Точность и сложность вычислений, необходимые для проверки изоморфизма графов сравнением полиномов

А. В. Пролубников
[1]Омский государственный университет
*Контактный e-mail: a.v.prolubnikov@mail.ru

В работе обоснована возможность численной реализации проверки изоморфизма графов с помощью её сведения к проверке равенства модифицированных характеристических полиномов графов. Показывается, что при достаточно больших значениях параметра алгоритма, использующего такое сведение, вероятность ошибки при решении им задачи проверки изоморфизма графов пренебрежимо мала. Доказывается, что для графов на n вершинах необходимое для численной реализации сравнение значений их модифицированных характеристических полиномов, имеющих экспоненциальное от n количество коэффициентов, может быть проведено за время $O(n^4)$ при растущей как $O(n^2)$ длине мантиссы используемых машинных чисел.

Ключевые слова: изоморфизм графов, вычислительная сложность, точность вычислений

Введение

В задаче проверки изоморфизма графов (далее «задача ИГр») даны два невзвешенных неориентированных помеченных графа без петель (два обыкновенных графа) G и H. $V(G)$, $V(H)$ — множества вершин этих графов, $V(G) = V(H) = \{1, \ldots, n\}$ ($|V(G)| = |V(H)| = n$), $E(G)$, $E(H)$ — множества их рёбер. Необходимо проверить, существует ли биекция $\varphi : V(G) \to V(H)$ такая, что

$$(i, j) \in E(G) \quad \Leftrightarrow \quad (\varphi(i), \varphi(j)) \in E(H).$$

Если биекция φ существует, то графы G и H *изоморфны* (обозначается «$G \simeq H$»), иначе — не изоморфны. Для решения задачи необходимо либо представить такую биекцию, называемую *изоморфизмом*, либо доказать её отсутствие.

Задача может быть поставлена в матричной формулировке. Пусть $(A)_{ij}$ обозначает ij-й элемент матрицы A. *Матрицей смежности* графа G называется матрица $A(G)$ размерности $n \times n$, элементы которой определяются следующим образом:

$$(A(G))_{ij} = \begin{cases} 1, & \text{если } (i, j) \in E(G), \\ 0, & \text{иначе.} \end{cases}$$

Пусть S_n обозначает симметрическую группу на множестве из n элементов. Биективному отображению $\varphi : V(G) \to V(H)$ может быть однозначно поставлена в соответствие

перестановка $\varphi \in S_n$. P_φ — матрица, соответствующая перестановке φ:

$$(P_\varphi)_{ij} = \begin{cases} 1, & \text{если } i = \varphi(j), \\ 0, & \text{иначе.} \end{cases}$$

Тогда

$$G \simeq H \quad \Leftrightarrow \quad \exists \varphi \in S_n : \; A(H) = P_\varphi A(G) P_\varphi^\top.$$

Исходя из этой постановки, два графа изоморфны тогда и только тогда, когда матрица смежности одного из них может быть получена из матрицы смежности другого в результате некоторой перестановки её рядов, то есть при помощи некоторой перестановки строк матрицы, совмещённой с такой же перестановкой её столбцов.

Задача ИГр — это задача проверки того, являются ли два графа принципиально отличными друг от друга, то есть обладают структурными отличиями, определяемыми заданным на множестве вершин отношением смежности, либо эти графы эквивалентны и отличаются друг от друга только нумерацией вершин. Задачу ИГр надо решать, например, при поиске графов с заданными свойствами, используя для этого перебор на множестве всех помеченных графов. Поскольку одному непомеченному графу на n вершинах соответствует $n!$ помеченных изоморфных графов, то, не храня изоморфные графы, обладающие заданным свойством, мы сокращаем объём используемой для такого поиска памяти и производим проверку этого свойства только для одного графа из класса изоморфных.

Задача ИГр принадлежит классу *NP*, поскольку проверка того, является ли изоморфизмом некоторое биективное отображение множества вершин одного графа на множество вершин второго, может быть произведена за квадратичное относительно n время. *NP*-полнота этой задачи не доказана, в то же время полиномиальных относительно n алгоритмов решения задачи для общего случая не разработано. Задача ИГр полиномиально разрешима для планарных графов и графов с ограниченным родом [1] в целом, для графов с ограниченной кратностью собственных значений матрицы смежности графа [2], для графов с ограниченной степенью вершин [3] и некоторых других классов графов. Изоморфизм графов тем сложнее проверить, чем более регулярна их структура, — регулярные, сильно-регулярные и изорегулярные графы дают примеры задач ИГр, которые не могут быть решены имеющимися алгоритмами за полиномиальное относительно n время.

Алгоритмы решения задачи ИГр могут быть разделены на алгоритмы двух типов. Это алгоритмы, решающие задачу ИГр для графов из некоторого класса, как, например, алгоритмы для классов графов, упомянутых выше, и эвристические алгоритмы, предназначенные для решения общего случая задачи, экспоненциальные в общем случае, но обладающие небольшой вычислительной сложностью «в среднем», такие как, например, алгоритмы Уллмана [4], Шмидта-Дрюффеля [5] и NAUTY Б. МакКэя [6]. Однако, относительно простые случаи задачи ИГр могут потребовать экспоненциального времени для их решения этими алгоритмами [5, 7].

Алгоритмы решения задачи ИГр в ходе своей работы проверяют инвариантные относительно изоморфизма, то есть равные для изоморфных графов, характеристики — *инварианты* графов. Примерами инвариантов графа являются такие его характеристики, как связность, род графа, степенная последовательность, характеристический полином матрицы смежности графа и её спектр. Инвариант является *полным* инвариантом графа, если из равенства его значений для двух графов следует их изоморфизм.

Представленная в [8] и используемая в этой работе модификация характеристического полинома графа является полным инвариантом графа в том смысле, что для неизоморфных графов никакая нумерация их вершин не даёт одинаковых полиномов. Модифицированный характеристический полином — это полином от n переменных, имеющий 2^n коэффициентов, поэтому за полиномиальное время вычислить значение такого полинома в заданной точке невозможно. В этой работе показывается, что возможна численная реализация алгоритма, решающего задачу ИГр проверкой равенства значений модифицированных характеристических полиномов в заданных точках, не проводя вычислений самих этих значений. Доказывается, что для графов на n вершинах сравнение значений их модифицированных характеристических полиномов от n переменных может быть реализовано за время $O(n^4)$ при растущей как $O(n^2)$ длине мантиссы используемых машинных чисел.

1. Модифицированный характеристический полином графа

Характеристический полином графа G — это полином

$$\chi_G(x) = \det(A(G) - xE),$$

где x — переменная, E — единичная матрица. Значение $\chi_G(x)$ представляет собой зависящий от переменной x ориентированный объём n-мерного параллелепипеда, стороны которого заданы вектор-столбцами матрицы $A(G)-xE$.

В [9, 10, 11] представлены модификации характеристического полинома графа, включая полиномы от нескольких переменных. Эти модификации характеристического полинома не являются полными инвариантами графа. Переменные в этих полиномах никак не связаны с вершинами графа. Мы модифицируем характеристический полином графа $\chi_G(x)$ для графа на n вершинах, переходя от полинома от одной переменной к полиному от n переменных так, что вершине $i \in V(G)$ соответствует переменная x_i. Пусть далее $x_1, \ldots, x_n$ — независимые переменные, $X = \mathrm{diag}(x_1, \ldots, x_n)$ — диагональная матрица с элементами x_i на диагонали.

Определение. $\eta_G(x_1, \ldots, x_n)$ — полином следующего вида:

$$\eta_G(x_1, \ldots, x_n) = \det(A(G) + X). \tag{1}$$

Если из равенства характеристических полиномов двух графов не следует того, что графы изоморфны, то, как будет показано далее, изоморфизм графов следует из равенства их модифицированных характеристических полиномов при некоторой перенумерации вершин одного из графов. То есть два графа изоморфны тогда и только тогда, когда существует такая перенумерация вершин, при которой объёмы, задаваемые для них по (1) и являющиеся функциями от n независимых переменных, равны при всех возможных значениях переменных.

Пусть c — некоторое подмножество элементов из $V(G)$. Через x_c обозначим произведение вида $\prod_{i \in c} x_i$. Коэффициент $A(G)_c$ перед этим произведением в полиноме $\eta_G(x_1, \ldots, x_n)$ — это определитель подматрицы $A(G)$, получаемой из $A(G)$ удалением рядов с номерами, принадлежащими подмножеству c. Для подмножества c и отображения $\varphi : V(G) \to V(H)$, соответствующего перестановке $\varphi \in S_n$, через $\varphi(c)$ обозначим множество образов элементов из c. Для $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ точка $x_\varphi = (x_{\varphi(1)}, \ldots, x_{\varphi(n)})$

— это точка, полученная перестановкой координат x в соответствии с φ. Верна следующая

Теорема 1. *$G \simeq H$ и $\varphi : V(G) \to V(H)$ — изоморфизм тогда и только тогда, когда*

$$\eta_G(x_1, \ldots, x_n) \equiv \eta_H(x_{\varphi(1)}, \ldots, x_{\varphi(n)}). \tag{2}$$

Замечание. Равенство (2) имеет место тогда, когда равны коэффициенты полиномов η_G и η_H при произведениях переменных, соответствующих друг другу по φ, то есть коэффициент $A(G)_c$ перед произведением $\prod_{i \in c} x_i$ равен коэффициенту $A(H)_{\varphi(c)}$ перед произведением $\prod_{i \in c} x_{\varphi(i)}$.

Доказательство. Если $G \simeq H$ и φ — изоморфизм, то выполняется (2), поскольку $A(H) = P_\varphi A(G) P_\varphi^\top$, и соответствующие друг другу по φ коэффициенты полиномов η_G и η_H равны.

Покажем, что если равенство (2) выполняется, то $G \simeq H$ и φ — изоморфизм. Обозначим $A(G)$ через $A = (a_{ij})$ и $B(G)$ через $B = (b_{ij})$. Если выполняется (2), то коэффициент перед x_c равен коэффициенту $x_{\varphi(c)}$ для всех подмножеств $c \subseteq V(G)$. Значит, выбрав такое c, что $c = V(G) \setminus \{i, j\}$ для некоторой пары вершин $i, j \in V(G)$, мы имеем $A_c = B_{\varphi(c)}$. Это равносильно $\det \begin{pmatrix} 0 & a_{ij} \\ a_{ij} & 0 \end{pmatrix} = \det \begin{pmatrix} 0 & b_{\varphi(i)\varphi(j)} \\ b_{\varphi(i)\varphi(j)} & 0 \end{pmatrix}$. Таким образом, $a_{ij} = b_{\varphi(i)\varphi(j)}$ и $(i, j) \in E(G)$ тогда и только тогда, когда $(\varphi(i), \varphi(j)) \in V(H)$, то есть $G \simeq H$ и φ — изоморфизм. ■

Замечание. Для того, чтобы графы G и H были изоморфны, достаточно равенства коэффициентов перед произведениями x_c и $x_{\varphi(c)}$ для некоторой биекции $\varphi : V(G) \to V(H)$, где c — подмножества из n–2 вершин из $V(G)$. В случае если это равенство имеет место, равенство остальных соответствующих друг другу коэффициентов обеспечивается тем, что они являются определителями подматриц, получаемых удалением соответствующих по φ рядов из $A(G)$ и $A(H)$, и равны, так как $A(H) = P_\varphi A(G) P_\varphi^\top$.

2. Решение задачи ИГр проверкой равенства значений модифицированных характеристических полиномов графов в заданных точках

Поскольку полином вида (1) имеет 2^n коэффициентов, то алгоритм решения задачи ИГр, представленный в [8], требует экспоненциального времени для любых классов графов, поскольку проверка равенства всех соответствующих друг другу коэффициентов полиномов вида (1), в том числе и для полиномов графов, для которых задача ИГр разрешима за полиномиальное время, имеет, как и в худшем случае, экспоненциальную сложность. Представленный далее алгоритм — это алгоритм, решающий задачу ИГр проверкой равенства значений полиномов графов вида (1) в заданных точках, что позволяет эффективно решать многие индивидуальные задачи ИГр, включая представленные в [12], а также задачи ИГр для сильно-регулярных графов из [13].

Пусть $N \in \mathbb{N}$, $M = \{k/10^N \mid 0 < k \leq 10^N,\ k \in \mathbb{N}\}$, $|M| = 10^N$, $M \subset]0, 1[$, ε_i — случайно равномерно и независимо выбираемые в ходе работы представленного далее алгоритма значения из M. $\varepsilon^{(i)}$ — точки из $\mathbb{R}^n$, заданные следующим образом: $\varepsilon^{(0)} = (0, \ldots, 0)$ и

$$\varepsilon^{(i)} = \varepsilon^{(i-1)} + \varepsilon_i e_i,\ i = \overline{1, n},$$

где $\{e_i\}_{i=1}^n$ — стандартный базис в $\mathbb{R}^n$. То есть $\varepsilon^{(i)}$ — это точки

$$(\varepsilon_1, 0, 0, \ldots, 0),$$

$$(\varepsilon_1, \varepsilon_2, 0, \ldots, 0),$$

$$\ldots$$

$$(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n).$$

В приводимом ниже алгоритме проверка двух графов на изоморфизм производится как попытка построения биекции $\varphi : V(G) \to V(H)$ такой, что $\eta_G(\varepsilon^{(i)}) = \eta_H(\varepsilon_\varphi^{(i)})$, $i = \overline{1,n}$, для чего в ходе итераций алгоритма для каждого $i \in V(G)$ ищется такое $j \in V(H)$, что

$$\eta_G(\varepsilon^{(i)}) = \eta_H(\varepsilon_\varphi^{(i-1)} + \varepsilon_i e_j). \tag{3}$$

Установить соответствие (i)

```
1  if i=n
2       begin
3         flag:=true;
4         φ[n]:=k, где k такое, что J={k};
5         выйти из процедуры.
6       end
7  else
8       begin
9         выбрать ε_i∈M;
10        for j:=1 to n
11           begin
12              if j∈J и η_G(ε^(i))=η_H(ε_φ^(i-1) + ε_i e_j)
13                 begin
14                    φ[i]:=j, J := J\{j};
15                    Установить соответствие (i+1);
16                    if flag=false
17                          J:=J∪{j}, φ[i] := 0;
18                 end
19           end
20      end
21 выйти из процедуры.
```

Алгоритм решения задачи ИГр (G, H)

```
1  flag:=false; J:=V(H);
2  for i := 1 to n
3       φ[i] := 0;
4  Установить соответствие (1);
5  if flag
6       выдать сообщение "G≃H, φ — изоморфизм", выдать φ,
7  else
8       выдать сообщение "G≄H";
9  работу алгоритма завершить.
```

В ходе работы алгоритма элемент $\varphi[i]$ массива φ либо содержит номер некоторой вершины из $V(H)=\{1,\ldots,n\}$, либо является неопределённым, что задаётся нами как $\varphi[i]=0$. Если графы, поданные на вход алгоритма, изоморфны, то по окончании работы алгоритма этот массив содержит подстановку, задающую изоморфизм графов.

Рекурсивно вызываемая в ходе работы алгоритма процедура Установить соответствие, получая на вход $i \in V(G)$, устанавливает $\varphi[i] = j$, где $j \in V(H)$ такое, что выполнено (3). Если такого j для i не оказывается, и после выхода из процедуры Установить соответствие мы имеем $flag = false$, то производится модификация значения $\varphi[i-1]$, назначенного нами ранее: мы полагаем $\varphi[i-1] = 0$, после чего рассматриваем другие варианты из J для того, чтобы задать значение $\varphi[i-1]$.

Если для графов G и H соответствие φ может быть построено за n последовательно выполняемых итераций, то из равенства полиномов в n парах точек $\varepsilon^{(i)}$ и $\varepsilon_\varphi^{(i)}$, $i=\overline{1,n}$, делается вывод о том, что $G \simeq H$ и φ — изоморфизм.

3. Вероятность ошибки

Предположим, что предложенный выше алгоритм может быть реализован численно, то есть проверка равенства (3) может быть осуществлена за полиномиальное от n время и с полиномиально растущей от n длиной мантиссы. Предложенный алгоритм проверяет равенство полиномов от n переменных в n точках, чего недостаточно для того, чтобы делать вывод об их равенстве или неравенстве. Покажем, что при достаточной величине параметра N вероятность ошибки при проверке равенства полиномов графов, а значит и ошибки при решении задачи ИГр, будет пренебрежимо мала.

Возможные для алгоритмов решения задачи ИГр ошибки — это ошибки двух типов: 1) неверный вывод о $G \simeq H$, при том, что $G \not\simeq H$, 2) неверный вывод о $G \not\simeq H$ при том, что $G \simeq H$. Пусть $\mathsf{P}(\,\cdot\,)$ обозначает вероятность события, указываемого в скобках. Известна [14, 15] следующая лемма:

Лемма 1. *Пусть $f \in F[x_1,\ldots,x_n]$ — ненулевой полином общей степени $d \geq 0$ над полем F. Пусть M — конечное подмножество F, и пусть $r_1,\ldots,r_n$ — значения, случайно равномерно и независимо выбранные из M. Тогда*

$$\mathsf{P}\big(f(r_1,\ldots,r_n)=0\big) \leq \frac{d}{|M|}.$$

Если в ходе работы алгоритма для всех $i \in V(G)$ установлено φ, то $\eta_G(\varepsilon^{(n)}) = \eta_H(\varepsilon_\varphi^{(n)})$.

$$g(x_1,\ldots,x_n) = \eta_G(x_1,\ldots,x_n) - \eta_H(x_{\varphi(1)},\ldots,x_{\varphi(n)})$$

— полином общей степени n. Компоненты $\varepsilon^{(n)}$ — случайно равномерно и независимо выбранные из M значения ε_i. Если $\eta_G(\varepsilon^{(n)}) = \eta_H(\varepsilon_\varphi^{(n)})$, то, по лемме 1, $g \equiv 0$ с вероятностью не меньшей $1 - n/10^N$. Следовательно, если в результате выполнения алгоритма получено сообщение «$G \simeq H$ и φ — изоморфизм», мы имеем $\eta_G \not\equiv \eta_H$ с вероятностью $\mathsf{P}(\text{ошибка}) \leq n/10^N$. Если положить $N = n$, то $\mathsf{P}(\text{ошибка}) \leq 1/10^{n-\lg n}$, и это сообщение верно с вероятностью не меньшей $1-1/10^{n-\lg n}$. Выдаваемое алгоритмом сообщение о неизоморфизме графов всегда верно, поскольку означает, что искомого φ не существует, а значит, по теореме 1, графы неизоморфны.

4. Точность и сложность, необходимые для численной реализации алгоритма

4.1. Численная реализация алгоритма и её корректность

Пусть d_i обозначает *степень* вершины $i \in V(G)$ — количество вершин, смежных с i. Будем считать, что графы G и H имеют один и тот же набор степеней вершин: $\{d_1, \ldots, d_n\}$. Пусть d — максимальная степень вершин: $d = \max\{d_1, \ldots, d_n\}$. Для численного решения задачи ИГр поставим G и H в соответствие модифицированные матрицы смежности A и B:

$$A := A(G) + 2dE, \qquad B := A(H) + 2dE. \tag{4}$$

$A(H) = P_\varphi A(G) P_\varphi^\top$ для некоторого φ тогда и только тогда, когда $A = P_\varphi B P_\varphi^\top$.

При $d > 0$ матрица $A = (a_{ij})$ вида (4) обладает строгим диагональным преобладанием:

$$a_{ii} = 2d \geq 2d_i > d_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} a_{ij},$$

и значит

$$a_{ii} - \sum_{\substack{j=1 \\ j \neq i}}^{n} a_{ij} > 0,$$

$i = \overline{1, n}$. Таким образом, по критерию регулярности Адамара [16] матрицы A и B обратимы.

При численной реализации предложенных выше алгоритмов будем проверять равенство в заданных точках полиномов η_G и η_H вида

$$\eta_G(x_1, \ldots, x_n) = \det(A + X), \qquad \eta_H(x_{\varphi(1)}, \ldots, x_{\varphi(n)}) = \det(B + X_\varphi), \tag{5}$$

где $X_\varphi = P_\varphi X P_\varphi^\top$. Переход к матрицам графов вида (4) и рассмотрение полиномов вида (5) эквивалентны замене переменных x_i полиномов вида (1) на переменные $x_i + 2d$.

Работу представленного выше алгоритма можно рассмотреть как попытку произвести согласованные изменения матриц A и B:

$$A^{(0)} := A, \qquad B^{(0)} := A,$$

$$A^{(i)} := A^{(i-1)} + \varepsilon_i E_i, \qquad B^{(i)} := B^{(i-1)} + \varepsilon_i E_j, \tag{6}$$

$i = 1, \ldots, n$. Под согласованностью понимается выбор для $i \in V(G)$ такого $j \in V(H)$, что выполняется равенство

$$((A^{(i)})^{-1})_{ii} = \frac{A^{(i)}_{\{i\}}}{\det A^{(i)}} = \frac{(B^{(i-1)} + \varepsilon_i E_j)_{\{j\}}}{\det(B^{(i-1)} + \varepsilon_i E_j)} = ((B^{(i-1)} + \varepsilon_i E_j)^{-1})_{jj}, \tag{7}$$

где E_i — $n \times n$-матрица, в которой равны нулю все элементы за исключением i-го диагонального элемента, который равен 1. Идея проверки изоморфизма графов с помощью согласованных изменений элементов их матриц смежности принадлежит Р.Т. Файзуллину и была предложена в [17].

Из равенства (7) следует равенство

$$\eta_G(\varepsilon^{(i)}) = \eta_H(\varepsilon_\varphi^{(i-1)} + \varepsilon_i e_j) \tag{8}$$

для полиномов η_G и η_H вида (5), поскольку (7) для матриц $A^{(i)}$ и $B^{(i-1)}+\varepsilon_i E_j$ эквивалентно

$$\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})} = \frac{\eta_{H\setminus\{j\}}(\varepsilon_\varphi^{(i-1)} + \varepsilon_i e_j)}{\eta_H(\varepsilon_\varphi^{(i-1)} + \varepsilon_i e_j)}, \tag{9}$$

где через $G\setminus\{i\}$ обозначается подграф G, получаемый из G удалением вершины i и всех инцидентных ей рёбер. Будем полагать $\eta_{G\setminus\{i\}}(\varepsilon^{(i)})=\eta_{G\setminus\{i\}}(\varepsilon^{(i-1)})$. Так как значения $\eta_{G\setminus\{i\}}(\varepsilon^{(i)})$ и $\eta_{H\setminus\{j\}}(\varepsilon_\varphi^{(i-1)}+\varepsilon_i e_j)$ при варьировании значения ε_i не изменяются, то, имея равенство (9) для $\varepsilon_i\neq 0$, мы имеем и равенство (8).

Для обоснования корректности численной реализации алгоритма надо показать, что для поданных на вход алгоритма графов G и H в случае $G\simeq H$ численной реализацией алгоритма будет выдано сообщение об изоморфизме графов и их изоморфизм φ, а в случае $G\not\simeq H$ — сообщение о том, что графы не изоморфны. Для того, чтобы обеспечить корректность работы алгоритма, необходимо:

а) оценить необходимое количество итераций численного метода для достижения требуемой для проверки (9) точности,

б) оценить требуемую для фиксирования результатов вычислений длину мантиссы машинных чисел.

В случае, если $G\not\simeq H$, имеем $\eta_G\not\equiv\eta_H$. Возможные варианты перед запуском алгоритма:

1) $\eta_G(0,\ldots,0)\neq\eta_H(0,\ldots,0)$,

2) $\eta_G(0,\ldots,0)=\eta_H(0,\ldots,0)$.

Корректность работы численной реализации алгоритма в первом случае обосновывается утверждением 1, во втором — утверждением 2. Корректность работы численной реализации алгоритма для случая $G\simeq H$ следует также из утверждения 2. Докажем

Утверждение 1. *Пусть $G\not\simeq H$ и $\eta_G(0,\ldots,0)\neq\eta_H(0,\ldots,0)$. Тогда при $N=n$ имеем*

$$\mathsf{P}\big(\text{ошибка}\big) \le \frac{1}{10^{n(n-\lg n)}}.$$

Доказательство. Алгоритмом устанавливается соответствие φ для $i=\overline{1,n}$ и делается ошибочный вывод о том, что $G\simeq H$, тогда, когда на итерациях алгоритма последовательно имеем:

$$\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})} = \frac{\eta_{H\setminus\{\varphi(i)\}}(\varepsilon_\varphi^{(i)})}{\eta_H(\varepsilon_\varphi^{(i)})},$$

тогда как $\eta_G\not\equiv\eta_H$.

Если $\eta_G(0,\ldots,0)\neq\eta_H(0,\ldots,0)$ и выполнено

$$\frac{\eta_{G\setminus\{1\}}(\varepsilon^{(1)})}{\eta_G(\varepsilon^{(1)})} = \frac{\eta_{H\setminus\{\varphi(1)\}}(\varepsilon_\varphi^{(1)})}{\eta_H(\varepsilon_\varphi^{(1)})},$$

то для значения $t = \eta_{G\setminus\{1\}}(\varepsilon^{(1)})/\eta_{H\setminus\{\varphi(1)\}}(\varepsilon_\varphi^{(1)})$, должно также выполняться

$$\eta_G(\varepsilon^{(1)}) = t \cdot \eta_H(\varepsilon_\varphi^{(1)}). \tag{10}$$

Поскольку ε_1 выбирается из M случайно, и имеет место (10), то для полиномов η_G и η_H, рассматриваемых как полиномы степени 1 от x_1 и $x_{\varphi(1)}$ при $x_i{=}0$, $x_{\varphi(i)}{=}0$, $i{\neq}1$, по лемме 1 имеем:

$$\mathsf{P}\left(\frac{\eta_{G\setminus\{1\}}(\varepsilon^{(1)})}{\eta_G(\varepsilon^{(1)})} = \frac{\eta_{H\setminus\{\varphi(1)\}}(\varepsilon_\varphi^{(1)})}{\eta_H(\varepsilon_\varphi^{(1)})}\right) = \mathsf{P}\left(\eta_G(\varepsilon^{(1)}) = t \cdot \eta_H(\varepsilon_\varphi^{(1)})\right) =$$

$$= \mathsf{P}\left(\eta_G(\varepsilon^{(1)}) - t \cdot \eta_H(\varepsilon_\varphi^{(1)}) = 0\right) \leq \frac{1}{10^N}.$$

Аналогично получаем для $i = \overline{2,n}$:

$$\mathsf{P}\left(\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})} = \frac{\eta_{H\setminus\{\varphi(i)\}}(\varepsilon_\varphi^{(i)})}{\eta_H(\varepsilon_\varphi^{(i)})}\right) \leq \frac{i}{10^N}.$$

Таким образом, вероятность ошибки может быть оценена как

$$\mathsf{P}\big(\text{ошибка}\big) \leq \frac{1}{10^N} \cdot \ldots \cdot \frac{i}{10^N} \cdot \ldots \cdot \frac{n}{10^N}.$$

Полагая $N{=}n$, будем иметь

$$\mathsf{P}\big(\text{ошибка}\big) \leq \frac{1}{10^{n(n-\lg n)}}.$$

■

Замечание. Утверждение 1 доказывается в предположении, что проверка выполнения равенства (9) может быть реализована численно, то есть с использованием машинных чисел с ограниченной полиномом от n длиной мантиссы и за полиномиальное от n время.

Вычислительная сложность решения СЛАУ с необходимой точностью. Нахождение элемента $((A^{(i)})^{-1})_{ii}$ обратной к $A^{(i)}$ матрицы будем производить, решая системы линейных уравнений вида

$$A^{(i)}y = e_i, \tag{11}$$

где $\{e_i\}_{i=1}^n$ — стандартный базис в $\mathbb{R}^n$. Значение $((A^{(i)})^{-1})_{ii}$ — это значение i-й компоненты y.

Нахождение сравниваемых в (9) значений как компонент вектора-решения СЛАУ позволяет оценить количество итераций методов их решения, которые надо сделать для достижения необходимой точности. Точность должна быть достаточна для того, чтобы, исходя из неравенства (9) машинных чисел с ограниченной длинной мантиссы, можно было делать вывод о неравенстве представляемых ими чисел из $\mathbb{R}$.

Для решения СЛАУ (11) могут быть использованы итерационные методы, такие как метод Гаусса-Зейделя или метод простой итерации. Диагональное преобладание, задаваемое (4), обеспечивает сходимость этих методов к точному решению со скоростью геометрической прогрессии. Для решения указанных выше тестовых задач при выборе

значений ε_i из интервала $[10^{-3}, 1]$ достаточно использования стандартного числового типа double.

Использование итерационного метода решения СЛАУ, в отличие от, например, использования метода Гаусса, позволяет нам, как это будет сделано далее, оценить полиномом от n вычислительную сложность получения приближённых решений СЛАУ (11) с заданной точностью.

Оценим вычислительную сложность решения СЛАУ (11) с необходимой для проверки равенства (9) точностью в общем случае задачи ИГр. Пусть для решения СЛАУ (11) используется метод Гаусса-Зейделя. Пусть $y^{(k)}$ — приближение точного решения y на k-й итерации метода Гаусса-Зейделя. Можно показать [18], что если для СЛАУ $Ay = b$ матрица A такая, что $\sum_{j \neq i} |a_{ij}| \leq \gamma |a_{ii}|$, $\gamma < 1$, $i = \overline{1, n}$, то

$$\|y - y^{(k)}\|_1 \leq \gamma \|y - y^{(k-1)}\|_1.$$

Для матриц вида (4) $\gamma \leq 1/2$. Следовательно,

$$|y_i - y_i^{(k)}| \leq \|y - y^{(k)}\|_1 \leq \frac{\delta_0}{2^k},$$

где δ_0 — погрешность начального приближения.

Рассмотрим следующую задачу. Пусть a, $b \in \mathbb{R}$ — некоторые точные значения, а $a^{(k)}$, $b^{(k)} \in \mathbb{R}$ — такие их приближения, полученные за k первых итераций численного метода, что

$$|a - a^{(k)}| \leq \frac{\delta_0}{2^k}, \qquad |b - b^{(k)}| \leq \frac{\delta_0}{2^k}.$$

Предположим, известно такое $\Delta > 0$, что если $a \neq b$, то $|a - b| > \Delta$. Надо определить, сколько требуется произвести итераций метода для того, чтобы неравенство машинных чисел $a^{(k)}$ и $b^{(k)}$ свидетельствовало о неравенстве точных значений $a, b \in \mathbb{R}$. Предполагая, что длина мантиссы используемых машинных чисел достаточна для фиксирования полученных результатов, если

$$|a - a^{(k)}| < \frac{\Delta}{4}, \qquad |b - b^{(k)}| < \frac{\Delta}{4},$$

будем иметь

$$|a^{(k)} - b^{(k)}| > \frac{\Delta}{2},$$

и на последующих итерациях метода Гаусса-Зейделя модуль разности приближённых значений $a^{(k)}$ и $b^{(k)}$ будет только расти. А значит, можно утверждать, что $a \neq b$. Таким образом, если $|a - b| > \Delta > 0$, то для фиксирования с помощью машинных чисел с достаточной длиной мантиссы неравенства $a \neq b$ точных значений надо провести такое число итераций K, что

$$\frac{\delta_0}{2^K} < \frac{\Delta}{4}, \tag{12}$$

то есть $K = O(\log \frac{1}{\Delta})$. С учётом того, что вычислительная сложность одной итерации метода Гаусса-Зейделя составляет $O(n^2)$, при его использовании вычислительная сложность решения СЛАУ с необходимой точностью в ходе работы алгоритма составит $K \cdot O(n^2)$.

4.2. Вычислительная сложность нахождения приближённых решений СЛАУ и длина мантиссы используемых машинных чисел

Как было указано выше, для численной реализации предложенного алгоритма необходимо в ходе его работы проверять равенства вида (3), а значит необходимо фиксировать неравенства

$$\eta_G(\varepsilon^{(i)}) \neq \eta_H(\varepsilon_\varphi^{(i)}) \tag{13}$$

за полиномиальное от n время, используя машинные числа с полиномиально растущей от n длиной мантиссы. То есть при таких ограничениях необходимо уметь сравнивать значения полиномов от n переменных с 2^n коэффициентами. Утверждения, доказываемые ниже, обосновывают возможность численной реализации этой операции сравнения.

Далее при доказательстве утверждений 2 и 3 нами используется известная теорема Гершгорина:

Теорема 2. *Любое собственное значение матрицы $A=(a_{ij})$ лежит по крайней мере в одном из кругов с центрами a_{ii} и радиусами $\sum\limits_{j\neq i}|a_{ij}|$.*

Доказываемое ниже утверждение 2 обосновывает тот факт, что если $\eta_G(\varepsilon^{(i)})=\eta_H(\varepsilon_\varphi^{(i)})$ для $i<k$, и на k-й итерации получаем неравенство $\eta_G(\varepsilon^{(k)})\neq\eta_H(\varepsilon_\varphi^{(k)})$, то это неравенство будет установлено в ходе работы численной реализации представленного выше алгоритма решения задачи ИГр. Это означает, что возможность построения алгоритмом соответствия φ есть только в том случае, если графы изоморфны. Для доказательства утверждения 2 нам потребуется следующая лемма.

Лемма 2. *Если верно* (13), *то* $|\eta_G(\varepsilon^{(i)})-\eta_H(\varepsilon_\varphi^{(i)})|=p/10^{iN}>1/10^{iN}$, $p\in\mathbb{N}$.

Доказательство. Пусть $A=A^{(i)}$. Тогда

$$\eta_G(\varepsilon^{(i)}) = \det A = \sum_{\pi\in S_n}\left(\sigma(\pi)\prod_{j=1}^{n} a_{j\pi(j)}\right), \tag{14}$$

где $\sigma(\pi)=1$, если π — чётная, и $\sigma(\pi)=-1$ иначе. Имеем:

$$\prod_{j=1}^{n} a_{j\pi(j)} = \frac{p}{10^{k(\pi)N}},$$

где $p\in\mathbb{N}$, а $k(\pi)$ — количество модифицированных на момент завершения i-й итерации диагональных элементов A в произведении, соответствующем π слева в (14). Следовательно,

$$\eta_G(\varepsilon^{(i)}) = \sum_{\pi\in S_n}\left(\sigma(\pi)\cdot\frac{p}{10^{k(\pi)N}}\right).$$

Так как A — матрица с диагональным преобладанием, то $\eta_G(\varepsilon^{(i)})>0$, и, следовательно, $\eta_G(\varepsilon^{(i)})=p_1/10^{iN}$, $\eta_H(\varepsilon^{(i)})=p_2/10^{iN}$ для некторых $p_1,p_2\in\mathbb{N}$. Получаем

$$\left|\eta_G(\varepsilon^{(i)})-\eta_H(\varepsilon_\varphi^{(i)})\right| = \left|\frac{p_1}{10^{iN}}-\frac{p_2}{10^{iN}}\right|.$$

Если $\eta_G(\varepsilon^{(i)})\neq\eta_H(\varepsilon_\varphi^{(i)})$, то $p_1\neq p_2$, и, следовательно, $|\eta_G(\varepsilon^{(i)})-\eta_H(\varepsilon_\varphi^{(i)})|=p/10^{iN}\geq 1/10^{iN}$, $p\in\mathbb{N}$. ■

Утверждение 2. *Если для некоторого* $\varphi \in S_n$ *имеем* $\eta_G(\varepsilon^{(i)}) = \eta_H(\varepsilon_\varphi^{(i)})$ *для* $i < k$ *и* $\eta_G(\varepsilon^{(k)}) \neq \eta_H(\varepsilon_\varphi^{(k)})$, *то*

$$\frac{\eta_{G\setminus\{k\}}(\varepsilon^{(k)})}{\eta_G(\varepsilon^{(k)})} \neq \frac{\eta_{H\setminus\{j\}}(\varepsilon_\varphi^{(k)})}{\eta_H(\varepsilon_\varphi^{(k)})}, \tag{15}$$

и (15) *может быть зафиксировано с помощью машинных чисел с мантиссой длины* $O(n^2)$ *за время* $O(n^4)$.

Доказательство. Пусть $a = \eta_G(\varepsilon^{(k)})$, $a' = \eta_{G\setminus\{k\}}(\varepsilon^{(k)})$. По лемме 2: $\eta_H(\varepsilon_\varphi^{(k)}) = a + p/10^{kN}$, $\eta_{H\setminus\{j\}}(\varepsilon_\varphi^{(k)}) = a' + q/10^{kN}$, $p, q \in \mathbb{N}$, $p \neq 0$. Следовательно,

$$\left|\frac{\eta_{G\setminus\{k\}}(\varepsilon^{(k)})}{\eta_G(\varepsilon^{(k)})} - \frac{\eta_{H\setminus\{j\}}(\varepsilon_\varphi^{(k)})}{\eta_H(\varepsilon_\varphi^{(k)})}\right| = \left|\frac{a'}{a} - \frac{a' + q/10^{kN}}{a + p/10^{kN}}\right| = \frac{1}{10^{kN}} \cdot \frac{|a'p - aq|}{\eta_G(\varepsilon^{(k)})\eta_H(\varepsilon_\varphi^{(k)})}.$$

По теореме Гершгорина, с учётом модификации диагональных элементов $(A(G))_{ii}$ и $(A(H))_{\varphi(i)\varphi(i)}$ для $i < k$ добавлением значений $\varepsilon_i < 1$, имеем $\eta_G(\varepsilon^{(k)}) < (3(d+1))^n$ и $\eta_H(\varepsilon_\varphi^{(k)}) < (3(d+1))^n$. Так как $a = p_1/10^{kN}$, $a' = p_2/10^{(k-1)N}$, где $p_1, p_2 \in \mathbb{N}$, то если $a'p - aq \neq 0$, имеем $|a'p - aq| \geq 1/10^{kN}$. Следовательно,

$$\left|\frac{\eta_{G\setminus\{k\}}(\varepsilon^{(k)})}{\eta_G(\varepsilon^{(k)})} - \frac{\eta_{H\setminus\{j\}}(\varepsilon_\varphi^{(k)})}{\eta_H(\varepsilon_\varphi^{(k)})}\right| > \frac{1}{10^{2kN}(3(d+1))^{2n}}. \tag{16}$$

Покажем, что $a'p - aq \neq 0$. Равенство $a'p - aq = 0$ равносильно равенству $a'/a = q/p$, которое равносильно

$$\frac{\eta_{G\setminus\{k\}}(\varepsilon^{(k)})}{\eta_G(\varepsilon^{(k)})} = \frac{\eta_{H\setminus\{j\}}(\varepsilon^{(k)}) - \eta_{G\setminus\{k\}}(\varepsilon^{(k)})}{\eta_H(\varepsilon^{(k)}) - \eta_G(\varepsilon^{(k)})} =$$

$$= \frac{p/10^{kN}}{\eta_G(\varepsilon^{(k)}) - \eta_H(\varepsilon_\varphi^{(k)})} = \frac{p/10^{kN}}{\eta_G(\varepsilon^{(k)}) - \eta_H(\varepsilon_\varphi^{(k)})} = \frac{p/10^{kN}}{\eta_G(\varepsilon^{(k-1)}) - \eta_H(\varepsilon_\varphi^{(k-1)}) + \varepsilon_k p/10^{kN}}. \tag{17}$$

Поскольку по условию теоремы $\eta_G(\varepsilon^{(k-1)}) = \eta_H(\varepsilon_\varphi^{(k-1)})$, то (17) эквивалентно

$$\frac{\eta_{G\setminus\{k\}}(\varepsilon^{(k)})}{\eta_G(\varepsilon^{(k)})} = \frac{1}{\varepsilon_k},$$

то есть

$$\frac{\eta_{G\setminus\{k\}}(\varepsilon^{(k)})}{\eta_G(\varepsilon^{(k-1)}) + \varepsilon_k \eta_{G\setminus\{k\}}(\varepsilon^{(k)})} = \frac{1}{\varepsilon_k},$$

что равносильно

$$\frac{\eta_G(\varepsilon^{(k-1)})}{\eta_{G\setminus\{k\}}(\varepsilon^{(k-1)})} = 0.$$

Но это невозможно, поскольку $\eta_G(\varepsilon^{(k-1)}) > 0$, так как по определению (4) матрица A обладает строгим диагональным преобладанием. Следовательно, $a'p - aq \neq 0$.

Покажем, что неравенство (15) может быть зафиксировано при указанных в формулировке утверждения длине машинных чисел и времени, требуемом для вычислений.

Из (16) следует, что для того, чтобы численно зафиксировать неравенство (15) требуется такая длина мантиссы L машинных чисел, чтобы выполнялось

$$\frac{1}{10^L} < \frac{1}{10^{2kN}(3(d+1))^{2n}},$$

что при $N=n$, с учётом того, что $d\leq n$, $k\leq n$, равносильно выполнению неравенства

$$L > 2n^2+2n\lg(3n+1),$$

из которого следует, что (15) может быть зафиксировано машинными числами с длиной мантиссы, растущей от n как $O(n^2)$.

При $N=n$ из (12), где Δ — значение из правой части (16), следует, что для решения СЛАУ с точностью, необходимой для фиксирования неравенства (15), требуется $O(\log(10^{2kn}(3(d+1))^{2n}))\cdot O(n^2)=O(n^4)$ элементарных машинных операций, поскольку k и d могут принимать значения от 1 до n:

$$O(\log(10^{2kn}(3(d+1))^{2n})) = O(\log(10^{2kn})) + O(\log 3^{2n}) + O(\log(d+1)^{2n})) =$$

$$= O(n^2) + O(n) + O(n\log n) = O(n^2).$$

■

5. Дерегуляризация графов в ходе работы алгоритма. Точность и сложность вычислений, необходимые для её реализации

Группа автоморфизмов $\mathrm{Aut}(G)$ графа G — это группа изоморфизмов графа на себя:

$$\mathrm{Aut}(G)=\{\psi\in S_n \mid a_{ij} = a_{\psi(i)\psi(j)},\ i,j=\overline{1,n}\}.$$

Орбитой вершины $i\in V(G)$ относительно $\mathrm{Aut}(G)$ называется множество

$$\mathrm{O}_i(G)=\{\varphi(i) \mid \varphi\in\mathrm{Aut}(G)\}.$$

Вычислительно сложные индивидуальные задачи ИГр имеют группы автоморфизмов большой мощности, поскольку в этом случае имеется большое число вариантов для перебора на множествах вершин графов при установлении изоморфизма алгоритмами решения ИГр. Чем меньше мощность группы автоморфизмов графа, тем менее регулярна структура графа. В ходе проведения итераций представленного алгоритма производится последовательная дерегуляризация графов, в ходе которой убывают мощности групп автоморфизмов последовательно получаемых в соответствии с (6) графов. То есть под дерегуляризацией графа нами понимается такая его модификация, при которой в нём уменьшается количество симметрий, представляемых изоморфизмами графа на себя. В нашем случае дерегуляризация графов G и H производится добавлением взвешенных петель, то есть получением из них графов $G^{(i)}$ и $H^{(i)}$ таких, что $E(G^{(i)})$ и $E(H^{(i)})$ содержат рёбра вида (j,j).

Следующая лемма показывает, что различные варианты установления изоморфизма для двух графов имеются в том случае, если орбиты вершин графов не тривиальны, то есть состоят более чем из одной вершины.

Лемма 3. *Пусть* $G\simeq H$, $i_1,i_2\in V(H)$. $i_1\in O_{i_2}(H)$ *тогда и только тогда, когда существуют вершина* $j\in V(G)$ *и такие изоморфизмы* $\varphi_1,\varphi_2 : V(G)\to V(H)$, *что* $\varphi_1(j)=i_1$, $\varphi_2(j)=i_2$.

Доказательство. Пусть $i_1\in\mathrm{O}_{i_2}(H)$. Значит, мы имеем $\psi\in\mathrm{Aut}(G)$ такое, что $\psi(i_1)=i_2$. Пусть φ_1 — изоморфимзм G на H и пусть $j=\varphi_1^{-1}(i_1)$, $j\in V(H)$. Тогда $\varphi_2=\psi\circ\varphi_1$. Имеем:

$\varphi_2(j)=(\psi\circ\varphi_1)(j)=\psi(i_1)=i_2$. Обратно, предположим, что есть $i_1,i_2\in V(H)$, $j\in V(G)$ и изоморфизмы φ_1, φ_2 такие, что $\varphi_1(j)=i_1$, $\varphi_2(j)=i_2$. Тогда $\psi=\varphi_2\circ\varphi_1^{-1}\in\mathrm{Aut}(H)$ и $\psi(j)=i_2$, то есть $i_1\in\mathrm{O}_{i_2}(H)$. ■

Из леммы 3 следует, что если $G\simeq H$, то при установлении изоморфизма этих графов наличие нескольких вариантов установления соответствия φ для вершины $i\in V(G)$ возможно только в том случае, если $|\mathrm{O}_i(G)|>1$.

Предположим, что устанавливаемое в ходе работы алгоритма соответствие φ совпадает с некоторым изоморфизмом графов G и H для $j<i$ для некоторого i. Вероятность того, что веса инцидентных вершинам графа петель, назначаемые алгоритмом, окажутся не уникальны, пренебрежимо мала при достаточной величине параметра N. В этом случае уникальность веса петель будет обеспечивать $|\mathrm{O}_j(G^{(i)})|=1$, $|\mathrm{O}_{\varphi(j)}(H^{(i)})|=1$ для $j<i$,

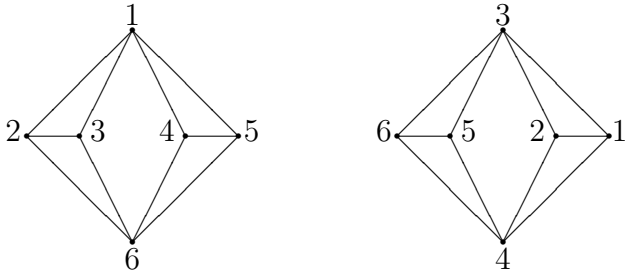
$$|\mathrm{Aut}(G^{(i+1)})|\le|\mathrm{Aut}(G^{(i)})|,\qquad|\mathrm{Aut}(H^{(i+1)})|\le|\mathrm{Aut}(H^{(i)})|$$

для $i=0,1,\ldots,t$, и

$$|\mathrm{Aut}(G^{(t)})|=|\mathrm{Aut}(H^{(t)})|=1,$$

$t\le n$, и при этом $G^{(i)}\simeq H^{(i)}$. Такая последовательная дерегуляризация графов позволяет уменьшить количество перебираемых вариантов установления φ. Если устанавливаемое в ходе работы соответствие изоморфизмом не является, этот факт будет установлен в ходе работы алгоритма, как следует из теоремы 1 и утверждения 1.

Рассмотрим пример, иллюстрирующий эти рассуждения. Пусть графы G и H, проверяемые на изоморфизм, — это графы, представленные на рисунке ниже. Уменьшение количества вариантов установления соответствия φ при работе алгоритма для этих графов отображено в табл. 1. В строках этой таблицы указываются вершины из $V(H)$ — варианты установления соответствия для вершин из $V(G)=\{1,2,3,4,5,6\}$, и мощность $\mathrm{Aut}(G^{(i)})$. После 4-й итерации имеем $|\mathrm{Aut}(G^{(4)})|=1$.



Т а б л и ц а 1. Уменьшение количества вариантов при установлении изоморфизма графов G и H.

i	Варианты установления соответствия φ						$\lvert\mathrm{Aut}(G^{(i)})\rvert$
	1	2	3	4	5	6	
0	3, 4	1, 2, 5, 6	1, 2, 5, 6	1, 2, 5, 6	1, 2, 5, 6	3, 4	16
1	3	1, 2, 5, 6	1, 2, 5, 6	1, 2, 5, 6	1, 2, 5, 6	4	8
2	3	1	2	5, 6	5, 6	4	2
3	3	1	2	5, 6	5, 6	4	2
4	3	1	2	5	6	4	1

В табл. 2 приводятся значения $((A^{(i)})^{-1})_{jj}$, рассчитанные в ходе работы алгоритма для графов G и H. Для всех $i=\overline{1,n}$ после установления соответствия $\varphi(i)$ набор

значений $((B^{(i)})^{-1})_{jj}$, $j=\overline{1,n}$, тот же, что и набор значений $((A^{(i)})^{-1})_{jj}$. Для нахождения представленных значений производилось 10 итераций метода Гаусса-Зейделя решения СЛАУ вида (11) при начальном приближении $y^{(0)}=(1,\ldots,1)$. В табл. 2 представлены рассчитанные на итерациях алгоритма значения $((A^{(i)})^{-1})_{jj}$.

Т а б л и ц а 2. Рассчитанные в ходе работы алгоритма значения $((A^{(i)})^{-1})_{jj}$, $i=\overline{1,3}$.

i	ε_i	$((A^{(i)})^{-1})_{11}$	$((A^{(i)})^{-1})_{22}$	$((A^{(i)})^{-1})_{33}$	$((A^{(i)})^{-1})_{44}$	$((A^{(i)})^{-1})_{55}$	$((A^{(i)})^{-1})_{66}$
0	0	0.078	0.094	0.094	0.094	0.094	0.078
1	0.861	0.070	0.095	0.095	0.095	0.095	0.078
2	0.672	0.070	0.087	0.095	0.095	0.095	0.079
3	0.372	0.071	0.087	0.091	0.094	0.094	0.079
4	0.475	0.072	0.087	0.091	0.089	0.095	0.080

Покажем, что уменьшение количества вариантов для перебора при установлении φ в ходе работы алгоритма может быть реализовано численно, то есть, имея после $(i{-}1)$-й итерации равенство

$$\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i-1)})}{\eta_G(\varepsilon^{(i-1)})}=\frac{\eta_{G\setminus\{j\}}(\varepsilon^{(i-1)})}{\eta_G(\varepsilon^{(i-1)})}, \tag{18}$$

после проведения i-й итерации мы имеем

$$\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}\neq\frac{\eta_{G\setminus\{j\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}. \tag{19}$$

Покажем, что неравенство (19) может быть зафиксированно численно с помощью машинных чисел с полиномиально растущей от n длиной мантиссы за полиномиальное от n время.

Утверждение 3. *Пусть верно (18). Тогда*

$$\left|\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}-\frac{\eta_{G\setminus\{j\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}\right|>\frac{1}{3^n10^Nd^2} \tag{20}$$

и (19) *может быть зафиксировано с помощью машинных чисел с мантиссой длины* $O(n)$ *за время* $O(n^3)$.

Доказательство.

$$\left|\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}-\frac{\eta_{G\setminus\{j\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}\right|=\left|\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})-(\eta_{G\setminus\{j\}}(\varepsilon^{(i-1)})+\varepsilon_i\eta_{G\setminus\{ij\}}(\varepsilon^{(i-1)}))}{\eta_G(\varepsilon^{(i)})}\right|=$$

$$=\varepsilon_i\cdot\frac{\eta_{G\setminus\{ij\}}(\varepsilon^{(i-1)}))}{\eta_G(\varepsilon^{(i)})}, \tag{21}$$

поскольку $\eta_{G\setminus\{i\}}(\varepsilon^{(i)})=\eta_{G\setminus\{i\}}(\varepsilon^{(i-1)})$ и, как следует из (18), $\eta_{G\setminus\{i\}}(\varepsilon^{(i-1)})=\eta_{G\setminus\{j\}}(\varepsilon^{(i-1)})$.

Из выполнения условий Адамара следует, что $\eta_{G\setminus\{ij\}}(\varepsilon^{(i-1)}))\geq d^{n-2}$. С другой стороны, по теореме Гершгорина для собственных значений λ_t матрицы смежности $A(G^{(i)})$ имеем $d\leq\lambda_t\leq 3d$, $t=\overline{1,n}$, следовательно, $d^n\leq\eta_G(\varepsilon^{(i)})=\prod_{r=1}^n\lambda_t\leq(3d)^n$. С учётом этого, из (21) получаем:

$$\left|\frac{\eta_{G\setminus\{i\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}-\frac{\eta_{G\setminus\{j\}}(\varepsilon^{(i)})}{\eta_G(\varepsilon^{(i)})}\right|\geq\varepsilon_i\cdot\frac{d^{n-2}}{(3d)^n}>\frac{1}{3^n10^Nd^2}.$$

Оценим длину мантиссы L машинных чисел, необходимую для того, чтобы численно зафиксировать неравенство (19). Для этого требуется выполнение неравенства

$$\frac{1}{10^L} < \frac{1}{3^n 10^N d^2},$$

которое равносильно неравенству

$$L > n \lg 3 + 2\lg d + N.$$

Так как $d \leq n$, то при $N = n$, используя машинные числа с длиной мантиссы L такой, что

$$L > n + n \lg 3 + 2\lg n,$$

мы можем фиксировать неравенство (19) численно, то есть $L = O(n)$.

При $N = n$ из (12), где Δ — значение из правой части (20), следует, что для решения СЛАУ вида (11) с точностью, необходимой для фиксирования неравенства (19), требуется $O(\log(3^n 10^n d^2)) \cdot O(n^2) = O(n^3)$ элементарных машинных операций. ■

Таким образом, из доказанных утверждений 2 и 3 следует, что для численной реализации представленного в работе алгоритма решения задачи ИГр требуется длина мантиссы машинных чисел, растущая как $\max\{O(n^2), O(n)\} = O(n^2)$, и время, оцениваемое как $\max\{O(n^4), O(n^2)\} = O(n^4)$ элементарных машинных операций.

6. Выводы

Доказаны утверждения, обосновывающие возможность численной реализации проверки изоморфизма графов, используя её сведение к проверке равенства модифицированных характеристических полиномов графов. Показано, что при достаточно больших значениях параметра алгоритма, использующего такое сведение, вероятность ошибочности решения задачи ИГр, полученного им, пренебрежимо мала. Доказано, что вычислительная сложность процедуры сравнения значений модифицированных характеристических полиномов в заданной точке составляет $O(n^4)$ при растущей как $O(n^2)$ длине мантиссы используемых машинных чисел.

Список литературы / References

[1] **Filotti, I.S., Mayer, J.N.** A polynomial-time algorithm for determining the isomorphism of graphs of fixed genus // Proceedings of the 12th Annual ACM Symposium on Theory of Computing. ACM Press. 1980. P. 236–243.

[2] **Babai, L., Grigoryev, D.Yu., Mount, D.M.** Isomorphism of graphs with bounded eigenvalue multiplicity // Proceedings of the 14th Annual ACM Symposium on Theory of Computing. ACM New York, NY, USA. 1982. P. 310—324.

[3] **Luks, E.M.** Isomorphism of graphs of bounded valence can be tested in polynomial time // Journal of Computer and System Sciences. Academic Press. 1982. Vol. 25, No. 1. P. 42–65.

[4] **Ullman, J.R.** An algorithm for subgraph isomorphism // Journal of the ACM. ACM Press. 1976. Vol. 23, No. 1. P. 31–42.

[5] **Schmidt, D.C., Druffel, L.E.** A fast backtracking algorithm to test directed graphs for isomorphism using distance matrices // Journal of the ACM. ACM Press. 1978. Vol. 23, No. 3. P. 433–445.

[6] **McKay, B.D.** Practical graph isomorphism // 10th. Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, 1980. Congressus Numerantium. 1981. Vol. 30. P. 45–87.

[7] **Foggia, P., Sansone, C., Vento, M.** A performance comparison of five algorithms for graph isomorphism // Proceedings of the 3rd IAPR TC-15 Workshop on Graph-based Representations in Pattern Recognition, Cuen. Springer-Verlag Berlin Heidelberg. 2001. P. 188–199.

[8] **Пролубников А.В.** Сведение задачи проверки изоморфизма графов к задаче проверки равенства полиномов от n переменных // Труды института математики и механики УрО РАН. 2016. Т. 22, №1. С. 235–240.
Prolubnikov, A.V. Reduction of the graph isomorphism problem to equality checking of polynomials of n-variables. // Trudy Instituta Matematiki i Mekhaniki, Ekaterinburg: IMM of Ural Department of Russian Academy of Sciences. 2016. V. 22, No. 1. P. 235–240. (In Russ.)

[9] **Цветкович Д., Дуб М., Захс Х.** Спектры графов. Теория и применение. Киев: Изд-во «Наукова Думка», 1984. 384 с.
Cvetkovic, D.M, Doob, M., Sachs, H. Spectra of Graphs. Academic Press, New York, 1980.

[10] **Seidel, J.J.** Strongly regular graphs with (-1,1,0) adjacency matrix having eigenvalue 3 // Linear Algebra and its Applications. Academic Press. 1968. Vol. 1, No. 2. P. 281–298.

[11] **Lipton, R.J., Vishnoi, N.K., Zalcstein, Z.** A generalization of the characteristic polynomial of a graph // Georgia Institute of Technology, CC Technical Report, GIT-CC-03-51, 2003. Available at: https://smartech.gatech.edu/bitstream/handle/1853/6511/GIT-CC-03-51.pdf (accessed: 24.02.2016).

[12] **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, Cuen. 2001. Springer-Verlag Berlin Heidelberg. P. 157–168.

[13] Strongly regular graphs on at most 64 vertices. Avaialble at: http://www.maths.gla.ac.uk/∼es/srgraphs.php (accessed: 24.02.2016).

[14] **Schwartz, J.** Fast probabilistic algorithms for verification of polynomial identities // Journal of the ACM. ACM New York, NY, USA. 1980. Vol. 27, No. 4. P. 701–717.

[15] **Zippel, R.** Probabilistic algorithms for sparse polynomials // EUROSAM '79 Proceedings of the International Symposium on Symbolic and Algebraic Computation. Springer-Verlag London, UK. 1979. P. 216–226.

[16] **Гантмахер Ф.Р.** Теория матриц. М.: Изд-во «Наука», 1967. 576 с.
Gantmacher, F.R. The Theory of Matrices. AMS Chelsea Publishing: Reprinted by American Mathematical Society. 2000. 660 p.

[17] **Faizullin, R.T., Prolubnikov, A.V.** An algorithm of the spectral splitting for the double permutation cipher // Pattern Recognition and Image Analysis. 2002. Vol. 12, No. 4. P. 365–375.

[18] **Березин И.С., Жидков Н.П.** Методы вычислений. Т. 2. М.: Гос. изд. физ.-мат. литературы, 1962. 620 с.
Berezin, I.S., Zhidkov, N.P. Computing Methods. V. 2. Pergamon Press, Oxford. 1965. 678 p.