Теорема 1. Пусть $t(Ca_n(n_2, n_3, \ldots))$ — число остовных деревьев в помеченном кактусе с $n \geqslant 2$ вершинами, имеющем $n_2 \geqslant 0$ блоков-рёбер и $n_i \geqslant 0$ блоков-многоугольников с i вершинами при $i \geqslant 3$. Тогда верна формула

$$t(Ca_n(n_2, n_3, \ldots)) = \prod_{i \geqslant 3} i^{n_i}\ , \text{где } n - 1 = n_2 + 2n_3 + \ldots$$

Доказательство. Пусть $k = \sum\limits_{i \geqslant 3} n_i$ — число циклов (цикломатическое число) в рассматриваемом кактусе, а $m = n_2 + 3n_3 + \ldots$ — число его рёбер. Поскольку $k = m - n + 1$, имеем равенство $n - 1 = n_2 + 2n_3 + \ldots$ Так как все блоки кактуса — или рёбра (деревья), или простые циклы, а число остовных деревьев простого цикла с n вершинами равно n, то с помощью леммы 1 получаем утверждение теоремы 1. ■

Следствие. Для числа остовных деревьев в кактусе $Ca_n(n_2, n_3, \ldots)$ верны неравенства

$$t(Ca_n(n_2, n_3, \ldots)) \leqslant \left(\frac{1}{k}(n + k - n_2 - 1)\right)^k \leqslant \left(\frac{1}{k}(n + k - 1)\right)^k \leqslant e^{n-1}.$$

Доказательство. С помощью теоремы 1 и неравенства между средним геометрическим и средним арифметическим имеем

$$t(Ca_n(n_2, n_3, \ldots)) = \prod_{i \geqslant 3} i^{n_i} \leqslant \left(\frac{1}{k}\sum_{i \geqslant 3} i n_i\right)^k = \left(\frac{1}{k}(n + k - n_2 - 1)\right)^k \leqslant \left(\frac{1}{k}(n + k - 1)\right)^k \leqslant e^{n-1}.$$

Доказательство закончено. ■

ЛИТЕРАТУРА

1. *Харари Ф., Палмер Э.* Перечисление графов. М.: Мир, 1977. 324 с.
2. *Myrvold W.* Reliable network synthesis: some recent developments // Proc. 8th Int. Conf. Graph Theory, Combinatorics, Algorithms, Appl. 1999. V. 2. P. 650–660.
3. *Зыков Ф.* Основы теории графов. М.: Наука, ГРФМЛ, 1987. 382 с.
4. *Татт Ф.* Теория графов. М.: Мир, 1988. 424 с.
5. *Харари Ф.* Теория графов. М.: Мир, 1973. 301 с.

УДК 519.713.4 DOI 10.17223/2226308X/10/55

МЕТОД ИДЕНТИФИКАЦИИ ОБРАТИМОГО АВТОМАТА С ИЗВЕСТНОЙ ФУНКЦИЕЙ ВЫХОДОВ

А. О. Жуковская, В. Н. Тренькаев

Предлагается метод построения простого условного эксперимента, идентифицирующего автомат с известной функцией выходов, являющийся одной из реализаций обратимого недетерминированного автомата R. Сначала строится граф преемников автомата R и определяются его разрешимые вершины. Показано, что когда вершина, соответствующая множеству состояний автомата R, разрешима, то можно провести простой условный установочный эксперимент по нахождению текущего состояния автомата-реализации. Далее проводится простой условный эксперимент по идентификации последнего при известном начальном состоянии.

Ключевые слова: *простой условный эксперимент по идентификации автомата, сильносвязный автомат, обратимый автомат.*

В работе рассматривается задача построения простых условных экспериментов [1] по идентификации автомата в классе, который задаётся как множество реализаций некоторого обратимого недетерминированного (онд-)автомата с одним или двумя вариантами перехода из каждого состояния при каждом входном символе. Условный эксперимент подразумевает, что вычисление подаваемых на автомат входных слов зависит от его реакций на ранее поданные слова.

Здесь под *онд-автоматом* понимается пятёрка $R = (X, S, Y, \Psi, \varphi)$, где X, Y и S — конечные множества соответственно входных символов, выходных символов и состояний; $\Psi : X \times S \to \{S' : S' \subseteq S, |S'| = 1, 2\}$ — функция переходов и $\varphi : X \times S \to Y$ — функция выходов со свойством биективности отображения $\varphi_s : X \to Y$ для каждого s, где $\varphi_s(x) = \varphi(x, s)$ и $s_1 \neq s_2 \Rightarrow \varphi_{s_1} \neq \varphi_{s_2}$. Детерминированный автомат $A = (X, S, Y, \psi, \varphi)$ называется *реализацией* онд-автомата $R = (X, S, Y, \Psi, \varphi)$, если для любой пары (x, s) выполняется $\psi(x, s) \in \Psi(x, s)$. Далее предполагается, что любая реализация A онд-автомата R является сильносвязным автоматом.

Постановка задачи. Для эксперимента представлен автомат A, являющийся некоторой реализацией онд-автомата R. Требуется с помощью простого условного эксперимента идентифицировать A, т. е. определить неизвестную функцию переходов автомата A. Отметим, что рассматриваемый здесь онд-автомат соответствует перестраиваемому автомату из [2], а сама задача имеет приложение в криптоанализе автоматных шифров.

Нетрудно показать, что класс автоматов, образованных реализациями онд-автомата, является исключительным, т. е. задача идентификации его реализации имеет решение. Случай, когда известно начальное состояние автомата, представленного для эксперимента, описан в [3]. Для решения задачи при неизвестном начальном состоянии предлагается использовать установочный эксперимент, когда требуется определить текущее состояние автомата, являющегося неизвестной реализацией заданного онд-автомата. Отметим, что в классической постановке установочная задача решается при условии, что автомат, предъявленный для эксперимента, известен полностью, а не с точностью до класса.

В онд-автомате R *множеством преемников* подмножества $S_0 \subseteq S$ по паре x/y, где $x \in X$ и $y \in Y$, назовём множество состояний $S_1 = \{s : \exists s_0 \in S_0 \ (s \in \Psi(x, s_0) \& \ \& \ \varphi(x, s_0) = y)\}$.

Граф преемников онд-автомата R — это граф, который строится по следующим правилам:

1) каждому подмножеству $S_0 \subseteq S$ ставится в соответствие вершина $v(S_0)$ графа (будем говорить, что вершина $v(S_0)$ содержит S_0);
2) вершина $v(S_0)$ называется концевой, если $|S_0| \leqslant 2$;
3) из каждой вершины $v(S_0)$, которая не является концевой, выходят дуги, помеченные парой (x/y), ведущие к вершинам, содержащим преемников S_0 по x/y.

Группу дуг, выходящих из вершины $v(S_0)$ и помеченных парами (x/y) с одним и тем же символом $x = x_0$, назовём x_0-*группой* множества S_0.

Вершину $v(S_0)$ графа преемников назовём *разрешимой*, если выполняется одно из двух условий:

1) вершина $v(S_0)$ концевая;
2) существует входной символ x_0, такой, что все дуги из x_0-группы подмножества S_0 ведут к разрешимым вершинам.

Теорема 1. Если вершина $v(S_0)$ графа преемников онд-автомата R разрешима, то для любой сильносвязной реализации автомата R, находящейся в одном из состояний $s \in S_0$, возможен простой условный установочный эксперимент.

Конструктивное доказательство теоремы, которое мы опускаем, позволяет предложить следующий метод построения простого условного эксперимента, идентифицирующего реализацию A онд-автомата R. Построить граф преемников автомата R и вычислить его разрешимые вершины. Если вершина $v(S)$ разрешима, то провести над A сначала простой условный установочный эксперимент, а затем эксперимент по идентификации автомата A при известном его начальном состоянии.

Предложенный метод реализован на языке C++ и апробирован на случайно сгенерированных автоматах. Компьютерные эксперименты показали, что для подавляющего большинства случайно сгенерированных онд-автоматов вершина $v(S)$ графа преемников разрешима, а следовательно, метод применим для практического использования.

ЛИТЕРАТУРА

1. *Гилл А.* Введение в теорию конечных автоматов. М.: Наука, 1966. 272 с.
2. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.
3. *Жуковская А. О., Тренькаев В. Н.* О простых условных экспериментах идентификации обратимых автоматов некоторого класса // Прикладная дискретная математика. Приложение. 2016. № 9. С. 115.

УДК 003.26, 004.021, 519.725.2 DOI 10.17223/2226308X/10/56

ПРИМЕНЕНИЕ РЁБЕРНОГО ЛОКАЛЬНОГО ДОПОЛНЕНИЯ В СТРУКТУРНОМ АНАЛИЗЕ КРИПТОСИСТЕМЫ МАК-ЭЛИСА

А. А. Соколова

Предлагается алгоритм для нахождения и перечисления классов эквивалентности циклических кодов с помощью графов и операции рёберного локального дополнения. Удалось увеличить максимальное количество вершин для обрабатываемого графа с 10 до 17. Построена полная классификация циклических кодов длины 19. Кроме того, реализован алгоритм для определения эквивалентности двух кодов, один из которых циклический. На персональном компьютере достигнута возможность за приемлемое время определять эквивалентность кодов длины 19.

Ключевые слова: *двоичные линейные коды, классификация, графы, рёберное локальное дополнение, криптосистема Мак-Элиса.*

В криптосистеме Мак-Элиса одному и тому же открытому ключу могут соответствовать несколько секретных ключей, следовательно, они могут быть разбиты на классы эквивалентности. Возможность подобрать эквивалентный ключ напрямую влияет на стойкость данного метода шифрования, так как ключ для расшифрования не уникален.

Имеющиеся исследования в данной области рассматривают ограниченный набор кодов с тривиальной группой автоморфизмов и неприменимы в структурном анализе криптосистемы Мак-Элиса. Возникает проблема поиска альтернативы предложенным методам, применимой к циклическим кодам. Вопрос изучения классов эквивалентности двоичных линейных кодов является основным в данной работе.