KYBERNETIKA — ТОМ *19* (1983), ВЫПУСК 1

ГЕНЕРАТОР РАНДОМИЗИРОВАННЫХ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Я. ГАВЕЛ, А. Н. МОРОЗЕВИЧ, В. Н. ЯРМОЛИК

Статья посвящена разработке принципов построения параллельных генераторов рандомизированных псевдослучайных чисел, как аппаратных средств систем статистической диагностики сложных электронных схем. В ней показана необходимость использования таких генераторов, описана методика синтеза генераторов, отличающихся от известных наличием нулевой комбинации и возможностью воспроизведения любого из множества допустимых порождающих полиномов, приведен пример конкретной реализации структуры параллельного генератора рандомизированных псевдослучайных чисел.

В последнее время большое внимание уделяется вопросам создания методов и средств проверки функционирования сложных вычислительных схем, имитационного моделирования, построению систем связи с использованием шумоподобных сигналов, и. т. д. Решение вышеназванных задач предопределяет необходимость создания быстродействующих высокоэкономичных и надежных генераторов равномернораспределенных псевдослучайных чисел [1, 2]. При этом все более возрастающую роль приобретают требования к качеству псевдослучайных последовательностей, особенно при построении автоматизированных систем контроля логических схем, основанных на статистическом методе [3] и методе сигнатурного анализа [4], которые характеризуются рядом существенных преимуществ по сравнению с традиционным методом тестового контроля. Подобные системы как правило включают генераторы псевдослучайных последовательностей испытательных сигналов, причем в подовляющем большинстве подобные генераторы строятся на базе регистра сдвига с обратной связью [5, 6]. Несомненно генераторы псевдослучайных испытательных сигналов, рассмотренные в [5] и в [6], отличаются рядом весьма существенных достоинств по сравнению с другими известными устройствами подобного типа. В тоже время использование таких устройств, в частности, при построении современных автоматизированных систем контроля, накладывает ограничения

принципиального характера на вид контролируемой схемы. Причина возникновения ограничений на вид контролируемых цифровых схем с памятью заключается в детерминированной структуре псевдослучайных последовательностей. Для любого генератора псевдослучайных последовательностей можно утверждать, что после определенного кода ξ_i на его выходе всегда будет следовать ξ_{i+1} заранее точно известное. В тоже время в физических генераторах случайных чисел ξ_{i+1} может принимать любое значение из множества возможных.

Влияние детерминированной структуры псевдослучайных последовательностей на их качественные показатели поясним на примере контроля функционирования некоторого типового элемента замены (*ТЭЗ*а) ЦВМ, приведенного

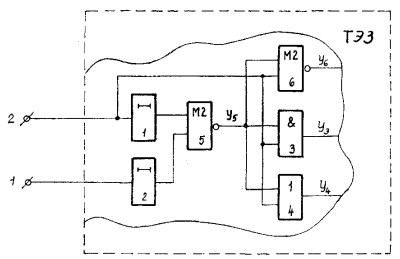

Рис. 1.

на рис. 1, статистическими методами. На рис. 1 приведен фрагмент цифровой схемы, состоящей из элементов задержки 1 и 2, элемента *ИЗ*, элемента *ИЛИ* 4 и двух двухвходовых сумматоров по модулю два с инверсными выходами 5, 6. Пусть на 1 и 2 входы *ТЭЗ*а подключены выходы $a_{j-i}(k)$ и $a_{m-i}(k)$-го разряда $i = 0, 1, \ldots, (j-1)$ генератора тестовых сигналов [5], последовательность состояний которых описывается следующей системой логических уравнений

$$(1) \qquad a_{m-i}(k+1) = a_{j-i}(k) \oplus a_{m-i}(k)\,; \quad i = 0, 1, \ldots, j-1\,,$$

$$a_{m-i}(k+1) = a_{2j-i}(k) \oplus a_{m+j-i}(k) \oplus a_{m-i}(k)\,;$$

$$i = j, j+1, \ldots, j+m-1\,,$$

где $a_{m-i}(k+1) \in \{0, 1\}$ – содержимое $m-i$-го разряда генератора в $k+1$ такт работы; m-разрядность генератора; j – определяется видом порождающего характеристического полинома $\varphi(x) = 1 + x^j + x^m$ и зависит от величины m, причем необходимо чтобы $j > \frac{1}{2}m$; $\oplus$ – знак суммы по модулю два. Учитывая то, что элементы задержки 1 и 2 задерживают информацию на один такт, в некоторый $(k+1)$ – ый такт контроля *ТЭЗ*а на выходах элементов 1 и 2 будут значения $a_{j-i}(k)$ и $a_{m-i}(k)$ соответсвенно. С учетом (1) значение

переключательной функции y_5 на выходе элемента 5 будет равняться $y_5 = \neg\, a_{m-i}(k+1)$. В тоже время значение переменной на входе *ТЭЗ*а 2: $a_{m-i}(k+1)$. Таким образом для переключательных функций на выходах элементов 3, 4, 6 можно записать

$$y_3 = \neg\,[a_{m-i}(k+1)]\, a_{m-i}(k+1) = 0\,;$$

$$y_4 = \neg\, a_{m-i}(k+1) + a_{m-i}(k+1) = 1\,;$$

$$y_6 = \neg\,[\neg\, a_{m-i}(k+1) \oplus a_{m-i}(k+1)] = 0\,.$$

Постоянные значения переключательных функций y_3, y_4 и y_6 говорят о том что неисправности вида *const* 1 и *const* 0 по выходам элементов 3, 4 и 6 при сколь угодно больших статистиках входных последовательностей не выявляются. При использовании сигнатурного анализа значения контрольных сумм (сигнатур) для исправного *ТЭЗ*а и *ТЭЗ*а с указанными неисправностями будут идентичны, что будет свидетельствовать о исправности неисправного *ТЭЗ*а.

Причина появления подобных пассивных цепей в контролируемых схемах обусловлена детерминированной природой входных испытательных сигналов. Введение большого количества промежуточных контрольных точек, использованние синхронных элементов памяти, перекоммутация выходных каналов генератора несколько снижает значение P — вероятность появления пассивных цепей в контролируемых схемах, однако принципиально $\mathsf{P} \neq 0$.

Подобным образом можно привести большое множество примеров, показывающих ограниченность применения псевдослучайных сигналов в силу их детерминированности. В частности как показано в [7] по тем же причинам псевдослучайные последовательности нельзя использовать для решения серьёзных задач криптографии.

Стремление улучшить качество случайных чисел приводит к необходимости использования физических принципов при построении генераторов исходных равномерно распределенных чисел. Однако необходимость обеспечения максимального быстродействия и требуемой разрядности, достигающей 180 разрядов [6], приводит к существенному усложнению аппаратуры.

Наиболее экономично многоразрядные последовательности равномерно распределенных чисел могут быть получены при помощи комбинированного подхода использующего псевдослучайные и случайные последовательности [8, 9, 12]. Преимущества данного подхода заключаются в том, что природа выходных последовательностей максимально приближена к истинно случайным, при том аппаратурные затраты практически не отличаются от затрат на построение генераторов псевдослучайных последовательностей.

В тоже время невозможность получения на выходе устройства описанного в [9] m-разрядного псевдослучайного числа $\xi_k = 000, \ldots, 0$, приводит к искажению равномерного закона распределения. Однако более существенным недостатком подхода описанного в [8, 9] является ограниченность его функциональ-

ных возможностей. При практической реализации ГПСЧ подобно [8, 9] оказывается возможным построение генератора только для узкого класса неприводимых примитивных характеристических многочленов, имеющих вид $\varphi(x) = 1 + x^j + x^m$.

В данной работе описывается методика синтеза генератора рандомизированных псевдослучайных чисел, отличающегося рядом весьма значительных достоинств.

Работа генератора псевдослучайных чисел для произвольного m при любых значениях коэффициентов $\alpha_i \in \{0, 1\}$, $i = 1, m$, определяющих топологию связей многовходового сумматора по модулю два включенному в цепь обратной связи регистра сдвига, описывается системой уравнений (2)

$$a_1(k+1) = \sum_{i=1}^{m}{}^{\oplus} \alpha_i a_i(k), \tag{2}$$

$$a_i(k+1) = a_{i-1}(k), \quad i = 2, 3, 4, \ldots, m,$$

где знак $\sum^{\oplus}$ означает операцию суммирования по модулю два. Применив методику описанную в [5] на основании (2) получим систему

$$a_m(k+1) = \sum_{i=1}^{m}{}^{\oplus} \alpha_i a_i(k), \tag{3}$$

$$a_{m-i}(k+1) = \sum_{n=1}^{i}{}^{\oplus} \alpha_i a_{m+n-i}(k+1) \oplus \sum_{n=i+1}^{m}{}^{\oplus} \alpha_i a_{n-i}(k), \quad i = 1, 2, \ldots, m-1$$

позволяющую получать очередное m-разрядное псевдослучайное число в $k+1$ такт на основании предыдущего m-разрядного числа, полученного в k-ом такте. Анализ уравнений (3) показывает, что подобно (1) и (2) последовательности на выходе устройства, построенного согласно (3), небудут содержать кода $\xi_k = 000\ldots0$. Учитывая то, что m принимает ограниченные небольшие значения, необходимым оказывается обеспечение возможности получения $\xi_k = 000\ldots0$.

Если все 2^m двоичные комбинации входят в циклическую последовательность m разрядных кодов, то такие последовательности называются последовательностями де Брюйна (de Bruijn) или циклами де Брюйна [10]. Очевидно, что использование подобных последовательностей в силу плохих корреляционных свойств в чистом виде нецелесообразно. В тоже время введение рандомизации таких последовательностей позволит получить абсолютную равномерность и независимость [9]. Введение нулевой комбинации в M-последовательность позволит получить подобный цикл, содержащий всевозможные m-разрядные двоичные комбинации. Функционирование устройства, генерирующего на выходе последовательность с периодом 2^m, описывается системой

уравнений

$$a_1(k+1) = \sum_{i=1}^{m}{}^{\oplus} \alpha_i\, a_i(k) \oplus \neg \Big[\bigvee_{p=1}^{m-1} a_p(k)\Big], \tag{4}$$

$$a_i(k+1) = a_{i-1}(k), \quad i = 2, 3, 4, \ldots, m.$$

В отличии от (2) система (4) позволяет получить нулевую комбинацию на m-разрядном регистре.

Используя систему уравнений (1), можно показать зависимость состояния m-го разряда регистра сдвига от значений каждого предыдущего разряда и количества выполненных тактов. Так для $n < m$

$$a_m(k+n) = a_{m-1}(k+n-1) = \ldots = a_{m-i}(k+n-i) = \ldots = a_{m-n}(k)$$

Тогда через $n = m$ тактов согласно (4)

$$a_m(k+m) = a_1(k+1) = \sum_{i=1}^{m}{}^{\oplus} \alpha_i\, a_i(k) \oplus \neg \Big[\bigvee_{p=1}^{m-1} a_p(k)\Big] \tag{5}$$

Подобным образом легко показать, что

(6)

$$a_{m-1}(k+m) = \alpha_1\, a_1(k+1) \oplus \sum_{l=1}^{m-1}{}^{\oplus} \alpha_{l+1}\, a_l(k) \oplus \neg\{a_1(k+1) \bigvee_{l=2}^{m-1} \Big[\bigvee a_l(k+1)\Big]\} =$$

$$= \alpha_1\, a_m(k+m) \oplus \sum_{l=1}^{m-1}{}^{\oplus} \alpha_{l+1}\, a_l(k) \oplus \neg\{a_m(k+m) \bigvee \Big[\bigvee_{l=1}^{m-2} a_l(k)\Big]\}$$

а для $a_{m-2}(k+m)$ получим

$$a_{m-2}(k+m) = \alpha_1\, a_{m-1}(k+m) \oplus \alpha_2\, a_m(k+m) \oplus \sum_{l=1}^{m-2}{}^{\oplus} \alpha_{l+2}\, a_l(k) \oplus \tag{7}$$

$$\oplus \neg\{a_m(k+m) \oplus a_{m-1}(k+m) \bigvee \Big[\bigvee_{l=1}^{m-3} a_l(k)\Big]\}$$

Обобщая (6) и (7) для $i = 1, 2, \ldots, m-2$ будем иметь

$$a_{m-i}(k+m) = \sum_{g=1}^{i}{}^{\oplus} \alpha_{i+1-g}\, a_{m+1-g}(k+m) \oplus \sum_{l=1}^{m-i}{}^{\oplus} \alpha_{l+i}\, a_l(k) \oplus \tag{8}$$

$$\oplus \{\Big[\bigvee_{l=1}^{m-i-1} a_l(k)\Big] \bigvee \Big[\bigvee_{p=1}^{i} a_{m+1-p}(k+m)\Big]$$

При $i = m-1$ для $a_{m-i}(k+m)$ получим

$$a_{m-m+1}(k+m) = a_1(k+m) = \sum_{g=1}^{m-1}{}^{\oplus} \alpha_{m-g}\, a_{m+1-g}(k+m) \oplus \alpha_m\, a_1(k) \oplus \tag{9}$$

$$\oplus \neg \Big[\bigvee_{l=1}^{m-1} a_{m+1-l}(k+m)\Big].$$

Окончательно система уравнений, на основании которой получаются последовательности m-разрядных кодов включающих и нулевой код, имеет вид

$$(10)\qquad a_m(k+1) = \sum_{l=1}^{m}{}^{\oplus}\, \alpha_l\, a_l(k) \oplus \neg\Big[\bigvee_{p=1}^{m-1} a_p(k)\Big];$$

$$a_{m-i}(k+1) = \sum_{g=1}^{i}{}^{\oplus}\, \alpha_{i+1-g}\, a_{m+1-g}(k+1) \oplus \sum_{l=1}^{m-i}{}^{\oplus}\, \alpha_{l+i}\, a_l(k) \oplus$$

$$\oplus \neg\Big\{\Big[\bigvee_{l=1}^{m-i-1} a_l(k)\Big] \vee \Big[\bigvee_{l=1}^{i} a_{m+1-l}(k+1)\Big]\Big\};$$

$$a_1(k+1) = \sum_{l=1}^{m-1}{}^{\oplus}\, \alpha_{m-l}\, a_{m+1-l}(k+1) \oplus \alpha_m\, a_1(k) \oplus \neg\Big[\bigvee_{l=1}^{m-1} a_{m+1-l}(k+1)\Big].$$

Структурная схема генератора рандомизированных псевдослучайных чисел,

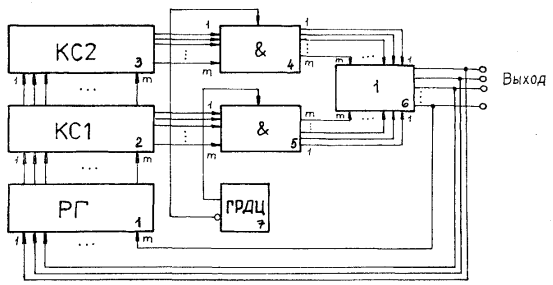

Рис. 2.

построенного с использованием системы уравнений (10), приведена на рис. 2. Блок 1 представляет собой регистр с установочными входами на который записывается последующий код по приходу тактирующего импульса. *КС*1 и *КС*2 построены согласно системы уравнений (10) и представляют собой комбинационные схемы на выходах которых формируются коды разрядов m-разрядных чисел $a_{m-i}(k+1)$, $i = 0, 1, \ldots, m-1$ и $a_{m-i}(k+2)$, $i = 0, 1, \ldots, m-1$ соотвественно. В зависимости от значения равновероятной двоичной цифры, получаемой на выходе блока 7 через m элементов *И* блока 4 или 5 и далее через блок m элементов *ИЛИ* 6, код числа $a_{m-i}(k+1)$ или числа $a_{m-i}(k+2)$ записывается на регистр 1. Блок 7 представляет собой генератор равновероятной двоичной цифры $x(k)$, построенный по простейшей схеме, где $\mathrm{P}[x(k) = 1] \approx 0{,}5$.

Последовательность состояний генератора рис. 2 представляет собой цепь Маркова. Полное вероятностное описание данной цепи Маркова достигаестся заданием матрицы **A** одношаговых вероятностей π_{ik} дважды стохастической

матрицы, определяющей работу структуры (рис. 2) на n-ом такте [11]. Для некоррелированной последовательности $x(k)$ для рассмотренного случая матрица примет следующий вид

$$\mathbf{A} = \begin{Vmatrix} 0 & p & (1-p) & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & p & (1-p) & \dots & 0 & 0 & 0 \\ . & . & . & . & \dots & . & . & . \\ 0 & 0 & 0 & 0 & \dots & 0 & p & (1-p) \\ (1-p) & 0 & 0 & 0 & \dots & 0 & 0 & p \\ p & (1-p) & 0 & 0 & \dots & 0 & 0 & 0 \end{Vmatrix} \tag{11}$$

В общем случае вероятность p_k-вероятность нахождения устройства в k-ом состоянии, если оно существует, находится в результате предельного перехода

$$p_k = \lim p_k(n), \quad k = 1, 2, \dots, 2^m$$

и называются финальными вероятностями. Финальные вероятности должны удовлетворять системе 2^m линейных алгебраических уравнений

$$p_k = \sum_{i=1}^{2^m} p_i \pi_{ik}, \quad k = 1, 2, \dots, 2^m \tag{12}$$

и дополнительному условию (12)

$$\sum_{k=1}^{2^m} p_k = 1, \quad p_k \geqq 0, \tag{13}$$

где π_{ij} определяются из (11). Так как 2^m уравнений (12) являются линейно зависимыми, по этому 2^m финальных вероятностей определим из $(2^m - 1)$ уравнений (12) и уравнения (13), Очевидным решением системы будет $p_k = (\frac{1}{2})^m$, $k = 1, 2, \dots, 2^m$. То есть вероятность появления любого кода на выходе генератора, приведенного на рис. 2, одинакова и равняется $(\frac{1}{2})^m$.

Преимущества генератора рандомизированных псевдослучайных чисел заключается в следующем. Природа выходных псевдослучайных чисел максимально приближена к истинно случайным числам. В данном устройстве, подобно как и в [9], нарушено жесткое условие, что после определенного ξ_i должно следовать ξ_{i+1} заранее точно известное, так как ξ_{i+1} может принимать равновероятно одно из двух значений. Так как состояние блока 7 случайно, то и порядок следования кодов M-последовательности, включающей нулевую комбинацию, будет абсолютно случайным, причем выходным значением устройства с равной вероятностью может быть любой m-разрядный код. Отсутствие запрещенных кодов в последовательности позволяет повысить надежность устройства.

При практической реализации генератора рандомизированных псевдослучайных чисел оказывается возможным построение такого генератора для любого неприводимого примитивного характеристического многочлена. Кроме того

для конкретного значения m в силу многообразия многочленов, позволяющих генерировать M-последовательность [1], возможно построение подобных устройств с одинаковой разрядностью выходных кодов равной m, что существенно расширяет его функциональные возможности.

Применение подобного генератора рандомизированных псевдослучайных чисел, отличающегося широкими функциональными возможностями, высокой надежностью функционирования и стабильностью его вероятностных характеристик, позволит повысит качество псевдослучайных последовательностей, а тем самым точность и достоверность решения задач методом Монте-Карло.

(Поступила в редакцию 1 июля 1981 г.)

ЛИТЕРАТУРА

[1] В. В. Яковлев, Р. Ф. Федоров: Вероятностные вычислительные машины. Машиностроение, Ленинград 1974.

[2] А. Е. Леусенко, А. А. Петровский, В. Н. Ярмолик: Цифровые методы и устройства для формирования и анализа вибропроцессов. Измерительная техника (1980), 10.

[3] М. С. Бернштейн, А. М. Романкевич: Метод статистического контроля логических схем. Кибернетика (1974), 1, 58—62.

[4] R. David: Testing by Feedback Shift Register. IEEE Trans. Com. *C-29* (1980), 7, 668—673.

[5] В. Н. Ярмолик, А. Н. Морозевич: Об одном подходе к синтезу параллельных ГПСЧ на регистре сдвига. Сб. „Радиотехника и электроника" (1977), 7, 66—69. Вышэйшая школа, Минск 1977.

[6] М. С. Бернштейн, Л. Ф. Карачун, А. М. Романкевич, А. М. Руккас: Генератор псевдослучайных последовательностей испытательных сигналов — В сб. „Механизация и автоматизация управления" (1978), 1, 57—60.

[7] Дж. Макуильямс, Н. Дж. Слоан: Псевдослучайные последовательности и таблицы. ТИЭР *64* (1976). 12.

[8] Б. Ф. Кирьянов и др.: Формирование случайных последовательностей при физическом моделировании дискретных каналов. Сб. „Кодирование и передача дискретных сообщений в системах связи", Наука, Москва 1976.

[9] В. Н. Ярмолик, А. Н. Морозевич: Генератор псевдо случайных чисел. Авторское свидетельство СССР № 708381 БИ № *1* 1980 г.

[10] H. Fredricksen: A Class of Nonlinear de Bruijn Cycles. J. Combin. Theory Ser. A *19* (1975), 192—199.

[11] А. Т. Баруча-Рид: Элементы теории марковских процессов и их приложения. Наука, Москва 1969.

[12] Я. Гавел: Генератор случайного процесса ГЕНАП-3. Автоматика и телемеханика (1975), 3, 171—175.

Ing. Jan Havel, DrSc, Ústav teorie informace a automatizace ČSAV (Институт теории информации и автоматизации ЧСАН), Pod vodárenskou věží 4, 182 08 Praha 8. ЧССР.

Морозевич Анатолий Николаевич, к.т.н., доцент, Ярмолик Вячеслав Николаевич, к.т.н., Минский радиотехнический институт, кафедра электронных вычислительных машин, 220069 Минск, ул. Подлесная 6. СССР.