Реализация заданной стохастической функции на основе системы многочленов над полем Галуа

С.В. Шалагин[1], В.М. Захаров[1]

[1]*Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ (КНИТУ-КАИ), Карла Маркса 10, Казань, Россия, 420111*

Аннотация

Предложен метод реализации стохастической функции, определенной на основе матрицы заданной размерности, при использовании системы многочленов от многих переменных над полем Галуа и массива равномерно распределенных некоррелированных (псевдо)случайных чисел заданной разрядности. Определена погрешность представления элементов стохастической матрицы в зависимости от количества переменных и степени поля, над которым определены многочлены. Получены оценки сложности вычисления системы указанных многочленов.

Ключевые слова

Стохастическая функция, многочлены, поле Галуа

1. Введение

Вероятностные автоматы (ВА) находят широкое применение в таких областях, как статистическое моделирование, распознавание образов, кодирование и декодирование информации [1, 2], техническая диагностика цифровых устройств, обработка сигналов в системах связи и управления. Применение ВА позволяет определить метод генерирования дискретных марковских процессов и их функций, как детерминированных, так и стохастических. Представляют интерес задачи синтеза конечных цепей Маркова и их стохастических функций, задаваемых стохастическими матрицами (СМ) [3, 4]. Известен метод разложения СМ на имплицирующий вектор и стохастические булевы матрицы [5 - 7].

Согласно [8, стр. 55] вероятностная функция, заданная СМ, представима как система генераторов дискретных случайных величин (ДСВ). Известен [9] метод синтеза ДСВ на основе многочленов над полем Галуа. В данной работе объединены указанные подходы: решена задача синтеза вероятностной функции, заданной СМ произвольного размера при использовании системы многочленов над полем Галуа вида $G = GF(2^v)$.

Данное обстоятельство позволяет выполнять моделирование сложных систем, заданных СМ, при использовании специализированных вычислителей – ПЛИС/FPGA, архитектура которых соответствует алгоритму распределенного вычисления системы указанных многочленов [10].

2. Стохастическая функция на основе многочленов

Рассмотрим решение задачи синтеза стохастической функции, заданной СМ вида:

$$P = \left(p_{ij} \right)_{k \times l}, \qquad (1)$$

СМ (1) представима как *n* дискретных случайных величин (ДСВ) X_i, принимающих одно из *l* возможных значений $\left(s_1 \quad s_2 \quad \ldots \quad s_l \right)$; закон распределения X_i задан элементами *i*-й строки СМ (1), $i = \overline{1, k}$. Каждый элемент p_{ij} приближенно определим как $p'_{ij} = s_{ij} / D_{ij}$, где s_{ij} и D_{ij} – целые положительные числа, $\left| p_{ij} - p'_{ij} \right| \le \varepsilon$, $i = \overline{1, k}$, $j = \overline{1, l}$. Определим $R = \mathrm{LOM}\left(D_{ij} \right)$ –

наименьший общий делитель чисел D_{ij}, $i=\overline{1,k}$, $j=\overline{1,l}$. Введем в рассмотрение многочлен от m переменных над полем G:

$$f(q_1,...,q_m)=\sum_{i_1=0}^{r}...\sum_{i_m=0}^{r}a_{i_1...i_m}q_1^{i_1}...q_m^{i_m},\quad r=2^v-1. \tag{2}$$

Справедлива

Теорема. Синтез генератора дискретной случайной величины X_i, $i=\overline{1,k}$, $j=\overline{1,l}$, производится на основе композиции m некоррелированных генераторов равномерно распределенных v-разрядных (псевдо)случайных чисел и многочлена вида (2), определенной над полем G, размерность которого удовлетворяет условиям $2^{v\cdot m}\geq\log_2 R$ и $2^v\geq l$, при этом погрешность представления элементов закона распределения X_i не превышает $\varepsilon=2^{-v\cdot m}$.

Теорема 1 обосновывает метод представления стохастической функции, заданной СМ вида (1) на основе системы из k полиномов вида (2). На основе метода получаем коэффициенты для k многочленов вида (2). Получены оценки сложности вычисления указанных многочленов согласно [10, 11].

3. Заключение

Предложен метод представления стохастической функции, заданной СМ размера $k\times l$ при использовании систем из k многочленов от m переменных, определенных над $GF(2^v)$. Функция представима на основе одного массива некоррелированных генераторов равномерно распределенных чисел разрядности v. Погрешность представления элементов СМ – не более $\varepsilon=2^{-v\cdot m}$. Получены оценки сложности вычисления системы из k указанных многочленов.

4. Литература

[1] Raikhlin,V.A. Reliable recognition of masked binary matrices. Connection to information security in map systems / V.A. Raikhlin, I.S. Vershinin, R.F. Gibadullin // Lobachevskii J Math. – 2013. – Vol. 34. – P. 319-325. DOI: 10.1134/S1995080213040112.

[2] Vershinin, I.S. Associative Steganography. Durability of Associative Protection of Information / I.S. Vershinin, R.F. Gibadullin, S.V. Pystogov // Lobachevskii J Math. – 2020. – Vol. 41. – P. 440-450. DOI: 10.1134/S1995080220030191.

[3] Бухараев, Р.Г. Специализированная ЭВМ для моделирования и обработки функций конечных однородных цепей Маркова / Р.Г. Бухараев, В.И. Геза // Всес. симп. по вероятностным автоматам: тезисы докл. – Казань: Изд-во КГУ, 1969. – С. 14-15.

[4] Бухараев, Р.Г. Управляемые генераторы случайных кодов / Р.Г. Бухараев, В.М. Захаров. – Казань: КГУ, 1978. – 160 с.

[5] Поспелов, Д.А. Вероятностные автоматы. – М.: Энергия, 1970. – 88 с.

[6] Ченцов, В.М. Об одном методе синтеза автономного стохастического автомата // Кибернетика. – 1968. – № 3. – С. 32-35.

[7] Лоренц, А.А. Синтез надежных вероятностных автоматов. – Рига: Зинатне, 1975. – 168 с.

[8] Захаров, В.М. Аппаратно-программная организация специализированных процессоров на основе автономных вероятностных автоматов. – Казань, 1992. – 297 с.

[9] Нурутдинов, Ш.Р. Основы теории полиномиальных моделей автоматных преобразований над полем Галуа. – Казань: Изд-во Казан. ун-та, 2005. – 155 с.

[10] Шалагин, С.В. Реализация цифровых устройств в архитектуре ПЛИС/FPGA при использовании распределенных вычислений в полях Галуа: монография. – Казань: Изд-во КНИТУ-КАИ, 2016. – 228 с.

[11] Zakharov, V.M. Executing discrete orthogonal transformations based on computations on the Galois field in the FPGA architecture / V.M. Zakharov, S.V. Shalagin // International Siberian Conference on Control and Communications (SIBCON). – Moscow, 2016. – P. 1-4. DOI: 10.1109/SIBCON.2016.7491652.