

ЭВРИСТИЧЕСКИЙ АЛГОРИТМ ДЕШИФРОВКИ ШИФРА ДВОЙНОЙ ПЕРЕСТАНОВКИ

А.В. Пролубников, Р.Т. Файзуллин

In the paper we consider heuristic algorithm for solving graph isomorphism problem. The algorithm based on a successive splitting of the eigenvalues of the matrices which are modifications (to positive defined) of graphs' adjacency matrices. Modification of the algorithm allows to find a solution for Frobenius problem. Formulation of the Frobenius problem is following one. Given a pair of two matrices with the same number of rows and columns. We must find out whether one of the matrix can be acquired from another by permutation of it's rows and strings or not. Solution of Frobenius problem can give to us efficient way for decrypting of double permutation cyphers problem for high dimension matrices.

1. Изоморфизм графов

В работе представлен эвристический алгоритм решения задачи определения изоморфности графов, основанный на последовательном расщеплении собственных чисел, видоизмененных (до положительно определенных) матриц смежности, и решении систем линейных уравнений, определяющих обратные матрицы. Сравнение норм столбцов обратных матриц позволяет получить решающую перестановку.

Задача проверки изоморфности графов принадлежит к задачам, относительно которых нет ясности: являются ли они полиномиально разрешимыми или нет [1]. В то же время известно, что задача определения изоморфности графа является полиномиально разрешимой для некоторых классов графов, в частности для планарных, регулярных графов и некоторых других построены эффективные алгоритмы, для решения этой задачи [2], [3], [4]. Предлагаемый нами алгоритм является эвристическим алгоритмом для проверки изоморфности графов.

В задаче даны два неориентированных графа $G_A = \langle V_A, E_A \rangle$ и $G_B = \langle V_B, E_B \rangle$, где V_A, V_B – множества вершин графов, E_A, E_B – множества ребер. Предполагается, что $|V_A| = |V_B|$, $|E_A| = |E_B|$. Задача изоморфизма графов формулируется следующим образом: существует ли биективное отображение $\varphi : V_A \rightarrow V_B$, такое, что если $(i, j) \in E_A$, то $(\varphi(i), \varphi(j)) \in E_B$?

Предлагаемый алгоритм для решения задачи определения изоморфности графов работает с видоизмененными матрицами смежности графов.

© 2002 А.В. Пролубников, Р.Т. Файзуллин

E-mail: e-mail: faizulin@univer.omsk.su, prolubnikov@math.omskreg.ru

Омский государственный университет

Пусть A_0 – матрица смежности G_A , то есть $A_0 = (a_{ij}^0)$, где

$$a_{ij}^0 = \begin{cases} 1, & \text{если } (i, j) \in E_A, \\ 0, & \text{иначе.} \end{cases}$$

B_0 – матрица смежности графа G_B .

По матрице A_0 строим матрицу D_{A_0} :

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}.$$

D_{A_0} – диагональная матрица со следующими элементами:

$$d_i = \sum_{j=1}^n a_{ij}^0 + 1.$$

Аналогично строится матрица D_{B_0} по матрице смежности графа G_B .

Рассматриваемые далее матрицы

$$A = A_0 + D_{A_0}, \quad B = B_0 + D_{B_0} \quad (1)$$

– матрицы, с которыми будет работать алгоритм, являются симметричными положительно определенными матрицами.

Если графы $G_A = \langle V_A, E_A \rangle$ и $G_B = \langle V_B, E_B \rangle$ изоморфны, то соответствующие им матрицы описанного типа могут быть получены одна из другой перестановкой строк с одновременной перестановкой столбцов с теми же номерами. Таким образом, задача проверки изоморфности двух графов может быть сформулирована как частный случай задачи Фробениуса: может ли быть получена матрица B из матрицы A последовательной перестановкой строк с одновременной перестановкой столбцов?

Для произвольной матрицы перестановка строк с номерами i и j эквивалентна ее умножению на матрицу перестановки P_{ij} . Перестановка столбцов матрицы эквивалентна ее умножению справа на ту же матрицу. При умножении вектора на матрицу P_{ij} как справа, так и слева происходит перестановка компонент вектора с номерами i и j .

Рассмотрим две системы уравнений следующего вида:

$$Ax = e_j, \quad By = e_k, \quad (2)$$

где векторы $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ – базисные векторы в пространстве R^n , матрицы A и B – описанного выше вида. Обе системы уравнений имеют решение, и решение единственно, так как A и B – матрицы с диагональным преобладанием, и, следовательно, их определители не равны нулю. Пусть далее x^j – решение системы линейных уравнений $Ax = e_j$, y^k – решение системы линейных уравнений $By = e_k$.

Отметим, что, решив системы уравнений (1), получим обратные матрицы для A и B . Так, для i -й компоненты вектора x^j верно: $x_i^j = (-1)^{i+j} A_{ij} / \det(A)$, где A_{ij} – алгебраическое дополнение элемента a_{ij} матрицы A . То есть векторы решений x^j , $j = 1, \dots, n$ являются столбцами обратной к A матрицы.

Если $B = P_{jk}AP_{jk}$, то для решения систем уравнений (2) должны выполняться равенства:

$$x_i = y_i, \quad i \neq j, \quad i \neq k;$$

$$x_j = y_k, \quad x_k = y_j.$$

Действительно: $(Ax = e_j) \sim (P_{jk}Ax = P_{jk}e_j) \sim (P_{jk}AxP_{jk} = P_{jk}e_jP_{jk}) \sim (P_{jk}AP_{jk}x = e_j) \sim (P_{jk}AP_{jk}xP_{jk} = e_jP_{jk}) \sim (BxP_{jk} = e_k)$. То есть $xP_{jk} = y$.

Если матрица B получена из матрицы A многократной одновременной перестановкой строк и столбцов, то:

$$B = P_{j_1k_1} \dots P_{j_1k_1}AP_{j_1k_1} \dots P_{j_1k_1},$$

и, соответственно, $xP_{j_1k_1} \dots P_{j_1k_1} = y$.

Таким образом, если мы будем менять вектор e_k в системе уравнений (2) при фиксированном j , то есть индекс k будет пробегать значения $1, \dots, n$, то векторы x^j и y^k – соответствующие друг другу решения полученных систем (2) будут совпадать с точностью до перестановки компонент только в том случае, если строке j матрицы A соответствует строка k матрицы B . То есть элементы строки k матрицы B есть переставленные элементы строки i матрицы A . То же верно и для столбцов матриц.

При нахождении в матрице B строки и столбца, соответствующих строке и столбцу с номером i матрицы A , на каждой i -й итерации алгоритма будем последовательно производить возмущения ее диагональных элементов. Алгоритм работает с симметричными матрицами, которые могут быть приведены к диагональной форме с помощью ортогональных преобразований. То есть

$$\tilde{A} = U_A A U_A^T,$$

$$\tilde{B} = U_B B U_B^T,$$

где \tilde{A} , \tilde{B} – диагональные матрицы с собственными значениями на диагонали, а U_A , U_B – матрицы ортогональных преобразований. Диагональные элементы \tilde{A} , \tilde{B} – собственные числа матриц A и B .

Спектры матриц смежности изоморфных графов совпадают [5]. То же можно сказать и о спектрах матриц, с которыми работает алгоритм, так как описанная выше процедура замены нулевых диагональных элементов матрицы смежности приводит лишь к сдвигу спектра матрицы. Причем, если матрицы соответствуют изоморфным графам, то спектры матриц будут совпадать и после сдвига.

Очевидно, если спектр каждой матрицы является простым, то есть среди собственных значений матрицы нет кратных, то задача определения изоморфности графов разрешима однозначно путем сопоставления матриц \tilde{A} , \tilde{B} , U_A и U_B .

Основные трудности возникают при рассмотрении графов, спектры которых содержат кратные собственные значения. Возмущая матрицы в ходе итераций алгоритма, мы будем получать возмущение спектра матриц, при котором происходит расщепление кратных собственных значений, что позволяет установить однозначное соответствие между строками и столбцами матриц.

В итоге, если среди собственных значений матриц A и B есть кратные, то в ходе работы алгоритма они будут расщеплены, и будет возможно получение перестановки, задающей искомое отображение φ , устанавливающее изоморфизм графов $G_A = \langle V_A, E_A \rangle$ и $G_B = \langle V_B, E_B \rangle$. Численные эксперименты показывают, что расщепление спектра матриц, необходимое для определения соответствующих друг другу строк и столбцов матриц, происходит значительно раньше заключительной итерации.

В ходе работы алгоритма на каждой итерации будем работать не с исходными, но с уже возмущенными в ходе предыдущих итераций алгоритма матрицами. Так, получив соответствие между строкой j матрицы A^j и строкой k матрицы B^j на итерации j , а также столбцами с теми же номерами, рассматриваем далее возмущенные матрицы A^{j+1} и B^{j+1} :

$$A^{j+1} = A^j + \varepsilon C^j, \quad B^{j+1} = B^j + \varepsilon C^k.$$

Возмущения производим с помощью диагональных матриц C^k с диагональными элементами

$$c_i = \begin{cases} 1, & \text{если } i = j = k, \\ 0, & \text{иначе.} \end{cases}$$

В результате, если матрица B может быть получена из матрицы A последовательными одновременными перестановками строк и столбцов, то пока j пробегает значения от 1 до n , будет получена, вообще говоря, одна из возможных перестановок строк и столбцов матрицы A :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

где k_j – номер строки матрицы B , полученный на j -й итерации работы алгоритма.

Перестановка задает такую перенумерацию вершин графа G_A , то есть отображение $\varphi : V_A \rightarrow V_B$, при которой матрицы A и B , представляющие графы, совпали бы, что возможно только в случае изоморфности графов.

Алгоритм спектрального расщепления проверки изоморфности графов

Шаг 0. $A^0 := A, j := 1$.

Шаг 1. Если $j < n$, то $A^j := A^{j-1} + \varepsilon C^j$, иначе работу алгоритма завершить.

Шаг 2. Решение системы уравнений $Ax = e_j$. x^j – полученное решение.

Шаг 3. $k := 1$. Если $k < n$, то – Шаг 3.1, иначе перейти на Шаг 4.

Шаг 3.1. $B^k := B^{k-1} + \varepsilon C^k$.

Шаг 3.2. Решение системы уравнений $B^k y = e_k$. y^k – полученное решение.

Шаг 3.3. $k := k + 1$. Перейти на Шаг 3.

Шаг 4. Сравнение норм x^j и y^k , $k = 1, \dots, n$.

Если $\forall k \ ||x^j|| \neq ||y^k||$, то графы G_A и G_B неизоморфны. Работу алгоритма завершить.

Если $\exists k : ||x^j|| = ||y^k||$ и $x_j^j = y_k^k$, то вершине j графа G_A ставим в соответствие вершину k графа G_B . Иначе графы G_A и G_B неизоморфны. Работу алгоритма завершить.

Шаг 5. $j := j + 1$. Перейти на Шаг 1.

Трудоёмкость представленной схемы алгоритма равна $O(n^4)$, где n — число строк в квадратных матрицах A и B , подающихся на вход алгоритма. Следует отметить, что с добавлением процедуры проверки спектра матриц A и B на расщепленность схема алгоритма может быть модифицирована до схемы с трудоёмкостью $O(n^{3.5})$.

2. Решение задачи Фробениуса для произвольных квадратных матриц полного ранга

Алгоритм спектрального расщепления проверки изоморфности неориентированных графов может быть применен без каких-либо модификаций для проверки изоморфности взвешенных неориентированных графов. Схема алгоритма остается в точности той же, модифицируются только представляющие графы матрицы, с которыми работает алгоритм.

В задаче даны два неориентированных графа $G_A = \langle V_A, E_A \rangle$ и $G_B = \langle V_B, E_B \rangle$, где V_A, V_B — множества вершин графов, E_A, E_B — множества ребер. Предполагается, что $|V_A| = |V_B|$, $|E_A| = |E_B|$. На множествах ребер графов G_A и G_B определены функции $H_A : E_A \rightarrow R$ и $H_B : E_B \rightarrow R$, задающие веса ребер. Задача определения изоморфизма взвешенных графов формулируется следующим образом: существует ли биективное отображение $\varphi : V_A \rightarrow V_B$, такое, что если $(i, j) \in E_A$, то $(\varphi(i), \varphi(j)) \in E_B$ и $H_A(i, j) = H_B(\varphi(i), \varphi(j))$?

Матрицы смежности взвешенных неориентированных графов также преобразуются до положительно определенных матриц с диагональным преобладанием, но при этом диагональные элементы подбираются так, чтобы числа обусловленности матриц, с которыми работает алгоритм, были ограничены.

Пусть $A_0 = (a_{ij}^0)$ — матрица смежности взвешенного ориентированного графа G_A . D_{A_0} — диагональная матрица с элементами d_i :

$$d_i = d + \sum_{j=1}^n a_{ij}^0,$$

где $d = \max_{1 \leq i \leq n} \sum_{j=1}^n a_{ij}^0$. Таким же образом строится матрица D_{B_0} для взвешенного неориентированного графа G_B по его матрице смежности B_0 .

Для числа обусловленности $\mu(A)$ симметричной матрицы A справедлива следующая оценка [6]:

$$\mu(A) \leq \frac{\eta(A)}{\chi(A)},$$

где $\eta(A) = \max_{1 \leq i \leq n} (a_{ii} + \sum_{j \neq i} |a_{ij}|)$, $\chi(A) = \min_{1 \leq i \leq n} (a_{ii} - \sum_{j \neq i} |a_{ij}|)$.

При нашем выборе d

$$\begin{aligned} \eta(A) &= \max_{1 \leq i \leq n} (a_{ii} + \sum_{j=1}^n |a_{ij}^0|) = a_{i_1 i_1} + \sum_{j=1}^n |a_{i_1 j}^0| = d_{i_1} + \sum_{j=1}^n |a_{i_1 j}^0| = d + 2 \sum_{j=1}^n |a_{i_1 j}^0| = \\ &= 3 \sum_{j=1}^n |a_{i_1 j}^0|, \end{aligned}$$

$$\begin{aligned} \chi(A) &= \min_{1 \leq i \leq n} (a_{ii} - \sum_{j=1}^n |a_{ij}^0|) = a_{i_2 i_2} - \sum_{j=1}^n |a_{i_2 j}^0| = d_{i_2} - \sum_{j=1}^n |a_{i_2 j}^0| = \sum_{j=1}^n |a_{i_2 j}^0| + d - \\ &- \sum_{j=1}^n |a_{i_2 j}^0| = \sum_{j=1}^n |a_{i_2 j}^0| + \sum_{j=1}^n |a_{i_1 j}^0| - \sum_{j=1}^n |a_{i_2 j}^0| = \sum_{j=1}^n |a_{i_1 j}^0|. \end{aligned}$$

Следовательно,

$$\mu(A) = \frac{\eta(A)}{\chi(A)} \leq \frac{3 \sum_{j=1}^n |a_{i_1 j}^0|}{\sum_{j=1}^n |a_{i_1 j}^0|} = 3.$$

В задаче Фробениуса даны две матрицы F_A и F_B с одинаковым числом строк и столбцов. Требуется определить, может ли одна из матриц быть получена из другой при помощи некоторой перестановки ее строк и столбцов.

Будем считать, что матрицы F_A и F_B — квадратные матрицы полного ранга с числом строк, равным n . Матрица A_0 вида

$$\begin{pmatrix} 0 & F_A \\ F_A^T & 0 \end{pmatrix}$$

может рассматриваться как матрица смежности некоторого взвешенного неориентированного графа. Построив для матрицы A_0 матрицу D_{A_0} описанного выше вида, ставим в соответствие исходной матрице F_A матрицу A :

$$A = A_0 + D_{A_0}.$$

То есть

$$A = \begin{pmatrix} D_{A_0}^1 & F_A \\ F_A^T & D_{A_0}^2 \end{pmatrix}$$

и

$$D_{A_0} = \begin{pmatrix} D_{A_0}^1 & 0 \\ 0 & D_{A_0}^2 \end{pmatrix},$$

где

$$D_{A_0}^1 = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}, \quad D_{A_0}^2 = \begin{pmatrix} d_{n+1} & 0 & \dots & 0 \\ 0 & d_{n+2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_{2n} \end{pmatrix}.$$

Итак, A — симметричная положительно определенная матрица с диагональным преобладанием, соответствующая некоторому двудольному взвешенному неориентированному графу. Матрица F_B — квадратная матрица с тем же числом строк, что и матрица F_A . Аналогично ставим в соответствие матрице F_B матрицу B . Применяя к матрицам A и B описанный выше алгоритм, формируем решающую перестановку строк и столбцов матриц A и B .

По перестановкам строк и столбцов матриц A и B формируем перестановки строк и столбцов исходных матриц F_A и F_B следующим образом. Пусть алгоритмом получено соответствие строки и столбца номер i матрицы A столбцу и строке номер j матрицы B . Очевидно, что если $1 \leq i \leq n$, $1 \leq j \leq n$, то перестановка пары строк $\{i, j\}$ и столбцов $\{i, j\}$ матрицы A соответствует перестановке строк i и j исходной матрицы F_A . Если $n+1 \leq i \leq 2n$, $n+1 \leq j \leq 2n$, то перестановка пары строк $\{i, j\}$ и столбцов $\{i, j\}$ матрицы A соответствует перестановке столбцов i и j исходной матрицы F_A . Так как матрицы A и B , с которыми работает алгоритм, имеют вид:

$$\begin{pmatrix} * & 0 & \dots & 0 & * & * & \dots & * \\ 0 & * & \dots & 0 & * & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & * & * & * & \dots & * \\ * & * & \dots & * & * & 0 & \dots & 0 \\ * & * & \dots & * & 0 & * & \dots & 0 \\ \vdots & \vdots & & * & \vdots & \vdots & \ddots & \vdots \\ * & * & \dots & * & 0 & 0 & \dots & * \end{pmatrix},$$

где $*$ обозначены позиции, допустимые для ненулевых элементов, то ситуация, когда алгоритм поставил бы в соответствие друг другу пару строк и столбцов матриц A и B с номерами $\{i, j\}$ и $1 \leq i \leq n$, $n+1 \leq j \leq 2n$ невозможна, так как после такой перестановки строк и столбцов, если исходные матрицы F_A и F_B не являются диагональными, в левой верхней части матрицы A (в матрице $D_{A_0}^1$) и правой нижней части (в матрице $D_{A_0}^2$) появились бы кроме диагональных дополнительные ненулевые элементы, чего не может быть по построению матриц A и B . Следовательно, получение такого соответствия в ходе работы алгоритма невозможно.

3. Дешифрование шифра двойной перестановки при помощи алгоритма спектрального расщепления

Пусть исходный текст представлен некоторой квадратной матрицей символов. Формируем матрицу шифра, где каждому символу текста поставлен в соответствие его некоторый числовой код. Вторая матрица представляет собой также некоторый кодированный таким же образом текст. Требуется определить, является ли текст, представленный второй матрицей, шифром двойной перестановки текста, представленного первой матрицей. То есть требуется определить,

является ли он текстом, полученным из первой текстовой матрицы при помощи перестановок ее строк и столбцов. Такая задача может быть интерпретирована как задача Фробениуса для пар числовых матриц, и, следовательно, для ее решения может быть применен алгоритм спектрального расщепления проверки изоморфности графов.

В ходе вычислительного эксперимента установлено, что для успешного решения задач проверки изоморфности неориентированных невзвешенных и взвешенных графов при решении систем линейных уравнений достаточно 60-ти итераций метода Зейделя для достижения необходимой точности при том, что расщепление спектра происходит за число итераций, не превышающее числа групп кратных собственных значений матриц A и B , подаваемых на вход алгоритма. Для задач проверки изоморфности графов проведены вычислительные эксперименты, в частности, для регулярных графов с числом вершин до 2500. Для задач дешифрования шифра двойной перестановки проведены вычислительные эксперименты с текстами с числом символов до 5000.

ЛИТЕРАТУРА

1. Гэри М., Джонсон Д. *Вычислительные машины и труднорешаемые задачи*. М.: Мир, 1982.
2. Hopcroft, Wong *A linear time algorithm for isomorphism of planar graphs*. Proceedings of the Sixth Annual ACM Symposium on Theory of Computing. 1974. P.172–184.
3. Luks *Isomorphism of graphs of bounded valence can be tested in polynomial time*. Proc. 21st IEEE FOCS Symp., 42, 49, 1980.
4. Hoffmann *Group-Theoretic Algorithms and Graph Isomorphism*. Lecture Notes in Computer Science (Chapter V). 1982. P.127–138.
5. Цветкович Д. и др. *Спектры графов. Теория и применение*. Киев: Наукова думка, 1984.
6. Годунов С.К. и др. *Гарантированная точность решения систем линейных уравнений в евклидовых пространствах*. Новосибирск: Наука, 1988.