Math-Net.Ru

Общероссийский математический портал

А. В. Бабаш, Запреты автоматов, *Матем. заметки*,
2012, том 91, выпуск 5, 667–673

DOI: <https://doi.org/10.4213/mzm8783>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.137.237

26 апреля 2023 г., 17:39:26

Запреты автоматов

А. В. Бабаш

Улучшена оценка сверху минимальной длины выходных слов, которые не могут быть получены на выходе произвольного автомата с двоичным входным и выходным алфавитами.

Библиография: 13 названий.

Известно (см., например, [1]), что в науке и технике и, в частности, в различных системах обеспечения безопасности широко применяются генераторы псевдослучайных последовательностей. Так, например, эти генераторы используются в синхронных поточных криптосхемах в качестве управляющих блоков поточных криптосхем. Основные требования к таким генераторам сформулированы в [2; с. 247]. Одно из этих требований состоит в том, что последовательность, вырабатываемая генератором, должна иметь большой период. Другое, не менее важное, требование состоит в том, что статистические свойства управляющей гаммы шифрующего блока должны приближаться к свойствам случайной равновероятной последовательности. В частности, последовательности таких генераторов должны содержать любые возможные k -граммы при небольших значениях k . Имеет определенный смысл решение вопроса о принципиальной возможности получения заданных мультиграмм в выходных последовательностях анализируемых узлов генераторов псевдослучайных чисел или решение обратной задачи о том, какие мультиграммы в принципе не могут быть получены на выходе заданного блока генератора, какова минимальная длина таких мультиграмм. Как показано в [2] может оказаться, что число различных мультиграмм, снимаемых с управляющих блоков шифратора, которые участвуют в образовании шифра шифрующего блока, мало. Это, очевидно, в худшую сторону отразится на криптографической стойкости рассматриваемого шифратора. Исследование поставленных вопросов стимулируется и другими соображениями. Например, зная мультиграммы, которые не могут быть получены с некоторого блока генератора псевдослучайных чисел, можно, при применении ряда методов определения ключей такого генератора, отбраковывать эти ключи, что может повысить эффективность этих методов.

Если моделировать функционирование генераторов псевдослучайных чисел автоматами, то естественно возникает задача описания автоматов, позволяющих вырабатывать любую конечную последовательность элементов выходного алфавита. Кроме того, представляет интерес задача описания выходных слов автомата, которые невозможно получить с заданного автомата. Прототипом указанных задач является

задача изучения запретов кодирующих устройств с конечной памятью без обратной связи (регистров сдвига), или адекватная задача изучения запретов двоичных функций (см. [3], [4]).

Исследуются следующие вопросы.

1) Существует ли алгоритм, проверяющий для каждого автомата A , все ли мультиграммы могут быть получены на его выходе?

2) Какова минимальная длина мультиграмм, которые не могут быть получены на выходе заданного автомата A ?

Заметим, что ранее в работе [4] поставленные выше вопросы исследовались для весьма узкого класса автоматов, именно для автоматов, представимых проходными линиями задержки. Результаты [4] послужили толчком в решении этих задач в общей постановке для класса конечных автоматов. Следуя определениям работы [4], условимся говорить, что некоторая мультиграмма является *запретной* для автомата A , если она не может быть получена на выходе автомата A . Минимальную длину запретной для автомата A мультиграммы будем называть *длиной запрета* автомата A и обозначать через $L(A)$. Сам автомат A будет называться *автоматом с запретом*, если для него существует запретная мультиграмма. В противном случае A будет называться автоматом без запрета или *автоматом-генератором*.

Пусть $A = (X, S, Y, h, f)$ – конечный автомат с входным алфавитом X , множеством состояний S , выходным алфавитом Y , функциями перехода $h: S \times X \rightarrow S$ и выхода $f: S \times X \rightarrow Y$. Ниже мы будем пользоваться так называемыми частичными функциями перехода $(h_x)_{x \in X}$ и частичными функциями выхода $(f_x)_{x \in X}$, определенными условиями $h_x(s) = h(s, x)$, $f_x(s) = f(s, x)$. Если для автомата $A = (X, S, Y, h, f)$ частичные функции выхода совпадают при любом $x \in X$, то такой автомат называют *автоматом Мура* и обозначают $A = (X, S, Y, h, \lambda)$, где $\lambda: S \rightarrow Y$. Введем следующие обозначения:

- $|S|$ – мощность множества S ;
- 2^S – множество всех подмножеств множества состояний S автомата A ; в частности, пустое множество $\emptyset$ и S принадлежат 2^S ;
- для $m \in 2^S$ и $y \in Y$ через m^y обозначим множество всех состояний $s' \in S$, для которых существует $s \in m$ со свойством: найдется $x \in X$, при котором $h_x(s) = s'$, $f_x(s) = y$;
- $A_S = (Y, 2^S, \delta)$ – автомат без выходов (автомат Медведева) с входным алфавитом Y , множеством состояний 2^S , функцией перехода δ , определенной частичными функциями перехода $(\delta_y)_{y \in Y}$, $\delta_y(m) = m^y$, $m \in 2^S$, $y \in Y$.

Автомат A_S является автоматом, представляющим язык, который перечисляется автоматом A (см. [5; с. 185], [6], [7]). Легко показывается, что каждой выходной мультиграмме $y(1), y(2), \dots, y(k)$, полученной с автомата A при некотором его начальном состоянии $s \in S$, соответствует в графе переходов автомата A_S путь вида

$$m_1 \xrightarrow{y(1)} m_2 \xrightarrow{y(2)} \dots \xrightarrow{y(k-1)} m_k \xrightarrow{y(k)} m_{k+1},$$

где m_1 – любое подмножество множества S , содержащее состояние s , а m_j , $j \in \{2, 3, \dots, k+1\}$, – некоторые непустые подмножества из 2^S . Верно также и обратное, если имеется такой путь в графе переходов автомата A_S , то найдутся состояние $s \in m_1$ и некоторая входная последовательность автомата A , которым соответствует выходная мультиграмма $y(1), y(2), \dots, y(k)$ автомата A . Мультиграмма

$y'(1), y'(2), \dots, y'(k)$ не может быть получена на выходе автомата A , т.е. является запретной для автомата A тогда и только тогда, когда в графе переходов автомата A_S существует путь указанного выше вида при $m_1 = S$ и $m_{k+1} = \emptyset$ при некотором k . Точнее говоря, запретные для A мультиграммы однозначно определены путями в графе переходов автомата A_S , ведущими из состояния S в состояние $\emptyset$. Напомним, что $S \in 2^S$, $\emptyset \in 2^S$ и число состояний в множестве состояний 2^S автомата A_S равно $2^{|S|}$. В [6], [7] доказано, что если перечисляющий автомат имеет $|S|$ состояний, то распознающий – не более $2^{|S|}$, причем эта оценка не улучшаема. В [8] доказано, что если язык перечисляется автоматом Мура с $|S|$ состояниями, то он представим в подходящем автомате с $2^{C(|S|)}$ состояниями, где

$$\frac{C(|S|)}{|S|/2} \rightarrow 1$$

при $|S| \rightarrow \infty$. Поэтому справедлива

ТЕОРЕМА 1 (см. [9]). *Существует алгоритм, проверяющий является ли каждый заданный автомат A автоматом с запретом. Если $A = (X, S, Y, h, f)$ автомат с запретом, то длина его запрета ограничена сверху величиной $2^{|S|} - 1$. Если автомат A является автоматом Мура, то длина его запрета $L(A)$ ограничена сверху величиной $2^{C(|S|)} - 1$, где величина $C(|S|)$ такова, что*

$$\frac{C(|S|)}{|S|/2} \rightarrow 1$$

при $|S| \rightarrow \infty$.

Положим

$$L(m, n, p) = \max_{|X|=m, |S|=n, |Y|=p} L(A),$$

где максимум берется по всем конечным автоматам, у которых алфавиты X, S, Y состоят из m, n, p символов, соответственно.

В параграфе 6 работы [10] и в [11] Подколзиным получен ряд оценок длины запрета автоматов:

- 1) $L(m, n, p) \leq 1 + \lceil \ln n / (\ln p - \ln m) \rceil$;
- 2) если $p \geq n, m \geq p + n - 2$, то $L(m, n, p) = 2^n - 1$;
- 3) если $p \geq 12, p < n, m \geq p + 16[(p - 3)/9]^2$, то $L(m, n, p) > 2^n(1 - 2^{1-c})$, где $c = [(p - 3)/9]$;
- 4) если $p \geq 3, m \geq p + 1, n - p \rightarrow \infty$, то $2 \lg_2 L / (n - p) \rightarrow 1$ (см. [11]);
- 5) если $n - p \rightarrow \infty$, то $\lg_2 L$ асимптотически не превосходит величины $(n - p)/2$ (см. [11]).

ОПРЕДЕЛЕНИЕ 1. Состояние s автомата Мили $A = (X, S, Y, h, f)$ называется *полным по выходу*, если уравнение относительно $x \in X$

$$f_x(s) = y$$

разрешимо при любом $y \in Y$.

Состояние s автомата Мура $A = (X, S, Y, h, \lambda)$ называется *муровски полным по выходу*, если уравнение

$$\lambda(h_x(s)) = y$$

разрешимо относительно $x \in X$ при любом $y \in Y$.

ОПРЕДЕЛЕНИЕ 2. Состояние s автомата $A = (X, S, Y, h, f)$ называется *полным по входу*, если система двух уравнений относительно неизвестных $x \in X$, $s' \in S$,

$$h_x(s') = s, \quad f_x(s') = y$$

разрешима при любом $y \in Y$.

Полнота по выходу состояния s означает существование в графе переходов автомата A ориентированных дуг, исходящих из состояния s , выходные отметки которых составляют весь выходной алфавит Y . Аналогично интерпретируется и полное по входу состояние s автомата A . Отличие лишь в том, что теперь надо рассматривать входящие в s ориентированные дуги. Из данных определений непосредственно вытекает

ТЕОРЕМА 2. Автомат, у которого все состояния являются одновременно полными по входу или же полными по выходу (муровски полными по выходу), является автоматом без запрета.

ПРИМЕР 1. Пусть автомат Мура $A = (X, S, Y, h, \lambda)$ представляет собой двоичную проходную линию задержки, т.е. $X = Y = F_2$ является полем из двух элементов, S -координатным векторным пространством над полем F_2 размерности n . Частичные функции переходов $(h_x)_{x \in X}$ определены соотношением

$$h_x(x_1, \dots, x_n) = (x_2, x_3, \dots, x_n, x),$$

где $(x_1, \dots, x_n) \in S$ – двоичные наборы длины n , а λ – фиксированная функция на S со значениями в F_2 , причем переменные x_1 и x_n являются существенными переменными функции λ . Состояния линии задержки A будут муровски полными по выходу тогда и только тогда, когда

$$\lambda(x_1, \dots, x_{n-1}, 0) \neq \lambda(x_1, \dots, x_{n-1}, 1)$$

при каждом двоичном наборе $x_1, \dots, x_{n-1}$, т.е. тогда и только тогда, когда переменная x_n входит в двоичную функцию λ линейно. Аналогично показывается, что состояния линии задержки будут полными по входу в том и только в том случае, когда переменная x_1 входит в функцию λ линейно. Таким образом, из теоремы 2 вытекает достаточное условие того, чтобы линия задержки A была без запрета. Это условие таково: хотя бы одна из переменных x_1 , x_n , входит в функцию λ линейно (см. теорему 4 в [4]).

Ниже мы ограничиваемся рассмотрением класса автоматов A с двухбуквенными входным и выходным алфавитами. Обозначим через $S(y)$ множество всех состояний автомата $A = (X, S, Y, h, f)$, для которых

$$f_x(s) = y, \quad y \in Y,$$

при любом $x \in X$.

Обозначим через C_n^k число сочетаний из n элементов по k . Основным результатом работы составляет

ТЕОРЕМА 3. Если автомат $A = (X, S, Y, h, f)$, $X = Y = F_2$ – автомат с запретом, то длина его запрета ограничена сверху величиной

$$C_{|S(0)|+|S(1)|}^{|S(0)|} \cdot 2^{|S|-|S(0)|-|S(1)|}.$$

ДОКАЗАТЕЛЬСТВО. Предварительно докажем ряд вспомогательных лемм.

ЛЕММА 1. Для любого состояния $m \in 2^S$ автомата $A_S = (Y, 2^S, \delta)$ (построенного для $A = (X, S, Y, h, f)$, $X = Y = F_2$) существует $y \in Y$, при котором мощность множества $\delta_y(m)$ не превосходит мощности множества m . Если, дополнительно, для данного $y \in Y$ выполняется неравенство

$$|m \cap S(y \oplus 1)| - |m \cap S(y)| \geq k, \quad k \geq 0$$

(сложение в поле F_2), то для величины $|\delta_y(m)|$ выполняется соотношение

$$|m| - |\delta_y(m)| \geq k.$$

ДОКАЗАТЕЛЬСТВО. Существует элемент $y \in F_2$, при котором мощности пересечений множеств $m \cap S(y)$ и $m \cap S(y \oplus 1)$ ($\oplus$ в поле F_2) удовлетворяют неравенству

$$|m \cap S(y)| \leq |m \cap S(y \oplus 1)|.$$

Мощность множества $\delta_y(m)$ не превосходит числа дуг, отмеченных выходным символом $y \in F_2$, идущих из состояний $s \in m$ автомата A , которое, очевидно, равно величине

$$2|m \cap S(y)| + |m| - |m \cap S(y)| - |m \cap S(y \oplus 1)|.$$

Последнее число не превосходит величины $|m|$. Дополнительное утверждение леммы теперь очевидно.

Обозначим через K_N число состояний $m' \in 2^S$ автомата A_S , для которых

$$|m' \cap S(0)| = |m' \cap S(1)|, \quad |m'| = N.$$

ЛЕММА 2. Пусть автомат A является автоматом с запретом. Тогда для любого состояния $m \in 2^S$ в графе переходов автомата A_S существует путь длины не больше величины $K_{|m|}$, ведущий из состояния m в некоторое состояние строго меньшей мощности.

ДОКАЗАТЕЛЬСТВО. Предположим, что не существует указанного в лемме 2 пути. Напомним (см. [12]), что j -м приемником начального состояния автомата называется состояние получаемое после подачи на него любого входного слова длины j . В силу предположения каждый j -й приемник m' , $j \in \{1, \dots, K_{|m|} - 1\}$, состояния m автомата A_S характеризуется равенством мощностей

$$|m' \cap S(0)| = |m' \cap S(1)|$$

и, как следует из доказательства леммы 1, при этих условиях должно выполняться равенство мощностей

$$|m'| = |m|.$$

Из этого факта и определения числа $K_{|m|}$ вытекает, что множество всех приемников состояния m совпадает с множеством всех j -х приемников $j \in \{1, \dots, K_{|m|} - 1\}$. Откуда вытекает, что не существует пути в графе автомата A_S , ведущего из состояния m в состояние $\emptyset$, что противоречит условию леммы.

Перейдем теперь к доказательству теоремы 2.

Утверждение леммы 2 состоит в том, что из любого состояния m в графе переходов автомата A_S существует путь длины, не превосходящей величины $K_{|m|}$, ведущий из m в состояние строго меньшей мощности. Следовательно, в том же графе существует путь из состояния S в состояние $\emptyset \in 2^S$ длины, не превосходящей

$$\sum_{j=1}^{|S|-1} K_j.$$

Эта величина представляет собой число подмножеств m множества S мощности $|m| \leq |S| - 1$, для которых

$$|m \cap S(0)| = |m \cap S(1)|.$$

Положим $T = \min(|S(1)|, |S(0)|)$ и подсчитаем значение величины

$$\sum_{j=1}^{|S|-1} K_j = 2^{|S|-|S(0)|-|S(1)|} \sum_{j=0}^T C_{|S(0)|}^j \cdot C_{|S(1)|}^j.$$

Используя равенство 9

$$\sum_{r=0}^{r=k} C_m^r C_n^{k-r} = C_{n+m}^k$$

из задачи 1.18 книги [13], получаем

$$\sum_{j=1}^{|S|-1} K_j = 2^{|S|-|S(0)|-|S(1)|} C_{|S(0)|+|S(1)|}^{|S(0)|}.$$

Теорема 3 полностью доказана.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] А. А. Варфоломеев, А. Е. Жуков, М. А. Пудовкина, *Поточные криптосхемы. Основные свойства и методы анализа стойкости*, МИИ, М., 2000.
- [2] А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин, *Основы криптографии*, Гелиос АРВ, М., 2002.
- [3] F. P. Preparata, "Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties", *IEEE Trans. Electron. Comput.*, **15**:6 (1966), 898–908.
- [4] С. Н. Сумароков, "Запреты двоичных функций и обратимость для одного класса кодирующих устройств", *Обзорение прикладной и промышленной математики*, **1**:1 (1994), 33–55.
- [5] Б. А. Трахтенброт, Я. М. Барздинь, *Конечные автоматы (поведение и синтез)*, Наука, М., 1970.
- [6] О. Б. Лупанов, "О сравнении двух типов конечных источников", *Проблемы кибернетики*, **9**, Физматгиз, М., 1963, 321–326.
- [7] Ю. Л. Ершов, "О гипотезе В. А. Успенского", *Алгебра и логика. Сем.*, **1**:4 (1962), 45–48.
- [8] В. С. Гринберг, "Детерминизация систем графов и синтез конечных автоматов", *Сиб. матем. журн.*, **7**:6 (1966), 1259–1267.

- [9] G. F. Rose, “Output completeness in sequential machines”, *Proc. Amer. Math. Soc.*, **13**:4 (1962), 611–614.
- [10] В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин, *Элементы теории автоматов*, Изд-во Моск. гос. ун-та, М., 1978.
- [11] А. С. Подколзин, “О сложности распознавания автоматов-генераторов”, *Дискретный анализ*, **21**, Новосибирск, 1972, 31–61.
- [12] А. Гилл, *Введение в теорию конечных автоматов*, Наука, М., 1966.
- [13] Г. П. Гаврилов, А. А. Сапоженко, *Задачи и упражнения по курсу дискретной математики*, Наука, М., 1992.

А. В. Бабаш

Российский государственный социальный университет,
г. Москва

E-mail: babash@yandex.ru

Поступило

14.02.2010