УДК 004.052

С.Ю. Мельников

Неавтономные двоичные регистры сдвига, сохраняющие значковые статистические свойства входной последовательности

Рассматриваются классы двоичных регистров сдвига, обеспечивающих равенство относительных частот встречаемости единиц во входной и выходной последовательностях длины N с точностью до $O(1/N)$. Построен критерий принадлежности регистра к этому классу, доказан ряд утверждений о свойствах функций выходов. Доказано, что мощность этого класса растет как двойная экспоненциальная функция от длины регистра.

Ключевые слова: генератор случайных последовательностей; регистр сдвига; граф де Брейна.

При построении генераторов случайных последовательностей часто используется каскадный метод, который заключается в выработке результирующих последовательностей из исходных с помощью автоматных преобразований, реализуемых в так называемых узлах усложнения. К таким узлам можно предъявить требование увеличения линейной сложности и другие требования. Естественным требованием является и то, чтобы равновероятная (по знакам) входная последовательность преобразовывалась бы в равновероятную. Случай, когда в качестве вероятностной модели входной последовательности автомата принимается модель независимых случайных величин, равномерно распределенных на входном алфавите автомата, хорошо изучен (см., например, [1, 2]). Однако последовательности, с которыми обычно приходится иметь дело при построении генераторов случайных последовательностей, «псевдослучайны», и говорить о независимости или об определенном виде зависимости (и вообще пользоваться вероятностными моделями) для их членов можно лишь с определенной степенью условности. С другой стороны, в ряде случаев можно иметь надежные границы для частот встречаемости знаков или n-грамм в этих последовательностях [3].

В статье рассматриваются автоматы, которые гарантируют, что частоты знаков во входной и выходной последовательностях будут не сильно различаться между собой. Пусть $A=(X,Y,Q,h,f)$ – конечный автомат Мили с двоичными входным и выходным алфавитами $X=Y=\{0,1\}$, множеством состояний Q, функцией переходов $h:Q\times X\to Q$, функцией выходов $f:Q\times X\to Y$. Начальное состояние, входную и выходную последовательности автомата обозначим $q^{(0)}\in Q$, $\left(x^{(1)},x^{(2)},\ldots\right)$, $\left(y^{(1)},y^{(2)},\ldots\right)$. Значение предела $\lim\limits_{t\to\infty}\frac{1}{t}\sum\limits_{j=1}^{t}x^{(j)}$, в случае его существования, можно интерпретировать [4] как среднюю частоту единиц в последовательности $\left(x^{(1)},x^{(2)},\ldots\right)$.

Назовем A автоматом, *сохраняющим значковые статистические свойства входной последовательности,* если равенство

$$\lim_{t\to\infty}\frac{1}{t}\sum_{j=1}^{t}x^{(j)}=\lim_{t\to\infty}\frac{1}{t}\sum_{j=1}^{t}y^{(j)} \qquad (1)$$

выполняется для всех $q^{(0)}\in Q$ и всех бесконечных двоичных периодических (возможно, с подходом) последовательностей $\left(x^{(1)},x^{(2)},\ldots\right)$.

Примером автомата, сохраняющего значковые статистические свойства входной последовательности, может служить произвольный конечный автомат Мили с функцией выходов $f_0(q,x)=x$.

Выходная последовательность такого автомата совпадает с входной, что обеспечивает справедливость равенства (1).

Статья является развитием работ [5, 6], в которых изучалось совместное поведение величин $\lim\limits_{t\to\infty}\frac{1}{t}\sum\limits_{j=1}^{t}x^{(j)}$ и $\lim\limits_{t\to\infty}\frac{1}{t}\sum\limits_{j=1}^{t}y^{(j)}$ для различных автоматов. Статья содержит три параграфа. В первом параграфе рассматриваются основные свойства функций выходов регистров сдвига, сохраняющих значковые статистические свойства входной последовательности, во втором доказывается критерий принадлежности регистра исследуемому классу, в третьем даются оценки мощности класса таких регистров.

1. Основные свойства регистров сдвига, сохраняющих значковые статистические свойства входной последовательности. Пусть V_n – пространство n-мерных двоичных векторов, F_n – множество всех булевых функций от n аргументов, $n=1,2,\ldots$. Для булевой функции $f(x_1,x_2,\ldots,x_n)\in F_n$ через $A_f=(X=\{0,1\},V_n,Y=\{0,1\},h,f)$ обозначим автомат Мура, являющийся двоичным проходным регистром сдвига с накопителем размера $n\geq 1$, множеством состояний V_n, функцией переходов h, определяемой по правилу $h((a_1,\ldots,a_n),x)=(a_2,\ldots,a_n,x)$, где $x,a_i\in\{0,1\}$, $i=1,2,\ldots,n$, функцией выходов $f(x_1,x_2,\ldots,x_n)$.

Пример. $n=9$, $f(x_1,x_2,\ldots,x_9)=x_1\oplus x_1x_2\ldots x_8\oplus x_2x_3\ldots x_9$. Ниже (Утверждение 9) показано, что A_f сохраняет значковые статистические свойства входной последовательности. Проводился следующий компьютерный эксперимент. Генерировался случайный двоичный вектор размера 9, который служил начальным состоянием автомата A_f. На вход автомата подавалась случайная двоичная последовательность $x^{(1)},x^{(2)},\ldots,x^{(50)}$ длины 50, генерировалась выходная последовательность $y^{(1)},y^{(2)},\ldots,y^{(50)}$. Вычислялись значения $\sum\limits_{i=1}^{50}x^{(i)}$ и $\sum\limits_{i=1}^{50}y^{(i)}$ сумм единиц во входной и выходной последовательностях. Эксперимент проводился 48 000 000 раз. Результаты эксперимента приведены на рис. 1. По горизонтальным осям откладывались значения $\sum\limits_{i=1}^{50}x^{(i)}$ и $\sum\limits_{i=1}^{50}y^{(i)}$, по вертикальной оси откладывалась частота встречаемости этой пары значений в серии экспериментов. Для генерирования случайных данных использовалась функция RandomInteger пакета Mathematica ver.10.0.

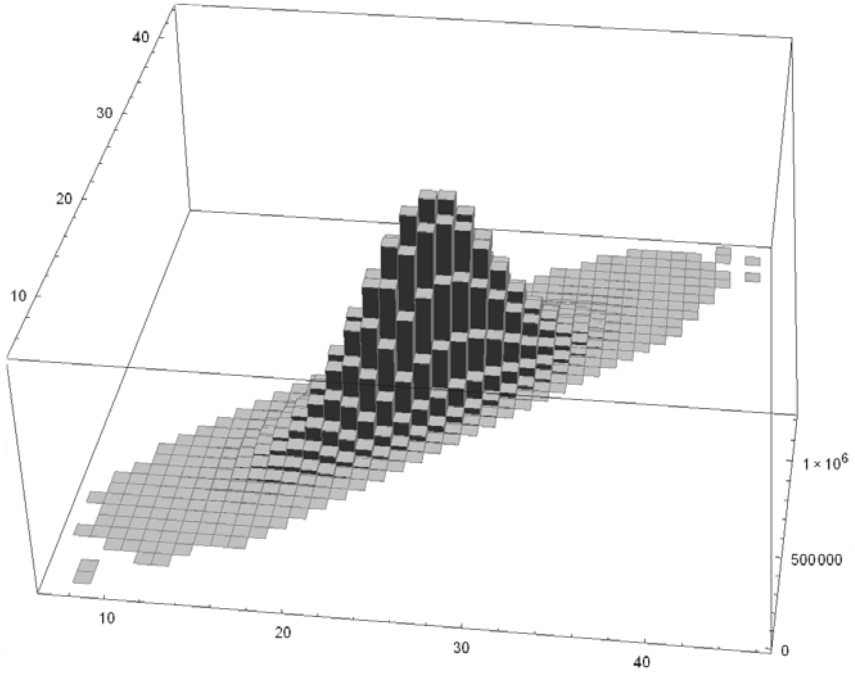

Рис. 1. Результаты эксперимента для функции $x_1\oplus x_1x_2\ldots x_8\oplus x_2x_3\ldots x_9$

На рисунке наглядно видно, что значения $\sum_{i=1}^{50} x^{(i)}$ и $\sum_{i=1}^{50} y^{(i)}$ близки друг к другу, и более того, выполняется неравенство $\left|\sum_{i=1}^{50} x^{(i)} - \sum_{i=1}^{50} y^{(i)}\right| \le \text{const}$.

Множество функций $f(x_1,x_2,...,x_n) \in F_n$, для которых автомат A_f сохраняет значковые статистические свойства входной последовательности, обозначим M_n. В работе [5] показано, что геометрическое место точек $\left(\lim_{t\to\infty} \frac{1}{t}\sum_{j=1}^{t} x^{(j)}, \lim_{t\to\infty} \frac{1}{t}\sum_{j=1}^{t} y^{(j)}\right)$ в квадрате $[0,1]\times[0,1]$ является выпуклым многоугольником. Многоугольники регистров A_f с функциями из этого класса являются в определенном смысле минимальными. Они в точности совпадают с диагональю квадрата, т.е. отрезком $\left[(0,0),(1,1)\right]$.

Замечание 1. На первый взгляд может показаться, что рассматриваемый класс должен состоять из всех равновероятных булевых функций (т.е. тех функций, вес которых равен 2^{n-1}). Однако, как показывает следующий простой пример для функции $x_1 \oplus x_2 \oplus x_3$, это не так. Предположим, что на вход $A_{x_1\oplus x_2\oplus x_3}$ поступает периодическая последовательность с периодом (10010011) длины 8. Очевидно, относительная частота встречаемости единиц в ней равна $1/2$, и даже частоты встречаемости биграмм 00, 01, 10, 11 равны $1/4$. Но выходная последовательность имеет период (11111010), и потому предел относительной частоты встречаемости единиц в выходной последовательности автомата $A_{x_1\oplus x_2\oplus x_3}$ равен $3/4$. ■

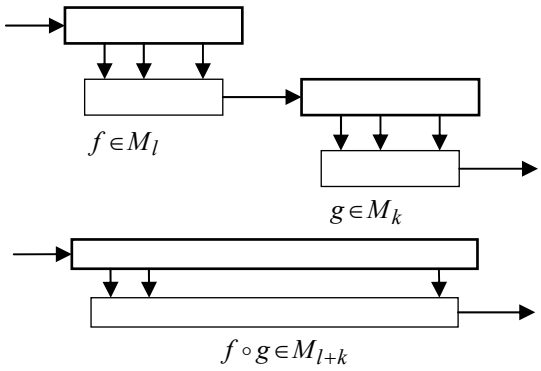

Рис. 2. Композиция двух функций

Замечание 2. Координатные функции $x_1,x_2,...,x_n$ не изменяют статистических свойств входной последовательности и поэтому принадлежат M_n.

Замечание 3. Рассмотрим последовательное соединение двух проходных регистров сдвига (рис. 2). Очевидным образом можно определить операцию композиции функций, которая функциям $f \in M_l$ и $g \in M_k$ ставит в соответствие функцию $f \circ g \in M_{l+k}$, однако далеко не все функции из M_{l+k} представимы в таком виде, т.е. допускают декомпозицию.

Замечание 4. В [6] показано, что все точки графика вероятностной функции ([1]) автомата A_f принадлежат его многоугольнику. Отсюда вытекает, что у любой функции из M_n вероятностная функция является линейной, т.е. полиномом первой степени. Однако не все булевы функции с линейным вероятностным полиномом принадлежат M_n.

Назовем двоичную бесконечную последовательность $\chi = \left(x^{(1)},x^{(2)},...\right)$ *1-равновероятной* в случае, когда существует предел $\lim_{t\to\infty} \frac{1}{t}\sum_{j=1}^{t} x^{(j)}$ и

$$\lim_{t\to\infty} \frac{1}{t}\sum_{j=1}^{t} x^{(j)} = \frac{1}{2}.$$

Оказывается, «почти все» двоичные бесконечные последовательности являются 1-равновероятными.

Утверждение 1. [7, гл. 2]. Пусть $(w_0,w_1,...)$ – представление действительного числа $\lambda \in (0,1)$ в виде двоичной бесконечной дроби. (В случае неоднозначного представления выбираем последова-

тельность с бесконечным количеством нулей). Мера Лебега множества тех $\lambda \in (0,1)$, для которых последовательность $(w_0, w_1, ...)$ является 1-равновероятной, равна 1.

К регистрам сдвига A_f, которые могут использоваться в качестве узлов генераторов псевдослучайных чисел для преобразования двоичных последовательностей, логично предъявить требование, чтобы 1-равновероятные последовательности перерабатывались бы в 1-равновероятные. Такое требование представляется вполне естественным и особенно важным в тех случаях, когда имеются определенные сомнения в независимости (в вероятностном смысле) членов входной последовательности.

Ниже показано, что класс M_n – единственный (с точностью до инверсии) класс, удовлетворяющий сформулированному выше требованию, в следующем смысле. Пусть $f(0,0,...,0) = 0$. Если $f \notin M_n$, то существует такая 1-равновероятная последовательность $\chi = \left(x^{(1)}, x^{(2)}, ...\right)$, для которой $\lim\limits_{t\to\infty} \frac{1}{t} \sum\limits_{j=1}^{t} x^{(j)} = \frac{1}{2}$, но $\lim\limits_{t\to\infty} \frac{1}{t} \sum\limits_{j=1}^{t} f\left(x^{(j)}, ..., x^{(j+n-1)}\right) \neq \frac{1}{2}$. Иными словами, либо автомат A_f сохраняет (инвертирует) значковые свойства входа для любой последовательности χ, либо для некоторой 1-равновероятной входной последовательности он их не сохраняет.

Утверждение 2. Пусть $f \notin M_n$, $f(0,0,...,0) = 0$, $n = 2,3,...$ Существует 1-равновероятная последовательность $\left(x^{(1)}, x^{(2)}, ...\right)$, для которой определен предел $\lim\limits_{t\to\infty} \frac{1}{t} \sum\limits_{j=1}^{t} f\left(x^{(j)}, ..., x^{(j+n-1)}\right)$ и

$$\left| \lim_{t\to\infty} \frac{1}{t} \sum_{j=1}^{t} f\left(x^{(j)}, ..., x^{(j+n-1)}\right) - \frac{1}{2} \right| \geq \frac{1}{2} 4^{-n}.$$

Доказательство. Согласно результатам [6] для A_f определен выпуклый многоугольник R_f, все вершины которого имеют вид $\left(\frac{i}{N}, \frac{j}{M}\right)$, где $1 \leq i \leq M \leq 2^n$, $1 \leq j \leq N \leq 2^n$. Отсюда вытекает, что если $f \notin M_n$, то в R_f найдется точка $\left(\frac{i}{N}, \frac{j}{M}\right)$ с $\frac{i}{N} \neq \frac{j}{M}$. Заметим, что $\min_{1\leq i,j,N,M\leq 2^n} \left| \frac{i}{N} - \frac{j}{M} \right| \geq \frac{1}{2^n (2^n - 1)} > 1/4^n, n \geq 2.$

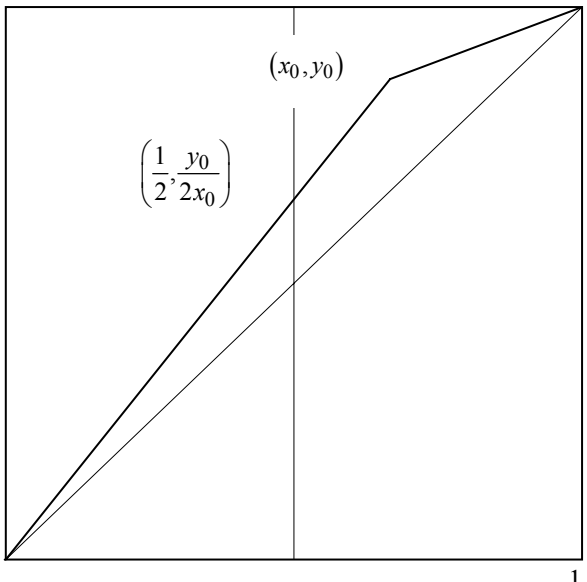

Рис. 3. Существование в R_f точки с абсциссой $\frac{1}{2}$

В силу геометрических соображений (см. рис. 3) в R_f существует точка с абсциссой $1/2$, ордината которой отличается от $1/2$ больше чем на $1/2*4^{-n}$. Согласно [8] это и означает существование требуемой последовательности.

Графом переходов автомата A_f является двоичный граф G_n де Брейна степени n, т.е. ориентированный граф с множеством вершин V_n, содержащий дугу, выходящую из вершины $(a_1,a_2,...,a_n)$ и заходящую в вершину $(b_1,b_2,...,b_n)$ в том и только в том случае, когда $(a_2,a_3,...,a_n)=(b_1,b_2,...,b_{n-1})$. Будем считать, что такая дуга помечена «входным» символом b_n и «выходным» символом $f(a_1,a_2,...,a_n)$. Через $C(G_n)$ обозначим множество всех простых циклов в G_n. Следующее утверждение вытекает из теоремы 1 работы [5].

Утверждение 3. Регистр A_f сохраняет значковые свойства входной последовательности тогда и только тогда, когда f сохраняет вес каждого цикла c графа G_n де Брейна на 2^n вершинах, т.е.

$$\|f/c\| = \sum_{(x_1,x_2,...x_n)\in c} f(x_1,x_2,...,x_n) = \sum_{(x_1,x_2,...x_n)\in c} x_1 = \|c\|,\ c\in C(G_n),$$

где суммирование производится по всем двоичным векторам – вершинам цикла c.

Утверждение 4. Пусть $f\in M_n$, на вход регистра A_f с начальным состоянием $\alpha^{(0)}\in V_n$ поступает двоичная последовательность $x^{(1)},x^{(2)},...,x^{(N)}$, снимается выходная последовательность $y^{(1)},y^{(2)},...,y^{(N)}$, $N\ge 1$. Тогда

$$\left|\sum_{i=1}^{N} x^{(i)} - \sum_{i=1}^{N} y^{(i)}\right| \le n.$$

Доказательство. Через $\alpha^{(N)}$ обозначим состояние, в которое перешел автомат A_f после обработки последовательности $x^{(1)},x^{(2)},...,x^{(N)}$, $\alpha^{(N)}\in V_n$. Пусть $\varepsilon^{(1)},\varepsilon^{(2)},...,\varepsilon^{(k)}$, $k\ge 0$ – кратчайшая входная двоичная последовательность, переводящая автомат A_f из состояния $\alpha^{(N)}$ в состояние $\alpha^{(0)}$. Соответствующую выходную последовательность обозначим $\delta^{(1)},\delta^{(2)},...,\delta^{(k)}$. Тогда входная последовательность $x^{(1)},x^{(2)},...,x^{(N)},\varepsilon^{(1)},\varepsilon^{(2)},...,\varepsilon^{(k)}$ переводит A_f из состояния $\alpha^{(0)}$ в $\alpha^{(0)}$. Поэтому она может быть представлена в виде последовательности циклов в графе переходов автомата. Поэтому согласно предыдущему утверждению

$$\sum_{i=1}^{N} x^{(i)} + \sum_{i=1}^{k} \varepsilon^{(i)} = \sum_{i=1}^{N} y^{(i)} + \sum_{i=1}^{k} \delta^{(i)}.$$

Тогда $\sum_{i=1}^{N} x^{(i)} - \sum_{i=1}^{N} y^{(i)} = \sum_{i=1}^{k} \delta^{(i)} - \sum_{i=1}^{k} \varepsilon^{(i)}$. Заметим, что k не превосходит диаметра графа автомата A_f, поэтому $k\le n$, и тогда $0\le \sum_{i=1}^{k} \varepsilon^{(i)}, \sum_{i=1}^{k} \delta^{(i)} \le n$. Отсюда вытекает доказываемое неравенство.

Утверждение 5. Если $f\in M_n$, то:

1) $f(0,0,...,0)=0$, $f(1,1,...,1)=1$.

2) $f(0,1,0,1...)+f(1,0,1,0,...)=1$.

3) f – равновероятна.

Доказательство. Эти свойства вытекают из того, что функции из класса M_n сохраняют вес произвольного цикла графа G_n. Для доказательства первого пункта достаточно рассмотреть два цикла, образованные петлями в нулевой и единичной вершинах, для второго – цикл (01), для третьего – полный цикл в графе.

Утверждение 6. Функции $f(x_1,x_2,...,x_n)$, $f(x_n,x_{n-1},...,x_1)$ и $\overline{f}(\overline{x_1},\overline{x_2},...,\overline{x_n})$ принадлежат или не принадлежат M_n одновременно.

Доказательство. Обозначим перечисленные функции f, g, h. Функции f и h обладают центрально-симметричными относительно центра квадрата многоугольниками ([6]), и поэтому принадлежат или не принадлежат M_n одновременно. Пусть теперь $f \in M_n$. Покажем, что и $g \in M_n$. Пусть c – произвольный цикл в G_n и $(\varepsilon_1,\varepsilon_2,...,\varepsilon_l)$ – его двоичная запись. Тогда

$$\|f/c\| = \sum f(x_1,x_2,...x_n) = \|c\| = \sum_{i=1}^{l} \varepsilon_i .$$

Через c' обозначим «обратный» к c цикл с двоичной записью $(\varepsilon_l,\varepsilon_{l-1},...,\varepsilon_1)$. Очевидно,

$$\|g/c'\| = \|f/c\| = \sum_{i=1}^{l} \varepsilon_i = \|c\| = \|c'\|.$$

Поскольку соответствие между циклами и «обратными» к ним взаимно однозначно, в качестве c' может выступать произвольный цикл графа G_n. Это означает, что $g \in M_n$. Аналогично можно показать, что из того, что $g \in M_n$, вытекает $f \in M_n$.

Утверждение 7. Пусть $f \in M_n$ и f отлична от координатных функций. Тогда f является нелинейной по всем аргументам, от которых она существенно зависит.

Доказательство. Предположим противное: пусть $f = g \oplus x_i$, где функция g не зависит от x_i. Поскольку $f \in M_n$, для произвольного цикла c графа G_n должно выполняться равенство

$$\left\| g \oplus x_i \Big/ c \right\| = \|c\|.$$

Множество векторов, составляющих цикл c, представим в виде объединения двух множеств $c = c^0 \cup c^1$, где c^0 – векторы из c, i-я координата которых равна нулю, c^1 – векторы из c, i-я координата которых равна 1. Преобразуем последнее равенство:

$$\sum_{\alpha \in c^0} (g(\alpha) \oplus x_i) + \sum_{\alpha \in c^1} (g(\alpha) \oplus x_i) = \|c\|,$$

$$\sum_{\alpha \in c^0} g(\alpha) + \|c\| - \sum_{\alpha \in c^1} g(\alpha) = \|c\|,$$

$$\sum_{\alpha \in c^0} g(\alpha) = \sum_{\alpha \in c^1} g(\alpha).$$

Покажем, что отсюда вытекает, что функция g тождественно равна нулю. Взяв в качестве c петлю графа G_n в нулевой вершине, получим $g(0,0,...,0) = 0$. Рассмотрим цикл веса 1 длины n. Имеем:

$$2g(0,...,0,1,0,...,0) = g(1,0,...,0) + g(0,1,0,...,0) + \ldots + g(0,0,...,1)$$

(здесь единица в аргументах функции в левой части равенства стоит на i-м месте). Поскольку g не зависит от x_i, левая часть равна нулю. Отсюда следует, что функция g равна нулю на векторах веса 0 и 1. Доказательство того, что g тождественно равна нулю, завершим индукцией по весу вектора-аргумента функции g. Пусть $g(\alpha) = 0$ для всех α таких, что $\|\alpha\| < k$. Для произвольного вектора β веса k рассмотрим цикл c_β в G_n, порожденный всеми сдвигами β. Имеем: $\left\|g/C_\beta^0\right\| = \left\|g/C_\beta^1\right\|$. Правая часть последнего равенства совпадает с весом функции f на некотором множестве векторов веса $k-1$ и по предположению индукции равна нулю. Следовательно, $g(\beta) = 0$.

2. Критерий принадлежности функции классу M_n. Под матрицей инцидентности орграфа (V,E) с множеством вершин V и множеством дуг E мы будем понимать матрицу размера $|E| \times |V|$, общий элемент которой имеет вид

$$b_{ij}=\begin{cases}1, \text{ если } i\text{-я дуга выходит из } j\text{-й вершины},\\ -1, \text{ если } i\text{-я дуга заходит в } j\text{-ю вершину},\\ 0, \text{ если } i\text{-я дуга не инцидентна } j\text{-й вершине},\end{cases}$$

кроме того, для определенности положим, что строка, соответствующая петле графа, является нулевой.

Пусть $\mathbf{B}_n$ – $2^{n+1}\times 2^n$ – матрица инцидентности графа де Брейна G_n.

Пусть $\tilde{G}_n$ – граф, получаемый из графа G_n переориентацией всех его дуг, помеченных векторами $(1,a_2,a_3,...,a_n)$, а $\tilde{\mathbf{B}}_n$ – его матрица инцидентности. Матрицы $\mathbf{B}_n$ и $\tilde{\mathbf{B}}_n$ связаны соотношением

$$\tilde{\mathbf{B}}_n=\begin{bmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1\end{bmatrix}\mathbf{B}_n,$$

где матрица-множитель перед $\mathbf{B}_n$ имеет размер $2^{n+1}\times 2^{n+1}$.

Пусть Θ_n обозначает количество различных циклов в графе G_n. Через $\mathbf{C}_n$ обозначим $(0,1)$ – матрицу размера $\Theta_n\times 2^{n+1}$, (i,j)-й элемент которой имеет вид:

$$c_{ij}=\begin{cases}1, & \text{если } i\text{-й цикл проходит через } j\text{-ю дугу},\\ 0, & \text{в противном случае.}\end{cases}$$

Лемма. Справедливы соотношения:

1) $\operatorname{rank}\mathbf{C}_n=2^n+1$;

2) $\operatorname{rank}\mathbf{B}_n=2^n-1$. Столбцы $\mathbf{B}_n^{(2)},\mathbf{B}_n^{(3)},...,\mathbf{B}_n^{(2^n)}$ линейно независимы;

3) $\mathbf{C}_n\mathbf{B}_n=\mathbf{0}$.

Доказательство леммы можно провести аналогично доказательствам известных [9] теоретико-графовых результатов об ортогональности цикломатической матрицы.

Через $\mathbf{f}$ будем обозначать вектор-столбец табличного задания функции $f(x_1,x_2,...,x_n)$:

$$\mathbf{f}=\left(f(0,0,...,0),f(0,0,...,1),...,f(1,1,...,1)\right)^T.$$

Основным результатом параграфа является

Утверждение 8. Пусть $f_0\in M_n$. Для каждой функции $f\in M_n$ существует единственный 2^{n-1}–мерный вектор $\mathbf{d}$ с условием $\mathbf{d}(0,0,...,0)=0$ такой, что

$$\mathbf{f}=\mathbf{B}_{n-1}\mathbf{d}+\mathbf{f}_0. \qquad (2)$$

Доказательство. Из утверждения 3 следует, что $f\in M_n$ тогда и только тогда, когда

$$\mathbf{C}_{n-1}\mathbf{f}=\mathbf{c}, \qquad (3)$$

где $\mathbf{c}=\left(c_1,c_2,...,c_{\Theta_{n-1}}\right)^T$, c_i – вес i-го цикла, $i=1,2,...,\Theta_n$. Соотношение (3) можно рассматривать как систему линейных уравнений относительно вектора неизвестных $\mathbf{f}$. Теперь, если $f_0\in M_n$, то $\mathbf{f}_0$ – частное решение этой системы. В силу леммы общее решение (3) имеет вид

$$\mathbf{f}=\mathbf{B}_{n-1}^{(2)}d_2+\mathbf{B}_{n-1}^{(3)}d_3+...+\mathbf{B}_{n-1}^{(2^{n-1})}d_{2^{n-1}}+\mathbf{f}_0,$$

где действительные коэффициенты d_i определены однозначно. Отсюда следует (2).

С другой стороны, если $\mathbf{d}$ удовлетворяет условию (2), то, применяя последнее утверждение леммы, получаем

$$\mathbf{C}_{n-1}\mathbf{f}=\mathbf{C}_{n-1}\left(\mathbf{B}_{n-1}\mathbf{d}+\mathbf{f}_0\right)=\mathbf{C}_{n-1}\mathbf{f}_0=\mathbf{c},$$

т.е. $\mathbf{f}$ удовлетворяет равенству (3).

Однозначно определенный в утверждении 8 вектор $\mathbf{d}$ назовем базисным вектором функции $f\in M_n$ относительно f_0. Вектор, базисный относительно функции $x_1\in F_n$, назовем базисным век-

тором. Нетрудно видеть, что базисными для координатных функций $x_1,x_2,...,x_n \in F_n$ являются векторы $\mathbf{0},\mathbf{y}_1,\mathbf{y}_1+\mathbf{y}_2,...,\mathbf{y}_1+...+\mathbf{y}_{n-2}+\mathbf{y}_{n-1}$ соответственно. Здесь $\mathbf{y}_i$ – вектор-столбец табличного задания координатной функции $x_i \in F_{n-1}$.

Утверждение 9. Базисный для функции $f \in M_n$ вектор является целочисленным, его координаты удовлетворяют неравенствам

$$0 \le \mathbf{d}(a_1,a_2,...,a_{n-1}) \le \sum_{i=1}^{n-1} a_i \,. \qquad (4)$$

Доказательство. Целочисленность координат вектора $\mathbf{d}$ следует из того, что квадратная размера $2^{n-1}-1$ подматрица матрицы $\mathbf{B}_{n-1}$ с множеством строк $\{(0,a_2,...,a_n),(a_2,...,a_n) \ne (0,0,...,0)\}$ и столбцов $\{(b_1,b_2,...,b_{n-1}),(b_1,b_2,...,b_{n-1}) \ne (0,0,...,0)\}$ является целочисленной нижнетреугольной матрицей с единичными элементами на главной диагонали (и, следовательно, обратимой над кольцом целых чисел). Такой вид $(0,1)$-матрицы $\mathbf{B}_{n-1}$, как нетрудно видеть, обеспечивает и неотрицательность координат вектора $\mathbf{d}$.

Для доказательства правой части неравенства (4) введем в рассмотрение подстановочную матрицу $\mathbf{S}_n$ размера $2^n \times 2^n$, соответствующую преобразованию по закону

$$\mathbf{S}_n : (a_1,a_2,...,a_n) \to (a_n,a_{n-1},...,a_1) \,.$$

Несложно убедиться в справедливости матричного равенства

$$\mathbf{S}_n\mathbf{B}_{n-1} = -\mathbf{B}_{n-1}\mathbf{S}_{n-1} \,.$$

Пусть $g(x_1,x_2,...,x_n) = f(x_n,x_{n-1},...,x_1) \in M_n$. Через $\mathbf{d}_f$ и $\mathbf{d}_g$ обозначим базисные векторы функций f и g соответственно. Пусть, кроме того, $\mathbf{y} = \mathbf{y}_1 + \mathbf{y}_2 + ... + \mathbf{y}_{n-1}$. Из цепочки равенств $\mathbf{f} = \mathbf{S}_n\mathbf{g} = \mathbf{S}_n(\mathbf{B}_{n-1}\mathbf{d}_g + \mathbf{x}_1) = \mathbf{x}_n - \mathbf{B}_{n-1}\mathbf{S}_{n-1}\mathbf{d}_g = \mathbf{B}_{n-1}(\mathbf{y} - \mathbf{S}_{n-1}\mathbf{d}_g) + \mathbf{x}_1$ следует, что

$$\mathbf{d}_f = \mathbf{y} - \mathbf{S}_{n-1}\mathbf{d}_g \,.$$

Теперь, поскольку $\mathbf{d}_g \ge \mathbf{0}$, получаем $\mathbf{d}_f \le \mathbf{y}$, что завершает доказательство.

Утверждение 10. Функции $f(x_1,x_2,...,x_n) = x_1 \oplus x_1x_2...x_{n-1} \oplus x_2...x_{n-1}x_n$ и $g(x_1,x_2,...,x_n) = x_n \oplus x_1x_2...x_{n-1} \oplus x_2...x_{n-1}x_n$ принадлежат классу M_n.

Доказательство. Базисный вектор для функции $f(x_1,x_2,...,x_n) = x_1 \oplus x_1x_2...x_{n-1} \oplus x_2...x_{n-1}x_n$ имеет вид $(0,0,...,0,1)$, в чем легко убедиться, проверив равенство (2). Для доказательства того, что $g \in M_n$, можно воспользоваться утверждением 6.

3. Оценки мощности класса M_n. Приведем таблицу мощностей классов M_n при начальных n (табл. 1).

Таблица 1

Мощности классов M_n для нескольких первых n

n	1	2	3	4	5	6
$\lvert M_n \rvert$	1	2	5	22	428	184256

Верхняя граница.

Утверждение 11. Справедливо неравенство

$$\lvert M_n \rvert \le 2^{2^{n-1}-1},\ n = 1,2,... \,. \qquad (5)$$

Доказательство. Заметим, что существует взаимно-однозначное соответствие между векторами табличного задания функций из M_n и булевыми векторами, представимыми в виде $\mathbf{l} = \tilde{\mathbf{B}}_{n-1}\mathbf{d}$, $\mathbf{d} \in R^{2^{n-1}}$. Это соответствие задается формулой

$$\mathbf{f} = \mathbf{l} \oplus \mathbf{x}_1 \,.$$

Воспользовавшись леммой предыдущего параграфа, нетрудно доказать, что подпространство над полем действительных чисел $\langle \mathbf{l} \rangle$, натянутое на векторы-столбцы матрицы $\tilde{\mathbf{B}}_{n-1}$, имеет ранг $2^{n-1}-1$. Следовательно, число $(0,1)$-векторов в этом подпространстве не превосходит $2^{2^{n-1}-1}$.

Нижняя граница (I).

Множество базисных векторов функций из M_n имеет сложную структуру. В этом пункте мы выделим достаточно простое подмножество базисных векторов и получим рекуррентную формулу для его мощности.

Утверждение 12. Количество r_n ненулевых базисных векторов вида

$$\left(0,0,...,0,\varepsilon_1,\varepsilon_2,...,\varepsilon_{2^{n-2}}\right),\ \varepsilon_i=0,1,\ i=1,2,...,2^{n-2}$$

подчиняется рекуррентному соотношению

$$r_n=r_{n-1}^2+1,\ n=2,3,...,\ \text{где}\ r_1=0.$$

Доказательство. Среди векторов рассматриваемого вида будем выделять множество тех, для которых вектор $\mathbf{l}=\tilde{\mathbf{B}}_{n-1}\mathbf{d}$ является булевым. Заметим, что при $a_1a_2=0$ структура матрицы $\tilde{\mathbf{B}}_n$ гарантирует булевость $(a_1,a_2,...,a_n)$-й координаты вектора $\mathbf{l}$. Поэтому условие булевости вектора $\mathbf{l}$ в рассматриваемом случае равносильно условию булевости вектора $\mathbf{D}_{n-2}\boldsymbol{\varepsilon}_{n-2}$, где $\boldsymbol{\varepsilon}_{n-2}\in V^{n-2}$, а $\mathbf{D}_{n-2}$ – подматрица матрицы $\tilde{\mathbf{B}}_{n-1}$ с множеством строк $\{(1,1,a_1,a_2,...,a_{n-2}),a_i=0,1\}$ и столбцов $\{(1,b_1,b_2,...,b_{n-1}),b_i=0,1\}$. Матрица $\mathbf{D}_{n-2}$, очевидно, является матрицей инцидентности графа полного двоичного дерева на 2^{n-2} вершинах с петлей в корне.

Можно считать, что вершина u данного графа помечена числом $\varepsilon(u)$. Возникающую при этом разметку вершин графа назовем допустимой, если существование дуги из вершины u в вершину v приводит к соотношению $\varepsilon(u)-\varepsilon(v)\in\{0,1\}$. Как нетрудно видеть, разметка является допустимой тогда и только тогда, когда $\mathbf{D}_{n-2}\boldsymbol{\varepsilon}_{n-2}$ – булев вектор. Обозначим число допустимых разметок r_n. Разбивая класс допустимых разметок на два подкласса в зависимости от значения $\varepsilon(1,1,...,1,0)$, приходим к доказываемой формуле $r_n=r_{n-1}^2+1$.

Следствие. $|M_n|\geq r_n,\ n=2,3,...$.

Нижняя граница (II).

В этом пункте рассматривается подмножество базисных векторов более сложного вида и выводятся рекуррентные соотношения для его мощности.

Пусть $G=(V,E)$ – орграф. Для $J\subset V$ через $G(J)$ обозначим подмножество вершин графа, смежных хотя бы с одной вершиной из J, т.е. множество концов дуг, имеющих своим началом вершины из J. Пусть u_k – количество таких подмножеств $J\subset V$, для которых $|G(J)|=k$, $k=0,1,...$. Рассмотрим производящую функцию $U_G(z)=\sum_{k=0}^{|V|}u_kz^k$, которую мы назовем производящей функцией числа прообразов графового отображения. Для графа $\tilde{G}_n$ такую функцию будем обозначать $U_n(z)$.

Утверждение 13. Число s_n двоичных базисных векторов вида

$$\left(0,0,...,0,\varepsilon(0,0,...,0),\varepsilon(0,0,...,0,1),...,\varepsilon(1,1,...,1),1,1,...,1\right),$$

где первые 2^{n-3} координат вектора равны 0, а последние 2^{n-3} координат равны 1, вычисляется по формуле

$$s_n=2^{2^{n-3}}U_{n-3}\left(\frac{1}{2}\right),\ n=3,4,... \qquad (6)$$

Доказательство. Нетрудно видеть, что s_n равно количеству допустимых (в указанном выше смысле) разметок графа Γ на 2^{n-2} вершинах, который является ограничением $\tilde{G}_{n-1}$ на множестве вершин $V'\cup V''$, где $V'=\{(0,1,\varepsilon_1,\varepsilon_2,...,\varepsilon_{n-3}),\varepsilon_i=0,1\}$, $V''=\{(1,0,\varepsilon_1,\varepsilon_2,...,\varepsilon_{n-3}),\varepsilon_i=0,1\}$. Очевидно, граф Γ является двудольным, все дуги направлены из множества V' в множество V''. Для $J\subset V'$ через

$\Gamma(J)$ обозначим множество вершин из V'', инцидентных J. Пусть I – множество вершин из V', которые помечены единицей. Если разметка графа допустима, то все вершины из $\Gamma(I)$ должны быть помечены единицей, а остальные вершины V'' могут быть помечены произвольно нулем или единицей. Таким образом,

$$s_n = \sum_{I\subset V'} 2^{|V''\setminus\Gamma(I)|} = 2^{2^{n-3}} \sum_{I\subset V'} \left(\frac{1}{2}\right)^{|\Gamma(I)|},\ n=3,4,\ldots.$$

Для множества вершин $I=\left\{\left(0,1,\varepsilon_1^{(k)},\varepsilon_2^{(k)},\ldots,\varepsilon_{n-3}^{(k)}\right),k=1,2,\ldots,|I|\right\}$ графа Γ через I^* обозначим соответствующее I множество вершин в графе $\tilde{G}_{n-3}$:

$$I^*=\left\{\left(\varepsilon_1^{(k)},\varepsilon_2^{(k)},\ldots,\varepsilon_{n-3}^{(k)}\right),k=1,2,\ldots,|I|\right\}.$$

Нетрудно убедиться, что $|\Gamma(I)|=\left|\tilde{G}_{n-1}\left(I^*\right)\right|$.

Для получения рекуррентных соотношений для функции $U_n(z)$ нам потребуется ввести ряд обозначений. Занумеруем вершины графа $\tilde{G}_n$ числами от 0 до 2^n-1 стандартным способом: вершине $(a_1,a_2,\ldots,a_n)$ припишем номер $\sum_{i=1}^{n} a_i 2^{n-i}$, что соответствует лексикографическому порядку на множестве V^n. Символами $[\![0]\!]$, $[\![1]\!]$, $[\![01]\!]$, $[\![10]\!]$ будем обозначать номера n-мерных двоичных векторов (0,0,...,0), (1,1,...,1), (0,1,0,1,...) и (1,0,1,0,...) соответственно. Запись $\overbrace{a,b}$ ($a\le b$) будет означать множество всех вершин графа $\tilde{G}_n$ с номерами i, $a\le i\le b$. Рассмотрим матрицу смежности графа $\tilde{G}_n$. Ее структура различна при четных и нечетных n.

Далее обозначим:

$t_{k,n}^{(0)}$ – количество подмножеств J множества $\overbrace{0,[\![01]\!]-2}$ при четном n, и множества $\overbrace{0,[\![01]\!]-1}$ при нечетном n, для которых $\left|\tilde{G}_n(J)\right|=k$.

$t_{k,n}^{(1)}$ – при четном n: количество подмножеств J множества $\overbrace{0,[\![01]\!]-1}$ с условием $[\![01]\!]-1\in J$, для которых $\left|\tilde{G}_n(J)\right|=k$, при нечетном n: количество подмножеств J множества $\overbrace{0,[\![01]\!]-1}$ с условием $[\![10]\!]-1\in\widetilde{G}_n(J)$, для которых $\left|\tilde{G}_n(J)\right|=k$.

$q_{k,n}^{(0)}$ – количество подмножеств J множества $\overbrace{[\![01]\!]+1,1}$ при четном n и множества $\overbrace{[\![01]\!]+2,1}$ при нечетном n, для которых $\left|\tilde{G}_n(J)\right|=k$.

$q_{k,n}^{(1)}$ – при четном n: количество подмножеств J множества $\overbrace{[\![01]\!]+1,1}$ с условием $[\![10]\!]+1\in G_n(J)$, для которых $\left|\tilde{G}_n(J)\right|=k$, при нечетном n: количество подмножеств J множества $\overbrace{[\![01]\!]+1,1}$ с условием $[\![01]\!]+1\in J$, для которых $\left|\tilde{G}_n(J)\right|=k$.

$u_{k,n}$ – количество подмножеств J множества $\overbrace{[\![0]\!],[\![1]\!]}$, для которых $\left|\tilde{G}_n(J)\right|=k$.

Пусть $T_n^{(i)}(z)=\sum_k t_{k,n}^{(i)} z^k$, $Q_n^{(i)}(z)=\sum_k q_{k,n}^{(i)} z^k$, $i=0,1$, $n=3,4,\ldots$ – производящие функции введенных выше последовательностей. Тогда $U_n(z)=\sum_k u_{k,n} z^k$. Для подсчета величины $u_{k,n}$ при четном n рассмотрим четыре возможных случая взаимного расположения точек $[\![01]\!]$, $[\![01]\!]-1$ и множества J.

1-й случай. $[\![01]\!] \notin J$, $[\![01]\!]-1 \notin J$. Имеем: $u_{k,n} = \sum_j t^{(0)}_{j,n} q^{(0)}_{k-j,n}$.

2-й случай. $[\![01]\!] \notin J$, $[\![01]\!]-1 \in J$. Имеем: $u_{k,n} = 1 + \sum_j t^{(0)}_{j,n} q^{(1)}_{k-j,n}$.

3-й случай. $[\![01]\!] \in J$, $[\![01]\!]-1 \notin J$. Имеем: $u_{k,n} = 1 + \sum_j t^{(1)}_{j,n} q^{(0)}_{k-j,n}$.

4-й случай. $[\![01]\!] \in J$, $[\![01]\!]-1 \in J$. Имеем: $u_{k,n} = 1 + \sum_j t^{(1)}_{j,n} q^{(1)}_{k-j,n}$.

Слагаемое 1 в последних трех случаях соответствует элементу $[\![10]\!] \in \widetilde{G}_n(J)$, который не перечисляется в $t_{k,n}$ и $q_{k,n}$. Следовательно, для четного n имеем

$$U_n(z) = T^{(0)}_n Q^{(0)}_n + z\left(T^{(1)}_n Q^{(0)}_n + T^{(0)}_n Q^{(1)}_n + T^{(1)}_n Q^{(1)}_n\right). \tag{7}$$

Для подсчета величины $u_{k,n}$ при нечетном n отнесем J к одному из четырех возможных классов в зависимости от принадлежности точек $[\![01]\!], [\![01]\!]+1$ к множеству J. Так же, как и при четном n, получается соотношение (7).

Получим рекуррентные соотношения для введенных производящих функций. При четном n величина $t^{(0)}_{k,n}$ определяется как число подмножеств, для которых $\left|\tilde{G}_n(J)\right| = k$. В $\tilde{G}_n(J)$ могут присутствовать или не присутствовать элементы $[\![10]\!]-1$ и $[\![10]\!]-2$. Пусть $W^{(1)}_1$ – множество всех таких $\alpha \in \overbrace{0,[\![01]\!]-2}$, для которых $[\![10]\!]-1 \in \tilde{G}_n(\{\alpha\})$, а $W^{(2)}_1$ – множество всех таких $\alpha \in \overbrace{0,[\![01]\!]-2}$, для которых $[\![10]\!]-2 \in \tilde{G}_n(\{\alpha\})$. Пусть далее $W^{(i)}_k = \tilde{G}^{-1}_n\left(\tilde{G}_n\left(W^{(i)}_{k-1}\right)\right)$, $k = 2,3,\ldots,n$, $W^{(i)} = \bigcup_{k=1}^{n} W^{(i)}_k$. Через $\tilde{G}^{-1}_n(A)$ здесь обозначено максимальное подмножество $I \subset \overbrace{[\![0]\!],[\![1]\!]}$ со свойством $\tilde{G}_n(I) = A$. Очевидно, $W^{(1)} \cup W^{(2)} = \overbrace{[\![0]\!],[\![1]\!]}$, $W^{(1)} \cap W^{(2)} = \varnothing$. Осталось заметить, что количество подмножеств $J \subset W^{(i)}$, для которых $\left|\tilde{G}_n(J)\right| = k$, равно $t^{(0)}_{k,n-1}$, $i = 1,2$. Отсюда для $n = 2m$ имеем

$$T^{(0)}_{2m}(z) = \left(T^{(0)}_{2m-1}(z)\right)^2. \tag{8}$$

Аналогичными рассуждениями можно получить формулы:

$$T^{(1)}_{2m}(z) = \left(T^{(1)}_{2m-1}(z)\right)^2, \tag{9}$$

$$T^{(0)}_{2m+1}(z) = \left(T^{(0)}_{2m}(z)\right)^2 + 2zT^{(0)}_{2m}(z)T^{(1)}_{2m}(z) + z\left(T^{(1)}_{2m}(z)\right)^2, \tag{10}$$

$$T^{(1)}_{2m+1}(z) = z\left(T^{(0)}_{2m}(z) + T^{(1)}_{2m}(z)\right)^2, \tag{11}$$

$$Q^{(0)}_{2m}(z) = \left(Q^{(0)}_{2m-1}(z)\right)^2 + 2zQ^{(0)}_{2m=1}(z)Q^{(1)}_{2m-1}(z) + z\left(Q^{(1)}_{2m-1}(z)\right)^2, \tag{12}$$

$$Q^{(1)}_{2m}(z) = z\left(Q^{(0)}_{2m-1}(z) + Q^{(1)}_{2m-1}(z)\right)^2, \tag{13}$$

$$Q^{(0)}_{2m+1}(z) = \left(Q^{(0)}_{2m}(z)\right)^2, \tag{14}$$

$$Q_{2m+1}^{(1)}(z)=\left(Q_{2m}^{(1)}(z)\right)^2. \tag{15}$$

Соотношения (8)–(15) справедливы при следующих начальных условиях:

$$T_1^{(0)}(z)=1,\ T_1^{(1)}(z)=z,\ Q_1^{(0)}(z)=1,\ Q_1^{(1)}(z)=1. \tag{16}$$

Таблица 2

Структура рекуррентных соотношений

	n – четно	n – нечетно
$T_{n+1}^{(0)}$	$F\left(T_n^{(0)},T_n^{(1)}\right)$	$G\left(T_n^{(0)}\right)$
$T_{n+1}^{(1)}$	$H\left(T_n^{(0)},T_n^{(1)}\right)$	$G\left(T_n^{(1)}\right)$
$Q_{n+1}^{(0)}$	$G\left(Q_n^{(0)}\right)$	$F\left(Q_n^{(0)},Q_n^{(1)}\right)$
$Q_{n+1}^{(1)}$	$G\left(Q_n^{(1)}\right)$	$H\left(Q_n^{(0)},Q_n^{(1)}\right)$

Введем следующие функции: $F(x,y)=x^2+2zxy+zy^2$, $G(x)=x^2$, $H(x,y)=z(x+y)^2$, которые позволяют свести в табл. 2 рекуррентные соотношения для $T_n^{(0)}$, $T_n^{(1)}$, $Q_n^{(0)}$, $Q_n^{(1)}$.

Сформулируем полученный результат в виде утверждения.

Утверждение 14. Производящая функция $U_n(z)$ числа прообразов графового отображения для графа $\tilde{G}_n$ подчиняется соотношению

$$U_n(z)=T_n^{(0)}Q_n^{(0)}+z\left(T_n^{(1)}Q_n^{(0)}+T_n^{(0)}Q_n^{(1)}+T_n^{(1)}Q_n^{(1)}\right),$$

где рекуррентные соотношения для $T_n^{(0)}$, $T_n^{(1)}$, $Q_n^{(0)}$, $Q_n^{(1)}$ описываются табл. 2, а начальные условия – формулами (16).

Выпишем первые три члена $U_n(z)$:

$$U_1(z)=1+z+2z^2;$$

$$U_2(z)=1+3z+4z^2+z^3+7z^4;$$

$$U_3(z)=1+6z+10z^2+24z^3+39z^4+31z^5+89z^6+15z^7+41z^8.$$

Воспользовавшись формулой (6), получаем: $s_4=8$, $s_5=65$, $s_6=3251$.

Таким образом, нами получены две нижние границы мощности множества M_n: $|M_n|\ge r_n$ и $|M_n|\ge s_n$. Однако обе эти оценки неудобны для вычислений. Выясним скорости роста r_n и s_n и сравним их между собой.

Асимптотический рост оценок мощности. Как показано выше, последовательность r_n подчиняется соотношению: $r_n=r_{n-1}^2+1$, $r_1=0$. Пусть $\rho_n=\sqrt[2^n]{r_n}$. Тогда $\rho_n^{2^n}=\rho_{n-1}^{2^n}+1$, откуда

$$\rho_n-\rho_{n-1}=\frac{1}{(\rho_n+\rho_{n-1})(\rho_n^2+\rho_{n-1}^2)\ldots(\rho_n^{2^{n-1}}+\rho_{n-1}^{2^{n-1}})}. \tag{17}$$

Очевидно, $\rho_n>\rho_{n-1}$ и последовательность ρ_n ограничена: $0\le\rho_n\le 2$. Следовательно, существует $\lim\limits_{n\to\infty}\rho_n=\rho$. Последовательность ρ_n сходится с дважды экспоненциальной скоростью: из (17) при $n\ge 5$ следует оценка

$$\rho-\rho_n<\frac{1}{2^{n-1}(11/10)^{2^n}}.$$

Пользуясь этой оценкой, можно вычислить ρ с любой степенью точности, например, уже ρ_{11} дает 87 верных десятичных знака ρ. Вычисления показывают, что $\rho=1{,}1072048...$.

Таким образом, $\sqrt[2^n]{r_n}\to\rho=1{,}107...$.

Перейдем теперь к последовательности s_n. Воспользуемся соотношениями (8)–(16). Для $i=0,1$, $n=1,2,...$ обозначим:

$$\tau_n^{(i)}=\sqrt[2^n]{T_n^{(i)}\left(\frac{1}{2}\right)},\ \theta_n^{(i)}=\sqrt[2^n]{Q_n^{(i)}\left(\frac{1}{2}\right)},\ \upsilon_n=\sqrt[2^n]{U_n\left(\frac{1}{2}\right)}.$$

Нетрудно видеть, что $\tau_n^{(0)}>\tau_n^{(1)}$, $\tau_n^{(0)}\ge\tau_{n-1}^{(0)}$. Теперь с учетом (8–11) можно получить неравенство

$$\left[\frac{\tau_{2m+1}^{(1)}}{\tau_{2m+1}^{(0)}}\right]^{2^{2m+1}}>\frac{1}{2}\frac{\left[\left(\tau_{2m-1}^{(0)}\right)^{2^{2m}}+\left(\tau_{2m-1}^{(1)}\right)^{2^{2m}}\right]^2}{\left[\left(\tau_{2m-1}^{(0)}\right)^{2^{2m}}+\left(\tau_{2m-1}^{(1)}\right)^{2^{2m}}\right]^2}=\frac{1}{2},$$

откуда

$$\frac{1}{2}<\left[\frac{\tau_n^{(1)}}{\tau_n^{(0)}}\right]^{2^n}<1,\ n=1,2,... .$$

Из последнего неравенства следует

$$0<\tau_n^{(0)}-\tau_n^{(1)}<\frac{4}{2^n}\frac{4}{2^n}\ . \tag{18}$$

Для оценки $\left|\tau_n^{(0)}-\tau_{n-1}^{(0)}\right|$ воспользуемся вытекающим из (8)–(16) соотношением

$$\left[\frac{\tau_{2m+1}^{(0)}}{\tau_{2m-1}^{(0)}}\right]^{2^{2m+1}}>\frac{(\tau_{2m-1}^{(0)})^{2^{2m+1}}+(\tau_{2m-1}^{(1)})^{2^{2m}}(\tau_{2m-1}^{(1)})^{2^{2m}}+\frac{1}{2}(\tau_{2m-1}^{(1)})^{2^{2m-1}}}{(\tau_{2m-1}^{(0)})^{2^{2m+1}}}.$$

Поскольку $\tau_n^{(0)}>\tau_n^{(1)}$, то

$$1<\left[\frac{\tau_n^{(0)}}{\tau_{n-2}^{(0)}}\right]^{2^n}<\frac{5}{2},$$

и, следовательно,

$$1<\frac{\tau_n^{(0)}}{\tau_{n-2}^{(0)}}<\frac{3}{2}2^{-n}.$$

Теперь легко устанавливаются существование предела τ последовательности $\tau_n^{(0)}$ и оценка $0\le\tau-\tau_n^{(0)}<6\times2^n$. С помощью (18) получаем $\left|\tau-\tau_n^{(1)}\right|<10\times2^n$, что, в частности, означает, что последовательность $\tau_n^{(1)}$ также имеет своим пределом τ.

Аналогичным образом можно показать существование общего для последовательностей $\theta_n^{(0)}$ и $\theta_n^{(1)}$ предела θ и получить оценку $\left|\theta-\theta_n^{(i)}\right|<10\times2^n$, $i=0,1$, $n=2,3,...$.

Полученные оценки с учетом (7) путем несложных вычислений приводят к неравенству

$$\tau\theta - 20\times 2^{-n} \le \upsilon_n \le \tau\theta + 82\times 2^{-n},\ n = 2,3,\ldots\ .$$

Воспользовавшись (6), с помощью непосредственного подсчета получаем:

$$\sqrt[2^n]{s_n} = \sqrt[2^n]{2^{2^{n-3}}\,\upsilon_{n-3}} \to \sqrt[8]{2\tau\theta} = 1{,}132\ldots\ .$$

Переформулируем полученные оценки для повторного логарифма рассматриваемых величин:

$$n - \log_2\log_2 r_n \to 2{,}767\ldots\,,$$

$$n - \log_2\log_2 s_n \to 2{,}485\ldots\ .$$

Таким образом, неравенство $|M_n| \ge s_n$ является более сильным, чем $|M_n| \ge r_n$. Поскольку неравенство (5) приводит к неравенству $n - \log_2\log_2|M_n| > 1$, мы получаем

Утверждение 15. Справедливы неравенства:

$$1 < n - \log_2\log_2|M|_n < \sigma(1+\varepsilon_n)\,,$$

где $\varepsilon_n \to 0$ при $n\to\infty$, $\sigma = \lim\limits_{n\to\infty}\left(n - \log_2\log_2 s_n\right) = 2.485\ldots$

В качестве следствия получаем

Утверждение 16.

$$\lim_{n\to\infty}\frac{\log_2\log_2|M_n|}{n} = 1\,.$$

Литература

1. Кудрявцев В.Б. Введение в теорию автоматов / В.Б. Кудрявцев, С.В. Алешин, А.С. Подколзин. – М.: Наука, 1985. – 320 с.

2. Мельников С.Ю. О задаче определения функции выходов автомата со случайным входом по статистике встречаемости слова в выходной последовательности // Доклады ТУСУРа. – 2011. – № 1 (23). – С. 101–117.

3. Камловский О.В. Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа / О.В. Камловский, А.С. Кузьмин // Фундамент. и прикл. матем. – 2000. – Т. 6, вып. 4. – С. 1083–1094.

4. Allouche J.-P. Automatic sequences. Theory, Applications, Generalizations / J.-P. Allouche, J. Shallit. – Cambridge Univ. Press, 2003. –571 p.

5. Мельников С.Ю. Многогранники, характеризующие статистические свойства конечных автоматов // Труды по дискр. мат. – 2003. – Т. 7. – С. 126–137.

6. Мельников С.Ю. Многоугольники, характеризующие статистические свойства булевых функций в схеме регистра сдвига // Вестник РГГУ. – 2010. – № 12. – С. 137–159.

7. Кац М. Статистическая независимость в теории вероятностей, анализе и теории чисел. – М.: Изд-во иностр. лит., 1962. –156 с.

8. Мельников С.Ю. О переработке конечными автоматами чезаровских последовательностей // Вестн. Моск. гос. ун-та леса. Лесной вестник. – 2004. – №1 (32). – С. 169–174.

9. Свами М. Графы, сети и алгоритмы / М. Свами, К. Тхуласираман. – М.: Мир, 1984. – 455 с.

Мельников Сергей Юрьевич
Канд. физ.-мат. наук, зам. ген. директора ООО «Лингвистические и информационные технологии», г. Москва
Тел.: 8 (495) 249-90-53
Эл. почта: melnikov@linfotech.ru

Melnikov S.Yu.

Non-autonomous binary shift registers without changing the relative frequencies of characters in the input sequence

The article deals with the class of binary shift registers, providing the equality of the relative frequencies of characters in the input and output sequences. Some properties of output functions of this class are formulated. It is proved that the power of this class increases as double exponent of the register length.

Keywords: pseudo-random sequence; shift register, de Bruijn graph.