3. Красненко, С. С. Многоканальный цифровой синтез в имитаторах радионавигационных сигналов // Журнал Сибирского федерального университета. Серия «Техника и технологии». 2013. Т. 6, № 5. С. 521–526.

4. Красненко С. С., Пичкалев А. В. Способы формирования сигналов в радионавигационных имитаторах // Навигационные спутниковые системы, их роль и значение в жизни современного человека: Тезисы доклада 2-й Междунар. науч.-техн. конф., посвященной 30-летию запуска на орбиту первого навигационного космического аппарата «Глонасс» / под общ. ред. Н. А. Тестоедова ; ОАО «Информационные спутниковые системы» ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2012. С. 75–77.

5. Красненко С. С., Пичкалев А. В. Имитатор радионавигационных сигналов в модульном исполнении // Решетневские чтения : матер. XIV Междунар. науч. конф. Красноярск, 2010. Ч. 1. С. 154–155.

6. Красненко С. С., Недорезов Д. А. Практическое применение модульных приборов компании National Instruments при разработке имитаторов радионавигационных сигналов // Интеллект и наука : тр. XII Междунар. науч. конф. Железногорск, 2012. С. 43–44.

References

1. Zubavichus V. A., Balabanov A. Z., Komarov V. A., Marareskul D. I., Furmanov V. V., Cvetkova O. I., Udin V. A., Ankudinov A. V. *Dvukhsistemnyy navigatsionnyy priyemnik kosmicheskogo apparata* [Two-system navigation receiver spacecraft]. Patent RF no. 112401, MPK G01C21/24.

2. Nepomnyashcy O. V., Shaidurov V. V., Veisov E. A. *Vestnik SibGAU*. 2013, № 2 (48), p. 133–136.

3. Krasnenko S. S, Nedorezov D. A., Kashkin V. B., Hazagarov U. G., Pichkalev A. V. *Zurnal Sibirskogo Federalnogo Universiteta, seria “Tehnaka I Tehnologia”* (Siberian Federal University. Engineering & Technologies). 2013, vol. 6, no. 5, p. 521–526.

4. Krasnenko S. S., Pichkalev A. V. [Ways of signal formation in radionavigating simulators]. *Tezisu doklada II Mezhdunarodnoy nauchno-tehnicheskoi konferentsii posvachennoi 30-letiu zapuska na orbity pervogo navigacionnogo kosmicheskogo apparata “Glonnas”; “Navigacionnue sputnikovue sistemu, ih rol i znachenie v zhizni sovremennogo cheloveka”* [Theses of the report 2nd International Scientific and Technical Conference devoted to the 30th anniversary of launching the into orbit of the first navigation of the spacecraft “Glonass”; “Navigation satellite systems, their role and importance in the life of modern man”]. Krasnoyrsk, 2012, 75 p. (In Russian).

5. Krasnenko S. S., Pichkalev A. V. *Materialy XIV Mezhdunarodnoy nauchnoy konferentsii “Reshetnevskie chteniya”* [Materials of the XIV Intern. scientific. conf. “Reshetnev reading”], Krasnoyrsk, 2010, 154 p. (In Russian).

6. Krasnenko S. S, Nedorezov D. A. *Trydy XII Mezhdunarodnoy nauchnoy konferentsii “Intelekt i nayka”* [Proceedings of the XII Intern. scientific. conf. “Intelligence and science”], Zheleznogorsk 2012, 43 p. (In Russian).

© Красненко С. С., Пичкалев А. В., Недорезов Д. А., Лапин А. Ю., Непомнящий О. В., 2014

УДК 519.6

ПАРАЛЛЕЛЬНЫЙ АЛГОРИТМ ДЛЯ ИССЛЕДОВАНИЯ ГРАФОВ КЭЛИ ГРУПП ПОДСТАНОВОК*

А. А. Кузнецов, А. С. Кузнецова

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660014, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: kuznetsov@sibsau.ru

Представлен алгоритм для вычисления диаметра, среднего диаметра и функции роста графа Кэли конечной группы, заданной фиксированным множеством порождающих элементов. Доказана его корректность. На основе данного алгоритма предложена его параллельная версия для исследования графов Кэли групп подстановок. Созданный алгоритм может быть полезен при проектировании топологии многопроцессорной вычислительной системы (МВС). В этом случае модель МВС будет представлена в виде графа Кэли, в котором процессоры являются вершинами графа, а ребра соответствуют физическим соединениям между процессорами. Применение указанного алгоритма позволяет изучить характеристики рассматриваемого графа, что, в свою очередь, дает возможность оценить производительность МВС.

Ключевые слова: граф Кэли, многопроцессорная вычислительная система.

* Работа выполнена при поддержке Министерства образования и науки РФ (проект Б 112/14).

A PARALLEL ALGORITHM FOR STUDY OF THE CAYLEY GRAPHS OF PERMUTATION GROUPS

A. A. Kuznetsov, A. S. Kuznetsova

Siberian State Aerospace University named after academician M. F. Reshetnev
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660014, Russian Federation
E-mail: kuznetsov@sibsau.ru

An algorithm for computing the diameter, the average diameter and the growth function of the Cayley graph of a finite group given a fixed set of generators is presented. The correctness of the algorithm is proved. After that a parallel version of the algorithm for study of the Cayley graphs of permutation groups is presented. This algorithm can be useful in the design of the topology of a multiprocessor computing system (MCS). In this case the model of MCS will be presented as the Cayley graph in which the processors are the vertices of the graph and the edges correspond to physical connections between processors. Using of this algorithm allows us to study the characteristics of the Cayley graph to evaluate the performance of MCS.

Keywords: the Cayley graph, a multiprocessor computing system.

Определение графа Кэли было дано известным английским математиком Артуром Кэли в 1878 г. для представления алгебраической группы, заданной фиксированным множеством порождающих элементов.

В последние десятилетия теория графов Кэли развивается как отдельная большая ветвь теории графов. Графы Кэли находят применение как в математике, так и за ее пределами. Заметим, что известная задача по определению так называемого числа Бога кубика Рубика 3×3×3, т. е. минимального количества поворотов граней кубика, за которое его можно собрать из любого начального положения, сводится к исследованию соответствующего графа Кэли [1].

Неожиданное применение графы Кэли нашли в информационных технологиях после пионерской работы 1986 г. С. Эйкерса и Б. Кришнамурти [2], которые впервые предложили применять указанные графы для представления компьютерных сетей, в том числе для моделирования топологий многопроцессорных вычислительных систем (МВС) – суперкомпьютеров. С тех пор данное направление активно развивается. Это связано с тем, что графы Кэли имеют много привлекательных свойств, из которых выделим их регулярность, вершинно-транзитивность, малые диаметр и степень при достаточно большом количестве вершин в графе. Кстати, такие базовые топологии сети, как «кольцо» и «гиперкуб», являются графами Кэли. Среди множества работ отдельно стоит отметить статью С. Шайбелла и Р. Стаффорда 1992 г. [3], в которой показано, что наряду с диаметром графа Кэли очень важное значение для производительности МВС имеет также средний диаметр графа.

Для вычисления диаметра графа требуется решить ряд задач дискретной оптимизации. В первую очередь необходимо найти кратчайшие пути, связывающие все пары вершин в графе. Затем из всех кратчайших путей выбрать наибольший путь, длина которого и будет являться диаметром графа. Соответственно, средний диаметр графа будет равен среднему арифметическому всех длин кратчайших путей.

Как известно, если граф задан в виде матрицы длин ребер, то задача по вычислению диаметра графа решается алгоритмом полиномиальной сложности. Специфика же графов Кэли такова, что в исходной ситуации известны только порождающие элементы и определяющие соотношения группы.

Чтобы вычислить диаметр графа Кэли, необходимо решить следующие задачи дискретной оптимизации. Сначала требуется найти для каждого элемента группы минимальное слово, т. е. представить элемент в виде комбинации из образующих наименьшей длины, после чего вычислить максимальную длину минимальных слов, которая и будет являться диаметром графа Кэли.

Поиск минимального слова в большой конечной группе является хотя и разрешимой, но достаточно сложной проблемой. Это связано с тем, что в общем случае задача по определению минимального слова в группе, а следовательно, и диаметра графа Кэли, как показали С. Ивен и О. Голдрейх в 1981 г., является NP-трудной [4]. Поэтому для эффективного решения задач оптимизации на графах Кэли, имеющих большое количество вершин, необходимо применять МВС. В связи с этим представляется актуальной проблема разработки параллельных алгоритмов для исследования графов Кэли частных классов групп.

Основные определения и понятия

Определение 1. Положим G – конечная группа и $X \subset G$. Множество $X = \{x_1, x_2, ..., x_m\}$ называют *порождающим множеством группы*, а его элементы – *порождающими* и записывают $G = \langle X \rangle$, если любой элемент из G можно представить в виде конечного произведения из порождающих:

$$G = \langle X \rangle \Rightarrow \forall g \in G \Rightarrow g = \alpha_1 \cdot \alpha_2 \cdot ... \cdot \alpha_s, \text{ где } \alpha_i \in X.$$

Порождающее множество X называют также *алфавитом*, а порождающие элементы x_i – *буквами*.

Определение 2. Пусть g элемент из G и $g = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_s$, где $\alpha_i \in X$. Правую часть данного выражения мы будем называть *словом* и записывать $\alpha_1\alpha_2\ldots\alpha_s$. Множество всех слов над алфавитом X будем обозначать X^*.

Если необходимо подчеркнуть, что слово $v \in X^*$ соответствует элементу $g \in G$, то следует писать: v_g. Очевидно, что фиксированное слово v соответствует только лишь одному элементу группы.

Определение 3. Если два различных слова $v = \alpha_1\alpha_2\ldots\alpha_r$ и $w = \beta_1\beta_2\ldots\beta_s$ представляют один элемент g группы G, т. е. $g = \alpha_1\alpha_2\ldots\alpha_r$ и $g = \beta_1\beta_2\ldots\beta_s$, то выражение $\alpha_1\alpha_2\ldots\alpha_r = \beta_1\beta_2\ldots\beta_s$ *(*или $v_g = w_g$*)* называют *соотношением в G*.

Определение 4. Положим v произвольное слово из X^*. Количество букв, входящее в v, будем называть *длиной слова* v и обозначать $\mathrm{length}(v)$.

Единица группы e будет представлена пустым словом, которое мы также обозначим e. По определению $\mathrm{length}(e) = 0$.

На множестве порождающих введем отношение порядка «$\prec$»:

$$\{x_1 \prec x_2 \prec \ldots \prec x_m\}.$$

Определение 5. Пусть v и w произвольные слова из X^*. Будем говорить, что слово $v = \alpha_1\alpha_2\ldots\alpha_r$ *меньше слова* $w = \beta_1\beta_2\ldots\beta_s$ и записывать $v \prec w$, если имеет место одно из следующих утверждений:

1) $r < s$;

2) если $r = s$, тогда $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, ..., $\alpha_{k-1} = \beta_{k-1}$, $\alpha_k \prec \beta_k$ для некоторого $1 \le k \le s$.

Данный способ упорядочивания элементов называют также *лексикографическим*.

Определение 6. Слово v будем называть *минимальным в G относительно введенного порядка*, если для любого другого слова w, удовлетворяющего условию $v_g = w_g$, будет выполняться $v \prec w$.

Определение 7. *Длиной* length(g, X) элемента g в алфавите X будем называть длину минимального слова $v_g \in X^*$, представляющего данный элемент, т. е.

$$\mathrm{length}(g, X) \ = \ \min\{\mathrm{length}(v_g) \mid v_g \in X\}.$$

Определение 8. *Диаметром* diam(G, X) группы G относительно порождающего множества X будем называть максимальную длину элементов данной группы. Другими словами:

$$\mathrm{diam}(G, X) = \max\{\mathrm{length}(g, X) \mid g \in G\},$$

или

$$\mathrm{diam}(G, X) = \max\{\min\{\mathrm{length}(v_g) \mid v_g \in X^*\} \mid g \in G\}.$$

Определение 9. Пусть $G = \langle X \rangle$. *Шаром* $K_r(G, X)$ *радиуса* r группы G относительно X будем называть множество

$$K_r(G, X) = \{ g \in G \mid \mathrm{length}(g, X) \le r\}.$$

Таким образом, шар $K_r(G, X)$ радиуса r представляет собой все элементы группы G, длины которых относительно порождающего множества X не превышают r.

Определение 10. *Функция роста* $\mathrm{growth}(G, X, r)$ группы $G = \langle X \rangle$ от аргумента $r \in \{0\} \bigcup \mathbb{N}$ задается соотношением $\mathrm{growth}(G, X, 0) = 1$ и $\mathrm{growth}(G, x, r) = = |K_r(G, X)| - |K_{r-1}(G, X)|$ при $r \in \mathbb{N}$.

Это означает, что каждое значение функции роста $\mathrm{growth}(G, X, r)$ равно числу элементов группы $G = \langle X \rangle$ фиксированной длины r.

Определение 11. *Средним диаметром* $\overline{\mathrm{diam}}(G, X)$ конечной группы G будем называть среднюю длину ее элементов в алфавите X. Другими словами:

$$\overline{\mathrm{diam}}(G, X) = \frac{\sum_{g \in G} \mathrm{lenght}(g, X)}{|G|} = = \frac{\sum_{r=0}^{\mathrm{diam}(G,X)} \mathrm{growth}(G, X, r) \cdot r}{|G|}.$$

Определение 12. *Графом* $\Gamma = (V, E)$ называют совокупность двух множеств – множества вершин $V = \{v_1, v_2, \ldots, v_m\}$ и множества ребер $E = \{e_1, e_2, \ldots, e_n\}$, где каждое ребро из E определяется неупорядоченной парой вершин $\{v_i, v_g\}$.

Отметим, что приведенная выше формулировка определяет *неориентированный* граф. Если же каждое ребро графа задается упорядоченной парой (v_i, v_g) вершин, то такой граф называют *ориентированным*.

Далее под графом будем понимать неориентированный граф. Пусть v_1 и v_2 – вершины графа, e_1 – соединяющее их ребро. Тогда вершина v_1 и ребро e_1 *инцидентны*, ребро e_1 и вершина v_2 также инцидентны. Два ребра, инцидентные одной вершине, называются *смежными*; две вершины, инцидентные одному ребру, также называются *смежными*.

Степенью вершины называют число инцидентных ей ребер. Граф называют *регулярным степени k*, если каждая его вершина имеет степень k.

Порядок графа определяется числом его вершин $|V|$.

Определение 13. *Автоморфизмом графа* $\Gamma = (V, E)$ называется отображение φ множества вершин на себя, сохраняющее смежность, т. е. если $\{u, v\} \in E$, то будет верно $\{\varphi(u), \varphi(v)\} \in E$.

Определение 14. Граф $\Gamma = (V, E)$ называют *вершинно-транзитивным*, если для любых двух вершин $u, v \in V$ существует автоморфизм φ, при котором $\varphi(u) = v$.

Определение 15. *Маршрутом в графе* $\Gamma = (V, E)$ называют последовательность вершин и ребер из Γ

$$v_{i_1}, e_{i_1}, v_{i_2}, e_{i_2}, \ldots, e_{i_p}, v_{i_{p+1}},$$

в которой любые два соседних элемента инцидентны, причем однородные элементы (вершины, ребра) через один смежны или совпадают. Число ребер маршрута p называют его *длиной.* Если все ребра различны, то маршрут называют *цепью.*

Граф является *связным*, если между любыми его двумя вершинами существует маршрут.

Определение 16. *Расстоянием* $d(u,v)$ *между вершинами* u и v в графе Γ будем называть длину кратчайшей цепи, связывающей эти две вершины.

Определение 17. *Диаметром* diam(Γ) графа Γ называется расстояние между двумя наиболее удаленными вершинами в графе, т. е.

$$\mathrm{diam}(\Gamma) = \max\{d(u,v) \mid u,v \in V\}. \tag{1}$$

Определение 18. *Средним диаметром* $\overline{\mathrm{diam}}(\Gamma)$ конечного непустого графа $\Gamma = (V,E)$ будем называть среднее расстояние между его вершинами. Другими словами:

$$\overline{\mathrm{diam}}(\Gamma) = \frac{\sum_{u,v\in V} d(u,v)}{|V|^2}. \tag{2}$$

Определение 19. Пусть X – порождающее множество группы G, т. е. $G = \langle X \rangle$. *Графом Кэли* $\Gamma = Cay(G,X) = (V,E)$ называют ориентированный граф, обладающий следующими свойствами:

1) множество вершин V(Γ) соответствуют элементам группы G;

2) множество ребер E(Γ) состоит из всех упорядоченных пар (g, xg), где $g \in G$ и $x \in X$.

В дальнейшем будем считать порождающее множество X симметричным и свободным от единичного элемента группы, т. е. $x \in X \Rightarrow x^{-1} \in X$ и $e \notin X$. Поскольку X является свободным от единичного элемента, то граф Γ не содержит петель. Симметричность порождающего множества означает, что граф будет неориентированным и без кратных ребер, т. е. если в графе имеется ребро из g в xg, то оно совпадает с ребром из xg в $x^{-1}(xg) = g$.

Таким образом,

$\Gamma = Cay(G,X) = (V,E)$, где $V = G$ и

$$E = \{\{g, xg\} \mid g \in G, x \in X\}.$$

Последовательный алгоритм A-I

В настоящем разделе будет представлен базовый алгоритм A-I для вычисления характеристик графа Кэли конечной группы, заданной фиксированным порождающим множеством.

Для обоснования корректности алгоритма A-I докажем сначала вспомогательные утверждения.

Лемма 1. Пусть $G = \langle X \rangle$ и $\Gamma = Cay(G,X)$ – граф Кэли группы G относительно X. Тогда

(i) Γ является связным |X|-регулярным графом;

(ii) Γ является вершинно-транзитивным графом;

(iii) $\forall g,h \in G \ \ d(g,h) = \mathrm{length}(hg^{-1}, X)$;

(iv) $\mathrm{diam}(\Gamma) = \mathrm{diam}(G,X)$;

(v) $\overline{\mathrm{diam}}(\Gamma) = \overline{\mathrm{diam}}(G,X)$.

Доказательство. (i) Так как X является порождающим множеством группы G, то граф Γ является связным, а в связи с тем, что X – симметричное порождающее множество, то каждая вершина в Γ имеет степень, равную |X|. Поэтому Γ является связным |X|-регулярным графом.

(ii) Если u и v две произвольные смежные вершины в Γ, то $v = xu$ для некоторого $x \in X$. Отсюда следует, что для смежных вершин всегда найдется такой элемент $x \in X$, что $vu^{-1} = x$. Обратно, если u и v не являются смежными, то $vu^{-1} \notin X$.

На множестве вершин из Γ рассмотрим отображение φ_h такое, что $\varphi_h(g) = gh$. Докажем, что φ_h сохраняет смежность, т. е. если u и v две смежные вершины, то $\varphi_h(u)$ и $\varphi_h(v)$ также будут являться смежными. Действительно,

$$\varphi_h(v)\varphi_h(u)^{-1} = vh(uh)^{-1} = vhh^{-1}u^{-1} = vu^{-1} \in X.$$

Если же u и v не являются смежными, то будет выполняться $\varphi_h(v)\varphi_h(u)^{-1} \notin X$, поэтому вершины $\varphi_h(u)$ и $\varphi_h(v)$ также не будут являться смежными. Так как отображение φ_h сохраняет смежность, то оно будет являться автоморфизмом графа Γ.

Положим $h = u^{-1}v$. Тогда $\varphi_h(u) = \varphi_{u^{-1}v}(u) = uu^{-1}v = v$. Следовательно, Γ является вершинно-транзитивным графом.

(iii) Пусть g и h – произвольные вершины в Γ. Согласно (i) данный граф является связным, а значит, существует путь, связывающий эти вершины. Предположим, что кратчайший путь имеет следующий вид: g, $\alpha_1 g$, $\alpha_2\alpha_1 g$, …, $\alpha_s \ldots \alpha_2\alpha_1 g$ $(\alpha_i \in X)$, т. е. $d(g, h) = s$. С другой стороны, $\alpha_s \ldots \alpha_2\alpha_1 = hg^{-1}$, следовательно, $\mathrm{length}(hg^{-1}, X) = s$. Таким образом, между длинами элементов группы G и кратчайшими цепями в графе Γ имеется взаимно однозначное соответствие, в частности, имеет место равенство

$$\forall g,h \in G \Rightarrow d(g,h) = \mathrm{length}(hg^{-1}, X). \tag{3}$$

(iv) Запишем формулу (1) с учетом (3):

$$\mathrm{diam}(\Gamma) = \max\{d(g,h) \mid g,h \in G\} =$$
$$= \max\{\mathrm{length}(hg^{-1}, X) \mid hg^{-1} \in G\} = \mathrm{diam}(G,X).$$

(v) Согласно (ii) граф Кэли является вершинно-транзитивным, и для любых двух его вершин u и v будет выполняться

$$\sum_{v\in V} d(u,v) = \sum_{u\in V} d(u,v). \tag{4}$$

С учетом (4) перепишем формулу (2):

$$\overline{\mathrm{diam}}(\Gamma) = \frac{\sum_{u,v\in V} d(u,v)}{|V|^2} = \frac{|V|\sum_{v\in V} d(u,v)}{|V|^2} = \frac{\sum_{v\in V} d(u,v)}{|V|}.$$

Пусть $u = e$ – единица G. Поскольку $V = G$, а также в силу (3), получим

$$\overline{\operatorname{diam}}(\Gamma)=\frac{\sum_{v\in V} d(e,v)}{|V|}=\frac{\sum_{g\in G}\operatorname{length}(g,X)}{|G|}=\overline{\operatorname{diam}}(G,X).$$

Беря во внимание свойства (*ii*) и (*iii*) вышеприведенной леммы, мы можем определить функцию роста графа Кэли $\operatorname{growth}(\Gamma,r)=\operatorname{growth}(G,X,r)$, которая задает количество вершин в графе, удаленных от любой заданной вершины на расстояние *r*.

Ниже представлен последовательный алгоритм для исследования графов Кэли конечных групп. Данный алгоритм можно распараллелить для эффективной реализации на МВС.

Вход: G = (G, ·) – конечная группа и $X=\{x_1 \prec x_2 \prec \ldots \prec x_m\}$ – упорядоченное порождающее множество *G*.

Выход: диаметр $\operatorname{diam}(\Gamma)$, средний диаметр $\overline{\operatorname{diam}}(\Gamma)$ графа Кэли $\Gamma=Cay(G,X)$, а также функция роста графа $\operatorname{growth}(r)=\operatorname{growth}(\Gamma,r)$, $0\le r\le \operatorname{diam}(\Gamma)$.

1. $s=0$, $K_s=K_s(G,X)=\{e\}$ – шар группы *G*, $T=K_s$.
2. $s=s+1$, $K_s=K_{s-1}$, $U=x_1\cdot T\cup x_2\cdot T\ldots\cup x_m\cdot T$ – лексикографически упорядоченное множество.
3. $T=\varnothing$, $i=1$.
4. Если $u_i\notin K_s$, то $K_s=K_s\cup u_i$, $T=T\cup u_i$.
5. Если $\begin{cases} i<|V|, \text{ то } i=i+1, \text{ переход в пункт 4;}\\ i=|V|, \text{ то переход в пункт 6.}\end{cases}$
6. Если $\begin{cases} T\ne\varnothing, \text{ то переход в пункт 2;}\\ T=\varnothing, \text{ то переход в пункт 7.}\end{cases}$
7. $\operatorname{diam}(\Gamma)=s-1$, $\operatorname{growth}(r)=|K_r|-|K_{r-1}|$ для $1\le r\le s-1$ и $\operatorname{growth}(0)=1$, $\overline{\operatorname{diam}}(\Gamma)=\dfrac{\sum_{r=0}^{s-1}\operatorname{growth}(r)\cdot r}{|K_{s-1}|}$.

Возврат полученных значений.

Теорема. Алгоритм А-I корректен, т. е. для любой конечной группы он за конечное число шагов находит характеристики соответствующего графа Кэли.

Доказательство. По построению А-I выражает каждый элемент группы *G* в виде уникального минимального слова. После каждого прохода от пункта 2 до пункта 6 множество K_s будет представлять собой шар радиуса *s* группы *G* в алфавите *X*. Поскольку количество элементов группы конечно, то через конечное число шагов все $g\in G$ будут записаны в формате минимальных слов, длины которых меньше *s*:

$$\forall g\in G\Rightarrow \exists! u_g\in K_{s-1}\Rightarrow \forall v_g\notin K_{s-1}\Rightarrow u_g\prec v_g.$$

Это означает, что $\operatorname{diam}(G,X)=s-1$ и K_{s-1} однозначно определяет функцию роста группы *G* в алфавите *X*. Как было сказано, $\operatorname{growth}(\Gamma,r)=\operatorname{growth}(G,X,r)$. По лемме 1 диаметр и средний диаметр графа Кэли Γ группы $G=\langle X\rangle$ равны соответствующим характеристикам *G*. Теорема доказана.

Параллельная версия алгоритма А-I для графов групп подстановок

Для увеличения скорости вычислений алгоритм А-I можно распараллелить следующим образом. Множество $K_s(S_n, X_n)$ разбивается на $m=n(n-1)(n-2)\ldots(n-k+1)$ непересекающихся классов элементов (подстановок):

$$K_s=\bigcup_{i=1}^{m}K_i,\ K_i\cap K_j=\varnothing \text{ при } i\ne j.$$

Каждый класс K_i будет однозначно определяться фиксированным набором значений $(i_1,i_2,\ \ldots,i_k)$, т. е.

$$\forall g\in K_i\Rightarrow g=\begin{pmatrix}1\,2\ldots k\ldots n\\ i_1\,i_2\ldots i_k\ldots i_n\end{pmatrix}.$$

Аналогичным образом массив *U* при каждом *s* также делится на *m* непересекающихся классов элементов:

$$U=\bigcup_{i=1}^{m}U_i,\ U_i\cap U_j=\varnothing \text{ при } i\ne j,$$

и дальнейшая обработка данных для каждой пары множеств U_i и K_i (пункты 4–5 алгоритма А-I) производится независимо.

Нетрудно заметить, что рассмотренное разделение массивов не влияет на корректность работы алгоритма.

Параметр *k* определяется экспериментально и зависит от строения группы, а также от характеристик МВС.

Таким образом, представленный выше параллельный алгоритм, как показали вычисления на МВС [5], дает существенный прирост скорости вычислений.

В будущем на основе данного алгоритма планируется провести серию экспериментов по исследованию графов Кэли различных классов групп с целью поиска перспективных топологий для МВС.

Библиографические ссылки

1. Holt D., Eick B., O'Brien E. Handbook of computational group theory. Boca Raton : Chapman & Hall/CRC Press, 2005. 514 p.
2. Akers S., Krishnamurthy B. A group theoretic model for symmetric interconnection networks // Proceedings of the International Conference on Parallel Processing, 1986. P. 216–223.
3. Schibell S., Stafford R. Processor interconnection networks and Cayley graphs // Discrete Applied Mathematics. 1992. Vol. 40. P. 337–357.
4. Even S., Goldreich O. The Minimum Length Generator Sequence is NP-Hard // J. of Algorithms. 1981. Vol. 2. P. 11–313.
5. Кузнецов А. А., Кузнецова А. С. О взаимосвязи функций роста в симметрических группах с задачами комбинаторной оптимизации // Вестник СибГАУ. 2012. № 6 (46). С. 93–97.

References

1. Holt D., Eick B., O'Brien E. Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.

2. Akers S., Krishnamurthy B. A group theoretic model for symmetric interconnection networks. Proceedings of the International Conference on Parallel Processing, 1986. P. 216–223.

3. Schibell S., Stafford R. Processor interconnection networks and Cayley graphs. Discrete Applied Mathematics. 1992. Vol. 40. P. 337–357.

4. Even S., Goldreich O. The Minimum Length Generator Sequence is NP-Hard. Journal of Algorithms. 1981. Vol. 2. P. 311–313.

5. Kuznetsov A. A., Kuznetsova A. S. [Relation between growth functions in symmetric groups and tasks of combinatorial optimization]. *Vestnik SibGAU*, 2012, no. 6 (46), p. 93–97.

© Кузнецов А. А., Кузнецова А. С., 2014

УДК 519.7

НЕПАРАМЕТРИЧЕСКАЯ ОЦЕНКА КРИВОЙ РЕГРЕССИИ В УСЛОВИЯХ БОЛЬШИХ ВЫБОРОК*

А. В. Лапко[1, 2], В. А. Лапко[1, 2], Д. В. Борисов[1]

[1]Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660014, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: valapko@yandex.ru
[2]Институт вычислительного моделирования СО РАН
Российская Федерация, 660036, г. Красноярск, Академгородок, 50, стр. 44. E-mail: lapko@icm.krasn.ru

Предлагается методика построения непараметрической регрессии в условиях обучающих выборок большого объема. Синтез модели основывается на декомпозиции исходных статистических данных и анализе вероятностных характеристик получаемых множеств случайных величин. Исследуются асимптотические свойства непараметрической регрессии и рассматриваются результаты вычислительного эксперимента. Устанавливается зависимость свойств непараметрической регрессии от количества интервалов дискретизации значений случайной величины и объёма исходных данных. Проводится сравнение аппроксимационных свойств предлагаемой модели и традиционной непараметрической регрессии. Результаты исследований имеют важное значение при решении задач доверительного оценивания плотности вероятности и кривой регрессии.

Ключевые слова: непараметрическая регрессия, плотность вероятности, регрессионная оценка, аппроксимационные свойства, методы дискретизации.

NONPARAMETRIC ESTIMATION OF REGRESSION CURVES IN THE CONDITIONS OF LARGE SAMPLES*

A. V. Lapko[1, 2], V. A. Lapko[1, 2], D. V. Borisov[1]

[1]Siberian State Aerospace University named after academician M. F. Reshetnev
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660014, Russian Federation
E-mail: valapko@yandex.ru
[2]Institute of Computational Modeling, Siberian Branch of RAS
50, Akademgorodok, Krasnoyarsk, 660036, Russian Federation
E-mail: lapko@icm.krasn.ru

The technique of construction of a nonparametric regression in the conditions of training samples of large volume is offered. Model synthesis is based on decomposition of initial statistical data and the analysis of probabilistic characteristics of received random variables sets. Asymptotic properties of a nonparametric regression are investigated and results of computing experiment are considered. Association of nonparametric regression properties on an amount of sampling intervals of values of an random variable and volume of input datas is established. Comparison of approximating properties of offered model and a traditional nonparametric regression is spent. The results of researches are important to the solution of problems of a confidential estimation of a probability density and a regression curves.

Keywords: nonparametric regression, probability density, regression estimations, approximating properties, sampling methods.

* Работа выполнена в рамках базовой части государственного задания Минобрнауки РФ (СибГАУ № Б121/14).