УДК 519.718

В.А. Романкевич, И.В. Майданюк

Структурный метод формирования двоичных псевдослучайных векторов заданного веса

Предложено решение задачи структурного синтеза автономного генератора равновесных псевдослучайных двоичных векторов на основе особых сдвиговых регистров, управление которыми осуществляется булевой функцией задержки. Рассмотрены свойства таких функций.

The solution of the problem of a structural synthesis of independent fixed weight pseudorandom binary vectors is suggested on the basis of the special shift registers controlled by a Boolean delay function. The properties of such functions are considered.

Запропоновано розв'язання задачі структурного синтезу автономного генератора рівноважних псевдовипадкових двійкових векторів на базі особливих зсувних регістрів, управління якими здійснюється булевою функцією затримки. Розглянуто властивості таких функцій.

Введение. Расчет вероятности безотказной работы отказоустойчивых реконфигурируемых многопроцессорных систем (ОМС) управления сложными объектами [1] на этапе проектирования часто выполняется путем проведения статистических экспериментов с моделями, адекватно отражающими реакцию ОМС на появление отказов. При этом в большинстве случаев не представляется возможным провести эксперимент с моделью на всем множестве векторов состояния системы $\mathbf{Z} = (z_1, z_2, \ldots, z_n)$, где z_n – состояние работоспособности i-го элемента системы (1 – отказ, 0 – работоспособен), n – их количество, в связи с тем, что такие ОМС имеют большое число составляющих модулей.

Всегда можно подобрать такие $k_{\min}$ и $k_{\max}$, что на всех $\mathbf{Z}$ с весом (по Хеммингу) строго меньше (больше) $k_{\min}$ ($k_{\max}$) система работоспособна (отказала). Это свойство позволяет сократить необходимое количество экспериментов с моделями. Вероятность нахождения системы в множестве состояний, описываемых векторами с весом вне диапазона $k_{\min},\ldots,k_{\max}$, легко определяется известными алгоритмами.

Подход к расчету надежности с использованием указанных свойств рассматривается в [3, 4], при этом статистический эксперимент выполняется последовательно для каждого значения $k = k_{\min},\ldots,k_{\max}$. В [4] для моделирования состояний системы предлагается использование генератора равновесных псевдослучайных двоичных векторов (ГПСВ), основой которого является многоканальный формирователь сигналов, построенный на базе так называемого управляемого регистра сдвига [5]. Принцип работы такой схемы заключается в организации сдвига двоичного вектора в выходном регистре *Reg* под управлением сигналов от задающего ГПСВ, который представляет собой сдвиговый регистр с линейной обратной связью (СРЛОС) и формирует свои равновероятные многоразрядные векторы. Циклический сдвиг вправо разрядов *Reg* осуществляется в каждом такте. При этом если значение некоторого разряда опорного СРЛОС равняется единице, то значение соответствующего разряда *Reg* фиксируется, и этот разряд не участвует в выполнении сдвига.

Недостаток такого формирователя – повторяемость состояний в течение одного периода, что вносит определенную погрешность в расчет надежности.

Структура генератора

В предлагаемом авторами генераторе управляющие сигналы для регистра *Reg* формируются на основе специальным образом выбранных булевых функций задержки, что фактически определяет автономность такого генератора.

Пусть n – количество разрядов регистра, т.е. длина генерируемых векторов, k – вес каждого такого вектора, $x_1, x_2, \ldots, x_n$ – булевы переменные, отражающие состояния соответствующих разрядов регистра, а $\mathbf{X} = (x_1, x_2, \ldots, x_n)$ – генерируемый двоичный вектор.

Назовем функцией задержки f_i булеву функцию, равную единице, если необходимо задержать i-й разряд регистра *Reg*, и нулю в противном случае. Отметим, что в общем случае функ-

ция задержки может зависеть не только от значений разрядов генератора.

Таким образом, значение i-го разряда в следующем $(t+1)$ такте определяется выражением $x_i(t+1) = x_l(t)$, где $l = \max\limits_{1 \le j < i}(j \mid f_j = 0)$, если $\prod\limits_{j=1}^{i-1} f_j = 0$ и $l = \max\limits_{i \le j \le n}(j \mid f_j = 0)$, если $\prod\limits_{j=1}^{i-1} f_j \neq 0$, а f_j – значение функции задержки для j-го разряда генератора в текущем такте t. На рис. 1 представлена схема такого генератора в общем виде.

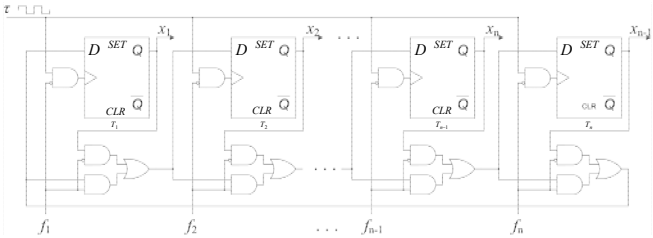

Рис. 1

Основной задачей при построении предлагаемого автономного генератора псевдослучайных векторов постоянного веса, который не повторяет свои состояния в течение одного периода, есть определение функций задержки.

Рассматривается частный случай генератора, у которого фактически определена функция задержки f только для первого разряда, остальные по умолчанию равны нулю.

Свойства генератора

Покажем, что предлагаемый генератор может сформировать все двоичные векторы определенной длины n и весом k.

Пусть B_n – множество всех двоичных векторов длины n, B_n^k – множество всех векторов длины n, вес которых равен k, $B_n^k \subset B_n$.

Обозначим через Sh (*Shift*) операцию циклического сдвига, $Sh\colon B_n^k \to B_n^k$, $Sh(\mathbf{X}) = Sh(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_n, x_1, x_2, \ldots, x_{n-1})$, $Sh^i(\mathbf{X}) = Sh \times (Sh^{i-1}(\mathbf{X}))$, $Sh^1(\mathbf{X}) = Sh(\mathbf{X})$. Для простоты изложения обозначим $Sh^{-1}(\mathbf{X}) = (x_2, \ldots, x_{n-1}, x_n, x_1) = \mathbf{X}'$, т.е. $Sh(\mathbf{X}') = \mathbf{X}$. А операцию циклического сдвига с задержкой первого разряда обозначим как Ds (*delay shift*), $Ds(\mathbf{X}) = Ds(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_1, x_n, x_2, \ldots, x_{n-1})$, $Ds^i(\mathbf{X}) = Ds \times (Ds^{i-1}(\mathbf{X}))$, $Ds^1(\mathbf{X}) = Ds(\mathbf{X})$, $Ds^{-1}(\mathbf{X}) = (x_1, x_3, \ldots, x_{n-1}, x_n, x_2)$.

Очевидно, что решение поставленной ранее задачи, можно свести к доказательству следующего утверждения.

Утверждение 1. Из произвольного вектора $\mathbf{X}_i \in B_n^k$ можно получить любой другой вектор $\mathbf{X}_j \in B_n^k$ путем выполнения ряда операций Ds и/или Sh.

Вначале докажем следующее положение. Пусть имеются векторы $\mathbf{X}_0, \mathbf{X}_\mathrm{T} \in B_n^k$, и $\forall\, l$ ($l \neq \alpha$, $l \neq \beta$): $x_l^0 = x_l^T$, $x_\alpha^0 = x_\beta^T$, $x_\beta^0 = x_\alpha^T$, где x_l^0 – значение l-го элемента вектора $\mathbf{X}_0$, x_l^T – значение l-го элемента вектора $\mathbf{X}_\mathrm{T}$, $\alpha, \beta \in [1,\ldots,n]$. Путем выполнения ряда операций Ds и/или Sh из вектора $\mathbf{X}_0$ можно получить вектор $\mathbf{X}_\mathrm{T}$:

$$(x_1,\ldots,x_{\alpha-1}, \underline{x}_\alpha, x_{\alpha+1},\ldots, x_{\beta-1}, \underline{x}_\beta, x_{\beta+1},\ldots, x_n) = \mathbf{X}_0,$$

$$(\underline{x}_\beta, x_{\beta+1},\ldots, x_n, x_1,\ldots,x_{\alpha-1}, \underline{x}_\alpha, x_{\alpha+1},\ldots, x_{\beta-1}) = Sh^{n-\beta}(\mathbf{X}_0) = \mathbf{X}_1,$$

$$(\underline{x}_\beta, \underline{x}_\alpha, x_{\alpha+1},\ldots, x_{\beta-1}, x_{\beta+1},\ldots, x_n, x_1,\ldots,x_{\alpha-1}) = Ds^{\beta-\alpha+1}(\mathbf{X}_1) = \mathbf{X}_2,$$

$$(\underline{x}_\alpha, x_{\alpha+1},\ldots, x_{\beta-1}, x_{\beta+1},\ldots, x_n, x_1,\ldots,x_{\alpha-1}, \underline{x}_\beta) = Sh^{-1}(\mathbf{X}_2) = \mathbf{X}_3,$$

$$(\underline{x}_\alpha, x_{\beta+1},\ldots, x_n, x_1,\ldots,x_{\alpha-1}, \underline{x}_\beta, x_{\alpha+1},\ldots,x_{\beta-1}) = Ds^{-(\beta-\alpha+1)}(\mathbf{X}_3) = \mathbf{X}_4,$$

$$(x_1,\ldots,x_{\alpha-1}, \underline{x}_\beta, x_{\alpha+1},\ldots, x_{\beta-1}, \underline{x}_\alpha, x_{\beta+1},\ldots,x_n) = Sh^{-(n-\beta)}(\mathbf{X}_4) = \mathbf{X}_5.$$

Полученный вектор $\mathbf{X}_5$ и есть искомый вектор $\mathbf{X}_\mathrm{T}$. Таким образом, можно утверждать, что из любого вектора можно получить другой вектор, отличающийся от исходного перестановкой значений только двух разрядов, путем выполнения последовательности операций Ds и/или Sh.

Далее, пусть имеются векторы $\mathbf{X}_i$, $\mathbf{X}_j \in B_n^k$. Поскольку оба вектора имеют одинаковый вес, то путем последовательной попарной перестановки разрядов вектора $\mathbf{X}_i$, значение которых не совпадает со значениями соответствующих разрядов в $\mathbf{X}_j$, в соответствии с доказанным положением всегда возможно преобразовать вектор $\mathbf{X}_i$ в $\mathbf{X}_j$. Утверждение **1** доказано.

Утверждение **1** подтверждает, что на основе предлагаемого генератора может быть сформирована последовательность векторов, содержа-

щая все векторы из B_n^k. Однако в такой последовательности не исключены повторения. Далее покажем, что избавиться от этого недостатка возможно, но прежде исследуем некоторые свойства множества B_n^k.

Разделение множества векторов на группы

Назовем S-группой упорядоченное множество векторов: $S = \bigcup_{i\in[1,|S|]} Sh^i(\mathbf{X})$, $\mathbf{X} \in S$, при этом упорядочивание векторов осуществляется по операции Sh таким образом, что $\mathbf{X}_{(i+1) \bmod |S|} = Sh(\mathbf{X}_i)$, при этом $\mathbf{X}_{(i+1) \bmod |S|}, \mathbf{X}_i \in S$.

Для заданных n, k количество S-групп обозначим через $NumS(n,k)$, понятно, что $B_n^k = \bigcup_i S_i$, причем $\bigcup_{i,j,j\neq i} S_i \cap S_j = \varnothing$, где $i, j \in [1, NumS(n,k)]$. Пример разделения множества векторов B_6^2 на S-группы для случая $n = 6$, $k = 2$ приведен на рис. 2.

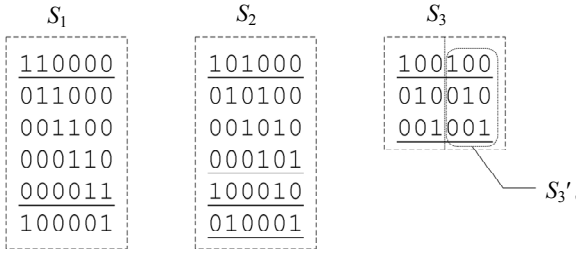

Рис. 2

Здесь и далее обозначим конкатенацию двух векторов (в том числе и единичной длины) символом «+», например, $\mathbf{X} = \sum_{i=1}^{n}(x_i)$.

В большинстве случаев мощность S-группы равна длине вектора, т.е. n, но как это видно из примера (рис. 2), – не всегда: количество векторов в группе S_3 равно трем, а не шести, что объясняется тем, что каждый вектор, принадлежащий S_3, состоит из двух одинаковых фрагментов. При циклическом сдвиге вектора (100100) = (100) + (100), он будет повторно получен через три такта. Понятно, что этот факт усложняет решение задачи.

Рассмотрим понятие повторяющегося фрагмента. Пусть $\mathbf{X} \in B_n^k$, $\mathbf{X} = \sum_{i=1}^{d} \boldsymbol{X}'$, где $\mathbf{X}' \in B_{n'}^{k'}$, $n' = n/d$, $k' = k/d$, где d – общий делитель чисел n и k, тогда $\mathbf{X}'$ – повторяющийся фрагмент, если $\mathbf{X}'$ не может быть записан как многократная конкатенация другого повторяющегося фрагмента (случай $\mathbf{X} = \mathbf{X}'$ вырожденный). Таким образом, если $\mathbf{X}'$ – повторяющийся фрагмент вектора $\mathbf{X} \in S$, то $|S| = n' = |S'|$, $\mathbf{X}' \in S' \subseteq B_{n'}^{k'}$, S, S' – сдвиговые группы. На примере (см. рис. 2), векторы групп S_1 и S_2 есть повторяющиеся фрагменты (вырожденный случай), а каждый вектор из группы S_3 состоит из двух таких фрагментов, т.е. группа S_3' – группа векторов множества B_3^1.

Пусть множество общих делителей величин n и k – $\{d_0, d_1, ..., d_m\}$, причем $d_0 = 1$, а $m + 1$ – мощность множества, пусть $n_i = n/d_i$ – длины соответствующих повторяющихся фрагментов, а количество единиц соответственно $k_i = k/d_i$. Тогда все векторы множества B_n^k, а, собственно, и множество S-групп можно разделять по значению величины n_i. Количество векторов, содержащих повторяющийся фрагмент длины n_i, равняется количеству векторов множества $B_{n_i}^{k_i}$, за исключением не вырожденных повторяющихся фрагментов.

Обозначим как $R(n, k)$ множество различных векторов длины n весом k, которые являются своими повторяющимися фрагментами (вырожденный случай), а $r(n, k)$ – его мощность. Согласно приведенным пояснениям:

$$r(n, k) = C_n^k - \sum_{i=1}^{m} r(n_i, k_i). \qquad (1)$$

По определению $R(n, k)$ состоит из векторов, в которых длина повторяющегося фрагмента равна n, следовательно, каждая S-группа содержит n векторов, и тогда $NumS(n, k) = \sum_{i=0}^{m} r(n_i, k_i)/n_i$. После упрощения получим:

$$NumS(n, k) = \frac{C_n^k + \sum_{i=1}^{m} (d_i - 1) \cdot r(n_i, k_i)}{n}. \qquad (2)$$

Теперь рассмотрим разделение множества B_n^k на группы векторов по операции циклического сдвига с задержкой первого разряда. Назовем D-группой упорядоченную по операции Ds совокупность векторов: $D = \bigcup_{i\in[1,|D|]} \{Ds^i(X)\}$, $\mathbf{X} \in D$. Количество таких групп обозначим $NumD(n,k)$. Таким образом, $B_n^k = \bigcup_i D_i$, причем $\bigcup_{i,j\neq i} D_i \cap D_j = \varnothing$, где $i, j \in [1, NumD(n, k)]$. Пример разделения множества B_7^3 на D-группы для случая $n=7$, $k=3$ приведен на рис. 3.

Рис. 3

Векторы B_n^k можно разбить на два множества по значению первого разряда: векторов, где $x_1=1$, получается C_{n-1}^{k-1}, а векторов с $x_1=0$ получим C_{n-1}^k. Фактически выполнение операции Ds это фиксация первого разряда и одновременно выполнение операции Sh над вектором $(x_2, x_3, \ldots, x_n)$. Таким образом, мощность D-группы равна мощности соответствующей S-группы множества B_{n-1}^{k-1} либо B_{n-1}^k. Следовательно:

$$NumD(n,k) = NumS(n-1,k) + NumS(n-1,k-1). \quad (3)$$

Теперь рассмотрим другую характеристику D-групп. Пусть $\mathbf{X} = (x_1, x_2, \ldots, x_{n-1}, x_n) \in B_n^k$, имеет место:

Утверждение 2. а) если $x_1 \oplus x_n = 1$, то $Sh(\mathrm{X}) \neq Ds(\mathrm{X})$, б) если $x_1 \oplus x_n = 0$, то $Sh(\mathbf{X}) = Ds(\mathbf{X})$.

Действительно, если сравнить $Sh(\mathbf{X}) = (x_n, x_1, x_2, \ldots x_{n-1})$ и $Ds(\mathbf{X}) = (x_1, x_n, x_2, \ldots, x_{n-1})$, увидим, что полученные векторы отличаются только перестановкой первых двух разрядов, следовательно, если в исходном векторе $\mathbf{X}$ значение разрядов $x_1 = x_n$, то $Sh(\mathbf{X}) = Ds(\mathbf{X})$, иначе $Sh(\mathbf{X}) \neq Ds(\mathbf{X})$.

Для простоты изложения назовем векторы $\mathbf{X} = (x_1, x_2, \ldots, x_{n-1}, x_n)$, в которых $x_1 \oplus x_n = 1$, переходными (на рис. 2 и 3 они подчеркнуты). Очевидно, что общее количество переходных векторов равно $2 \cdot C_{n-2}^{k-1}$.

Пусть D_0, D_1 – сдвиговые группы, причем $\forall\, \mathbf{X} \in D_0 \;\; x_1 = 0$, $\forall\, \mathbf{X} \in D_1 \;\; x_1 = 1$. Обозначим $CrsD(D)$ количество переходных векторов в группе D. Вектор $\mathbf{X} \in D_0$ – переходный, если $x_n = 1$, следовательно, $CrsD(D_0) = k \cdot |D_0|/(n-1)$. С другой стороны, количество переходных векторов в группе $D_1 - CrsD(D_1) = (n-k) \times |D_1|/(n-1)$. В общем виде:

$$CrsD(D) = \frac{(n \cdot x_1 - k) \cdot |D|}{(n-1)}. \quad (4)$$

Функция задержки

Определим F как множество функций задержки $f(\mathbf{X})$, таких, что для $\forall\, f(\mathbf{X}) \in F$ период генератора максимален и равен $|B_n^k| = C_n^k$ тактов. Это требование эквивалентно тому, что $\mathbf{X}_i \neq \mathbf{X}_j$ $(i \neq j)$ для любых $i, j \in 1..C_n^k$, i, j – номера векторов в генерируемой последовательности. Далее, если это не оговорено, под обозначением f будем понимать $f(\mathbf{X})$, т.е. функцию задержки, зависящую только от разрядов генератора.

Далее, путем доказательства ряда утверждений покажем, что если функция задержки $f \in F$ существует, то она не зависит от значений первого и последнего разрядов генератора.

Прежде всего заметим, что функция задержки – частично определена, поскольку не определена на множестве векторов $B_n \setminus B_n^k$. Кроме того, покажем, что значение функции $f \in F$ не определено на некоторых векторах множества B_n^k.

Напомним, что при выполнении операции $Ds(\mathbf{X})$ $f(\mathbf{X}) = 1$, и при $Sh(\mathbf{X})$ – $f(\mathbf{X}) = 0$. Согласно п. «*б*» утверждения 2, если $x_1 \oplus x_n = 0$, то $Ds(\mathbf{X}) = Sh(\mathbf{X})$, и, следовательно, результат не зависит от выполняемой операции, а значит и от значения функции на векторе **X.** Это доказывает следующее утверждение.

Утверждение 3. Для $f \in F$, значение $f(x_1, x_2, \ldots, x_{n-1}, x_n)$ можно считать неопределенным, если $x_1 \oplus x_n = 0$.

Пусть $\mathbf{X}_1 \in B_n^k$ – переходный вектор, тогда пусть $\mathbf{X}_2 = Sh(\mathbf{X}_1)$, $\mathbf{X}_4 = Ds(\mathbf{X}_1)$, $\mathbf{X}_3 = Sh^{-1}(\mathbf{X}_4)$. Далее рассмотрим данную четверку попарно различных векторов (рис. 4), где показаны возможные переходы между векторами и группами.

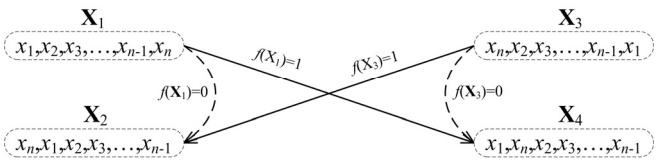

Рис. 4

В общем случае из вектора $\mathbf{X}_i$ можно перейти в вектор $\mathbf{X}_j$, если $\mathbf{X}_j = Ds(\mathbf{X}_i)$ либо $\mathbf{X}_j = Sh(\mathbf{X}_i)$.

Докажем, что $Ds(\mathbf{X}_3) = \mathbf{X}_2$. Если $\mathbf{X}_1 = (x_1, x_2, \ldots, x_{n-1}, x_n)$, тогда $Sh(\mathbf{X}_1) = \mathbf{X}_2 = (x_n, x_1, x_2, \ldots, x_{n-1})$. $Ds(\mathbf{X}_1) = \mathbf{X}_4 = (x_1, x_n, x_2, \ldots, x_{n-1})$, $\mathbf{X}_3 = Sh^{-1}(\mathbf{X}_4) = (x_n, x_2, \ldots, x_{n-1}, x_1)$. Теперь $Ds(\mathbf{X}_3) = (x_n, x_1, x_2, \ldots, x_{n-1})$, и, действительно, полученный вектор равен $\mathbf{X}_2$.

В вектор $\mathbf{X}_2$ можно перейти только из $\mathbf{X}_1$ либо из $\mathbf{X}_3$. Пусть $f'(\mathbf{X}_1) = 0$, $f'(\mathbf{X}_3) = 1$, тогда $Sh(\mathbf{X}_1) = Ds(\mathbf{X}_3) = \mathbf{X}_2$, другими словами, в последовательности генерируемых под воздействием функции f' векторов, вектор $\mathbf{X}_2$ появится дважды, следовательно, $f' \notin F$. Аналогично, если $f'(\mathbf{X}_1) = 1$, $f'(\mathbf{X}_3) = 0$, то $f' \notin F$.

Таким образом, если функция $f \in F$, то $f(\mathbf{X}_1) = f(\mathbf{X}_3)$. Заметим, что векторы $\mathbf{X}_1$ и $\mathbf{X}_3$ отличаются только значениями первого и n-го разрядов. Сказанное подтверждает справедливость:

Утверждение 4. Для любой $f \in F$ выполняется: $f(x_1, x_2, \ldots, x_{n-1}, x_n) = f(x_n, x_2, \ldots, x_{n-1}, x_1)$, если $x_1 \oplus x_n = 1$.

Основываясь на утверждениях 3 и 4, можно сделать вывод, что функция задержки $f \in F$ действительно не зависит от значений разрядов x_1 и x_n векторов $(x_1, x_2, \ldots, x_{n-1}, x_n) \in B_n^k$ (т.е. фактически не зависит от значений первого и последнего разряда генератора).

Пусть $\mathbf{Y} = (x_2, x_3, \ldots, x_{n-1})$. Далее наряду с обозначением $f(\mathbf{X})$, будем использовать $f(\mathbf{Y})$, причем $f(\mathbf{Y}) = f((0) + \mathbf{Y} + (1)) = f((1) + \mathbf{Y} + (0))$, напомним, что знаком «+» обозначена операция конкатенации над векторами.

Исходя из изложенного, можно сказать, что значение функции f фактически не определено на векторах $\mathbf{Y} \in B_{n-2} / B_{n-2}^{k-1}$, что в определенной степени упрощает форму и реализацию функции задержки. На основе этого свойства можно провести упрощение совершенной дизъюнктивной нормальной формы функции и получить ДНФ из термов (соответствующих векторам $\mathbf{Y}$ при $f(\mathbf{Y}) = 1$) следующего вида:

$$K = \prod_{x_i = 1, x_i \in \mathbf{Y}} x_i \quad . \qquad (5)$$

Граф переходов

Для решения вопроса о существовании хотя бы одной функции $f \in F$ введем понятие графа переходов и исследуем его свойства.

Пусть $\Gamma = \{V\Gamma, E\Gamma\}$ – ориентированный маркированный граф, где $V\Gamma = B_n^k$ – множество вершин, а множество дуг $E\Gamma = E\Gamma_S \cup E\Gamma_D$, где $E\Gamma_S = \{<\mathbf{X}, Sh(\mathbf{X})> | \mathbf{X} \in V\Gamma\}$, $E\Gamma_D = \{<\mathbf{X}, Ds(\mathbf{X})> | \mathbf{X} \in V\Gamma\}$. Присвоим дугам из множества $E\Gamma_S$ маркер «0», а дугам $E\Gamma_D$ – маркер «1».

Упростим граф Г путем последовательного стягивания обеих дуг, исходящих из вершин, обозначенных непереходными векторами. Другими словами, обе дуги (с разными маркерами), исходящие из вершины $\mathbf{X}_i$ ($\mathbf{X}_i$ – переходный вектор) и входящие в одну вершину $\mathbf{X}_j$, удаляются, как и вершина $\mathbf{X}_i$. При этом оставшиеся дуги, ранее инцидентные $\mathbf{X}_i$, становятся инцидентными $\mathbf{X}_j$. Обозначим полученный после упрощения граф как Ф.

Понятно, что множество $V\Phi$ вершин Ф-графа есть множество переходных векторов, следовательно, $|V\Phi| = 2 \cdot C_{n-2}^{k-1}$, и, поскольку из каждой вершины исходит две дуги, то общее количество дуг равно $4 \cdot C_{n-2}^{k-1}$. На рис. 5 представлен пример Ф-графа для случая $n = 7$, $k = 3$, на котором отмечены D-группы согласно нумерации на рис. 3.

Пусть имеется некая функция задержки f, причем не обязательно $f \in F$, но f удовлетворяет требованию утверждения 4. Обозначим через $\Phi(f)$ – частичный граф графа Ф, в котором присутствуют только дуги $\mathbf{X}_i \rightarrow \mathbf{X}_j$, маркер ко-

торых равен значению функции $f(\mathbf{X}_i)$. По построению полустепень исхода каждой вершины графа Ф(f) равна единице, также на основе утверждения 4 можно сделать вывод, что полустепень захода равна единице. Следовательно, если Ф(f) связный, то тогда Ф(f) – гамильтонов контур графа Ф. Обход графа Ф по гамильтонову контуру соответствует некой последовательности векторов, причем функция задержки f, порождающая такую последовательность, однозначно принадлежит F. Следовательно, $f \in F$ только тогда, когда Ф(f) – связный, а задачу поиска функции $f \in F$ можно свести к поиску гамильтонова контура в графе Ф при упомянутых ограничениях.

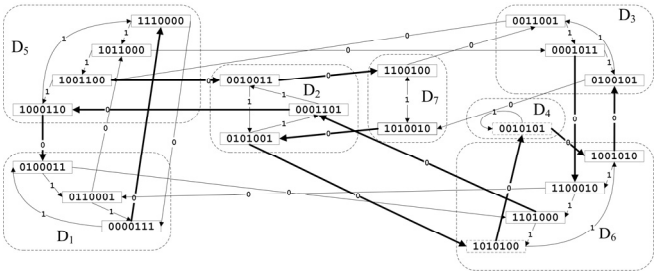

Рис. 5

Понятно, что граф Ф($f = 1$) представляет собой $NumD(n, k)$ циклов, каждый из которых состоит из $CsrD$ вершин, обозначенных переходными векторами одной D-группы, а граф Ф($f = 0$) будет состоять из $NumS(n,k)$ циклов S-групп.

Пусть Γ_D – неориентированный мультиграф, множество вершин $V\Gamma_D$ которого есть множество D-групп, а множество ребер $E\Gamma_D = \{\{D_i, D_{j>i}\} | \mathbf{X} \in D_i,\ Sh(\mathbf{X}) \in D_j\}$. Пусть $\Gamma_D(f)$ – частичный граф графа Γ_D и $E\Gamma_D(f) = \{\{D_i, D_{j>i}\} | \boldsymbol{Y} \in D_i,\ \boldsymbol{Y} \in \in D_i,\ f(\boldsymbol{Y}) = 0\}$, где запись $\boldsymbol{Y} \in D_i$ означает, что $((0) + \boldsymbol{Y} + (1)) \in D_i$ либо $((1) + \boldsymbol{Y} + (0)) \in D_i$. На рис. 6 приведен пример Γ_D графа для $n = 7$, $k = 3$, причем номера D-групп соответствуют нумерации, использованной на рис. 3 и 5.

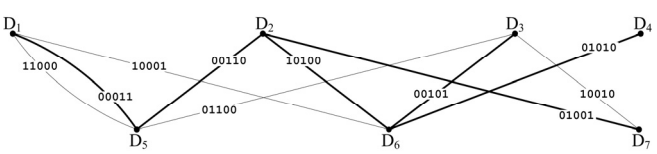

Рис. 6

Очевидно, что на основе Ф-графа можно сформировать граф Γ_D путем слияния вершин одной D-группы и замены соответствующей пары противоположно направленных дуг, маркированных нулем и исходящих из вершин $(x_1, x_2, \ldots, x_{n-1}, x_n)$ и $(x_n, x_2, \ldots, x_{n-1}, x_1)$ графа Ф, одним ребром. Полученные ребра графа Γ_D соответствуют векторам $\mathbf{Y} = (x_2, \ldots, x_{n-1})$. Промаркируем эти ребра значениями соответствующих векторов $\mathbf{Y}$ (см. рис. 6). Аналогичным образом можно на основе графа Ф(f) построить граф $\Gamma_D(f)$.

Основное утверждение

Утверждение 5. $F \neq \varnothing$ для любых n и k.

Для доказательства рассмотрим граф Γ_D, построенный на основе графа Ф (см. рис. 6). Основываясь на утверждении **1**, можно сказать, что граф Ф связный, а следовательно, связным будет и граф Γ_D. Тогда в Γ_D существует остов, покрывающий все его вершины.

Обозначим Γ_O остов графа Γ_D, $E\Gamma_O$ – множество его ребер, определим f такую, что $\forall\ \mathbf{Y} = (x_2, \ldots, x_{n-1}) \in E\Gamma_O$ выполняется $f(\mathbf{Y}) = 0$, и $\forall\ \mathbf{Y} \in B_{n-2}^{k-1} / E\Gamma_O - f(\mathbf{Y}) = 1$. Отметим, что по построению f соответствует требованиям утверждения 4. Покажем, что Ф(f) – гамильтонов контур графа Ф. Для этого, как было показано, достаточно доказать связность графа Ф(f). Пойдем от противного, если Ф(f) – не связный, то не связен и построенный на его основе граф $\Gamma_D(f)$. Но по построению $\Gamma_D(f) = \Gamma_O$, а следовательно, Ф(f) связный. На рис. 6 ребра остова Γ_O и дуги соответствующего ему гамильтонова цикла графа Ф (см. рис. 5) выделены.

Граф Ф – гамильтонов (даже с учетом ограничений утверждения 4), следовательно, существует функция $f \in F$. Утверждение доказано.

Отметим следующие свойства графа Γ_D:

- граф Γ_D – двудольный, одна часть вершин соответствует D-группам из векторов с $x_1 = 1$ (их количество $NumS(n-1, k-1)$), а вторая – D-группам с $x_1 = 0$ (их количество $NumS(n-1, k)$);
- если $k < n$, то всегда существует переход из группы одной доли в группу другой;
- Γ_D граф не содержит петель, поскольку каждое ребро соединяет вершины из разных долей.

Окончание на стр. 58.