Изоморфизм графов с ограниченными степенями вершин может быть установлен за полиномиальное время[1)]

Юджин М. Лакс

Предположим, что задано множество образующих группы G перестановок раскрашенного множества A. Задача о нахождении цветных автоморфизмов группы G заключается в поиске образующих подгруппы группы G, стабилизирующей классы элементов одного цвета. Показано, что установление изоморфизма графов с ограниченными степенями вершин сводимо за полиномиальное время к задаче о нахождении цветных автоморфизмов групп с композиционными факторами ограниченного порядка. Алгоритм, позволяющий решить последнюю задачу, требует троекратного применения принципа «разделяй и властвуй». Эта задача решается последовательно на G-орбитах. Орбита разбивается на минимальную систему блоков импримитивности. С этой точки зрения гипотеза о группе G гарантирует существование подгруппы P «малого» индекса, действующей на блоках как p-группа. Применением принципа «разделяй и властвуй» к группе задача для G сводится к небольшому числу аналогичных задач на P. В случае кубических графов имеем $p = 2$ и $P = G$, и для анализа требуются лишь элементарные понятия. Для графов с бо́льшими значениями степеней вершин обоснование метода требует некоторых новых утверждений о примитивных группах перестановок.

ВВЕДЕНИЕ

Известно, что задача распознавания изоморфизма графов за полиномиальное время сводима к задаче нахождения множества образующих группы автоморфизмов $\mathrm{Aut}(X)$ графа X. Напомним это сведение.

Пусть нужно сравнить на изоморфизм два *связных* графа X_1, X_2. Образуем их непересекающееся объединение $X = X_1 \cup X_2$. В таком случае X_1 и X_2 изоморфны тогда и только тогда, когда некоторый автоморфизм графа X переставляет две компоненты связности этого графа. Кроме того, если такие автоморфизмы графа X существуют, то по крайней мере один из них должен встретиться в любом множестве образующих $\mathrm{Aut}(X)$.

Задача нахождения образующих $\mathrm{Aut}(X)$ в свою очередь сводится несколькими способами по существу алгебраическим вопросам. В этой статье мы будем иметь дело с *задачей о нахождении цветных автоморфизмов*, которая формулируется следующим образом.

Дано: раскрашенное множество A и образующие группы G перестановок множества A. *Найти*: образующие подгруппы, состоящей из отображений, сохраняющих цвет элементов множества A.

Нахождение группы $\mathrm{Aut}(X)$ является частным случаем. Именно, пусть G — это группа всех перестановок множества вершин $\mathscr{V}(X)$, но будем рассматривать ее действующей на множестве A неупорядоченных пар вершин, раскрашенном в два цвета с целью различения ребер и неребер графа X; тогда $\mathrm{Aut}(X)$ является подгруппой G, сохраняющей цвета элементов A. Обратим внимание, что для любого графа X получаем задачу о нахождении цветных автоморфизмов, когда группа G является полной симметрической группой S_n (действующей на $\binom{n}{2}$-элементном множестве). Будет показано, что для особых классов графов имеются независимые сведения к задачам о нахождении цветных автоморфизмов и с другими группами. Действительно решающим обстоятельством при расчете времени работы основного алгоритма является то, что группа имеет такое свойство (в частности, наличие небольших композиционных факторов), которого нет у группы S_n.

Хотя подобных сведе́ний задач в литературе не было, в ряде статей по установлению изоморфизма графов существенным образом как в теоретическом, так и вычислительном отношении использовался аппарат групп перестановок. Так, важнейший прорыв имел место в недавней работе Бабаи [2]. Он рассмотрел вершинно-раскрашенные графы с ограниченными классами элементов одного цвета и описал полиномиальный по времени вероятностный $(R \cap coR)$ алгоритм для вычисления $\mathrm{Aut}(X)$. Алгоритм в значительной степени использует тот факт, что группа $\mathrm{Aut}(X)$ содержится в заданном прямом произведении малых групп. Успех Бабаи привел к более внимательному изучению алгоритмов на группах перестановок и их связи с проблемой изоморфизма графов [8, 9]. В частности, было показано, что идеи Бабаи можно реализовать без существенной потери эффективности детерминированным образом. В действительности аналогичные алгоритмы известны в литературе по вычислительным аспектам теории групп, но они не анализировались.

Отметим, что вскоре после сообщения Бабаи Хоффман [11] опубликовал алгоритм для «конических графов». Эти графы были определены так, чтобы допустить рекурсивное применение методов Бабаи. Утверждалось, что установление изоморфизма требует лишь времени порядка $n^{\log n}$. Это в свою очередь

[1)]) Engene M. Luks, Isomorphism of graphs of bounded valence can be tested in polinomial time, Journal of Computer and System Sciences, 25, 42—65 (1982).

© 1982 by Academic Press, Inc.
© перевод на русский язык, «Мир», 1985

привело к созданию Фурстом и др. [8] $n^{\log n}$ алгоритма для кубических графов. Последняя работа, используя естественное задание структуры двоичного дерева силовских 2-подгрупп S_n, сводит изоморфизм кубических графов к изоморфизму конических графов. Хотя в целом сведéние остается без изменений, представляется, что в анализе Хоффмана имеется пробел, который также лишает основания утверждение о том, что алгоритм [8] требует времени порядка $n^{\log n}$.

В настоящей статье начинается более глубокое исследование соответствующих групп. Будет представлено несколько новых алгебр и новых алгоритмов. Установление изоморфизма графов со степенями вершин, не превышающими t, сводится к задаче о нахождении цветных автоморфизмов для групп, композиционными факторами которых являются подгруппы S_{t-1}. Для этого класса групп на основном множестве вводятся два наивных (хотя ранее не замеченных) приема использования принципа «разделяй и властвуй». Тогда для кубических графов очень просто установить полиномиальную временную оценку. Ключевым фактом является то, что прием «разделяй и властвуй» дает «отбой» лишь тогда, когда он встречается с примитивными группами. Однако в случае кубических графов эти группы являются 2-группами, а порядок у примитивных 2-групп может быть равным лишь 2. В общем случае примитивные p-группы могут иметь порядок p. Отсюда следует, что алгоритм нахождения цветных автоморфизмов в действительности одинаково эффективен на p-группах. Именно это используется для ускорения установления изоморфизма графов с бóльшими значениями степеней. Хотя возникающие примитивные группы не являются p-группами, они почти таковы. Точнее будет показано, что эти группы имеют p-подгруппы полиномиального индекса, и их можно найти за полиномиальное время. Эти положения лежат в основе обобщения на случай графов с бóльшими значениями степеней вершин. Поэтому третье применение принципа «разделяй и властвуй» вводится для разбиения задачи на небольшое число аналогичных задач для p-групп.

В разд. 1 приводятся нужные определения и напоминаются некоторые основные предложения и алгоритмы. В разд. 2 описывается алгоритм в том виде, как он применяется для кубических графов. Распространение его на графы с ограниченными степенями изложено в разд. 3. Теоретико-групповое обоснование процедуры представлено в разд. 3.2. В разд. 4 приводится несколько замечаний, относящихся к обобщениям, другим приложениям и нерешенным проблемам.

Наконец, заметим, как это ясно знакомым с литературой в этой области, что основной результат заключается в том, что рассматриваемая задача является полиномиальной. Поэтому

мы избегаем ненужных усложнений, к которым привели бы попытки нахождения точных верхних оценок. И действительно, мы не всегда приводим наши «лучшие» алгоритмы (см. 4.1).

1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

1.1. Обозначения и основные предложения

Для графа X вводятся обозначения: $\mathscr{V}(X)$ — множество вершин, $\mathscr{E}(X)$ — множество ребер, $\langle v, w\rangle$ — ребро, соединяющее вершины v и w, $\mathrm{Aut}(X)$ — группа автоморфизмов графа X, $\mathrm{Aut}_e(X)$ — подгруппа группы $\mathrm{Aut}(X)$, оставляющая неподвижным ребро e.

Группа перестановок n-элементного множества обозначается S_n, и если требуется явное указание множества, то $\mathrm{Sym}(A)$. Будем говорить, что подмножество G группы $\mathrm{Sym}(A)$ *стабилизирует* подмножество $B \subseteq A$, если $\sigma(B) = B$ для $\sigma \in G$. В некоторых случаях мы будем говорить о *действии* группы G на множестве B, т. е. предполагать, что существует гомоморфизм $G \to \mathrm{Sym}(A)$. Такие действия в нашей статье возникают совершенно естественно, так как для данной группы $G \subseteq \mathrm{Sym}(A)$ мы часто будем рассматривать индуцированные действия на G-устойчивые подмножества A и на семейства подмножеств A. Действие G на B называется *полным*, если гомоморфизм $G \to \mathrm{Sym}(A)$ является инъективным. Если G действует на B и $b \in B$, то *G-орбита* элемента b является множеством $\{\sigma(b) \mid \sigma \in G\}$. Будем говорить, что группа G действует *транзитивно* на B, если B является G-орбитой. Пусть G — группа, действующая транзитивно на множестве A. *G-блоком* назовем подмножество B множества A, $B \neq \varnothing$, $B \neq A$, такое что $\sigma(B) = \tau(B)$ или $\sigma(B) \cap \tau(B) = \varnothing$ для любых $\sigma, \tau \in G$. (Мы здесь отходим от традиции, предполагающей, что $|B| > 1$.) Если B является G-блоком, то будем называть семейство $\{\sigma(B) \mid \sigma \in G\}$ *системой G-блоков на A*. В этом случае группа G действует транзитивно на блоках системы. Будем говорить, что группа G действует *примитивно* на A (или если $G \subseteq \mathrm{Sym}(A)$, то будем называть G *примитивной* группой), если не существует G-блоков размера больше 1. Говорят, что система G-блоков является *минимальной*, если G действует примитивно на блоках. (Отметим, что именно это число блоков является минимальным.) Число блоков в минимальной системе G-блоков в общем случае не определяется однозначно. Однако известен следующий результат:

Лемма 1.1. *Пусть P — транзитивная p-подгруппа* $\mathrm{Sym}(A)$, *где* $|A| > 1$. *Тогда любая минимальная система p-блоков со-*

стоит только из p блоков. Кроме того, подгруппа P', стабилизирующая все блоки, имеет в P индекс, равный p.

Доказательство. Факторгруппа P/P' является примитивной p-группой (действующей на блоках), и поэтому порядок P/P' равен числу блоков, а следовательно, равен p [10, стр. 66]. ∎

За другими основными фактами по группам перестановок мы отсылаем читателя к [12] или [26].

Если Ф — подмножество группы G, то через $\langle\Phi\rangle$ будем обозначать подгруппу G, порожденную Ф. Если H является подгруппой G, то через $[G:H]$ обозначим индекс подгруппы H в G. Будем обозначать I как единичный элемент группы, так и тривиальную подгруппу, состоящую лишь из этого элемента. Будем писать $N \lhd G$, если N является нормальной подгруппой G. *Композиционным рядом* группы G назовем последовательность подгрупп

$$1 = G^m \lhd \ldots \lhd G^2 \lhd G^1 \lhd G^0 = G,$$

в которой факторгруппы G^i/G^{i+1} являются простыми группами. По теореме Жордана — Гёльдера [10, 12] семейство факторгрупп не зависит от выбора композиционного ряда. Группы этого семейства называются *композиционными факторами* группы G.

1.2. Некоторые базисные алгоритмы

Поскольку любая группа G имеет множество образующих мощности $\log|G|$ или меньше, на задание подгрупп группы S_n затрачивается память, объем которой полиномиально зависит от n. Требования к экономичности таких представлений ставят следующую проблему: на какие фундаментальные вопросы о группах ответы могут быть получены за полиномиальное время? Поиск *эффективных* методов для действий с большими группами перестановок имеет, естественно, давнюю историю (см. [24]). Однако работы по анализу сложности алгоритмов появились относительно недавно. В статье [9] автор вместе с Фурстом и Хопкрофтом привел ряд основных вычислительных задач, имеющих полиномиальные по времени решения. Основное средство (последовательность подгрупп $\{G_i\}$) вероятнее всего принадлежит Симсу [23, 24] и применяется уже некоторое время. Мы выделили из работы [9] следующий результат.

Лемма 1.2 (Фурст — Хопкрофт — Лакс). *Для данного множества образующих подгруппы G группы S_n за полиномиальное время могут быть определены*:

(i) *порядок группы G*;

(ii) *принадлежит ли данная перестановка группе G*;

(iii) *образующие для любой подгруппы G, о которой известно, что она имеет индекс, ограниченный полиномом от порядка G, для которой имеется полиномиальный по времени тест проверки принадлежности элемента к G.*

Для удобства чтения наметим алгоритмы установления свойств из леммы 1.2. Предположим, что G является подгруппой $\mathrm{Sym}(A)$, где $A = \{a_1, \ldots, a_n\}$. Обозначим через G_i подгруппу G, оставляющую неподвижными все элементы $\{a_1, \ldots, a_i\}$. Тогда мы получаем последовательность подгрупп

$$1 = G_{n-1} \subseteq \ldots \subseteq G_1 \subseteq G_0 = G.$$

Алгоритм определения (i) из леммы 1.2 заключается в совместном построении полных множеств представителей классов смежности C_i группы G_i по подгруппе G_{i+1}, $0 \leqslant i \leqslant n-2$. Тогда порядок $|G|$ равен произведению $|C_0| \cdot |C_1| \ldots |C_{n-2}|$. Строительным блоком этой конструкции является следующая подпрограмма. На ее вход поступает элемент $\alpha \in G$. Списки C_i содержат (не обязательно полные) множества представителей левых классов смежности группы G_i по подгруппе G_{i+1}.

```
procedure Фильтр (α)
    for i = 0 until n − 2 do
      begin
        if γ⁻¹α ∈ G_{i+1} для некоторого γ ∈ C_i
          then α ← γ⁻¹α
          else добавить α к C_i; return
      end
    return
```

Таким образом, подпрограмма отыскивает представителя класса смежности α по подгруппе G_1 в списке C_0. Если он не находится, то элемент α представляет не найденный ранее класс смежности и α добавляется к списку. Если же он найден «под маской» γ, то $\gamma^{-1}\alpha$ принадлежит G_1 и его класс по подгруппе G_2 ищется в C_1, и т. д. Поскольку для $\sigma \in G_i$ принадлежность к G_{i+1} устанавливается за константное время, то вся процедура требует лишь полиномиального времени. Заметим, что результат вызова процедуры *Фильтр* для $\alpha \in G$ таков же, когда начальный класс принадлежит $C_0C_1 \ldots C_{n-2}$. Это имеет место независимо от того, вызывает ли α увеличение некоторого C_i или он «выдерживает» фильтрацию.

Алгоритм для определения (i) из леммы 1.2 теперь легко описать.

(1) Первоначально положить $C_i \leftarrow \{1\}$ для всех i;

(2) фильтровать множество образующих G;

(3) фильтровать множества C_iC_j с $i \geqslant j$.

Конечно, вызовы подпрограммы могут приводить к возрастанию некоторых C_i, тем самым требуя более частых обраще-

ний к (3). Однако априорно известно, что на любом этапе $|C_i| \leqslant [G_i : G_{i+1}] \leqslant n - i$. Поэтому процесс заканчивается за полиномиальное время. Результат (2) заключается в том, что исходное множество образующих содержится в $C_0C_1 \ldots C_{n-2}$. Фактическим выводом из (3) при данном (1) является то, что $C_iC_j \subseteq C_jC_{j+1} \ldots C_{n-2}$. Эти результаты могут быть использованы [9] для доказательства того, что $G = C_0C_1 \ldots C_{n-2}$. Отсюда непосредственно следует, что C_i представляет G_i по подгруппе G_{i+1}.

Если утверждение (i) леммы 1.2 дано, алгоритм для предложения (ii) леммы 1.2 непосредственно следует из такого замечания: $\sigma \in \langle \Phi \rangle$ тогда и только тогда, когда $|\langle \Phi, \sigma \rangle| = |\langle \Phi \rangle|$. Анализируя несколько глубже, мы заметим, что установление принадлежности может быть проведено посредством построения списков $\{C_i\}$ для $\langle \Phi \rangle$ в результате вызова процедуры *Фильтр* (σ). Поэтому элемент σ принадлежит G тогда и только тогда, когда он проходит фильтрацию (т. е. не вызывает увеличения какого-либо C_i).

Для доказательства предложения (iii) леммы 1.2 мы изменим последовательность групп на

$$1 = H_{n-1} \subseteq \ldots \subseteq H_2 \subseteq H_1 \subseteq H \subseteq G$$

и применим тот же самый алгоритм для порождения полных множеств представителей классов смежности. Заметим, что полиномиальность индекса подгруппы H в G и требование, чтобы принадлежность к H была полиномиально разрешима, опять же гарантируют нам, что на весь процесс требуется лишь полиномиальное время. Игнорируя первый список, а именно представителей G по подгруппе H получаем, что остальные списки содержат множество образующих H. (Другое описание сущности этого алгоритма может быть дано после доказательства предложения 3.10.)

Пусть даны образующие группы $G \subseteq \mathrm{Sym}(A)$. Тогда, используя алгоритм транзитивного замыкания легко определить G-орбиты. Этот процесс будет использоваться как программа. Для транзитивного случая нужно разбить множество дальше на нетривиальные блоки импримитивности (если такие существуют) относительно действия группы. Заметим теперь, что эта цель также достижима за полиномиальное время. Более точно, фиксируем $a \in A$ и для каждого элемента $b \in A$, $b \neq a$ сгенерируем (единственный) наименьший G-блок, содержащий $\{a, b\}$. Как отметил Симс в работе [22], это будет в точности компонента связности a в графе X с $\mathscr{V}(X) = A$ и $\mathscr{E}(X)$, которое является G-орбитой $\{a, b\}$ в множестве всех (неупорядоченных) пар элементов A. Если группа G импримитивна, то при некотором выборе элемента b блок должен быть собственным. В этом случае компоненты связности X определяют систему G-блоков. Тогда, повторяя процесс с порожденным действием G на блоки столько раз, сколько необходимо, мы действительно получаем алгоритм для следующей леммы.

Лемма 1.3. *Для данного множества образующих подгруппы G группы G_n и G-орбиты B можно определить за полиномиальное время минимальную систему G-блоков B.*

Заметим, что Аткинсон [1] предложил чрезвычайно эффективную реализацию выше приведенных идей. Для наших же приложений необходимо также определить подгруппу G, стабилизирующую все блоки.

Лемма 1.4. *Пусть G и B такие же, как в лемме* 1.3. *Образующие подгруппы G, стабилизирующие все блоки системы G-блоков B, могут быть найдены за полиномиальное время*

Это утверждение вытекает, например, из предположений (iii) леммы 1.2. Пусть $G_{(i)}$ обозначает подгруппу, стабилизирующую любой из первых i блоков. Тогда (взяв $G = G_{(0)}$) получим, что $[G_{(i)} : G_{(i+1)}]$ не меньше числа блоков минус i.

2. СЛУЧАЙ КУБИЧЕСКИХ ГРАФОВ

2.1. Сведение к задаче о нахождении цветных автоморфизмов

Докажем, что задача установления изоморфизма кубических графов сводима за полиномиальное время к задаче о нахождении цветных автоморфизмов для 2-групп. На первом шаге модифицируется сведение к задаче о нахождении автоморфизмов. Побуждающей причиной служит утверждение Татта (предложение 2.2), что $\mathrm{Aut}_e(X)$ является 2-группой.

Предложение 2.1. Установление изоморфизма кубических графов сводимо за полиномиальное время к задаче нахождения образующих группы $\mathrm{Aut}_e(X)$, где X — связный кубический граф, а e — выделенное ребро.

Доказательство. Предположим, что имеется полиномиальный по времени алгоритм, который позволяет находить образующие для любой такой группы $\mathrm{Aut}_e(X)$. Тогда достаточно осуществить сравнение двух связных кубических графов X_1 и X_2. Фиксируем некоторое ребро $e_1 \in \mathscr{E}(X_1)$. Проверим для любого ребра $e_2 \in \mathscr{E}(X_2)$, существует ли изоморфизм из X_1 в X_2, отображающий ребро e_1 в ребро e_2, следующим образом. Построим связный кубический граф X из непересекающегося объединения $X_1 \cup X_2$ посредством (i) помещения новой вершины v_1 на ребро e_1 и новой вершины v_2 на ребро e_2 и (ii) соединения вершин v_1 и v_2 новым ребром. В таком случае изоморфизм X_1 в X_2, отображающий e_1 в e_2, существует тогда и только тогда, когда

некоторый элемент группы $\mathrm{Aut}_e(X)$ переставляет вершины v_1 и v_2. Кроме того, если такие автоморфизмы существуют, любое множество образующих $\mathrm{Aut}_e(X)$ должно содержать один из них. ∎

Теперь фиксируем связный кубический граф X с $|\mathscr{V}(X)|=n$. Группа $\mathrm{Aut}_e(X)$ определяется посредством естественного ряда следующих одна за другой «апроксимаций» $\mathrm{Aut}_e(X_r)$, $r=1,2,\ldots$, где X_r — подграф, состоящий из всех вершин и всех ребер X, которые появляются на цепях длины не более r, проходящих через ребро e. Так что X_1 — это само ребро e_1, а $X_{n-1}=X$. Эти группы связаны посредством порожденных гомоморфизмов

$$\pi_r:\mathrm{Aut}_e(X_{r+1})\to\mathrm{Aut}_e(X_r),$$

где $\pi_r(\sigma)$ есть сужение σ на X_r. Следовательно, предполагая, что группа $\mathrm{Aut}_e(X_r)$ известна, поиск $\mathrm{Aut}_e(X_{r+1})$ приводит к двум задачам.

(I) найти множество образующих $\mathscr{R}$ для K_r — ядра гомоморфизма π_r;

(II) найти множество образующих $\mathscr{S}$ для $\pi_r(\mathrm{Aut}_e(X_{r+1}))$ — образа π_r.

Поэтому если $\mathscr{S}'$ — некоторый, не обязательно полный прообраз $\mathscr{S}$ в $\mathrm{Aut}_e(X_{r+1})$ (т. е. $\pi_r(\mathscr{S}')=\mathscr{S}$), то $\mathscr{R}\cup\mathscr{S}'$ порождает $\mathrm{Aut}_e(X_{r+1})$.

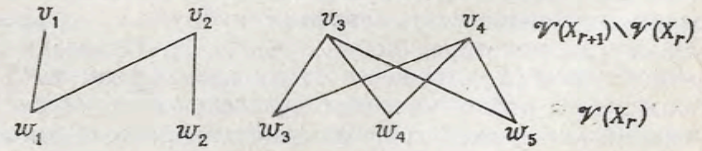
Мы увидим, что более существенной и трудной задачей является (II). Отметим, что именно эта задача была сведена в работе [8] к проблеме изоморфизма конических графов.

Для решения этих задач рассмотрим $\mathscr{V}(X_{r+1})\setminus\mathscr{V}(X_r)$. Каждая вершина из этого множества связана с одной, двумя или тремя вершинами из X_r. Осуществим кодирование этого отношения следующим образом. Пусть A обозначает семейство всех подмножеств $\mathscr{V}(X_r)$ мощности один, два или три. Определим отображение

$$f:\mathscr{V}(X_{r+1})\setminus\mathscr{V}(X_r)\to A$$

посредством формулы $f(v)=\{w\in\mathscr{V}(X_r)\,|\,\langle v,w\rangle\in\mathscr{E}(X)\}$.

Пример.



Здесь

$$f(v_1)=w_1,\quad f(v_2)=\{w_1,w_2\},\quad f(v_3)=\{w_3,w_4,w_5\}.$$

Пару различных вершин v, v' назовем *близнецами*, если $f(v)=f(v')$ (отметим, что тройни не может быть). В приведенном выше примере v_3 и v_4 являются близнецами, а v_1 и v_2 нет. Теперь

$$\text{из } \sigma\in\mathrm{Aut}_e(X_{r+1}) \text{ следует } f(\sigma(v))=\sigma(f(v)). \qquad (*)$$

Следовательно, в частности, если $\sigma\in K_r$ (т. е. фиксирует все элементы X_r), то $f(v)=f(\sigma(v))$; так что или $v=\sigma(v)$, или v и $\sigma(v)$ — близнецы. Отсюда следует, что K_r является элементарной абелевой 2-группой, порожденной перестановками внутри каждой пары близнецов.

Так как $|\mathrm{Aut}_e(X_{i+1})|=|\mathrm{Im}\,\Pi_r|\cdot|K_r|$, доказательство по индукции дает

Предложение 2.2 (Татт). *Для любого r, $\mathrm{Aut}_e(X_r)$ является 2-группой.*

Для того чтобы получить (II), отметим, что из (*) следует, что любой $\sigma\in\pi_r(\mathrm{Aut}_e(X_{r+1}))$ стабилизирует множество отцов, имеющих одного сына, т. е. $A_1=\{a\in A\,|\,a=f(v)$ для некоторого единственного $v\in\mathscr{V}(X_{r+1})\setminus\mathscr{V}(X_r)\}$. Кроме того, любой $\sigma\in\pi_r(\mathrm{Aut}_e(X_{r+1}))$ должен стабилизировать подмножество A, состоящее из отцов близнецов, т. е.

$$A_2=\{a\in A\,|\,a=f(v_1)=f(v_2) \text{ для некоторых } v_1\neq v_2\}.$$

Далее, помимо ребер из $\mathscr{V}(X_{r+1})\setminus\mathscr{V}(X_r)$ имеются элементы $\mathscr{E}(X_{r+1})\setminus\mathscr{E}(X_r)$, которые соединяют две вершины из $\mathscr{V}(X_r)$. Они соответствуют следующему подмножеству A:

$$A'=\{\{w_1,w_2\}\in A\,|\,\langle w_1,w_2\rangle\in\mathscr{E}(X_{r+1})\}.$$

Некоторый элемент из $\pi_r(\mathrm{Aut}_e(X_{r+1}))$ также должен стабилизировать A'. Теперь можно сформулировать условие, при котором $\sigma\in\mathrm{Aut}_e(X_r)$ лежит в образе гомоморфизма π_r. Именно,

Предложение 2.3. *Множество $\pi_r(\mathrm{Aut}_e(X_{r+1}))$ состоит в точности из тех $\sigma\in\mathrm{Aut}_e(X_r)$, которые стабилизируют любое из семейств A_1, A_2, A'.*

Доказательство. Нужно доказать только, что если σ стабилизирует A_1, A_2, A', то он действительно может быть продолжен до элемента группы $\mathrm{Aut}_e(X_{r+1})$. Для таких σ определим продолжение следующим образом. Для каждого единственного сына v, $f(v)\in A_1$ справедливо $\sigma(f(v))\in A_1$, поэтому отобразим v на единственного сына перестановки $\sigma(f(v))$. Для каждой пары близнецов v, v', $f(v)\in A_2$ имеем $\sigma(f(v))\in A_2$, поэтому отобразим пару $\{v,v'\}$ на сыновей-близнецов перестановки $\sigma(f(v))$ в произвольном порядке. По построению это продолжение стабилизирует множество ребер между $\mathscr{V}(X_r)$ и $\mathscr{V}(X_{r+1})\setminus\mathscr{V}(X_r)$ (заметим, что $f(v)$ и $\sigma(f(v))$ автоматически имеют одну и ту же мощность, как подмножества $\mathscr{V}(X_r)$). То,

что оно стабилизирует «новые» ребра между «старыми» точками, неявно было заключено еще до продолжения в условии $\sigma(A') = A'$. ∎

Пусть $A_0 = A \setminus (A_1 \cup A_2)$. Для того чтобы выделить сущность задачи, раскрасим множество A в шесть цветов с тем, чтобы различать шесть непересекающихся областей

$$A_0 \cap A',\ A_1 \cap A',\ A_2 \cap A',\ A_0 \setminus A',\ A_1 \setminus A',\ A_2 \setminus A'.$$

(Наблюдательный читатель мог бы заметить, что в действительности могут встретиться лишь пять из этих случаев. Этот факт несуществен для настоящего рассмотрения.) Теперь рассмотрим элементы $\mathrm{Aut}_e(X_{r+1})$, сохраняющие цвет при их действии на A. Тогда задача об установлении изоморфизма кубических графов сводится за полиномиальное время к следующей задаче.

Задача 1. Дано: Множество образующих 2-подгруппы G группы $\mathrm{Sym}(A)$, где A — раскрашенное множество. *Найти*: Множество образующих подгруппы $\{\sigma \in G \mid \sigma$ сохраняет цвет$\}$.

2.2. Алгоритм нахождения цветных автоморфизмов для 2-групп

Наличие действия группы на множестве показывает два способа применения принципа «разделяй и властвуй»: разбиение множества на орбиты, а в транзитивном случае разбиение множества на блоки импримитивности. Оба способа играют существенную роль в алгоритме решения задачи 1, но они требуют такого обобщения задачи, которое допускает рекурсивную процедуру.

Фиксируем раскрашенное множество из n элементов. Количество и распределение цветов не существенно. Для $a, b \in A$ отношение «a имеет тот же цвет, что и b» будем сокращенно записывать «$a \sim b$». Предположим, что $B \subseteq A$ и $K \subseteq \mathrm{Sym}(A)$.

Введем множество $\mathscr{C}_B(K) = \{\sigma \in K \mid$ для всех $b \in B$, $\sigma(b) \sim b\}$. Следующие свойства получаются непосредственно:

(i) $\mathscr{C}_B(K \cup K') = \mathscr{C}_B(K) \cup \mathscr{C}_B(K')$;

(ii) $\mathscr{C}_{B \cup B'}(K) = \mathscr{C}_B \mathscr{C}_B(K)$.

Требуемое обобщение задачи 1 — это

Задача 2. Дано: Образующие 2-подгруппы G группы $\mathrm{Sym}(A)$, G-устойчивое подмножество B и $\sigma \in \mathrm{Sym}(A)$. *Найти*: $\mathscr{C}_B(\sigma G)$.

Задача 1 является ее частным случаем при $B = A$, $\sigma = 1$. Сначала получим следующее утверждение:

Лемма 2.4. *Если множество $\mathscr{C}_B(\sigma G)$ непусто, то оно является левым классом смежности подгруппы $\mathscr{C}_B(G)$.*

Доказательство. G-устойчивость множества B гарантирует, что $\mathscr{C}_B(G)$ является подгруппой. Если $\sigma_0 \in \mathscr{C}_B(\sigma G)$, то, в частности, $\sigma G = \sigma_0 G$. Для $\tau \in G$, $b \in B$ известно, что $\tau(b) \in B$, и поэтому $\sigma_0 \tau(b) \sim \tau(b)$. Следовательно, $\sigma_0 \tau \in \mathscr{C}_B(\sigma_0 G)$ тогда и только тогда, когда $\tau \in \mathscr{C}_B(G)$, т. е. $\mathscr{C}_B(\sigma_0 G) = \sigma_0 \mathscr{C}_B(G)$. ∎

В силу леммы мы можем ожидать, что программа для решения задачи 2 на входе принимает классы смежности группы. Каждый из классов смежности можно задать парой, состоящей из элемента-представителя и множества образующих группы.

Алгоритм решения задачи 2 продолжается следующим образом. Если B является объединением G-устойчивых подмножеств B' и B'', то

$$\mathscr{C}_C(\sigma G) = \mathscr{C}_{B''} \mathscr{C}_{B'}(\sigma G).$$

Если же это не так, т. е. G действует транзитивно на B, то в силу лемм 1.1 и 1.3 запишем B в виде объединения двух G-блоков. $B = B' \cup B''$. Заметим, что на этот раз мы не пытаемся вычислить $\mathscr{C}_{B'}(\sigma G)$ непосредственно; B' не является G-устойчивым. Однако можно найти за полиномиальное (от n) время подгруппу H группы G, стабилизирующую B' и B''. Тогда

$$G = H \cup \tau H,$$

и поэтому

$$\mathscr{C}_B(\sigma G) = \mathscr{C}_B(\sigma H) \cup \mathscr{C}_B(\sigma \tau H)$$
$$= \mathscr{C}_{B''} \mathscr{C}_{B'}(\sigma H) \cup \mathscr{C}_{B''} C_{B'}(\sigma \tau H).$$

Важно заметить, что лемма 2.4 гарантирует, что когда как $\mathscr{C}_B(\sigma H)$, так и $\mathscr{C}_B(\sigma \tau H)$ не пусты, они должны привести к одному и тому же классу смежности подгруппы $\mathscr{C}_B(G)$. В таком случае, имеем

$$\mathscr{C}_B(\sigma H) = \rho_1 \mathscr{C}_B(H), \quad \mathscr{C}_B(\sigma \tau H) = \rho_2 \mathscr{C}_B(H)$$

и основной ответ может быть выражен в виде

$$\mathscr{C}_B(\sigma G) = \rho_1 \langle \mathscr{C}_B(H),\ \rho_1^{-1} \rho_2 \rangle.$$

(Решение должно включать правую сторону, так как $\mathscr{C}_B(H)$ и $\rho_1^{-1}\rho_2$ содержатся в $\mathscr{C}_B(G)$; с другой стороны, ясно, что правая сторона содержит решения обеих подзадач.)

Мы показали, как в интранзитивном случае множество разбивается на непересекающиеся части и задача решается на каждой из частей. В транзитивном случае вычисление $\mathscr{C}_B(\sigma G)$ заключается в четырех рекурсивных обращениях к решению таких же задач на множествах B', B'', имеющих мощность в два раза меньше. Остается лишь проверить случай $|B| = 1$.

Но если $B=\{b\}$ и $GB=B$, то

$$\mathscr{C}_B(\sigma G)=\begin{cases}\sigma G, & \text{если } \sigma(b)\sim b;\\ \varnothing, & \text{если } \sigma(b)\not\sim b,\end{cases}$$

так что в этом случае решение получается за константное время. Стандартное проведение доказательства по индукции показывает, что алгоритм в целом требует только полиномиального времени.

3. СЛУЧАЙ ОГРАНИЧЕННЫХ СТЕПЕНЕЙ ВЕРШИН

3.1. Группы, необходимые для рассмотрения данного случая

Рассмотрим теперь графы со степенями вершин, не превышающими $\leqslant t$, где t — фиксированное число. Процедура разд. 2.1 обобщается для сведения задачи установления изоморфизма к определенной задаче о нахождении цветных автоморфизмов. Первым барьером является выделение решающих свойств групп.

Вкратце опишем рассматриваемую ситуацию. Сведение к определению ядра и образа гомоморфизма π_r: $\mathrm{Aut}_e(X_{r+1})\to\mathrm{Aut}_e(X_r)$ сохраняется без изменений. Множество A теперь состоит из всех непустых подмножеств $\mathscr{V}(X_r)$ мощности не более $t-1$, и, следовательно, «отцовское отображение» $\mathscr{V}(X_{r+1})\setminus\mathscr{V}(X_r)\to A$ имеет прежний смысл. Элемент $\sigma\in\mathrm{Aut}_e(X_{r+1})$ принадлежит теперь $K_r=\ker(\pi_r)$ тогда и только тогда, когда он стабилизирует каждый полный прообраз $f^{-1}(a)$ для $a\in A$. Множества $f^{-1}(a)$ образуют разбиение множества $\mathscr{V}(X_{r+1})\setminus\mathscr{V}(X_r)$, а K_r является прямым произведением:

$$K_r=\mathop{\times}_{a\in A}\mathrm{Sym}(f^{-1}(a)).$$

Каждый множитель этого прямого произведения может быть представлен с помощью по крайней мере двух образующих.

Теперь заметим, что элемент $\sigma\in\mathrm{Aut}_e(X_r)$ принадлежит образу π_r тогда и только тогда, когда σ стабилизирует для каждого $0\leqslant s\leqslant t-1$ как множество «отцов» s-элементных подмножеств вида

$$A_s=\{a\in A\mid |f^{-1}(a)|=s\},$$

так и множество A' новых ребер. Раскрасим A соответственно в $2t$ цветов. Задача опять же заключается в нахождении цветных автоморфизмов в группе $G=\mathrm{Aut}_e(X_r)$, действующей на A.

Отметим, что для алгоритма разд. 2.2 было существенно то, что группы в случае кубических графов были 2-группами (а

именно, при декомпозиции множества на два блока импримитивности). Доказательство основывается на том, что ядра K_r — это 2-группы. Природа же ядер в рассматриваемой ситуации проясняется следующим понятием.

Обозначим через Γ_k, $k\geqslant 2$ класс групп G, таких что все композиционные факторы G являются подгруппами S_k. Заметим, что простые множители порядка $|G|$ группы G из Γ_k не превышают k.

Замечание. На самом деле достаточно потребовать, чтобы композиционные факторы имели ограниченный порядок. По существу это и является утверждением первой публикации представленных результатов в [15], и этого достаточно для доказательства утверждения, объявленного в заголовке статьи. Действительно, это позволяет избежать сложностей леммы 3.2. Однако в будущем тщательном анализе алгоритма нужно использовать более точное описание. Такая версия Γ_k и была предложена Л. Бабаи.

Если $N\lhd G$, то из теоремы Жордана — Гёльдера следует, что семейство композиционных факторов группы G является объединением композиционных факторов N и G/N. Следовательно, имеет место

Лемма 3.1. *Если $N\lhd G$, то G принадлежит классу Γ_k тогда и только тогда, когда как N, так и G/N принадлежат классу Γ_k.*

Для того чтобы показать, что Γ_k замкнута относительно извлечения произвольных подгрупп, нам необходима следующая лемма. Этот результат несомненно известен специалистам, однако так как мы не нашли подходящей ссылки, то мы приводим его краткое доказательство.

Лемма 3.2. *Подгруппы S_k принадлежат Γ_k.*

Доказательство. Необходимо показать, что если $N\lhd G\subseteq S_k$, причем факторгруппа G/N проста, то G/N изоморфна подгруппе S_k. Пусть G_i — подгруппа G, оставляющая неподвижными элементы $\{1,2,\ldots,i\}$. Образуем последовательность подгрупп, порожденную G_i и N:

$$N=G_{n-1}N\subseteq\ldots\subseteq G_2N\subseteq G_1N\subseteq G_0N=G.$$

Заметим, что

$$|G_iN:G_{i+1}N|\leqslant|G_i:G_{i+1}|\leqslant k-i\leqslant k.$$

Так как $N\subset G$, существует наименьшее целое j, такое что $G_{j+1}N\subset G_jN$. Группа $G=G_jN$ действует транзитивно на множестве C классов смежности G_jN по подгруппе $G_{j+1}N$ (фактически уже G_j обладает этим свойством). Поскольку $N\lhd G$, то N действует тривиально на C. Следовательно, действие G/N индуцируется на C. Это действие нетривиально, поскольку оно

транзитивно, а так как факторгруппа G/N проста, то оно и точно. ∎

Заметим, что из вышеприведенной леммы вытекает существование полиномиального по времени алгоритма получения вложения G/N в S_k.

Теперь мы можем доказать следующий результат.

Лемма 3.3. *Если $G \in \Gamma_k$, то любая подгруппа G принадлежит Γ_k.*

Доказательство. Предположим, что $G \in \Gamma_k$. Композиционный ряд для группы G

$$1 = G^m \lhd \ldots \lhd G^2 \lhd G^1 \lhd G^0 = G$$

дает для любой ее подгруппы H ряд

$$1 = G^m \cap H \lhd \ldots \lhd G^2 \cap H \lhd G^1 \cap H \lhd G^0 \cap H = H$$

(который не обязательно является композиционным). Согласно лемме 3.1, достаточно показать, что каждая факторгруппа $G^i \cap H / G^{i+1} \cap H$ принадлежит Γ_k. Однако эта факторгруппа является подгруппой G_i/G_{i+1}, которая по предположению есть подгруппа группы S_k. ∎

Наконец, для того чтобы связать этот класс групп с рассматриваемой задачей, заметим, что $\mathrm{Sym}(f^{-1}(a)) = S_m$ для некоторого $m \leqslant t-1$. Поэтому, опираясь на леммы, по индукции получаем

$$K_r \in \Gamma_{t-1}.$$

Предложение 3.4. $\mathrm{Aut}_\rho(X_r) \in \Gamma_{t-1}$ *для любого r.*

Следовательно, задача установления изоморфизма графов с ограниченными значениями степеней вершин сводима за полиномиальное время к следующей задаче 3. (Здесь k — фиксированное число.)

Задача 3. Дано: Множество образующих подгруппы G группы $\mathrm{Sym}(A)$, где $G \in \Gamma_k$, а A — раскрашенное множество. *Найти*: Множество образующих подгруппы $\{\sigma \in G \mid \sigma$ сохраняет цвет$\}$.

Алгоритм решения задачи 3 будет следовать из применения стратегии принципа «разделяй и властвуй» разд. 2.2. Однако мы введем один дополнительный прием. В следующих двух подразделах развивается необходимая техника.

3.2. Примитивные группы класса Γ_k

Требуемое свойство заключается в том, что у таких групп имеются p-подгруппы «малого» индекса. В частности, имеет место

Предложение 3.5. *Существует вычислимая константа c ($c = c(k)$), такая что если G-примитивная подгруппа группы S_n и $G \in \Gamma_k$, то для некоторого простого числа p группа G имеет силовскую p-подгруппу индекса, не превышающего n^c.*

По традиции, принятой при изучении примитивных групп, в доказательстве выделяются два случая в соответствии с тем, является ли цоколь абелевым или неабелевым. Напоминаем, что цоколь конечной группы есть подгруппа, порожденная всеми минимальными нормальными подгруппами.

Рассмотрим структуру цоколя примитивной группы. В любой конечной группе минимальная нормальная подгруппа обязательно является прямым произведением изоморфных простых групп [12, доказательство предложения 1.9.13]. Пусть N — заданная минимальная нормальная подгруппа примитивной группы G. Предположим, что G обладает второй минимальной подгруппой N'. Тогда N и N' коммутируют, а так как нормальные подгруппы примитивной группы транзитивны [26, стр. 17], мы приходим к заключению [26, разд. 1.4], что:

(i) N изоморфна N';

(ii) N' является централизатором N в G.

В частности, из (ii) вытекает, что у G не может быть других минимальных нормальных подгрупп. Следовательно, цоколь G есть или N, или $N \times N'$, и в любом случае он является прямым произведением изоморфных простых групп.

Если примитивная группа $G \subseteq S_n$ имеет абелев цоколь, то в классическом результате [12, предложения 11.3.2 и 11.3.5] утверждается, что для некоторого простого p справедливо $n = p^d$ и G может быть отождествлена с подгруппой d-мерной аффинной группы над $\mathbb{Z}_p$, обозначаемой $AGL(d, p)$ ($AGL(d, p)$ порождается группой $GL(d, p)$ всех невырожденных линейных преобразований $\mathbb{Z}_p^d$ и группой всех трансляций, т. е. аддитивной группой $\mathbb{Z}_p^d$). Трансляции образуют цоколь группы G. Известно также, что

$$|AGL(d, p)| = p^{(d(d+1))/2}(p-1)(p^2-1)(p^3-1)\ \ldots\ (p^d-1). \quad (*)$$

(См. [12], например обсуждение $|GL(d, p)|$.)

Для дальнейшего потребуется следующая теоретико-числовая лемма.

Лемма 3.6. *Пусть p, q — различные простые числа. Существует такая константа α ($\alpha = \alpha(p, q)$), что если q^x делит $|AGL(d, p)|$, то $x < d\alpha$.*

Доказательство. Обозначим через $\gamma(y)$ показатель наибольшей степени q, делящей $p^y - 1$. Таким образом, $p^y = 1 + aq^{\gamma(y)}$, $(a, q) = 1$. Тогда для любого z

$$p^{yz} = (1 + aq^{\gamma(y)})^z \equiv 1 + azq^{\gamma(y)} \bmod q^{2\gamma(y)}.$$

Тем самым для $\gamma(y) \geqslant 1$ получаем:

(i) если $(z, q) = 1$, то $\gamma(yz) = \gamma(y)$;

(ii) $\gamma(yq) \geqslant \gamma(y) + 1$, и если $\gamma(y) \geqslant 2$, то имеет место равенство.

Далее, пусть r — порядок p по модулю q. Положим $s = \gamma(r)$ и $t = \gamma(rq)$. Тогда $s \geqslant 1$ и в силу (ii) $t \geqslant s + 1 \geqslant 2$. (В действительности равенство $t = s + 1$ нарушается только когда $q = 2$ и $s = 1$.) Используем эти соотношения для того, чтобы описать $\gamma(y)$ в общем случае. Ясно, что $\gamma(y) = 0$, если только r не делит y. В силу (i) и (ii) получаем, что если $(u, q) = 1$, то

$$\gamma(ruq^b) = \begin{cases} s, & \text{если } b = 0; \\ t + b - 1, & \text{если } b \geqslant 1. \end{cases}$$

Из (*) следует, что наибольшее x, такое что q^x делит $|AGL(d, p)|$, равно

$$x = s\left[\frac{d}{r}\right] + (t - s)\left[\frac{d}{qr}\right] + \left[\frac{d}{q^2 r}\right] + \left[\frac{d}{q^3 r}\right] + \ldots.$$

Раскрывая квадратные скобки и суммируя бесконечный геометрический ряд, получаем оценку

$$x < d\left(\frac{s}{r} + \frac{t - s}{qr} + \frac{1}{q(q-1)r}\right). \quad \blacksquare$$

Замечание. В действительности о структуре силовских q-подгрупп $AGL(d, p)$ известно значительно больше. (См. [25] для случая $q \neq 2$ и [7] для $q = 2$.) Выражение для «наибольшего x» выведено из результатов этих работ.

В таком случае имеет место

Предложение 3.7. *Заключение предложения 3.5 остается в силе, если цоколь группы G абелев.*

Доказательство. Мы знаем, что $G \subseteq AGL(d, p)$ при $n = p^d$. Для каждого $q \neq p$, наибольшая степень q^* в $|G|$ не превышает

$$q^{d\alpha(p, q)} = n^{\alpha(p, q)\log_p q}.$$

Следовательно, произведение степеней всех простых чисел, не равных p, в $|G|$ не превышает n^c, где

$$c = \operatorname*{Max}_{p \leqslant k}\left(\sum_{\substack{q \neq p \\ q \leqslant k}} \alpha(p, q)\log_p q\right). \quad \blacksquare$$

Вернемся теперь к случаю неабелева цоколя. Если N является цоколем примитивной группы, потребуется следующая лемма. В этом случае не пригодны утверждения из приложения статьи [21].

Лемма 3.8. *Предположим, что множество A допускает полное транзитивное действие прямого произведения*

$$N = T_1 \times T_2 \times \ldots \times T_r$$

r неабелевых простых групп. Тогда $|A| \geqslant 5^r$.

Доказательство. Результат верен для $r = 0$ или 1 (если $r = 0$, то под N понимается 1). Предположим теперь, что $r \geqslant 2$ и результат верен для групп, имеющих меньше чем r простых факторов. Для заданного i орбиты T_i образуют блоки импримитивности N и у всех них одинаковая мощность. Предположим, что T_1 имеет кратчайшие орбиты. Пусть

$$A = B_1 \cup \ldots \cup B_m$$

является декомпозицией по T_1-орбитам. Обозначим через K подгруппу N, стабилизирующую любой из блоков B_i. Так как подгруппа K нормальна в группе N, то она состоит из прямого произведения некоторых T_i [12, предложение 1.9.12]. Без потери общности можно считать, что $K = T_1 \times \ldots \times T_s$ для некоторого $s \geqslant 1$.

Положим

$$K' = T_{s+1} \times \ldots \times T_r.$$

Тогда $K' \cong N/K$ действует полно и транзитивно на m-элементном множестве $\{B_i\}_{1 \leqslant i \leqslant m}$. По предложению индукции $m \geqslant 5^{r-s}$. Рассмотрим два случая.

Случай 1. $s = 1$. Поскольку T_1 действует полно на B_1, то $|B_1| \geqslant 5$. Поэтому $n = |B_1| m \geqslant 5 \cdot 5^{r-1} = 5^r$.

Случай 2. $s > 1$. Положим

$$K'' = T_2 \times \ldots \times T_s.$$

Мы утверждаем, что K'' действует полно на B_1. Для того чтобы показать это, предположим, что $\sigma \in K''$ оставляет неподвижной каждую точку B_1. Для любого i, $2 \leqslant i \leqslant m$, существует некоторый элемент $\tau \in K'$, такой что $\tau(B_1) = B_i$. Поскольку σ, τ коммутируют, то получаем, что σ также оставляет неподвижной каждую точку B_i. Тогда $\sigma = 1$, что и доказывает утверждение. Так как T_1 имеет кратчайшие орбиты, то K'' действует транзитивно на B_1. Следовательно, T_1 и K'' являются точно представимыми как коммутирующие транзитивные подгруппы $\mathrm{Sym}(B_1)$. Используя [26, разд. 4], получаем $T_1 \cong K''$ и $|B_1| = |T_1|$. Поэтому $s = 2$ и $|B_1| \geqslant 60$. В этом случае $n = |B_1| m \geqslant 60 \cdot 5^{r-2} > 5^r$. $\blacksquare$

В случае неабелева цоколя докажем более сильный результат, чем предложение 3.5.

Предложение 3.9. *Существует вычисляемая константа c $(c = c(k))$, такая, что если $G \subseteq S_n$ примитивна, имеет неабелев цоколь и $G \in \Gamma_k$, то $|G| \leqslant n^c$.*

Доказательство. Цоколь равен $N = T_1 \times \ldots \times T_r$, где T_i — изоморфные неабелевы простые группы. Рассмотрим действие G на N посредством внутренних автоморфизмов, и пусть K — его ядро, т. е. централизатор N. Поскольку подгруппа N нормальна в G, то если бы она была нетривиальной, то ее пересечение с цоколем также должно быть нетривиальным. Но это невозможно, поскольку N имеет тривиальный центр. Следовательно, G изоморфна подгруппе $\mathrm{Aut}(N)$. Причина для подчеркивания этого вложения G заключается в том, что структура $\mathrm{Aut}(N)$ совершенно ясна. Из того что T_i — единственные минимальные нормальные подгруппы N [12, предложение 1.9.12], следует, что любой автоморфизм N состоит из перестановки этих факторов, за которой следует некоторый автоморфизм в каждом факторе. Другими словами, G является подгруппой

$$\mathrm{Aut}(N) \cong \mathrm{Aut}(T_1) \mathrm{wr}\, S_r$$

(«wr» обозначает операцию сплетения [10, 12]). Но поскольку в $|G|$ входят лишь простые числа, не превышающие k, то проекция G на S_r имеет порядок не более a^r, где a есть функция одного лишь k. Следовательно,

$$|G| \leqslant |\mathrm{Aut}(T_1)|^r a^r.$$

Порядок $|\mathrm{Aut}(T_1)|$ ограничен, так как $G \in \Gamma_k$ и $T_1 \subseteq S_k$. Поэтому $|G \leqslant b^r$ для $b = b(k)$. С другой стороны, из леммы 3.8 следует, что $n \geqslant 5^r$. Следовательно, $|G| \leqslant n^{\log_5 n}$. ∎

Доказательство предложения 3.5 является непосредственным следствием предложений 3.7 и 3.9. Для случая неабелева цоколя можно использовать любую силовскую подгруппу, даже единичную.

3.3. Нахождение p-подгруппы

В предыдущих разделах было установлено, что для некоторых классов групп перестановок гарантировано существование силовских p-подгрупп небольшого индекса. Вопрос о том, можно ли найти образующие таких подгрупп за полиномиальное время, остается открытым. Этот вопрос похож на задачу, о которой идет речь в лемме 1.2 (iii). Трудности заключаются в том, что определение «P является силовской p-подгруппой» не определяет P однозначно и поэтому не дает эффективного теста на установление принадлежности. Однако для заданной (образующими) некоторой p-подгруппы P и элемента $\sigma \in G$ легко установить, учитывая, является ли порядок $\langle \sigma, P \rangle$ степенью p, принадлежат ли σ и P общей силовской p-подгруппе. Именно это используется для доказательства следующего результата.

Предложение 3.10. *Для фиксированного c существует полиномиальный по времени алгоритм нахождения образующих силовской p-подгруппы $G \subseteq S_n$, при условии, что $|G| = p^s m$ и $m \leqslant n^c$.*

Начинаем с алгоритма. Построим сразу множество Π образующих силовской p-подгруппы P и полное множество C представителей левых классов смежности группы G по подгруппе P. Начнем с

$$\Pi \leftarrow \varnothing, \quad C \leftarrow \{1\}, \quad P \leftarrow 1.$$

Далее используем следующую подпрограмму. На вход поступает α — элемент группы G.

procedure p-Построение (α)
 if для некоторого $\gamma \in C$, $\langle \gamma^{-1}\alpha, \Pi \rangle$ является p-группой
  then if $\langle \gamma^{-1}\alpha, \Pi \rangle = P$
   then return
   else добавить $\gamma^{-1}\alpha$ к Π и положить $P = \langle \Pi \rangle$
  else добавить α к C
 returne

Пусть Φ — данное множество образующих G. Мы вызываем процедуру p-Построение (α) для всех α из ΦC. Ясно, что в результате таких вызовов будет увеличиваться множество C. Однако в любой момент построения $P = \langle \Pi \rangle$ является p-группой и элементы C попарно не конгруэнтны по любой силовской p-подгруппе, содержащей P. В частности, в C существует не более чем m элементов. Поэтому весь процесс заканчивается за полиномиальное время. Когда происходит остановка, $\Phi C \subseteq CP$, и поэтому CP замкнуто относительно левого умножения на Φ. Отсюда $CP = G$. Итак, поскольку $\langle \gamma, P \rangle$ не является p-группой для любого $\gamma \in C$ и $\gamma \neq 1$, то P есть силовская p-подгруппа. ∎

На самом деле ситуация, которая возникает при построении алгоритма нахождения цветных автоморфизмов, охватывается следующим результатом.

Предложение 3.11. *Предположим, что $G \subseteq \mathrm{Sym}(A)$ и $G \in \Gamma_k$. Пусть B — G-орбита в A. Тогда минимальную систему G-блоков в B*

$$B = B_1 \cup B_2 \cup \ldots \cup B_m$$

и подгруппу P группы G индекса, не превышающего $m^{c(k)}$, такую что P действует как p-группа на семействе $\{B_1, B_2, \ldots, B_m\}$, можно найти за полиномиальное время.

Доказательство. Так как G действует примитивно на блоках, то, согласно предложению 3.5, такая подгруппа P существует. Можно найти ее, например, модифицируя алгоритм предложения 3.10 так, чтобы он проверял, действует ли $\langle \gamma^{-1}\alpha, \Pi \rangle$ как p-группа на семействе блоков. ∎

3.4. Алгоритм нахождения цветных автоморфизмов для групп из Γ_k

Мы будем следовать обозначениям разд. 2.2 и 3.2.

Задача 3 обобщается следующим образом.

Задача 4. Дано: Образующие подгруппы G группы $\mathrm{Sym}(A)$, где $G \in \Gamma_k$, G-устойчивое подмножество B и $\sigma \in \mathrm{Sym}(A)$. *Найти*: $C_B(\sigma G)$.

Как и прежде, если B есть объединение непересекающихся G-устойчивых подмножеств B', B'', то

$$\mathscr{C}_B(\sigma G) = \mathscr{C}_{B''}\mathscr{C}_{B'}(\sigma G).$$

Если это не так, то найдем минимальную систему G-блоков в B

$$B = B_1 \cup B_2 \cup \ldots \cup B_m.$$

На этот раз мы не имеем m в своем распоряжении. Вместо этого, воспользовавшись предложениями 3.5 и 3.11, определим подгруппу P с индексом $[G:P] \leqslant m^c$ так, что P действует как p-группа на семействе блоков $\mathscr{B} = \{B_1, \ldots, B_m\}$. Если записать G как объединение не более чем m^c классов смежности P

$$G = \bigcup_i \tau_i P$$

(τ_i входит «для свободы» при построении P), то задача разобьется аналогично:

$$\mathscr{C}_B(\sigma G) = \bigcup_i \mathscr{C}_B(\sigma \tau_i P).$$

Продолжим теперь на каждом классе смежности P, но при этом для того, чтобы воспользоваться леммой 1.1, мы будем сохранять целостность индивидуальных блоков B_i как можно дольше. Более точно, принцип «разделяй и властвуй» применяется к действию P на $\mathscr{B}$ (p-групповое действие), а не на B. Поэтому если $\mathscr{B}$ — непересекающееся объединение P-устойчивых подсемейств $\mathscr{B}'$ и $\mathscr{B}''$, то задача решается последовательно для этих подсемейств. Если это не так, то находим минимальную систему P-блоков на $\mathscr{B}$. Теперь такая система будет состоять точно из p подсемейств и подгруппы P, имеющей индекс p и стабилизирующей все подсемейства. Итак, в транзитивном случае задача для P на $\mathscr{B}$ разбивается на p^2 аналогичных задач для подгрупп P на подсемействах мощности $|\mathscr{B}|/p$. Каждая из них в худшем случае эквивалентна p^2 аналогичных задач для подсемейств мощности $|\mathscr{B}|/p^2$ и т. д. Мы продолжим подобным образом до тех пор, пока подсемейство не будет состоять в точности из одного из исходных блоков B_i. Исчерпав p-групповое действие, мы встретимся, наконец, с задачей

вида $\mathscr{C}_{B_i}(\bar{\sigma}\bar{P})$, где $\bar{P}$ — остаточная группа. Однако, теперь $|B_i| = |B|/m$. Теперь важно отметить, что задача для каждого класса смежности преобразуется в самое большое m^2 задач на множествах мощности $|B|/m$. Следовательно, исходная задача для G на B была разбита на самое большое $m^c \cdot m^2 = m^{c+2}$ подзадач на множествах мощности $|B|/m$. Результаты разд. 1.2 и 1.3 гарантируют, что сложность каждого сведения ограничена полиномом от n, подтверждая тем самым утверждение в заголовке статьи.

Ниже будет описан алгоритм для нахождения $\mathscr{C}_B(\sigma G)$. Особый подход к P позволяет удобно описать вычисления в двух подпрограммах; одна — для $\mathscr{C}_B(\sigma G)$ и другая для

$$\hat{\mathscr{C}}_{\mathscr{B}}(\sigma P) = \mathscr{C}_{\mathscr{B}}(\sigma P),$$

причем про P известно, что она действует как p-группа на семействе $\mathscr{B} = \{B_1, \ldots, B_m\}$ и $B = \bigcup_i B_i$. Читатель, вероятно, уже заметил, что у этих подпрограмм имеется общее обобщение.

I. Вычисление $\mathscr{C}_B(\sigma G)$

Вход: Раскрашенное множество A, образующие группы $G \subseteq \mathrm{Sym}(A)$, $\sigma \in \mathrm{Sym}(A)$, G-устойчивое множество B.

Выход: $\mathscr{C}_B(\sigma G)$.

Метод:

(i) Если $B = \{b\}$, то

$$\mathscr{C}_B(\sigma G) = \begin{cases} \varnothing, & \text{если } \sigma(b) \not\sim b; \\ \sigma G, & \text{если } \sigma(b) \sim b. \end{cases}$$

(ii) Если B — объединение непересекающихся G-устойчивых подмножеств B' и B'', то

$$\mathscr{C}_B(\sigma G) = \mathscr{C}_{B'}\mathscr{C}_{B''}(\sigma G).$$

(iii) Если G транзитивно на B и $|B| > 1$, то найдем минимальную систему G-блоков в

$$B = B_1 \cup \ldots \cup B_m.$$

Выберем подгруппу P, такую что P действует как p-группа на $\mathscr{B} = \{B_1, \ldots, B_m\}$ и $[G:P] \leqslant m^c$. Разобьем группу G,

$$G = \bigcup_i \tau_i P.$$

Тогда получаем

$$\mathscr{C}_B(\sigma G) = \bigcup_i \hat{\mathscr{C}}_{\mathscr{B}}(\sigma \tau_i P).$$

II. Вычисление $\widehat{\mathscr{C}}_{\mathscr{B}}(\sigma P)$

Вход: Раскрашенное множество A, образующие группы $P \subseteq \mathrm{Sym}(A)$, $\sigma \in \mathrm{Sym}(A)$, P-устойчивое семейство $\mathscr{B}$ непересекающихся подмножеств A с $\bar{P}$, действующей как p-группа на $\mathscr{B}$.

Выход: $\widehat{\mathscr{C}}_{\mathscr{B}}(\sigma\bar{P})$

Метод:

(i) Если $\mathscr{B} = \{B_0\}$, то $\widehat{\mathscr{C}}_{\mathscr{B}}(\sigma P) = \mathscr{C}_{B_0}(\sigma P)$.

(ii) Если $\mathscr{B}$ — объединение P-устойчивых подсемейств $\mathscr{B}'$ и $\mathscr{B}''$, то

$$\widehat{\mathscr{C}}_{\mathscr{B}}(\sigma P) = \widehat{\mathscr{C}}_{\mathscr{B}'}\widehat{\mathscr{C}}_{\mathscr{B}''}(\sigma P),$$

(iii) Если P транзитивна на $\mathscr{B}$ и $|\mathscr{B}| > 1$, то найдем минимальную систему p-блоков на $\mathscr{B}$

$$\mathscr{B} = \mathscr{B}_1 \cup \ldots \cup \mathscr{B}_p.$$

Выберем подгруппу P', которая стабилизирует все подсемейства $\mathscr{B}_i$. Разобьем P:

$$P = \bigcup_{i=1}^{p} \tau_i P'.$$

Тогда

$$\widehat{\mathscr{C}}_{\mathscr{B}}(\sigma P) = \bigcup_{i=1}^{p} \widehat{\mathscr{C}}_{\mathscr{B}}(\sigma\tau_i P').$$

(Части правой стороны также входят в (ii).)

Замечание. Еще раз подчеркнем, что лемма 2.4 гарантирует возможность комбинировать решения подзадач из I (iii) или II (iii) в единственный класс смежности. Если результатом являются несколько непустых решений подзадач, то все они могут быть классом смежности одной и той же подгруппы, и нужно добавить их к смежному классу группы, т. е. объединение

$$\bigcup_{i=1}^{s} \rho_i H$$

можно представить в виде

$$\rho_1 \langle H, \{\rho_1^{-1}\rho_i\}_{1<i\leqslant s}\rangle.$$

4. ЗАМЕЧАНИЯ

4.1. Более быстрый алгоритм для кубических графов

Алгоритм для установления изоморфизма кубических графов представлен здесь таким способом, который четко подтверждает утверждение о полиномиальности времени его работы и легко обобщается. С несколько большими усилиями можно предложить ряд специальных модификаций, которые повышают его эффективность. Имеющийся наилучший алгоритм для распознавания, изоморфны ли два связных n-вершинных кубических графа, требует $O(n^5)$ шагов [17].

4.2. Пересечение групп

Общая задача о нахождении цветных автоморфизмов сводима за полиномиальное время к следующей задаче о пересечении групп:

Дано: Образующие групп $G, H \subseteq \mathrm{Sym}(A)$.

Найти: Образующие $G \cap H$.

Задача о нахождении цветных автоморфизмов является частным случаем, в котором H есть прямое произведение симметрических групп на компонентах разбиения A. (В работе [16] показано, что в общей постановке эти задачи по времени полиномиально эквивалентны.) Следовательно, основной алгоритм статьи решает также и задачу о пересечении для таких групп: ограниченного H и G из класса Γ_k. Но если G принадлежит Γ_k, то ограничения на H могут быть сняты с сохранением полиномиальности времени.

Приведем набросок доказательства. Рассмотрим прямое произведение $\mathrm{Sym}(A) \times \mathrm{Sym}(A)$. Существуют два естественных действия этих групп на A, когда используются соответственно проекции pr_1 и pr_2 на факторы, т. е.

$$\mathrm{pr}_1(\alpha, \beta) = \alpha, \quad \mathrm{pr}_2(\alpha, \beta) = \beta.$$

Эти обозначения используются в обобщении задачи, которое опять допускает рекурсию.

Дано: Образующие $K \subseteq \mathrm{Sym}(A) \times \mathrm{Sym}(A)$ с $\mathrm{pr}_1(K) \in \Gamma_k$; $\mathrm{pr}_1(K)$ — устойчивое подмножество B множества A, $\sigma \in \in \mathrm{Sym}(A) \times \mathrm{Sym}(A)$.

Найти: $\mathscr{J}_B(\sigma K) = \{\tau \in \sigma K \mid \mathrm{pr}_1(\tau)\,|_B = \mathrm{pr}_2(\tau)\,|_B\}$.

В частности,

$$\mathscr{J}_A(G \times H) = \{(\alpha, \alpha)\,(\alpha \in G \cap H\}.$$

Так как хорошие гипотезы касаются лишь pr_1-действия, то продолжим по принципу «разделяй и властвуй» (орбиты, блоки и др.), используя это действие. Сведéние к основному случаю $|B| = 1$ выполняется так, как в разд. 3. В этом случае мы видим, что задача в точности заключается в нахождении для некоторых фиксированных элементов b, c остаточной группы K, отображающих b на c с помощью pr_2-действия. Тогда решением является или пустое множество, или класс смежности стабилизатора элемента b.

4.3. Другие приложения задачи установления изоморфизма

Основные идеи разд. 3 и 4.2 применимы к решению задачи установления изоморфизма целого ряда классов графов. Например:

(i) Раскрашенные графы с ограниченными одноцветными классами — класс графов, рассмотренный Бабаи в [2], — также охватываются алгоритмом цветных автоморфизмов (все «цвета» различны) групп из Γ_k. Требуется лишь изменить сведéние, изложенное во введении, когда вместо S_n в качестве исходной группы берется прямое произведение симметрических групп одноцветных классов (элемент Γ_k, где k — заданная граница). Хотя тем самым задача относится к классу P, но алгоритм работает уже не столь быстро, как исходный.

(ii) Изоморфизм турниров также может быть установлен за время $n^{\log n}$ [5]. В доказательстве этого результата используется другой способ сведéния к задаче о нахождении цветных автоморфизмов, а также тот факт, что турниры имеют нечетный порядок, и вследствие этого их группы автоморфизмов разрешимы.

(iii) Изоморфизм (v, k, λ)-схем для ограниченных λ может быть установлен за время $n^{\log\log n}$. Заметим, что случай $\lambda = 1$ соответствует проективным плоскостям, и это обобщает результат Миллера [19]. Важно заметить, что в указанном классе число общих соседей пар точек ограниченно. Этот и связанные с ним результаты будут опубликованы позже.

(iv) Недавно мы узнали, что В. Н. Земляченко использовал методы этой статьи для установления верхней оценки $\exp(n^{1-c})$ для некоторого положительного c в общей задаче установления изоморфизма графов. См. работу [3] для ознакомления с результатом Земляченко.

4.4. Новые результаты о примитивных группах перестановок

В нашей более ранней аннотации [15] основного результата этой статьи мы указывали на новый результат Палфи [20], который показал, что примитивные разрешимые группы имеют полиномиально ограниченный порядок. Это и другие соображения побудили нас предположить, что примитивные группы в Γ_k, когда k фиксировано, также являются полиномиально ограниченными. И нам приятно было узнать, что эта гипотеза была подтверждена Бабаи — Камероном — Палфи [4]. На самом деле они ослабили нашу гипотезу, получив ограниченность лишь неабелевых композиционных факторов. Это означает, что

более простой вариант нашего основного алгоритма также требует полиномиального времени. Это является более очевидным обобщением случая 2-групп. Когда мы приходим к группе G, действующей примитивно на m блоках, можно сразу же перейти к подгруппе H, стабилизирующей блоки и задать G как объединение классов смежности H. И оказывается, что индекс $[G:H]$ ограничен полиномом степени m. Мы без предубеждения отметим, что алгоритм разд. 3 работает быстрее.

Мы отсылаем читателя также к работе [6], где Камерон делает заключение о порядках примитивных групп, используя недавно законченную классификацию простых групп. В частности, он приводит результаты о структуре примитивных групп в S_n, в которых больше чем $n^{\log n}$ элементов. Например, они содержат большие знакопеременные группы. Поэтому на класс групп можно наложить различные допущения, чтобы избежать «больших» групп и гарантировать субэкспоненциальный алгоритм нахождения пересечения. Вероятно, что будут найдены также и другие приложения в изучении сложности задач.

4.5. Распознавание принадлежности к Γ_k

Хотя нужды в этом результате здесь нет, возникает естественный вопрос, является ли задача проверки принадлежности к Γ_k (k фиксировано) разрешимой за полиномиальное время (для групп перестановок). Это действительно так.

Для доказательства отметим, что если G принадлежит Γ_k, то любая максимальная нормальная подгруппа G имеет индекс не больше $b = k!$. С учетом этого приведем сначала набросок процедуры, которая при вводе G будет возвращать собственную нормальную подгруппу N индекса не больше b или вывод «G не принадлежит Γ_k». Возьмем любые $b+1$ различных элементов G, скажем $\alpha_0, \ldots, \alpha_b$. Следовательно, если G имеет нормальную подгруппу индекса не больше b, то некоторые два из выбранных элементов должны быть эквивалентны по модулю этой подгруппе. Поэтому порождаем нормальные замыкания [9] N_{ij} для $\langle \alpha_i \alpha_1^{-1} \rangle$ при условии $i \neq j$. Если $N_{ij} = G$ для всех i, j, то G не имеет нормальной подгруппы индекса b и G не принадлежит Γ_k. В противном случае выбирается собственная нормальная подгруппа N'. Если $[G:N'] > b$, то продолжим этот процесс следующим образом. Возьмем любые $b+1$ элементов G, скажем $a_0, \ldots, a_b$, которые попарно неконгруэнтны по подгруппе N'. Если G принадлежит Γ_k, то N' содержится в собственной нормальной подгруппе индекса не больше b. После этого порождаем нормальные замыкания $\langle \alpha_i, \alpha_1^{-1}, N' \rangle$. Если ни одно из них не является собственным, G не принадлежит

Γ_k; в противном случае получаем бо́льшую собственную нормальную группу, чем N', и этот процесс продолжается аналогично.

Используем вышеприведенную процедуру для установления принадлежности G к Γ_k. Если возвращена подгруппа N индекса не больше b, то проверяем принадлежность G/N к Γ_k (в точном смысле разд. 3.1) прямым образом. Если G/N принадлежит Γ_k, то достаточно проверить N, и так далее.

Существует другая полиномиальная по времени процедура для проверки принадлежности к Γ_k, о которой стоит упомянуть. Ее легко описать, но описание зависит от результата Бабаи — Камерона — Палфи, указанного в 4.4. Сведем задачу к транзитивному случаю (проверим N, ядро действия на орбите B, и проверим образ G/N группы G в $\mathrm{Sym}(B)$), а затем к примитивному случаю (проверка N, стабилизатора блоков, и проверка действия G/N на множестве блоков). Если G принадлежит Γ_k, то она должна быть достаточно мала для непосредственной проверки.

Любой из этих алгоритмов может быть изменен по выводу, для G из Γ_k, композиционным рядом. Интересно знать, можно ли это использовать в другом алгоритме для нахождения $G \cap H$. Например, предположим, что N — максимальная нормальная подгруппа G и что пересечение $N \cap H$ найдено. Известно, что $G \cap H/N \cap H$ является подгруппой G/N. Предположим, что известно, какая была подгруппа (существует лишь ограниченное число возможностей). Можно ли это использовать для получения $G \cap H$?

Отметим, наконец, что у нас имеется более общий алгоритм, который за полиномиальное время строит композиционный ряд любой группы перестановок. Он требует классификации простых групп, только лишь для гипотезы Шрейера (внешний групповой автоморфизм конечной простой группы разрешим). Этот результат также будет опубликован.

4.6. Нахождение силовских подгрупп

В разд. 3.3 мы имели дело с частным случаем, в котором силовские p-подгруппы могли быть найдены за полиномиальное время. Общая задача нахождения силовских p-подгрупп представляет независимый интерес, и сложность ее решения неизвестна. Связанной с ней, но, возможно, более легкой задачей является нахождение какого-нибудь элемента, имеющего порядок p (для простого p, делящего $|G|$). Если p фиксировано (т. е. ограничено), то можно рассмотреть G-действие на A^p; найти любой пример некоторого $(a_2, \ldots, a_p, a_1)$ в орбите $(a_1, \ldots, a_p)$ и взять любой элемент σ из G, отображающий

единицу в другой элемент (соответствующая степень σ имеет порядок точно p). В случае произвольного p лучшее, что можно сейчас указать, это время $n^{\log n}$. Этот алгоритм, кроме прочего, использует указанный выше общий алгоритм композиционных факторов. Даже в этом случае мы не знаем субэкспоненциального способа обобщения алгоритма для получения силовских p-подгрупп.

4.7. Удостоверения (certificates)

«Удостоверением» графа является полный инвариант класса изоморфных графов, например min lex матрицы смежности. В большинстве известных случаев алгоритмов установления изоморфизма графов, удостоверения строятся не сложно [18, 14]. В работе [2] Бабаи спрашивает, может ли теоретико-группой подход быть использован для ответа на этот потенциально более полезный вопрос. Автором этой статьи и П. Клинбергом [13] был дан утвердительный ответ для графов Бабаи. Мы, однако, не знаем, можно ли распространить подход настоящей статьи для нахождения удостоверения для графов с ограниченными степенями вершин. Заметим, что отношение между сведе́нием общей задачи установления изоморфизма графов к задаче о цветных автоморфизмах и сведе́нием разд. 2.1 и 3.1 имеет аналог для удостоверений. Удостоверение для произвольного графа может быть найдено с помощью алгоритма решения следующей задачи:

Дано: Образующие для $G \subset S_n$, n-разрядное двоичное число m.

Найти: Наибольшее число в G-орбитах m, когда S_n действует на n-разрядные числа, осуществляя перестановку разрядов.

Можно, например, применить такой алгоритм к действию S_n на матрицы смежности, $A \mapsto PAP'$ (P — матрица перестановок). Приемы, подобные предложенным здесь, могут быть использованы для получения удостоверений графов с ограниченными степенями вершин из решения вышеприведенной задачи для групп из Γ_k. Однако сложность этой задачи неизвестна даже в случае 2-групп.

БЛАГОДАРНОСТИ

Автору очень приятно выразить свою благодарность за радушный прием факультету вычислительной математики Корнельского университета, где он в захватывающих дискуссиях с Дж. Хопкрофтом узнал много интересного об изоморфизме и других вещах. Я также должен поблагодарить Л. Бабаи и

Т. Клингсберга за стимулирующие обсуждения и переписку в ходе развития идей, лежащих в основе данной статьи.

Замечание при корректуре. Сделаем несколько последних замечаний к разд. 4. Оценка $O(n^5)$ для кубических графов (разд. 4.1) была улучшена сначала до $O(n^4 \log n)$ К. Шнорром и А. Вебером, затем до $O(n^4)$ К. Хоффманом и, наконец, недавно З. Галилом, Е. Лаксом, К. Шнорром и А. Вебером до $O(n^3 \log n)$.

Оценка В. Н. Земляченко для сложности нахождения решения общей проблемы установления изоморфизма графов (разд. 4.3) была $\exp(n^{3/4+o(1)})$. Бабаи сначала улучшил ее до $\exp(n^{2/3+o(1)})$, а затем автор до $\exp(n^{1/2+o(1)})$. Последнее улучшение существенно использует более быстрый $(O(n^{cd \log d}))$ алгоритм для графов со степенями d.

Нами показано, что задача, сформулированная в разд. 4.7, является NP-трудной, даже если G — элементарная абелева 2-группа.

ЛИТЕРАТУРА

[1] ATKINSON M. D. An algorithm for finding the blocks of a permutation group, Math. Comp. **29** (1975), 911—913.
[2] BABAI L. Monte-Carlo algorithms in graph isomorphism testing, manuscript, 1979.
[3] BABAI L. Moderately exponential bound for graph isomorphism, in «Proceedings Conf. on Fund. Comp. Thy., Szeged (1981»,) Lecture Notes in Computer Science, Springer-Verlag, Berlin/New York, in press.
[4] BABAI L., CAMERON P. J., PALEY P. On the order of primitive permutation groups with bounded nonabelian composition factors, to appear.
[5] BABAI L., LUKS E. A subexponential algorithm for tournament isomorphism, to appear.
[6] CAMERON P. J. Finite permutation groups and finite simple groups, Bull. London Math. Soc. **13** (1981), 1—22.
[7] CARTER R., FONG P. The Sylow 2-subgroups of the finite classical groups, J. Algebra **1** (1964), 139—151.
[8] FURST M., HOPCROFT J., LUKS E. «A Subexponential Algorithm for Trivalent Graph Isomorphism», Tech. Report 80—426, Computer Science, Cornell Univ., 1980.
[9] FURST M., HOPCROFT J., LUKS E. Polynomial-time algorithms for permutation groups, in «21st IEEE Symp. on Foundations of Comp. Sci. (1980)», pp. 36—41.
[10] HALL M., «The Theory of Groups», Macmillan Co., New York, 1959. [Имеется перевод: Холл М. Теория групп. — М.: ИЛ, 1962.]
[11] HOFFMAN C. M. Testing isomorphism of cone graphs, in «Proc. 12th Symp. Thy. Comp.», pp. 244—251, ACM, New York, 1980.
[12] HUPPERT B. «Endliche Gruppen 1», Springer-Verlag, Berlin, 1967.
[13] KLINGSBERG P., LUKS E. Succinct certificates for a class of graphs, to appear.
[14] LIPTON R. J. The beacon set approach to graph isomorphism, SIAM J. Comput. **9** (1980).
[15] LUKS E. Isomorphism of graphs of bounded valence can be tested in polynomial time, in «21st IEEE Symp. Found. Comp. Sci. (1980)», pp. 42—49.

[16] LUKS E. The complexity of permutation group problems, to appear.
[17] LUKS E. A faster algorithm for trivalent graph isomorphism, to appear.
[18] MILLER G. Graph isomorphism, general remarks, J. Comput. System Sci. **18** (1979), 128—142.
[19] MILLER G. L. On the $n^{\log n}$ isomorphism technique, in «Proc. 10th Symp. Thy. Comp.», pp. 51—58, ACM, New York, 1978.
[20] PALEY P. P. A polynomial bound for the orders of primitive solvable groups, to appear.
[21] SCOTT L. L. Representation in characteristic p, in «The Santa Cruz Conference on Finite Groups», pp. 319—332, Amer. Math. Soc., Providence, R. I., 1980.
[22] SIMS C. C. Graphs and finite permutation groups, Math. Z. **95** (1967), 76—86.
[23] SIMS C.C. Computational methods for permutation groups, in «Computational Problems in Abstract Algebra», pp. 169—184, Pergamon, Oxford, 1970.
[24] SIMS C. C. «Some Group-Theoretic Algorithms», Lecture Notes in Math. No. 697, Springer-Verlag, Berlin, pp. 108—124, 1978.
[25] WEIR A. J. Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p, Proc. Amer. Math. Soc. **6** (1955), 529—533.
[26] WIELANDT H. «Finite Permutation Groups», Academic Press, New York, 1964.

Примечание редактора перевода

Обобщения данного результата получены в статье И. Н. Пономаренко («Полиномиальный алгоритм изоморфизма для графов, не стягиваемых на $K_{3,g}$.». — Записки ЛОМИ АН СССР, 1984, 137, 99 — 114) и в работах Миллера (G. L. Miller. «Isomorphism of k-contractible graphs. A generalization of bounded valence and bounded genus.».— Information and Control 1983, 56, No. 1—2, 1—20; «Isomorphism of graphs which are pairwise k-separable.» — Information and Control, 1983, 56, No. 1—2, 21—33). Описание этих результатов можно найти в обзоре В. П. Козырева и С. В. Юшманова «Теория графов (алгоритмические, алгебраические и метрические проблемы).», сер. «Итоги науки», 1985, т. 23, с. 68—117. — *В. Козырев.*