ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 22 № 1 2016

УДК 519.178

СВЕДЕНИЕ ЗАДАЧИ ПРОВЕРКИ ИЗОМОРФИЗМА ГРАФОВ К ЗАДАЧЕ ПРОВЕРКИ РАВЕНСТВА ПОЛИНОМОВ ОТ n ПЕРЕМЕННЫХ

А. В. Пролубников

Доказывается, что два графа изоморфны, если существует такая нумерация вершин одного из них, при которой равны модифицированные характеристические полиномы графов. Представлен алгоритм решения задачи проверки изоморфизма графов. При выполнении этого алгоритма определяется нумерация вершин одного из графов, при которой равны коэффициенты полиномов.

Ключевые слова: изоморфизм графов, полный инвариант.

A. V. Prolubnikov. Reduction of the graph isomorphism problem to checking the equality of polynomials of n variables.

It is proved that two graphs are isomorphic if there exists an enumeration for vertices of one of the graphs such that modified characteristic polynomials of the graphs are equal. An algorithm for solving the graph isomorphism problem is presented. The algorithm finds an enumeration for vertices of one of the graphs that provides the equality of coefficients of the polynomials if such an enumeration exists.

Keywords: graph isomorphism, complete invariant.

Введение

В задаче проверки изоморфизма графов (далее “задача ИГ”) даны два невзвешенных неориентированных графа без петель (два обыкновенных графа) G и H. $V(G)$, $V(H)$ — множества вершин этих графов, $V(G) = V(H) = \{1,\dots,n\}$ ($|V(G)| = |V(H)| = n$). $E(G)$, $E(H)$ — множества ребер G и H. Необходимо проверить, существует ли биекция $\varphi : V(G) \to V(H)$ такая, что

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

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 ее 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 $A(G)$ и $A(H)$ — матрицы смежности графов G и H. Тогда

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

где

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

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 ее рядов.

Задача ИГ принадлежит классу NP, поскольку любое биективное отображение множества вершин одного графа на множество вершин второго может быть проверено на предмет того, является ли оно изоморфизмом или нет, 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.

Алгоритмы решения задачи ИГ в ходе своей работы проверяют инвариантные относительно изоморфизма, т. е. 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 ее спектр. Инвариант является *полным* инвариантом графа, если из равенства его значений для двух графов следует их изоморфизм.

Примером подхода к проверке инвариантных характеристик является известный алгоритм Вейсфейлера — Лемана, модификации которого позволяют решать задачу ИГ за полиномиальное время для широкого класса графов. В [1] показано, как могут быть построены пары неизоморфных графов на n вершинах с тем, чтобы их нельзя было различить с помощью k-мерного алгоритма Вейсфейлера — Лемана при $k = \Omega(n)$, что равносильно неполиномиальности такого алгоритма.

Одним из подходов к построению полных инвариантов графа является использование некоторой процедуры канонизации графа, дающей его канонический код — некоторую битовую строку, являющуюся его полным инвариантом. Таким полным инвариантом графа G с матрицей смежности A является, например, канонический код $c_0(G)$:

$$c_0(G) = \max_{\pi \in S_n}\{(A)_{\pi(1)}||(A)_{\pi(2)}||\dots||(A)_{\pi(n)}\},$$

где “$||$” обозначает операцию конкатенации битовых строк, $(A)_i$ — i-ю строку матрицы A.

Не являющийся результатом канонизации полный инвариант представлен в [2] — это полный инвариант для гиперграфов, который в случае обыкновенных графов представляет собой систему из $n^2 + 1$ полиномов над полем характеристики q, где q — простое число или нуль. Также в [2] рассмотрено сведение задачи проверки изоморфизма графов к задаче разложения полинома на неприводимые множители.

В нашей работе задача ИГ для двух графов сводится к задаче проверки равенства полиномов от n переменных при некоторой перестановке номеров переменных. Полином, который ставится в соответствие графу, представляет собой модифицированный характеристический полином графа, линейный по каждой из переменных. Этот полином не является инвариантом графа в смысле неизменности его значения при различных нумерациях вершин, однако он является полным инвариантом графа в том смысле, что для пары неизоморфных графов никакая нумерация их вершин не даст одинаковых полиномов.

1. Модифицированный характеристический полином графа

Рассмотрим характеристический полином графа и некоторые его модификации, которые использовались для характеризации графов, исходя из их структурных свойств. Характеристический полином графа G — это полином

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

где x — переменная, E — единичная матрица.

Пусть $D(G) = diag(d_1, \dots, d_n)$ — диагональная матрица со степенями d_i вершин $i \in V(G)$ на диагонали. В [3] рассматриваются такие модификации характеристического полинома графа, как характеристические полиномы лапласиана $L(G)$ графа, определяемого как $L(G) = D(G) - A(G)$, беззнакового лапласиана $Q(G)$, определяемого как $Q(G) = D(G) + A(G)$, и некоторые другие модификации, обобщением которых является полином вида

$$\xi_G(x,y) = \det(xE - (A(G) - yD(G))).$$

Еще одной модификацией характеристического полинома, получаемой с помощью модификации матрицы смежности графа, является полином Зейделя [4]:

$$\zeta_G(x) = \det(xE - (F - E - 2A(G))),$$

где $(F)_{ij} = 1$ для всех $i, j = \overline{1, n}$. В [5] рассматривается обобщение характеристического полинома графа как полинома от трех переменных x, y, λ вида $\psi_G(x,y) = \det(A(x,y) - \lambda E)$, где $A(x,y)$ — матрица смежности графа G, в которой элементы, равные 1, заменяются на переменную x, а элементы, равные 0, заменяются на переменную y.

Таких модификаций характеристического полинома графа, которые являлись бы полным инвариантом графа, не представлено. Заметим, что во всех упомянутых случаях модификаций характеристического полинома рассматриваемые полиномы — это полиномы с переменными, которые 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, $X = diag(x_1, \ldots, x_n)$ — диагональная матрица с элементами x_i на диагонали.

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

$$\eta_G(x_1, \ldots, x_n) = \det(A(G) + X). \tag{1.1}$$

Представим полиномы вида (1.1) для графов на $n = 1, 2, 3$ вершинах:

1) $n = 1$: x_1;

2) $n = 2$: x_1x_2, $x_1x_2 - 1$;

3) $n = 3$: $x_1x_2x_3$, $x_1x_2x_3 - x_1$, $x_1x_2x_3 - x_1 - x_3$, $x_1x_2x_3 - x_1 - x_2 - x_3 + 2$.

Нетрудно проверить, что ни при какой нумерации вершин для пары неизоморфных графов при $n = 1, 2, 3$ мы не получим равенства их полиномов.

Далее, пусть c — некоторое подмножество элементов из $V(G)$. Через x_c обозначим произведение вида $\prod x_i$, где $i \in c$. 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 $\varphi \in S_n$ через $\varphi(c)$ обозначим множество образов элементов из c. $x_\varphi = (x_{\varphi(1)}, \ldots, x_{\varphi(n)})$ — это точка, полученная из точки $x = (x_1, \ldots, x_n)$ перестановкой ее координат в соответствии с φ.

Может быть доказана следующая теорема.

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

$$\eta_G(x_1, \ldots, x_n) = \eta_H(x_{\varphi(1)}, \ldots, x_{\varphi(n)}). \tag{1.2}$$

Равенство (1.2) имеет место в том случае, если равны коэффициенты полиномов η_G и η_H при произведениях переменных, соответствующих друг другу по φ: требуется, чтобы коэффициент $A(G)_c$ перед произведением $\prod x_i$, где $i \in c$, был равен коэффициенту $A(H)_{\varphi(c)}$ перед произведением $\prod x_{\varphi(i)}$.

Доказательство теоремы. Необходимость выполнения (1.2) для изоморфных графов G и H и их изоморфизма φ имеет место, поскольку если $G \simeq H$, то

$$A(H) = P_\varphi A(G) P_\varphi^\top, \tag{1.3}$$

а значит, коэффициенты полиномов η_G и η_H при соответствующих по φ произведениях переменных равны.

Покажем достаточность (1.2) для изоморфизма графов G и H и для того, чтобы отображение φ задавало этот изоморфизм. Обозначим $A(G)$ через $A = (a_{ij})$, а $A(H)$ через $B = (b_{ij})$.

Если верно (1.2), то из равенства полиномов следует равенство коэффициентов перед соответствующими произведениями переменных. В том числе и для любого c такого, что $c = V(G) \setminus \{i, j\}$ для пары вершин i и j, равны коэффициенты перед произведениями x_c и $x_{\varphi(c)}$, т. е. $A_c = B_{\varphi(c)}$, что эквивалентно равенству $\det\begin{pmatrix} 0 & a_{ij} \\ a_{ij} & 0 \end{pmatrix} = \det\begin{pmatrix} 0 & b_{\varphi(i)\varphi(j)} \\ b_{\varphi(i)\varphi(j)} & 0 \end{pmatrix}$, или $a_{ij} = b_{\varphi(i)\varphi(j)}$, а значит, $(i, j) \in E(G)$ тогда и только тогда, когда $(\varphi(i), \varphi(j)) \in V(H)$, т. е. $G \simeq H$ 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 в силу (1.3).

2. Проверка равенства коэффициентов модифицированных характеристических полиномов

В ходе работы представленного ниже алгоритма решения задачи ИГ производится попытка построения отображения, задающего изоморфизм графов. Для построения этого отображения производится проверка равенства коэффициентов полиномов вида (1.1) этих графов. Если построение такого отображения возможно, то графы изоморфны, иначе — не изоморфны.

Пусть $I = \{i_1, \ldots, i_m\}$ — некоторый набор без повторений из m элементов множества $\{1, \ldots, n\}$. Обозначим через C_I^k множество всех подмножеств из k элементов множества I, $C_I = \cup_{k=1}^{|I|} C_I^k$. Пусть $\{e_i\}_{i=1}^n$ — стандартный базис $\mathbb{R}^n$. Для подмножеств $c \in C_I$ определим вектор e_c как $e_c = \sum_{i \in c} e_i$. Точку ε_c для подмножества c определим как $\varepsilon \cdot e_c$, где ε — переменная, с помощью варьирования которой в ходе представленных ниже алгоритмов будем проверять равенство коэффициентов модифицированных характеристических полиномов графов. Для подмножества из одного элемента $i \in \{1, \ldots, n\}$ определим $\varepsilon_i = \varepsilon \cdot e_i$.

Представленный ниже алгоритм проверки изоморфизма графов, вызывающий рекурсивную процедуру Проверка, позволяет сравнить коэффициенты полиномов вида (1.1) для двух графов. Запись “$a \leftarrow b$” означает, что переменной a присваивается значение b. I — подмножество вершин G, для которых установлено соответствие φ, J — подмножество вершин H, являющихся образами элементов из I относительно φ.

```
ПРОВЕРКА($i$)
if $i = n$
    $flag \leftarrow true$;
    выход из процедуры
else
    for $j \leftarrow 1$ to $n$
        if ($j \notin J$ и $\forall c \in C_I$ : $\eta_G(\varepsilon_c + \varepsilon_i) = \eta_H(\varepsilon_{\varphi(c)} + \varepsilon_j)$)
            $\varphi(i) \leftarrow j$;
            $I \leftarrow I \cup \{i\}$;
            $J \leftarrow J \cup \{j\}$;
            ПРОВЕРКА($i + 1$);
$I \leftarrow I \setminus \{i\}$;
$J \leftarrow J \setminus \{\varphi(i)\}$;
значение $\varphi(i)$ не определено;
$flag \leftarrow false$.
```

```
Алгоритм проверки изоморфизма $(G, H)$
1  $I \leftarrow \varnothing$; $J \leftarrow \varnothing$; значение $\varphi(i)$ не определено для $i = \overline{1, n}$;
2  Проверка(1);
3  if $flag$
4      выдать сообщение, что $G$ и $H$ изоморфны, $\varphi$ — изоморфизм;
5  else
6      выдать сообщение, что $G$ и $H$ неизоморфны.
```

Проверка равенства коэффициентов, которая производится на 6-м шаге процедуры, состоит в поиске такого $j \in V(H) \setminus J$, что для него выполнялось бы равенство

$$\eta_G(\varepsilon_c + \varepsilon_i) = \eta_H(\varepsilon_{\varphi(c)} + \varepsilon_j). \tag{2.1}$$

Проверка производится для всех $c \in C_I$. Если ни для одного $j \in V(H) \setminus J$ равенство (2.1) не выполняется, то происходит возврат из рекурсивно вызываемой процедуры со значением $flag$, равным $false$. Выход из этой процедуры со значением $flag$, равным $true$, происходит только в случае установления изоморфизма φ графов G и H.

Сравнение коэффициентов полиномов η_G и η_H для графов G и H и подмножеств $c \in C_I$ производится последовательно: от подмножеств меньшей мощности к подмножествам большей мощности. На старте алгоритма $I = \varnothing$, $C_I = \varnothing$, $J = \varnothing$. Для $i = 1$ проверка равенства (2.1) — это проверка равенства

$$\eta_G(\varepsilon_1) = \eta_H(\varepsilon_j) \tag{2.2}$$

для $j \in V(H)$. Равенство (2.2) эквивалентно равенству

$$\det A + A_{\{1\}}\varepsilon = \det B + B_{\{j\}}\varepsilon. \tag{2.3}$$

Если мы имеем (2.3) при $\varepsilon = 0$ и некотором $\varepsilon > 0$, то $\det A = \det B$, $A_{\{1\}} = B_{\{j\}}$, что приводит к установлению соответствия для $\varphi(1)$: $\varphi(1) \leftarrow j$. Если в дальнейшем произойдет выход из процедуры Проверка со значением $flag$, равным $false$, то значение $\varphi(1)$, возможно, снова будет не определено.

Для $i = 2$, когда мы имеем $I = \{1\}, C_I = C_I^1 = \{\{1\}\}$, $J = \{\varphi(1)\}$, необходимо найти $j \in V(H) \setminus J$ такое, что

$$\eta_G(\varepsilon_2) = \eta_H(\varepsilon_j) \tag{2.4}$$

и

$$\eta_G(\varepsilon_1 + \varepsilon_2) = \eta_H(\varepsilon_{\varphi(1)} + \varepsilon_j). \tag{2.5}$$

Проверка равенства (2.4) — это проверка равенства

$$\det A + A_{\{2\}}\varepsilon = \det B + B_{\{j\}}\varepsilon, \tag{2.6}$$

проверка равенства (2.5) — это проверка равенства

$$\det A + A_{\{1\}}\varepsilon + A_{\{2\}}\varepsilon + A_{\{1,2\}}\varepsilon^2 = \det B + B_{\{\varphi(1)\}}\varepsilon + B_{\{j\}}\varepsilon + B_{\{\varphi(1),j\}}\varepsilon^2. \tag{2.7}$$

Если (2.3) имеет место при $\varepsilon = 0$ и некотором $\varepsilon > 0$, то выполнение (2.6) для некоторого $\varepsilon > 0$ дает равенство $A_{\{2\}} = B_{\{j\}}$, что при выполнении (2.7) дает равенство $A_{\{1,2\}} = B_{\{\varphi(1),j\}}$. Если это так, то алгоритмом будет установлено соответствие $\varphi(2) \leftarrow j$, которое в дальнейшем, если произойдет выход из процедуры Проверка со значением $flag$, равным $false$, может снова оказаться не определенным.

На момент проверки равенства коэффициентов $A_{c\cup\{i\}}$ и $B_{\varphi(c)\cup\{j\}}$ $(\varphi(c) \subset \varphi(I) = J)$ для $c \in C_I$ имеем равенства $A_c = B_{\varphi(c)}$ для всех таких c, поскольку в противном случае ранее произошел бы выход из рекурсивно вызываемой процедуры Проверка со значением $flag$ равным $false$. Таким образом,

$$\eta_G(\varepsilon_c + \varepsilon_i) = \sum_{c' \in P(c)} \varepsilon^{|c'|} A_{c'} + \varepsilon^k A_{c \cup \{i\}}, \tag{2.8}$$

$$\eta_H(\varepsilon_{\varphi(c)} + \varepsilon_j) = \sum_{\varphi(c') \in Q(c)} \varepsilon^{|c'|} B_{\varphi(c')} + \varepsilon^k B_{\varphi(c) \cup \{j\}}, \tag{2.9}$$

где $P(c) = \{c' \in C_{I \cup \{i\}} \,|\, c' \subset c\}$, $Q(c) = \{\varphi(c') \in C_{\varphi(I) \cup \{j\}} \,|\, c' \subset c\}$, $k = |c| + 1 > |c'|$ для любого $c' \in P(c)$. Так как для любого $c' \in P(c)$ на момент проверки равенства (2.1) имеем $A_{c'} = B_{\varphi(c')}$, где $\varphi(c') \in Q(c)$, то, если (2.1) имеет место для любого $c \in C_I$, из него по (2.8) и (2.9) следует, что для тех же $c \in C_I$ выполняется равенство $A_{c \cup \{i\}} = B_{\varphi(c) \cup \{j\}}$. Полагая $\varphi(i) \leftarrow j$ и $I \leftarrow I \cup \{i\}$, $J \leftarrow J \cup \{j\}$, мы снова будем получать $A_c = B_{\varphi(c)}$ для любого подмножества $c \in C_I$.

В итоге, если выход из рекурсивно вызываемой процедуры Проверка происходит со значением $flag$, равным $true$, то это означает следующее: в ходе работы алгоритма найдена биекция φ такая, что равны все 2^n соответствующих коэффициентов η_G и η_H для всех $c \in C_I$, где $I = \{1, \ldots, n\}$, а значит, по доказанной теореме φ — изоморфизм графов G и H.

Выводы

В работе представлено сведение задачи проверки изоморфизма графов для двух графов на n вершинах к задаче проверки равенства ставящихся им в соответствие полиномов от n переменных при некоторой перенумерации вершин одного из графов. Полином, ставящийся в соответствие графу, — это модифицированный характеристический полином графа, линейный по каждой из переменных.

СПИСОК ЛИТЕРАТУРЫ

1. **Cai J-Y., Fürer M., Immerman N.** An optimal lower bound on the number of variables for graph identification // Combinatorica. 1992. Vol. 12, no. 4. P. 389–410.
2. **Григорьев Д.Ю.** Два сведения изоморфизма графов к задачам о полиномах // Записки науч. семинара ЛОМИ. Т. 88. Л.: Наука, 1979. С. 56–61.
3. **Цветкович Д., Дуб М., Захс Х.** Спектры графов. Теория и применение. Киев: Наук. Думка, 1984. С. 24–28.
4. **Seidel J.J.** Strongly regular graphs with $(-1, 1, 0)$ adjacency matrix having eigenvalue 3 // Lin. Alg. Appl. 1968. Vol. 1, no. 2. P. 281–298.
5. **Lipton R.J., Vishnoi N.K., Zalcstein Z.** A generalization of the characteristic polynomial of a graph [e-resource] // CC Technical Report, GIT-CC-03-51. 2003. URL: https://smartech.gatech.edu/bitstream/handle/1853/6511/GIT-CC-03-51.pdf (дата обращения: 07.09.2015).

Пролубников Александр Вячеславович
канд. физ.-мат. наук
доцент
Омский государственный университет
e-mail: a.v.prolubnikov@mail.ru

Поступила 26.12.2014