УДК 681.3.06: 519.248.681

И.В. ЛИСИЦКАЯ канд. тех. наук, Т.В. ЦЕПУРИТ, С.В. СУПРОНЮК

АЛГОРИТМ ПОРОЖДЕНИЯ ПРОТИВОРЕЧИВЫХ ПОДСТАНОВОК

В работе [1] обоснована возможность применения для построения долговременных ключей алгоритма ГОСТ 28147-89 противоречивых подстановок. Показано, что порождать таблицы, построенные из таких подстановок случайным образом, безнадежно. В этой работе будет обоснован один из практически реализуемых алгоритмов порождения таблиц, составленных из противоречивых подстановок.

Будем рассматривать таблицу из m подстановок n-ой степени в виде матрицы $S_{m,n}$, нулевая строка которой – упорядоченная перестановка 1,2,3, . . . , n в сочетании с любой другой строкой-перестановкой матрицы образует подстановку. Нас будет интересовать задача построения матрицы $S_{m,n}$, в столбцах которой отсутствуют совпадения чисел, а в строках нет повторений, т.е. латинского прямоугольника размером $m \times n$ [2]. Она может быть интерпретирована как задача о нахождении максимального паросочетания в двудольном графе [2] (в нашем случае – графе $B_{n,n}$ с равными долями). Иногда для наглядности эту задачу представляют также как задачу нахождения максимальной системы браков: вершины одной доли графа интерпретируются как мужчины, вершины другой доли - как женщины, ребра графа задают допустимые браки. Нужно найти максимальное паросочетание в смысле числа брачных пар [3].

Продемонстрируем идею предлагаемого метода на примере определения системы подстановок $S_{4,5}$.

Для латинского прямоугольника 4 × 5 первая подстановка (нулевая и первая строка матрицы) не должна содержать идентичных элементарных переходов i в i. В терминах браков нулевая строка, которая не проставляется, – это мужчины 1, 2, 3, 4, 5, а другие строки – это женщины 1′, 2′, 3′, 4′, 5′. Для $i = 1 \div 5$, i-ый мужчина может жениться на любой женщине кроме той, которая имеет одинаковый с ним номер, т.е. в графе $B_{5,5}$ присутствуют все ребра, кроме (1, 1), (2, 2), (3, 3), (4, 4) и (5, 5). Представим такой граф матрицей E диагонального типа, с элементами 0 и 1 в виде:

$$E = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Номера столбцов матрицы соответствуют номерам вершин одной доли графа (номерам женщин), а номера строк соответствуют номерам вершин второй доли графа (номерам мужчин). Наличие 1 на позициях E_{ii}, $i = 1 \div 5$ обозначает отсутствие соответствующих ребер графа, наличие нуля на пересечении i-ого столбца и j-ой строки обозначает возможность соединения соответствующих вершин ребром (возможность брака i-ой женщины и j-ого мужчины).

Породим случайное число из интервала [1, n-k], где n –число столбцов матрицы, а k – номер цикла алгоритма (на данный момент - это первый цикл). Под циклом будем понимать построение полного паросочетания графа. Пусть для первого цикла это будут числа $r_1 = 4, r_2 = 1, r_3 = 1, r_4 = 2$.

Далее алгоритм продолжается так: для i-ой вершины (i-ого мужчины) $i = 1, 2, 3, 4, 5$, просматриваются в порядке возрастания номеров (с циклическим возвратом в наименьший номер) все ребра, исключая те, которые ведут к запрещенным вершинам другой доли графа (занятым женщинам). В качестве состоявшегося ребра (брака) будет считаться соединение i-ой вершины одной доли графа с r_i-той вершиной из числа свободных вершин другой доли графа. Таким образом, мужчина 1 женится

на женщине 5; мужчина 2 женится на женщине 3; мужчина 3 женится на женщине 4; мужчина 4 женится на женщине 2; мужчина 5 женится на женщине 1, как это показано на рисунке 1.

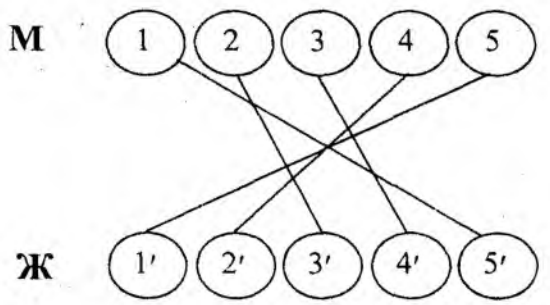

Рис. 1

Эта процедура применительно к матрице E может быть интерпретирована как последовательный просмотр каждой из строк $j = 1, 2, 3, 4, 5$, начиная со столбца, соответствующего номеру мужчины, для которого ищется женщина. Отсчитывается с циклическим возвратом r_i нулей в строке, и r_i-тый ноль при таком просмотре заменяется на единицу, обозначающую, что эта вершина уже занята (заключается брак между i-ым мужчиной и j-ой женщиной). Для того чтобы обозначить для последующих просмотров строк, что j-ая женщина уже занята, единицы проставляются для всего столбца, соответствующего рассмотренному мужчине. В результате мы последовательно получим:

$$\begin{bmatrix} 1&0&0&0&[1] \\ 0&1&0&0&1 \\ 0&0&1&0&1 \\ 0&0&0&1&1 \\ 0&0&0&0&1 \end{bmatrix} \rightarrow \begin{bmatrix} 1&0&1&0&1 \\ 0&1&[1]&0&1 \\ 0&0&1&0&1 \\ 0&0&1&1&1 \\ 0&0&1&0&1 \end{bmatrix} \rightarrow \begin{bmatrix} 1&0&1&1&1 \\ 0&1&1&1&1 \\ 0&0&1&[1]&1 \\ 0&0&1&1&1 \\ 0&0&1&1&1 \end{bmatrix} \rightarrow \begin{bmatrix} 1&1&1&1&1 \\ 0&1&1&1&1 \\ 0&1&1&1&1 \\ 0&[1]&1&1&1 \\ 0&1&1&1&1 \end{bmatrix} \rightarrow \begin{bmatrix} 1&1&1&1&1 \\ 1&1&1&1&1 \\ 1&1&1&1&1 \\ 1&1&1&1&1 \\ 1&1&1&1&1 \end{bmatrix}.$$

шаг 1	шаг 2	шаг 3	шаг 4
$r_1 = 4$	$r_2 = 1$	$r_3 = 1$	$r_4 = 2$

На последнем шаге мы выбираем единственный оставшийся ноль. Единицы, отмеченные в матрицах квадратными скобками, фиксируются как реализованные при рассматриваемом варианте паросочетания (ребра графа). В терминах построения системы подстановок это означает, что в первом столбце первой строки ставится число 5, во втором столбце - 4 и т.д., т.е.

$$S_{1,5} = \begin{pmatrix} 1&2&3&4&5 \\ 5&3&4&2&1 \end{pmatrix}.$$

Затем снова решается задача о браках, но теперь в графе $B_{5,5}$ нет ребер (1, 1) и (1, 5), (2, 2) и (2, 3), (3, 3) и (3, 4), (4, 4) и (4, 2), (5, 5) и (5, 1), что соответствует исходной матрице типа E вида:

$$E = \begin{bmatrix} 1&0&0&0&1 \\ 0&1&1&0&0 \\ 0&0&1&1&0 \\ 0&1&0&1&0 \\ 1&0&0&0&1 \end{bmatrix}$$

Породим случайные числа из интервала [1; 3], так как это делалось ранее. Пусть, например, это будут числа $r_1 = 2$, $r_2 = 3$, $r_3 = 1$, $r_4 = 1$. Применяя вышеописанную процедуру, получаем последовательно:

$$\begin{bmatrix} 1 & 0 & [1] & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ [1] & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & [1] \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \rightarrow \blacksquare$$

шаг 1	шаг 2	шаг 3	шаг 4
$r_1 = 2$	$r_2 = 3$	$r_3 = 1$	$r_4 = 1$

На шаге 4 для четвертого мужчины женщины заняты (нет допустимых вершин второй доли графа). Приведенному результату соответствует граф, представленный на рис. 2:

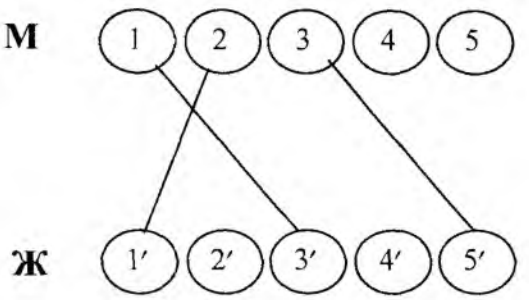

Рис. 2

В этом случае мы не получим полного паросочетания, так как мужчина под номером 4 не нашел пары. Его потенциальные невесты 1′, 2′, 3′, 5′ оказались уже занятыми с учетом состоявшихся выборов невест.

Здесь начинается другая часть алгоритма, связанная с текущей коррекцией выполняемой процедуры с тем, чтобы она реализовала вариант полного паросочетания.

Эта коррекция становится понятной, если возвратиться к матрице E на 2-ом шаге. Из нее видно, что после выполнения второго шага в матрице появилась строка с одним нулем, т.е. альтернативы выбора для 4-ого мужчины нет. Здесь вполне естественно пойти по пути назначения сразу 4-ому мужчине 5-ой женщины, т.е. если в матрице появилась строка с одним нулем, то этот нуль принудительно следует заменить единицей (в графе проставляется ребро).

Теперь появилась новая строка с одним нулем, который снова принудительно меняется на единицу и далее опять остается строка с одним нулем, и мы приходим к графу:

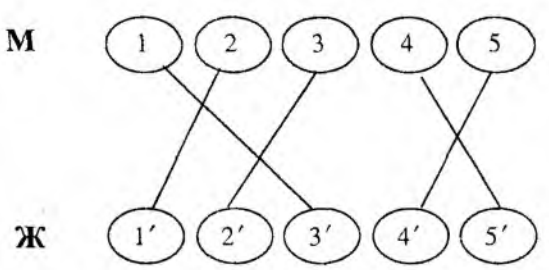

Рис. 3

В терминах подстановок мы получим допустимую систему:

$$S_{2,5} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,3\,4\,2\,1 \\ 3\,1\,2\,5\,4 \end{pmatrix}.$$

Снова решаем задачу о браках для графа заданного теперь матрицей:

$$E = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Пусть получены случайные числа из интервала [1, 2] $r_1 = 1$, $r_2 = 2$, $r_3 = 1$, $r_4 = 1$. Применяя оговоренные выше процедуры, последовательно получим:

$$\begin{bmatrix} 1\,[1]\,1\,0\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 1\,1\,0\,1\,1 \end{bmatrix} \rightarrow \begin{bmatrix} 1\,1\,1\,0\,1 \\ 1\,1\,1\,0\,[1] \\ 0\,1\,1\,1\,1 \\ 0\,1\,0\,1\,1 \\ 1\,1\,0\,1\,1 \end{bmatrix} \rightarrow \begin{bmatrix} 1\,1\,1\,0\,1 \\ 1\,1\,1\,0\,1 \\ [1]\,1\,1\,1\,1 \\ 1\,1\,0\,1\,1 \\ 1\,1\,0\,1\,1 \end{bmatrix} \rightarrow \begin{bmatrix} 1\,1\,1\,0\,1 \\ 1\,1\,1\,0\,1 \\ 1\,1\,1\,1\,1 \\ 1\,1\,[1]\,1\,1 \\ 1\,1\,1\,1\,1 \end{bmatrix}.$$

Шаг 1	шаг 2	шаг 3	шаг 4
$r_1 = 1$	$r_2 = 2$	$r_3 = 1$	$r_4 = 1$

И снова не получено полного паросочетания. Здесь, когда нулей в матрице остается мало, на первый план выступают не статистические, а детерминированные переходы, а поэтому выходом из создавшегося положения будет использование альтернативного решения, заключающегося в выборе тех значений подстановки, используя которые вероятность полного паросочетания увеличивается. Необходимо в процессе построения подстановки отслеживать количество нулей в строках графа. В случае, когда в строке оказывается сравнительно малое количество нулей, необходимо в первую очередь фиксировать соответствующий переход. Когда выбор перехода не однозначен, необходимо фиксировать то значение подстановки, которое минимально ограничивает выбор последующих, т.е. фиксируется то значение, при котором вычеркивается меньшее количество нулей в столбце графа.

Используя приведенные соображения, в нашем случае получим:

$$\begin{bmatrix} 1\,[1]\,1\,0\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 1\,1\,0\,1\,1 \end{bmatrix} \rightarrow \begin{bmatrix} 1\,1\,1\,1\,1 \\ 1\,1\,[1]\,0 \\ 0\,1\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 1\,1\,0\,1\,1 \end{bmatrix} \rightarrow \begin{bmatrix} 1\,1\,1\,1\,1 \\ 1\,1\,1\,1 \\ 0\,1\,1\,1\,[1] \\ 0\,1\,0\,1\,1 \\ 1\,1\,0\,1\,1 \end{bmatrix} \rightarrow \begin{bmatrix} 1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1 \\ [1]\,1\,0\,1\,1 \\ 1\,1\,01\,1 \end{bmatrix} \rightarrow \begin{bmatrix} 1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1 \\ 1\,1\,[1]\,1\,1 \end{bmatrix}$$

Этому решению соответствует граф, представленный на рис. 4.

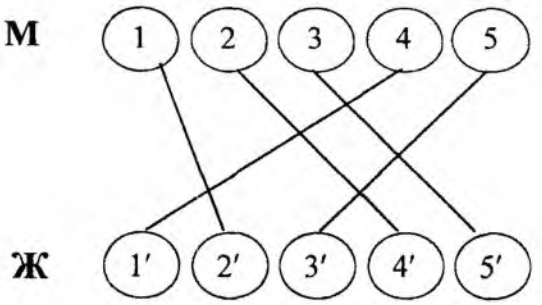

Рис. 4

В других обозначениях построена система:

$$S_{4,5} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,3\,4\,2\,1 \\ 3\,1\,2\,5\,4 \\ 2\,4\,5\,1\,3 \end{pmatrix}.$$

Последняя подстановка получается единственным образом:

$$S_{5,5} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,3\,4\,2\,1 \\ 3\,1\,2\,5\,4 \\ 2\,4\,5\,1\,3 \\ 4\,5\,1\,3\,2 \end{pmatrix}.$$

Подобные способы порождения таблиц противоречивых подстановок значительно ограничивают их случайность, поэтому рекомендуется использовать минимальное количество ограничений. Для увеличения случайности таблицы необходимо выбирать разрешенные позиции переходов в произвольном (случайном) порядке.

В реальном случае для шифра ГОСТ требуется не квадратная таблица, а прямоугольник размером 8x16. В этом случае анализ графа Е при генерации подобных таблиц можно не производить, задача будет решена за один проход без возвратов. Однако исключить анализ графа при построении таблиц большего размера нельзя. Вышеупомянутые методы построения противоречивых подстановок могут быть использованы для построения таблиц с другими свойствами, такими как цикличность подстановок. Отличие будет сказываться лишь на построении графа Е.

Программа позволяет, при использовании ПЭВМ, формировать матрицу 256x256 противоречивых подстановок за 1 минуту или 10-15 таблиц подстановок за одну минуту.

Список литературы: 1. *Лисицкая И.В.* Противоречивые подстановки в алгоритме ГОСТ 28147-89//. Информационные системы: Сб. научн. тр.-Харьков: НАНУ, ПАНУ, ХВУ, 1995. 9 с. 2. Математическая энциклопедия. Сов. энциклопедия – М.: 1979.Т. 2.1103с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 24.04.2002