УДК 681.326; 531.19

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ТРЁХЗНАЧНОЙ ЛОГИКИ

Е. Л. Столов

Казанский федеральный университет, г. Казань, Россия

E-mail: yevgeni.stolov@ksu.ru

Предложена математическая модель физического генератора случайных чисел, реализованного в виде кольцевого соединения комбинационных схем, работающих в трёхзначной логике. Доказана равномерность распределения сигнала, снимаемого с любого выхода.

Ключевые слова: *асинхронный генератор, трёхзначная логика, марковский процесс.*

Введение

Увеличение производительности цифровых устройств является одной из основных задач современной схемотехники. Достигнутая тактовая частота уже близка к предельной, распараллеливание пригодно не для любой задачи. В этой связи внимание исследователей снова обращается к схемам, использующим трёхзначную логику. В последнее время созданы элементарные физические устройства, реализующие указанную логику (см., например, работу [1]), где говорится о разработке технологии, позволяющей реализовать произвольную комбинационную схему, работающую в троичной логике. Физические генераторы случайных последовательностей дают примеры устройств, применение в которых k-значных логик позволяет увеличить их производительность, поскольку в любой момент времени снимаемый сигнал имеет большую длину по сравнению с аналогичной схемой, работающей в двоичной логике. Упомянутые генераторы используются для создания криптографических ключей. В работах [2, 3] рассмотрен цифровой стохастический генератор бинарных последовательностей, составленный из сумматоров по модулю 2 с обратными связями. В предлагаемой работе рассматриваются аналогичные устройства, только вместо сумматора используются блоки с двумя входами и одним выходом, реализующие комбинационную схему, работающую в трёхзначной логике. Пример подобного генератора представлен на рис. 1. Здесь символом F обозначен упомянутый блок, а сигнал снимается с выхода любого из блоков.

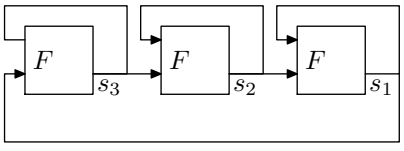

Рис. 1. Пример генератора тернарных последовательностей

При создании указанных генераторов возникают следующие проблемы:

1) возможность перехода генератора в стационарное состояние;
2) доказательство независимости сгенерированных символов.

После перехода генератора в стационарное состояние снимаемый с его выхода сигнал не меняется во времени. Ниже показано, что при надлежащем выборе блока F генератор не имеет стационарных состояний. Что касается независимости символов генерируемой последовательности, то о ней можно говорить лишь после того, как будут выбраны математическая модель функционирования отдельных блоков и способ их соединения. Кроме того, потребуем равномерности распределения выходного сигнала на выходе блока. Это требование является естественным, поскольку появляется возможность преобразования выходного сигнала в сигнал с произвольным распределением.

1. Математическая модель генератора

Общий подход к исследованию генератора, составленного из нелинейных блоков, представлен в работе [4], однако применение трёхзначной логики вносит некоторые упрощения в описание ситуации. Каждый из блоков реализует некоторую функцию $c = F(a, b)$, $a, b, c \in \{0, 1, 2\}$. При изменении входных сигналов блок срабатывает, реализуя функцию F. Относительно срабатывания блоков сделаны следующие предположения:

1) время срабатывания блока является случайной величиной с экспоненциальным распределением, то есть вероятность того, что после поступления изменённого сигнала на вход блока время изменения сигнала на выходе меньше T, равна $1 - \exp(-T)$;
2) срабатывания отдельных блоков являются независимыми событиями, причём никакие два блока не могут сработать одновременно.

Определение 1. Перенумеруем блоки генератора. Состоянием генератора в момент времени t называется вектор $\mathbf{s}(t)$, компонента которого $\mathbf{s}(t)[k], k = 1, \ldots, N$ есть сигнал на выходе блока с номером k в момент времени t.

В дальнейшем будем пользоваться векторным обозначением состояния в форме

$$\mathbf{s} = \langle s_1, s_2, \ldots, s_N \rangle.$$

Если генератор содержит N блоков, то число его состояний $M = 3^N$. Соединения блоков друг с другом задаются списком Con. Элемент списка $Con[k] = [i_k, j_k]$, где i_k, j_k — номера блоков, с выходов которых сигналы поступают на вход блока с номером k. Например, структура генератора, представленного на рис. 1, задается списком $Con = ([1, 2]; [2, 3]; [3, 1])$.

Наложенные ограничения аналогичны предположениям, накладываемым на системы массового обслуживания, благодаря чему функционирование генератора описывается уравнениями Эрланга [5]. Выпишем систему дифференциальных уравнений Эрланга, описывающих динамику генератора. Перенумеруем все состояния генератора числами от 1 до M. Пусть $\mathbf{s}_n$ — состояние с номером n, а $P_n(t)$ — вероятность того, что в момент времени t генератор находится в состоянии $\mathbf{s}_n$. Обозначим через $i_1, i_2, \ldots, i_m$ все номера состояний, свои для каждого n, из которых можно попасть в состояние $\mathbf{s}_n$ в результате срабатывания только одного блока. Вероятность того, что через момент Δt генератор окажется в состоянии $\mathbf{s}_n$, складывается из вероятности того, что генератор находился в этом состоянии прежде и ни один из N блоков не сработал, и из вероятностей перейти в состояние $\mathbf{s}_n$ из одного из состояний с номерами $i_1, i_2, \ldots, i_m$ в результате срабатывания только одного блока. Имеем

$$\frac{dP_n(t)}{dt} = -NP_n(t) + \sum_{k=1}^{m} P_{i_k}(t). \tag{1}$$

2. Выбор функции F и способа соединения блоков

При выводе уравнения (1) не делалось никаких предположений о виде функции F и способе соединения блоков между собой. Как отмечалось выше, нужно гарантировать отсутствие стационарных состояний генератора. Предположим, что функция F обладает следующим свойством:

$$c = F(a, b), \quad \forall a, b \quad (c \neq a, c \neq b). \tag{2}$$

Из условия (2) следует, что при срабатывании любого блока состояние генератора изменится при любом соединении блоков между собой. Таким образом, данное условие исключает наличие стационарных состояний. Перечислим все функции, обладающие свойством (2). Значение $F(a, b)$ определено однозначно, если $a \neq b$, поэтому $F(a, b) = F(b, a)$. Это означает, что достаточно определить функцию лишь для совпадающих аргументов. Если σ — произвольная перестановка чисел $0, 1, 2$, то функции $F(a, b)$ и $\sigma(F(\sigma(a), \sigma(b))$ будем считать неразличимыми. Отсюда следует, что существуют лишь две существенно разные функции, обладающие свойством (2):

	$F(0,0)$	$F(1,1)$	$F(2,2)$
F_1	1	2	0
F_2	1	2	1

Изучаемый генератор предназначен для генерации последовательностей, в которых каждый из элементов появляется с одной и той же вероятностью. В этой связи далее в качестве функции F будем использовать только F_1.

Остановимся на выборе соединения блоков друг с другом. Рассмотрим соединение, определенное списком $Con = ([1, 2], [2, 3], \ldots, [N - 1, N], [N, 1])$. На рис. 1 представлен указанный вид соединения для $N = 3$. Достоинством указанной схемы является равноправность всех выходов блоков и одинаковая электрическая нагрузка на выходе каждого блока. Далее показано, что схема обладает свойством «забывания» начального состояния, поэтому в силу отмеченной симметрии на выходе любого блока при снятии сигнала через достаточно большой интервал времени T_0 генерируется тернарная последовательность, в которой каждый символ появляется с одной и той же вероятностью.

3. Матрица переходов генератора

Обозначим через A матрицу размера $M \times M$ переходов генератора. Эта матрица состоит из нулей и единиц, причём $A[i, k] = 1$ тогда и только тогда, когда при срабатывании какого-либо блока генератор переходит из состояния с номером i в состояние с номером k. Изучим особенности матрицы переходов исследуемого генератора. Рассмотрим произвольное состояние

$$\mathbf{s} = \langle s_1, \ldots, s_k, \ldots, s_N \rangle. \tag{3}$$

В силу свойства (2) в результате срабатывания любого из N блоков состояние генератора изменится, причем все получившиеся состояния будут разными. Это означает, что каждая строка матрицы A имеет ровно N единиц.

Утверждение 1. Состояния (3), в которых все сигналы равны между собой, при указанных выборе функции F и способе соединения блоков недостижимы из других состояний генератора.

Доказательство. Рассмотрим состояние $\mathbf{s_0} = \langle 0, \ldots, 0\rangle$. Если из некоторого состояния $\mathbf{s_1}$ возможен переход в состояние $\mathbf{s_0}$ в результате срабатывания одного блока, то все компоненты вектора $\mathbf{s_1}$, кроме одной, равны 0. Легко видеть, что после срабатывания любого блока, в силу (2), переход в состояние $\mathbf{s_0}$ невозможен. Поскольку в рассматриваемой схеме все троичные значения равноправны, аналогичные утверждения справедливы для векторов $\langle 1, \ldots, 1\rangle$ и $\langle 2, \ldots, 2\rangle$. ■

Из доказанного утверждения следует, что столбцы с номерами, отвечающими трем недостижимым состояниям, являются нулевыми. Удалим из A эти три столбца и три столбца с теми же номерами и обозначим через A' получившуюся матрицу.

Напомним некоторые известные факты из теории матриц.

Определение 2 [6]. Матрица B с неотрицательными элементами называется разложимой, если существует матрица перестановки P, такая, что

$$P^{\mathrm{T}} \cdot B \cdot P = \begin{pmatrix} B_{11} & 0 \\ B_{21} & B_{22} \end{pmatrix}.$$

В противном случае матрица называется неразложимой.

Согласно [6, с. 166–168], неотрицательная матрица B неразложима тогда и только тогда, когда для любой пары индексов i, j существует натуральное число k, такое, что $B^k[i, j] > 0$. Кроме того, наибольшее характеристическое число r неразложимой матрицы является простым корнем характеристического многочлена этой матрицы.

Свойства генерируемой последовательности базируются на следующей теореме.

Теорема 1. Матрица A' является неразложимой.

Доказательство. Под множеством состояний будем понимать множество всех состояний генератора, кроме трёх отмеченных недостижимых состояний. Достаточно доказать, что из любого состояния можно перейти в любое другое. Пусть $\mathbf{s_1} = \langle 1, 0, \ldots, 0\rangle$. Покажем, что из $\mathbf{s_1}$ можно перейти в любое другое состояние. После двукратного срабатывания второго блока генератор перейдет в состояние $\langle 1, 1, 0, \ldots, 0\rangle$, а затем — в состояние $\langle 1, 2, 0, \ldots, 0\rangle$. Итак, из $\mathbf{s_1}$ можно перейти в состояние $\langle 1, a, 0, \ldots, 0\rangle$, где a — любой элемент множества $L = \{0, 1, 2\}$. При срабатывании первого блока переходим из состояния $\mathbf{s_1}$ в состояние $\langle 2, 0, 0, \ldots, 0\rangle$. После этого, как и выше, доказывается, что достигается любое состояние $\langle 2, a, 0, \ldots, 0\rangle$, где $a \in L$. Предположим, что уже доказана достижимость из состояния $\mathbf{s_1}$ любого состояния вида $\langle 1, a_2, a_3, \ldots, a_k, 0, \ldots, 0\rangle$ или $\langle 2, a_2, a_3, \ldots, a_k, 0, \ldots, 0\rangle$, где $a_2, a_2, \ldots, a_k$ — любые элементы множества L. Если $k < N-1$, то при срабатывании блока с номером $k+1$ из состояния $\langle 1, a_2, a_3, \ldots, a_k, 0, 0, \ldots, 0\rangle$ переходим в состояние $\langle 1, a_2, a_3, \ldots, a_k, 1, 0, \ldots, 0\rangle$, а затем — в $\langle 1, a_2, a_3, \ldots, a_k, 2, 0, \ldots, 0\rangle$. Если $k = N-1$, то при срабатывании блока с номером N из состояния $\langle 1, a_2, a_3, \ldots, a_k, 0\rangle$ переходим в состояние $\langle 1, a_2, a_3, \ldots, a_k, 2\rangle$, а из состояния $\langle 2, a_3, \ldots, a_k, 0\rangle$ — в $\langle 2, a_2, a_3, \ldots, a_k, 1\rangle$. После срабатывания первого блока переходим в состояние $\langle 2, 0, a_3, \ldots, a_k, 0\rangle$ и после срабатывания блока с номером N — в состояние $\langle 2, 0, a_3, \ldots, a_k, 1\rangle$. Наконец, покажем достижимость состояния вида $\langle 1, \ldots, 1, b_p, \ldots, b_{N-1}, 1\rangle$, где $b_p \neq 1$. Согласно предположению, достижимо состояние $\langle 2, 0, \ldots, 0, b_p, \ldots, b_{N-1}, 1\rangle$. После последовательного срабатывания блоков с номерами $1, 2, \ldots, p-1$ получим состояние $\langle 1, \ldots, 1, b_p, \ldots, b_{N-1}, 1\rangle$, поскольку $b_p = 0$ или $b_p = 2$.

Теперь покажем, что из любого состояния $\mathbf{s}$ можно перейти в состояние $\mathbf{s_1}$. При срабатывании первого блока происходит переход из состояния $\langle 0, a_2, \ldots, a_N\rangle$ в со-

стояние $\langle b, a_2, \ldots, a_N\rangle$, где $b = 1$ или $b = 2$. Это означает, что можем ограничиться состояниями, начинающимися с 1 или 2. Из состояния $\langle 1, 0, \ldots, 0, 1\rangle$ после двукратного срабатывания блока с номером N получаем состояния $\langle 1, 0, \ldots, 0, 2\rangle$, $\langle 1, 0, \ldots, 0, 0\rangle$. Из состояния $\langle 2, 0, \ldots, 0, 0\rangle$ после срабатывания блока с номером N получается состояние $\langle 2, 0, \ldots, 0, 1\rangle$, а после срабатывания первого блока — $\langle 1, 0, \ldots, 0, 1\rangle$. Из состояния $\langle 2, 0, \ldots, 0, 2\rangle$ после срабатывания блока с номером N получается состояние $\langle 2, 0, \ldots, 0, 0\rangle$. Это означает, что состояние $\mathbf{s_1}$ достижимо из состояний вида $\langle 1, 0, \ldots, 0, a\rangle$, $\langle 2, 0, \ldots, 0, a\rangle$ для любых $a \in L$. Пусть уже доказана достижимость $\mathbf{s_1}$ из состояний вида $\langle 1, 0, \ldots, 0, b_p, \ldots, b_N\rangle$ для любых $b_i \in L$. Рассмотрим произвольное состояние вида $\langle 1, 0, \ldots, 0, b_{p-1}, b_p, \ldots, b_N\rangle$, $b_{p-1} \neq 0$. Возможны следующие наборы значений b_{p-1}, b_p : (1,2), (2,1), (2,2), когда после срабатывания блока с номером $p-1$ получаем 0 в позиции $p-1$; (1,1), когда после двукратного срабатывания блока с номером $p-1$ получаем 0 в позиции $p-1$; (2,0), (1,0) — последняя ситуация требует дополнительного рассмотрения. Рассмотрим состояние $\langle 1, 0, \ldots, 0, 1, 0, b_{p+1}, \ldots, b_N\rangle$. При срабатывании блока с номером p в этой позиции появится 1 или 2, что сводит эту ситуацию к предыдущему случаю. Для завершения доказательства достаточно поменять местами значения 1 и 2. ■

4. Статистические свойства генерируемой последовательности

Введем обозначение $B = A^{\mathrm{T}}$. Согласно определению матрицы A, каждая строка матрицы B с номером i содержит 1 в позиции j тогда и только тогда, когда возможен переход из состояния с номером j в состояние с номером i в результате срабатывания одного блока. Рассмотрим более подробно систему уравнений (1). Положим $\mathbf{p}(t) = (P_1(t), \ldots, P_M(t))$. Указанная система может быть переписана в виде

$$\frac{d\mathbf{p}(t)}{dt} = (B - N \cdot I)\mathbf{p}(t) = D\mathbf{p}(t). \tag{4}$$

Решение данной системы имеет вид

$$\mathbf{p}(t) = \exp(Dt)\mathbf{e},$$

где $\mathbf{e}$ — произвольный стохастический вектор, определяющий начальное состояние. Матрица B имеет три нулевых строки; пусть это строки с номерами 1, 2, 3. Из (4) следует, что

$$P_k(t) = e_k \exp(-Nt), \quad k \in \{1, 2, 3\}, \tag{5}$$

где $0 \leqslant e_k \leqslant 1$. Отсюда вытекает, что $P_k(t) \to 0$ при $t \to \infty$, $k \in \{1, 2, 3\}$. Исключим из векторов компоненты с индексами 1, 2, 3, а из матриц — строки и столбцы с этими номерами. В результате получим векторы $\mathbf{e}'$, $\mathbf{p}'(t)$, $D' = A'^{\mathrm{T}} - N \cdot I'$, а решение системы (4) сведется к решению системы

$$\mathbf{p}'(t) = \exp(D't)\mathbf{e}'.$$

Теорема 2. Пусть $C(t) = \exp(Dt)$. Тогда $C(t) \to C_0$ при $t \to \infty$, где C_0 — матрица с одинаковыми столбцами, равными стохастическому вектору $\mathbf{d}$, такому, что $\mathbf{d} = (0, 0, 0, \mathbf{d}')^{\mathrm{T}}$, $A'^{\mathrm{T}}\mathbf{d}' = N\mathbf{d}'$.

Доказательство. Из (5) вытекает, что первые три строки матрицы C_0 нулевые. Сумма элементов в каждой строке матрицы A равна N, и при выбранной нумерации состояний её первые три столбца нулевые. Таким образом, матрица A'/N

стохастическая, её максимальное характеристическое число равно 1, все остальные характеристические числа имеют модули, не превосходящие 1 (см. [6, с. 200]), а из неразложимости этой матрицы вытекает, что 1 является простым корнем. Другими словами, если $\xi_1, \ldots, \xi_{M-3}$ — все характеристические числа матрицы A' и ξ_1 — максимальный по модулю корень, то $\xi_1 = N$, $|\xi_i| \leqslant N, i > 1$. По определению $D' = A'^{\mathrm{T}} - N \cdot I'$, поэтому для характеристических чисел μ_j этой матрицы выполнены условия $\mu_1 = 0$, $\mathrm{real}(\mu_i) < 0$, $i = 2, \ldots, M-3$. Характеристические числа матрицы $C'(t) = \exp(D't)$ равны $\exp(\mu_i t)$, поэтому существует предел $C'_0 = \lim\limits_{t\to\infty} C'(t)$ и матрица C'_0 имеет ранг 1. Если $A'^{\mathrm{T}}\mathbf{d}' = N\mathbf{d}'$, то $D'\mathbf{d}'$ — нулевой вектор, а из представления матрицы $C'(t)$ в виде ряда вытекает, что $C'(t)\mathbf{d}' = \mathbf{d}'$ для любого t. Это означает, что $C'_0\mathbf{d}' = \mathbf{d}'$. Далее, $(1, 1, \ldots, 1)A'^{\mathrm{T}} = N(1, 1, \ldots, 1)$, поэтому $(1, 1, \ldots, 1)D'$ — нулевой вектор и $(1, 1, \ldots, 1)C'_0 = (1, 1, \ldots, 1)$, т. е. сумма элементов в каждом столбце этой матрицы равна 1. ■

Вектор $\mathbf{d}'$ задает финальное распределение вероятностей состояний генератора. Из теоремы 2 следует независимость этого распределения от начального состояния, а финальные вероятности появления 0, 1 и 2 на выходе любого блока равны $1/3$. Следует, однако, заметить, что отсюда нельзя заключить, что финальные вероятности каждого из состояний генератора совпадают между собой.

5. Результаты численных экспериментов

При практическом использовании разработанного генератора возникает вопрос о скорости сходимости решения уравнения (4) к финальному вектору в зависимости от числа N блоков в схеме. В качестве меры близости выбрано среднеквадратическое отклонение δ финального вектора — собственного вектора матрицы D, отвечающего собственному значению 0, — от первого столбца матрицы $\exp(Dt)$. Результаты экспериментов представлены в следующей таблице.

Зависимость δ от N и t

$N\backslash t$	2	4	6	8	10
2	0,0095249	0,0001857	0,0000034	6,288e−08	1,141e−09
3	0,0026750	0,0000398	0,0000005	7,596e−09	1,102e−10
4	0,0014727	0,0000404	0,0000011	3,592e−08	1,113e−09
5	0,0004785	0,0000077	8,981e−08	9,856e−10	3,056e−11
6	0,0001991	0,0000055	0,0000002	6,546e−09	2,868e−10

Из приведённых результатов следует, что при любом N схема практически забывает своё начальное состояние при $t \geqslant 5$. Расчёт проведён для параметра экспоненциального распределения $\lambda = 1$.

Заключение

Рассмотренный в работе физический генератор, составленный из одинаковых блоков, реализующих специальную функцию трёхзначной логики, может использоваться для генерации случайных ключей. Генерация возникает за счёт наличия обратных связей и случайности времени срабатывания. Если время срабатывания блока определяется экспоненциальным распределением, то при одном и том же значении параметра распределения трёхзначный генератор обеспечивает большую производительность по сравнению с бинарной схемой, работающей в том же режиме. Выбранный способ соединения блоков обеспечивает одинаковую электрическую нагрузку на выходах всех устройств. Использование более чем трёх блоков не уменьшает время «забывания» начального состояния генератора.

ЛИТЕРАТУРА

1. *Sheng L., Yong-Bin K., and Lombardi F.* CNTFET-Based Design of Ternary Logic Gates and Arithmetic Circuits //IEEE Trans. Nanotechnology. 2011. V. 10. No. 2. P. 217–225.
2. *Кузнецов В. М., Песошин В. А., Столов Е. Л.* Марковская модель цифрового стохастического генератора //АиТ. 2008. № 9. С. 62–68.
3. *Кузнецов В. М., Песошин В. А., Столов Е. Л.* Стабильные состояния асинхронного генератора //Учёные записки Казанского государственного университета. 2010. Т. 152. Кн. 1. Сер. Физико-математические науки. С. 174–180.
4. *Столов Е. Л.* Генератор случайных чисел, составленный из нелинейных асинхронных элементов // Исследования по прикладной математике. Вып. 26. Казань: Институт информатики КГУ, 2006. С. 101–106.
5. *Хинчин А. Я.* Работы по математической теории массового обслуживания. М.: Физматгиз, 1963. 236 с.
6. *Маркус М., Минк Х.* Обзор по теории матриц и матричных неравенств. М.: Наука, 1972. 232 с.