УДК 004.05

**А. М. РОМАНКЕВИЧ, И. В. МАЙДАНЮК, В. А. РОМАНКЕВИЧ**

***Национальный технический университет Украины «Киевский политехнический институт», Украина***

# О ФОРМИРОВАНИИ ФУНКЦИЙ УПРАВЛЕНИЯ ДЛЯ ГЕНЕРАТОРА ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДВОИЧНЫХ ВЕКТОРОВ

*Работа посвящена формированию функций управления автономного генератора последовательности равновесных псевдослучайных двоичных векторов, в основе которого лежит особый управляемый сдвиговый регистр. Предложен метод построения графа переходов рассматриваемого генератора. Предложен и доказан алгоритм построения функций управления генератора для случая формирования последовательности равновесных двоичных векторов с весом 3. Отличительной особенностью предлагаемого генератора является отсутствие повторов в последовательности векторов, что важно при выполнении статистических экспериментов – уменьшается погрешность.*

***Ключевые слова:*** *генератор псевдослучайных векторов, алгоритм формирования функций управления, равновесные векторы.*

## Введение

На этапе разработки отказоустойчивых реконфигурируемых многопроцессорных систем (ОМС) управления сложными объектами одной из главных задач, которые необходимо решить проектировщику, является достижение заданного значения вероятности безотказной работы системы, что невозможно без адекватных методов ее оценки. Если речь идет об ОМС управления, то такие ее особенности, как неоднородность и иерархичность структуры, большой разброс по типу составляющих элементов (процессоров) и сложность самой системы в целом приводят к различным затруднениям при использовании известных методов расчета надежности. Одним из возможных путей решения является использование наиболее универсального метода – проведение статистических экспериментов с моделями, адекватно отражающими реакцию (работоспособность – отказ) ОМС на появления отказов ее модулей [1]. При этом статистический эксперимент выполняется последовательно, отдельно для каждого значения веса (количества отказавших модулей) в установленных пределах. Для моделирования состояний модулей системы целесообразно использование генератора равномерно распределенных двоичных векторов заданного веса.

Существует достаточно много решений, позволяющих формировать выходную последовательность векторов заданного веса, но большинство из них обладает теми или иными недостатками, главным из которых является повторение векторов в формируемой последовательности.

Приведем формулу, которая позволяет оценить преимущество бесповторного генератора по сравнении с равновесным, имеющим равномерный закон распределения, но при этом повторяющим свои состояния генератором (например [2]):

$$N_{П} = \left( \eta^{K-1} + \frac{\eta^{K-2} - 1}{\eta - 1} \right); \eta = 1 - 1 \Big/ C_n^k, \qquad (1)$$

где n–количество разрядов регистра, то есть длина генерируемого вектора, k – вес вектора, K – количество сгенерированных векторов, $N_{П}$ – количество уникальных векторов в сгенерированной последовательности. В качестве примера можно отметить, что для 20% векторов (5,15) согласно (1) бесповторный генератор сформирует на 10% больше уникальных векторов. Таким образом, использование бесповторной последовательности для моделирования состояний системы позволит увеличить точность а следовательно и эффективность указанного метода.

## 1. Постановка задачи

В [3] предложен формирователь бесповторной последовательности векторов на основе циклического сдвигового регистра с возможностью исключения из выполняемого сдвига определенного множества разрядов. Пусть $x_1, x_2, \ldots, x_n$ – булевы переменные, отражающие состояния соответствующих разрядов регистра, а $\mathbf{X} = (x_1, x_2, \ldots, x_n)$ – генерируемый двоичный вектор.

Принцип работы рассматриваемого генератора можно описать следующим образом: в каждом такте, в общем случае, осуществляется последователь-

ный циклический сдвиг содержимого регистра вправо, при этом если i-й разряд в данном такте t не принимает участия в сдвиге, то его значение задерживается, т.е. $x_i(t) \rightarrow x_i(t+1)$, а $x_{i-1}(t) \rightarrow x_{i+1}(t+1)$.

Каждому разряду (переменной) $x_i$ ставится в соответствие функция управления: $f_i(x_1, x_2, \ldots, x_n)$ – булева функция, которая равна 1, если необходимо задержать i-й разряд, и 0 в противном случае. В данной статье рассматривается частный случай такого формирователя, в котором определена функция управления f (задержки) только первого разряда (рис. 1).

Введем ряд обозначений. Пусть $B_n^k$ – множество всех двоичных векторов длины n, вес которых равен k. Определим F – множество или класс функций управления f таких, что каждая из них формирует на выходе генератора полную бесповторную последовательность векторов, т.е. для $\forall$ f$\in$F период генератора максимален и равен $|B_n^k| = C_n^k$ тактов. В работе [3] доказано, что для любого допустимого значения n и k множество F не пустое.

Ключевой задачей при синтезе рассматриваемого генератора является выбор или формирование функции задержки f $\in$ F. Решением является формирование так называемого графа переходов генератора и нахождение его гамильтонова цикла, но очевидно, что такой подход далеко не всегда целесообразен, в виду его трудоемкости. В таких условиях актуальным является способ быстрого получения хотя бы одной f $\in$ F для любых значений n, k.

Фактически, вопрос построения и поиска аналитического представления функций управления для k=2 можно считать решенным. В работе [3] представлена достаточно простая формула получения всего множества F для любых значений n при k=2. Однако предложенное решение для k=2 с легкостью распространить на большие значения веса (k>2) не получается. Ввиду этого большой интерес представляет решение задачи нахождения алгоритма формирования f $\in$ F, для k>2. В данной статье решается задача поиска алгоритма получения функций управления без проверки и перебора для случая k=3.

## 2. Базовые обозначения

Вслед за [3] обозначим через Sh (shift) операцию циклического сдвига, которая действует на множестве $B_n^k$, $Sh(\mathbf{X}) = Sh(x_1,x_2,\ldots,x_{n-1},x_n) = (x_n,x_1,x_2,\ldots,x_{n-1})$, $Sh^i(\mathbf{X}) = Sh(Sh^{i-1}(\mathbf{X}))$, $Sh^{-1}(\mathbf{X}) = Sh(x_2,\ldots,x_{n-1},x_n, x_1)$. Назовем S-группой упорядоченную совокупность векторов $S=\{\mathbf{X}\}\cup\bigcup_{\forall i\in[1,|S|]} Sh^i(X)$, $\mathbf{X} \in S$. Упорядочивать векторы в S-группе будем путем циклического сдвига. Для заданных n, k количество S-групп обозначим через NumS(n, k), понятно, что $B_n^k = \bigcup S_i$, причем $\bigcup S_i \cap S_j = \varnothing$, где i, j $\in$[1, NumS(n, k)],i$\neq$j.

Пример разделения множества $B_9^3$ на S-группы приведен на рис. 2.

Количество векторов в группе будем называть глубиной или мощностью группы. Пусть повторяющийся фрагмент вектора $\mathbf{X}=(x_1,x_2,\ldots,x_n)$ – это вектор длины n/d, где d – общий делитель n и k, и конкатенация d таких повторяющихся фрагментов составляет вектор **X**, и в этом случае $x_i = x_{(i+j\cdot n/d) \bmod n}$, где i$\in$[1..n/d], j$\in$[1..d].

В [3] приведена формула расчета количества S-групп:

$$\mathrm{NumS}(n,k) = \sum_{i=0}^{m} \frac{r(n_i,k_i)}{n_i}, \qquad (2)$$

где $r(n,k) = C_n^k - \sum r(n_i,k_i)$, i=1..m, $n_i = n/d_i$, $n_i = k/d_i$, $d_i$ – общий делитель n и k. Определим количество сдвиговых групп для рассматриваемого случая. Подставив значение k=3 в (2) получим:

1) $\mathrm{NumS}(n, 3) = (n^2-3n+2)/6$, если n не кратно 3;
2) $\mathrm{NumS}(n, 3) = (n^2-3n)/6+1$, если n кратно 3.

Операцию циклического сдвига с задержкой первого разряда обозначим как Ds,

$Ds(\mathbf{X}) = Ds(x_1,x_2,\ldots,x_{n-1},x_n) = (x_1,x_n,x_2,\ldots,x_{n-1})$,

$Ds^i(\mathbf{X}) = Ds(Ds^{i-1}(\mathbf{X}))$, $Ds^1(\mathbf{X}) = Ds(\mathbf{X})$.

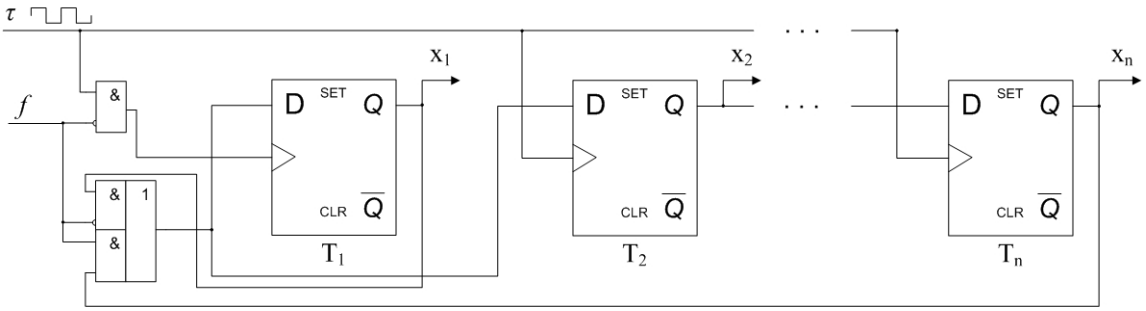



Рис. 1. Схема генератора

| $S_{1(1,1,7)}$ | $S_{2(1,2,6)}$ | $S_{3(1,3,5)}$ | $S_{4(1,4,4)}$ | $S_{5(1,5,3)}$ | $S_{6(1,6,2)}$ | $S_{7(2,2,5)}$ | $S_{8(2,3,4)}$ | $S_{9(2,4,3)}$ | $S_{10(2,4,3)}$ |
|---|---|---|---|---|---|---|---|---|---|
| 111000000 | 110100000 | 110010000 | 110001000 | 110000100 | 110000010 | 101010000 | 101001000 | 101000100 | 100100100 |
| 011100000 | 011010000 | 011001000 | 011000100 | 011000010 | 011000001 | 010101000 | 010100100 | 010100010 | 010010010 |
| 001110000 | 001101000 | 001100100 | 001100010 | 001100001 | 101100000 | 000101010 | 001010010 | 001010001 | 001001001 |
| 000111000 | 000110100 | 000110010 | 000110001 | 100110000 | 010110000 | 000010101 | 000101001 | 100101000 | |
| 000011100 | 000011010 | 000011001 | 100011000 | 010011000 | 001011000 | 100001010 | 100010100 | 010010100 | |
| 000001110 | 000001101 | 100001100 | 010001100 | 001001100 | 000101100 | 010000101 | 010001010 | 001001010 | |
| 000000111 | 100000110 | 010000110 | 001000110 | 000100110 | 000010110 | 101000010 | 001000101 | 000100101 | |
| 100000011 | 010000011 | 001000011 | 000100011 | 000010011 | 000001011 | 010100001 | 100100010 | 100010010 | |
| 110000001 | 101000001 | 100100001 | 100010001 | 100001001 | 100000101 | 101010000 | 010010001 | 010001001 | |

Рис. 2. S-группы, n=9, k=3

Пусть $\mathbf{Y}= (x_2, x_3,\ldots, x_{n-1})$, далее наряду с обозначением f(**X**), будем использовать f(**Y**), причем если $f(X)\in F$, то f(**Y**)= f((0)+**Y**+(1))=f((1)+**Y**+(0)), знаком «+» обозначена операция конкатенации над двоичными векторами. Векторы **X** $=(x_1, x_2,\ldots, x_{n-1}, x_n)$ для которых $x_1\oplus x_n=1$ будем называть переходными, поскольку только для таких векторов Ds(**X**) ≠ Sh(**X**), на рис. 2, такие векторы подчеркнуты. Функция задержки $f(X)\in F$ не зависит от $x_1$ и $x_n$, и при этом что $f(x_1, x_2,\ldots, x_{n-1}, x_n) = f(x_n, x_2,\ldots, x_{n-1}, x_1)$.

Обозначим $\Gamma_S$ – неориентированный мультиграф, множество вершин $V\Gamma_S$ которого – множество S-групп, а множество ребер $E\Gamma_S = \{\{S_i,S_{j>i}\}|\ \mathbf{X} \in S_i, Ds(\mathbf{X}) \in S_j\}$. Пусть $\Gamma_S(f)$ – частичный граф графа $\Gamma_S$ и $E\Gamma_S(f)= \{\{S_i,S_{j>i}\}|\ \mathbf{Y} \in S_i, \mathbf{Y} \in S_j, f(\mathbf{Y})=1\}$, где запись $\mathbf{Y} \in S_i$ означает, что ((0)+**Y**+(1)) $\in S_i$ либо ((1)+**Y**+(0)) $\in S_i$. В [3] показано, что если $\Gamma_S(f)$ – остов графа $\Gamma_S$ то $f\in F$, т.е. для формирования $f\in F$ достаточно выбрать остов графа $\Gamma_S$. На рис. 3 приведен пример $\Gamma_S$ графа для n=9 и k=3, ребра подписаны соответствующими векторами Y.

Построение графа $\Gamma_S$ связанно с определенными трудностями, поскольку для его формирования необходимо рассмотреть все переходные векторы множества $B_n^k$ и провести ребра. В ходе дальнейших изложений будет показан способ построения изоморфного к $\Gamma_S$ графа, но уже без анализа всего множества $B_n^k$.

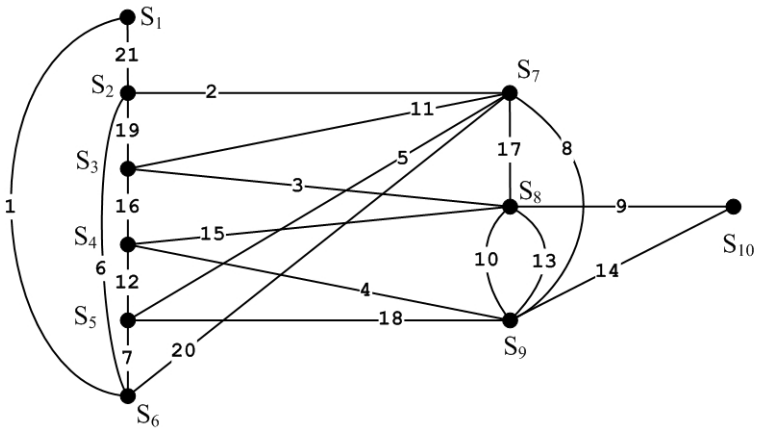
## 3. A-вектор

Введем понятие вектора натуральных десятичных чисел, обозначим такой вектор как A-вектор. Пусть множество k-разрядных векторов $A=(a_1, \ldots, a_k)$ – $N_n^k$ такое, что $\sum a_p = n$, $\forall A\in N_n^k$.

Введем операцию сравнения для A-векторов: A>A', если $a_p=a'_p\ \forall\ p\in[1..l-1]$, и $a_l>a'_l$, также A= A', если $a_p= a'_p\ \forall\ p\in[1..k]$.

Определим операцию $Sn^p$ на множестве $N_n^k$ – $Sn: N_n^k \to N_n^k$, $Sn(A)= Sn(a_1,\ldots, a_{n-1}, a_k)= (a_k, a_1,\ldots, a_{k-1})$, $Sn^p(A)= Sn(Sn^{p-1}(A))$, $Sn^1(A)= Sn(A)$. Обозначим $Sn^{-1}(A)= (a_2,\ldots, a_k, a_1)= A'$, т.е. $Sn(A')= A$.

Теперь покажем соответствие векторов X, S-групп и векторов A. Пусть $\mathbf{X}\in B_n^k$, также пусть $I(\mathbf{X}) =(i_1, i_2, \ldots, i_k)$ – упорядоченный по возрастанию вектор натуральных чисел, причем $\forall\ x_i \in X$ и $x_i = 1$ $i \in I(\mathbf{X})$. Определим функцию $\alpha(X)= (a_1,\ldots, a_{k-1}, a_k)$ – которая возвращает вектор A такой, что $a_p=(I_{(p+1)\bmod k} - I_p)$. Другими словами $A=\alpha(X)$ – вектор расстояний между ближайшими единичными разрядами в векторе X.




| | | | |
|---|---|---|---|
| 1 | 1100000 | 11 | 0100001 |
| 2 | 1010000 | 12 | 0011000 |
| 3 | 1001000 | 13 | 0010100 |
| 4 | 1000100 | 14 | 0010010 |
| 5 | 1000010 | 15 | 0010001 |
| 6 | 1000001 | 16 | 0001100 |
| 7 | 0110000 | 17 | 0001010 |
| 8 | 0101000 | 18 | 0001001 |
| 9 | 0100100 | 19 | 0000110 |
| 10 | 0100010 | 20 | 0000101 |
| | | 21 | 0000011 |

Рис. 3. Граф ГS для n=9, k=3

Рассмотрим векторы некой группы S. Пусть $Z = \bigcup_{X_i \in S} \alpha(X_i)$. Поскольку расстояния между «ближайшими» единичными разрядами $\forall X \in S$ неизменно, то очевидно, что $Z = \bigcup_{p=1..k} Sn^p(\alpha(X)) = \bigcup_{p=1..k} Sn^p(A)$, для $\forall X \in S$, где $A=\alpha(X)$. Заметим, что аналогично векторам X векторы A могут состоять из нескольких повторяющихся фрагментов, в этом случае $|Z|<k$, но всегда $|Z|= k|S|/n$.

В дальнейшем для удобства наименьший вектор из множества Z будем называть правильным. Очевидным свойством правильного вектора $A=(a_1,\ldots, a_k)$, является то, что $a_1 \le a_2,\ldots, a_k$. Таким образом, каждая S-группа и соответствующая ей Z-группа может быть обозначена своим уникальным правильным вектором A, на рис. 2 они записаны в скобках. Обозначим $R_n^k$ – кортеж всех возможных правильных векторов A, при заданных n и k. Понятно, что $|R_n^k| = NumS(n, k)$.

Пусть $\chi(A)$ – функция, которая возвращает такой вектор $X=(x_1,\ldots, x_n)$, что $\alpha(X) = A$ и $x_1 =1$. Например, для вектора (0,1,0,1,0,1,0,0,0) A-вектор будет: (2,2,5), тогда как $\chi(2,2,5)$= (1,0,1,0,1,0,0,0,0).

Поскольку нескольким векторам **X** может соответствовать один и тот же вектор A, то очевидно $X = Sh^{i-1}(\chi(\alpha(X)))$, где i – позиция первого единичного разряда вектора X. Следовательно, нельзя говорить об однозначном соответствии векторов множества S и Z. Но, для наших целей достаточно сопоставить только переходные векторы множества S, поскольку значение функции определено только на этих векторах. Для этих целей сопоставим каждому вектору $A=(a_1,\ldots,a_k)$ два вектора $X \in B_n^k : X_1= \chi(A)$ и $X_2= Sh^{-1}(\chi(A))$, при этом если $a_k>1$, то $X_1$ переходной вектор, если $a_1>1$, то и/или $X_2$. Таким образом, на основе множества $N_n^k$ можно однозначно сформировать множество всех возможных переходных векторов $X \in B_n^k$.

Заметим, что в общем случае количество переходных векторов в S-группе можно определить как удвоенное количество элементов в соответствующем векторе A, для которых $a_p>1$.

Обозначим операцией Inc: $N_n^k \rightarrow N_n^k$, $B=Inc_p(A)$, если $\forall$ $j\ne p$, $j\ne(p-1)\bmod_k$ $b_j=a_j$ и $b_i= a_i+1$, $b_{(p-1) \bmod k} = a_{(p-1) \bmod k} -1$, при этом операция выполнима только над разрядами (p) для которых $a_{(p-1) \bmod k} \ge 2$, p, $j\in[1..k]$, $Inc_1(A)=Inc(A)$. Другими словами, в этой операции инкрементируется значение некого разряда за счет декрементации значения разряда левее, например, $Inc_2(2,2,5) = (1,3,5)$. Аналогично, введем операцию Dec: $N_n^k \rightarrow N_n^k$, $B =Dec_p(A)$, если $b_j= a_j$ $\forall$ $j\ne p$, $j\ne(p-1) \bmod_k$ и $b_p = a_p -1$, $b_{(p-1) \bmod k} = a_{(i-1) \bmod k} +1$, при этом необходимо выполнение условия $a_p \ge 2$, p, $j\in[1..k]$. Например, $Dec_2(2,2,5) = (3,1,5)$. $Dec_1(A)=Dec(A)$. Понятно, что $Inc_i(Dec_i(A))= A$.

Теперь сопоставим выполнение операций $Ds(\mathbf{X})$ и операций Inc(A), Dec(A) над соответствующим вектором A.

Пусть $A = (a_1,\ldots, a_k)$. Покажем, что $\chi(Inc(A)) = Ds(\chi(A))$. Пусть $a_k \ge 2$, т.е. операцию Inc(A) можно выполнить, тогда $\chi(A)= (1, x_2,\ldots, x_{n-1},0)$. $I(\chi(A))=(1,1+a_1,\ldots, 1+a_1+\ldots+a_k)$, тогда $I(Ds(\chi(A)))=(1,2+a_1,\ldots, 2+a_1+\ldots+a_k) \rightarrow A'= (a_1+1, a_2,\ldots, a_k-1)$, и действительно A'= Inc(A). Следуя аналогичным рассуждениям, можно показать что $\chi(Dec(A)) = Ds(Sh^{-1}(\chi(A)))$.

Подытожим сказанное в виде утверждения:

*Утверждение 1*: $Inc(A) \rightarrow Ds(\chi(A))$; $Dec(A) \rightarrow Ds(Sh^{-1}(\chi(A)))$.

Говорить об обратном соответствии, можно только для переходных векторов ($x_1 \oplus x_n=1$): $Ds(\mathbf{X})$ соответствует $Inc(\alpha(X))$ если $x_1 =1$, и $Dec(Sn(\alpha(X)))= Dec(\alpha(Sh(X)))$ если $x_n =1$.

Ранее упоминалось о том, что если $f \in F$, то f(0, Y, 1) = f(1, Y,0). Покажем это условие в терминах A векторов. Пусть $\alpha(1, Y,0)= (a_1,\ldots, a_k)=A$. Выполнение операции $Ds(0, Y, 1) \rightarrow Dec(\alpha(1,0, Y)) = Dec(a_1+1,\ldots, a_k-1)$, а $Ds(1, Y,0) \rightarrow Inc(a_1,\ldots, a_k)$, понятно, что $Dec(a_1+1,\ldots, a_k-1) = A$. Таким образом, если на векторе A выполняется операция Dec, то на результирующем векторе A'=Dec(A), должна выполнятся операция Inc(A') и наоборот. Следовательно, для определения множества векторов Y, на которых выполняется операция Ds, достаточно указать множество векторов A, над которыми нужно выполнить операцию Inc. Таким образом, сформировать функцию f можно на основе множества векторов A, на которых выполняется операция Inc.

Пусть $A_p$, A – p-й и первый (правильный) векторы $\in$ Z. Согласно ранее приведенным определениям: $Inc_p(A)= Sn^{p-1}(Inc(Sn^{k-p+1}(A))) = A' \in Z'$. Тогда, опираясь на утверждение 1, можно записать следующее:

*Утверждение 2*: Если $Inc_p(A) \in Z'$, то $Ds(\chi(Sn^{k-p+1}(A))) \in S'$; аналогично $Dec_p(A) \rightarrow Ds(Sh^{-1}(\chi(Sn^{k-p+1}(A))))$.

Обозначим $\Gamma_A$ – ориентированный маркированный мультиграф, множество вершин $V\Gamma_A$ которого – множество правильных векторов, а множество дуг $E\Gamma_A = \{\{A_i, A_j\}| Inc_p(A_i) \in Z_j\}$, причем дуга маркируется значением p. Согласно ранее изложенным выкладкам о соответствии операций Inc(A) и

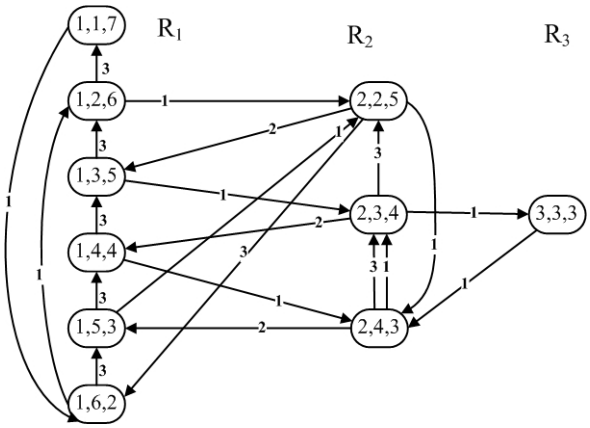



Рис. 4 Граф $\Gamma_A$ для n=9, k=3.

Ds(1,Y,0) можно утверждать что графы $\Gamma_A$ и $\Gamma_S$ – изоморфны. Следовательно, для построения f∈F достаточно выбрать остов графа $\Gamma_A$.

## 4. R-группа

Остановимся теперь на способе формирования графа $\Gamma_A$ без предварительного построения графа $\Gamma_S$. Прежде всего, необходимо сформировать множество вершин, т.е. фактически построить кортеж $R_n^3$.

Приведем формулу для формирования множества $R_n^3$ в общем виде:

$$R_n^3 = \bigcup_{a_1=1}^{[n/3]} \bigcup_{a_2=a_1}^{n-2a_1-q(n,a_1)} (a_1, a_2, n-a_1-a_2), \qquad (3)$$

где $q(n, a_1) = 0$, если $a_1 = [n/3]$ и n кратно 3, и $q(n, a_1) = 1$ в других случаях.

Докажем эту формулу. Каждый вектор $A \in R_n^3$ состоит из трех элементов: $(a_1, a_2, a_3)$. Очевидно, что $a_3$ можно представить как $a_3=n-(a_1+a_2)$, также, что $a_1 \geq 1$ и $a_1 \leq a_2$. Поскольку A – правильный вектор, то по определению: $a_1 \leq a_2$, $a_1 \leq a_3 \rightarrow 2a_1 \leq a_2+a_3 \rightarrow 3a_1 \leq n \rightarrow a_1 \leq n/3 \rightarrow a_1 \leq [n/3]$. Теперь поясним верхнюю границу второго объединения. Если $a_3 = a_1$, то вектор $(a_1, a_2, a_1)$ – не правильный поскольку $(a_1, a_2, a_1) > (a_1, a_1, a_2)$, за исключением случая, когда $a_1=a_2$, т.е. когда $a_1=a_2=a_3=[n/3]$, следовательно, кроме указанного случая: $a_3 > a_1 \rightarrow n-a_2-a_1 > a_1 \rightarrow n-2a_1 > a_2 \rightarrow n-2a_1-1 \geq a_2$. Таким образом, $q(n, a_1) = 1$, всегда кроме случая, когда n кратно 3 и $a_1 = [n/3]$. Полученные по формуле (3) векторы различны по операции Sn, а последовательность упорядочена по возрастанию.

Рассчитаем мощность кортежа $R_n^3$ сформированного по формуле (3) для случая n кратное 3 ($n_1 = [n/3]$): $|R_n^3| = 1 + \sum_{i=1}^{n_1-1} (n-2i-1) - i + 1 = n(n_1-1) - 3n_1(n_1-1)/2 + 1 = (n^2-3n)/6 + 1$. Если n не кратно 3, то $|R_n^3| = \sum_{i=1}^{n_1} (n-2i-1) - i + 1 = nn_1 - 3n_1(n_1+1)/2$. Если n не кратно 3, то $n_1 = (n-1)/3$ либо $n_1 = (n-2)/3$, подставив оба значения получим $-(n^2-3n+2)/6$. Как мы видим полученные выражения совпадают с рассчитанными ранее по (2) для NumS(n,3). Следовательно, множество $R_n^3$, полученное по выражению (3), действительно является полным множеством правильных векторов A. Выражение (3) позволяет достаточно быстро сформировать множество $R_n^3$ т.е. множество вершин графа $\Gamma_A$.

Теперь когда есть множество вершин графа $\Gamma_A$ можно провести дуги, для этого для $\forall A \in R_n^3$ необходимо выполнить (если это возможно) операцию $Inc_p$, p=[1..3], и провести соответствующею дугу и маркировать ее значением p. Напомним, что если $\Gamma_A(f)$ – остов графа $\Gamma_A$ то $f \in F$. Но поиск остова, а тем более построение графа, хоть и более простым способом, чем графа $\Gamma_S$, занимает время.

Путем последующих изложений будет показан способ выбора множества правильных векторов A и операций над ними, которые образуют остов графа $\Gamma_A$, без построения самого графа.

## 5. Алгоритм

Обозначим $R_p$ – упорядоченная по возрастанию группа правильных векторов A, таких что $\forall A=(a_1,\ldots,a_k) \in R_p$ $a_1=p$.

Идея предлагаемого алгоритма заключается в том, что остов графа $\Gamma_A$ в целом можно сформировать путем связывания деревьев, каждое из которых

состоит из вершин определенного множества $R_p$ ($R_n^3 = \bigcup R_p$) Приведем ряд утверждений позволяющих связывать вершины графа $\Gamma_A$ предлагаемым образом.

Пусть $A_i=(p,i,n-p-i) \in R_p$, очевидно любой вектор из $R_p$ можно идентифицировать по значению второго элемента, кроме этого, согласно выражению (3) $A_p$ – наименьший вектор $\in R_p$.

*Утверждение 3*: $\forall A_i \neq A_p \in R_p$: $Inc_3(A_i) = A_{i-1} \in R_p$.

Доказательство. $Inc_3(A_i)=(p,i-1,n-p-i+1)= A'$, чтобы доказать $A' \in R_p$ достаточно того, что $p \le i-1$ и это действительно так, поскольку согласно условию $p+1 \le i$.

*Утверждение 4*: $\forall A_i \in R_p$, $p \neq 1$: $Inc_2(A_i) = A_j \in R_{p-1}$.

Доказательство. Понятно, что $p \ge 2$, для того чтобы $A_j \in R_{p-1}$ должно выполнятся $p-1 \le j \le n-2(p-1)-1$. Рассмотрим вектор $A_j = Inc_2(A_i)= Inc_2(p,i,n-p-i) = (p-1,i+1, n-p-i)$, т.е. $j=i+1$. Раз $A_i \in R_p$, то $p \le i \le n-2p-1 \rightarrow p+1 \le i+1 \le n-2p \rightarrow p-1 \le p+1 \le i+1 \le n-2p \le n-2p+1 \rightarrow p-1 \le j \le n-2(p-1)-1$, следовательно $A_j \in R_{p-1}$.

*Утверждение 5*: $\forall A_i \in R_p$, $p \neq 1$: $\exists A_j \in R_{p-1}$: $Inc_1(A_j) = A_i$.

Фактически необходимо доказать, что $\forall A_i \in R_p$ $Dec_1(A_i) \in R_{p-1}$. Рассмотрим вектор $A_j = Dec_1(A_i)= Dec_1 (p-1,i,n-p-i+1)$, понятно что $p-1 \le p \le i \le n-2p-1 \le n-2p+1 \rightarrow p-1 \le j \le n-2(p-1)-1$, следовательно $A_j \in R_{p-1}$.

Таким образом, связать вершины множества $R_p$ в дерево можно выполнив операцию $Inc_3(A)$ над векторами множества (утверждения 3), с указанными ограничениями. Связать же полученные деревья можно путем выполнения $Inc_1(A)$ и/или $Dec_2(A)$ над одним из векторов множества $R_p$ – утверждения 4, 5.

Пусть O – множество дуг (т.е. операция с указанным вектором) $Dec_i(A)$ или $Inc_i(A)$. Тогда, согласно приведенным утверждениям множество O, которому соответствует остов графа $\Gamma_A$, можно получить:

$$O = \bigcup_{p=1}^{[n/3]} \bigcup_{A \in R_p / A_p} Inc_3(A) \cup \bigcup_{p=2}^{[n/3]} o_p , \qquad (4)$$

где $o_p = Dec_1(A')$ или $Inc_2(A')$, A' – один из векторов множества $R_p$.

Искомый алгоритм может быть представлен следующим образом:

1. Сформировать все множества $R_p$ согласно выражению (3).
2. Получить множество O согласно (4)
3. На основе множества O получить множество соответствующих векторов X согласно утверждению 2.
4. Определить множество векторов Y соответствующее множеству, полученному на предыдущем шаге.
5. $f = \bigvee_Y K(Y)$, где K(Y) - конституента единицы, соответствующая вектору Y.

Рассмотрим пример формирования функции управления по выше приведенному алгоритму для k=3, n = 9:

1. $R_1=\{(1,1,7),\ldots,(1,6,2)\}$, $R_2=\{(2,2,5),\ldots,(2,4,3)\}$, $R_3=\{(3,3,3)\}$.
2. $O=\{Inc_3(1,2,6),\ldots, Inc_3(1,6,2)\} \cup \{Inc_3(2,4,3), Inc_3(2,3,4)\} \cup \{Inc_2(2,3,4)\} \cup \{Inc_2(3,3,3)\}$.
3. $MX=\{\chi(Sn(1,2,6)),\ldots, \chi(Sn(1,6,2))\} \cup \{\chi(Sn(2,4,3)), \chi(Sn(2,3,4))\} \cup \{\chi(Sn^2(2,3,4))\} \cup \{\chi(Sn^2(3,3,3))\} = \{\chi(6,1,2),\ldots, \chi(2,1,6)\} \cup \{\chi(3,2,4), \chi(4,2,3)\} \cup \{\chi(3,4,2)\} \cup \{\chi(3,3,3)\} = \{(100000110),\ldots, (101100000)\} \cup \{(100101000), (100010100)\} \cup \{(100100010)\} \cup \{(100100100)\}$.
4. $MY=\{(0000011),\ldots, (0110000)\} \cup \{(0010100), (0001010), (0010001),(0010010)\}$.
5. $f= \bar{x}_2\bar{x}_3\bar{x}_4\bar{x}_5\bar{x}_6x_7x_8 \vee \ldots \vee \bar{x}_2x_3x_4\bar{x}_5\bar{x}_6\bar{x}_7\bar{x}_8 \vee \vee \bar{x}_2\bar{x}_3x_4\bar{x}_5x_6\bar{x}_7\bar{x}_8 \vee \bar{x}_2\bar{x}_3\bar{x}_4x_5\bar{x}_6x_7\bar{x}_8 \vee \vee \bar{x}_2\bar{x}_3x_4\bar{x}_5\bar{x}_6\bar{x}_7x_8 \vee \vee \bar{x}_2\bar{x}_3x_4\bar{x}_5x_6x_7\bar{x}_8 = x_7x_8 \vee x_6x_7 \vee x_5x_6 \vee x_4x_5 \vee \vee x_3x_4 \vee x_4x_6 \vee x_5x_7 \vee x_4x_8 \vee x_4x_7 = = x_7(x_4 \vee x_5 \vee x_6 \vee x_8) \vee \vee x_4(x_3 \vee x_5 \vee x_6 \vee x_8) \vee x_5x_6.$

Сложность ДНФ функций полученных по выше приведенному алгоритму, будет в общем виде 2(NumS(n,k)-1).

## Заключение

В статье представлен достаточно простой алгоритм формирования ряда функций управления $f \in F$ для случая k=3, при любом значении n. Преимущество алгоритма в том, что для построения функции управления нет необходимости в построении графа переходов или его модификаций.

Объектом дальнейших исследований является поиск аналогичных решений для больших значений k, а также анализ аналитических представлений этих функций.

## Литература

*1. Романкевич, А. М. Графологические модели для анализа сложных отказоустойчивых вычислительных систем [Текст] / А. М. Романкевич, Л. Ф. Карачун, В. А. Романкевич // Электронное моделирование. – 2001. – Т. 23, №1. – С. 102 – 111.*

*2. Структурный метод генерации псевдослучайных последовательностей специального вида [Текст] / В. В. Гроль, В. А. Романкевич, Е. Р. Потапова, Мораведж Сейед Милад // Радіоелектронні і комп'ютерні системи. –2010. – № 5.– С. 230 – 236.*

*3. Романкевич, В. А. Структурный метод формирования двоичных псевдослучайных векторов заданного веса [Текст] / В. А. Романкевич, И. В. Майданюк // УСиМ. – 2011. – № 5. – С. 28 – 33, 58.*

*Поступила в редакцию 4.02.2014, рассмотрена на редколлегии 25.03.2014*

**Рецензент:** д-р техн. наук, проф. М. Ф. Каравай, Институт проблем управления РАН, Москва, Российская Федерация.

## ПРО ФОРМУВАННЯ ФУНКЦІЙ УПРАВЛІННЯ ДЛЯ ГЕНЕРАТОРА ПОСЛІДОВНОСТЕЙ ДВІЙКОВИХ ВЕКТОРІВ

***О. М. Романкевич, І. В. Майданюк, В. О. Романкевич***

Робота присвячена формуванню функцій управління автономного генератора послідовності рівновагових псевдовипадкових двійкових векторів, в основу якого покладено особливий керований регістр зсуву. Запропоновано метод побудови графа переходів генератора, що розглядається. Запропоновано та доведено алгоритм побудови функцій управління генератора для випадку формування послідовності рівновагових двійкових векторів з вагою 3. Відмінною особливістю генератора, що пропонується, є відсутність повторів у послідовності векторів, що важливо при виконанні статистичних випробувань – зменшується похибка.

**Ключові слова:** генератор псевдовипадкових векторів, алгоритм формування функцій управління, рівновагові вектори.

## ABOUT FORMATION OF FUNCTIONS OF CONTROL FOR THE SEQUENCE GENERATOR OF BINARY VECTORS

***A. M. Romankevich, I. V. Maydaniuk, V. A. Romankevich***

Operation is devoted to formation of functions of control of an independent sequence generator of equilibrium pseudorandom binary cornerstone at the heart of which the special controlled shift register is. The method of creation of a transition graph of the considered generator is offered. The algorithm of creation of functions of control of the generator for a case of formation of sequence of equilibrium binary vectors weighing 3 is offered and proved. The distinguishing peculiarity of proposed generator is an absence of iteration of vector's sequences. It is important in time of execution of statistical experiments (we have reduction of error).

**Key words:** generator of pseudorandom vectors, formation of management functions algorithm, equilibrium vectors

**Романкевич Алексей Михайлович** – д-р техн. наук, профессор, профессор кафедры Системного программирования и специализированных компьютерных систем, Факультет прикладной математики, Национальный технический университет Украины «Киевский политехнический институт», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.

**Майданюк Иван Викторович** – канд. техн. наук, инженер - программист ТОВ "Ес. Ди. Эл. Тридион Девелопмент Лаб Юкрейн", Киев, Украина, e-mail: miv1984@gmail.com.

**Романкевич Виталий Алексеевич** – канд. техн. наук, доц., доц. каф. Системного программирования и специализированных компьютерных систем, Факультет прикладной математики, Национальный технический университет Украины «Киевский политехнический институт», Киев, Украина, e-mail: romankev@scs.ntu-kpi.kiev.ua.