УДК 517.1:519.1

О. Д. Глухов (Нац. авіац. ун-т, Київ)

ПРО ЗАСТОСУВАННЯ ГРУП ПЕРЕСТАНОВОК У ДЕЯКИХ КОМБІНАТОРНИХ ЗАДАЧАХ

We show how certain properties of permutation groups can be applied to the construction of combinatorical objects with given properties.

Показано, как некоторые свойства групп перестановок можно применить к конструированию комбинаторных объектов с заданными свойствами.

1. Постановка задачі. Нехай група G діє на множині U, а $B = \{u\colon u \in U, P(u)\}$ — множина елементів множини U, які мають певну властивість P. Виникає питання: чи існує таке перетворення $g \in G$, що для будь-якого $u \in U$ принаймні один з елементів u або $g(u)$ має властивість P? Виявляється, що таке перетворення завжди існує, якщо, наприклад, група G є транзитивною [1] і виконано умову $|U \setminus B|^2 = |U|$. Хоча це твердження нескладно довести (а також узагальнити на випадок не обов'язково транзитивних груп), однак воно має низку наслідків, що дозволяють, зокрема, встановлювати існування деяких комбінаторних об'єктів із заданими властивостями.

2. Основна теорема і її узагальнення. Доведемо спочатку наступне твердження.

Лема 1. *Якщо група G діє на множині U транзитивно, $|U| = n$ і A, $B \subset U$, $|A| = k$, $|B| = r$, $A \bigcap B = \varnothing$, то знайдеться $g \in G$ таке, що $|g(A) \bigcap B| > rk/n$.*

Доведення. Нехай в умовах леми $|G| = m$, $\{g_i(a_j)\}$ — прямокутна $(m \times n)$-матриця, $i = 1(1)n$, $j = 1(1)m$, і, крім того, s — середнє, а t — максимальне число елементів множини B у рядках $g_i(A)$, $i = 1(1)n$. Легко підрахувати, що в кожнім стовпці матриці міститься mr/n елементів з B і тому в матриці зустрічаються елементи множини B mrk/n разів, а отже, $s = rk/n$. Однак у рядку, що відповідає одиниці групи, за умовою немає елементів з B і тому $t > s$, звідси і випливає твердження леми.

Лема 2. *Якщо група G діє на множині U транзитивно і $A \subset U$, $|U| = n$, $|A| = k$, то має місце нерівність*

$$|g \in G : g(A) \bigcap A \neq \varnothing| \leq mk^2/n,$$

причому для $k \geq 2$ виконується нерівність

$$|g \in G : g(A) \bigcap A \neq \varnothing| < mk^2/n.$$

Доведення повністю аналогічне доведенню леми 1 для випадку $B = U \setminus A$.

Теорема 1. *Якщо група G діє на множині U транзитивно, $A \subset U$ і виконується нерівність $|A|^2 \leq |U|$, то існує $g \in G$ таке, що $g(A) \bigcap A = \varnothing$.*

Доведення безпосередньо випливає з леми 1, якщо покласти $B = U \setminus A$, $r = n - k$, $k = \sqrt{n}$.

Використовуючи індукцію, можна довести наступне узагальнення теореми 1.

Теорема 2. *Якщо група G діє на множині U транзитивно і виконується нерівність $|A|^{2k/(2k-1)} \leq |U|$, то знайдеться така множина $\{g_i\}_{i=0}^{k}$ елементів групи G, де g_0 — одиниця групи G, що $\bigcap_{i=0}^{k} g_i(A) = \varnothing$.*

З теореми 2 випливає, що якщо G — транзитивна група перетворень на множині з n елементів і число елементів цієї множини, які не мають властивості P, не більше ніж $n^{1-1/2k}$, то існують k таких перетворень $g_1, \ldots, g_k \in G$, що для будь-якого елемента x заданої множини принаймні один з елементів x, $g_1(x), \ldots, g_k(x)$ має зазначену властивість.

Наступна теорема є узагальненням теореми 1 на випадок не обов'язково транзитивної групи.

Теорема 3. *Якщо група G діє на множині U, $U = \sum_{i=1}^{p} U_i$, U_i — G-орбіта, $i = 1(1)p$, і для деякої підмножини $A \subset U$ виконано умову*

$$\sum_{i=1}^{p} |A \cap U_i|^2 / |U_i| < 1,$$

то найдеться $g \in G$ таке, що $g(A) \cap A = \varnothing$.

Доведення. Нехай умови теореми виконано і $|G| = m$. Позначимо $A_i = A \cap U_i$, $t_i = |A_i|^2 / |U_i|$, $i = 1(1)p$. Використовуючи лему 2, легко показати, що для всіх $i = 1(1)p$ виконується нерівність $|g : g(A_i) \cap A_i \neq \varnothing| \leq m\, t_i$. Тому має місце нерівність

$$|g : g(A) \cap A \neq \varnothing| \leq \sum_{i=1}^{p} m t_i < m,$$

звідки одразу випливає твердження теореми.

3. Приклад і застосування. ***Приклад* 1.** Наступний приклад показує, що оцінка $k = \sqrt{n}$ у теоремі 1 є досяжною. Нехай група Z_{16} лишків по модулю 16 діє на множині своїх елементів природним чином, тобто $x(y) = x + y$, де $x, y \in Z_{16}$. Тоді $k = 4$, а для множини $A = \{0, 1, 4, 9, 11\}$ з 5 елементів умова леми вже не виконується, оскільки легко перевірити, що для будь-якого $g \in Z_{16}$ $g(A) \cap A \neq \varnothing$.

***Приклад* 2.** Покажемо, що для довільного n оцінку, отриману в теоремі 1, не можна істотно покращити. Дійсно, нехай G — реберна група автоморфізмів повного p-вершинного графа [2], U — множина його ребер, $|U| = n$, $n = p(p-1)/2$, A_i — множина ребер, що інцидентні вершині i цього графа, $|A_i| = k = p - 1$. Зрозуміло, що хоча k близьке до $\sqrt{2n}$, однак для будь-якого $g \in G$ $g(A_i) = A_j$ і $A_i \cap A_j \neq \varnothing$, $i, j = 1(1)p$.

***Приклад* 3** (наслідок теореми 1). Якщо H_n — вершинно-симетричний граф на n вершинах, а F_k — його k-вершинний підграф і $k \leq \sqrt{n}$, то в графі H_n знайдеться принаймні ще один ізоморфний F_k підграф, який не має з ним спільних вершин.

Цікаві результати можна отримати, якщо розглянути в якості множини U

множину $X^{(r)}$ усіх r-підмножин деякої множини X, а в якості групи G симетричну групу S_n, $n = |X|$, яка діє транзитивно на множині $X^{(r)}$ таким чином: якщо $g \in S_n$, $A \in X^{(r)}$, то $g(A) = \{g(a) : a \in A\}$.

Далі нам знадобиться наступне твердження про біноміальні коефіцієнти.

Лема 3. *Якщо* $n, m \geq 2$, $0 < \alpha < 1$, $k = [\alpha m]$, *то справджуються оцінки*

$$C_{2n}^n \geq \frac{3}{4\sqrt{2n}} 2^{2n}, \qquad C_m^k \leq (em/k)^k, \qquad C_m^k \leq 2^{\alpha^* m},$$

де $\alpha^* = \alpha \log_2(e/\alpha)$, *зокрема, якщо* $\alpha \leq 0{,}1$, *то* $\alpha^* < 0{,}48$.

Задача про перемішування. Розглянемо $(0,1)$-послідовність $a_1, a_2, \ldots, a_{2n}$, яка складається з однакового числа нулів і одиниць (такі послідовності будемо називати збалансованими). Варіацією послідовності будемо називати величину, задану таким чином:

$$\operatorname{var}\{a_1, a_2, \ldots, a_{2n}\} = \frac{1}{2n} \sum_{i=1}^{2n-1} |a_{i+1} - a_i|.$$

Послідовність будемо називати малоперемішаною, якщо її варіація не більша ніж $0{,}1$. Покажемо, що для досить великих n існує „універсальна перестановка, що переміщує“ g, тобто така, що задовольняє умову: для будь-якої збалансованої малоперемішаної послідовності $a_1, a_2, \ldots, a_{2n}$ послідовність $a_{g(1)}$, $a_{g(2)}, \ldots, a_{g(2n)}$ уже не буде малоперемішаною. Відповідно до теореми 1 для цього досить оцінити число p збалансованих послідовностей з варіацією не більшою ніж $0{,}1$ і перевірити, що виконується нерівність $p^2 \leq q$, де $q = C_{2n}^n$ — число всіх збалансованих $(0,1)$-послідовностей. Поставивши у відповідність послідовності з варіацією не більшою ніж $0{,}1$ послідовність початків її сегментів, кожен з яких складається з нулів або одиниць, і використавши лему 2 при $m = 2n$, $\alpha = 0{,}1$, $k = [\alpha m]$, отримаємо співвідношення

$$p \leq \sum_{i \leq k} C_{2n}^i < 0{,}2n\, C_{2n}^k \leq 0{,}2n\, 2^{0{,}96n}.$$

Тому для досить великих n $p^2 < p^{2n}$ і, отже, $p^2 \leq q$, що й потрібно було довести.

Задача про квазізбільшувачі. Розглянемо тепер одну задачу з теорії графів. Нехай H_n — граф на n вершинах із множинами H_n^0 вершин і H_n^1 ребер. Валентністю графа будемо називати найбільшу степінь його вершин. Будемо також використовувати позначення

$$\rho(X, H_n) = \left|\left\{(xy) : (xy) \in H_n^1,\ x \in X,\ y \notin X\right\}\right|, \quad X \subset H_n^0.$$

Граф H_{2n} назвемо квазізбільшувачем, якщо для будь-якого $X \subset H_{2n}^0$, $|X| = n$, виконується нерівність $\rho(X, H_n) \geq \alpha n$, де $\alpha > 0$ — деяка константа [3]. Зауважимо, що такі графи використовують в задачах забезпечення живучості і діагнозоспроможності складних технічних систем [4]. Покажемо, як, використовуючи отримані результати, можна довести існування квазізбільшувачів H_{2n} валентності 4 для будь-яких досить великих n. Нехай Z_{2n} — граф, що є простим циклом порядку $2n$, $Z_{2n}^0 = \{1, 2, \ldots, 2n\}$, $g(Z_{2n})$ — граф, що одержується із графа Z_{2n} перестановкою g множини його вершин, причому якщо в графі Z_{2n} є ребро (i, j), то в графі $g(Z_{2n})$ є ребро $(g(i), g(j))$. Вибравши згідно з теоремою 1 потрібну перестановку g, побудуємо квазізбільшувач H_{2n} таким чином: $H_{2n} = Z_{2n} \bigcup g(Z_{2n})$. Цю конструкцію будемо називати „склейкою двох графів за допомогою перестановки”. Доведення існування необхідної перестановки g зводиться тепер до підрахунку числа

$$p = \left|\left\{X : X \subset Z_{2n}^0,\ |X| = n,\ \rho(X, Z_{2n}) < \alpha n\right\}\right|$$

при $\alpha = 0,1$ і перевірки нерівності $p^2 \le q$, де $q = C_{2n}^n$ і, таким чином, практично повторює міркування з задачі про перемішування.

Тут виникає питання про величину константи α при обмеженні валентності квазізбільшувача H_{2n}. Застосувавши замість теореми 1 теорему 2 і склеївши замість двох циклів k циклів для деякого фіксованого k, покажемо, що можна взяти $\alpha = 0{,}327$. Дійсно, згідно з лемою 3 маємо нерівність $p \le 2\alpha n 2^{\alpha^* 2n}$. Легко перевірити, що якщо $\alpha = 0{,}327$, то $\alpha^* < 1$ і, взявши $k > 1/2(1-\alpha^*)$, для досить великих n отримаємо нерівність $p^{2k/(2k-1)} < q$, $q = C_{2n}^n$. Таким чином, згідно з теоремою 2 для досить великих n існують квазізбільшувачі H_{2n} обмеженої валентності з константою $\alpha = 0{,}327$ (щоправда, валентність графа при такій константі дорівнює 1104).

Задача про збільшувачі. Використовуючи теорему 3, можна довести існування графів, що є збільшувачами [5] валентності 4, аналогічно тому, як за допомогою теореми 1 було доведено існування квазізбільшувачів. Нагадаємо, що граф H_n називається збільшувачем, якщо для будь-якого $X \subset H_n^0$, $|X| \le n/2$ виконується нерівність $\rho(X, H_n) \ge \alpha|X|$, де $\alpha > 0$ — деяка константа. Дійсно, покладемо $Z_n^0 = \{1, 2, \ldots, n\}$, $U = \left\{X : X \subset Z_n^0,\ |X| \le n/2\right\}$, $A = \{X : X \in U,\ \rho(X, Z_n) < \alpha|X|\}$ і нехай на множині U діє симетрична група $G = S_n$ так, як описано вище; $U_1, \ldots, U_p$ — її орбіти, $p = [n/2]$. Тоді при $1 \le k \le n/2$ виконуються наступні співвідношення:

$$|A \cap U_k|^2 < \left(\sum_{j \le \alpha k} C_n^j\right)^2 < \alpha^2 k^2 (en/\alpha k)^{2\alpha k}, \qquad |U_k| = C_n^k \ge (n/k)^k.$$

Елементарні оцінки показують, що для досить великих n і досить малих α виконується нерівність $|A \cap U_k|^2 / |U_k| < 2/n$. Тепер для доведення існування збільшувачів досить застосувати теорему 3 і конструкцію „склейки двох графів за допомогою перестановки”.

1. *Холл М.* Теория групп. – М.: Изд-во иностр. лит., 1962.
2. *Харари Ф.* Теория графов. – М.: Мир, 1973. – 337 с.
3. *Alon N.* Eigenvalues and expanders // Combinatorica. – 1986. – **6**, № 2. – P. 83 – 96.
4. *Глухов А. Д.* Диагнозоспособность, связностная функция и спектр графа // Электрон. моделирование. – 1995. – № 2. – С. 92 – 94.
5. *Глухов О. Д.* Дослідження існування деяких комбінаторних об’єктів методами теорії груп перестановок // Тези доп. 1-го Укр. мат. конгресу. – Київ, 2001. – 2001. – С. 62 – 63.

Одержано 19.10.06