ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 29 МАТЕМАТИКИ Выпуск 2
2022

Д. С. Богданов, **А. С. Логачев**, **В. О. Миронкин** (Москва, МИЭМ НИУ ВШЭ, Лаб. ТВП)**. Об обобщении одного алгоритма формирования равновероятных последовательностей произвольного модуля на основе реализаций равновероятной полиномиальной схемы.**

УДК 519.212.2+004.032.2 DOI https://doi.org/10.52513/08698325_2022_29_1_1

Резюме: Предложено обобщение вероятностного алгоритма жадной отбраковки, используемое для преобразования последовательностей, представляющих собой реализации произвольной равновероятной полиномиальной схемы, в равновероятные последовательности произвольного модуля. Получены точные выражения для среднего и дисперсии объема исходных данных, используемых для выработки одного знака выходной последовательности.

Ключевые слова: кодирование, отбраковка, равновероятная полиномиальная схема, разложение по степеням.

Введение. Механизмы защиты информации, построенные на основе случайных данных, широко внедрены в различные практические приложения информационной безопасности. Как правило, в качестве такого типа данных выступают двоичные последовательности, формируемые с использованием программных, физических, биологических и других процессов. Двоичные последовательности адаптированы под архитектуру ЭВМ, но в ряде случаев представляют собой далеко не самый удобный объект для непосредственного применения конечным пользователем. Например, при аутентификации посредством ввода PIN-кода и автоматически сгенерированного пароля пользователю проще запомнить и использовать строки, состоящие из десятичных цифр или букв некоторого алфавита, чем соответствующие двоичные последовательности. В связи с этим возникает естественная потребность в использовании процедур формирования равновероятных случайных последовательностей элементов произвольного алфавита, отличного от двоичного.

Некоторые существующие практические решения в указанной области детерминированны, просты в реализации и описании, но построены для конкретных значений мощностей алфавитов (далее — модулей) [1–4]. Альтернативой им являются недетерминированные алгоритмы [5, 6], которые хоть и сложнее, но позволяют из реализаций равновероятной схемы Бернулли довольно эффективно получать равновероятные случайные последовательности элементов произвольного модуля.

Представленное данным докладом исследование посвящено обобщению некоторых алгоритмов второго типа на случай использования в качестве входных данных реализации произвольной равновероятной полиномиальной схемы.

1. Алгоритм жадной отбраковки. Приведем краткое описание алгоритма [5] формирования одного элемента последовательности произвольного модуля $q \geqslant 2$ из входных данных, представляющих собой реализацию $\overline{z} = (z_1, z_2, \ldots)$ равновероятной схемы Бернулли.

Итак, для произвольного заданного $q \geqslant 2$ определим число $n \in \mathbb{N}$, удовлетворяющее двойному неравенству

$$2^{n-1} < q \leqslant 2^n.$$

В случае $q < 2^n$ определим числа $d_1, d_2, \ldots, d_k \in \mathbb{N}$, для которых

$$2^n - q = 2^{d_1} + 2^{d_2} + \cdots + 2^{d_k},$$

где $0 \leqslant d_1 < d_2 < \cdots < d_k \leqslant n-2$.

Для дальнейшего изложения введем следующие обозначения:

- $\xi := Y$ — операция присваивания величине ξ значения Y;
- $r_{n,m}(\cdot) : \{0, 1, \ldots, m-1\}^n \to \mathbb{Z}$ — биективное отображение, сопоставляющее строке $\overline{x} = (x_1, x_2, \ldots, x_n)$ такое число z, что

$$z = x_1 + m \cdot x_2 + \cdots + m^{n-1} \cdot x_n;$$

- $LSB_{n,m} : \bigcup\limits_{i=0}^{\infty} \{0, 1, \ldots, m-1\}^i \to \{0, 1, \ldots, m-1\}^n$

  — отображение, сопоставляющие строке $\overline{x} = (x_1, x_2, \ldots)$ ее младшие n элементов $x_1, x_2, \ldots, x_n$.

Алгоритм жадной отбраковки, формирующий один элемент последовательности, можно представить в следующем виде.

Алгоритм 1. Алгоритм жадной отбраковки

Вход: $q, n, d_1, d_2, \ldots, d_k, \overline{z}$;

1: $\overline{x} := \emptyset$;
2: **цикл**
3: Дополнить $\overline{x}$ реализацией равновероятной схемы Бернулли (ранее неиспользованным отрезком последовательности $\overline{z}$) до длины n;
4: $y := r_{n,2}(\overline{x})$;
5: **если** $y \in \{0, \ldots, q-1\}$, **то**
6: выход из цикла;
7: **если** $y \in [2^n - 2^{d_k}; 2^n - 1]$, **то**
8: $\overline{x} := \mathrm{LSB}_{d_k,2}(\overline{x})$;
9: **если** $y \in [2^n - 2^{d_k} - 2^{d_{k-1}}; 2^n - 2^{d_k} - 1]$, **то**
10: $\overline{x} := \mathrm{LSB}_{d_{k-1},2}(\overline{x})$;
11: $\vdots$
12: **если** $y \in [2^n - 2^{d_k} - \cdots - 2^{d_2} - 2^{d_1}; 2^n - 2^{d_k} - \cdots - 2^{d_2} - 1]$, **то**
13: $\overline{x} := \mathrm{LSB}_{d_1,2}(\overline{x})$;
конец цикла

Выход: y.

Процедура формирования равновероятной случайной последовательности элементов произвольного модуля q длины, большей 1, из реализации равновероятной схемы Бернулли заключается в итерировании Алгоритма 1 в количестве раз, равному соответствующей длине.

Теперь перейдем к описанию основного результата настоящего исследования.

2. Обобщение алгоритма жадной отбраковки. Алгоритм 1 допускает естественное обобщение на случай, когда входные данные $\overline{z}$ представляют собой реализацию $\overline{z} = (z_1, z_2, \ldots)$ произвольной фиксированной равновероятной полиномиальной схемы с $m \geqslant 2$ исходами.

По аналогии с разделом 1 определим число $N \in \mathbb{N}$, удовлетворяющее двойному неравенству

$$m^{N-1} < q \leqslant m^N, \tag{1}$$

а в случае $q < m^N$ определим такие числа $a_1, a_2, \ldots, a_s \in \{1, 2, \ldots, m-1\}$ и $l_1, l_2, \ldots, l_s \in \{0, 1, \ldots, N-1\}$: $l_1 < l_2 < \cdots < l_s$, что

$$m^N - q = a_1 \cdot m^{l_1} + a_2 \cdot m^{l_2} + \cdots + a_s \cdot m^{l_s}. \tag{2}$$

Тогда обобщенный алгоритм жадной отбраковки, формирующий один элемент последовательности, представляется в следующем виде.

Алгоритм 2. Обобщенный алгоритм жадной отбраковки

Вход: $q, m, N, a_1, a_2, \ldots, a_s, l_1, l_2, \ldots, l_s, \overline{z}$;

$\overline{x} := \emptyset$;

цикл

  Дополнить $\overline{x}$ реализацией равновероятной полиномиальной схемы с m исходами (ранее неиспользованным отрезком последовательности $\overline{z}$) до длины N;

  $y := r_{N,m}(\overline{x})$;

  если $y \in \{0, \ldots, q-1\}$, **то**

    выход из цикла;

  если $y \in [m^N - a_s \cdot m^{l_s}; m^N - 1]$, **то**

    $\overline{x} := \mathrm{LSB}_{l_s,m}(\overline{x})$;

  если $y \in [m^N - a_s \cdot m^{l_s} - a_{s-1} \cdot m^{l_{s-1}}; m^N - a_s \cdot m^{l_s} - 1]$, **то**

    $\overline{x} := \mathrm{LSB}_{l_{s-1},m}(\overline{x})$;

  $\vdots$

  если $y \in [m^N - a_s \cdot m^{l_s} - \cdots - a_2 \cdot m^{l_2} - a_1 \cdot m^{l_1}; m^N - a_s \cdot m^{l_s} - \cdots - a_2 \cdot m^{l_2} - 1]$, **то**

    $\overline{x} := \mathrm{LSB}_{l_1,m}(\overline{x})$;

конец цикла

Выход y.

Процедура формирования равновероятной случайной последовательности элементов произвольного модуля q длины, большей 1, из реализации произвольной фиксированной равновероятной полиномиальной схемы с m исходами заключается в итерировании Алгоритма 2 в количестве раз, равному соответствующей длине.

З а м е ч а н и е 1. Сохраненные в результате выполнения шагов 3–13 Алгоритма 2 младшие l_j элементов, где $j \in \{1, 2, \ldots, s\}$, являются независимыми и равновероятно распределенными на множестве $\{0, 1, \ldots, m-1\}$. Кроме того, (l_j+1)-й элемент вектора $\overline{x}$ равновероятно распределен на множестве $\{0, 1, \ldots, a_j - 1\}$. Последний факт может быть использован для формирования вспомогательной реализации равновероятной полиномиальной схемы с a_j исходами, к которой также может быть применен Алгоритм 2.

3. Оценка используемого объема входных данных Алгоритма 2. Одной из наиболее значимых характеристик алгоритмов формирования случайных последовательностей заданного модуля является объем исходных данных, используемый для формирования одного элемента на выходе.

Обобщенный алгоритм жадной отбраковки является вероятностным алгоритмом, а указанная характеристика представляет собой случайную величину $\xi_{m,q}$, принимающую значения из $\mathbb{N}$, распределение которой индуцировано равновероятным распределением на множестве реализаций полиномиальной схемы с m исходами.

Сформулируем результат, описывающий среднее и дисперсию указанной случайной величины.

Утверждение 1. *Пусть* $q, m \in \mathbb{N}$: $m \geqslant 2, q \geqslant 2$, *и пусть* $N \in \mathbb{N}$ *удовлетворяет* (1), *а* $a_1, a_2, \ldots, a_s \in \mathbb{N}$ *и* $l_1, l_2, \ldots, l_s \in \mathbb{N} \cup \{0\}$ *удовлетворяют* (2). *Тогда справедливы соотношения*

$$\begin{aligned} \mathbf{E}\,\xi_{m,q} &= n + \sum_{j=1}^{s} \frac{(n-l_j)\,a_j\,m^{l_j}}{q} \\ \mathbf{D}\,\xi_{m,q} &= \frac{m^{2N} - q m^N}{q^2} \left(\alpha^2 + \frac{q}{m^N}\left(\beta - \alpha^2\right)\right), \end{aligned} \tag{3}$$

где

$$\begin{aligned} \alpha &= \frac{1}{m^N - q} \sum_{j=1}^{s} a_j\, m^{l_j}\,(N - l_j), \\ \beta &= \frac{1}{m^N - q} \sum_{j=1}^{s} a_j\, m^{l_j}\,(N - l_j)^2. \end{aligned}$$

З а м е ч а н и е 2. Формула (3) может быть представлена в виде

$$\mathbf{E}\,\xi_{m,q} = \frac{N m^N}{q} - \sum_{j=1}^{s} \frac{a_j\, l_j\, m^{l_j}}{q},$$

отражающем тот факт, что Алгоритм 2 требует в среднем меньше элементов исходной последовательности для выработки одного элемента по модулю q по сравнению с алгоритмом полной отбраковки [7], в котором соответствующее среднее составляет $N m^N / q$.

З а м е ч а н и е 3. Обобщенный алгоритм жадной отбраковки допускает оптимизацию за счет подбора двух дополнительных параметров $R_1, R_2 \in \mathbb{N}$, минимизирующих величину $|m^{R_1} - q^{R_2}|$ и, как следствие, уменьшающих среднюю длину используемой реализации полиномиальной схемы для выработки одного элемента по модулю q.

При таком преобразовании параметров обобщенный алгоритм жадной отбраковки будет вырабатывать не один элемент по модулю q, а вектор длины R_2, состоящий из элементов по модулю q. Данный способ удобен, например, при формировании последовательностей, длины которых существенно больше R_2.

СПИСОК ЛИТЕРАТУРЫ

1. *Hiasat A. A.*, *Abdel-Aty-Zohdy S. H.,* Residue-to-binary arithmetic converter for the moduli set $(2^k, 2^k-1, 2^{k-1}-1)$. — IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 1998, v. 45, is. 2, p. 204–209.
2. *Krstić I.*, *Stamenković N.*, *Stojanović V.* Binary to RND encoder for the moduli set $\{2^n-1, 2^n, 2^n+1\}$ with embedded diminished-1 channel for DSP application. — Facta Universitatis. Ser. Electronics and Energetics, 2016, **29**:1, v. 29, № 1, p. 101–112.
3. *Cao B.*, *Chang C.-H.*, *Srikanthan T.* A residue-to-binary converter for a new five-moduli set. — IEEE Transactions on Circuits and Systems I: Regular Papers, 2007, v. 54, is. 5, p. 1041–1049.
4. *Wang Y.*, *Swamy M. N. S.*, *Abmad M. O.* Residue-to-binary number converters for three moduli sets. — IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 1999, v. 46, is. 2, p. 180–183.
5. *Миронкин В. О.* Об алгоритме формирования равновероятных последовательностей произвольного модуля на основе схемы независимых равновероятных испытаний Бернулли. — Обозрение прикл. и промышл. матем., 2021, т. 28, в. 1, с. 103–106. // *Mironkin V. O.* On the algorithm for generation of equiprobable sequences of an arbitrary module based on the scheme of independent equiprobable Bernoulli trials. — OPPM Surveys Appl. Industr. Math., 2021, v. 28, is. 1, p. 13–16. (In Russian.)
6. *Koo B.*, *Roh D.*, *Kwon D.* Converting random bits into random numbers. — J. Supercomput., 2014, **70**:1, v. 70, is. 1, p. 236–246.
7. *Barker E.*, *Kelsey J.* Recommendation for Random Number Generation Using Deterministic Random Bit Generators NIST Special Publication 800-90A. Gaithersburg, MD: National Inst. Standards Technol., 2012, ix+128 p.

Поступила в редакцию
22.IX.2022

UDC 519.212.2+004.032.2 DOI https://doi.org/10.52513/08698325_2022_29_1_1

Bogdanov D. C., Logachov A. C. Mironkin V. O. (Moscow, HSE Tikhonov Moscow Institute of Electronics and Mathematics, National Research University Higher School of Economics, TVP Laboratories)**. On the generalization of an algorithm for generation of equiprobable sequences of an arbitrary module based on implementations of an equiprobable polynomial scheme.**

Abstract: A generalization of the probabilistic algorithm of greedy rejection, used to transform sequences representing implementations of an arbitrary equiprobable polynomial scheme into equally probable sequences of an arbitrary module is proposed. Explicit expressions for the mean and variance of the size of the initial data used to generate one sign of the output sequence are obtained.

Keywords: Equally probable polynomial scheme, rejection, coding, power decomposition.