УДК 004.421.5

КАСКАДНЫЙ МЕТОД ПОРОЖДЕНИЯ ПЕРИОДИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НАД ЭЛЕМЕНТАМИ ЦИКЛИЧЕСКОЙ ГРУППЫ

В.В. РУМБЕШТ

Белгородский государственный национальный исследовательский университет, г. Белгород

e-mail: rumbesht@bsu.edu.ru

В статье предлагается метод порождения периодических последовательностей над элементами циклической группы, основанный на последовательном применении однотипных преобразований (каскадов). Показано, что наращивание количества уровней преобразований на один позволяет увеличить период порождаемой последовательности в количество раз, равное порядку группы.

Ключевые слова: порождение последовательностей, период последовательности, циклическая группа.

Иногда в различных прикладных областях информационных технологий возникает потребность в порождении периодических последовательностей содержащих элементы некоторого конечного множества [2]. На практике данная потребность удовлетворяется путем применения программных или аппаратных генераторов (датчиков) псевдослучайных последовательностей [1, 3]. Каждая предметная область предъявляет свои требования к используемым последовательностям и их генераторам. Однако, одним из общих свойств является большой период, формируемой последовательности [1, 3], причем прагматически считается, что чем больше этот период, тем лучше. Другим общим свойством является простота и эффективность аппаратной и программной реализации генератора [1].

Существующие генераторы, как правило, обладают этими свойствами. Тем не менее, в них существует ограничение на максимальный период порождаемой последовательности. Попытки преодолеть это ограничение приводят к нарушению концептуальной общности генератора и, как следствие, усложнению его реализации. Эта ситуация объясняется тем, что методы, положенные в основу построения данных генераторов, изначально закладывают ограничение на максимальный период (ограничение обуславливается количественной характеристикой математических объектов, используемых в методе, например, количестве элементов кольца вычетов или конечного поля, прядке подстановок, и т.п.) и не предусматривают естественного пути для его снятия. Таким образом, актуальной является задача разработки метода порождения периодических последовательностей над конечным множеством, основанного на концептуально едином математическом аппарате и обладающего возможностью варьировать их период сверх количественной характеристики этого аппарата.

Предлагаемый в статье метод является одним из решений указанной задачи. Он базируется на идее единообразного построения ряда последовательностей все более возрастающего периода так, что бы первая последовательность из этого ряда строилась наиболее простым способом, а при формировании членов каждой последующей использовались члены предыдущей, при этом требованием к любому уровню преобразования является формирование последовательности максимально возможного периода. В итоге получается несколько последовательных уровней преобразования (каскадов), в которых результатом каждого уровня является своя периодическая последовательность, зависящая от результата предыдущего уровня. Математическим объектом для построения метода выбрана циклическая группа, как наиболее простая в этом случае алгебраическая структура. Каскадное порождение последовательностей и математический объект, на базе которых они строятся, вынесены в название метода.

Математический аппарат каскадного метода

Формально, последовательность есть функция из множества натуральных чисел в некоторое множество произвольной природы. В данной статье областью значений, рассматриваемых последовательностей, является конечное множество $U=\{u\}$, состоящее из $N\geq 2$ элементов. Считаем, что на множестве U задана двухместная коммутативная операция $\otimes: U\times U\to U$, такая, что алгебраическая структура $<U,\otimes>$ является циклической группой. Далее групповую операцию будем называть умножением, и использовать мультипликативную символику. Нейтральный элемент группы будем обозначать символом e. Последовательность с такой областью значений назовем последовательностью над U и будем обозначать ее как $X_{\to}=(x_1,x_2,\ldots,x_i,\ldots)$, если речь будет идти об ее отдельных членах, или просто $X_{\to}$, если речь будет идти о последовательности в целом.

По определению [6], последовательность $X_{\to}=(x_1,x_2,\ldots,x_i,\ldots)$ называется периодической с предпериодом λ и периодом τ, если $\lambda+1$ и τ – наименьшие из натуральных чисел, при которых $x_{i+\tau}=x_i$ для всех натуральных $i>\lambda$. Если $\lambda=0$, то последовательность называется чисто периодической. Далее, вне определений и формулировок утверждений, когда будем говорить о последовательностях, всегда будем иметь ввиду чисто периодические последовательности.

Определение 1. *Периодическим отрезком* чисто периодической последовательности $X_{\to}=(x_1,x_2,\ldots,x_i,\ldots)$ с периодом τ будем называть упорядоченное мультимножество $[X_{\to}]$, составленное из всех ее членов, начиная с x_1 и заканчивая x_τ. Отношение линейного порядка для элементов периодического отрезка определяется естественным следованием членов последовательности.

Очевидно, что периодический отрезок однозначно определяет чисто периодическую последовательность.

Если абстрагироваться от упорядоченности периодического отрезка, т.е. рассматривать его как обычное мультимножество, то периодический отрезок можно описать так называемой характеристической функцией [5]. Характеристическая функция $\chi_{[X_{\to}]}: U\to\{0,1,\ldots\}$ из U во множество целых неотрицательных чисел ставит в соответствие каждому элементу $u\in U$ число, указывающее сколько раз данный элемент встречается в периодическом отрезке последовательности. Поскольку характеристическая функция периодического отрезка вводится без учета его упорядоченности, то она определяет не отдельно взятую последовательность, а целый класс последовательностей, обладающих одинаковыми структурными свойствами.

Одним из таких структурных свойств является τ – период последовательности, который в терминах характеристической функции выражается следующим образом: $\tau=\sum\limits_{\forall u\in U}\chi_{[X_{\to}]}(u)$.

Если периодическая последовательность является последовательностью над U – множеством элементов циклической группы, то структурным свойством последовательности так же является элемент группы, полученный путем перемножения всех элементов из периодического отрезка последовательности.

Определение 2. *Характеристическим элементом* $h_{X_{\to}}\in U$ чисто периодической последовательности $X_{\to}=(x_1,x_2,\ldots,x_i,\ldots)$ над U с периодом τ назовем элемент

$$h_{X_{\to}}=x_1\otimes x_2\otimes\ldots\otimes x_\tau, \qquad (1)$$

где все элементы, составляющее произведение, суть элементы периодического отрезка $[X_{\rightarrow}]$. Характеристический элемент можно так же выразить в терминах характеристической функции: $h_{X_{\rightarrow}} = \bigotimes_{\forall u \in U} u^{\chi_{[X_{\rightarrow}]}(u)}$.

Для любой группы конечного порядка N справедливо соотношение $\forall a \in U : a^N = e$. Кроме этого, в теории групп [4] существует понятие порядка элемента группы. Порядком $Ord(a)$ элемента группы $a \in U$ называется наименьшее натуральное число q, такое что $a^q = e$.

По определению циклической группы [4], в группе $<U, \otimes>$ существуют элементы, порядок которых совпадает с ее порядком. Эти элементы обычно называются образующими элементами. Если указать образующий элемент $g \in U$, то любой элемент $a \in U$ может быть представлен в виде $a = g^{q \cdot N + r}$, где q, r – целые неотрицательные числа, N – порядок группы, причем $r < N$. Число r назовем *индексом* элемента a по основанию g, и будем обозначать $Ind(a)$.

Для любого элемента $a \in U$ циклической группы $<U, \otimes>$ порядка N между $Ord(a)$ и $Ind(a)$ истинно отношение [4]:

$$Ord(a) = \frac{N}{\gcd(Ind(a), N)}, \qquad (2)$$

где $\gcd(x, y)$ – наибольший общий делитель чисел x и y.

Выражение (2) устанавливает однозначное соответствие между индексами и порядками элементов. Обратное соответствие, за исключением групп второго порядка, не является однозначным, т.е. в циклической группе порядка большего 2 существуют неравные меду собой элементы, имеющие одинаковый порядок. В частности, в любой циклической группе существует ровно $\varphi(N)$ образующих элементов, где φ – функция Эйлера [3].

Обозначим символом $G_{<U,\otimes>}$ множество образующих элементов циклической группы $<U, \otimes>$. В этом множестве будем особо выделять элемент $g_{Base} \in G_{<U,\otimes>}$. Назовем его "базовым", поскольку индексы элементов группы будем рассматривать по его основанию. Все элементы множества $G_{<U,\otimes>}$ можно получить, возводя g_{Base} в степени меньшие чем порядок группы и взаимно простые с ним.

Таким образом, помимо характеристического элемента $h_{X_{\rightarrow}}$ к структурным свойствам последовательности $X_{\rightarrow}$ относятся так же его индекс $Ind(h_{X_{\rightarrow}})$ и порядок $Ord(h_{X_{\rightarrow}})$. Индекс характеристического элемента представляет собой сумму индексов всех элементов, входящих в периодический отрезок, взятую по модулю порядка группы N: $Ind(h_{X_{\rightarrow}}) = \left(\sum_{i=1}^{\tau} Ind(x_i)\right) \bmod N$. Порядок характеристического элемента вычисляется по известному индексу и порядку группы с помощью формулы (2).

Через характеристическую функцию перечисленные структурные свойства определяются следующим образом:

$$Ind(h_{X_{\rightarrow}}) = \left(\sum_{\forall u \in U} (Ind(u) \cdot \chi_{[X_{\rightarrow}]}(u))\right) \bmod N; \qquad (3)$$

$$Ord(h_{X_{\rightarrow}}) = \frac{N}{gcd\left(\left(\sum_{\forall u \in U} (Ind(u) \cdot \chi_{[X_{\rightarrow}]}(u))\right) \bmod N, N\right)}. \qquad (4)$$

Введем понятие кумулятивной последовательности и докажем два важных для определения каскадного метода утверждения, касающихся структурных свойств кумулятивных последовательностей.

Определение 3. Пусть $X_{\to} = (x_1, x_2, \ldots, x_i, \ldots)$ и $Y_{\to} = (y_1, y_2, \ldots, y_i, \ldots)$ последовательности над U. Последовательность $X_{\to}$ называется *порождающей* по отношению к $Y_{\to}$, если существует элемент $y_0 \in U$ и для всех натуральных i имеет место: $y_i = y_{i-1} \otimes x_i$. Такой $y_0 \in U$ назовем *начальным элементом*, а $Y_{\to}$ – *кумулятивной последовательностью* с начальным элементом y_0 и порождающей $X_{\to}$.

Утверждение 1. Если последовательность $X_{\to}$ над U является чисто периодической с периодом τ, то кумулятивная последовательность $Y_{\to}$ с начальным элементом y_0 и порождающей $X_{\to}$, так же является чисто периодической над U с периодом

$$\pi = \tau \cdot Ord(h_{X_{\to}}), \tag{5}$$

где $h_{X_{\to}}$ – характеристический элемент $X_{\to}$.

Доказательство. Из определения кумулятивной последовательности явно следует, что последовательность $Y_{\to}$ является последовательностью над U. В последовательности $Y_{\to}$ выберем произвольный член y_k. Свойство периодичности $Y_{\to}$ может возникнуть тогда, когда существует минимальное π, такое, что $y_{k+\pi} = y_k$ и π кратно τ. Пусть $n = \pi/\tau$, тогда по определениям 2 и 3 имеет место $y_{k+\pi} = y_k \otimes h^n_{X_{\to}}$. Если $n = Ord(h_{X_{\to}})$, то $h^n_{X_{\to}} = e$. Отсюда следует, что $y_{k+\pi} = y_k \otimes h^n_{X_{\to}} = y_k$. По определению прядка элемента группы, n – такое минимально возможное целое число. Тогда $\pi = \tau \cdot n = \tau \cdot Ord(h_{X_{\to}})$ – минимальное целое, такое, что $y_{k+\pi} = y_k$. Это доказывает существование и единственность π. Поскольку элемент y_k выбран произвольным образом, то можем положить $k = 1$. Следовательно, $Y_{\to}$ – чисто периодическая последовательность. *Что и требовалось доказать.*

Таким образом, структурные свойства чисто периодической кумулятивной последовательности зависят от структурных свойств порождающей последовательности. В частности, минимальный период кумулятивной последовательности совпадает с τ – периодом порождающей последовательности (при $h_{X_{\to}} = e$), а максимальный период равен $\tau \cdot N$ (при $h_{X_{\to}} \in G_{<U,\otimes>}$).

Утверждение 2. Если характеристический элемент $h_{X_{\to}}$ последовательности $X_{\to}$ с периодом τ является образующим элементом группы ($h_{X_{\to}} \in G_{<U,\otimes>}$), то структурные свойства кумулятивной последовательности $Y_{\to}$ с начальным элементом y_0 и порождающей $X_{\to}$ выражаются характеристической функцией $\forall u \in U : \chi_{[Y_{\to}]}(u) = \tau$, или, другими словами, периодический отрезок содержит все элементы группы, причем каждый элемент встречается ровно τ раз.

Доказательство. Согласно утверждению 1 период кумулятивной последовательности составляет $\pi = N \cdot \tau$. Если разбить периодический отрезок $[Y_{\to}]$ на N участков, то несложно заметить, что $y_{\tau+1} = y_1 \otimes h_{X_{\to}}$, $y_{2\cdot\tau+1} = y_1 \otimes h^2_{X_{\to}}$,... $y_{N\cdot\tau+1} = y_1 \otimes h^N_{X_{\to}} = y_1$. Поскольку $h_{X_{\to}}$ является образующим группы, то элементы $y_1, y_{\tau+1}, y_{2\cdot\tau+1}, \ldots, y_{(N-1)\cdot\tau+1}$ пробегают все множество U. Аналогичные рассуждения можно

провести для y_i, где $i = 2,3,\ldots\tau$. Таким образом, получается, что периодический отрезок содержит все элементы группы, причем каждый элемент встречается ровно τ раз. *Что и требовалось доказать.*

Описание каскадного метода

Понятия порождающей и кумулятивной последовательностей (см. определение 3), а так же свойство изменения периода кумулятивной последовательности по отношению к порождающей (см. утверждение 1) позволяют реализовать идею каскадного метода. При этом утверждение 2 гарантирует увеличение периода кумулятивной последовательности по отношению к периоду порождающей в N раз, где N – прядок группы.

Основу метода составляет *процедура-генератор*, позволяющая на основании заданных параметров и своего внутреннего состояния за каждый акт ее использования порождать очередной элемент последовательности.

Простейшим примером такой процедуры является *процедура порождения стационарной последовательности*. Стационарная последовательность (СП) – это периодическая последовательность с периодом равным 1. Параметром этой процедуры является элемент u множества U, над которым строится последовательность. Внутренним состоянием она не обладает. После каждого обращения к этой процедуре она выдает на выход значение своего параметра, то есть u.

Дальнейшим развитием процедуры-генератора выступает *процедура порождения кумулятивной последовательности* (процедура порождения КП) (см. рис 1).

Рис. 1. Процедура порождения КП как черный ящик

Параметрами этой процедуры выступают начальный элемент и очередной член порождающей 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 порождающей последовательности. При этом очередное внутреннее состояние принимается равным выходу.

Не сложно заметить, что процедура порождения КП является обобщением процедуры порождения СП. Это утверждение становится очевидным, если процедура порождения КП примет в качестве начального элемента $u \in U$, а в качестве очередного элемента порождающей последовательности каждый раз будет выступать нейтральный элемент группы.

Если последовательно применить эти две процедуры, так, что бы выход процедуры порождения СП являлся входом процедуры порождения КП, то в зависимости от выбора начального элемента $u \in U$ период результирующей последовательности может изменяться от 1 до N. Эффект получения результирующей последовательности максимального периода N возникает, если $u \in G_{<U,\otimes>}$. Этот эффект соответствует циклическому перечислению всех элементов группы, что давно известно и используется в частности в мультипликативных конгруэнтных генераторах [3].

Элемент $u \in G_{<U,\otimes>}$ обозначим символом $g^{(1)}$. И дополнительно введем обозначения: $X^{(1)}_{\rightarrow} = (x^{(1)}_1, x^{(1)}_2, \ldots x^{(1)}_i, \ldots)$ – последовательность, полученная описанным выше способом, $\chi_{[X^{(1)}_{\rightarrow}]}$, $x^{(1)}_0$, $h_{X^{(1)}_{\rightarrow}}$ и $\pi^{(1)}$ – характеристическая функция ее периодического отрезка, начальный элемент, характеристический элемент и период соответственно.

Более того, далее будем считать, что верхний индекс, указанный в скобках, будет выражать уровень преобразования.

Во введенных обозначениях последовательность $X_{\rightarrow}^{(1)} = (x_1^{(1)}, x_2^{(1)}, \ldots x_i^{(1)}, \ldots)$ первого уровня преобразования определяется выражением:

$$x_0^{(1)} \in U,\ g^{(1)} \in G_{<U,\otimes>},$$
$$\forall i \in \{1, 2, \ldots\}:\ x_i^{(1)} = x_{i-1}^{(1)} \otimes g^{(1)}. \qquad (6)$$

Пусть $\forall u \in U:\ \chi_{[X_{\rightarrow}^{(1)}]}(u) = 1$ и, соответственно $\pi^{(1)} = N$. Посмотрим, как зависит период $\pi^{(2)}$ последовательности $X_{\rightarrow}^{(2)} = (x_1^{(2)}, x_2^{(2)}, \ldots x_i^{(2)}, \ldots)$ полученной посредством процедуры порождения КП, на вход которой подаются члены $X_{\rightarrow}^{(1)}$.

По формуле (5) этот период зависит от $Ord(h_{X_{\rightarrow}^{(1)}})$, а учитывая (2) от $Ind(h_{X_{\rightarrow}^{(1)}})$. По формуле (3) имеем: $Ind(h_{X_{\rightarrow}^{(1)}}) = \left(\sum_{\forall u \in U} (Ind(u) \cdot \chi_{[X_{\rightarrow}^{(1)}]}(u)) \right) \bmod N = \left(\sum_{\forall u \in U} Ind(u) \right) \bmod N$. Учитывая, что индексы всех элементов U пробегают числа от 0 до $N-1$, получим:

$$Ind(h_{X_{\rightarrow}^{(1)}}) = \left(\sum_{j=0}^{N-1} j \right) \bmod N = \left(N \cdot (N-1)/2 \right) \bmod N.$$

Несложно заметить, что это выражение может принимать только два значения:

$$Ind(h_{X_{\rightarrow}^{(1)}}) = \begin{cases} 0, \textit{если } N \textit{ нечетное}; \\ N/2, \textit{если } N \textit{ четное}. \end{cases}$$

То есть характеристический элемент $h_{X_{\rightarrow}^{(1)}}$ является нейтральным элементом группы, если N нечетно, или элементом второго порядка, равным $g_{Base}^{N/2}$, если N четно.

В итоге получается, что такое наращивание уровня преобразования не приводит к желаемому эффекту – увеличению периода результирующей последовательности в N раз. Период результирующей последовательности увеличится в 2 раза, либо вообще не увеличится.

Одним из возможных решений возникшей проблемы является преобразование $X_{\rightarrow}^{(1)} = (x_1^{(1)}, x_2^{(1)}, \ldots x_i^{(1)}, \ldots)$ в последовательность $\widetilde{X}_{\rightarrow}^{(1)} = (\widetilde{x}_1^{(1)}, \widetilde{x}_2^{(1)}, \ldots \widetilde{x}_i^{(1)}, \ldots)$ такого же периода $\pi^{(1)}$, что бы $\widetilde{X}_{\rightarrow}^{(1)}$ на периодическом отрезке отличалась от $X_{\rightarrow}^{(1)}$ не более чем одним элементом и при этом $h_{\widetilde{X}_{\rightarrow}^{(1)}} \in G_{<U,\otimes>}$. Как один из вариантов такого решения можно предложить следующее. Зададим желаемый характеристический элемент $h_{\widetilde{X}_{\rightarrow}^{(1)}} \in G_{<U,\otimes>}$ (обозначим его $g^{(2)}$) и целое $0 \le m \le \pi^{(1)} - 1$. Преобразование заключается в:

$$\forall i \in \{1,2,\ldots\}: \widetilde{x}_i^{(1)} = \begin{cases} x_i^{(1)}, \textit{если } m \neq i \bmod \pi^{(1)}; \\ x_i^{(1)} \otimes g^{(2)}, \textit{если } m \equiv i \bmod \pi^{(1)} \textit{ и } N \textit{ нечетное}; \\ x_i^{(1)} \otimes g^{(2)} \otimes g_{Base}^{N/2}, \textit{если } m \equiv i \bmod \pi^{(1)} \textit{ и } N \textit{ четное}. \end{cases}$$

Таким образом, преобразование заключается в замене каждого i-го члена последовательности $X_{\rightarrow}^{(1)}$, находящегося в позиции m сравнимой с i по модулю $\pi^{(1)}$, на элемент зависящий от $x_i^{(1)}$, $g^{(2)}$ и четности порядка группы. Число m назовем позицией замены.

Приведенные выше рассуждения приводят к введению дополнительной *процедуры-фильтра*, которая принимает на вход члены периодической последовательности, а так же заданные для замены параметры и формирует в качестве результата соответствующие члены выходной периодической последовательности (см. рис. 2). Параметрами, использующимися для замены, являются характеристический

элемент выходной последовательности, позиция замены и период входной последовательности. Последний параметр обозначим символом D.

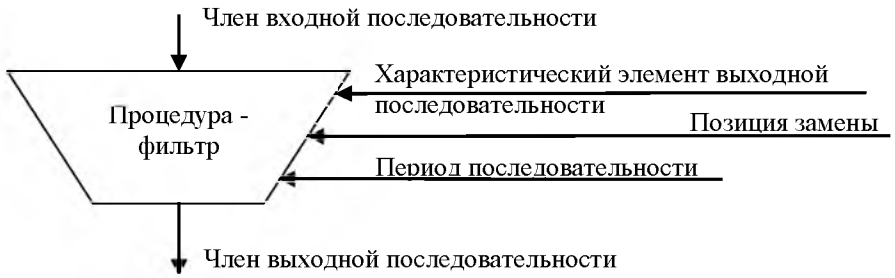

Рис. 2. Процедура-фильтр как черный ящик

Действие процедуры-фильтра заключается в следующем:

$$\widetilde{x}_i = \begin{cases} x_i, \text{если } m \neq (i \bmod D); \\ x_i \otimes z, \text{если } m = (i \bmod D). \end{cases} \quad (7)$$

Здесь x_i, $\widetilde{x}_i$ – члены входной и выходной последовательности соответственно, z – элемент U, зависящий от уровня преобразования и четности порядка группы. В частности для второго уровня преобразования $z = \begin{cases} g^{(2)}, \text{если } N \text{ нечетно}; \\ g^{(2)} \otimes g_{Base}^{N/2}, \text{если } N \text{ четно}; \end{cases}$, и как будет показано дальше $\forall k > 2$: $z = g^{(k)}$. Фактически для любого уровня преобразования $z = g^{(k)} \otimes h^{-1}_{X_{\rightarrow}^{(k-1)}}$.

Таким образом, второй уровень преобразования состоит в последовательном применении процедуры-фильтра и процедуры порождения КП. На вход процедуры-фильтра подаются члены последовательности $X_{\rightarrow}^{(1)} = (x_1^{(1)}, x_2^{(1)}, \ldots x_i^{(1)}, \ldots)$, характеристический элемент $g^{(2)} \in G_{<U,\otimes>}$, позиция замены $m^{(2)} \in \{0, 1, \ldots, N-1\}$ и период $D = N$. Сформированные этой процедурой члены порождающей последовательности $\widetilde{X}_{\rightarrow}^{(1)} = (\widetilde{x}_1^{(1)}, \widetilde{x}_2^{(1)}, \ldots \widetilde{x}_i^{(1)}, \ldots)$ вместе с параметром $x_0^{(2)} \in U$ подаются на вход процедуры порождения КП, которая и формирует последовательность второго уровня преобразования $X_{\rightarrow}^{(2)} = (x_1^{(2)}, x_2^{(2)}, \ldots x_i^{(2)}, \ldots)$.

Во введенных обозначениях $X_{\rightarrow}^{(2)} = (x_1^{(2)}, x_2^{(2)}, \ldots x_i^{(2)}, \ldots)$ определяется выражением:

$$x_0^{(2)} \in U,\ g^{(2)} \in G_{<U,\otimes>},\ m^{(2)} \in \{0, 1, \ldots, N-1\}$$
$$\forall i \in \{1, 2, \ldots\}:\ x_i^{(2)} = \begin{cases} x_{i-1}^{(2)} \otimes x_i^{(1)}, \text{если } m^{(2)} \neq (i \bmod N), \\ x_{i-1}^{(2)} \otimes x_i^{(1)} \otimes g^{(2)}, \text{если } m^{(2)} = (i \bmod N) \text{ и } N \text{ нечетно}, \\ x_{i-1}^{(2)} \otimes x_i^{(1)} \otimes g^{(2)} \otimes g_{Base}^{N/2}, \text{если } m^{(2)} = (i \bmod N) \text{ и } N \text{ четно}. \end{cases} \quad (8)$$

Как было показано выше, $(h_{\widetilde{X}_{\rightarrow}^{(1)}} = g^{(2)}) \in G_{<U,\otimes>}$, последовательность $\widetilde{X}_{\rightarrow}^{(1)}$ имеет период $\pi^{(1)} = N$ и является порождающей для $X_{\rightarrow}^{(2)}$. Следовательно, согласно утверждениям 1 и 2: $\forall u \in U : \chi_{[X_{\rightarrow}^{(2)}]}(u) = N$ и $\pi^{(2)} = N^2$. Более того, не сложно заметить, что $Ind(h_{X_{\rightarrow}^{(2)}}) = 0$, а $h_{X_{\rightarrow}^{(2)}} = e$ в независимости от четности порядка группы.

По этому, если использовать последовательность $X_{\rightarrow}^{(2)}$ в качестве входной на третьем уровне преобразования, формирующем кумулятивную последовательность $X_{\rightarrow}^{(3)} = (x_1^{(3)}, x_2^{(3)}, \ldots x_i^{(3)}, \ldots)$ максимального периода $\pi^{(3)} = N^3$, то сначала ее необходимо

подвергнуть обработке процедурой-фильтром с параметрами: $g^{(3)} \in G_{<U,\otimes>}$, $m^{(3)} \in \{0,1,\ldots, N^2-1\}$ и $D = N^2$. Сформированную процедурой-фильтром последовательность $\widetilde{X}_{\rightarrow}^{(2)}$ подаем на вход процедуры порождения КП, которая и выдает члены $X_{\rightarrow}^{(3)}$. Для последовательности $X_{\rightarrow}^{(3)}$ характерно $\forall u \in U : \chi_{[X_{\rightarrow}^{(3)}]}(u) = N^2$, $\pi^{(3)} = N^3$, $Ind(h_{X_{\rightarrow}^{(3)}}) = 0$ и $h_{X_{\rightarrow}^{(3)}} = e$.

Четвертый и все последующие уровни преобразования могут быть построены аналогично третьему. Таким образом, последовательность $X_{\rightarrow}^{(k)} = (x_1^{(k)}, x_2^{(k)}, \ldots x_i^{(k)}, \ldots)$, формируемая k-тым уровнем преобразования ($k \geq 3$), определяется выражением:

$$\forall k \in \{3,4,\ldots\} : x_0^{(k)} \in U,\ g^{(k)} \in G_{<U,\otimes>},\ m^{(k)} \in \{0,1,\ldots, N^{k-1}-1\}$$
$$\forall i \in \{1,2,\ldots\} :\ x_i^{(k)} = \begin{cases} x_{i-1}^{(k)} \otimes x_i^{(k-1)}, \text{ если } m^{(k)} \neq (i \bmod N^{k-1}); \\ x_{i-1}^{(k)} \otimes x_i^{(k-1)} \otimes g^{(k)}, \text{ если } m^{(k)} = (i \bmod N^{k-1}). \end{cases} \quad (9)$$

Структурные свойства последовательности $X_{\rightarrow}^{(k)}$ для $k \geq 3$: $\forall u \in U : \chi_{[X_{\rightarrow}^{(k)}]}(u) = N^{k-1}$, $\pi^{(k)} = N^k$, $Ind(h_{X_{\rightarrow}^{(k)}}) = 0$ и $h_{X_{\rightarrow}^{(k)}} = e$.

На рис. 3 приведена схема порождения периодических последовательностей каскадным методом.

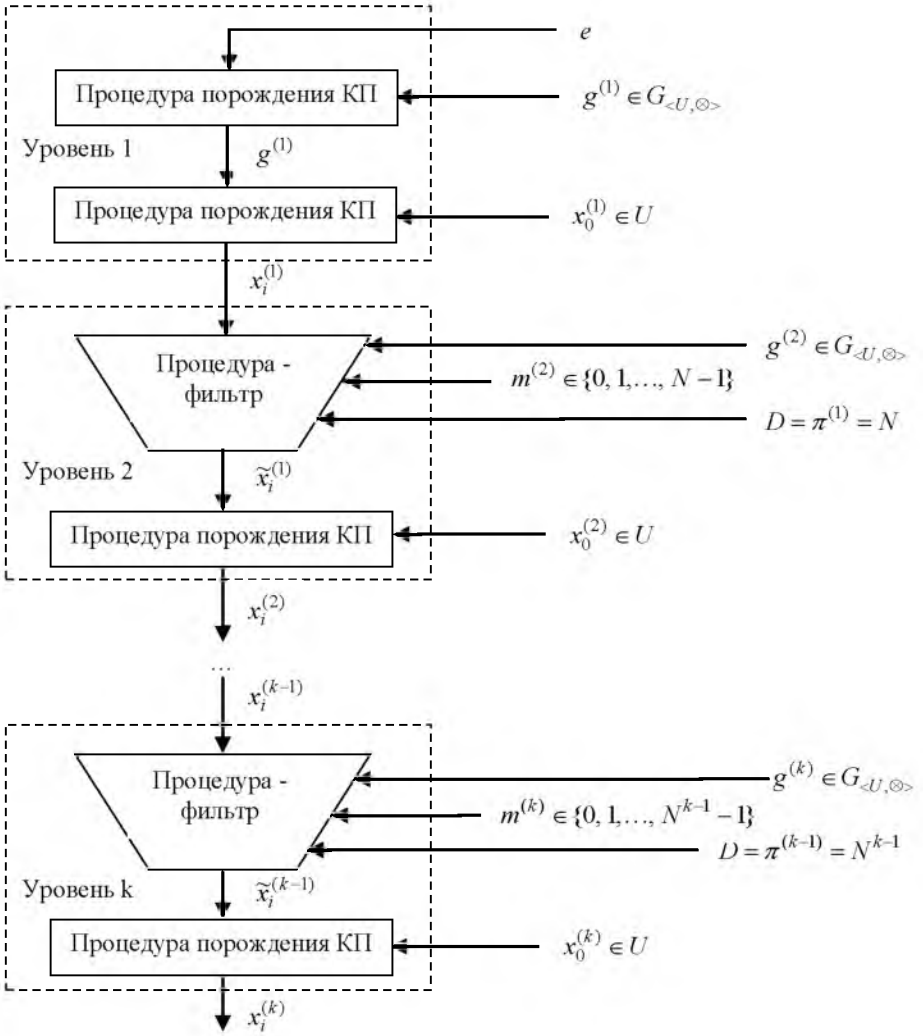

Рис. 3. Схема порождения периодических последовательностей

Пример применения каскадного метода

Пусть $U=\{0,1,2,3\}$, $N=4$, а групповая операция $\otimes$ – сумма по модулю 4. В этой группе нейтральный элемент $e=0$. Группа $<U,\otimes>$ является циклической. В качестве g_{Base} выберем 1. Множество образующих элементов данной группы суть $G_{<U,\otimes>}=\{1,3\}$. Элемент второго порядка $g_{Base}^{N/2}=2$.

Приведем пример применения каскадного метода порождения периодических последовательностей, в котором в качестве группы будем использовать $<U,\otimes>$. Ограничимся тремя уровнями преобразования.

Первый уровень преобразования. Параметрами этого уровня являются $x_0^{(1)}\in U$ и $g^{(1)}\in G_{<U,\otimes>}$. Пусть $x_0^{(1)}=2$, а $g^{(1)}=3$. В соответствии с формулой (6) получим выходную кумулятивную последовательность: $X_{\rightarrow}^{(1)}=(1,0,3,2,\ldots)$. Несложно видеть, что период этой последовательности $\pi^{(1)}=N=4$, характеристическая функция принимает значения: $\chi_{[X_{\rightarrow}^{(1)}]}(0)=1$, $\chi_{[X_{\rightarrow}^{(1)}]}(1)=1$, $\chi_{[X_{\rightarrow}^{(1)}]}(2)=1$, $\chi_{[X_{\rightarrow}^{(1)}]}(3)=1$, характеристический элемент $h_{X_{\rightarrow}^{(1)}}=g_{Base}^{N/2}=2$.

Второй уровень преобразования. Параметрами процедуры-фильтра на этом уровне являются $g^{(2)}\in G_{<U,\otimes>}$, $m^{(2)}\in\{0,1,2,3\}$ и $D=N=4$. Пусть $g^{(2)}=1$ и $m^{(2)}=2$. В соответствии с формулой (7) при четном порядке группы $z=g^{(2)}\otimes g_{Base}^{N/2}=1\otimes 2=3$ и процедура-фильтр на выходе выдаст члены последовательности: $\widetilde{X}_{\rightarrow}^{(1)}=(1,3,3,2,\ldots)$. Характеристическая функция принимает значения: $\chi_{[\widetilde{X}_{\rightarrow}^{(1)}]}(0)=0$, $\chi_{[\widetilde{X}_{\rightarrow}^{(1)}]}(1)=1$, $\chi_{[\widetilde{X}_{\rightarrow}^{(1)}]}(2)=1$, $\chi_{[\widetilde{X}_{\rightarrow}^{(1)}]}(3)=2$, а характеристический элемент $h_{\widetilde{X}_{\rightarrow}^{(1)}}=g^{(2)}=1$.

Члены последовательности $\widetilde{X}_{\rightarrow}^{(1)}$ подаются на вход процедуры порождения КП, имеющей параметр $x_0^{(2)}\in U$. Пусть $x_0^{(2)}=1$. В соответствии с формулой (8) на выходе процедуры порождения КП будет формироваться следующая кумулятивная последовательность:

$$X_{\rightarrow}^{(2)}=(2,1,0,2,3,2,1,3,0,3,2,0,1,0,3,1,\ldots).$$

Период этой последовательности $\pi^{(2)}=N^2=16$, характеристическая функция принимает значения $\chi_{[X_{\rightarrow}^{(2)}]}(0)=4$, $\chi_{[X_{\rightarrow}^{(2)}]}(1)=4$, $\chi_{[X_{\rightarrow}^{(2)}]}(2)=4$, $\chi_{[X_{\rightarrow}^{(2)}]}(3)=4$, а характеристический элемент $h_{X_{\rightarrow}^{(2)}}=e=0$.

Третий уровень преобразования. Параметрами процедуры-фильтра на этом уровне являются $g^{(3)}\in G_{<U,\otimes>}$, $m^{(3)}\in\{0,1,\ldots,15\}$ и $D=N^2=16$. Пусть $g^{(3)}=1$ и $m^{(3)}=9$. В соответствии с формулой (7) вне зависимости от четности порядка группы $z=g^{(3)}=1$ и процедура-фильтр на выходе выдаст члены последовательности: $\widetilde{X}_{\rightarrow}^{2}=(2,1,0,2,3,2,1,3,1,3,2,0,1,0,3,1,\ldots)$. Характеристическая функция этой последовательности принимает значения: $\chi_{[\widetilde{X}_{\rightarrow}^{(2)}]}(0)=3$, $\chi_{[\widetilde{X}_{\rightarrow}^{(2)}]}(1)=5$, $\chi_{[\widetilde{X}_{\rightarrow}^{(2)}]}(2)=4$, $\chi_{[\widetilde{X}_{\rightarrow}^{(2)}]}(3)=4$, а характеристический элемент $h_{\widetilde{X}_{\rightarrow}^{(2)}}=g^{(3)}=1$.

Члены последовательности $\widetilde{X}_{\rightarrow}^{2}$ подаются на вход процедуры порождения КП, имеющей параметр $x_0^{(3)}\in U$. Пусть $x_0^{(3)}=3$. В соответствии с формулой (9) при $k=3$ на выходе процедуры порождения КП будет формироваться последовательность:

$$X_{\rightarrow}^{(3)}=(1,2,2,0,3,1,2,1,2,1,3,3,0,0,3,0,2,3,3,1,0,2,3,2,3,2,0,0,1,1,0,1,$$
$$3,0,0,2,1,3,0,3,0,3,1,1,2,2,1,2,0,1,1,3,2,0,1,0,1,0,2,2,3,3,2,3,\ldots)$$

Таким образом, период последовательности, формируемой третьим уровнем преобразования, составляет $\pi^{(3)} = N^3 = 64$. Ее характеристическая функция принимает значения: $\chi_{[X^{(3)}_{\rightarrow}]}(0) = 16$, $\chi_{[X^{(3)}_{\rightarrow}]}(1) = 16$, $\chi_{[X^{(3)}_{\rightarrow}]}(2) = 16$, $\chi_{[X^{(3)}_{\rightarrow}]}(3) = 16$, а характеристический элемент $h_{X^{(3)}_{\rightarrow}} = e = 0$.

Заключение

Описание и пример применения каскадного метода демонстрируют его возможности по наращиванию максимального периода порождаемых последовательностей в зависимости от порядка группы и количества уровней. Эта зависимость выражается формулой: $\pi = N^k$, где π – период порождаемой последовательности, N – порядок группы, k – количество каскадов.

Если провести сравнение предложенного метода, например с мультипликативным конгруэнтным генератором [3] по модулю 257, то максимальный период, который можно "выжать" из конгруэнтного генератора составляет 256, и члены порождаемой им последовательности пробегают все числа от 1 до 256. Аналогичные результаты можно получить и каскадным методом, применяя мультипликативную группу $GF(257)$ и используя только один уровень преобразования. Более того, указанный мультипликативный конгруэнтный генератор практически делает то же самое, что и первый уровень преобразования в каскадном методе. Увеличив количество каскадов до 2 максимальный период последовательностей, порождаемых каскадным методом, составит уже 65536. Ну и вообще, наращивание каскадов на 1 приводит к увеличению максимального периода в 256 раз.

Все каскады, ну может быть за исключение первого, устроены одинаково, что придает методу определенную концептуальную общность. Это в свою очередь создает преимущества в простоте и эффективности программной или аппаратной реализации метода.

Достоинством каскадного метода является то, что он сформулирован для абстрактной циклической группы, и соответственно при его реализации имеется возможность выбора конкретной группы, и даже совмещения в одной реализации нескольких конкретных групп. Что еще больше увеличивает "гибкость" предложенного метода.

Список литературы

1. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

2. Корсунов Н.И., Титов А.И. Повышение эффективности зашиты информации модификацией шифра Вижинера // Научные ведомости БелГУ. – 10. N 7 (78) вып. 14. – С. 171 – 175.

3. Кнут Д. Искусство программирования, том 2. Получисленные алгоритмы = The Art of Computer Programming, vol.2. Seminumerical Algorithms – 3-е изд. – М.: Вильямс, 2007. – 832 с.

4. Курош А.Г. Теория групп. – М.: Наука, 1967. – 648 с.

5. Петровский А.Б. Основные понятия теории мультимножеств. – М.: Едиториал УССР, 2002. – 80 с.

6. Фомичев В.М. Дискретная математика и криптология. – М.: Диалог-МИФИ, 2003. –400 с.

THE CASCADE METHOD OF GENERATION OF PERIODIC SEQUENCES OVER ELEMENTS OF A CYCLIC GROUP

V.V. RUMBESHT

Belgorod National Research University, Belgorod

e-mail: rumbesht@bsu.edu.ru

The article proposes a method of generation of periodic sequences over elements of cyclic groups based on the consistent application of similar transformations (cascades). It is shown that increasing the number of levels of conversions per allows to increase a period generated sequence in the number of times equal to the order of the group.

Key words: generating sequences, the period of the sequence, a cyclic group.