УДК 004.272.26

DOI: 10.21779/2542-0321-2023-38-3-28-33

В.М. Захаров, С.В. Шалагин, А.И. Гумиров

Генератор дискретной случайной величины с заданным законом распределения в архитектуре ПЛИС/FPGA

Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ; Россия, 420111, г. Казань, ул. Карла Маркса, 10; Gilvv@mail.ru, SShalagin@mail.ru, neporebrik@mail.ru

Аннотация. Получены оценки аппаратной сложности генератора дискретной случайной величины с заданным законом распределения в архитектуре ПЛИС класса FPGA при использовании однотипных IP-ядер. Определена структурная схема данного IP-ядра на структурном и функционально-логическом уровне, в архитектуре ПЛИС/FPGA. Оценки для IP-ядра вычислены по количеству LUT-таблиц для различных ПЛИС класса FPGA в зависимости от разрядности случайных величин, подаваемых на вход генератора, и от количества значений генерируемой случайной величины. Определено количество однотипных IP-ядер, которые могут разместиться в одном корпусе ПЛИС/FPGA при заданных ограничениях на долю задействованных ресурсов – LUT-таблиц.

Ключевые слова: дискретная случайная величина, распределение, сложность, ПЛИС.

Введение

Задача высокоскоростного генерирования массивов случайных чисел, распределённых по заданному закону, является актуальной [1; 2]. Их генерация основана на порождении последовательностей равномерно распределённых (псевдо)случайных чисел (ПСЧ) [3–6] и важна для генерирования марковских последовательностей [7], применяемых для многих приложений в микроэлектронике, например для тестирования и диагностики сложных изделий. Кроме того, стохастические процессы находят применение в различных областях науки и техники [8–16], что имеет значение для развития направления по разработке аппаратных средств статистического моделирования [1]. Технические аспекты решения данной задачи связаны с созданием специальных процессоров, структура которых позволяет варьировать логику функционирования и реализовать вероятностные алгоритмы при использовании распределённых вычислений [1]. В частности, генераторы дискретных случайных величин (ДСВ) [1; 17].

Перспективным является подход, связанный с реализацией различных цифровых устройств на программируемых логических интегральных схемах класса FPGA [18–21] (далее – ПЛИС) при использовании однотипных IP-ядер [3]. В данной работе указанный подход применён к решению задачи синтеза генератора ДСВ (ГДСВ) с заданным законом распределения. Задача решена на примере ПЛИС семейства Virtex-4 [18]. Представленная проработка схемы ГДСВ на структурном уровне при использовании однотипных IP-ядер [22] (далее – Ядер) в базисе LUT-таблиц (логический аппарат ПЛИС) позволяет реализовать указанное устройство на различных ПЛИС класса FPGA, как на существующих, так и на перспективных.

Основные понятия и определения

Рассмотрим алгоритм формирования ДСВ (АДСВ) [17]. Закон ДСВ задан в виде:

$$\left(x_0, p_0\right), \left(x_1, p_1\right), ..., \left(x_{q-1}, p_{q-1}\right), \quad (1)$$

где ДСВ x принимает значение x_i с вероятностью p_i, $i = \overline{0, q-1}$, $\sum_{i=0}^{q-1} p_i = 1$. На вход АДСВ поступает значение $z \in \left[A, B\right]$: равномерно распределённое целое ПСЧ на интервале от A до B включительно [3 – 6]. Примем $N = B - A + 1$. На выход АДСВ выдаётся x_i:

$$N_i < z \le N_{i+1},\ N_0 = A,\ N_i = A + N \cdot \sum_{j=0}^{i-1} p_j, \quad (2)$$

$N_i \in \left[A, B\right]$, $i = \overline{0, q-1}$. Значение N ограничено неравенством: $2^{n-1} < N \le 2^n$, где n – разрядность двоичных чисел N_i, z, $i = \overline{0, q-1}$, $n \in \left[3, 24\right]$. Элементы p_i из (1) приближённо определены по формуле (2) как $p_i' = \left(N_{i+1} - N_i\right)/N$, $i = \overline{0, q-2}$, $p_{q-1}' = \left(B - N_{q-1}\right)/N$, при этом $\left|p_i - p_i'\right| \le \left(2N\right)^{-1}$, $i = \overline{0, q-1}$, $q \in \left[1, N-1\right]$.

Структурная модель генератора дискретной случайной величины

Для реализации ГДСВ, заданного (1), значениям p_i ставятся в соответствие $q-1$ значений N_i согласно (2), $i = \overline{1, q-1}$. Требуется $q-1$ компаратор n-разрядных чисел (Comp), выдающих единицу, когда $N_i < z$, и $q-1$ n-разрядных регистров для хранения N_i (Rg). Для определения значения x_i согласно (2) требуется посчитать количество единиц, снимаемых с выходов Comp. Схема подсчёта единиц реализована согласно [23, с. 28–31].

В структурной схеме ГДСВ, заданного согласно (1), реализацию алгоритма (2) выполним при использовании k однотипных IP-ядер [22] в базисе LUT-таблиц, $k = \left]q/m - 1\right[$. Каждое из ядер включает в свой состав $m-1$ Comp, $m < q$, выдающих единицу когда $N_i^{(l)} < z$, и $m-1$ Rg для хранения $N_i^{(l)}$, $i = \overline{1, m-1}$; позволяет сформировать $m-1$ значение ДСВ от x_0 до x_{m-2} и признак условия $N_{m-1}^{(l)} < z$, $l = \overline{1, k}$. Выполнение условия для l-го ядра означает, что выработка значения ДСВ осуществляется ядром с номером, большим, чем l, $l = \overline{1, k-1}$.

Выработка ДСВ происходит следующим образом. На вход каждого из k ядер подаётся значение z. С выхода l-го ядра $l = \overline{2, k}$ снимается значение x_M, $M = \left(m-1\right)\left(l-1\right) + x_i$ при выполнении условия вида:

$$\left(N_{m-1}^{(l-1)} < z\right) \& \left(N_{m-1}^{(l)} \ge z\right). \quad (3)$$

Для ядра с номером 1 требуется отслеживать только часть условия (3), реализуемого одним компаратором внутри данного ядра: $\left(N_{m-1}^{(1)} \ge z\right)$. Для ядер с номерами $l = \overline{2, k}$ вычисление условия (3) требует по одному конъюнктору с прямым (для Comp с $\left(l-1\right)$-го ядра) и инверсным (для Comp с l-го ядра) входами; всего $\left(k-1\right)$ конъюнкторов.

Замечание 1. Количество значений, снимаемых с ГДСВ, не превышает $q \le k\left(m-1\right)$.

Реализация в одном корпусе ПЛИС нескольких ядер требует, чтобы оценки количества LUT-таблиц не превышали заданных граничных значений [24]:

$$Q\left(n,m\right) \le k_Q \cdot Q_{\max},\ I\left(n,q\right) \le k_I \cdot I_{\max}, \quad (4)$$

где $Q_{\max}$ и $I_{\max}$ – максимальное количество доступных пользователю LUT-таблиц и БВВ в одном корпусе заданной ПЛИС, а *c* и k_I – допустимые коэффициенты использования ресурсов ПЛИС, установленные эмпирическим путём. Обычно $k_Q, k_I \in \left[0{,}5,\ 0{,}7\right]$ [25]; $I\left(n,q\right) \in \left[\right]\log_2 q\left[, n+\right]\log_2 q\left[\right]$ – количество БВВ, требуемое для реализации ГДСВ на основе *k* ядер, $k = \left]q/m-1\right[$.

Замечание 2. Количество используемых БВВ ПЛИС при любом количестве ядер не превышает величины $\left]\log_2 q\right[$; если же источник *n*-разрядного равномерно распределённого ПСЧ находится вне ПЛИС, то количество используемых БВВ не превышает $n+\left]\log_2 q\right[$.

Эксперименты по реализации генератора дискретной случайной величины на ПЛИС

Проведены эксперименты по реализации ядер на ПЛИС XC4VFX12-12-SF363 семейства Virtex-4 [18], для которых значения разрядности *n* величин *z* и $N_i^{(l)}$, $i = \overline{1, m-1}$, равны 8, 16 и 24, а количество значений *m* – 8 и 16. Обозначим как $Q\left(n,m\right)$ количество LUT-таблиц, требуемых для реализации ядра при заданных значениях *n* и *m*. Указанные значения при заданных *n* и *m* получены при использовании специализированной САПР ISE DESIGN SUITE 14.7 и приведены в таблице 1 и на рис. 1. Величина $Q\left(n,m\right)$ согласно экспериментальным данным является фактором ограничения при реализации ядер на ПЛИС XC4VFX12-12-SF363.

Для ПЛИС XC4VFX12-12-SF363 семейства Virtex-4 $Q_{\max} = 10944$, $I_{\max} = 240$.

Таблица 1. Значение $Q\left(n,m\right)$

m	*n*		
	8	16	24
8	21	40	57
16	43	101	122

Согласно (4) величина $I\left(n,q\right)$ не должна превышать величину от 120 (при $k_I = 0{,}5$) до 168 (при $k_I = 0{,}7$).

Рассмотрим случай, когда генератор равномерно распределённого ПСЧ находится внутри ПЛИС XC4VFX12-12-SF363. Тогда, согласно замечанию 2, $I\left(n,q\right) = \left]\log_2 q\right[= \left]\log_2 m \cdot k\right[$. Откуда следует, что $\log_2 m \cdot k \le k_I \cdot I_{\max}$, т. е. $m \cdot k \le 2^{k_I \cdot I_{\max}}$. Второй случай – когда $I\left(n,q\right) = n+\left]\log_2 m \cdot k\right[$. Тогда, согласно замечанию 2, $\log_2 m \cdot k \le \left(k_I \cdot I_{\max} - n\right)$, т. е. $m \cdot k \le 2^{k_I \cdot I_{\max} - n}$. Значение $k_I \cdot I_{\max} - n$, степень числа 2, будет не менее 96 (для $n = 24$), что делает количество БВВ рассматриваемой ПЛИС несущественным фактором, ограничивающим количество ядер *k*.

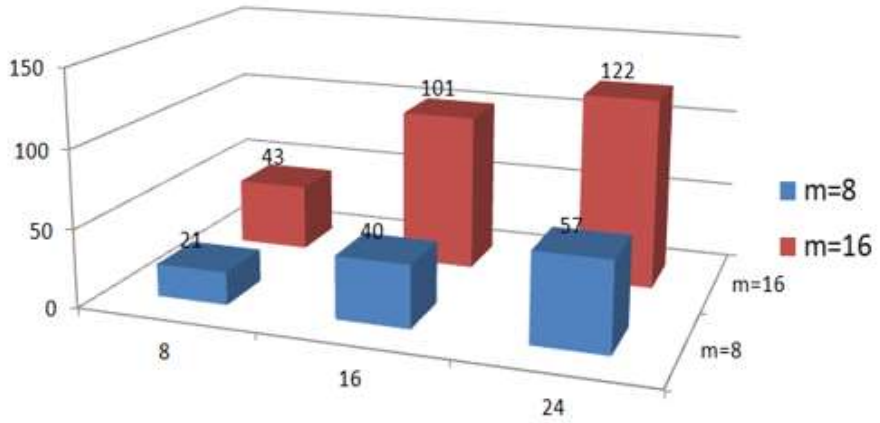

Рис. 1. Значение $Q(n,m)$ в зависимости от разрядности *n* и количества *m*

При использовании 50 % ресурсов LUT-таблиц указанной ПЛИС ($k_Q = 0,5$) на ней, согласно (4), могут разместиться от 44 до 260 ядер (см. табл. 2), а при использовании 70 % ресурсов ($k_Q = 0,7$) – от 62 до 364 ядер (см. табл. 3). Каждое из ядер *k* занимает от 21 до 122 LUTs, количество которых является фактором ограничения при выполнении условия (4). Количество значений ДСВ, определенное согласно замечанию 1 как $q \le k(m-1)$, указано в таблице 4. Для $k_Q = 0,5$ значение *q* принадлежит интервалу от 660 до 1905, а для $k_Q = 0,7$ – от 930 до 2670.

Таблица 2. Количество ядер *k* при $k_Q = 0,5$

m	*n*		
	8	16	24
8	260	136	95
16	127	54	44

Таблица 3. Количество ядер *k* при $k_Q = 0,7$

m	*n*		
	8	16	24
8	364	191	134
16	178	75	62

Таблица 4. Количество значений ДСВ при заданных k_Q, *n* и *m*

m	$k_Q = 0,5$			$k_Q = 0,7$		
	N			*n*		
	8	16	24	8	16	24
8	1820	952	665	2548	1337	938
16	1905	810	660	2670	1125	930

Ядра имеют задержку от 10,1 до 13,0 нс, что позволяет обеспечить генерирование ДСВ с частотой от 76,9 до 99,0 МГц. Данная частота составляет от 17,1 до 22,0 % относительно максимальной тактовой частоты работы ПЛИС XC4VFX12-12-SF363, равной 450 МГц [18].

Заключение

Решена задача высокоскоростного генерирования дискретных случайных величин согласно заданному закону распределения при использовании однотипных IP-ядер в архитектуре программируемых логических интегральных схем. Получены оценки аппаратной сложности (по количеству задействованных ядер и количеству значений ДСВ) и времени задержки функционирования ГДСВ, реализованных при использовании ядер на примере ПЛИС семейства Virtex-4.

Авторы выражают благодарность обучающемуся магистратуры КНИТУ-КАИ Алимову А.Р. за помощь в получении экспериментальных данных.

Литература

1. *Захаров В.М.*, *Шалагин С.В.* О развитии аппаратных средств статистического моделирования // ТРУДЫ SORUCOM-2014. Третья Межд. конф. «Развитие вычислительной техники и ее программного обеспечения в России и странах бывшего СССР: история и перспективы», Казань, 13–17 октября 2014 года. – Казань: КГТУ им. А.Н. Туполева, 2014. – С. 109–114.

2. *Захаров В.М.*, *Шалагин С.В.*, *Гумиров А.И.* Аппаратно-программный модуль генератора марковских последовательностей на основе программируемых логических интегральных схем // Вестник Казанского государственного технического университета им. А.Н. Туполева. 2022. Т. 78, № 4. – С. 164–172.

3. *Алферов А.П.*, *Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.

4. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

5. *Иванов М.А.*, *Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

6. *Песошин В.А.*, *Кузнецов В.М.* Генераторы псевдослучайных и случайных чисел на регистрах сдвига. – Казань: Изд-во КГТУ им. А.Н. Туполева, 2007. – 296 с.

7. *Kemeny J.G. and Snell J.L.* Finite Markov Ghains. – Princeton: Van Nostrand, 1960. – 210 p.

8. *Pesoshin V.A.*, *Kuznetsov V.M.*, *Rakhmatullin A.K.* Pseudo-random sequences with nonmaximal length based on the shift register and reducible polynomia l // Journal of Physics: Conference Series, Veliky Novgorod, June 27–28 2019. – Veliky Novgorod, 2019. – P. 012035. – DOI 10.1088/1742-6596/1352/1/012035.

9. *Песошин В.А.*, *Кузнецов В.М.*, *Кузнецова А.С.* Генераторы псевдослучайных последовательностей немаксимальной длины на регистрах сдвига с линейной обратной связью на основе примитивного многочлена в степени // Известия высших учебных заведений. Поволжский регион. Технические науки. 2019. № 4 (52). – С. 14–26.

10. *Русилко Т.В.*, *Сальников Д.А*. G-сеть как математическая модель сети передачи данных // Вестник Дагестанского государственного университета. Серия 1: Естественные науки. 2022. Т. 37, вып. 2. – С. 7–15. – DOI 10.21779/2542-0321-2022-37-2-7-15.

11. *Кондратенко А.Е.*, *Соболев В.Н.* О максимизации энтропии при свертке с равномерным распределением // Вестник Дагестанского государственного университета. Серия 1: Естественные науки. 2022. Т. 37, вып. 1. – С. 7–11. – DOI 10.21779/2542-0321-2022-37-1-7-11.

12. Генераторы псевдослучайных последовательностей немаксимальной длины на регистрах сдвига/ *В.А. Песошин*, *В.М. Кузнецов*, *А.С. Кузнецова*, *А.Р. Шамеева* // Известия высших учебных заведений. Поволжский регион. Технические науки. 2019. № 1 (49). – С. 3–17.

13. *Latypov R.*, *Stolov E.* True Random Generators and Hidden Transfer of Keys // Proceedings – 2019 International Russian Automation Conference, RusAutoCon 2019, Sochi, 8–14 sep. 2019. – Sochi: Institute of Electrical and Electronics Engineers Inc., 2019. – P. 8867784. – DOI 10.1109/RUSAUTOCON.2019.8867784.

14. *Шалагин С.В.* Стохастическая модель измерения состояния кудита // Вестник Дагестанского государственного университета. Серия 1: Естественные науки. 2023. Т. 38, вып. 2. – С. 74–80. – DOI 10.21779/2542-0321-2023-38-2-74-80.

15. *Песошин В.А.*, *Кузнецов В.М.*, *Рахматуллин А.Х.* Синтез и анализ алгоритмов поиска множества инверсно-сегментных последовательностей с заданным периодом // Программные системы и вычислительные методы. 2019. № 3. – С. 73–84.

16. *Захаров В.М.*, *Шалагин С.В.*, *Эминов Б.Ф.* Метод представления множеств стохастических матриц для многопараметрического анализа укрупненных и расширенных цепей Маркова // Вестник Дагестанского государственного университета. Серия 1: Естественные науки. 2020. Т. 35, вып. 3. – С. 53–62. – DOI 10.21779/2542-0321-2020-35-3-53-62.

17. *Гладкий В.С.* Вероятностные вычислительные модели. – М.: Наука, 1973. – 300 с.

18. Семейство Virtex-4. 1998-2016. ООО Рынок микроэлектроники. – Режим доступа: http://www.gaw.ru/html.cgi/txt/ic/Xilinx/plis/virtex/ virtex-4.htm (дата обращения: 14.05.2023).

19. FPGA Leadership across Multiple Process Nodes/ Advanced Micro Devices, Inc. 2023. – Режим доступа: https://www.xilinx.com/products/silicon-devices/fpga.html

20. ПЛИС Altera. ООО «Электроника-РА». 2014–2021. – Режим доступа: https://el-ra.ru/mikroskhemy/plis-cpld/plis-altera/

21. Новые российские ПЛИС // Современная электроника. Новости. 2019. – Режим доступа: https://www.soel.ru/novosti/2019/novye_rossiyskie_plis/ (дата обращения: 20.03.2023).

22. *Зотов, В.Ю.* Проектирование встраиваемых микропроцессорных систем на основе САПР фирмы Xilinx. – М.: Горячая линия – Телеком, 2006. – 522 с.

23. *Гашков С.Б.* Сложение однобитных чисел. Треугольник Паскаля, салфетка Серпинского и теорема Куммера. – М.: МЦНМО, 2014. – 40 с.

24. *Шалагин С.В.* Сложность вычисления нелинейных полиномиальных функций над полем $GF(2^2)$ на ПЛИС/FPGA// Поиск эффективных решений в процессе создания и реализации научных разработок в российской авиационной и ракетно-космической промышленности: Межд. научно-практ. конф., Казань, 5–8 августа 2014 года. Т. II. – Казань: Издательство Казанского государственного технического университета, 2014. – С. 661–664.

25. *Пономарев В.И.*, *Шабалин Л.А.* Проектирование реконфигурируемых устройств обработки цифровых потоков данных. Информационные технологии. 1996. № 5. – С. 24–28.

Поступила в редакцию 5 августа 2023 г.
Принята 5 сентября 2023 г.

UDC 004.272.26

DOI: 10.21779/2542-0321-2023-38-3-28-33

Discrete Random Variable Generator With the Given Distribution Law in FPGA-Architecture

V.M. Zakharov, S.V. Shalagin, A.I. Gumirov

Kazan National Research Technical University named after A.N. Tupolev – KAI; Russia, 420111, Kazan, Karl Marks st., 10; Gilvv@mail.ru, SShalagin@mail.ru, neporebrik@mail.ru

Abstract. The estimates of the hardware complexity of a discrete random variable generator with given distribution law in FPGA-architecture using the same type of IP-cores are obtained. The block diagram of this IP-core is defined at the structural and functional-logical level, in the FPGA-architecture. The estimates for the IP-core are calculated from the number of LUT-tables for various FPGAs, depending on the bit depth of random variables supplied to the generator input and the number of the generated random variable values. The number of IP-cores of the same type that can be placed in one FPGA enclosure under specified restrictions on the share of resources involved – LUT-tables.

Keywords: a discrete random variable, distribution, complexity, FPGA.

Received 5 August 2023
Accepted 5 September 2023