạ ảnh hữu hạn

Một mặt phẳng xạ ảnh hữu hạn bậc n là một (v, b, k) -cấu hình với $v = n^2 + n + 1, k = n + 1, \lambda = 1$.

Ngôn ngữ của hình học thường được sử dụng trong việc mô tả các mặt phẳng xạ ảnh hữu hạn. Các phần tử của tập X được gọi là các điểm còn các khối $X_1, \dots, X_v \subseteq X$ được gọi là các đường thẳng. Nếu $x_j \in X_i$ thì ta nói rằng điểm x_j nằm trên đường thẳng X_i hoặc đường thẳng X_i đi qua điểm x_j . Tương tự, bao hàm thức $x_j \in X_i \cap X_k$ có nghĩa là đường thẳng X_i và X_k giao nhau tại điểm x_j .

Với việc sử dụng các thuật ngữ như trên ta có thể nhìn nhận lại các tính chất cơ bản của một (v, b, k) -cấu hình cho trường hợp các mặt phẳng xạ ảnh hữu hạn như sau:

- (1) Mỗi đường thẳng đi qua đúng $n + 1$ điểm.
- (2) Hai đường thẳng bất kỳ giao nhau tại một điểm.
- (3) Mỗi điểm là giao của $n + 1$ đường.
- (4) Chỉ có duy nhất một đường thẳng đi qua hai điểm cho trước.

Các tính chất (2) và (4) là các tính chất của điểm và đường thẳng trong một mặt phẳng thông thường và chúng giải thích cho việc tại sao ta lại sử dụng các thuật ngữ hình học.

Tiếp theo ta sẽ nêu ra một điều kiện cần cho sự tồn tại của một mặt phẳng xạ ảnh hữu hạn bậc n .

Kết quả 12. (Bruck – Ryser) Điều kiện cần để tồn tại một mặt phẳng xạ ảnh bậc n với $n \equiv 1, 2 \pmod{4}$ là tồn tại các số nguyên a và b sao cho $n = a^2 + b^2$.

Chứng minh. Dễ dàng nhận ra rằng khẳng định trên là một hệ quả của định lý Bruck-Chowla-Ryser với $v = n^2 + n + 1, k = n + 1, \lambda = 1$. Khi đó, giá trị $t = \frac{v-1}{2}$ là một số nguyên nên $v = 2t + 1$ là một số lẻ. Do đó ta tìm được các số nguyên x, y, z sao cho $x^2 + y^2 + z^2 \neq 0$ và $z^2 = nx^2 + (-1)^{\frac{n(n+1)}{2}} y^2$.

Nếu $n \equiv 1, 2 \pmod{4}$ thì $\frac{n(n+1)}{2}$ là một số lẻ nên phương trình trên có dạng $nx^2 = z^2 + y^2$.

Từ các hiểu biết quen thuộc về lý thuyết số ta dễ dàng suy ra rằng để tồn tại các số nguyên x, y, z không đồng thời bằng không thỏa mãn hệ thức $nx^2 = z^2 + y^2$ thì ta phải tìm được các số nguyên a và b sao cho $n = a^2 + b^2$, điều phải chứng minh.

2.5.2. Mối liên hệ giữa mặt phẳng xạ ảnh hữu hạn với các hình vuông Latin trực giao

Xét ma trận $C = (c_{ij})_{i=1, \dots, n^2; j=1, \dots, t+2}$ trong đó $c_{ij} \in \{1, \dots, n\}$ và $(c_{ik}, c_{il}) \neq (c_{jk}, c_{jl}), i \neq j, k \neq l$.

Điều kiện trong định nghĩa trên có nghĩa là các hàng của mỗi ma trận con cấp $n^2 \times 2$ của C biểu diễn n^2 cặp phần tử phân biệt (có tính đến thứ tự) được chọn tạo ra từ các số $1, 2, \dots, n$.

Sắp xếp lại các hàng của C sao cho các hàng của ma trận con cấp $n^2 \times 2$ tương ứng với hai cột đầu tiên xuất hiện theo thứ tự sau:

$$(1, 1), \dots, (1, m), (2, 1), \dots, (2, m), \dots, (n, 1), \dots, (n, m).$$

Khi đó hai cột đầu tiên của C được gọi là hai cột chuẩn và ma trận thu được như trên được ma trận chuẩn. Chú ý rằng việc hoán đổi vị trí các cột của ma trận C không làm thay đổi đi điều kiện nêu trong định nghĩa nên quá trình chuẩn hóa trên luôn thực hiện được.

Bây giờ ta xét một tập gồm t hình vuông Latin bậc n đôi một trực giao được tạo thành từ các hoán vị tác động trên tập $\{1, \dots, n\}$. Ta có kết quả cơ bản sau đặt nền tảng cho các khảo sát được thực hiện trong mục này của bài viết.

Kết quả 13. Với $n \geq 3, t \geq 2$, một tập $\mathcal{M}_t$ gồm t hình vuông Latin bậc n đôi một trực giao tương đương với một ma trận C cấp $n^2 \times (t+2)$ thỏa mãn các điều kiện nêu trong định nghĩa ở trên, tức là ta có thể xây dựng được một ma trận C từ tập $\mathcal{M}_t$ và ngược lại.

Chứng minh. Giả sử ta được cho trước một tập $\mathcal{M}_t$ gồm t hình vuông Latin bậc n , $L_n^{(1)}, \dots, L_n^{(t)}$, đôi một trực giao. Ta xây dựng ma trận $C = (c_{ij})_{i=1, \dots, n^2; j=1, \dots, t+2}$ tương ứng với tập $\mathcal{M}_t$ như sau:

Đầu tiên ta xây dựng ma trận con cấp $n^2 \times 2$ tương ứng với hai cột chuẩn trong đó các hàng được đánh thứ tự bởi các cặp phần tử phân biệt (có tính đến thứ tự) được chọn tạo ra từ các số $1, 2, \dots, n$. Tiếp theo, cột thứ l của ma trận này thu được bằng cách đặt tuần tự các hàng của hình vuông Latin $L_n^{(l-2)}$ từ trên xuống dưới, $l = 3, 4, \dots, t+2$.

Ma trận C thu được từ phép xây dựng trên thỏa mãn tất cả các yêu cầu trong định nghĩa.

Thật vậy, hệ thức $(c_{i1}, c_{i2}) = (c_{j1}, c_{j2}), i \neq j$, mâu thuẫn với tính chất của hai cột chuẩn. Các hệ thức $(c_{i1}, c_{ik}) = (c_{j1}, c_{jk}), (c_{i2}, c_{ik}) = (c_{j2}, c_{jk}), i \neq j, k = 3, \dots, t+2$, mâu thuẫn với tính chất không có hai phần tử nằm trên cùng hàng hoặc cùng cột của một hình vuông Latin bị trùng lặp. Sau cùng, các hệ thức $(c_{ik}, c_{il}) = (c_{jk}, c_{jl}), i \neq j, k = 3, \dots, t+2$, mâu thuẫn với tính chất trực giao của các hình vuông Latin ban đầu.

Bây giờ, giả sử ta được cho trước một ma trận $C = (c_{ij})_{i=1, \dots, n^2; j=1, \dots, t+2}$ trong đó $c_{ij} \in \{1, \dots, n\}$ và $(c_{ik}, c_{il}) \neq (c_{jk}, c_{jl}), i \neq j, k \neq l$. Đầu tiên ta chuẩn hóa ma trận C về dạng đặc biệt được nêu ở phần đầu của phân tích. Tiếp theo, ta cho tương ứng cột thứ $(l+2)$ trong dạng chuẩn của ma trận C với hình vuông Latin $L_n^{(l)}$ bằng cách đặt tuần tự các phần độ dài n của cột này làm các hàng của hình vuông Latin $L_n^{(l)}$. Các tính chất xác định một hình vuông Latin được thỏa mãn, do $(c_{ik}, c_{il}) \neq (c_{jk}, c_{jl}), i \neq j, l = 1, \dots, t$, với $k = 1, 2$. Tính

trực giao từng đôi một của các hình vuông Latin $L_n^{(1)}, \dots, L_n^{(t)}$ được suy ra từ điều kiện $(c_{ik}, c_{il}) \neq (c_{jk}, c_{jl})$ với mọi $k \neq l$.

Kết quả 14. Nếu tồn tại các tập $\mathcal{M}_{nt}$ và $\mathcal{M}_{mt}$ gồm t hình vuông Latin bậc n và m trực giao từng đôi một thì đồng thời cũng tồn tại tập $\mathcal{M}_{mn,t}$ gồm t hình vuông Latin bậc mn trực giao từng đôi một.

Chứng minh.

Đặt $C_1 = (c_{ij}^{(1)})_{i=1, \dots, n^2; j=1, \dots, t+2}$, $C_2 = (c_{ij}^{(2)})_{i=1, \dots, n^2; j=1, \dots, t+2}$ là các ma trận ở dạng chuẩn tương ứng với các tập $\mathcal{M}_{nt}$ và $\mathcal{M}_{mt}$. Dựa trên cơ sở của các ma trận C_1 và C_2 , ta xây dựng ma trận C' với $(mn)^2$ hàng:

$$\left[(c_{i1}^{(1)}, c_{j1}^{(2)}), (c_{i2}^{(1)}, c_{j2}^{(2)}), \dots, (c_{i,t+2}^{(1)}, c_{j,t+2}^{(2)}) \right], i=1, \dots, n^2, j=1, \dots, m^2.$$

Ma trận C' có $(mn)^2$ hàng và $t+2$ cột, các hàng của ma trận này được đánh thứ tự bởi các bộ:

$$(1,1), \dots, (1,m), (2,1), \dots, (2,m), \dots, (n,1), \dots, (n,m).$$

Ma trận này thỏa mãn yêu cầu nêu trong Kết quả 13.

Thật vậy, giả sử $C' = (c'_{\alpha\beta})$, trong đó α chạy trên $(mn)^2$ cặp sắp thứ tự có dạng $(i, j), i=1, \dots, n^2, j=1, \dots, m^2$ còn $\beta=1, \dots, t+2$. Khi đó, hệ thức $(c'_{\alpha k}, c'_{\alpha l}) = (c'_{\alpha' k}, c'_{\alpha' l}), \alpha \neq \alpha', k \neq l$ với $\alpha = (i, j), \alpha' = (p, q)$ tương đương với

$$\begin{aligned} c_{ik}^{(1)} &= c_{pk}^{(1)}, c_{il}^{(1)} = c_{pl}^{(1)}, \\ c_{jk}^{(2)} &= c_{qk}^{(2)}, c_{jl}^{(2)} = c_{ql}^{(2)}. \end{aligned}$$

Điều này mâu thuẫn với định nghĩa của các ma trận C_1 và C_2 .

Bằng cách áp dụng Kết quả 13 ta suy ra được rằng ma trận C' tương ứng với một tập gồm t hình vuông Latin bậc mn trực giao nhau từng đôi một và các hoán vị tương ứng với các hình vuông Latin này tác động trên tập các cặp sắp thứ tự $(1,1), \dots, (1,m), (2,1), \dots, (2,m), \dots, (n,1), \dots, (n,m)$.

Bây giờ ta nhận thấy rằng bằng việc áp dụng phương pháp Bose-Stevens xây dựng được một tập đầy đủ gồm $p^a - 1$ hình vuông Latin bậc p^a trực giao từng đôi một, trong đó p là một số nguyên tố. Kết hợp khẳng định này với Kết quả 14 vừa chứng minh được ở phần trên ta nhận được kết quả sau

Hệ quả. Cho $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ và $t = \min_{1 \leq i \leq r} (p_i^{\alpha_i} - 1)$. Khi đó, với mọi $t \geq 2$, luôn tồn tại một tập gồm t hình vuông Latin bậc n trực giao với nhau từng đôi một.

Mặt khác từ Kết quả 13 ta cũng thiết lập được một mối hệ giữa sự tồn tại của một mặt phẳng xạ ảnh hữu hạn bậc n và sự tồn tại của một tập đầy đủ các hình vuông Latin trực giao nhau từng đôi một.

Kết quả 15. Một mặt phẳng xạ ảnh hữu hạn bậc $n \geq 2$ tồn tại khi và chỉ khi tồn tại một tập đầy đủ gồm $n-1$ hình vuông Latin bậc n trực giao với nhau từng đôi một.

Chứng minh. Giả sử ta được cho trước một mặt phẳng xạ ảnh hữu hạn bậc n bao gồm các đường thẳng $X_1, \dots, X_{n^2+n+1}$. Ký hiệu các điểm nằm trên đường thẳng X_1 là $x_1, \dots, x_{n+1}$ và các điểm còn lại của mặt phẳng là $y_1, \dots, y_{n^2}$. Đánh số các đường thẳng khác X_1 đi qua điểm x_1 bởi các số $1, 2, \dots, n$. Sử dụng cách thức tương tự ta đánh số các đường thẳng khác X_1 đi qua điểm $x_2, \dots$, các đường thẳng khác X_1 đi qua điểm x_{n+1} cũng bởi các số $1, 2, \dots, n$.

Nếu c_{ij} là nhãn của đường thẳng đi qua điểm y_i và x_j thì ma trận $C = (c_{ij})_{i=1, \dots, n^2; j=1, \dots, n+1}$ thỏa mãn tính chất $(c_{ik}, c_{il}) \neq (c_{jk}, c_{jl}), i \neq j, k \neq l$.

Thật vậy, giả sử $c_{ik} = c_{jk}, c_{il} = c_{jl}$. Từ hệ thức thứ nhất ta suy đường thẳng đi qua điểm y_i và x_k có cùng nhãn với đường thẳng đi qua điểm y_j và x_k , nói cách khác y_i, y_j và x_k cùng nằm trên một đường thẳng. Tương tự, từ hệ thức thứ hai ta suy ra được rằng y_i, y_j và x_l cũng cùng nằm trên một đường thẳng. Kết hợp hai kết quả trên lại ta suy ra được y_i và y_j nằm trên đường thẳng xác định bởi hai điểm x_k và x_l , tức là y_i

và y_j nằm trên X_1 , mâu thuẫn. Bằng cách áp dụng Kết quả 13 ta xây dựng được một tập đầy đủ gồm $n-1$ hình vuông Latin bậc n trực giao với nhau từng đôi một.

Giả sử ta được cho trước ma trận $C = (c_{ij})_{i=1, \dots, n^2; j=1, \dots, n+1}$ trong đó $c_{ij} \in \{1, \dots, n\}$ và $(c_{ik}, c_{il}) \neq (c_{jk}, c_{jl})$, $i \neq j, k \neq l$. Bây giờ ta tiến hành xây dựng mặt phẳng xạ ảnh hữu hạn tương ứng ma trận C này.

Xét đường thẳng $X_1 = \{x_1, \dots, x_{n+1}\}$ và ký hiệu $y_1, \dots, y_{n^2}$ là các điểm không nằm trên đường thẳng này.

Khi đó ta sử dụng số c_{ij} để gán nhãn cho đường thẳng L_{ij} đi qua hai điểm y_i và x_j . Từ cách gán nhãn các đường thẳng vừa trình bày ở trên ta suy ra được rằng mỗi đường thẳng chứa chính xác $n+1$ điểm, do cột thứ j của ma trận C có n phần tử giống với c_{ij} . Hơn nữa, hai đường thẳng bất kỳ giao nhau tại chính xác một điểm. Thật vậy, giả sử $\{y_\mu, y_\nu\} \subseteq X_k \cap X_l, \mu \neq \nu, k \neq l$. Khi đó, ta tìm được các chỉ số k' và l' sao cho

$c_{\mu k'} = c_{\nu k'}, c_{\mu l'} = c_{\nu l'}, k' \neq l'$, điều này mâu thuẫn với điều kiện nêu trong định nghĩa của ma trận C . Hai tính chất vừa chỉ ra ở trên xác định cho ta một mặt phẳng xạ ảnh; do đó ta đã xây dựng được một cấu trúc mặt phẳng xạ ảnh bậc n tương ứng với ma trận C , hoặc một cách tương đương, với một tập đầy đủ gồm $n-1$ hình vuông Latin bậc n trực giao với nhau từng đôi một.

3. Block design

Trong phần này của bài viết ta xét một dạng mở rộng của (v, b, k) -cấu hình được gọi là (b, v, r, k, λ) -cấu hình. Khái niệm (v, b, k) -cấu hình và (b, v, r, k, λ) -cấu hình đều được gọi tên chung là block design và được sử dụng nhiều trong các tính toán thiết kế các thí nghiệm khoa học.

3.1. (b, v, r, k, λ) -cấu hình

Một họ các tập con $X_1, \dots, X_b$ của tập $X = \{x_1, \dots, x_v\}$ được gọi là một (b, v, r, k, λ) -cấu hình nếu các điều kiện sau được thỏa mãn:

- (1) $|X_i| = k, i = 1, \dots, b$.
- (2) Với mọi phần tử $x_i \in X$, có chính xác r tập con $X_{\mu_1}, \dots, X_{\mu_r}$ chứa x_i .
- (3) Với mọi cặp phần tử $x_i, x_j \in X, i \neq j$, có chính xác λ tập con $X_{\nu_1}, \dots, X_{\nu_\lambda}$ chứa đồng thời x_i và x_j .
- (4) Các số v, k và λ thỏa mãn các điều kiện $\lambda > 0, k < v-1$.

Đặt $A = (a_{ij})_{i=1, \dots, b; j=1, \dots, v}$ là ma trận liên thuộc của một (b, v, r, k, λ) -cấu hình, có nghĩa là $a_{ij} = \begin{cases} 1, & x_j \in X_i, \\ 0, & x_j \notin X_i. \end{cases}$

Ký hiệu J_v là ma trận vuông cấp v và $J_{b \times v}$ là ma trận cấp $b \times v$ trong đó tất cả các phần tử đều bằng 1.

Ta có một số tính chất cơ bản sau của ma trận liên thuộc A :

$$(1) \quad AJ_v = kJ_{bv}.$$

Tính chất trên tương đương với khẳng định rằng $\sum_{j=1}^v a_{ij} = |X_i| = k, i = 1, \dots, b$, và điều này được suy trực tiếp từ định nghĩa của (b, v, r, k, λ) -cấu hình.

$$(2) \quad J_b A = rJ_{bv}.$$

Tính chất trên nói lên rằng $\sum_{i=1}^b a_{ij} = r, j = 1, \dots, v$ và bản thân điều này thì tương đương với điều kiện (2) trong định nghĩa của (b, v, r, k, λ) -cấu hình.

$$(3) \quad A^T A = \lambda J_v + (r - \lambda)I_v.$$

Tính chất này tương đương với việc $\sum_{l=1}^b a_{li} a_{lj} = \begin{cases} r, & i = j, \\ \lambda, & i \neq j, \end{cases}$ và bản thân chúng thì lại biểu thị cho các điều kiện (2) và (3) trong định nghĩa của (b, v, r, k, λ) -cấu hình.

$$(4) \quad bk = vr.$$

Thật vậy, bằng cách cố định phần tử $x_i \in X$. Theo định nghĩa, phần tử x_i nằm trong chính xác r tập con của họ $X_1, \dots, X_b$ nên số các phần tử được chứa trong họ $X_1, \dots, X_b$, tính luôn cả các phần tử bị lặp lại, bằng vr . Mặt khác, do $|X_i| = k, i = 1, \dots, b$ nên ta cũng có thể tính số này theo công thức bk .

$$(5) \quad r(k-1) = \lambda(v-1).$$

Ta thực hiện tính số các cặp phần tử trong đó có một phần tử $x_i \in X$ cố định bằng hai cách khác nhau, lưu ý nếu hai phần tử này cùng nằm trong nhiều tập của họ thì chúng sẽ được tính lặp lại với số lần tương ứng. Với mỗi tập con trong số r tập con có chứa phần tử x_i , phần tử x_i có thể được ghép với một điểm bất kỳ nào đó trong số $k-1$ điểm còn lại để tạo thành một cặp. Do đó, tổng số các cặp cần tính bằng $r(k-1)$. Mặt khác, phần tử x_i có thể x_j cùng nằm trong chính xác λ tập con và bản thân phần tử x_j có thể được chọn theo $v-1$ cách khác nhau nên tổng số các cặp là $\lambda(v-1)$.

$$(6) \quad \det(AA^T) = (r + \lambda(v-1))(r - \lambda)^{v-1}.$$

$$\text{Từ tính chất (3), } \det(AA^T) = \det(\lambda J_v + (r - \lambda)I_v) = (r + \lambda(v-1))(r - \lambda)^{v-1}.$$

$$(7) \quad b \geq v.$$

Tính chất này thường được gọi là bất đẳng thức Fisher. Kết hợp điều kiện $k < v-1$ và tính chất (5) kéo theo rằng $r > \lambda$, nên kết hợp với (6) ta suy ra $\det(AA^T) \neq 0$. Do hạng của tích hai ma trận không lớn hơn hạng của mỗi nhân tử nên $v = \text{rank}(AA^T) \leq \text{rank} A \leq b$.

Kết hợp bất đẳng thức Fisher và tính chất (4) ta suy ra được đánh giá sau:

$$(8) \quad r \geq k.$$

Chú ý rằng (v, k, λ) -cấu hình là một trường hợp riêng của (b, v, r, k, λ) -cấu hình khi $b = v$ hoặc $r = k$. Do đó dưới các điều kiện nhất định các tính chất của (b, v, r, k, λ) -cấu hình sẽ tương ứng với các tính chất của (v, k, λ) -cấu hình và ngược lại.

3.2. Bộ ba Steiner

Một họ các tập con của một tập $X, |X| = v$, mỗi tập con chứa đúng ba phần tử, được gọi là một bộ ba Steiner nếu mỗi tập con gồm hai phần tử của X nằm trong chính xác một bộ ba.

Một bộ ba Steiner, với $v > 3$, là một (b, v, r, k, λ) -cấu hình với $k = 3$ và $\lambda = 1$. Từ tính chất (4) và (5) ta suy ra rằng $2r = v-1, 3b = vr$ nên ta suy ra $b = \frac{v(v-1)}{6}, r = \frac{v-1}{2}$. Do đó ta suy ra rằng $v \equiv 1, 3 \pmod{6}$.

Thật vậy, do $v = 2r + 1$ nên v lẻ và $b = \frac{(2r+1)r}{3}$. Do đó, $r = 3\mu$ hoặc $2r + 1 = 3(2\mu + 1)$, trong đó μ và v là các số tự nhiên nào đó. Suy ra $v = 6\mu + 1$, hoặc $v = 6\mu + 3$.

Kết quả 16. Nếu tồn tại bộ ba Steiner S_1 bậc v_1 và bộ ba Steiner S_2 bậc v_2 thì đồng thời cũng tồn tại bộ ba Steiner S bậc $v_1 v_2$.

Chứng minh. Giả sử S_1 được định nghĩa trên tập $A = \{a_1, \dots, a_{v_1}\}$ còn S_2 được định nghĩa trên tập

$$B = \{b_1, \dots, b_{v_2}\}.$$

Xét tích Descartes $A \times B$ và tiến hành xây dựng hệ S trên tập này như sau:

Một bộ ba $\{(a_i, b_r), (a_j, b_s), (a_k, b_t)\}$ nằm trong S nếu một trong các điều kiện sau được thỏa mãn:

$$\{a_i, a_j, a_k\} \in S_1, b_r = b_s = b_t;$$

$$\{b_r, b_s, b_t\} \in S_2, a_i = a_j = a_k;$$

$$\{a_i, a_j, a_k\} \in S_1, \{b_r, b_s, b_t\} \in S_2.$$

Dễ dàng kiểm tra được rằng có chính xác một bộ ba trong hệ S chứa một cặp phần tử cho trước. Bậc của hệ S là $|A \times B| = v_1 v_2$. Số các bộ ba của hệ S bằng $b = \frac{v_1 v_2 (v_1 v_2 - 1)}{6}$. Số các bộ ba của hệ S cùng chứa một phần tử cho trước là $r = \frac{v_1 v_2 - 1}{2}$.

Tài liệu tham khảo:

- [1]. Trương Phước Nhân, BIBD, 02/02/2018.
- [2]. Trương Phước Nhân, Bộ ba Steiner, 02/02/2018.
- [3]. Trương Phước Nhân, Cấu hình đối xứng, 06/02/2018.
- [4]. Trương Phước Nhân, Designs, 22/07/2018.
- [5]. Trương Phước Nhân, Định lý Bruck-Ryser-Chowla về design đối xứng, 07/02/2018.
- [6]. Trương Phước Nhân, Lý thuyết cấu hình tổ hợp, 02/02/2018.
- [7]. Trương Phước Nhân, Ma trận Hadamard, 10/02/2018.
- [8]. Trương Phước Nhân, Mô hình designs - Tập difference, 22/07/2018.
- [9]. Trương Phước Nhân, Tiếp cận sơ cấp bất đẳng thức Fisher, 10/02/2018.
- [10]. Vladimir N. Sachkov, Combinatorial Methods in Discrete Mathematics, Cambridge University Press.