Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Изоморфизм графов некоторых классов

АВТОРЕФЕРАТ

дипломной работы

студенки 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Яруниной Анастасии Александровны

Научный руководитель

старший преподаватель ___________ М. Р. Мирзаянов

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. ___________ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Дискретные структуры являются фундаментальной основой информатики. Одними из важнейших таких структур являются графы. Сведения из теории графов широко используются не только в организации структур данных и разработке алгоритмов, но и во всех остальных разделах информатики. По мере развития информатики, все более и более сложные методы анализа оказывают влияние на научные и практические проблемы. Графы являются удобным языком для формулировки и эффективным инструментом для решения задач относящихся к широкому кругу этих проблем. Можно упомянуть в этой связи вопросы конструирования систем автоматизированного проектирования программирования для ЭВМ и создания операционных систем, исследования операций и управления, а также ряда задач экономики, статистики и теоретической физики, теории информации, социологии, математической лингвистики. Широкое распространение в последнее время получило использование графов в задачах распознавания образов. Задачи на графах и алгоритмы их решения играют одну из ключевых ролей при алгоритмизации комбинаторных задач. Формулировка той или иной задачи дискретной математики па языке теории графов часто облегчает ее решение. В этом случае использование эффективных алгоритмов, существующих в теории графов, позволяет найти конструктивное решение рассматриваемой задачи.

Возможность приложения теории графов к широкому кругу задач из различных научных областей заложена, в сущности, уже в самом понятии графа, сочетающего в себе теоретико-множественные, комбинаторные и топологические аспекты, и, поскольку графы представляют собой гибкую структуру для представления других структур, задача проверки изоморфизма графов имеет фундаментальное значение.

Необходимо уметь отвечать на вопрос, являются ли некоторые конечные структуры внутренне, принципиально различными, или же они являются лишь различными представлениями одной и той же структуры. По этой причине необходимость решать задачу проверки изоморфизма графов возникает в различных областях естествознания, и методы ее решения имеют множество приложений в практической деятельности.

Проблема изоморфизма графов состоит в нахождении наиболее эффективного алгоритма, распознающего, являются ли два заданных графа изоморфными; более точно, мы интересуемся вычислительной сложностью следующей задачи: для графов G_1 и G_2 определить верно ли, что $G_1 \cong G_2$.

Вероятно, первый анализ проблемы изоморфизма графов возникает в статье Р. Рида и Д. Корнейла, "Graph isomorphism disease". Приведенная в ней библиография из 36 работ и последующая библиография из ещё 32 работ содержат ссылки на большое число алгоритмов, которые по предположению их авторов, распознают изоморфизм произвольных графов за полиномиальное время. Однако, все эти предположения оказались несостоятельными. Один из наилучших результатов к настоящему времени получен Л. Бабаи, Ю. Лаксом и В. Кантором (1983) и опирается на классификацию конечных простых групп.

Наилучший алгоритм, не использующий теорию групп, был построен М. Годбергом (1983). Стоит упомянуть, что наиболее быстрый с практической точки зрения алгоритм проверки графов на изоморфизм принадлежит Б. Маккею.

Несмотря на десятилетия попыток решения, задача проверки изоморфизма графов принадлежит к тем задачам, которые до сих пор не удается классифицировать относительно их сложности. Задача по-прежнему не может быть помещена ни в один из подклассов класса NP.

Тогда как доказано, что задача проверки изоморфизма подграфу является NP-полной, и к ней очевидным образом полиномиально сводится, например, такая NP-полная задача, как задача проверки графа на наличие в нем гамильтонова цикла, можно сказать только то, что она принадлежит классу NP: любое взятое наугад биективное отображение множества вершин одного графа на множество вершин другого за полиномиальное время может быть проверено на предмет того, является оно изоморфизмом или нет. Действительно, формируем в соответствии с проверяемым биективным отображением матрицу перестановки и обратную к ней матрицу (транспонированную матрицу перестановки). Производим преобразование подобия матрицы смежности второго графа, являющееся перестановкой строк его матрицы, соединенной с такой же перестановкой ее столбцов, и сравниваем полученные матрицы. Если матрицы поэлементно равны, то указанное биективное отображение – изоморфизм, и графы изоморфны. Иначе биективное отображение изоморфизмом не является. Указанная процедура, очевидно, полиномиальна.

В целом, не получено ответа ни на один из следующих вопросов:

- задача принадлежит классу P;
- задача является NP-полной;
- задача принадлежит классу co-NP.

Не построено алгоритмов, решавших бы задачу без каких-либо ограничений на структуру проверяемых на изоморфизм графов. Нет доказательств и того, что задача принадлежит классу co-NP, то есть нет ответа на вопрос: принадлежит ли классу NP дополнение к задаче, а именно следующая задача: даны два графа; необходимо показать, что между этими графами не существует изоморфизма. Необходимо отметить, что сложность задачи не меняется при переходе от проверки изоморфизма невзвешенных неориентированных графов к проверке изоморфизма взвешенных графов, ориентированных графов, мультиграфов. В ходе попыток классифицировать задачу по сложности был введен новый класс задач – класс изоморфизм-полных задач. Этот класс включает в себя задачи, полиномиально сводимые к задаче проверки изоморфизма графов, и к которым полиномиально сводится сама задача проверки изоморфизма графов.

В данной работе будут рассмотрены алгоритмы проверки графов на изоморфизм среди таких классов графов, как деревья, функциональные графы и кактусы, а так же алгоритмы генерации деревьев и кактусов.

Дипломная работа состоит из определений, введения, 7 разделов, заключения, списка использованных источников и 4 приложений. Общий объем работы – 72 страницы, из них 36 страниц – основное содержание, включая 12 рисунков, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе *сравнение циклических строк* приводятся теоретические данные, необходимые для того, чтобы уметь сравнивать циклические строки за оптимальное время. В частности, циклические строки сравниваются с помощью своих наименьших циклических сдвигов, которые находятся с помощью декомпозиции Линдона алгоритмом Дюваля за линейное время, доказывается корректность данного подхода. Показано, что для набора из n строк суммарной длины m за время $O(m)$ можно разбить строки на классы эквивалентности, считая эквивалентными те, которые равны с точностью до циклического сдвига.

Во втором разделе под названием *изоморфизм деревьев* рассматривается алгоритм проверки деревьев на изоморфизм. В подразделе *изоморфизм корневых деревьев* данная задача решается для корневых деревьев и приводится алгоритм нахождения канонического индекса для поддерева с корнем в вершине u, а в подразделе *сведение задачи о проверки на изоморфизм деревьев к проверке на изоморфизм корневых деревьев* предыдущее решение переносится на все неориентированные деревья с помощью подвешивания их за центры, приводится алгоритмы нахождения центров неориентированного дерева и алгоритм проверки на изоморфизм двух деревьев.

В третьем разделе *изоморфизм функциональных графов* мной предлагается решение задачи проверки функциональных графов на изоморфизм. Доказывается теорема о существовании линейного алгоритма, решающего задачу о изоморфизме двух функциональных графов, в качестве доказательства приводится данный алгоритм. Алгоритм использует идею, что два связных функциональных графа изоморфны тогда и только тогда, когда циклические строки, состоящие из канонических индексов их поддеревьев, совпадают. Предложенный мной алгоритм имеет линейную временную сложность.

В четвертом разделе *изоморфизм кактусов* мной предложено решение задачи о проверки двух кактусов на изоморфизм. Вводится понятие скелета кактуса, приводится алгоритм нахождения канонического индекса скелета кактуса с корнем в вершине *u*. Утверждается, что два связных кактуса изоморфны тогда и только тогда, когда их канонические индексы их скелетов совпадают. Предложенный мной алгоритм имеет линейную временную сложность.

В разделах *генерация деревьев*, *генерация кактусов* под номером пять и шесть соответственно приводятся алгоритмы, позволяющий генерировать все неизоморфные деревья и кактусы с заданным количеством вершин. В частности, эти алгоритмы применялись для тестирования реализаций алгоритмов из предыдущих разделов.

В седьмом разделе *реализация* и подразделах *деревья*, *функциональные графы*, *кактусы* приводятся описания работы реализованных описанных ранее алгоритмов.

ЗАКЛЮЧЕНИЕ

В данной работе были рассмотрены некоторые классы графов – деревья, функциональные графы, кактусы. В ходе работы мной были разработаны алгоритмы проверки на изоморфизм функциональных графов и кактусов. Оба алгоритма могут быть реализованы за линейное время. Кроме того, предложены алгоритмы генерации неизоморфных деревьев и кактусов с заданным числом вершин. Все алгоритмы были реализованы на языке Java, написанные реализации были тщательно протестированы, а результаты работы генераторов совпали с общедоступными табличными данными.

Рассмотренные классы графов являются подклассами планарных графов, для которых существуют линейные алгоритмы проверки на изоморфизм. Однако предложенные мной алгоритмы для функциональных графов и кактусов отличаются простотой реализации и меньшей скрытой константой в асимптотической временной сложности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Понятие отображения. Виды отображений. [Электронный ресурс] // Царица математика [Электронный ресурс] : [сайт]. URL: http://mathematike.ru/lektsii/vysshaya-matematika/matematicheskiy-analiz/vvedeniye-v-matematicheskiy-analiz/ponyatiye-otobrazheniya-vidy-otobrazheniy (дата обращения: 21.10.2016). Загл. с экрана. Яз. рус.

2 Зыков, А. А. Основы теории графов [Электронный ресурс] / А. А. Зыков. М. : Вузовская книга, 2004. 664 с.

3 Харари, Ф. Теория графов [Электронный ресурс] / Ф.Харари. М. : Едиториал УРСС, 2003. 48 с.

4 Функциональный граф [Электронный ресурс] // Wolfram MathWorld [Электронный ресурс]. URL: http://mathworld.wolfram.com/FunctionalGraph.html (дата обращения: 10.05.2015). Загл. с экрана. Яз. англ.

5 Skiena, S. Computational Discrete Mathematics: Combinatorics and Graph Theory with Mathematica / S. Skiena. MA : Addison-Wesley, 1990. Гл. 4.5.2. С. 164-165.

6 Cactus Graph [Электронный ресурс] // Wolfram MathWorld [Электронный ресурс] : [сайт]. URL: http://mathworld.wolfram.com/CactusGraph.html (дата обращения: 03.10.2016). Загл. с экрана. Яз. англ.

7 Read R. C. The Graph Isomorphism Disease [Электронный ресурс] / R. C. Read, D. G. Corneil // Journal of Graph Theory. 1977. Т. 1, № 4. С. 339-363.

8 Gati G. Further annotated bibliography on the isomorphism disease [Электронный ресурс] / G. Gati // Journal of Graph Theory. 1979. Т. 3, № 2. С. 95-109.

9 Babai L. Computational complexity and the classification of finite simple groups [Электронный ресурс] / L. Babai, W. Kantor,E. M. Luks // Proceedings 24th Annual Symposium on Foundations of Computer Science. New York : IEEE. 1983. С. 162-171.

10 Goldberg M. K. A nonfactorial algorithm for testing isomorphism of two graphs [Электронный ресурс] / M. K. Goldberg // Discrete Applied Mathematics. 1983. Т. 6, № 3. С. 229-236.

11 Brendan McKay [Электронный ресурс] // Brendan McKay [Электронный ресурс] : [сайт]. URL: http://users.cecs.anu.edu.au/~bdm/ (дата обращения: 28.10.2016). Загл. с экрана. Яз. англ.

12 Гэри, М. Вычислительные машины и труднорешаемые задачи [Электронный ресурс] / М. Гэри, Д. Джонсон. М. : Мир, 1982. 416 с.

13 Miller, G. L. Graph isomorphism, general remarks [Электронный ресурс] / G. L. Miller // Conference record of the 9th annual ACM Symposium on Theory of Computing. New York : ACM Press, 1977. C. 143-150.

14 Декомпозиция Линдона [Электронный ресурс] // Викиконспекты ИТМО [Электронный ресурс]. URL: http://neerc.ifmo.ru/wiki/index.php?title=Декомпозиция_Линдона (дата обращения: 10.05.2015). Загл. с экрана. Яз. рус.

15 Лексикографический порядок [Электронный ресурс] // Викиконспекты ИТМО [Электронный ресурс]. URL: https://neerc.ifmo.ru/wiki/index.php?title=Лексикографический_порядок (дата обращения: 29.10.2016). Загл. с экрана. Яз. рус.

16 Земляченко, В. Н. Установление изоморфизма деревьев [Электронный ресурс] / В. Н. Земляченко // Вопросы кибернетики. М. : Советское радио, 1975. С. 54-60.

17 Кормен, Т. Алгоритмы: построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест. М. : МЦНМО, 2000. 465 с.

18 Number of trees with n unlabeled nodes. [Электронный ресурс] // The On-Line Encyclopedia of Integer Sequences [Электронный ресурс] : [сайт]. URL: https://oeis.org/A000055 (дата обращения 25.09.2016). Загл. с экрана. Яз. англ.

19 Number of mixed Husimi trees with n nodes; or polygonal cacti with bridges. [Электронный ресурс] // The On-Line Encyclopedia of Integer Sequences

[Электронный ресурс] : [сайт]. URL: http://oeis.org/A000083 (дата обращения: 20.09.2016). Загл. с экрана. Яз. англ.

20 Wilson R.A. Graphs, colourings and the four-colour theorem [Электронный ресурс] / R.A. Wilson London : Oxford University Press, 2002.