DOI: https://doi.org/10.15407/emodel.43.02.029
УДК 519.1 + 681.5

О.Д. Глухов, канд. фіз.-мат. наук
Національний авіаційний університет України
Україна, 03058, Київ, пр-т Любомира Гузара, 1,
тел. 044 4067841; e-mail: glukhov07@gmail.com

Теорема про випадкові перестановки та деякі її застосування

Розглянуто метод випадкових перестановок та його застосування до теорії графів та структурного аналізу складних дискретних систем. Запропоновано метод перестановочної склейки двох графів, який дозволяє будувати графи з даними зв' язнісними властивостями, що, у свою чергу, надає можливість конструювати складні дискретні системи з необхідними структурними якостями.

К л ю ч о в і   с л о в а: складна дискретна система, граф, група перестановок.

При дослідженні структурних властивостей складних дискретних систем широко застосовується теорія графів. Зокрема, для оцінки можливості системи зберігати певні структурні властивості при порушенні зв'язків між її елементами важливими є дослідження різних видів зв'язності графа та їх узагальнень [1—3]. Відомо, що в деяких випадках складно побудувати графи, які мають певну властивість, але водночас «випадкові» графи можуть мати задану властивість з високою ймовірністю. Ідея використання випадкових графів для побудови графів з потрібними властивостями була запропонована ще в класичній роботі Ердеша і Реньї [4].

Розглянемо новий, відмінний від класичного, спосіб побудови випадкових графів, а саме графів, які мають потрібні зв'язністні властивості, за допомогою операції випадкової перестановочної склейки двох заданих графів достатньо простої структури.

Випадкові перестановки і диз'юнктні множини.

Означення 1. Нехай група Γ діє на множині U, пара (A, B) множин $A, B \subset U$ називається диз'юнктною, якщо існує таке $g \in \Gamma$, що $g\,(A) \cap B = \varnothing$.

Зауважимо, що оскільки $g^{-1}(g(A) \cap B) = A \cap g^{-1}(B)$, пари (A, B) і (B, A) є диз'юнктними одночасно. Якщо пара (A, A) є диз'юнктною, то будемо вважати, що множина A є диз'юнктною.

Лема 1. Якщо група Γ діє на множині U транзитивно, $A, B \subset U$, $|U| = n, |A| = k, |B| = r$, $g \in \Gamma$, то

$$\mathrm{Prob}\,(g(A) \cap B = \varnothing) \geq 1 - kr / n.$$

Д о в е д е н н я. Підрахуємо кількість пар (a, g), $a \in A$, $g \in \Gamma$, $g(a) \in U \setminus B$. Оскільки Γ діє на множині U транзитивно, легко бачити, що

$$|\{(a, g) \mid a \in A,\, g(a) \in U \setminus B\}| = mk\,(n-k)/n, \text{ де } |U| = m.$$

Нехай $x = |\{g \mid g(A) \not\subset U \setminus B\}|$. Нескладно порахувати, що дійсна наступна нерівність: $x(k-1) + (m-x)\,k \geq mk\,(n-k)/n$. Отже, справедлива нерівність $x/m \leq kr/n$, з якої одразу випливає твердження леми 1. За допомогою леми 1 легко довести наступну теорему.

Теорема 1. Якщо група Γ діє на множині U, де $\{U_k\}_{k=1}^{s}$ — множина орбіт цієї групи, $A, B \subset U$, g — випадковий елемент групи Γ, то

$$\mathrm{Prob}\,(g(A) \cap B = \varnothing) \geq 1 - \sum_{k=1}^{s} |A \cap U_k|\,|B \cap U_k| / |U_k|.$$

Наступне твердження, яке також випливає з леми 1, доводить існування диз'юнктних підмножин даної множини U при певних обмеженнях на число елементів підмножини A.

Теорема 2 [5]**.** Якщо група Γ діє транзитивно на множині U, $A, B \subset U$, і виконано умову $|A|\,|B| < |U|$, то пара (A, B) множин $A, B \subset U$ буде диз'юнктною. Зокрема, якщо $|U| = n$, $|A| = k$, де $k < \sqrt{n}$, то множина A буде диз'юнктною.

Виникає питання щодо точності оцінки $k < \sqrt{n}$, а саме: якщо група Γ транзитивно діє на множині U, $|U| = n$, то при якому максимально можливому значенні k кожна підмножина порядка не більше k, буде диз'юнкною? Покажемо, що цю оцінку в певному сенсі покращити неможливо, а саме можна побудувати приклад множини U якого завгодно великого порядку n, на якій деяка група Γ діє транзитивно і в якій існує не диз'юнктна підмножина A, $|A| = \lceil \sqrt{n} \rceil$.

Розглянемо скінченну проективну площину Галуа $PG(2, m)$, яка містить $n = m^2 + m + 1$ точок (і стільки ж прямих) та існує для усіх $m = p^s$. Відомо [6], що група автоморфізмів $PG(2, m)$ містить циклічну підгрупу Z_n, яка діє транзитивно на множині точок і на множині прямих цієї площини. Нехай тепер A — будь-яка пряма даної площини, а $g \in Z_n$ — будь-яка перестановка. Тоді і $A_1 = g(A)$ також є прямою цієї площини, при цьому $|A| = |A_1| = m + 1 = \lceil \sqrt{n} \rceil$. Але $g(A) \cap A = A_1 \cap A \neq \varnothing$, тому що кожна пара прямих має точно одну спільну точку.

Нехай $G = G_n$ — звичайний неорієнтований граф з множиною G_n^0 вершин і множиною G_n^1 ребер, де $|G_n^0| = n, |G_n^1| = m$. Для будь-якої множини $A \subset G^0$ графа G степінь $\rho(A, G)$ підмножини в A вершин графа G визначимо так:

$$\rho(A, G) = |\{(a, b) : (a, b) \in G^1,\ a \in A,\ b \notin A]|.$$

Означення 2. Нехай F, H — два графи, $F^0 \cap H^0 = \varnothing$, $|F^0| = \{a_1, a_2, ... a_n\}$, $|H^0| = \{b_1, b_2, ..., b_n\}$ і нехай g — деяка перестановка на множині $\{1, 2, ..., n\}$, яка задає бієкцію $\varphi : H^0 \to F^0$ за правилом: $\varphi(b_i) = a_{g(i)}$. Граф $G = F \langle g \rangle H$, отриманий склейкою (ототожненням) кожної вершини $b_k \in H^0$ з вершиною $a_{g(k)} \in F^0$, будемо називати перестановочною склейкою графів F і H.

Застосуваня. ***Експандери.*** Покажемо, як теореми 1 і 2 можна застосувати в деяких задачах теорії графів, зокрема, наприклад, для побудови збільшувачів або експандерів, які містять даний підграф.

Експандери — це особливий вид графів, який широко застосовуються в теорії інформації, обчислювальній техніці та в багатьох інших галузях науки і техніки [3, 7]. Тому значний інтерес викликають складні дискретні системи, структура яких базується на графах, що є експандерами. Нагадаємо, що граф $G_n, |G_n^0| = n$, називається експандером (збільшувачем), якщо для будь-якого $A \subset G_n^0$, $|A| \leq n/2$, справедлива нерівність $\rho(A, G_n) \geq \alpha |A|$, де $\alpha > 0$ — деяка константа [3].

Розглянемо довільний зв'язний граф H_n, де $H_n^0 = V_n = \{1, 2, ..., n\}$. Множини U, A визначимо наступним чином:

$$U = \{X : X \subset V_n,\ |X| \le n/2\},$$
$$A = \{X : X \in U,\ \rho(X, H_n) < \alpha |X|\}.$$

Нехай тепер на множині V_n діє (транзитивно) симетрична група S_n. Тоді група S_n також діє і на множині за правилом

$$g \in S_n,\ X \in U \Rightarrow g(X) = \{g(x) : x \in X\}.$$

При цьому орбітами будуть, очевидно, множини U_k, де $U_k = \{X : X \in U,\ |X| = k\}$, $k \in V_n, k \le n/2$.

Отже, розглянемо множинуU, на якій діє транзитивно група S_n, і її підмножину $A \subset U$, визначену вище. Візьмемо тепер граф F_n, ізоморфний графу H_n, і розглянемо граф $G_n = H_n \langle g \rangle F_n$, який є перестановочною склейкою цих двох ізоморфних графів по перестановці $g \in S_n$. Якщо підмножина A виявиться диз'юнктною, то граф G_n буде збільшувачем.

Дійсно, припустимо, що A диз'юнктна і для деякого $g \in S_n$ $g(A) \cap A = \varnothing$. Якщо $X \in A$, то $g(X) \notin A$, а значить, якщо $\rho(X, H_n) < \alpha |X|$, то $\rho(X, F_n) < \alpha |X|$. Таким чином, для кожного $X \in U$ або $\rho(X, H_n) \ge \alpha |X|$ або $\rho(X, F_n) \ge \alpha |X|$, а отже, завжди дійсна нерівність$\rho(X, G_n) < \alpha |X|$.

Лема 2. Якщо H_n — довільний зв'язний граф, то при достатньо малому значенні$\alpha > 0$ дійсною є нерівність $|A \cap U_k|^2 / |U_k| < (ck/n)^{1-2\alpha}$, де $0 < c < 2$.

Лема 3. Якщо $0 < c < 2$, $\theta > 0$, то справедливою є оцінка

$$\sum_{k=1}^{\lceil n/2 \rceil} (ck/n)^{\theta k} = o(1).$$

Теорема 3. Перестановочна склейка $G_n = H_n \langle g \rangle F_n$ двох ізоморфних зв'язних графів по випадковій перестановці $g \in S_n$ буде збільшувачем (при достатньо малому значенні $\alpha > 0$) з ймовірністю $1 - o(1)$.

Д о в е д е н н я одразу випливає з теореми 1 та лем 2 і 3. Зауважимо, що існує ефективний спосіб перевірки, чи даний граф, зокрема отриманий граф $G_n = H_n \langle g \rangle F_n$, дійсно буде збільшувачем [1, 3].

Реберна зв'язність. Розглянемо наступну задачу. Нехай G_{2n}^0 граф на $2n$ вершинах є k-реберно зв'язним. Чи можна додати до нього n ребер, щоб в результаті отримати новий граф, який буде (k+1)-реберно зв'язним? Покажемо, що це можливо, більше того, якщо до даного графа випадковим способом приклеїти паросполуку, то з достатньо великою ймовірністю отримаємо граф, реберна зв'язність якого, принаймні, на одиницю більша.

Нехай G_{2n}^0 — граф на $2n$ вершинах з множиною вершин G_{2n}^0 і множиною ребер G_{2n}^1. Реберна зв'язність цього графа $\kappa^1(G_{2n})$, а H_{2n} — деяка паросполука (1-регулярний граф) на тих же вершинах. Покажемо, що для довільного графа G_{2n}, $\kappa^1(G_{2n}) = k \geq 1$, існує така перестановка g множини G_{2n}^0, що $\kappa^1(G_{2n}\langle g\rangle H_{2n}) \geq k+1$, тобто для деякої випадкової перестановки g множини G_{2n}^0 умову $\kappa^1(G_{2n}\langle g\rangle H_{2n}) \geq k+1$ буде виконано з деякою додатною ймовірністю при достатньо великих значеннях n.

Будемо також використовувати твердження, яке випливає з результатів роботи [8].

Лема 4. Якщо $\kappa^1(G_{2n}) = r$, то $\forall k \,|\{X : X \subset G^0,\ |X| = k, \rho(X, G_{2n}) = = r\}| \leq 2n$.

Конструкція. Нехай в умовах теореми 1:

$U = 2^V$,

$V = G_{2n}^0 = \{1, 2, ..., 2n\}$,

$U_k = \{V_k : V_k \subset V, |V_k| = k\}$,

$A = \{X : X \subset V, \rho(X, G) = r\}$,

$B = \{X : X \subset V, \rho(X, H) = 0\}$,

$A_k = A \cap U_k = \{X : X \subset V,\ \rho(X, G) = r, |X| = k\}$, де $1 \leq k \leq n$.

Зауважимо, що дійсні наступні рівності:

$$|U_{2k}| = \binom{2n}{k}, \quad |B \cap U_k| = \binom{n}{k/2},$$

якщо k — парне, і $B \cap U_k = \varnothing$, якщо k— непарне.

Поширимо дію симетричної групи S підстановок на множині V на множину $U = 2^V$ наступним чином:

$$\forall s \in S\ \forall X \in U:\ s(X) = \{s(x) : x \in X\}.$$

Очевидно, що орбітами цієї групи будуть множини $\{U_k\}_0^n$. Тепер можна застосувати теорему 1 при $k > 2$ (випадок $k = 2$ вимагає окремої оцінки) і отримати наступне твердження.

Теорема 4. Нехай G_{2n} граф на $2n$ вершинах $\kappa^1(G_{2n}) = r$, а H_{2n} — деякий 1-регулярний граф на тих же вершинах, g — випадкова перестановка, $g \in S_{2n}$. Тоді запишемо

$$\mathrm{Prob}\,(\kappa^1(G_{2n}\langle g\rangle\, H_{2n}) \geq r+1\,) \geq 1/3 - \varepsilon\,,$$

де $\varepsilon = O\,(1/n)$.

Д о в е д е н н я. Розглянемо спочатку випадок $k \geq 3$. Застосуємо теорему 1 і підрахуємо величини $|A_k|\cdot|B\cap U_k|/|U_k|$ при $3 \leq k \leq n$. Оскільки для усіх непарних $k|B\cap U_k| = 0$, залишається розглянути випадок парних k, $4 \leq k \leq n$. Для парних k згідно з лемою 4 маємо нерівність

$$|A_k|\cdot|B\cap U_k|/|U_k| \leq 2n\binom{n}{k/2}\Big/\binom{2n}{k}.$$

Враховуючи справедливість нерівності $\binom{2n}{k} \geq \binom{n}{k/2}^2$, отримаємо нерівність

$$|A_k|\cdot|B\cap U_k|/|U_k| \leq 2n/\binom{n}{k/2}.$$

Легко перевірити, що при $k = 4$ справедлива оцінка

$$2n/\binom{n}{k/2} = 4/(n-1) = O\,(n^{-1}),$$

а при $6 \leq k \leq n$ — оцінка

$$2n/\binom{n}{k/2} = O\,(n^{-2}).$$

Таким чином, маємо оцінку

$$\sum_{k=3}^{n} |A_k|\cdot|B\cap U_k|/|U_k| = o\,(1).$$

Розглянемо далі випадок $k = 2$. Нехай граф F визначено так: $F^0 = V$, $F^1 = A_2$. Нескладно довести, що максимальна степінь вершини такого графа буде не більше двох. Враховуючи цей факт, ймовірність того, що $F^1 \cap H_{2n}^1 = \varnothing$, можна оцінити за нерівністю Бонферроні [9]:

$$P(\cup X_k) \le \sum_k P(X_k) - \sum_{i<j} P(X_i \cap X_j) + \sum_{i<j<s} P(X_i \cap X_j \cap X_s).$$

Нехай $|A_2| = \{u_1, u_2, ..., u_m\}$, $m \le 2n$ і X_k — подія, яка полягає в тому, що $u_k \in A_2 \cap H_{2n}^1$. Тоді нескладно підрахувати, що справедлива наступна оцінка:

$$P(\cup X_k) \le 2n/(2n-1) - (1/2)(2n/(2n-1)) + (1/6)(2n/(2n-1)).$$

Отже, $P(\cup X_k) \le 2/3 + \varepsilon$, де $\varepsilon = O(1/n)$. Таким чином, отримуємо

$$|A_2||B \cap U_2|/|U_2| \le 2/3 + \varepsilon,$$

звідки остаточно випливає твердження теореми 4.

Висновки

Доведена теорема 4 про випадкові перестановки дозволяє будувати графи з заданими властивостями за допомогою об'єднання двох графів простої структури з використанням так званої перестановочної склейки. Це відкриває нові можливості конструювання складних дискретних систем з необхідними структурними якостями.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Глухов А.Д.* Квазислучайные графы и структурная устойчивость сложных дискретных систем//Электрон. моделирование, 2016 , **38**, №5, с.35—41.
2. *Глухов О.Д., Коростіль Ю.М.* Структурна безпека складних дискретних систем при випадкових відмовах// Зб. наук. праць ІПМЕ НАНУ «Моделювання та інформаційні технології», вип. 27. Київ, 2004, с. 91—95.
3. *Diestel R.* Graph Theory. NY: Springer-Verlag, 2000, 322 p.
4. *Erdős P., Rényi A.* On Random Graphs I // Publ. Math, 1959, Vol. 6, pp. 290—297.
5. *Глухов О.Д.* Про застосування груп перестановок в деяких комбінаторних задачах // Укр. мат. журнал, 2008, **60**, №11, с.1568—1571.
6. *Картеси Ф.* Введение в конечные геометрии. М.: Наука, 1980, 320 с.
7. *Hoory S., Linial N., Wigderson A.* Expander graphs and their applications // Bulletin of the American Mathematical Society, 2006, Vol. 43, № 4, pp. 439 —561.
8. *Диниц Е.А., Карзанов А.В., Ломоносов М.В.* О структуре системы минимальных реберных разрезов графа. Исследования по дискретной оптимизации. М.: Наука, 1976, с. 290—306.
9. *Сачков В.Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978, 288 с.

Отримано 30.12.21

REFERECES

1. Glukhov, O. (2016), "*Quasi-Random Graphs and Structural Stability of Complex Discrete Systems*", *Elektronnoe modelirovaniye*, Vol. 38, no. 5, pp. 35-41.
2. Glukhov, O. and Korostil, Ju. (2004), "Structural safety of complex discrete systems with random failures", *Modelirovanie ta informaziyni tehnologii*, Vol. 27, pp. 91-95.
3. Diestel, R. (2000), Graph Theory, Springer-Verlag, NY, USA.
4. Erdős, P. and Rényi, A. (1959), "On Random Graphs I", *Publicationes Mathematicae Debrecen*, Vol. 6, pp. 290-297.
5. Glukhov, O. (2008), "On the application of permutation groups in some combinatorial problems", *Ukrayinskyy matematychnyy zhurnal*, Vol. 60, no. 11, pp.1568-1571.
6. Kartesi, F. (1980), *Vvedenie v konechnye geometrii* [Introduction to finite geometries], Nauka, Moscow, Russia.
7. Hoory, S., Linial, N. and Wigderson, A. (2006), "Expander graphs and their applications", *Bulletin of the American Mathematical Society*, Vol. 43, no. 4. pp. 439-561.
8. Diniz, E.A, Karzanov, A.V. and Lomonosov, M.V. (1976), "About a structure of a system of minimum cut sets of the graph", *Issledovaniya po diskretnoy optimizatsii*, pp. 290-306.
9. Sachkov, V. (1978), *Veroyatnostnye metody v kombinatornom analise* [Probabilistic methods in combinatorial analysis], Nauka, Moscow, Russia.

Received 30.12.21

A.D. Glukhov

RANDOM PERMUTATION THEOREM AND SOME OF ITS APPLICATIONS

In the study of the structural properties of complex discrete systems, graph theory is widely used. Thus, to assess the ability of a system to retain certain structural properties when breaking the relationships between its elements, it is important to study different types of connectivity of the graph and their generalizations. Of particular interest is the question of how likely it is that a given graph will remain connected or have a sufficiently large connected component when a certain number of its edges are removed? In this paper, the theorem on random permutations is proved and a number of its applications in graph theory are considered. The operation of "permutation gluing of graphs" is introduced. It is shown how with the help of such gluing of two given graphs of a rather simple structure it is possible to construct graphs which with sufficient probability have the necessary connected properties. In particular, the constructions are described, which with a given probability allow to build expanders as well as graphs of greater connectivity. This approach allows you to synthesize graphs with certain properties as a result of some stochastic process followed by selection.

K e y w o r d s: complex discrete system, graph, permutation group.

ГЛУХОВ Олександр Дмитрович, канд. фіз.-мат. наук, доцент кафедри вищої математики Національного авіаційного університету. В 1977 г. закінчив Київский політехнічний ін-т. Область наукових досліджень — теорія графів та її застосування.