ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 28 МАТЕМАТИКИ Выпуск 1
2021

В. О. Миронкин (Москва, Национальный исследовательский университет «Высшая школа экономики»)**. Об алгоритме формирования равновероятных последовательностей произвольного модуля на основе схемы независимых равновероятных испытаний Бернулли.**

УДК 528.852.1

Резюме: Предложен алгоритм преобразования отрезка длины $n \in \mathbb{N}$ двоичной последовательности, представляющей собой реализацию схемы независимых равновероятных испытаний Бернулли, в отрезок равновероятной последовательности произвольного модуля $m > 2$. Указанный алгоритм представляет собой модификацию известного алгоритма отбраковки и позволяет уменьшить расход исходной последовательности.

Ключевые слова: Метод отбраковки, кодирование, разложение по степеням.

Введение

Настоящая работа посвящена изучению вопросов [1, 2], связанных с преобразованием отрезков длины $n \in \mathbb{N}$ двоичной последовательности (далее — исходной последовательности), представляющей собой реализацию схемы независимых равновероятных испытаний Бернулли, в отрезки равновероятной последовательности произвольного модуля $m > 2$ (далее — результирующей последовательности).

Так, одним из наиболее простых решений в указанной области является метод отбраковки [3], обеспечивающий в рассматриваемых условиях равновероятное распределение на множестве формируемых отрезков, но в ряде случаев (в зависимости от соотношения параметров n и m) требующий значительного количества знаков исходной последовательности.

Модификация метода отбраковки

Согласно [3] для формирования одного знака $y \in \mathbb{Z}_m \bigcup \varnothing$ вырабатывается отрезок $\overline{x}$ длины $n = \min\left\{t \in \mathbb{N} | 2^t \geqslant m\right\}$ исходной последовательности по схеме независимых равновероятных испытаний Бернулли. Пусть при этом $r = r(\overline{x})$ численное представление $\overline{x}$ в кольце $\mathbb{Z}_{2^n}$. Тогда правило формирования знака y определяется следующим образом:

$$y = \begin{cases} r, & 0 \leqslant r < m, \\ \varnothing, & m \leqslant r < 2^n. \end{cases}$$

Очевидно, что при $m \approx 2^{n-1} + 1$ вероятность отбраковки знаков исходной последовательности будет близка к $\frac{1}{2}$.

Таким образом, при реализации данного метода остается актуальным вопрос, связанный с возможностью использования отбракованной доли знаков исходной последовательности для формирования элементов модуля m.

Опишем модификацию метода отбраковки (далее — метод Миронкина), основанную на некоторых результатах теории кодирования, изложенных, например, в [4], и позволяющую решить обозначенную выше проблему оптимизации.

Метод Миронкина

1. Вырабатываем двоичный отрезок $\overline{x}$ длины n.

2. Если $0 \leqslant r(\overline{x}) < m$, то реализуем элемент $r(\overline{x})$ и завершаем алгоритм.
3. Если $m \leqslant r(\overline{x}) < 2^n$, то $\overline{x}$ преобразуем в отрезок $\overline{x'}$ длины $j < n$ по следующему правилу:
   (a) Определяем двоичное представление числа $2^n - m$:
   $$2^n - m = 2^d + \alpha_{d-1}2^{d-1} + \cdots + \alpha_1 2 + \alpha_0.$$
   (b) Определяем $j \leqslant d$, для которого выполняется двойное неравенство
   $$\alpha_{j-1}2^{j-1} + \alpha_{j-2}2^{j-2} + \cdots + \alpha_1 2 + \alpha_0 \leqslant$$
   $$\leqslant r(\overline{x}) - m < \alpha_j 2^j + \alpha_{j-1}2^{j-1} + \cdots + \alpha_1 2 + \alpha_0.$$
   (c) Формируем отрезок $\overline{x'}$, состоящий из j младших разрядов двоичного представления $r(\overline{x}) - m$.
4. Вырабатываем двоичный отрезок $\overline{x''}$ длины $n - j$, с использованием которого формируем отрезок $\overline{x} = \overline{x''}||\overline{x'}$. Переходим к шагу 2.

З а м е ч а н и е. Метод Миронкина допускает реализацию (с очевидными изменениями) в случае формирования знаков исходной последовательности с использованием k-ичного источника сообщений [5], где $k > 1$.

СПИСОК ЛИТЕРАТУРЫ

1. *Krstic I.*, *Stamenkovic N.*, *Stojanovic 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. — Electronics and Energetics, 2016, v. 29, is. 1, p. 101-112
2. *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.
3. *Мартышенко С. Н.* Компьютерный анализ данных: Учебное пособие, Владивосток: Изд-во ВГУЭС, 2010, 80 с.// *Martishenko S. N.* Komp'uterniy analiz dannih: Uchebnoye posobiye, Vladivostok: Izdatelstvo VGUES, 2010, 80 p. (in Russian)
4. *Балыгин К. А.*, *Зайцев В. И.*, *Климов А. Н.*, *Кулик С. П.*, *Молотков С. Н.* Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью около 100 Мбит/с, ЖЭТФ, 2018, v. 153, is. 6, p. 879–894.// *Baligin K. A.*, *Zaycev V. I.*, *Klimov A. N.*, *Kulik S. P.*, *Molotkov S. N.* Kvantovii generator sluchaynih chisel, osnovannii na puassonovskoy statistike fotootschetov, so skorost'u okolo 100 Mbit/s, ZETF, 2018, v. 153, is. 6, p. 879–894 (in Russian).
5. *Бабкин В. Ф.* Метод универсального кодирования источника независимых сообщений неэкспоненциальной трудоемкости. — Проблемы передачи информации, 1971, v. 7, is. 4, p. 13-21.// *Babkin V. F.* Metod universal'nogo kodirovaniya istichnika nezavisimih soobshenii neeksponencialnoy trdoyomkosti. — Probl. peredachi inform., 1971, v. 7, is. 4, p. 13–21 (in Russian).

UDC 528.852.1

Mironkin V. O. (National Research University Higher School of Economics, Moscow)**. On the algorithm for the formation of equiprobable sequences of an arbitrary module based on the scheme of independent equiprobable Bernoulli tests**

Abstract: An algorithm for transforming a segment of length n *in mathbbN* of a binary sequence, which is an implementation of the scheme of independent equiprobable Bernoulli tests, into a segment of an equiprobable sequence of an arbitrary modulus $m > 2$, is proposed. This algorithm is a modification of the well-known rejection algorithm and allows to reduce the consumption of characters in the original sequence.

Keywords: Culling method, coding, power expansion.