УДК 004.421.5

ОЦЕНКА КОЛИЧЕСТВА ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОРОЖДАЕМЫХ КАСКАДНЫМ МЕТОДОМ

В.В. РУМБЕШТ
А.З. ЯДУТА

Белгородский государственный национальный исследовательский университет

e-mail:
rumbesht@bsu.edu.ru

В статье выводится формула, оценивающая количество последовательностей, порождаемых каскадным методом, в зависимости от порядка группы и количества каскадов.

Ключевые слова: каскадный метод, кумулятивная последовательность, количество последовательностей.

В работе [1] предложен каскадный метод порождения периодических последовательностей над элементами циклической группы. В этой статье показано, что порождаемые этим методом последовательности имеют следующие структурные свойства.

1. Период последовательности зависит от порядка группы и количества каскадов (уровней преобразования). Эта зависимость выражается формулой: $\pi = N^k$, где π – период последовательности; N – порядок группы; k – количество каскадов.

2. Характеристическая функция периодического отрезка последовательности, порожденной каскадным методом, имеет вид $\forall u \in U : \chi_{[X_{\rightarrow}^{(k)}]}(u) = N^{k-1}$, где U – множество элементов группы, над которой строится последовательность; $X_{\rightarrow}^{(k)}$ – чисто периодическая последовательность k-го уровня преобразования; $[X_{\rightarrow}^{(k)}]$ – ее периодический отрезок. Т.е. любые две из таких последовательностей совпадают с точностью до порядка следования элементов их периодических отрезков.

Очевидно, что мощность множества Ω – всех возможных чисто периодических последовательностей с такими структурными свойствами равна количеству перестановок с повторениями из N элементов, каждый из которых повторяется N^{k-1} раз, за вычетом количества перестановок из N элементов, каждый из которых повторяется N^{k-2} раз:

$$|\Omega| = \frac{N^k!}{(N^{k-1}!)^N} - \frac{N^{k-1}!}{(N^{k-2}!)^N},$$

а последовательности, порождаемые каскадным методом, составляют лишь относительно небольшую часть этого множества. Поэтому, для каскадного метода актуальной является задача оценки количества последовательностей им порождаемых.

Каскадный метод сформулирован для абстрактной циклической группы. Такая формулировка определяет лишь общие структурные свойства элементов множества последовательностей, порождаемых посредством применения каскадного метода, но не позволяет установить мощность и состав этого множества. Поэтому далее будем предполагать, что на всех уровнях преобразования применятся одна и та же конкретная группа.

В этом случае количество последовательностей, порождаемых каскадным методом, зависит от N – порядка группы и k – количества каскадов. Обозначим это количество как $\nu(N,k)$. *Целью данной статьи является нахождение указанной зависимости.*

Далее в работе будем использовать определения и обозначения, введенные в [1]: $<U,\otimes>$ – циклическая группа порядка $N > 2$ (это принципиально); $G_{<U,\otimes>}$ – множество ее образующих элементов; $Ind(u)$ – индекс элемента $u \in U$ по основанию $g_{Base} \in G_{<U,\otimes>}$; $X_{\rightarrow} = (x_1, x_2, \ldots, x_t, \ldots)$ – последовательность над U; $[X_{\rightarrow}]$ – периодический отрезок чисто

периодической последовательности $X_{\to}$, $\chi_{[X_{\to}]}$ – характеристическая функция периодического отрезка, $h_{X_{\to}}$ – характеристический элемент чисто периодической последовательности $X_{\to}$.

Для оценки количества последовательностей необходимо определить отношение, позволяющее различать либо не различать две последовательности.

Определение 1. Две последовательности $X_{\to}=(x_1,x_2,\ldots,x_i,\ldots)$ и $Y_{\to}=(y_1,y_2,\ldots,y_i,\ldots)$ называются равными (обозначается $X_{\to}=Y_{\to}$), если для всех натуральных i имеет место $x_i=y_i$.

Поскольку чисто периодические последовательности однозначно задаются своими периодическими отрезками, то о равенстве таких последовательностей можно судить по равенству периодических отрезков.

Каскадный метод использует два вида преобразований: процедуру порождения кумулятивной последовательности (процедура порождения КП) и процедуру-фильтр [1].

Параметрами процедуры порождения КП выступают начальный элемент $y_0 \in U$ и очередной член входной последовательности. Внутренне состояние процедуры на момент инициализации совпадает с начальным элементом. После каждого обращения к этой процедуре она выдает на выход значение равное результату групповой операции примененной к внутреннему состоянию и очередному члену входной последовательности. При этом очередное внутреннее состояние принимается равным выходу. Таким образом, процедура порождения КП формирует на выходе кумулятивную последовательность с начальным элементом y_0 и порождающей последовательностью, подаваемой на вход данной процедуры [1].

Докажем два утверждения об условии равенства кумулятивных последовательностей.

Утверждение 1. Кумулятивная последовательность $Y_{\to}=(y_1,y_2,\ldots,y_i,\ldots)$ с начальным элементом y_0 и порождающей $X_{\to}=(x_1,x_2,\ldots,x_i,\ldots)$ равна кумулятивной последовательности $Y'_{\to}=(y'_1,y'_2,\ldots,y'_i,\ldots)$ с начальным элементом y'_0 и порождающей $X'_{\to}=(x'_1,x'_2,\ldots,x'_i,\ldots)$ тогда и только тогда, когда для всех натуральных $i>1$ имеет место $x_i=x'_i$ и $y_0\otimes y'^{-1}_0=x^{-1}_1\otimes x'_1$.

Доказательство. С одной стороны, по определению кумулятивной последовательности (см. определение 3 в [1]), для всех $i>1$: $x_i=y_i\otimes y^{-1}_{i-1}$, $x_i'=y_i'\otimes y'^{-1}_{i-1}$. Отсюда следует, что, если $Y_{\to}=Y'_{\to}$, то и для всех $i>1$ имеет место $x_i=x'_i$. Кроме этого, если $y_1=y'_1$, то $y_1\otimes y'^{-1}_1=y_0\otimes x_1\otimes x'^{-1}_1\otimes y'^{-1}_0=e$. Умножив левую и правую части выражения $y_0\otimes x_1\otimes x'^{-1}_1\otimes y'^{-1}_0=e$ на $x^{-1}_1\otimes x'_1$ получим $y_0\otimes y'^{-1}_0=x^{-1}_1\otimes x'_1$. Следовательно, если $Y_{\to}=Y'_{\to}$, то для всех натуральных $i>1$ имеет место $x_i=x'_i$ и $y_0\otimes y'^{-1}_0=x^{-1}_1\otimes x'_1$.

С другой стороны, если $y_0\otimes y_0'^{-1}=x^{-1}_1\otimes x_1'$, то $y_1=y_0\otimes x_1=y_0'\otimes x_1'=y'_1$. А, если $y_1=y'_1$ и для всех $i>1$ имеет место $x_i=x_i'$, то $Y_{\to}=Y'_{\to}$. *Что и требовалось доказать.*

Утверждение 2. Пусть кумулятивная последовательность $Y_{\to}=(y_1,y_2,\ldots,y_i,\ldots)$ с начальным элементом y_0 и порождающей $X_{\to}=(x_1,x_2,\ldots,x_i,\ldots)$ и кумулятивная последовательность $Y'_{\to}=(y'_1,y'_2,\ldots,y'_i,\ldots)$ с начальным элементом y'_0 и порождающей $X'_{\to}=(x'_1,x'_2,\ldots,x'_i,\ldots)$ являются чисто периодическими. Эти последовательности равны тогда и только тогда, когда $X_{\to}=X'_{\to}$ и $y_0=y'_0$.

Доказательство этого утверждения становится очевидным, если принять во внимание тот факт, что согласно части утверждения 1 кумулятивные последовательности равны, когда для всех натуральных $i>1$ имеет место $x_i = x'_i$. Для чисто периодических последовательностей это условие должно быть истинным и при $x_1 = x'_1$. Из второй части утверждения 1 с учетом сказанного автоматически следует $y_0 = y'_0$. *Что и требовалось доказать.*

Поскольку каскадный метод имеет дело только с чисто периодическими последовательностями, то, согласно утверждению 2, выход процедуры порождения КП уникален для любой возможной комбинации значений параметров на ее входе. Входные параметры этой процедуры не зависимы друг от друга, а так же для начального элемента существует возможность выбора из N вариантов. Таким образом, количество последовательностей на выходе k-го уровня преобразований в зависимости от N составляет:

$$\nu(N,k) = N \cdot \omega(N,k), \quad (1)$$

где $\omega(N,k)$ – количество входных порождающих последовательностей, поступающих на вход процедуры порождения КП k-го уровня.

В частности, на первом уровне преобразований на вход процедуры порождения КП подаются элементы стационарных последовательностей [1], члены которых суть образующие элементы группы $<U,\otimes>$. Очевидно, что всего таких стационарных последовательностей существует ровно $\varphi(N)$. Таким образом, количество последовательностей порождаемых первым уровнем преобразования каскадного метода составляет:

$$\nu(N,1) = N \cdot \varphi(N). \quad (2)$$

Для всех уровней преобразования, начиная со второго, применению процедуры порождения КП предшествует применение процедуры фильтра, а последовательность, подаваемая на вход этой процедуры, есть результат предыдущего уровня преобразования.

Процедура-фильтр принимает на вход члены чисто периодической последовательности $X_{\rightarrow} = (x_1, x_2, \ldots, x_i, \ldots)$ с периодом π и характеристическим элементом $h_{X_{\rightarrow}}$, а так же заданные для замены параметры: характеристический элемент выходной последовательности $g \in G_{<U,\otimes>}$ и позиция замены $m \in \{0, 1, \ldots, \pi - 1\}$. Она формирует в качестве результата соответствующие члены выходной чисто периодической последовательности $\widetilde{X}_{\rightarrow} = (\widetilde{x}_1, \widetilde{x}_2, \ldots, \widetilde{x}_i, \ldots)$ такого же периода, но с характеристическим элементом $h_{\widetilde{X}_{\rightarrow}} = g$:

$$\forall i \in \{1, 2, \ldots\}: \ \widetilde{x}_i = \begin{cases} x_i, \text{ если } m \neq (i \bmod \pi); \\ x_i \otimes g \otimes h_{X_{\rightarrow}}^{-1}, \text{ если } m = (i \bmod \pi). \end{cases} \quad (3)$$

Пусть $X_{\rightarrow} = (x_1, x_2, \ldots, x_i, \ldots)$ и $Y_{\rightarrow} = (y_1, y_2, \ldots, y_i, \ldots)$ – чисто периодические последовательности такие, что $\chi_{[X_{\rightarrow}]} = \chi_{[Y_{\rightarrow}]} = \chi$; $\widetilde{X}_{\rightarrow} = (\widetilde{x}_1, \widetilde{x}_2, \ldots, \widetilde{x}_i, \ldots)$ – последовательность, сформированная процедурой-фильтром из $X_{\rightarrow}$ с применением параметров g_1 и m_1; $\widetilde{Y}_{\rightarrow} = (\widetilde{y}_1, \widetilde{y}_2, \ldots, \widetilde{y}_i, \ldots)$ – последовательность, сформированная процедурой фильтром из $Y_{\rightarrow}$ с применением параметров g_2 и m_2.

Условие равенства характеристических функций периодических отрезков $[X_{\rightarrow}]$ и $[Y_{\rightarrow}]$ выражает тот факт, что данные отрезки совпадают с точностью до порядка следования их элементов. Структурные свойства $X_{\rightarrow}$ и $Y_{\rightarrow}$ – период: $\pi_{X_{\rightarrow}} = \pi_{Y_{\rightarrow}} = \pi = \sum_{\forall u \in U} \chi(u)$ и характеристический элемент: $h_{X_{\rightarrow}} = h_{Y_{\rightarrow}} = h = \bigotimes_{\forall u \in U} u^{\chi(u)}$.

Докажем утверждения об условиях равенства последовательностей, сформированных процедурой-фильтром.

Утверждение 3. Необходимым условием равенства $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ является равенство g_1 и g_2.

Доказательство. Из $\widetilde{X}_{\to} = \widetilde{Y}_{\to}$ следует, что $\chi_{[\widetilde{X}_{\to}]} = \chi_{[\widetilde{Y}_{\to}]}$. В свою очередь из $\chi_{[\widetilde{X}_{\to}]} = \chi_{[\widetilde{Y}_{\to}]}$ следует, что $h_{\widetilde{X}_{\to}} = \bigotimes\limits_{\forall u \in U} u^{\chi_{[\widetilde{X}_{\to}]}(u)}$ равен $h_{\widetilde{Y}_{\to}} = \bigotimes\limits_{\forall u \in U} u^{\chi_{[\widetilde{Y}_{\to}]}(u)}$. Поскольку $g_1 = h_{\widetilde{X}_{\to}}$ а $g_2 = h_{\widetilde{Y}_{\to}}$, то $g_1 = g_2$. *Что и требовалось доказать.*

Утверждение 4. Необходимым условием равенства $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ при $g_1 = g_2 = g$ и $m_1 = m_2 = m$ является равенство $X_{\to}$ и $Y_{\to}$.

Доказательство. По формуле (3): $\widetilde{x}_{q\cdot\pi+m} = x_{q\cdot\pi+m} \otimes g \otimes h^{-1}$, $\widetilde{y}_{q\cdot\pi+m} = y_{q\cdot\pi+m} \otimes g \otimes h^{-1}$ для $\forall q \in \{0,1,\ldots\}$, а все остальные члены $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ совпадают с соответствующими членами $X_{\to}$ и $Y_{\to}$. С учетом этого, из равенства $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ следует равенство $X_{\to}$ и $Y_{\to}$. *Что и требовалось доказать.*

Утверждение 5. Необходимым условием равенства $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ при $g_1 = g_2 = g$ и $m_1 \neq m_2$ является

$$(\forall i \in \{1,2,\ldots\} \setminus \{q\cdot\pi + m_1, q\cdot\pi + m_2 \mid q \in \{0,1,\ldots\}\} : x_i = y_i)\ \&$$
$$(\forall q \in \{0,1,\ldots\} : (y_{q\cdot\pi+m_1} = x_{q\cdot\pi+m_1} \otimes g \otimes h^{-1})\ \&\ (x_{q\cdot\pi+m_2} = y_{q\cdot\pi+m_2} \otimes g \otimes h^{-1})).$$

Другими словами, последовательности $X_{\to}$ и $Y_{\to}$ должны отличаться только членами, стоящими в позициях $q\cdot\pi + m_1$ и $q\cdot\pi + m_2$, где $q \in \{0,1,\ldots\}$, и для этих членов должно быть характерно $(y_{q\cdot\pi+m_1} = x_{q\cdot\pi+m_1} \otimes g \otimes h^{-1})\ \&\ (x_{q\cdot\pi+m_2} = y_{q\cdot\pi+m_2} \otimes g \otimes h^{-1})$.

Доказательство. По формуле (3): $\widetilde{x}_{q\cdot\pi+m_1} = x_{q\cdot\pi+m_1} \otimes g \otimes h^{-1}$, $\widetilde{y}_{q\cdot\pi+m_1} = y_{q\cdot\pi+m_1}$, $\widetilde{y}_{q\cdot\pi+m_2} = y_{q\cdot\pi+m_2} \otimes g \otimes h^{-1}$, $\widetilde{x}_{q\cdot\pi+m_2} = x_{q\cdot\pi+m_2}$ для $\forall q \in \{0,1,\ldots\}$, а все остальные члены $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ совпадают с соответствующими членами $X_{\to}$ и $Y_{\to}$. С учетом этого, из равенства $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ следует $(y_{q\cdot\pi+m_1} = x_{q\cdot\pi+m_1} \otimes g \otimes h^{-1})\ \&\ (x_{q\cdot\pi+m_2} = y_{q\cdot\pi+m_2} \otimes g \otimes h^{-1})$ и $x_i = y_i$ при $i \neq q\cdot\pi + m_1$, $i \neq q\cdot\pi + m_2$. *Что и требовалось доказать.*

Утверждение 6. Для равенства $\widetilde{X}_{\to}$ и $\widetilde{Y}_{\to}$ необходимо и достаточно

$$(g_1 = g_2)\ \&\ (((m_1 = m_2)\ \&\ (\forall i \in \{1,2,\ldots\} : x_i = y_i)) \vee$$
$$((m_1 \neq m_2)\ \&\ (\forall i \in \{1,2,\ldots\} \setminus \{q\cdot\pi + m_1, q\cdot\pi + m_2 \mid q \in \{0,1,\ldots\}\} : x_i = y_i)\ \& \qquad (4)$$
$$(\forall q \in \{0,1,\ldots\} : (y_{q\cdot\pi+m_1} = x_{q\cdot\pi+m_1} \otimes g_1 \otimes h^{-1})\ \&\ (x_{q\cdot\pi+m_2} = y_{q\cdot\pi+m_2} \otimes g_2 \otimes h^{-1})))$$

Доказательство. Необходимость этого составного условия уже доказана по частям (см. утверждения 3, 4 и 5). Докажем его достаточность. Это доказательство удобнее провести не в терминах последовательностей, как это было в предыдущих утверждениях, а в терминах их периодических отрезков.

Пусть $\widetilde{X}_{\to} \neq \widetilde{Y}_{\to}$. Это равносильно тому, что множество позиций, в которых имеет место несовпадение элементов в периодических отрезках $[\widetilde{X}_{\to}]$ и $[\widetilde{Y}_{\to}]$, не пусто. Обозначим это множество символом $S \subseteq \{1,2,\ldots,\pi\}$.

Случай 1. $\exists s \in S : s \neq \begin{cases} m_1, \text{если } m_1 > 0; \\ \pi, \text{если } m_1 = 0; \end{cases}$ $\&\ s \neq \begin{cases} m_2, \text{если } m_2 > 0; \\ \pi, \text{если } m_2 = 0; \end{cases}$ По формуле (3) имеем: $\widetilde{x}_s = x_s$ и $\widetilde{y}_s = y_s$. Из этого следует $x_s \neq y_s$, что, очевидно, противоречит (4).

Случай 2. Пусть $m_1 = m_2 = m$ и $\exists s \in S : s = \begin{cases} m, \text{если } m > 0; \\ \pi, \text{если } m = 0; \end{cases}$ По формуле (3) имеем: $\tilde{x}_s = x_s \otimes g_1 \otimes h^{-1}$ и $\tilde{y}_s = y_s \otimes g_2 \otimes h^{-1}$. Из этого следует $x_s \otimes g_1 \neq y_s \otimes g_2$. Это в свою очередь влечет $x_s \neq y_s \vee g_1 \neq g_2$, что, очевидно, противоречит (4).

Случай 3. Пусть $m_1 \neq m_2$ и $\exists s_1, s_2 \in S : s_1 = \begin{cases} m_1, \text{если } m_1 > 0; \\ \pi, \text{если } m_1 = 0; \end{cases}$ & $s_2 = \begin{cases} m_2, \text{если } m_2 > 0; \\ \pi, \text{если } m_2 = 0; \end{cases}$

По формуле (3): $\tilde{x}_{s_1} = x_{s_1} \otimes g_1 \otimes h^{-1}$; $\tilde{y}_{s_1} = y_{s_1}$; $\tilde{y}_{s_2} = y_{s_2} \otimes g_2 \otimes h^{-1}$; $\tilde{x}_{s_2} = x_{s_2}$. Из этого следует $y_{s_1} \neq x_{s_1} \otimes g_1 \otimes h^{-1}$ и $x_{s_2} \neq y_{s_2} \otimes g_2 \otimes h^{-1}$, что, очевидно, противоречит (4).

Три случая, рассмотренных выше, исчерпывают все возможности существования элементов S, и каждый из них приводит к ложности условия (4). Это, в свою очередь, доказывает достаточность. *Что и требовалось доказать.*

Из утверждения 6 следует, что две разные комбинации значений параметров на входе процедуры-фильтра могут привести к одному и тому же результату. Чтобы такого не случилось достаточно, чтобы, введенное в доказательстве утверждения 6, множество S содержало более чем два элемента.

Последовательности, формируемые на выходе первого уровня преобразования каскадного метода, имеют вид $X_{\to} = (x_0 \otimes g, x_0 \otimes g^2, \ldots, x_0 \otimes g^N, \ldots)$, где $x_0 \in U$, $g \in G_{<U,\otimes>}$ [1]. Период $X_{\to}$ равен N. Пусть $X_{\to} = (x_1, x_2, \ldots, x_i, \ldots)$ – такая последовательность при x_0 и g_1, а $Y_{\to} = (y_1, y_2, \ldots, y_i, \ldots)$ – при y_0 и g_2. В этом случае условие равенства q-тых элементов периодических отрезков $[X_{\to}]$ и $[Y_{\to}]$ запишется как $x_0 \otimes g_1^q = y_0 \otimes g_2^q$, где $q \in \{1,2,\ldots,N\}$. Если перейти индексам элементов, то это условие эквивалентно сравнению:

$$Ind(x_0) + q \cdot Ind(g_1) \equiv (Ind(y_0) + q \cdot Ind(g_2)) \bmod N.$$

Выполнив несложные преобразования, получим:

$$q \cdot (Ind(g_1) - Ind(g_2)) \equiv (Ind(y_0) - Ind(x_0)) \bmod N. \quad (5)$$

Таким образом, оценка мощности множества S сводится к определению количества решений сравнения (5) относительно q.

Пусть $d = \gcd((Ind(g_1) - Ind(g_2)) \bmod N, N)$, тогда мощность S есть:

$$|S| = \begin{cases} N, \text{если } (Ind(y_0) - Ind(x_0)) \bmod N \text{ не кратно } d; \\ N - d, \text{иначе.} \end{cases} \quad (6)$$

Если $Ind(g_1) = Ind(g_2)$, то $d = N$. Следовательно, при $Ind(x_0) \neq Ind(y_0)$ имеем: $|S| = N$, иначе $|S| = 0$. Если $Ind(g_1) \neq Ind(g_2)$, то $1 \leq d \leq N/c$, где c – наименьший простой делитель N. Не сложно видеть, что при $N > 4$ получается, что $|S| > 2$, если $(Ind(g_1) \neq Ind(g_2)) \vee (Ind(x_0) \neq Ind(y_0))$.

Приведенные выше рассуждения свидетельствуют, что на втором уровне преобразований при $N > 4$ любая комбинация значений параметров процедуры-фильтра приводит к уникальной последовательности на ее выходе. Остаются два интересных случая: $N = 3$ и $N = 4$.

Рассмотрим случай $N = 3$.

$$|S| = \begin{cases} 0, \text{если } (Ind(g_1) = Ind(g_2)) \& (Ind(x_0) = Ind(y_0)); \\ 2, \text{если } Ind(g_1) \neq Ind(g_2); \\ 3, \text{если } (Ind(g_1) = Ind(g_2)) \& (Ind(x_0) \neq Ind(y_0)). \end{cases}$$

При $Ind(g_1) \neq Ind(g_2)$ имеем $|S| = 2$ и существуют пары различных между собой комбинаций значений параметров процедуры-фильтра, которые приводят к формированию одной и той же последовательности на ее выходе.

Несложно видеть, что периодические отрезки последовательностей, формируемые первым уровнем преобразований каскадного метода при $N = 3$, представляют собой перестановки из 3-х элементов. Всего таких перестановок существует 6. Количество последовательностей, формируемых на первом уровне преобразования, то же равно $\nu(3,1) = 6$. Следовательно, периодические отрезки всех элементов множества последовательностей, формируемых первым уровнем, суть все возможные такие перестановки.

Значения параметров процедуры-фильтра выбираются независимо друг от друга. Количество различных комбинаций таких значений на втором уровне преобразования при $N = 3$ составляет 36. Это число получается произведением количества входных последовательностей ($\nu(3,1) = 6$) на количество вариантов выбора характеристического элемента выходной последовательности ($\varphi(3) = 2$) и на количество вариантов выбора позиции замены, равное 3.

Последовательность, у которой периодический отрезок представляет собой перестановку 3-х элементов, процедура-фильтр преобразует в последовательность такую, что ее периодический отрезок представляет собой перестановку с повторениями. В такой перестановке с повторениями два элемента, причем один из них имеет кратность 2, а другой кратность 1. Всего таких перестановок с повторениями 3, возможность выбора одного из элементов ограничивается 3-мя случаями, а возможность выбора другого элемента – 2-мя случаями. Всего таких перестановок с повторениями существует 18, и каждая из них при соответствующем подборе значений параметров может быть получена в качестве периодического отрезка последовательности на выходе процедуры-фильтра.

Таким образом, 36 комбинаций значений на входе процедуры-фильтра приводит к формированию лишь $\omega(3,2) = 18$ различных последовательностей на выходе.

Рассмотрим теперь случай $N = 4$.

$$|S| = \begin{cases} 0, \textit{если } (Ind(g_1) = Ind(g_2)) \,\&\, (Ind(x_0) = Ind(y_0)); \\ 2, \textit{если } (Ind(g_1) \neq Ind(g_2)) \,\&\, ((Ind(y_0) - Ind(x_0)) \equiv 0 \bmod 2); \\ 4, \textit{если } ((Ind(y_0) - Ind(x_0)) \equiv 1 \bmod 2) \vee ((Ind(g_1) = Ind(g_2)) \,\&\, (Ind(x_0) \neq Ind(y_0)). \end{cases}$$

При $(Ind(g_1) \neq Ind(g_2)) \,\&\, ((Ind(y_0) - Ind(x_0)) \equiv 0 \bmod 2)$ имеем $|S| = 2$. Как и в предыдущем случае, существуют пары различных между собой комбинаций значений параметров процедуры-фильтра, которые приводят к формированию одной и той же последовательности на ее выходе. Но такие пары можно найти, если предоставить возможность выбора входной последовательности из множества всех последовательностей, периодические отрезки которых суть перестановки множества из 4 элементов.

Последовательности, порождаемые на первом уровне преобразования каскадного метода, принадлежат лишь подмножеству указанного множества. Что само по себе уже не гарантирует существование пар таких комбинаций.

Составим систему сравнений, решение которой позволяет установить пару комбинаций значений параметров процедуры-фильтра, при которой выполняется условие (4) и условие (5) при $N = 4$:

$$\begin{cases} Ind(y_0) - Ind(x_0) \equiv 0 \bmod 2; \\ Ind(g_1) - Ind(g_2) \equiv 2 \bmod 4; \\ Ind(g_1) \equiv 1 \bmod 2; \\ Ind(g_2) \equiv 1 \bmod 2; \\ Ind(g) \equiv 1 \bmod 2; \\ Ind(y_0) + m_1 \cdot Ind(g_2) \equiv (Ind(x_0) + m_1 \cdot Ind(g_1) + Ind(g) + 2) \bmod 4; \\ Ind(x_0) + m_2 \cdot Ind(g_1) \equiv (Ind(y_0) + m_2 \cdot Ind(g_2) + Ind(g) + 2) \bmod 4; \end{cases} \quad (7)$$

В этой системе сравнений одна из комбинаций значений параметров $<< x_0, g_1 >, g, m_1 >$, а вторая $<< y_0, g_2 >, g, m_2 >$, где $x_0 \in U$, $g_1 \in \{g_{Base}^1, g_{Base}^3\}$ однозначно задают входную последовательность $X_{\rightarrow}$; $y_0 \in U$, $g_2 \in \{g_{Base}^1, g_{Base}^3\}$ однозначно задают входную последовательность $Y_{\rightarrow}$; $g \in \{g_{Base}^1, g_{Base}^3\}$ – совпадающий по условию (3) параметр "характеристический элемент выходной последовательности"; m_1 и m_2 – позиции замены.

Система сравнений (7) противоречива. В этом легко убедиться, если привести 7-ое сравнение в системе к виду $m_2 \cdot (Ind(g_1) - Ind(g_2)) \equiv (Ind(y_0) - Ind(x_0) + Ind(g) + 2) \bmod 4$ и учесть, что $Ind(g_1) - Ind(g_2) \equiv 2 \bmod 4$, а $Ind(y_0) - Ind(x_0) \equiv 0 \bmod 2$ и $Ind(g) \equiv 1 \bmod 2$.

Следовательно, любая, допустимая каскадным методом, комбинация значений параметров процедуры-фильтра на втором уровне преобразования при $N = 4$, приводит к уникальной последовательности на ее выходе. То есть, $\omega(4,2) = 64$.

Таким образом, общий вывод по количеству последовательностей, формируемых каскадным методом на втором уровне преобразования, есть:

$$\nu(N,2) = \begin{cases} \dfrac{N^2 \cdot \varphi(N) \cdot \nu(N,1)}{2}, \text{если } N = 3; \\ N^2 \cdot \varphi(N) \cdot \nu(N,1), \text{если } N > 3. \end{cases} \quad (8)$$

Перейдем теперь к оценке $\nu(N,k)$ при $k > 2$. В этом случае, последовательности $X_{\rightarrow} = (x_1, x_2, \ldots, x_i, \ldots)$, формируемые на выходе $k-1$-го уровня и подаваемые на вход процедуры-фильтра k-го уровня преобразования каскадного метода, имеют период N^{k-1} и обладают следующей структурой: $\forall i \in \{1,2,\ldots,N^{k-2}\}, \forall q \in \{0,1,\ldots\} : x_{N^{k-2} \cdot q + i} = x_i \otimes g^{q \bmod N}$, где $g \in G_{<U,\otimes>}$ [1]. Пусть $X_{\rightarrow} = (x_1, x_2, \ldots, x_i, \ldots)$ – последовательность такой структуры при g_1, а $Y_{\rightarrow} = (y_1, y_2, \ldots, y_i, \ldots)$ – при g_2.

На основе $X_{\rightarrow}$ определим N^{k-2} последовательностей $X_{J_{\rightarrow}} = (x_{J_1}, x_{J_2}, \ldots, x_{J_i}, \ldots)$, а на основе $Y_{\rightarrow}$ – N^{k-2} последовательностей $Y_{J_{\rightarrow}} = (y_{J_1}, y_{J_2}, \ldots, y_{J_i}, \ldots)$ таких, что $\forall i \in \{1,2,\ldots\}, \forall j \in \{1,2,\ldots,N^{k-2}\} : x_{J_i} = x_{(i-1) \cdot N^{k-2} + J}; y_{J_i} = y_{(i-1) \cdot N^{k-2} + J}$. Не сложно заметить, что любая из последовательностей $X_{J_{\rightarrow}}$ или $Y_{J_{\rightarrow}}$ имеет период равный N и при этом $X_{J_{\rightarrow}} = (x_{J_1} \otimes g_1^0, x_{J_1} \otimes g_1^1, \ldots, x_{J_1} \otimes g_1^{N-1}, \ldots)$, $Y_{J_{\rightarrow}} = (y_{J_1} \otimes g_2^0, y_{J_1} \otimes g_2^1, \ldots, y_{J_1} \otimes g_2^{N-1}, \ldots)$. То есть они устроены аналогично последовательностям, формируемым первым уровнем преобразования.

Проведем оценку мощности множества S при сравнении $X_{\rightarrow}$ и $Y_{\rightarrow}$. Очевидно, что $|S| = \sum_{j=1}^{N^{k-2}} |S_j|$, где S_j – множество позиций несовпадения элементов на периодических отрезках $[X_{j_{\rightarrow}}]$ и $[Y_{j_{\rightarrow}}]$.

О равенстве $X_{\rightarrow}$ и $Y_{\rightarrow}$ можно судить по выполнению условия $(\forall j \in \{1,2,\ldots,N^{k-2}\} : x_j = y_j) \,\&\, (g_1 = g_2)$. В этом случае $\forall j \in \{1,2,\ldots,N^{k-2}\} : X_{j_{\rightarrow}} = Y_{j_{\rightarrow}}$ и, естественно, $|S| = 0$ и любое $|S_j| = 0$

Если $(\exists j \in \{1,2,\ldots,N^{k-2}\} : x_j \neq y_j) \,\&\, (g_1 = g_2)$, то найдется хотя бы одна пара $X_{j_{\rightarrow}}$ и $Y_{j_{\rightarrow}}$, для которой, как было показано ранее $|S_j| = N$. Следовательно $|S| > 2$.

Если $g_1 \neq g_2$, то пар неравных между собой $X_{j_{\rightarrow}}$ и $Y_{j_{\rightarrow}}$ найдется N^{k-2}, причем $\forall j \in \{1,2,\ldots,N^{k-2}\} : |S_j| \geq 2$. Следовательно, в независимости от порядка группы и любых других условий, общая сумма $|S| > 2$.

Таким образом, любая, допустимая каскадным методом комбинация значений параметров процедуры-фильтра на уровне преобразования $k > 2$, приводит к уникальной последовательности на ее выходе и $\omega(N,k) = N^{k-1} \cdot \varphi(N) \cdot \nu(N,k-1)$.

Количество последовательностей, формируемыхо на k-том уровне преобразований при $k > 2$ составляет:

$$\nu(N,k) = N^k \cdot \varphi(N) \cdot \nu(N,k-1). \qquad (9)$$

Вывод

Формулы (2), (8) и (9) позволяют вычислить количество последовательностей, порождаемых каскадным методом, в зависимости от N и $k = 1$, $k = 2$ и $k > 2$ соответственно. Видно, что при $N > 3$, формулу (9) можно обобщить и на случай $k \geq 2$.

Формула (9) рекурсивна. Пусть $N > 3$. Избавимся от рекурсии.

$$\nu(N,1) = N \cdot \varphi(N);$$
$$\nu(N,2) = N^2 \cdot \varphi(N) \cdot \nu(N,1) = N^2 \cdot N \cdot \varphi(N)^2;$$
$$\nu(N,3) = N^3 \cdot \varphi(N) \cdot \nu(N,2) = N^3 \cdot N^2 \cdot N \cdot \varphi(N)^3;$$
$$\ldots$$
$$\nu(N,k) = \prod_{j=1}^{k} N^j \cdot \varphi(N)^k = N^{\sum_{j=1}^{k} j} \cdot \varphi(N)^k = N^{\frac{k^2+k}{2}} \cdot \varphi(N)^k.$$

В случае $N = 3$ можно провести аналогичные рассуждения, но с учетом того, что $\nu(N,2) = \frac{N^2 \cdot N \cdot \varphi(N)^2}{2}$. В итоге получим, что при $N = 3$ и $k \geq 2$:

$$\nu(N,k) = \frac{N^{\frac{k^2+k}{2}} \cdot \varphi(N)^k}{2}.$$

Сведя эти промежуточные результаты в единое целое, окончательно получаем зависимость количества последовательностей от порядка группы и количества уровней преобразования:

$$\nu(N,k)=\begin{cases} N\cdot\varphi(N), \text{если } k=1 \text{ и } N=3; \\ \dfrac{N^{\frac{k^2+k}{2}}\cdot\varphi(N)^k}{2}, \text{если } k\geq 2 \text{ и } N=3; \\ N^{\frac{k^2+k}{2}}\cdot\varphi(N)^k, \text{во всех остальных случаях.} \end{cases}$$

Список литературы

1. Румбешт В.В. Каскадный метод порождения периодических последовательностей над элементами циклической группы // Научные ведомости БелГУ. Серия: История. Политология. Экономика. Информатика. № 8 (179) 2014 Выпуск 30/1. Белгород: БелГУ, С. 103-112.

EVALUATION OF THE NUMBER OF SEQUENCES GENERATED BY THE CASCADE METHOD

V.V. RUMBESHT
A.Z. YADUTA

Belgorod State National Research University

e-mail: rumbesht@bsu.edu.ru

In this article, we derive a formula that estimates the number of sequences generated by a cascade method, depending on the order of the group and the number of cascades.

Key words: cascade method, cumulative sequence, the number of sequences.