МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Укладки графов

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Далабаева Адилбека Насроллаевича

Научный руководитель
Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2020 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2020 г.

Саратов 2020

ВВЕДЕНИЕ

Планарность графа является очень важным его свойством. На планарных графах, с одной стороны, были найдены более эффективные решения многих задач, таких как раскраски графов, максимальный поток или проверка на изоморфизм. С другой стороны, планарные графы могут быть использованы в криптографии, где в качестве характеристики, на которой основано построение шифров, выступают грани укладки графа на плоскости.

Укладки графов на поверхности являются логичным расширением понятия планарности. Появляется возможность перенести некоторые наработки на графы, укладывающиеся на поверхности ограниченного рода. Однако укладки графов еще недостаточно изучены, а потому многие современные достижения в данной области имеют чисто теоретическую ценность, либо же направлены на определение укладок некоторых специфических графов, таких как граф Грея или граф Дойла-Холта.

Фактически, определение укладываемости произвольного графа даже совсем небольшого размера на заданную поверхность уже является трудно вычислимой задачей. Поэтому целью работы является разработка алгоритма и реализация программы, определяющей поверхность минимального рода, на которую можно уложить заданный граф для графов до девяти вершин. Стоит отметить, что уже для девяти вершинных графов наблюдается недостаток информации в публичном доступе, а именно, известно только количество планарных графов. А потому, любое продвижение в данном направлении уже будет полезным и актуальным.

В работе будут определены необходимые свойства поверхности и свойства укладок. Далее будет предложен базовый алгоритм решения поставленной задачи. Будут представлены различные асимптотические и константные оптимизации, которые позволяют ускорить базовое решение. С другой стороны, будут реализованы дополнительные алгоритмы, позволяющие быстрее

определять графы специального вида, такие как графы рода 0 (планарные) и рода 1.

Результатом работы является программа, реализующая построенный алгоритм. В ходе работы также был получен каталог графов с соответствующим каждому графу родом, а в текст включен каталог графов из 8 вершин рода 2. Данные каталоги можно будет использовать в дальнейшем в каких-либо других задачах.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 9 приложений. Общий объем работы – 80 страниц, из них 48 страниц – основное содержание, включая 14 рисунков и 2 таблицы, список использованных источников из 27 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

1 Общая информация

1.1 Поверхности и их свойства

Назовем *поверхностью* фигуру, у которой каждая точка x имеет окрестность, гомеоморфную кругу. Далее в работе будут рассматриваться только ориентируемые поверхности.

Родом поверхности назовем наибольшее число непересекающихся простых замкнутых кривых, которые можно провести на поверхности, не разделяя ее на части. Далее будем обозначать поверхность рода n через S_n.

1.2 Укладка графа на поверхности

Граф *укладывается* на поверхности S, если его можно изобразить на ней так, чтобы никакие два ребра в этом изображении не пересекались. Части, на которые разбивается поверхность, (*грани*) должны быть гомеоморфны открытому плоскому диску.

Род графа $\gamma(G)$ – это наименьшее число g такое, что существует укладка графа G на поверхность S_g.

Комбинаторное вложение кодирует вложение графа в поверхность, описывая его через циклический порядок ребер у каждой вершины. Каждое комбинаторное вложение однозначно определяет вложение графа в поверхность.

Теорема (Расширенная формула Эйлера). Пусть $G = (V, E)$ – связный граф с вложением в S_g, а F – множество его граней, тогда

$$|V| - |E| + |F| = 2 - 2g. \quad (1)$$

1.3 Подграфы K_8

Теорема: для любого подграфа $G \subseteq K_8$:

1) $\gamma(G) = 0$, если G не содержит K_5 или $K_{3,3}$;

2) $\gamma(G) = 1$, если G содержит K_5 или $K_{3,3}$, но не содержит $B_1 = K_8 - K_3$, $B_2 = K_8 - (K_2 \cup K_2 \cup P_3)$ или $B_3 = K_8 - K_{2,3}$;

3) $\gamma(G) = 2$, если G содержит B_1, B_2 или B_3.

2 Построение алгоритма

2.1 Вид графов

Можно ограничиться рассмотрением только связных неизоморфных графов, которые будут разбиваться на компоненты двусвязности.

2.2 Выделение компонент двусвязности

Воспользуемся однопроходным алгоритмом выделения компонент двусвязности из [10]. Одно ребро так же является компонентой двусвязности.

2.3 Проверка графа на планарность

Используем алгоритм Демукрона, представленный в [17]. Данный алгоритм позволяет строить укладку графа на плоскость с заданными гранями. Данный алгоритм реализован с асимптотикой порядка $O(|V|^3)$.

2.4 Проверка графа на тороидальность

2.4.1 Базис циклов минимальной суммарной длины

Базис циклов графа G определяется как базис пространства циклов графа G. Существует жадный алгоритм нахождения базиса минимальной суммарной длины.

Хортон, в [21], доказал, что все базисные циклы имеют вид: для каждой вершины x и для каждого ребра $\{y, z\}$ рассмотрим цикл $P(x, y) \cup P(x, z) \cup \{y, z\}$, где $P(x, y)$ – кратчайший путь между вершинами x и y.

2.4.2 Нахождение двух вершинно-непересекающихся путей

Для заданного связного графа G и двух его подмножеств вершин S и T, таких что $|S|, |T| \geq 2$ и $S \cap T = \emptyset$, найти два независимых по вершинам пути из S в T можно с помощью метода потоков, для которого строится определенная сеть.

2.4.3 Основной алгоритм проверки на тороидальность

Алгоритм был представлен в [23]. Алгоритм в своем составе использует алгоритмы из подраздела 2.3 и пунктов 2.4.1 и 2.4.2. Суммарная сложность алгоритма равна $O\left(|V|^3 + |V|2^r(|V|^2 + |V|^3)\right) = O(|V|^4 2^r)$, где r – это максимальное количество ребер в базисном цикле.

2.5 Алгоритм перебора

Для определения рода графа в общем случае будет использоваться алгоритм перебора комбинаторного вложения, который представляет из себя процедуру рекурсивного перебора с отсечениями.

2.6 Возможные оптимизации и отсечения

2.6.1 Нахождение оптимальной стартовой вершины

Рассмотрим первую вершину v. Назовем смежные ей вершины $u_1, u_2, \dots, u_{d(v)}$. Скажем, что u_x и u_y эквивалентны, если их списки смежности совпадают, тогда вершины можно разбить на классы C_i. Вершину v необходимо выбирать с наибольшим значением $|C_1|!\,|C_2|!\,\dots\,|C_l|!$.

2.6.2 Выбор оптимального порядка для последней вершины

Для последней вершины w можно определить циклический порядок, при котором количество полученных граней максимально без перебора всех возможных вариантов.

2.6.3 Оценка рода графа снизу

Из формулы (1) получим оценку на род поверхности $g \geq \left\lceil 1 - \frac{|V|}{2} + \frac{|E|}{6} \right\rceil$.

За оценку снизу можно взять максимум по всем подграфам, отличающимся от заданного отсутствием одного ребра, или же $\gamma_{lower} = \max\limits_{H \subset G} \gamma(H)$.

2.6.4 Оценка рода графа сверху

Согласно [11], определено точное значение рода полного графа K_n:

$$\gamma(K_n) = \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil. \quad (7)$$

2.6.5 Отсечение из-за недостатка граней

Данное отсечение требует ситуации $\gamma_{lower} + 1 = \gamma_{upper}$. Для отсечения веток перебора будем на каждом шаге оценивать максимально возможное количество граней, учитывая только зафиксированные циклические порядки.

2.7 Финальный вид

Алгоритм состоит из 6 основных этапов: выделение компонент двусвязности; подсчет для каждой компоненты оценки γ_{lower} и γ_{upper}; проверка на планарность; проверка на тороидальность; запуск перебора с отсечениями; определение суммарного рода и сохранение для дальнейшего использования.

3 Запуск программы и результаты работы

3.1 Особенности реализации

Программа представляет из себя консольное приложение, реализованное на языке C++. Программа состоит из нескольких классов, каждый описан в своем header-файле, листинг которых представлен в соответствующих приложениях.

3.2 Анализ полученных данных

Программа была запущена для коллекций графов из n вершин для $n \leq 9$. Данные для 9 вершин не были получены в полном объеме: для графов рода не менее 2 было проведено отдельное тестирование. Основные данные сведены в таблицу 1. Данные проверки графов рода не менее 2 представлены в таблице 2.

3.3 Иллюстрации некоторых графов

В данном разделе приведены укладки некоторых графов, таких как K_4, K_5, K_6, K_7, $K_{3,3}$ и некоторые другие. Также в приложении Л представлены все 15 неизоморфных графов из 8 вершин рода 2.

ЗАКЛЮЧЕНИЕ

В ходе работы был разработан алгоритм определения рода графа для всех связных графов с заданным количеством вершин. Были разработаны и реализованы различные методы его оптимизации: асимптотические и константные. Была написана и протестирована программа, реализующая заданный алгоритм. Программа быстро обрабатывает графы до 8 вершин включительно, однако все еще недостаточно, чтобы обработать все графы из 9 вершин.

Несмотря на это, было сделано серьезное продвижение в классе 9 вершинных графов, а именно, определены все тороидальные графы, а также частично проверены графы рода не менее 2. Как можно судить по OEIS, данный результат является лучшим достигнутым на данный момент, что делает его актуальным, а данные, полученные программой, – востребованными. Данные о роде графов в дальнейшем можно использовать либо как справочную информацию в составе какой-либо электронной энциклопедии, либо как опорную точку для более тщательного изучения природы и свойств укладок графов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Богомолов, А.М. Алгебраические основы теории дискретных систем. / А.М. Богомолов, В.Н. Салий – М.: Наука. Физмалит, 1997. – 368 с.

2 Yamuna, M. Planar graph in data encryption / M. Yamuna, A.Elakkiya // International Journal of Advance Research In Science And Engineering. – March 2015. – Vol. 4, № 1. – P. 1600-1606. – Сведения доступны также по Интернет: https://www.ijarse.com/images/fullpdf/1427437040_1235_IJARSE.pdf (дата обращения: 17.01.2020). – Яз. англ.

3 Bhapkar, H.R. Applications of Planar Graph to Key Cryptography / H.R. Bhapkar // International Journal of Pure and Applied Mathematics. – 2018. – Vol. 120, № 8. – P. 89-96. – Сведения доступны также по Интернет: https://acadpubl.eu/hub/2018-120-8/1/10.pdf (дата обращения: 17.01.2020). – Яз. англ.

4 Thomassen, C. The graph genus problem is NP-complete / C. Thomassen // Journal of Algorithms. – Elsevier Inc., December 1989. – Vol. 10, № 4. – P. 568-576. – Сведения доступны также по Интернет: http://people.scs.carleton.ca/~kranakis/ROUTING/Papers/np-complete-genus.pdf (дата обращения: 10.12.2019). – Яз. англ.

5 Kawarabayashi, K. A Simpler Linear Time Algorithm for Embedding Graphs into an Arbitrary Surface and the Genus of Graphs of Bounded Tree-Width / K. Kawarabayashi, B. Mohar, B. Reed // 2008 49th Annual IEEE Symposium on Foundations of Computer Science. – Philadelphia, PA, 2008. – P. 771-780. – Сведения также доступны по Интернет: https://ieeexplore.ieee.org/document/4691009 (дата обращения: 17.01.2020). – Яз. англ.

6 Myrvold, W. Errors in graph embedding algorithms / W. Myrvold, W. Kocay // Journal of Computer and System Sciences – Elsevier Inc., March 2011. – Vol. 77, № 2. – P. 430–438. – Сведения также доступны по Интернет:

https://www.sciencedirect.com/science/article/pii/S0022000010000863 (дата обращения: 17.01.2020). – Яз. англ.

7 Болтянский, В.Г. Наглядная топология / В.Г. Болтянский, В.А. Ефремович – М.: Наука. Гл. ред. ф.-м. лит., 1983. – 160 с. (Библиотечка «Квант», Вып. 21).

8 Курант, Р. Что такое математика? / Р. Курант, Г. Роббинс; пер. под ред. А.Н. Колмогорова – 3-е изд., испр. и доп. – М.: МЦНМО, 2004. – 568 с.

9 Худенко, В.Н. Лекции по топологии / В.Н. Худенко, В.В. Махоркин; Калинигр. ун-т. – Калининград, 2000. – 111 с.

10 Асанов, М.О. Дискретная математика: графы, матроиды, алгоритмы / М.О. Асанов, В.А. Баранский, В.В. Расин. – 2-е изд., испр. и доп. – СПб.: Издательство «Лань», 2010. – 368 с.

11 Gross, J.L. Minimum and Maximum Genus [Электронный ресурс] / J.L. Gross // курс лекций Topics in Graph Theory (COMS 6204) – Spring 2010 [Электронный ресурс]. URL: http://www.cs.columbia.edu/~cs6204/files/Lec2-Min&MaxGenus.pdf (дата обращения: 10.12.2019). – Яз. англ.

12 Gross, J.L. The topological theory of current graphs / J.L. Gross, S.R. Alpert // Journal of Combinatorial Theory, Series B. - Elsevier Inc., December 1974. – Vol. 17, № 3. – P. 218-233. – Сведения доступны также по Интернет: https://www.sciencedirect.com/science/article/pii/0095895674900288 (дата обращения: 10.12.2019). – Яз. англ.

13 Perez, A. Determining the Genus of a Graph [Электронный ресурс] / A. Perez // The Pennsylvania State University, student article [Электронный ресурс]. – 2009. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.560&rep=rep1&type=pdf (дата обращения: 10.12.2019). – Яз. англ.

14 Duke, R.A. The genus of subgraphs of K8 / R.A. Duke, G. Haggard // Israel J. Math. – 1972. – Vol. 11. – P. 452-455.

15 Battle, J. Additivity of the genus of a graph / J. Battle, F. Harary, Y. Kodama // Bull. Amer. Math. Soc. – 1962. – Vol. 68. – P. 565-568. – Сведения доступны также по Интернет: https://www.ams.org/journals/bull/1962-68-06/S0002-9904-1962-10847-7/home.html (дата обращения: 10.12.2019). – Яз. англ.

16 Hopcroft, J. Efficient Planarity Testing / J. Hopcroft, R. Tarjan // Journal of ACM. – October 1974. – Vol. 21, № 4. – P. 549–568. Сведения доступны также по Интернет: https://dl.acm.org/doi/10.1145/321850.321852 (дата обращения: 17.01.2020). – Яз. англ.

17 Walther, H. Ten Applications of Graph Theory / H. Walther. – Dordrecht; Boston: D. Reidel Pub. Co.; Hingham, MA, U.S.A.: Distributors for the U.S.A. and Canada, Kluwer Academic Publishers, 1984. – 252 с.

18 Kohnert, A. Algorithm of Demoucron, Malgrange, Pertuiset [Электронный ресурс] / A. Kohnert. – URL: http://www.mathe2.uni-bayreuth.de/EWS/demoucron.pdf (дата обращения: 17.01.2020) – Яз. англ.

19 Харари, Ф. Теория графов / Ф. Харари; пер. В.П. Козырева; под ред. Г.П. Гаврилова. – М.: Мир, 1973. – 300 с.

20 Алгоритмы: построение и анализ / Т.Х. Кормен [и др.]; пер. с англ. – 3-е изд. – М.: ООО «И.Д. Вильямс», 2013. – 1328 с.

21 Horton, J.D. A polynomial-time algorithm to find the shortest cycle basis of a graph / J.D. Horton // SIAM Journal of Computing. – April 1987. – Vol. 16, № 2. – Сведения доступны также по Интернет: https://pdfs.semanticscholar.org/9843/4b3c3457461679f60c57018c3da5832cb0f4.pdf (дата обращения: 17.01.2020). – Яз. англ.

22 Новиков, Ф.А. Дискретная математика для программистов: Учебник для вузов / Ф.А. Новиков. – 3-е изд. – СПб.: Питер, 2009. – 384 с.

23 Neufeld, E. Practical Toroidality Testing / E. Neufield, W. Myrvold // SODA'97: Proceedings of the eighth annual ACM-SIAM symposium on Discrete algorithms. – January 1997. – P. 574-580. – Сведения доступны также по Интернет:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.50.4704&rep=rep1&type=pdf (дата обращения: 17.01.2020). – Яз. англ.

24 Иванов, М. Нахождение всех граней, внешней грани планарного графа. [Электронный ресурс] / М. Иванов // Maximal :: algo, 2011 [Электронный ресурс]. – URL: https://e-maxx.ru/algo/facets (дата обращения: 10.12.2019) –Загл. с экрана. –Яз. рус.

25 Абросимов, М.Б. Практические задания по графам / М.Б. Абросимов, А.А. Долгов. – 2-е изд.: Учеб. пособие. – Саратов: Изд-во «Научная книга», 2009. – 76 с.

26 McKay, B. Nauty and Traces [Программный пакет] / B. McKay, A. Piperno, доступен через Интернет, URL: http://pallini.di.uniroma1.it (дата обращения 09.09.2019). –Яз. англ.

27 The On-line Encyclopedia of Integer Sequences [Электронный ресурс] / The OEIS Foundation Inc. – URL: https://oeis.org (дата обращения: 20.12.2019). – Загл. с экрана. –Яз. англ.