Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

О МИНИМАЛЬНЫХ ПРИМИТИВНЫХ МАТРИЦАХ

Р. И. Бар-Гнар, В. М. Фомичев

Исследуется подход к минимизации реализации преобразований, степень которых реализует полное перемешивание входных данных. Введены понятия минимальной примитивной матрицы и высоты примитивной матрицы. Получены оценки числа минимальных примитивных матриц порядка n. Построены и проанализированы алгоритмы поиска минимальных примитивных матриц и оценки близости примитивной матрицы к множеству минимальных примитивных матриц.

Ключевые слова: *примитивная матрица, решётка, антицепь, вычислительная сложность алгоритма.*

Введение

Для оценки свойства перемешивания входов композиции преобразований часто применяется матрично-графовый подход [1, гл. 10], основанный на определении экспонентов перемешивающих матриц (графов). Обзор основных результатов по этому направлению имеется в [2].

Аппаратная и программная реализация совершенных преобразований, реализующих полное перемешивание, затруднена необходимостью реализации большого количества связей между компонентами входных и выходных векторов. В связи с этим в работе введено и исследовано понятие минимальной примитивной матрицы, позволяющей оценить предельные возможности уменьшения количества связей между входом и выходом при сохранении свойства полного перемешивания у композиции преобразований.

1. Свойства минимальных примитивных матриц

Обозначим через $M_0(n)$ множество квадратных $0,1$-матриц порядка n, $S(n)$ — множество подстановочных матриц, $P(n)$ — множество примитивных матриц.

Примитивная матрица (граф) называется минимальной, если после замены любой единицы нулём (после удаления любой дуги) получается непримитивная матрица (граф). Обозначим множество минимальных примитивных матриц через $P_{\min}(n)$.

Утверждение 1. Если примитивные матрицы $A, B \in M_0(n)$ сопряжены в $S(n)$ и примитивны, то они одновременно минимальные или неминимальные.

Рассмотрим на множестве $M_0(n)$ отношение частичного порядка: $A \leqslant B \Leftrightarrow a_{i,j} \leqslant b_{i,j}$ для всех $i, j = 1, \ldots, n$, где $A = (a_{i,j}), B = (b_{i,j})$. Множество $M_0(n)$ образует решётку в смысле отношения $\leqslant$, где матрица, все элементы которой равны 1, является наибольшим элементом, а нулевая матрица — наименьшим. Подмножество примитивных

матриц $P(n)$ множества $M_0(n)$ является верхней полурешёткой. Минимальные примитивные матрицы — это все минимальные элементы верхней полурешётки $P(n)$.

В частично упорядоченном множестве X антицепь Y назовем наибольшей, если она имеет наибольшую мощность, и максимальной, если любой элемент множества X сравним с некоторым элементом антицепи Y.

Утверждение 2. $P_{\min}(n)$ есть максимальная антицепь полурешётки $P(n)$.

Число единиц матрицы $A \in M_0(n)$ называется весом матрицы A (обозначается $||A||$). Назовём k-м слоем подрешётки R решётки $M_0(n)$ подмножество (обозначается $R^{(k)}$), состоящее из матриц веса k, где $k = 0, 1, \ldots, n^2$. Заметим, что $R^{(k)}$ есть антицепь решётки R при всех k.

Утверждение 3. При $n > 3$ выполнена оценка

$$3n! \leqslant |P_{\min}(n)| \leqslant C_m^{\lfloor m/2 \rfloor}, \text{ где } m = n^2.$$

Нижняя оценка получена с использованием свойства $P^{(n+1)}(n) \subseteq P_{\min}(n)$, где $P^{(n+1)}(n)$ содержит три класса орграфов, порядки которых равны $n!$:

1) полный цикл с добавленной дугой $(i-1, i+1), i \in \{1, \ldots, n\}$ (рис. 1,*а*);
2) полный цикл с добавленной петлей в вершине $i \in \{1, \ldots, n\}$ (рис. 1,*б*);
3) класс графов, вид которых зависит от чётности числа n: при чётном n граф состоит из двух циклов длины 2 и $l = n - 1$ (рис. 1,*в*); при нечётном — из двух циклов длины 2 и $l = n$ (рис. 1,*г*). В обоих случаях $(2, l) = 1$, поэтому в соответствии с критерием [3, с. 226] графы примитивные.

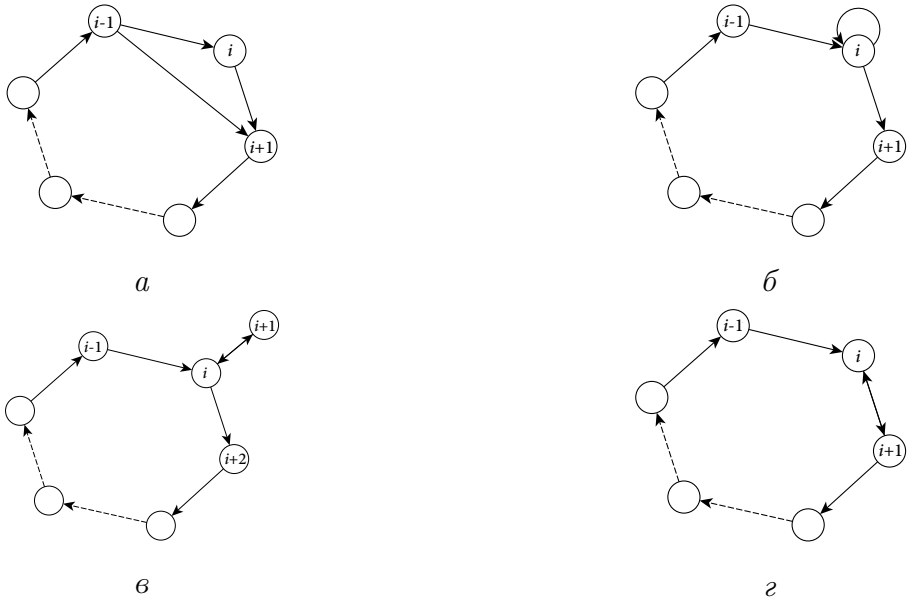

Рис. 1. Примеры минимальных графов из $P^{(n+1)}(n)$

Улучшение нижней оценки возможно на основе обобщения случая 3 (рассмотрения некоторых классов графов из слоев $P^{(n+r)}(n)$ при $r > 1$).

2. Высота примитивной матрицы

Расстоянием по Хэммингу между $0,1$-матрицами A и B (обозначается $\mathrm{d}(A, B)$) называется число различных соответствующих элементов матриц A и B:

$$\mathrm{d}(A, B) = \sum_{i,j} (a_{i,j} \oplus b_{i,j}).$$

Высотой примитивной матрицы A (обозначается $\mathrm{h}(A)$) называется расстояние по Хэммингу между A и ближайшей минимальной примитивной матрицей $M \in P_{\min}(n)$:

$$\mathrm{h}(a) = \min_{M \in P_{\min}(n)} \mathrm{d}(A, M).$$

Величина $\mathrm{h}(A)$ является определённой мерой избыточности при построении связей между элементами входа и выхода преобразований информации.

Алгоритм оценивания $\mathbf{h}(A)$ (метод координатного спуска):

1) последовательно просматривая элементы матрицы A, находим единицы;
2) заменяем найденный единичный элемент в матрице A нулевым и для полученной матрицы A' выполняем:
   - проверяем в A' наличие нулевых строк и столбцов; если таковые есть, возвращаемся к выполнению п. 2 для следующей единицы матрицы A;
   - матрицу A' без нулевых строк и столбцов проверяем на примитивность;
   - если матрица A' не примитивная, возвращаемся к матрице A, восстанавливаем замененную единицу и выполняем п. 2 для следующей единицы матрицы A;
   - примитивную матрицу A' проверяем на минимальность;
   - если A' минимальная, то определяем m — число единиц, заменённых нулями;
   - если A' не минимальная, то переходим к выполнению п. 1 для матрицы A'.

На выходе алгоритма получим минимальную примитивную матрицу M, где

$$\mathrm{h}(A) \leqslant \mathrm{d}(A, M) = m.$$

Сложность алгоритма полиномиальная. Пусть $||A|| = k$, где $n < k \leqslant n^2$ для примитивной матрицы A. Тогда вычислительная сложность алгоритма в битовых операциях в худшем случае не превышает величины $\mathrm{O}(k^2 n^3 \log n)$. Объём памяти требуется порядка $\mathrm{O}(n^2)$ битов. Данный метод можно использовать для поиска минимальных матриц, близких к перемешивающим матрицам раундовых подстановок блочных шифров (DES, ГОСТ 28147-89 и др.).

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
3. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.

УДК 519.1:511.2

ЧИСЛА ЭЙЛЕРА НА МНОЖЕСТВАХ ПЕРЕСТАНОВОК И АНАЛОГИ ТЕОРЕМЫ ВИЛЬСОНА

Л. Н. Бондаренко, М. Л. Шарапова

Определяются числа Эйлера на множествах перестановок и с их помощью доказываются аналоги теоремы Вильсона для чисел стандартных полных отображений и чисел стандартных сильных полных отображений.

Ключевые слова: *перестановка, числа Эйлера, полные отображения, теорема Вильсона.*