В докладе будут подробно рассмотрены алгоритмы генерации корневых деревьев с использованием процедуры полного разбиения, основанной на разложениях, композициях и разбиениях натурального числа n.

ЛИТЕРАТУРА

1. *Виленкин Н. Я.* Комбинаторика. М.: Наука, 1969.
2. *Стенли Р.* Перечислительная комбинаторика. Деревья, производящие функции и симметрические функции. М.: Мир, 2005.
3. *Кручинин В. В.* Методы построения алгоритмов генерации и нумерации комбинаторных объектов на основе деревьев И/ИЛИ. Томск: Изд-во «В-Спектр», 2007.

УДК 519.175.1

АЛГОРИТМЫ ПРОВЕРКИ ИЗОМОРФИЗМА ГРАФОВ НА ОСНОВЕ ИХ ПОСЛЕДОВАТЕЛЬНОЙ СОГЛАСОВАННОЙ ДЕРЕГУЛЯРИЗАЦИИ

И. В. Широков, А. В. Пролубников

В задаче проверки изоморфизма графов (задача ИГ) даны два обыкновенных графа с одинаковым числом вершин и ребер. Необходимо ответить на вопрос, существует ли такое биективное отображение (изоморфизм) множества вершин одного графа на множество вершин второго, которое сохраняло бы смежность соответствующих вершин?

По причине неопределенности своего положения в иерархии теории сложности, задача ИГ имеет большое теоретическое значение, а также часто возникает и в приложениях. Алгоритмы решения задачи ИГ используются при решении многих прикладных задач: в задачах распознавания образов, в протоколах доказательства с нулевым разглашением; к задаче ИГ может быть сведена и вычислительно-эффективно решена задача дешифрования шифра двойной перестановки [1]. Поскольку для вычислительно сложных случаев задачи ИГ не разработано полиномиальных алгоритмов решения, возможно построение криптографических схем, основанных на вычислительной сложности решения для них задачи ИГ, например, как в [2].

Под последовательной согласованной дерегуляризацией пары графов мы понимаем такое последовательное изменение элементов матриц смежности графов (весов вершин и ребер), вследствие которого понижается мощность групп автоморфизмов графов при сохранении равенства некоторых вычисляемых в ходе дерегуляризации инвариантных характеристик графов. В докладе рассматриваются полиномиальные схемы алгоритмов для задачи ИГ, основанные на таком подходе и в качестве инварианта использующие элементы обратной матрицы к модифицированной матрице смежности.

Предложенные алгоритмы протестированы на библиотеке задач [3]. Не найдено примеров неправильного решения или невозможности нахождения решения представленными алгоритмами задачи ИГ для деревьев, случайных, планарных графов, регулярных k-мерных сеток ($k \leqslant 4$) и некоторых других классов графов. Установлено, что алгоритм решает и те задачи изоморфизма графов из библиотеки, на которых время работы алгоритмов Ullman и NAUTY — наиболее эффективных алгоритмов решения общего случая задачи ИГ — становится экспоненциальным при некоторой нумерации вершин [4]. Кроме этого, задача ИГ успешно решается предложенными алгоритмами и для сильно регулярных графов из наиболее обширной их библиотеки [5] — эти графы представляют собой класс, для которого задача проверки изоморфизма графов име-

ет наибольшую вычислительную сложность. Получены орбиты групп автоморфизмов всех графов, представленных в библиотеке [5], что также свидетельствует об эффективности предложенного подхода.

ЛИТЕРАТУРА

1. *Faizullin R. T., Prolubnikov A. V.* An algorithm of the spectral splitting for the double permutation cipher // Recognition and Image Analysis. MAIK, Nauka. 2002. V. 12. No. 4. P. 310–324.
2. *Пролубников А. В., Файзуллин Р. Т.* Построение защищенного видеоканала с использованием изоморфизма графов // Вестник Томского госуниверситета. Приложение. №9(I). 2004. С. 71–74.
3. *Foggia P., Sansone C., Vento M.* A Database of graphs for isomorphism and sub-graph isomorphism benchmarking // Proc. of the 3rd IAPR TC-15 international workshop on graph-based representations, Italy, 2001. P. 157–168.
4. *Miyazaki T.* The complexity of McKay's canonical labeling algorithm // Groups and Computation, II. Amer. Math. Soc., Providence, RI, 1997. P. 239–256.
5. `http://www.maths.gla.ac.uk/~es` — Strongly Regular Graphs.