УДК 004.421.5

АНАЛИЗ ПРИМЕНЕНИЯ КОНКРЕТНЫХ ГРУПП В КАСКАДНОМ МЕТОДЕ

ANALYSIS OF THE APPLICATION SPECIFIC GROUPS IN THE CASCADE METHOD

В.В. Румбешт, А.З. Ядута
V.V. Rumbesht, A.Z. Yaduta

Белгородский государственный национальный исследовательский университет,Россия, 308015, Белгород, ул. Победы, 85
Belgorod State National Research University, 85 Pobeda St, Belgorod, 308015, Russia

e-mail: rumbesht@bsu.edu.ru, yaduta@bsu.edu.ru

Аннотация. В статье проводится анализ применения конкретных групп в каскадном методе.
Для этого определяется множество операций, элементы которого будут использоваться для конкретизации циклической группы, и оценивается его мощность. Затем на этом множестве операций вводится отношение конгруэнтности. Далее формулируется и доказывается утверждение об условиях равенства кумулятивных последовательностей с учетом применения различных конкретных групп, вводится формальное определение конфигурации каскадов и уточняется оценка количества последовательностей, порождаемых каскадным методом в любой допустимой конфигурации, рассматривается множество последовательностей, порождаемых во всех конфигурациях в целом, и устанавливается его мощность. В завершении статьи приводятся условия, при которых в каждой конфигурации формируется уникальное множество последовательностей.

Resume. The article analyzes the application of specific groups in a cascade method.
This defines the set of operations whose elements will be used to specify a cyclic group, and its capacity is estimated. Then on this set of operations is entered, the relation of congruence. Next we formulate and prove a statement about the equality of cumulative sequences with regard to the application of various specific groups, introduces a formal definition of the configuration of the cascades and refined the estimate of the number of sequences generated by the cascade method in any valid configuration, the set of sequences generated in all configurations in General, and set its power. At the end of the article describes the conditions under which each configuration is formed by a unique set of sequences.

Ключевые слова: каскадный метод, конфигурация каскадов, отношение конгруэнтности операций, кумулятивная последовательность, количество последовательностей.
Keywords: cascade method, the configuration of the cascades, congruence relation operations, cumulative sequence, the number of sequences.

Введение

Каскадный метод порождения периодических последовательностей, предложенный в статье [Румбешт, 2014], 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. Тем ни менее, в [Румбешт, 2014] отмечается, что при реализации каскадного метода имеется возможность выбора конкретной группы, и даже совмещения в одной реализации нескольких конкретных групп.

В работе [Румбешт, Ядута, 2014] показано, что конкретизация одной циклической группы позволяет установить состав множества порождаемых последовательностей и оценить его мощность. При этом конкретизация единственной группы сама по себе дает уникальный результат применения каскадного метода.

Другое дело, когда конкретизируется несколько групп (в идеале - все возможные конкретные циклические группы заданного конечного порядка), и предоставляется возможность применения на каждом уровне преобразования любой из них. Это приводит к появлению множества конфигураций каскадов. Совсем не очевидно, что метод в двух различных конфигурациях порождает уникальное множество последовательностей. Вполне возможна ситуация, при которой в двух различных конфигурациях порождаются пересекающиеся или даже совпадающие результаты.

Целью данной статьи является исследование влияния конфигураций каскадов на множество порождаемых последовательностей и нахождение условий, при которых каскадный метод в каждой допустимой конфигурации формировал свой уникальный результат.

Множество операций для конкретизации циклической группы

Вообще говоря, конкретизация группы предполагает точное указание множества ее элементов и точное указание алгоритма вычисления результата групповой операции. Для нашей цели

такая полная конкретизация не требуется. Мы будем исходить из того, что имеется произвольное конечное множество U, содержащее $N > 2$ элементов, и над ним задано множество двуместных операций, которые, совместно с U, образуют циклическую группу. Обозначим это множество операций символом Θ и определим его, как $\Theta = \{\otimes : U \times U \to U \mid < U, \otimes > - \textit{циклическая группа порядка } N\}$. Будем предполагать, что каждый элемент Θ задается таблицей Кэли. Исходя из этих постулатов, под конкретизацией группы будем понимать выбор конкретного элемента Θ.

Чтобы различать элементы множества Θ примем следующее определение.

Определение 1. Операция $\otimes \in \Theta$ равна операции $\overline{\otimes} \in \Theta$, если $\forall x, y \in U: \; x \otimes y = x \,\overline{\otimes}\, y$.

Для ответа на вопрос о количестве двуместных операций, образующих над U циклическую группу, сформулируем и докажем следующее утверждение.

Утверждение 1. Мощность множества Θ составляет $\frac{N!}{\varphi(N)}$, где N - порядок группы, φ - функция Эйлера.

Доказательство. Все циклические группы заданного порядка N изоморфны между собой. В частности, любая такая группа $< U, \otimes >$ изоморфна аддитивной группе кольца вычетов по модулю N. Обозначим аддитивную группу этого кольца как $< Z_N, + >$, где $Z_N = \{0, 1, \ldots, N-1\}$, "+" – операция сложения по модулю N. Рассмотрим изоморфизм $\psi : Z_N \to U$, такой, что $\forall z \in Z_N: \; \psi(z) = g^z$, где g - образующий элемент группы $< U, \otimes >$. Очевидно, что $\forall a, b \in Z_N: \; \psi(a) \otimes \psi(b) = g^a \otimes g^b = g^{a+b} = \psi(a+b)$.

Всего таких изоморфизмов существует столько, сколько существует перестановок из N элементов, то есть $N!$. Каждый из таких изоморфизмов зависит от операции $\otimes \in \Theta$ и выбора образующего элемента g. Для конкретной группы $< U, \otimes >$ существует $\varphi(N)$ возможностей выбора g. Следовательно, всего операций, образующих из U циклическую группу, есть $|\Theta| = \frac{N!}{\varphi(N)}$.

Что и требовалось доказать.

Отношение конгруэнтности операций

Определение 2. Операция $\otimes \in \Theta$ и операция $\overline{\otimes} \in \Theta$ называются конгруэнтными (обозначается $\otimes \simeq \overline{\otimes}$), если $\forall x, y \in U, \exists p \in U: \; x \,\overline{\otimes}\, y = x \otimes y \otimes p$ и $\forall x, y \in U, \exists q \in U: \; x \otimes y = x \,\overline{\otimes}\, y \,\overline{\otimes}\, q$. Элементы $p, q \in U$ будем называть параметрами конгруэнтности, p - параметр конгруэнтности $\otimes$ и $\overline{\otimes}$, q - параметр конгруэнтности $\overline{\otimes}$ и $\otimes$.

Если для операций $\otimes$ и $\overline{\otimes}$ существуют параметры конгруэнтности, то между ними выполняются соотношения $q = p^{-1} \otimes p^{-1}$ и $p = q^{-1} \,\overline{\otimes}\, q^{-1}$, где p^{-1} - элемент обратный элементу p в группе $< U, \otimes >$, q^{-1} - элемент обратный q в группе $< U, \overline{\otimes} >$. Действительно, по определению 2, с одной стороны имеем $x \otimes y = x \otimes y \otimes p \otimes q \otimes p$, то есть $q = p^{-1} \otimes p^{-1}$, а с другой стороны: $x \,\overline{\otimes}\, y = x \,\overline{\otimes}\, y \,\overline{\otimes}\, q \,\overline{\otimes}\, p \,\overline{\otimes}\, q$, то есть $p = q^{-1} \,\overline{\otimes}\, q^{-1}$.

Более того, элемент p^{-1} является нейтральным в группе $< U, \overline{\otimes} >$, а элемент q^{-1} является нейтральным в группе $< U, \otimes >$. Покажем это.

Пусть $\otimes \simeq \overline{\otimes}$, а $p \in U$ и $q \in U$ - параметры конгруэнтности. Рассмотрим биекцию $f : U \to U$ такую, что $\forall x \in U: f(x) = x \otimes p^{-1}$. Это отображение является автоморфизмом группы $< U, \otimes >$ на группу $< U, \overline{\otimes} >$, в чем несложно убедиться: $\forall x, y \in U$ по определению 2 имеем

$$f(x) \,\overline{\otimes}\, f(y) = (x \otimes p^{-1}) \,\overline{\otimes}\, (y \otimes p^{-1}) = x \otimes p^{-1} \otimes y \otimes p^{-1} \otimes p = x \otimes y \otimes p^{-1} = f(x \otimes y).$$

Аналогично, биекция $f':U\to U$ такая, что $\forall x\in U: f'(x)=x\overline{\otimes}q^{-1}$ является автоморфизмом группы $<U,\overline{\otimes}>$ на группу $<U,\otimes>$:

$$\forall x,y\in U: f'(x)\otimes f'(y)=(x\overline{\otimes}q^{-1})\otimes(y\overline{\otimes}q^{-1})=x\overline{\otimes}q^{-1}\overline{\otimes}y\overline{\otimes}q^{-1}\overline{\otimes}q=f'(x\overline{\otimes}y).$$

Очевидно, что отображения f и f' должны быть взаимообратными ($f'=f^{-1}$ и $f=f'^{-1}$). Обращение биекций f и f' приводит к выражениям: $\forall x\in U: f^{-1}(x)=x\otimes p$ и $\forall x\in U: f'^{-1}(x)=x\overline{\otimes}q$.

С учетом этого, по определению 2 получим:

$$\forall x\in U: f'(x)=x\overline{\otimes}q^{-1}=x\otimes q^{-1}\otimes p=x\otimes p=f^{-1}(x),$$
$$\forall x\in U: f(x)=x\otimes p^{-1}=x\overline{\otimes}p^{-1}\overline{\otimes}q=x\overline{\otimes}q=f'^{-1}(x).$$

Но такое возможно только, если элемент q^{-1} является нейтральным в группе $<U,\otimes>$, а элемент p^{-1} является нейтральным в группе $<U,\overline{\otimes}>$.

Можно заметить что, задавшись некоторой конкретной группой $<U,\otimes>$ и применяя автоморфизмы вида f, в которых параметр p^{-1} пробегает все множество U, можно получить N конкретных групп, групповые операции которых являются конгруэнтными между собой. То есть для любой операции $\otimes\in\Theta$ существую ровно N операций ей конгруэнтных.

Утверждение 2. Конгруэнтность операций есть отношение эквивалентности.

Доказательство. Рефлексивность отношения конгруэнтности операций очевидна при параметрах конгруэнтности, равных нейтральному элементу группы. Симметричность этого отношения очевидна по определению.

Докажем транзитивность. Пусть $\otimes\simeq\overline{\otimes}$ с параметрами конгруэнтности p_1, q_1 и $\overline{\otimes}\simeq\overline{\overline{\otimes}}$ с параметрами конгруэнтности p_2, q_2. То есть $\forall x,y\in U:\ x\overline{\otimes}y=x\otimes y\otimes p_1$, $x\otimes y=x\overline{\otimes}y\overline{\otimes}q_1$ и $\forall x,y\in U:\ x\overline{\overline{\otimes}}y=x\overline{\otimes}y\overline{\otimes}p_2$, $x\overline{\otimes}y=x\overline{\overline{\otimes}}y\overline{\otimes}q_2$. Выполнив подстановку первого выражения в третье и четвертого выражения во второе, получим:

$$\forall x,y\in U:\ x\overline{\overline{\otimes}}y=x\otimes y\otimes p_1\otimes p_2\otimes p_1=x\otimes y\otimes p_3 \text{ и}$$
$$\forall x,y\in U:\ x\otimes y=x\overline{\overline{\otimes}}y\overline{\otimes}q_2\overline{\overline{\otimes}}q_1\overline{\otimes}q_2=x\overline{\overline{\otimes}}y\overline{\otimes}q_3,$$

где $p_3=p_1\otimes p_2\otimes p_1$ и $q_3=q_2\overline{\overline{\otimes}}q_1\overline{\otimes}q_2$. Следовательно, $\otimes\simeq\overline{\overline{\otimes}}$ с параметрами конгруэнтности p_3, q_3. *Что и требовалось доказать.*

Таким образом, отношение конгруэнтности операций разбивает множество Θ на $\frac{(N-1)!}{\varphi(N)}$ классов эквивалентности, имеющих по N операций в каждом классе.

По теореме Кэли [Калужнин, Сущанский, 1985] любая конечная группа $<U,\otimes>$ изоморфна некоторой подгруппе симметрической группы $S(U)$. Рассмотрим такие изоморфизмы для групп $<U,\otimes>$ и $<U,\overline{\otimes}>$, в которых $\otimes\simeq\overline{\otimes}$: каждому элементу $u\in U$ сопоставляются перестановки π_u и η_u, такие что $\forall x\in U:\pi_u(x)=u\otimes x$ и $\forall x\in U:\eta_u(x)=u\overline{\otimes}x$. Очевидно, что $\forall u\in U:\pi_{u\otimes p}=\eta_u$. То есть группы $<U,\otimes>$ и $<U,\overline{\otimes}>$ оказываются изоморфными одной и той же группе подстановок. Более того, все группы, операции которых принадлежат одному классу конгруэнтности, по изоморфизмам указанного вида, имеют один и тот же изоморфный образ.

Следствием этого наблюдения является то, что таблицы Кэли конгруэнтных операций совпадают с точностью до порядка следования строк (столбцов), в то время как в таблицах Кэли не конгруэнтных операций совпадают лишь строки (столбцы), соответствующие нейтральным элементам групп.

Условия равенства последовательностей, порождаемых каскадным методом

Последовательности, порождаемые каскадным методом, являются так называемыми чисто периодическими и кумулятивными. В статье [Румбешт, 2014] даны определения этим понятиям. В соответствии с определением 1 из [Румбешт, Ядута, 2014], две последовательности над U являются равными, если каждый член первой последовательности равен соответствующему члену второй.

Кроме того, в работе [Румбешт, Ядута, 2014] сформулировано утверждение о том, что две чисто периодические кумулятивные последовательности равны тогда и только тогда, когда равны их начальные элементы и равны их порождающие последовательности. В этом утверждении не явно предполагается, что кумулятивные последовательности формируются с использованием одной и той же конкретной группы. В контексте статьи [Румбешт, Ядута, 2014] это утверждение справедливо. Однако, в общем случае применения конкретных групп с операциями из Θ, это не верно.

Действительно, понятия начального элемента, порождающей и кумулятивной последовательностей имеют смысл только для последовательностей над элементами группы. Более того, если задаться конкретной циклической группой $<U,\otimes>$, то любая последовательность над U является кумулятивной, и для нее можно установить порождающую последовательность с точностью до начального элемента. Если же, при этом, данная последовательность является чисто периодической, то установление начального элемента и порождающей однозначно. То есть, например, при наличии двух конкретных циклических групп $<U,\otimes>$ и $<U,\overline{\otimes}>$, для одной и той же чисто периодической кумулятивной последовательности соответствующие порождающие последовательности не обязательно равны.

Поэтому, утверждение о равенстве кумулятивных последовательностей, порождаемых каскадным методом, требует уточнения. Здесь важно то, что в каскадном методе порождающие последовательности не произвольные, а обладают определенными структурными свойствами, и метод гарантирует наличие этих свойств. Для формализации этого будем использовать определения и обозначения, введенные в [Румбешт, 2014]:

- $X_{\rightarrow}=(x_1,x_2,\ldots,x_i,\ldots)$ и $\overline{X}_{\rightarrow}=(\overline{x}_1,\overline{x}_2,\ldots,\overline{x}_i,\ldots)$ - чисто периодические последовательности над U, имеющие одинаковый период τ;
- $h_{X_{\rightarrow}}=x_1\otimes x_2\otimes\ldots\otimes x_\tau$ - характеристический элемент $X_{\rightarrow}$ в группе $<U,\otimes>$, $h_{\overline{X}_{\rightarrow}}=\overline{x}_1\,\overline{\otimes}\,\overline{x}_2\,\overline{\otimes}\ldots\overline{\otimes}\,\overline{x}_\tau$ - характеристический элемент $\overline{X}_{\rightarrow}$ в группе $<U,\overline{\otimes}>$, причем $Ord(h_{X_{\rightarrow}})=Ord(h_{\overline{X}_{\rightarrow}})=N$ (то есть $h_{X_{\rightarrow}}\in G_{<U,\otimes>}$, а $h_{\overline{X}_{\rightarrow}}\in G_{<U,\overline{\otimes}>}$, где $G_{<U,\otimes>}$ и $G_{<U,\overline{\otimes}>}$ - множества образующих элементов в группах $<U,\otimes>$ и $<U,\overline{\otimes}>$ соответственно);
- $Y_{\rightarrow}=(y_1,y_2,\ldots,y_i,\ldots)$ и $\overline{Y}_{\rightarrow}=(\overline{y}_1,\overline{y}_2,\ldots,\overline{y}_i,\ldots)$ - кумулятивные последовательности с начальными элементами $y_0\in U$ и $\overline{y}_0\in U$, а так же порождающими $X_{\rightarrow}$ и $\overline{X}_{\rightarrow}$ соответственно.

Будем считать, что для формирования $Y_{\rightarrow}$ применяется операция группы $<U,\otimes>$, а для формирования $\overline{Y}_{\rightarrow}$ - операция группы $<U,\overline{\otimes}>$, то есть для всех натуральных i: $y_i=y_{i-1}\otimes x_i$ и $\overline{y}_i=\overline{y}_{i-1}\,\overline{\otimes}\,\overline{x}_i$.

Утверждение 3. Необходимым условием для равенства $Y_{\rightarrow}$ и $\overline{Y}_{\rightarrow}$ является $y_0=\overline{y}_0$.

Доказательство. По утверждению 1 в статье [Румбешт, 2014] в силу периодичности $Y_{\rightarrow}$ и $\overline{Y}_{\rightarrow}$ имеем $y_{\tau\cdot N}=y_0$ и $\overline{y}_{\tau\cdot N}=\overline{y}_0$. Пусть $y_0\neq\overline{y}_0$. Тогда $y_{\tau\cdot N}\neq\overline{y}_{\tau\cdot N}$, что противоречит равенству $Y_{\rightarrow}$ и $\overline{Y}_{\rightarrow}$. *Что и требовалось доказать.*

Утверждение 4. Необходимым условием для равенства $Y_{\rightarrow}$ и $\overline{Y}_{\rightarrow}$ является $\otimes\simeq\overline{\otimes}$.

Доказательство. Согласно утверждению 1 в статье [Румбешт, 2014] период кумулятивной последовательности $Y_{\rightarrow}$ составляет $\pi=N\cdot\tau$. Если разбить периодический отрезок $[Y_{\rightarrow}]$ на N участков, то несложно заметить, что $y_{\tau+1}=y_1\otimes h_{X_{\rightarrow}}$, $y_{2\cdot\tau+1}=y_{\tau+1}\otimes h_{X_{\rightarrow}}$,..., $y_{N\cdot\tau+1}=y_{(N-1)\cdot\tau+1}\otimes h_{X_{\rightarrow}}=y_1$. Аналогично, для кумулятивной последовательности $\overline{Y}_{\rightarrow}$: $\overline{y}_{\tau+1}=\overline{y}_1\,\overline{\otimes}\,h_{\overline{X}_{\rightarrow}}$, $\overline{y}_{2\cdot\tau+1}=\overline{y}_{\tau+1}\,\overline{\otimes}\,h_{\overline{X}_{\rightarrow}}$,... $\overline{y}_{N\cdot\tau+1}=\overline{y}_{(N-1)\cdot\tau+1}\,\overline{\otimes}\,h_{\overline{X}_{\rightarrow}}=\overline{y}_1$. Получается, что члены $y_1,y_{\tau+1},y_{2\cdot\tau+1},\ldots,y_{(N-1)\cdot\tau+1}$ пробегают все множество U и формируют строку (столбец), соответствующую элементу $h_{X_{\rightarrow}}$ в таблице Кэли для операции $\otimes$, а члены $\overline{y}_1,\overline{y}_{\tau+1},\overline{y}_{2\cdot\tau+1},\ldots,\overline{y}_{(N-1)\cdot\tau+1}$ - строку (столбец), соответствующую элементу $h_{\overline{X}_{\rightarrow}}$ в таблице Кэли для операции $\overline{\otimes}$.

Пусть $\otimes \neq \overline{\otimes}$. Как было показано выше, если операции не конгруэнтны, то в таблицах Кэли данных операций нет совпадающих строк (столбцов) за исключением тех, которые соответствуют нейтральным элементам соответствующих групп. Элементы $h_{X_\to}$ и $h_{\overline{X}_\to}$ не являются нейтральными и, следовательно $\exists i \in \{0,1,\ldots,N-1\} : y_{i\cdot\tau+1} \neq \overline{y}_{i\cdot\tau+1}$, такие что $y_{i\cdot\tau+1} = y_{(i-1)\cdot\tau+1} \otimes h_{X_\to}$, $\overline{y}_{i\cdot\tau+1} = \overline{y}_{(i-1)\cdot\tau+1} \overline{\otimes} h_{\overline{X}_\to}$ при $y_{(i-1)\cdot\tau+1} = \overline{y}_{(i-1)\cdot\tau+1}$. Это противоречит равенству $Y_\to$ и $\overline{Y}_\to$. *Что и требовалось доказать.*

Утверждение 5. При $\otimes \simeq \overline{\otimes}$ необходимым условием для равенства $Y_\to$ и $\overline{Y}_\to$ является $\overline{x}_i = x_i \otimes p^{-1}$ для всех натуральных i, где p - параметр конгруэнтности $\otimes$ и $\overline{\otimes}$.

Доказательство. Пусть $\exists i \in \{1,2,\ldots\} : \overline{x}_i \neq x_i \otimes p^{-1}$. По начальным условиям: $y_i = y_{i-1} \otimes x_i$ и $\overline{y}_i = \overline{y}_{i-1} \overline{\otimes} \overline{x}_i = \overline{y}_{i-1} \otimes \overline{x}_i \otimes p$. Случай $y_{i-1} \neq \overline{y}_{i-1}$ сразу противоречит равенству $Y_\to$ и $\overline{Y}_\to$. При $y_{i-1} = \overline{y}_{i-1}$ и $\overline{x}_i \neq x_i \otimes p^{-1}$ имеем: $\overline{y}_i \neq y_i$, что так же противоречит равенству $Y_\to$ и $\overline{Y}_\to$. *Что и требовалось доказать.*

Утверждение 6. Для равенства $Y_\to$ и $\overline{Y}_\to$ необходимо и достаточно $y_0 = \overline{y}_0$, $\otimes \simeq \overline{\otimes}$ и для всех натуральных i: $\overline{x}_i = x_i \otimes p^{-1}$, где p - параметр конгруэнтности $\otimes$ и $\overline{\otimes}$.

Доказательство. Необходимость этого условия уже доказана по частям (см. утверждения 3, 4 и 5). Достаточность доказывается по индукции.

1) $\overline{y}_1 = \overline{y}_0 \overline{\otimes} \overline{x}_1 = \overline{y}_0 \otimes x_1 \otimes p^{-1} \otimes p = y_0 \otimes x_1 = y_1$;

2) пусть $i > 1$ и $y_{i-1} = \overline{y}_{i-1}$, тогда $\overline{y}_i = \overline{y}_{i-1} \overline{\otimes} \overline{x}_i = \overline{y}_{i-1} \otimes x_i \otimes p^{-1} \otimes p = y_{i-1} \otimes x_i = y_i$.

Следовательно $Y_\to = \overline{Y}_\to$. *Что и требовалось доказать.*

Учитывая рефлексивность отношения конгруэнтности операций и то, что параметр конгруэнтности равных операций является нейтральным элементом соответствующей группы, утверждение 6 в этом частном случае полностью соответствует упомянутому выше утверждению из работы [Румбешт, Ядута, 2014].

Обобщением утверждения 6 на случай $y_0 \neq \overline{y}_0$ является то, что для всех натуральных i: $\overline{y}_i = y_i \otimes \overline{y}_0 \otimes y_0^{-1}$ тогда и только тогда, когда $\otimes \simeq \overline{\otimes}$ и $\overline{x}_i = x_i \otimes p^{-1}$, где p - параметр конгруэнтности $\otimes$ и $\overline{\otimes}$.

Конфигурации в каскадном методе

Определение 3. Конфигурация каскадов - это вектор $C = <\otimes^{(1)}, \otimes^{(2)}, \ldots, \otimes^{(k)}>$, компонентами которого являются операции из Θ, такие, что на первом уровне преобразования каскадного метода применяется группа $<U, \otimes^{(1)}>$, на втором – группа $<U, \otimes^{(2)}>$, и так далее, вплоть до k-го уровня, на котором применяется группа $<U, \otimes^{(k)}>$. На каждом уровне преобразования, начиная со второго, соответствующая группа применяется и в процедуре-фильтре, и в процедуре порождения кумулятивной последовательности.

Конфигурации, в которых все операции равны между собой будем называть однородными, а все остальные – смешанными. Когда требуется уточнение количества компонентов в конфигурации, будем применять термин "k-уровневая конфигурация".

Две конфигурации будем называть эквивалентными, если каскадный метод в этих конфигурациях порождает равные между собой множества последовательностей. То есть, для любой последовательности, порожденной каскадным методом в первой конфигурации, найдется равная ей последовательность, порожденная во второй конфигурации, и наоборот.

Утверждение 7. Любая k-уровневая конфигурация каскадов $C = <\otimes^{(1)}, \otimes^{(2)}, \ldots, \otimes^{(k)}>$, в которой все операции конгруэнтны, эквивалентна однородной k-уровневой конфигурации $\overline{C} = <\overline{\otimes}, \ldots>$, в которой операция $\overline{\otimes}$ конгруэнтна операциям из C.

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

Процедура порождения КП применяется на всех уровнях преобразования. Ее входным параметром является начальный элемент $x_0^{(i)}$, где i - номер уровня преобразования. Кроме этого, на первом уровне преобразования применяется параметр $g^{(1)}$ - характеристический элемент стационарной последовательности, поступающей на вход процедуры порождения КП [Румбешт, 2014]. Для всех уровней преобразования i, начиная со второго, применению процедуры порождения КП предшествует применение процедуры-фильтра. Эта процедура принимает на вход параметры: характеристический элемент выходной последовательности $g^{(i)}$ и позицию замены $m^{(f)}$ [Румбешт, 2014]. Поскольку количества комбинаций значений указанных параметров не зависят от применяемой конфигурации, примем гипотезу о равной мощности множеств последовательностей, порождаемых каскадным методом в конфигурациях C и $\overline{C}$.

Для доказательства утверждения требуется показать, что с одной стороны, при равенстве порождаемых последовательностей выполняется условие конгруэнтности операций, а с другой стороны, для любого возможного набора значений параметров в конфигурации $\overline{C}$ найдется набор значений параметров в конфигурации C, такой, что каскадный метод и в первом и во втором случае порождает равные последовательности. Для этого достаточно ограничиться рассмотрением случаев 1 и 2-уровневых конфигураций, поскольку рассуждения для количества уровней больше 2 оказываются аналогичными.

Случай 1-уровневых конфигураций. Пусть $X_{\rightarrow}^{(1)}$ - последовательность, порожденная каскадным методом в конфигурации C при заданных параметрах $g^{(1)} \in G_{<U,\otimes^{(1)}>}$, $x_0^{(1)} \in U$; $\overline{X}_{\rightarrow}^{(1)}$ - последовательность, порожденная каскадным методом в конфигурации $\overline{C}$ при заданных параметрах $\overline{g}^{(1)} \in G_{<U,\overline{\otimes}>}$, $\overline{x}_0^{(1)} \in U$.

С одной стороны, если $X_{\rightarrow}^{(1)} = \overline{X}_{\rightarrow}^{(1)}$, то по утверждению 6: $\overline{\otimes} \simeq \otimes^{(1)}$. С другой стороны, пусть $\overline{\otimes} \simeq \otimes^{(1)}$ и p_1 - параметр конгруэнтности $\overline{\otimes}$ и $\otimes^{(1)}$. Биекция $f: U \to U$, такая, что $\forall x \in U : f(x) = x \,\overline{\otimes}\, p_1^{-1}$, является автоморфизмом группы $<U,\overline{\otimes}>$ на группу $<U,\otimes^{(1)}>$. Следовательно $(\overline{g}^{(1)} \,\overline{\otimes}\, p_1^{-1}) \in G_{<U,\otimes^{(1)}>}$. По утверждению 6, при $g^{(1)} = \overline{g}^{(1)} \,\overline{\otimes}\, p_1^{-1}$ и $x_0^{(1)} = \overline{x}_0^{(1)}$ имеем $X_{\rightarrow}^{(1)} = \overline{X}_{\rightarrow}^{(1)}$.

Случай 2-уровневых конфигураций. Пусть $\overline{X}_{\rightarrow}^{(1)}$, $\overline{X}_{\rightarrow}^{(2)}$, $X_{\rightarrow}^{(1)}$ и $X_{\rightarrow}^{(2)}$ - последовательности, порожденные первым и вторым уровнями преобразования каскадного метода в конфигурациях $\overline{C}$ и C соответственно; $\overline{g}^{(1)}, \overline{g}^{(2)} \in G_{<U,\overline{\otimes}>}$, $\overline{x}_0^{(1)}, \overline{x}_0^{(2)} \in U$, $\overline{m}^{(2)} \in \{0,1,\ldots,N-1\}$ - параметры каскадного метода в конфигурации $\overline{C}$; $g^{(1)} \in G_{<U,\otimes^{(1)}>}$, $g^{(2)} \in G_{<U,\otimes^{(2)}>}$, $x_0^{(1)}, x_0^{(2)} \in U$, $m^{(2)} \in \{0,1,\ldots,N-1\}$ - параметры каскадного метода в конфигурации C.

С одной стороны, если $X_{\rightarrow}^{(2)} = \overline{X}_{\rightarrow}^{(2)}$, то по утверждению 6: $\overline{\otimes} \simeq \otimes^{(2)}$ и $\widetilde{x}_i = \widetilde{\overline{x}}_i \,\overline{\otimes}\, p_2^{-1}$ для $\forall i \in \{1,2,\ldots\}$. Здесь $\widetilde{x}_i$ и $\widetilde{\overline{x}}_i$ - члены последовательностей $\widetilde{X}_{\rightarrow}$ и $\widetilde{\overline{X}}_{\rightarrow}$, формируемых процедурой-фильтром из $X_{\rightarrow}^{(1)}$ и $\overline{X}_{\rightarrow}^{(1)}$, p_2 - параметр конгруэнтности $\overline{\otimes}$ и $\otimes^{(2)}$.

Очевидно, что такой результат может быть получен только при $m^{(2)} = \overline{m}^{(2)}$. В силу автоморфизма группы $<U,\overline{\otimes}>$ на группу $<U,\otimes^{(2)}>$ имеем: $h_{X_{\rightarrow}^{(1)}} = h_{\overline{X}_{\rightarrow}^{(1)}} \,\overline{\otimes}\, p_2^{-1}$ и $h_{\widetilde{X}_{\rightarrow}} = h_{\widetilde{\overline{X}}_{\rightarrow}} \otimes p_2^{-1}$, где $h_{X_{\rightarrow}^{(1)}}$ и $h_{\widetilde{X}_{\rightarrow}}$ - характеристические элементы $X_{\rightarrow}^{(1)}$ и $\widetilde{X}_{\rightarrow}$ в группе $<U,\otimes^{(2)}>$, а $h_{\overline{X}_{\rightarrow}^{(1)}}$ и $h_{\widetilde{\overline{X}}_{\rightarrow}}$ - характеристические элементы $\overline{X}_{\rightarrow}^{(1)}$ и $\widetilde{\overline{X}}_{\rightarrow}$ в группе $<U,\overline{\otimes}>$. По определению процедуры-фильтра [Румбешт, 2014]: $h_{\widetilde{X}_{\rightarrow}} = g^{(2)}$ и $h_{\widetilde{\overline{X}}_{\rightarrow}} = \overline{g}^{(2)}$. Проведем обращение результата применения процедуры-фильтра. Получим члены $\overline{X}_{\rightarrow}^{(1)}$ и $X_{\rightarrow}^{(1)}$, такие, что $\forall i \in \{1,2,\ldots\}$:

$$\overline{x}_i^{(1)} = \begin{cases} \overline{\widetilde{x}}_i \text{, если } \overline{m}^{(2)} \neq (i \bmod N); \\ \overline{\widetilde{x}}_i \mathbin{\overline{\otimes}} \overline{g}^{(2)^{-1}} \mathbin{\overline{\otimes}} h_{\overline{X}^{(1)}_{\rightarrow}} \text{, если } \overline{m}^{(2)} = (i \bmod N); \end{cases}$$

$$x_i^{(1)} = \begin{cases} \widetilde{x}_i \text{, если } m^{(2)} \neq (i \bmod N); \\ \widetilde{x}_i \otimes^{(2)} g^{(2)^{-1}} \otimes^{(2)} h_{X^{(1)}_{\rightarrow}} \text{, если } m^{(2)} = (i \bmod N); \end{cases}$$

Учитывая, что $m^{(2)} = \overline{m}^{(2)}$, $h_{X^{(1)}_{\rightarrow}} = h_{\overline{X}^{(1)}_{\rightarrow}} \mathbin{\overline{\otimes}} p_2^{-1}$ и $g^{(2)^{-1}} = \overline{g}^{(2)^{-1}} \mathbin{\overline{\otimes}} p_2^{-1}$, получим соотношение между членами последовательностей $X^{(1)}_{\rightarrow}$ и $\overline{X}^{(1)}_{\rightarrow}$: $x_i^{(1)} = \overline{x}_i^{(1)} \otimes p_2^{-1}$ для $\forall i \in \{1,2,\ldots\}$. Из этого, по обобщению утверждения 6, следует, что $\overline{\otimes} \simeq \otimes^{(1)}$. И в силу того, что конгруэнтность есть отношение эквивалентности, $\otimes^{(2)} \simeq \otimes^{(1)}$.

С другой стороны, несложно видеть, при $\overline{\otimes} \simeq \otimes^{(1)}$, $\overline{\otimes} \simeq \otimes^{(2)}$, $\otimes^{(2)} \simeq \otimes^{(1)}$ и значениях параметров $g^{(1)} = \overline{g}^{(1)} \mathbin{\overline{\otimes}} p_1^{-1}$, $x_0^{(1)} = \overline{x}_0^{(1)} \otimes^{(1)} (p_2^{-1} \mathbin{\overline{\otimes}} p_1^{-1})$, $g^{(2)} = \overline{g}^{(2)} \mathbin{\overline{\otimes}} p_2^{-1}$, $m^{(2)} = \overline{m}^{(1)}$, $x_0^{(2)} = \overline{x}_0^{(2)}$ каскадный метод в конфигурациях C и $\overline{C}$ порождает равные последовательности $X^{(2)}_{\rightarrow}$ и $\overline{X}^{(2)}_{\rightarrow}$. *Что и требовалось доказать.*

Следствием утверждения 7 является то, что конфигурации каскадов, все компоненты которых принадлежат одному и тому же классу эквивалентности конгруэнтных операций, эквивалентны между собой. Это позволяет сделать вывод о том, что для построения конфигураций каскадов применение всех возможных операций из Θ избыточно.

Во множестве Θ выделим подмножество $\Theta_{\neq} \subset \Theta$, элементами которого являются операции такие, что они попарно не конгруэнтны, и их состав покрывает все классы эквивалентности конгруэнтных операций. Другими словами, элементами множества $\Theta_{\neq}$ являются операции, выбранные по одной из каждого класса эквивалентности.

Для построения конфигураций каскадов ограничимся операциями из $\Theta_{\neq}$. Это ограничение гарантирует, что среди всех различных конфигураций не будет эквивалентных.

Обозначим символом $Conf_k$ множество всех возможных k-уровневых конфигураций каскадов, компоненты которых выбираются из $\Theta_{\neq}$. Мощность множества $\Theta_{\neq}$ есть $\frac{(N-1)!}{\varphi(N)}$ и, следовательно, мощность $Conf_k$ составляет: $|Conf_k| = \left(\frac{(N-1)!}{\varphi(N)}\right)^k$.

Уточнение оценки количества последовательностей, порождаемых каскадным методом в любой допустимой конфигурации

В работе [Румбешт, Ядута, 2014] оценивалось количество последовательностей, порождаемых каскадным методом, но результаты, в ней полученные, справедливы для отдельно взятых однородных конфигураций. Для оценки количества последовательностей, порождаемых смешанными конфигурациями, требуется дополнительный анализ.

Этот анализ показывает, что для групп более чем 4-го порядка оценка, полученная в статье [Румбешт, Ядута, 2014], остается справедливой для любой допустимой конфигурации (как однородной, так и смешанной). Дело в том, что любые две неравные последовательности, поступающие на вход любой процедуры-фильтра, не удовлетворяют условию равенства последовательностей, ею формируемых [Румбешт, Ядута, 2014], поскольку их периодические отрезки имеют более двух позиций не совпадения. Эта ситуация никак не зависит от того, какая группа применяется для порождения таких последовательностей, и какая группа применяется в процедуре-фильтре. Полученная оценка справедлива и для групп 3-го порядка, поскольку в этом случае множество $\Theta_{\neq}$ содержит только одну операцию и, следовательно, k-уровневая конфигурация единственна и является однородной.

Исключение составляет оценка для групп 4-го порядка. Анализируя последовательности, порожденные первым уровнем преобразования при $N = 4$, можно заметить, что из них можно выделить пары последовательностей, такие, что их периодические отрезки имею две позиции несовпадения. Элементы, находящиеся в позициях несовпадения, являются образующими группы

$<U,\otimes^{(1)}>$, где $\otimes^{(1)}$ - групповая операция первого уровня преобразования. Если на втором уровне преобразования применяется операция $\otimes^{(2)}=\otimes^{(1)}$, то условие равенства последовательностей, формируемых процедурой-фильтром, не выполняется и количество последовательностей, порождаемых на втором уровне преобразования, составляет 256. Это показано в [Румбешт, Ядута, 2014].

Если же $\otimes^{(2)}\neq\otimes^{(1)}$, то в силу не конгруэнтности операций, эти же элементы получают другой "статус" в группе $<U,\otimes^{(2)}>$: один из них все так же остается образующим, а другой является либо нейтральным, либо элементом второго порядка. В этом случае условие равенства последовательностей, формируемых процедурой-фильтром, может стать истинным. То есть, существуют пары различных между собой комбинаций значений параметров процедуры-фильтра, которые приводят к формированию одной и той же последовательности на ее выходе. Следовательно, количество последовательностей, порождаемых на втором уровне преобразования при $\otimes^{(2)}\neq\otimes^{(1)}$ вдвое меньше, чем при $\otimes^{(2)}=\otimes^{(1)}$, и составляет 128.

Для уровней преобразования больших, чем 2, любые две неравные последовательности, поступающие на вход процедуры-фильтра, не удовлетворяют условию равенства последовательностей, ею формируемых, поскольку их периодические отрезки имеют более двух позиций не совпадения. Эта ситуация также никак не зависит от того, какая группа применяется для порождения этих последовательностей, и, какая группа применяется в процедуре-фильтре. То есть, при любой комбинации значений параметров, порождается уникальная последовательность. Оценка количества последовательностей при $\otimes^{(2)}=\otimes^{(1)}$ совпадает с результатами [Румбешт, Ядута, 2014], а при $\otimes^{(2)}\neq\otimes^{(1)}$ вдвое меньше, чем при $\otimes^{(2)}=\otimes^{(1)}$. Таким образом, уточненная оценка есть:

$$\nu(N,k)=\begin{cases} N\cdot\varphi(N), \text{ если } k=1; \\ \dfrac{N^{\frac{k^2+k}{2}}\cdot\varphi(N)^k}{2}, \text{ если } k>1\ \&\ (N=3\vee(N=4\ \&\otimes^{(2)}\neq\otimes^{(1)})); \\ N^{\frac{k^2+k}{2}}\cdot\varphi(N)^k, \text{ если } k>1\ \&\ (N>4\vee(N=4\ \&\otimes^{(2)}=\otimes^{(1)})); \end{cases} \quad (1)$$

где N - порядок группы, k - количество уровней преобразования, $\nu(N,k)$ - количество последовательностей, порождаемых каскадным методом в любой конфигурации из $Conf_k$, $\otimes^{(1)}$ и $\otimes^{(2)}$ - операции первого и второго уровней преобразования.

Множество последовательностей, порождаемых во всех конфигурациях каскадов, и его мощность

Введение множества $Conf_k^*$ позволяет говорить не только о множестве последовательностей, порождаемых в отдельной конфигурации $C\in Conf_k$, но и множестве последовательностей, порождаемых во всех конфигурациях в целом. Обозначим через Δ_C - множество последовательностей, порождаемых каскадным методом в k-уровневой конфигурации $C\in Conf_k$, а через $\Delta_k=\bigcup_{C\in Conf_k}\Delta_C$ - множество последовательностей, порождаемых во всех возможных конфигурациях из $Conf_k$. Согласно выше приведенному уточнению $\forall C\in Conf_k:\ |\Delta_C|=\nu(N,k)$, где $|\Delta_C|$ обозначает мощность Δ_C (см. формулу 1).

Выбор конфигураций из $Conf_k^*$ гарантирует, что каскадный метод в любых двух не равных конфигурациях порождает не равные между собой множества последовательностей. Однако, это не означает, что в любых конфигурациях порождаются не пересекающиеся множества последовательностей. По этому, вообще говоря, все Δ_C, в которых $C\in Conf_k$, не образуют разбиение Δ_k, и для нахождения мощности Δ_k нельзя просто воспользоваться оценкой $\nu(N,k)$.

Для упрощения дальнейшего описания введем отображение $Op:Conf_k\times\{1,2,\ldots,k\}\to\Theta_{\mp}$, которое определяет, какая конкретная операция применяется в заданной конфигурации на заданном уровне преобразования.

Учитывая утверждение 6, с уверенностью можно говорить о том, что $\forall C_1, C_2 \in Conf_k$: $\Delta_{C_1} \cap \Delta_{C_2} = \varnothing$, если $Op(C_1,k) \neq Op(C_2,k)$.

Рассмотрим $\Delta_{(k,\otimes)} = \bigcup_{\substack{C \in Conf_k \ \& \\ Op(C,k)=\otimes}} \Delta_C$ - множество последовательностей, порождаемых каскадным методом во всех конфигурациях, имеющих операции равные $\otimes$ на k-том (последнем) уровне преобразования, и $\eta(N,k)$ - оценку количества последовательностей, порождаемых методом во всех конфигурациях с фиксированной операцией на k-том уровне. Очевидно, что $\forall \otimes \in \Theta_{\neq}$: $\left|\Delta_{(k,\otimes)}\right| = \eta(N,k)$.

Множество Δ_k можно рассматривать как $\Delta_k = \bigcup_{\otimes \in \Theta_{\neq}} \Delta_{(k,\otimes)}$. По утверждению 6: $\forall \otimes, \overline{\otimes} \in \Theta_{\neq}$: $\Delta_{(k,\otimes)} \cap \Delta_{(k,\overline{\otimes})} = \varnothing$, если $\otimes \neq \overline{\otimes}$.

Отсюда следует, что

$$\left|\Delta_k\right| = \sum_{\otimes \in \Theta_{\neq}} \left|\Delta_{(k,\otimes)}\right| = \eta(N,k) \cdot \frac{(N-1)!}{\varphi(N)}. \quad (2)$$

Для 1-уровневых конфигураций имеем $\forall \otimes \in \Theta_{\neq}$: $\Delta_{(1,\otimes)} = \Delta_C$, где $C \in Conf_1$ и $Op(C,1) = \otimes$. Следовательно, $\eta(N,1) = \nu(N,1)$ и по формулам (1) и (2):

$$\left|\Delta_1\right| = N \cdot \varphi(N) \cdot \frac{(N-1)!}{\varphi(N)} = N! \quad (3)$$

Таким образом, получается, что Δ_1 содержит последовательности, имеющие периодические отрезки, являющиеся всеми возможными перестановками элементов U.

Во всех 2-уровневых конфигурациях, в которых каскадный метод порождает множество последовательностей $\Delta_{(2,\otimes)}$, на вход процедуры-фильтра поступают последовательности из Δ_1.

Количество комбинаций значений параметров, поступающих на вход процедуры-фильтра, составляет $N \cdot \varphi(N) \cdot N!$. Поскольку Δ_1 содержит последовательности, имеющие периодические отрезки, являющиеся всеми возможными перестановками элементов U, то для любой комбинации значений параметров найдется единственная, не равная ей, но такая, при которой условие равенства последовательностей, формируемых процедурой фильтром, становится истинным. Следовательно, при двух неравных комбинациях значений параметров на выходе этой процедуры формируется один и тот же результат. Получается, что на вход процедуры порождения КП во всех 2-уровневых конфигурациях с фиксированной операцией второго уровня поступает ровно $\frac{N \cdot \varphi(N) \cdot N!}{2}$ различных последовательностей. Учитывая, что существует N вариантов выбора начального элемента этой процедуры, окончательно получим: $\eta(N,2) = \frac{N^2 \cdot \varphi(N) \cdot N!}{2}$.

По формуле 2:

$$\left|\Delta_2\right| = \frac{N \cdot (N!)^2}{2} \quad (4)$$

В отличии от 2-уровневых конфигураций, при порождении последовательностей из $\Delta_{(k,\otimes)}$ $(k > 2)$, на вход процедуры-фильтра k-го уровня преобразования поступают элементы Δ_{k-1}, которые уже не удовлетворяют условию равенства последовательностей, ею формируемых, поскольку периодические отрезки любых двух не равных элементов Δ_{k-1} имеют более двух позиций не совпадения. Поэтому, при $k > 2$ на выходе k-го уровня преобразования формируются последовательности в количестве равном произведению возможных вариантов выбора значений параметров этого уровня: $\eta(N,k) = \left|\Delta_{k-1}\right| \cdot N^k \cdot \varphi(N)$. Устранив рекурсию, окончательно получим:

$$\eta(N,k)=\begin{cases} N\cdot\varphi(N), \text{ если } k=1; \\ \dfrac{N^{\frac{k^2-k+2}{2}}\cdot\varphi(N)\cdot(N!)^{k-1}}{2}, \text{ если } k>1; \end{cases}$$ и по формуле (2)

$$|\Delta_k|=\begin{cases} N!, \text{ если } k=1; \\ \dfrac{N^{\frac{k^2-k}{2}}\cdot(N!)^k}{2}, \text{ если } k>1; \end{cases} \quad (5)$$

Заключение

Об уникальности результата каскадного метода в конфигурации $C_1\in Conf_k$ можно говорить, если Δ_{C_1} не пересекается ни с каким другим Δ_{C_2}, где $C_2\in Conf_k$ и $C_2\neq C_1$. По этому, уникальные результаты каскадного метода формируются только в 1-уровневых конфигурациях. При $k>1$, для любой $C_1\in Conf_k$ найдется $C_2\in Conf_k$, такая, что $C_2\neq C_1$ и $\Delta_{C_2}\cap\Delta_{C_1}\neq\varnothing$. Причиной этому является показанная выше особенность порождения последовательностей на 2 уровне преобразования во всех возможных конфигурациях.

Добиться уникальности результатов каскадного метода в общем случае можно за счет введения ограничений на значения параметров уровней преобразования. Действительно, если для всех конфигураций каскадов зафиксировать значение позиции замены $m^{(2)}\in\{0,1,\ldots,N-1\}$ на втором уровне преобразования, то условие равенства последовательностей, формируемых процедурой фильтром, не будет выполняться для не равных входных последовательностей, и в каждой конфигурации на выходе 2-го уровня, как и на выходе всех последующих уровней, будет формироваться уникальный результат.

Количество последовательностей, порождаемых при таком ограничении в любой конфигурации, сократиться до:

$$\nu'(N,k)=\begin{cases} N\cdot\varphi(N), \text{ если } k=1; \\ N^{\frac{k^2+k-2}{2}}\cdot\varphi(N)^k, \text{ если } k>1; \end{cases} \quad (6)$$

Но каждой формируемой последовательности будет соответствовать единственный набор значений параметров вне зависимости от дополнительных условий.

Пусть $k>1$. Обозначим символом $\Delta_C(m)\subset\Delta_C$ множество последовательностей, порождаемых каскадным методом в k-уровневой конфигурации $C\in Conf_k$ при значении $m^{(2)}=m$. Очевидно, что $\forall C\in Conf_k, \forall m\in\{0,1,\ldots,N-1\}: |\Delta_C(m)|=\nu'(N,k)$.

Множество $\Delta_k(m)=\bigcup_{C\in Conf_k}\Delta_C(m)$ содержит последовательности, порождаемые во всех возможных конфигурациях при $m^{(2)}=m$. Соответственно, все $\Delta_C(m)$ суть разбиение $\Delta_k(m)$ на непересекающиеся подмножества. Для любого $m\in\{0,1,\ldots,N-1\}$ мощность $\Delta_k(m)$ легко найти:

$$|\Delta_k(m)|=\nu'(N,k)\cdot\left(\frac{(N-1)!}{\varphi(N)}\right)^k=\begin{cases} N!, \text{ если } k=1; \\ N^{\frac{k^2-k-2}{2}}\cdot(N!)^k, \text{ если } k>1; \end{cases} \quad (7)$$

Таким образом, введение указанного ограничения уменьшает общее количество порождаемых последовательностей в $\frac{N}{2}$ раз, по сравнению с $|\Delta_k|$, если $k>1$.

Список литературы
References

Калужнин Л. А., Сущанский В. И. 1985. Преобразования и перестановки. М., Наука, 160.

Kaluzhnin L. A., Sushhanskij V. I. 1985. Preobrazovanija i perestanovki [Transformations and permutations]. Moscow, Nauka, 160. (in Russian)

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

Rumbesht V.V. 2014. The cascade method of generation of periodic sequences over elements of a cyclic group. Nauchnye vedomosti BelGU. Serija: Istorija. Politologija. Jekonomika. Informatika. [Belgorod State University Scientific Bulletin. History. Political science. Economics. Information technologies] № 8 (179) 30/1: 103-112. (in Russian)

Румбешт В.В., Ядута А.З. 2014. Оценка количества последовательностей, порождаемых каскадным методом. Научные ведомости БелГУ. Серия: История. Политология. Экономика. Информатика. № 21 (192) Выпуск 32/1: 109-117.

Rumbesht V.V., Jaduta A.Z. 2014. Evaluation of the number of sequences generated by the cascade method. Nauchnye vedomosti BelGU. Serija: Istorija. Politologija. Jekonomika. Informatika. [Belgorod State University Scientific Bulletin. History. Political science. Economics. Information technologies] № 21 (192) 32/1: 109-117. (in Russian)