

УСЛОЖНЕНИЕ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПОМОЩЬЮ КОНЕЧНЫХ АВТОМАТОВ

Злобина Елена Витальевна

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: sheveleva.e.v@yandex.ru

Работа посвящена описанию алгебраических свойств генератора псевдослучайных чисел, составленного так, что выходная последовательность линейного регистра сдвига подаётся на вход конечного автомата, а в качестве выходных значений генератора используются выходные значения автомата. В такой постановке задача фигурирует в [2]. Данный вид генератора является усложнением линейных рекуррентных последовательностей с помощью конечных автоматов. В настоящее время отсутствует общая теория регистров сдвига с нелинейной обратной связью [1].

В данной работе рассматриваются генераторы, являющиеся композицией линейных регистров сдвига максимального периода и конечных автоматов, группа которых порождается двумя подстановками. В качестве групп рассматриваются группа Диэдра $D_m = \langle t_m, z \rangle$, где t_m — подстановка сдвига, а z — «зеркальное отражение», и аффинная группа $\text{Aff}(p) = \langle t_p, a \rangle$, где a — образующий элемент мультипликативной группы $GF(p)$ [3].

В работе получены следующие результаты:

Теорема 1. *В зависимости от выбора начального состояния генератора и выходной функции конечного автомата период выходной последовательности генератора псевдослучайных чисел, функции перехода конечного автомата которого образуют группу D_m , либо равен периоду линейного регистра сдвига, либо превышает его в два раза. Для каждого начального заполнения линейного регистра существует ровно одно, если m — нечётное, или ровно два, если m — чётное, начальных состояния конечного автомата, при которых период генератора равен периоду линейного регистра сдвига.*

Теорема 2. *Если функции перехода конечного автомата образуют группу $\text{Aff}(p)$ и выполнено равенство $\text{НОД}(2^{n-1}-1, p-1) = 1$, то для каждого начального заполнения линейного регистра сдвига максимального периода существует единственное начальное состояние*

конечного автомата (со специальной функцией выхода), при котором период генератора будет равен $2^n - 1$, где n — длина регистра; при других начальных состояниях конечного автомата период генератора будет равен числу $(p - 1) \cdot (2^n - 1)$.

Литература

1. Solomon T. Golomb. Shift Register Sequences. Singapore: World Scientific, 2017.
2. Асосков А. В., Иванов М. А., Мирский А. А. и другие. Поточные шифры. КУДИЦ-Образ, 2003.
3. Холл М. Теория групп. М.: Издательство иностранной литературы, 1962.