УДК 681.326

В.В. ГРОЛЬ, В.А. РОМАНКЕВИЧ, Е.Р. ПОТАПОВА, МОРАВЕДЖ СЕЙЕД МИЛАД

Национальный технический университет Украины «КПИ», Украина

СТРУКТУРНЫЙ МЕТОД ГЕНЕРАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СПЕЦИАЛЬНОГО ВИДА

Предложен структурный метод формирования управляемых псевдослучайных последовательностей специального вида, характеризующийся использованием средств генерации псевдослучайных последовательностей, построенных по классической схеме, за счет чего получена возможность значительного повышения производительности процедур формирования последовательностей выходных наборов. Рассмотрены особенности схемотехнической реализации основных узлов формирователя. Приведены количественные оценки и примеры расчета основных параметров предложенного генератора.

Ключевые слова: *псевдослучайная последовательность, сдвиговый регистр, линейная обратная связь, двоичные наборы постоянного веса.*

Введение

Важность решения задачи формирования псевдослучайных (ПС) последовательностей с различными параметрами обусловила разработку широкого класса специализированных цифровых схем, устройств и систем для получения таких последовательностей. Так в работе [1] рассматриваются схемы генерации цифровых сигналов с изменяемой вероятностью переключения битов в последовательности. В работе [2] предложены структурные решения для получения последовательностей, обладающих свойствами «глубины», то есть получения подпоследовательностей соседних наборов с полным перебором всех возможных состояний этих наборов. В работе [3] предлагается схема формирователя ПС-последовательностей равновесных наборов (наборов вида (k, N), k – вес набора, N – его разрядность). Недостатком некоторых из известных структур является фиксированная на уровне 0.5 вероятность единичного (нулевого) состояния сигналов на выходах. Кроме того, структура, рассматриваемая в работе [2], характеризуется наличием в подпоследовательностях повторяющихся (но не являющихся избыточными) наборов. К недостаткам схемы [3] следует отнести весьма низкое быстродействие, обусловленное наличием цепи последовательного переноса при управляемом сдвиге данных.

Особенности сфер практического применения рассматриваемых структурных методов и средств формирования ПС-последовательностей специального вида обуславливают ряд требований к параметрам таких формирователей. Например, в процессе моделирования поведения отказоустойчивых многопроцессорных систем (ОМС) в потоке отказов необходимо обеспечить возможность формирования признаков отказов компонентов системы заданной (произвольной) кратности с высокой производительностью. Повышенные требования к тактовой частоте работы схемы таких формирователей выдвигаются и в системах диагностирования сложных цифровых устройств в случае необходимости тестирования на рабочих частотах объектов контроля. При контроле схем оперативной памяти целесообразным может оказаться разработка специализированной аппаратуры для высокопроизводительной генерации тестовых последовательностей, обеспечивающих проверку взаимного влияния некоторых подмножеств ячеек памяти.

С учетом вышесказанного можно сформировать задачу разработки метода и его структурной реализации, направленных на получение с высокой производительностью ПС-последовательностей N-битных двоичных наборов, каждый из которых имеет равное число единиц $1 \le k < N$, причем любая подпоследовательность из k соседних наборов не содержит повторяющихся двоичных векторов.

1. Метод генерации и его структурная реализация

При рассмотрении сути метода, положенного в основу построения формирователя ПС-последовательностей специального вида примем следующие допущения. Если N – разрядность выходного вектора (эта величина может соответствовать, например, числу компонентов (процессорных элементов) моделируемой ОМС), k = 1, 2, 3, …, N – 1 – вес выходного набора (например, соответствует числу неисправных модулей ОМС, т.е. кратности отказов в системе), тогда искомая ПС-последовательность специального вида может быть описана соотношением:

$$S = V_1, V_2, V_3, \ldots, V_{i-1}, V_i, V_{i+1}, \ldots, \qquad (1)$$

где V_i – выходной вектор с номером i, разрядность n компонентов V_i $n = \log_2 N$, причем

$$\forall\ i = 1, 2, 3, \ldots, p,\ q = i, i+1, i+2, \ldots,$$

$$i+k-1,\ p \neq q,\ (V_p \neq V_q). \qquad (2)$$

Структурная реализация формирователя, генерирующего последовательность (2), может быть выполнена в соответствии со схемой на рис.1 (схема синхронизации цепи сдвига в регистрах Rg_1 – Rg_k для упрощения не показана). Для выполнения схемой рис. 1 заданных функций необходимо сформировать последовательность S достаточно большого периода (например, величина этого периода должна быть не меньше длительности рабочего цикла формирователя).

Очевидно, что если для получения последовательности S использовать традиционный генератор псевдослучайных чисел (ГПСЧ) [4], для которого $T = 2^m - 1 \geq S$, T – период генератора, m – разрядность сдвигового регистра с линейной обратной связью, m > n, то в этом случае в n–разрядном «окне» такого ГПСЧ будет формироваться последовательность n–битных ($n = \log_2 N$) наборов с периодом T, однако выполнение условия (1) не будет гарантировано, так как в любой подпоследовательности из k соседних (то есть идущих один за другим) наборов могут встретиться и повторяющиеся наборы. Если же реализовать схему на ГПСЧ с $T = 2^n - 1$, то хотя при определенных условиях соотношения (2) и будет выполняться, однако период выходной последовательности будет небольшим, так как при этом $T = 2^n - 1 = N$ тактов

Для преодоления указанного недостатка можно использовать в структуре формирователя два ГПСЧ. Первый (ГПСЧ G_1) предназначен для формирования однобитной последовательности большого периода, который, как указывалось выше, должен, как правило, существенно превышать длительность рабочего цикла формирователя (эта величина может определяться, например, длительностью выполнения моделирования ОМС либо максимальной длиной ПС – теста в системах автоматизированного контроля сложных цифровых объектов).

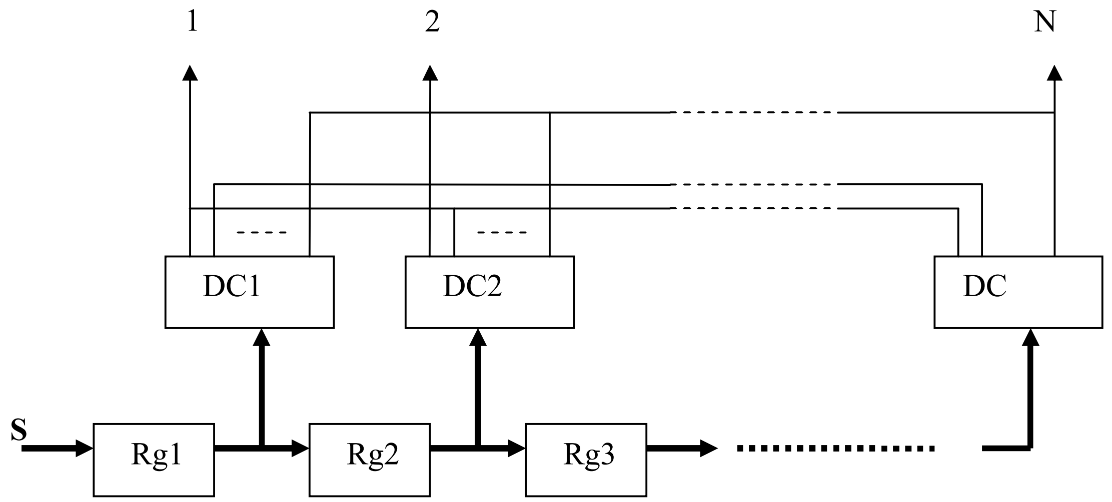

Рис. 1. Выходной узел формирователя

Второй ГПСЧ (G_2) может быть построен на основе сдвигового n–разрядного регистра (напомним, что $n = \log_2 N$) с управляемой цепью линейной обратной связи. Пусть при этом цепь F обратной связи G_2 состоит из двух различных цепей F_1 и F_2, следовательно, генератор G_2 может работать в двух режимах в зависимости от состояния управляющего выхода генератора G_1, а именно:

$$(G_1 = 1) \rightarrow [G_2 = G_2(F_1)], \qquad (3)$$

$$(G_1 = 0) \rightarrow [G_2 = G_2(F_2)], \qquad (4)$$

где G_1 выход (любой из m бит) генератора G_1, G_2 – текущее состояние ГПСЧ G_2, $G_2(F_1(F_2))$ – текущее состояние G_2 при подключенной к регистру генератора цепи линейной обратной связи F_1 или F_2 соответственно.

С учетом вышесказанного структура узла формирования последовательности S может быть представлена на рис. 2.

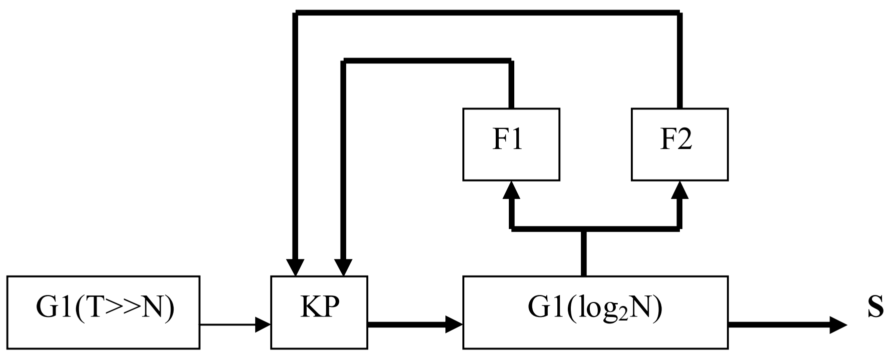

Рис. 2. Формирователь входной ПС – последовательности

Рассмотрим принцип построения цепей обратной связи F_1 и F_2.

Линейная обратная связь F_1 может быть реализована, например, в соответствии с характеристическим полиномом вида $\varphi(x) = 1 + x^i + \ldots + x^j + \ldots + x^n$ [4], где n – разрядность сдвиговою регистра G_1, $n = \log_2 N$.

Пример конкретного варианта G_1 для случая $n = 4$ и $\varphi(x) = 1 + x^3 + x^4$ приведен на рис. 3.

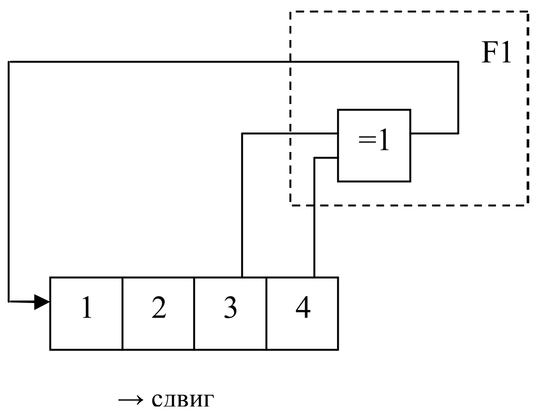

Рис. 3. Пример структуры генератора G1

Что же касается схемотехники цепи F_2, то для её конкретизации можно воспользоваться методикой, предложенной, например, в работе [5], в соответствии с которой записывается последовательность изменения состояний регистра генератора при работе цепи линейной обратной связи согласно выбранному полиному, например, $\varphi(x) = 1 + x^i + x^n$, где $1 \le i < n$. Пусть исходное состояние регистра будет иметь вид: $a_1, a_2, a_3, \ldots a_i, \ldots a_n$, где $a_i \in \{0,1\}$, i – номер соответствующего бита в регистре сдвига генератора. Очевидно, что каждый такт сдвига будет сопровождаться изменением состояния регистра:

1) $a_1 + a_n, a_1, a_2, \ldots a_{n-1}$;
2) $a_{i-1} + a_{n-1}, a_i + a_n, a_1, \ldots a_{n-2}$;
3) $a_{i-2} + a_{n-2}, a_{i-1} + a_{n-1}, a_i + a_n, a_1, \ldots a_{n-3}$.

В последних соотношениях суммирование состояний элементов памяти регистра сдвига осуществляется по модулю два. Рассмотрим табл. 1, в которой представлена последовательность смены состояний генератора (рис. 3).

Таблица 1

Последовательность смены состояний генератора

		a_i			
		a_1	a_2	a_3	a_4
Такт	1	$a_3 + a_4$	a_1	a_2	a_3
	2	$a_2 + a_3$	$a_3 + a_4$	a_1	a_2
	3	$a_1 + a_2$	$a_2 + a_3$	$a_3 + a_4$	a_1
	4	$a_1 + a_3 + a_4$	$a_1 + a_2$	$a_2 + a_3$	$a_3 + a_4$
	5	$a_2 + a_4$	$a_1 + a_3 + a_4$	$a_1 + a_2$	$a_2 + a_3$
	…	………………………………………………			

Очевидно, что если цепь обратной связи реализовать в соответствии с суммами для некоторого (любого) такта из табл. 1, то генератор будет формировать последовательность наборов, выбираемых из исходной последовательности (для схемы, реализованной согласно характеристическому полиному) с некоторым смещением $\Delta \ge 1$.

Отметим, что выбор $\Delta = 1$ соответствует такту 1 в табл. 1 и схема F_2 будет в этом случае полностью тождественна цепи обратной связи F_1. Следует отметить, что при выборе величины $\Delta = 2,3,4\ldots$ согласно [5] необходимо руководствоваться требованием, чтобы значения Δ и $2^n - 1$ были взаимно простыми числами, т.е. Н.О.К. $(\Delta, 2^n - 1) = \Delta \cdot (2^n - 1)$.

Предположим, что значение Δ выбрано равным «4» (табл. 1), т.е. из последовательности в табл. 1 будут выбираться наборы с номерами 1, 4, 7, 3, 6, … .

Структурная реализация генератора ПС–последовательности с цепью линейности обратной связи F_2 представлена на рис. 4. Достаточно простой анализ структуры на рис. 4 приводит к возможности её модификации (рис. 5), причем очевидно, что эти два варианта схемы генератора полностью тождественны. Более конкретная схемотехника для разрядов 2, 3 и 4 генератора приводится на рис. 6, которая учитывает коммутацию цепей обратной связи F_1 и F_2 генератора G_1 с помощью генератора G_2 (схема начальной установки элементов памяти для упрощения не изображена).

В соответствии с рис. 5 на входе первого (T_1) разряда генератора будет присутствовать выход элемента XOR, выполняющего суммирование состояний T_3 и T_4.

Таким образом, совместная работа двух структур, представленных на рис. 1 и 2 позволяет получить последовательность ПС-наборов в соответствии с условием (1).

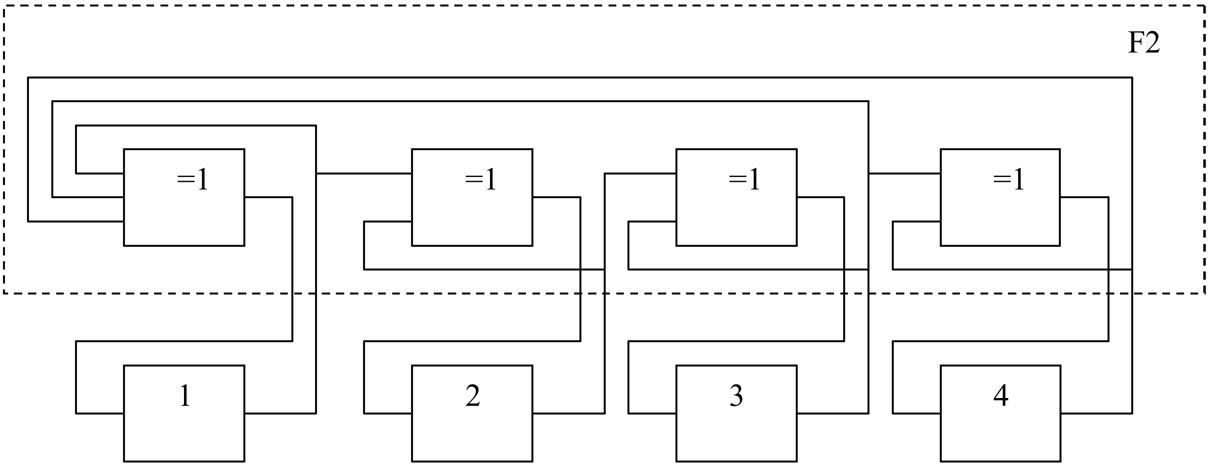

Рис. 4. Топология цепи обратной связи модифицированного ГПСЧ

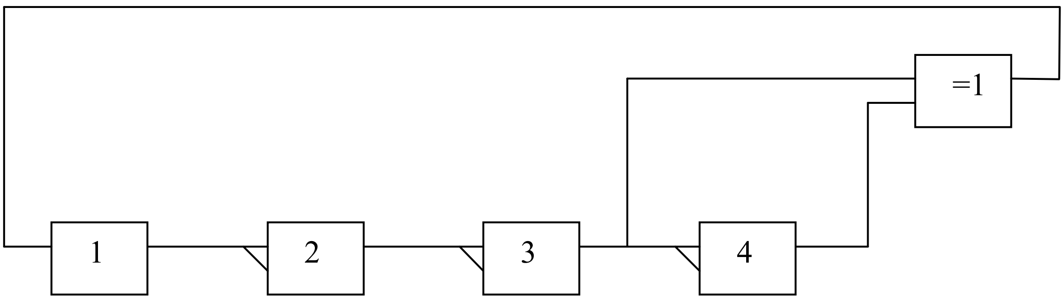

Рис. 5. Результирующая структура модифицированного ГПСЧ

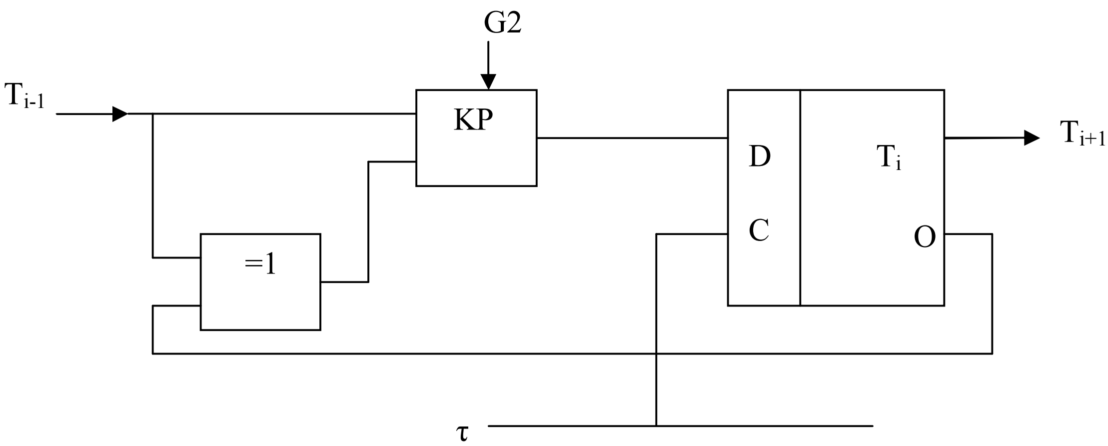

Рис. 6. Схемотехника одного бита задающего формирователя

2. Взаимозависимость параметров формирователя

Генератор имеет три основных параметра, а именно, величины k, Δ и n. Для оценки их взаимной зависимости следует более детально проанализировать структурную реализацию генератора. В регистрах $R_{gl} - R_{gk}$ (рис. 1) в каждый момент дискретного времени хранятся k «соседних» наборов – состояний ГПСЧ G_1, которые получены из некоторой подпоследовательности

$$A = k_1\Delta + k_2, \quad (5)$$

причем k_1 наборов получено в режиме работы генератора, когда G_2=1 (т.е. при включенной цепи обратной связи F_2), а k_2 наборов выбрано в режиме при $G_2 = 0$ (включена цепь F_1). При этом $k = k_1 + k_2$. Очевидно, что при $\Delta > 1$: $(k_1 = 0) \rightarrow (A = A_{min} = k)$, $(k_2 = 0) \rightarrow (A = A_{max} = k\Delta)$. Размерность области A, из которой получено k отличающихся друг от друга наборов (см. условие (1)), в зависимости от значений величин k и Δ может составлять различную долю от периода $2^n - 1$ генератора G_1 (последнее справедливо без учета влияния генератора G_2 на работу генератора G_1).

Рассмотрим ситуацию, когда

$$A = A_{max} \leq 2^n - 1. \quad (6)$$

Обозначим A_r область, из которой получено r новых наборов (по отношению к области A, из которой уже получено ранее k отличающихся наборов): $A_r = k_{1r}\Delta + k_{2r}$, причем k_{1r} наборов по-прежнему получено при G_2 =1, а k_{2r} – при $G_2 = 0$. Аналогично, обозначив $A_k = A$, получаем $A_k = k_1\Delta + k_2$ при тех же условиях по отношению к сигналу G_2, что и для k_{1r} и k_{2r}. Очевидно, что после отработки r тактов выбора r наборов область A_k сократится на A_{kr} наборов (это следует из рис. 1, когда новый набор заносится в R_{gl}, а крайний правый – удаляется из R_{gk}): $A_{kr} = k_{1kr}\Delta + k_{2kr}$, причем условия для k_{1kr} и k_{2kr} – те же. При выполнении неравенства вида $A_r \leq 2^n - 1 - (A_k - A_{kr})$ в области A_r будут содержаться только наборы, отличающиеся от наборов в сократившейся до размеров $(A_k - A_{kr})$ области A_k (последнее обстоятельство обусловлено свойствами ПС-последовательности на периоде $2^n - 1$, содержащей только отличающиеся друг от друга двоичные наборы).

Приведенное выше неравенство будет с очевидностью выполняться, если A_r и A_k имеют максимально возможные, а A_{kr} – минимально возможное значения, то есть, если $A_k - A_{kr}$ – максимально.

Для $1 \leq r \leq k$

$$A_{rmax} = r\Delta,\ A_{kmax} = k\Delta,\ A_{krmin} = k_{2krmax}\ .$$

Но так как $k_{2krmax} = r$, то

$$(A_k - A_{kr})_{max} = (k - r)\Delta.$$

Окончательно получаем, что

$$r\Delta \leq 2^n - 1 - (k - r)\Delta\ ,$$

иными словами, для любого $1 \leq r \leq k$

$$k{\cdot}\Delta \leq 2^n - 1.$$

Учитывая, что любое нетривиальное значение Δ>0, то есть, $\Delta_{min} = 2$, получаем:

$$k_{max} = (2^n - 1)/2. \quad (7)$$

Следует уточнить, что в качестве k_{max} берется ближайшее меньшее целое, то есть реально

$$k_{max} = [(2^n - 1)/2].$$

Основываясь на последнем соотношении, полученном для значения k_{max}, можно предположить, что при $\Delta = 2$ нельзя получить величины $N/2 \leq k < N$, что в принципе может потребоваться как в случаях моделирования поведения ОМС в потоке отказов произвольной кратности, так и в вероятностных контрольно-диагностических комплексах для формирования псевдослучайных сигналов в диапазоне вероятностей $0 \leq P_c \leq 1$.

Из известного комбинаторного равенства для числа сочетаний из N элементов по k следует, что $C_N^k = C_N^{N-K}$. Иными словами, если инвертировать выходные наборы предлагаемого формирователя, то диапазон значений $1 \leq k \leq [(2^n - 1)/2]$ можно преобразовать в диапазон $[(2^n - 1)/2] < k < 2^n - 1$, т.е. существует возможность получения наборов с весами, находящимися в области $1 \leq k < ([2^n - 1] = N)$. Для оценки основных характеристик предлагаемого формирователя ПС-последовательностей специального вида и сравнения этих параметров с аналогичными значениями для известных структур следует учесть, что, например, схема, рассматриваемая в работе [3], реализуется в виде N-битного кольцевого сдвигового регистра с нелинейной цепью обратной связи, управляемой классическим ГПСЧ с линейной обратной связью и содержащим также N-битный регистр сдвига.

3. Оценка сложности реализации

Как следует из работы [3] структура специализированной комбинационной схемы управляемого сдвига описывается следующим логическим соотношением:

$$N\ (C_i = T_iG_i \cup \overline{G_i}\, C_{i-1},\ T_i = G_iC_{i-1}),\ \forall\ i=1, 2, \ldots, \quad (8)$$

где G_i – выход i-го разряда управляющего ГПСЧ; T_i – состояние i-го бита в выходном наборе генератора или, что то же, – состояние i-го разряда выходного регистра, C_i – сигнал переноса из i-го разряда формирователя.

В соответствии с рис. 1 предложенная схема оперирует в основном с ($\log_2 N$)-битными наборами. Если сложность одного дешифратора DC на выходе R_{gi}, $i = \overline{1,k}$ принять равной $N \bullet \log_2 N$ двухвходовых элементов (дв. эл.), то сложность схемы L_{out}, приведенной на рис.1, можно оценить как

$$L_{out} = L_т \bullet k \bullet \log_2 N + k \bullet N \bullet \log_2 N = (L_т + N) \cdot \log_2 N.$$

Далее, для схемы на рис. 2 сложность L_{gen} её реализации можно оценить в виде

$$L_{gen} = (L_т + L_{кр}) \cdot \log_2 N + L_т \bullet \log_2 W,$$

где W – период (цикл) ГПСЧ G_2 (пренебрегая сложностью реализации цепей линейной обратной связи G_1 и G_2).

Окончательно, сложность L_2 предлагаемого формирователя можно найти, как:

$$L_2 = L_{out} + L_{gen} =$$

$$= (L_т + N)\log_2 N + (L_т + L_{кр})\log_2 N + L_т \bullet \log_2 W. \quad (9)$$

Например, полагая $L_{кр}$ = 3 дв. эл., в случае, если N = 255, k = 10, W = 2^{30} легко найти, что L_1 = 6120 дв. эл., а для рассматриваемой структуры L_2 = 2524 дв. эл. Полученный выигрыш в сложности объясняется тем, что сложность известной схемы линейно зависит от значения числа N, в то время, как предлагаемый метод построения формирователя характеризуется в основном нелинейной (логарифмической) зависимостью сложности от числа выходов генератора.

4. Оценка быстродействия

Более существенным и весомым параметром формирователя представляется быстродействие его работы (максимально допустимая тактовая чистота).

Как следует из анализа соотношения (2) частота работы известного устройства определяется неравенством

$$f_1 \le 1/(D_c + D_т),$$

причем D_c – задержка сигнала в цепи последовательного переноса, $D_т$ – время срабатывания элемента памяти.

Тогда

$$f_1 \le 1/(2N\tau_e + D_т),$$

где τ_e – абсолютное время задержки двухвходового логического элемента (точнее, среднее значение этого времени).

Принимая, что τ_e = 20 нс, а $D_т$ = 50 нс, получаем, что для N = 255 $f_{1max} = 10^5$ Гц.

Для предложенной структуры тактовая частота f_2 определяется временем D_{G1} срабатывания (переключения) ГПСЧ G_1, временем D_{Rg} переключения (записи) элементов памяти R_{gi}, $i = \overline{1,k}$, а также задержкой, вносимой дешифраторами DC_i, $i = \overline{1,k}$.

При реализации элементов конъюнкции дешифраторов в виде цепочки двухвходовых элементов И задержка дешифратора составляет

$$D_{дш} = (\log_2 N - 1)\tau_e.$$

Тогда

$$f_2 \le 1/(D_{G1} + D_{Rg} + (\log_2 N - 1)\tau_e).$$

Принимая

$$D_{G1} = D_{Rg} = D_т = 50 \text{ нс}, \ \tau_e = 20 \text{ нс},$$

получаем, что

$$f_{2max} = 4 \bullet 10^6 \text{ Гц}.$$

Следует отметить, что в случае применения предложенного метода в системах технической диагностики (например, для организации испытаний схем оперативной памяти) достаточно использовать только структуру, приведенную на рис. 2, которая на выходе S формирует последовательность согласно условию (1) и представляет собой аппаратный генератор теста ОЗУ для проверки взаимного влияния k «соседних» ячеек оперативной памяти.

Заключение

Таким образом, проведенный анализ и расчеты показывают, что предлагаемый структурный метод формирования ПС-последовательностей наборов постоянного веса типа «k-Out-of-N» отличается от известных технических решений значительным повышением производительности, в частности, ростом более чем на порядок рабочей тактовой частоты специализированного устройства, а также помимо этого метод характеризуется также и заметным сокращением сложности его схемотехнической реализации.

Литература

1. Гроль В.В. Генерация ПС-последова. тельностей с управлением по двум параметрам / В.В. Гроль, А.М. Романкевич, Али Фаллаги // Вісник НТУУ "КПІ". - Інформатика, управління та ОТ. - 2006. - № 45. - С. 85-92.

2. Romankevich A. Generation of Test Sequence's by Means of Shift Register Structures / A. Romankevich, V. Groll, L. Karachun // XI International Conference on Fault Tolerant Systems and Diagnostics. - Berlin. - 1988. - Vol. 2. - P. 129-134.

3. Романкевич А.М. Генераторы псевдослучайных тестовых наборов постоянного веса / А.М. Романкевич, Л.Ф. Карачун, Бассем Аль Хадиди // Вестник НТУУ "КПИ". Информатика, управление и ВТ. – 1998. – Вып. 31. - С. 34-39.

4. Ярмолик В.Н. Проектирование самотестируемых СБИС / В.Н. Ярмолик и др. – Минск: БУИР, 2001. - Т. 1. – 159 с.

5. Яковлев В.В. Стохастические вычислительные машины / В.В. Яковлев, Р.Ф. Федоров // Л.: Машиностроение, 1974. – 334 с.

Поступила в редакцию 10.02.2009

Рецензент: д-р техн. наук, проф., проф. кафедры вычислительной техники В.П. Широчин, Национальный технический университет Украины «Киевский политехнический институт», Киев, Украина.

СТРУКТУРНИЙ МЕТОД ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ СПЕЦІАЛЬНОГО ВИДУ

В.В. Гроль, В.О. Романкевич, Є.Р. Потапова, Мораведж Сейєд Мілад

Запропоновано структурний метод формування керованих псевдовипадкових послідовностей спеціального виду, який характеризується використанням засобів генерації псевдовипадкових послідовностей, побудованих за класичною схемою, за рахунок чого одержано можливість значного підвищення продуктивності процедур формування послідовностей вихідних наборів. Розглянуто особливості схемотехнічної реалізації основних вузлів формувача. Наведено кількісні оцінки та приклади розрахунку основних параметрів запропонованого генератора.

Ключові слова: псевдовипадкова послідовність, зсувний регістр, лінійний зворотний зв'язок, двійкові набори постійної ваги.

STRUCTURAL METHOD OF SPECIAL TYPE PSEUDORANDOM SEQUENCES GENERATION

V.V. Grol, V.A. Romankevich, E.R. Potapova, Moravej Seyed Milad

Structural method to generate controlled special type pseudorandom sequences which can be characterized by using of means to obtain the pseudorandom sequences and which is constructed on the basis of classic circuit is proposed; such approach is resulted in the possibility of sufficient increase in productivity of the procedures forming the output patterns sequences. Features of schematic implementation of the generator's basic units are reviewed. Estimations and an examples for calculation of proposed generator's main characteristics are applied.

Key words: pseudorandom sequence, shift register, linear feedback, binary patterns of fixed weight.

Гроль Владимир Васильевич – д-р техн. наук, старший научный сотрудник, профессор кафедры специализированных компьютерных систем Национального технического университета Украины «КПИ», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.

Романкевич Виталий Алексеевич – канд. техн. наук, доцент, доцент кафедры специализированных компьютерных систем Национального технического университета Украины «КПИ», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.

Потапова Екатерина Романовна – канд. техн. наук, доцент кафедры специализированных компьютерных систем Национального технического университета Украины «КПИ», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.

Мораведж Сейед Милад – аспирант кафедры специализированных компьютерных систем Национального технического университета Украины «КПИ», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.