где $a, b, c \in \{0, 1\}$,

$$\nu_{abc} = (n-2)^{-1} \sum_{i=0}^{n-3} \mathbf{I}\{Y_i = a, Y_{i+1} = b, Y_{i+2} = c\},$$

$$\nu_{ab} = (n-1)^{-1} \sum_{i=0}^{n-2} \mathbf{I}\{Y_i = a, Y_{i+1} = b\}, \quad \nu_a = n^{-1} \sum_{i=0}^{n-1} \mathbf{I}\{Y_i = a\},$$

при этом в [1] рассматривается не двоичный, а произвольный конечный алфавит состояний цепи Маркова.

Рассмотрим критерий проверки гипотезы H_0 против H_1, основанный на статистике (1):

$$\text{принимается гипотеза} \begin{cases} H_0, \text{ если } S < t_{\chi_2^2, 1-\alpha}, \\ H_1, \text{ если } S \geqslant t_{\chi_2^2, 1-\alpha}, \end{cases} \tag{2}$$

где $\alpha = \mathbf{P}\left\{S \geqslant t_{\chi_2^2, 1-\alpha} \middle| H_0\right\}$ – вероятность ошибки первого рода; $t_{\chi_2^2, \alpha}$ – квантиль уровня α распределения χ-квадрат с двумя степенями свободы.

Теорема 1. Пусть в модели вкраплений $p_a \neq \pi_a$, $a \in \{0, 1\}$, и среди элементов матрицы переходных вероятностей Π есть хотя бы один, отличный от 1/2. Тогда при выполнении условий

$$\tau \to 0, \ n \to \infty, \tag{3}$$

$$\sqrt{n}\tau \to \infty, \ n \to \infty, \tag{4}$$

критерий (2) проверки гипотезы H_0 против альтернативы H_1 является состоятельным.

Замечание 1. При отсутствии вкраплений ($\tau \equiv 0$) и при наличии вкраплений во всех позициях последовательности X ($\tau \equiv 1$) гипотезы H_0 и H_1 неразличимы, поскольку в обоих случаях Y является простой однородной цепью Маркова (с глубиной зависимости 1 и 0 соответственно). Критерий будет состоятельным, когда вкраплений «не слишком много», что гарантируется условием (3), но в то же время когда число вкраплений превосходит по порядку квадратный корень из длины наблюдаемого отрезка последовательности X (условие (4)).

ЛИТЕРАТУРА

1. *Шойтов А. М.* О выявлении факта зашумления конечной цепи Маркова с неизвестной матрицей переходных вероятностей // Прикладная дискретная математика. Приложение. 2010. №3. С. 44–45.

УДК 519.7 DOI 10.17223/2226308X/9/3

АЛГОРИТМ РАСПОЗНАВАНИЯ ПОЛНОТЫ МНОЖЕСТВА СЛОВ И ДИНАМИКА ЗАПРЕТОВ[1]

А. А. Евдокимов

Вводятся инвариантные операции и даётся описание алгоритма распознавания полноты множества слов. Приводится теорема о результатах работы алгоритма и их отношении к свойству полноты исходного множества слов. Формулируется

[1]Работа поддержана Новосибирским государственным университетом и грантом РФФИ, проект №14-01-00507.

нерешённая задача об оценке мощностей полных тупиковых множеств слов.

Ключевые слова: *множество слов, полнота, динамика запретов, алгоритм распознавания.*

Задачи о полноте множества слов и избегаемости запрещённых подслов бесконечными символьными последовательностями были впервые сформулированы в [1] и исследованы в [2–4]. Литературу можно посмотреть в [4, 5] в контексте более широкой области исследования, называемой «Combinatorics on words».

Исследованию языков, определяемых заданием запрещённых подслов и иначе называемых в последние годы «антисловарями», посвящено большое число публикаций с указанием различных приложений. В частности, это задачи анализа и синтеза криптографических функций и символьных последовательностей, в которых важны информационные и сложностные характеристики, связанные с изучением взаимосвязи со свойствами их подфункций или подслов.

Множество S слов (запретов) в алфавите A называется *полным* (или *блокирующим*), если любая бесконечная последовательность букв из A не свободна от S, то есть содержит в качестве своего подслова хотя бы одно слово из S [1, 2].

Подмножество $T \subseteq S$, $T = \{X_1 a_{i_1}, \ldots, X_m a_{i_m}\}$, где $m = |A|$, образует тупиковую относительно S систему слов (ТСС), если

1) все последние буквы слов в T различны (т. е. это все m букв алфавита A);
2) для всех $i = 1, \ldots, m-1$ слово X_i есть суффикс слова X_{i+1}.

Если в S существует ТСС, то применение к ней T-операции состоит в удалении в самом длинном слове $X_m a_{i_m}$ его последней буквы a_{i_m} (если в ТСС самое длинное слово не единственно, то выбираем любое). Удобно считать, что если $S = A$, то есть S — это множество всех букв алфавита A, то T-операция применима к S и её результатом является пустое множество. Сочетая T-операцию сокращения множества S с двумя другими естественными операциями сокращения — удалением из S одного из двух одинаковых слов и удалением слова X, если в S содержится подслово слова X, получаем последовательность множеств, которая в силу конечности S стабилизируется:

$$S \to S_1 \to S_2 \to \ldots \to S^*.$$

Теорема 1. Приведённые операции инвариантны относительно свойства множества S быть полным. Их применение (в любом порядке) распознает полноту множества S:

1) либо $S^* = \varnothing$, и тогда S — полное множество;
2) либо $S^* \neq \varnothing$ и к S^* неприменимы операции сокращения, и тогда S — неполное.

Основанный на теореме алгоритм распознавания полноты прост, но этап проверки наличия в S тупиковой системы слов, к которой применима T-операция, трудоёмок. Однако, в отличие от полиномиального алгоритма в [3], этот алгоритм позволяет работать со словами различной длины в множестве S и получить сокращённое множество S^*, эквивалентное S.

Представляет интерес более широкая постановка вопроса о сохранении свойства полноты при изменениях в S, а также то, насколько свойство устойчиво к «ошибкам», например удалению букв в словах или самих слов из S. Расширяя неполные множества и сужая полные, можно находить границы перехода и управлять динамикой изменения свойства полноты и избегаемости запретов S. В этой связи важно получить ответ на следующий вопрос: насколько велико может быть различие мощностей полных тупиковых (несокращаемых) множеств S, $S \subseteq A^n$? Например, как ведёт себя (по n при фиксированном m) функция

$$f(m,n) = \max |S_1|/|S_2|,$$

где $m = |A|$, а максимум берётся по всем парам $\{S_1, S_2\}$ полных тупиковых множеств, $S_1, S_2 \subseteq A^n$? Можно доказать, что эта функция не ограничена никакой константой. Более точные оценки её роста значительно прояснили бы структуру полных множеств слов.

ЛИТЕРАТУРА

1. *Евдокимов А. А., Крайнев В. А.* Задачи о полноте систем слов // XXII Обл. науч.-технич. конф. Тезисы. Новосибирск, 1979. С. 105–107.
2. *Евдокимов А. А.* Полные множества слов и их числовые характеристики // Методы дискретного анализа в исследовании экстремальных структур: сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1983. Вып. 39. С. 7–19.
3. *Евдокимов А. А.* Исследование полноты множеств слов и языков с запретами // Вестник Томского государственного университета. Приложение. 2004. № 9(1). С. 8–12.
4. *Evdokimov A. A. and Kitaev S. V.* Crucial words and the complexity of some extremal problems for sets of prohibited words // J. Comb. Theory. Ser. A. 2004. V. 105. P. 273–289.
5. *Berstel J. and Karhumäki J.* Combinatorics on words — a tutorial // Bull. EATCS. 2003. V. 79. P. 178–229.

УДК 512.624.5 DOI 10.17223/2226308X/9/4

О ДОСТАТОЧНОМ УСЛОВИИ ДЛЯ ОТСУТСТВИЯ ВОЗМОЖНОСТИ СОКРАЩЕНИЯ ПЕРИОДА В СТАРШИХ ДВОИЧНЫХ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ НАД ПРИМАРНЫМИ КОЛЬЦАМИ

С. А. Кузьмин

Рассматриваются двоичные разрядные последовательности над примарными кольцами нечётной характеристики. Указано достаточное условие для отсутствия сокращения периода в старших разрядных последовательностях в 2 раза при наличии не всех элементов на цикле исходной линейной рекурренты.

Ключевые слова: *линейные рекуррентные последовательности, периоды последовательностей, примарные кольца, разрядные последовательности.*

В настоящее время наблюдается особый интерес к изучению p-ичных разрядных последовательностей над кольцами вычетов по модулю p^n. Это связано с тем, что данные последовательности обладают высокой линейной сложностью и могут быть использованы в датчиках псевдослучайных последовательностей. Со списком работ по данной тематике можно ознакомиться, например, в [1].

Большое внимание уделяется задаче восстановления линейных рекуррентных последовательностей (ЛРП) над примарными кольцами вычетов по их усложнению, особенно в тех случаях, когда ЛРП максимального периода (ЛРП МП) отображается в свою старшую координатную последовательность [2].

Меньше работ посвящено r-ичным разрядным последовательностям, где $r \neq p$, которые также могут быть рассмотрены как усложнения линейных рекуррент над простыми полями и кольцами Галуа. Такие последовательности рассматривались