УДК 512.542.66 ISSN 1995-5499
DOI: https://doi.org/10.17308/sait.2021.1/3370
Поступила в редакцию 22.11.2020
Подписана в печать 26.04.2021

ПОДГРУППЫ СИММЕТРИЧЕСКИХ ГРУПП ПОДСТАНОВОК РЯДА ФАКТОРИАЛЬНЫХ МНОЖЕСТВ

© 2021 А. П. Мартынов[1], И. А. Мартынова[2], Д. Б. Николаев[1], Д. В. Сплюхин✉[1], В. Н. Фомченко[1]

[1]Российский федеральный ядерный центр — Всероссийский научно-исследовательский институт экспериментальной физики
пр. Мира, 37, 607188 Саров, Нижегородская область, Российская Федерации
[2]Объединённый институт высоких температур РАН
ул. Ижорская, 13/2, 000000 Москва, Российская Федерация

Аннотация. В основе любых криптографических алгоритмов и протоколов используются простейшие функции — перестановки и подстановки элементов заданного конечного множества. Объединяя и трансформируя данные элементы, организуется структурная ячейка защиты информации — математическое преобразование, обладающее необходимой криптографической стойкостью. Главная проблема в выработке таких преобразованиях заключается в том, что в процессе формирования более мощных алгоритмов разработчики используют все больше данных и вычислительных мощностей, полагаясь при этом на аппаратные возможности информационной системы. Это не только увеличивает потребление ресурсов, но также ограничивает скорость и конфиденциальность приложений. Однако изучая математические аспекты формирования перестановок и систему счисления рядов факториальных множеств необходимо перейти к активному изучению проблемы накопления данных, чтобы предложить новые алгоритмы, которые уменьшают модели аппаратного хранения больших объемов перестановок без потери возможностей.

Система счисления ряда факториальных множеств позволяет использовать алгоритм формирования любого элемента факториального множества без хранения перестановок в оперативной памяти. Таким образом, функция хранения массивов данных для криптографических алгоритмов уже не является необходимостью, так как ее функциональные возможности заменяет использование алгоритма формирования перестановок из системы счисления рядов факториальных множеств.

В работе рассматриваются аксиомы и способы построения подгрупп симметрических групп подстановок ряда факториальных множеств. Новые понятия ряда факториальных множеств и симметрических групп подстановок ряда факториальных множеств, введенные в 2014 г., позволяют расширить возможности анализа симметрических групп подстановок, позволяют их нумеровать, идентифицировать, структурировать и сделать более наглядными процессы группового и индивидуального преобразования. В работе приведен вариант классификации подгрупп по способам их построения.

Ключевые слова: ряд факториальных множеств, симметрическая группа подстановок, подгруппы преобразований, групповая операция, способы построения, классификация.

✉ Сплюхин Денис Валерьевич
e-mail: staff@vniief.ru

ВВЕДЕНИЕ

Анализ групп преобразований и симметрических групп подстановок ряда факториальных множеств, а также определение взаимосвязей между ними должно сопровождаться установлением зависимости между групповыми операциями. Для данных групп выполняются четыре аксиомы, это аксиомы замкнутости, ассоциативности, наличия единичного и обратных элементов.

Прежде чем приступать к изучению подгрупп групп, образованных подстановками ряда факториальных множеств, рассмотрим, каким образом можно выяснить, образуют ли элементы, принадлежащие к некоторому подмножеству элементов группы, подгруппу или не образуют.

1. АКСИОМЫ ПОДГРУПП

Первое, на что необходимо обратить внимание, это операция, обеспечивающая замкнутость преобразования. Такой операцией является композиция или иначе умножение (последовательное выполнение) [1, 2]. Мы должны не задавать операцию на выбранном подмножестве, а проверить, не выходит ли за его пределы операция, определенная в исходной группе. Если же операция не выходит за пределы, то выполняется аксиома замкнутости, и произведение двух элементов подмножества принадлежит данному подмножеству.

Следующая на очереди — аксиома ассоциативности группового умножения. Отметим, что аксиома ассоциативности выполняется для любых трех элементов исходной группы, следовательно, она выполняется и для тех элементов, которые входят в выбранное подмножество исходного множества, а это означает то, что свойство ассоциативности можно не проверять.

В работе «Аксиоматические основы функций подстановки в системе счисления ряда факториальных множеств и их характеристики» [2] показано, что во всех факториальных множествах существует только один единичный элемент e [1, 2]. Если мы хотим, чтобы выбранное подмножество некоторого факториального множества было подгруппой, оно должно включать в свой состав этот единичный элемент e относительно выбранной операции.

В заключении следует проверить, для каждого ли элемента подмножества существует принадлежащий подмножеству обратный элемент, т. е. вместе с каждым элементом подмножество должно содержать обратный к нему элемент.

В дальнейшем при рассмотрении подгрупп ряда факториальных множеств мы не будем задавать на ней операцию, т.к. групповая операция в подгруппе всегда совпадает с операцией, определенной в исходной группе.

Результаты предварительно проведенного анализа подстановок ряда факториальных множеств Φ_n [1, 2] позволяют отметить следующее:

1) все симметрические группы подстановок $G_n(S)$ содержат в качестве подгруппы множество, состоящее только из одного единичного элемента $e : ee = e,\ e^{-1} = e$, назовем его единичной подгруппой;

2) любая симметрическая группа подстановок $G_n(S)$ содержит себя в качестве подгруппы. Это очевидно, т. к. аксиомы группы заранее считаются выполненными. В алгебре такие подгруппы называют тривиальными. Сохраним это название для подгрупп ряда факториальных множеств.

Важнейшей подгруппой симметрических групп подстановок является знакопеременная группа, состоящая из четных подстановок, она соответствует своему классическому определению [3, 4].

Есть еще одна подгруппа, характерная для факториальных множеств, это группа, образованная подстановками предыдущего факториального множества. Известно, что предыдущее факториальное множество (Φ_{n-1}) входит в состав последующего факториального множества (Φ_n) в качестве его начального подмножества, значит группа подстановок предыдущего факториального множества $G_{n-1}(S)$ автоматически является подгруппой последующего факториального множества $G_n(S)$ [2].

Учитывая, что единичный элемент принадлежит всем группам и подгруппам подстановок ряда факториальных множеств ($SS^{-1} = e$) для подмножеств на их соответствие подгруппам необходимо проверять только два условия:

1) замкнутость относительно умножения;

2) наличие обратного элемента.

Необходимо особо отметить, что данный вывод относится к подгруппам конкретной группы, если мы рассматриваем подгруппу отдельно, то для нее формально должны выполняться все аксиомы группы преобразований.

В результате можно констатировать следующее, что если некоторое подмножество элементов конечной группы содержит единичный элемент и замкнуто относительно умножения, то оно является подгруппой.

2. ЗАДАНИЕ ПОДГРУПП И СВОЙСТВА ВЗАИМНО ОДНОЗНАЧНЫХ ОТОБРАЖЕНИЙ

Как показывают результаты анализа, элементы каждой подгруппы обычно обладают отличительными признаками или свойствами. Исходя из этого, подгруппу можно задавать, указывая эти отличительные признаки или свойства, при этом каждый из них можно рассматривать отдельно. Определенное значение для теории множеств имеет теорема, в соответствии с которой взаимно однозначные отображения любого множества на себя образуют группу относительно произведения отображений [5]. Она означает следующее. Если потребуется доказать, что некоторые взаимно однозначные отображения, обладающие тем или иным свойством, образуют группу, то можно не заниматься проверкой ассоциативности и взаимной однозначности произведения отображений или обратных отображений. Необходимо лишь проверить, обладает ли произведение отображений отличительным свойством интересующего нас множества отображений.

Для свойств отображений, влияющих на выбор подгрупп, можно выделить несколько закономерностей:

1) если в качестве отличительного свойства выбрать способность отображений не изменять периодичность на множестве, то отображения образуют подгруппу;

2) если отличительных свойств несколько, то каждое из них можно рассматривать в отдельности. Элементы группы, обладающие каждым из свойств, образуют подгруппу;

3) образуют подгруппу также и те элементы, которые обладают полным набором отличительных свойств. Эта подгруппа состоит из элементов, каждый из которых принадлежит всем подгруппам, выделенным при рассмотрении отдельных отличительных свойств.

Аналогичная взаимосвязь существует и между подгруппами всех других групп ряда факториальных множеств — это следующее свойство: элементы группы, принадлежащие двум или большему числу подгрупп, образуют подгруппу.

3. РЯД ФАКТОРИАЛЬНЫХ МНОЖЕСТВ И ИХ ПОДМНОЖЕСТВ

Вернемся к непосредственному рассмотрению групп и подгрупп подстановок ряда факториальных множеств. Напомним некоторые сведения о них, приведенные в работах [1,2]. Основой построения ряда факториальных множеств является функция факториала $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot n$ и множества элементов, образующихся на каждом шаге умножения. Функцию факториала можно выразить в следующем виде $n! = (n-1)! \cdot n$, т. е. факториальное множество включает в себя n предыдущих подмножеств. Число подмножеств факториального множества Φ_n равно его номеру n. Номер факториального множества равен числу образующих его элементов $1, 2, 3, 4, \ldots, n$. Число элементов факториального множества равно $m = (n-1)! \cdot n = n!$. В простых факториальных множествах физическая суть элементов не важна. Рассмотрим вариант, когда элементами факториального множества являются подстановки S. В этом случае каждое факториальное множество представлено таблицей, в которой столбцами являются образующие элементы, а строками конкретные

подстановки. Число образующих элементов n подстановки равно номеру факториального множества (n), а число подстановок S_m равно $m=(n-1)!\cdot n=n!$.

Ряд факториальных множеств и их подмножеств приведен в табл. 1.

Предыдущие факториальные множества являются подмножествами последующих факториальных множеств [1,2]

$$\Phi_1 \subset \Phi_2 \subset \Phi_3 \subset \Phi_4 \subset \Phi_5 \subset ...\Phi_{n-1} \subset \Phi_n. \quad (1)$$

Каждое предыдущее факториальное множество входит в состав последующего факториального множества в качестве его начального подмножества, в котором максимальный образующий элемент остается стационарным. Это отражено в последнем столбце табл. 1.

Подстановки факториальных множеств Φ_n образуют ряд симметрических групп подстановок $G_n(S)$. Предыдущие группы подстановок являются подгруппами последующих групп

$$G_1(S) \subset G_2(S) \subset G_3(S) \subset ...G_{n-1}(S) \subset G_n(S). \quad (2)$$

4. СТАЦИОНАРНЫЕ ПОДГРУППЫ СИММЕТРИЧЕСКИХ ГРУПП ПОДСТАНОВОК

Выберем в качестве отличительного свойства подстановки способность отображений не изменять значение одного из образующих элементов, т. е. он будет оставаться стационарным и не будет участвовать в перестановке.

Введем обозначение для стационарных подгрупп:

$H_n^i(S)$ — стационарная подгруппа подстановок, n — порядок симметрической группы подстановок $G_n(S)$, i — номер стационарного образующего элемента, S — подстановка.

Зафиксируем последовательно образующие элементы 1, 2, 3 в группе подстановок $G_3(S)$. В результате получим три подгруппы, включающие в свой состав по две подстановки:

$$\begin{cases} H_3^1(S)=\{S_0,S_3\}, \\ H_3^2(S)=\{S_0,S_5\}, \\ H_3^3(S)=\{S_0,S_1\}. \end{cases} \quad (3)$$

Имеет место соответствие

$$H_3^3(S)=\{S_0,S_1\} \Leftrightarrow G_2(S)=\{S_0,S_1\}. \quad (4)$$

Группа $G_3(S)$ содержит три стационарные подгруппы с фиксацией по одному образующему элементу (3) и одну единичную подгруппу с фиксацией всех образующих элементов

$$H_3^{1,2,3}(S)=\{e\}. \quad (5)$$

Стационарные подгруппы группы $G_3(S)$ приведены в табл. 2.

Группа $G_3(S)$ содержит еще одну подгруппу, состоящую из подстановок e, S_2, S_4. Подстановки S_2 и S_4 являются взаимно обратными. Нумерация подстановок соответствует работам [1, 2].

Зафиксируем последовательно образующие элементы 1, 2, 3, 4 в группе подстановок $G_4(S)$. В результате получим четыре стацио-

Таблица 1. Ряд факториальных множеств и их подмножеств
[Table 1. A number of factorial sets and their subsets]

Группы	Факториальные множества			Образующие элементы							
				1	2	3	4	5	…	n	
$G_1(S)$	←	Φ_1	→	Φ_1^1							$\Phi_1^1=\Phi_0$
$G_2(S)$	←	Φ_2	→	Φ_2^1	Φ_2^2						$\Phi_2^2=\Phi_1$
$G_3(S)$	←	Φ_3	→	Φ_3^1	Φ_3^2	Φ_3^3					$\Phi_3^3=\Phi_2$
$G_4(S)$	←	Φ_4	→	Φ_4^1	Φ_4^2	Φ_4^3	Φ_4^4				$\Phi_4^4=\Phi_3$
$G_5(S)$	←	Φ_5	→	Φ_5^1	Φ_5^2	Φ_5^3	Φ_5^4	Φ_5^5			$\Phi_5^5=\Phi_4$
…	…	…		…	…	…	…	…			…
$G_n(S)$	←	Φ_n	→	Φ_n^1	Φ_n^2	Φ_n^3	Φ_n^4	Φ_n^5	…	Φ_n^n	$\Phi_n^n=\Phi_{n-1}$
				Подмножества факториального множества							

Таблица 2. Стационарные подгруппы группы $G_3(S)$
[Table 2. Stationary subgroups of the group $G_3(S)$]

Φ_3					Подгруппы		
S	образующие элементы			Группа	стационарный элемент		
	1	**2**	**3**		1	2	3
S_0	1	2	3	e	e	e	e
S_1	2	1	3	(12)			(12)
S_2	3	1	2	(132)			
S_3	1	3	2	(23)	(23)		
S_4	2	3	1	(123)			
S_5	3	2	1	(13)		(13)	
				$G_3(S)$:	$H_3^1(S)$	$H_3^2(S)$	$H_3^3(S)$

нарные подгруппы, включающие в свой состав по шесть подстановок:

$$\begin{cases} H_4^1(S) = \{S_0, S_3, S_7, S_{10}, S_{14}, S_{17}\}, \\ H_4^2(S) = \{S_0, S_5, S_9, S_{10}, S_{19}, S_{20}\}, \\ H_4^3(S) = \{S_0, S_1, S_{16}, S_{17}, S_{20}, S_{21}\}, \\ H_4^4(S) = \{S_0, S_1, S_2, S_3, S_4, S_5\}. \end{cases} \quad (6)$$

Имеет место соответствие

$$H_4^4(S) = \{S_0, S_1, S_2, S_3, S_4, S_5\} \Leftrightarrow G_3(S) = \\ = \{S_0, S_1, S_2, S_3, S_4, S_5\}. \quad (7)$$

Группа $G_4(S)$ содержит четыре стационарные подгруппы с фиксацией по одному образующему элементу (6) и одну единичную подгруппу с фиксацией всех образующих элементов

$$H_4^{1,2,3,4}(S) = \{e\}. \quad (8)$$

Стационарные подгруппы группы $G_4(S)$ приведены в табл. 3.

В работе [5] понятие стационарной подгруппы введено при определении смежных классов для одного стационарного элемента. Расширим понятие стационарной подгруппы.

Если фиксировать не по одному образующему элементу, а по два или более (для факториальных множеств с $n > 4$), то мы получим дополнительные подгруппы. В этом случае мы получим подгруппы с числом стационарных образующих элементов $n > 1$, для группы $G_4(S)$ это два стационарных образующих элемента.

Таблица 3. Стационарные подгруппы группы $G_4(S)$
[Table 3. Stationary subgroups of the group $G_4(S)$]

Φ_4						Подгруппы			
S	образующие элементы				Группа	фиксируемый элемент			
	1	**2**	**3**	**4**		1	2	3	4
S_0	1	2	3	4	e	e	e	e	e
S_1	2	1	3	4	(12)			(12)	(12)
S_2	3	1	2	4	(132)				(132)
S_3	1	3	2	4	(23)	(23)			(23)
S_4	2	3	1	4	(123)				(123)
S_5	3	2	1	4	(13)		(13)		(13)
S_6	4	1	2	3	(1432)				
S_7	1	4	2	3	(243)	(243)			
S_8	2	4	1	3	(1243)				
S_9	4	2	1	3	(143)		(143)		
S_{10}	1	2	4	3	(34)	(34)	(34)		
S_{11}	2	1	4	3	(12)(34)				
S_{12}	3	4	1	2	(13)(24)				
S_{13}	4	3	1	2	(1423)				
S_{14}	1	3	4	2	(234)	(234)			
S_{15}	3	1	4	2	(1342)				
S_{16}	4	1	3	2	(142)			(142)	
S_{17}	1	4	3	2	(24)	(24)		(24)	
S_{18}	2	3	4	1	(1234)				
S_{19}	3	2	4	1	(134)		(134)		
S_{20}	4	2	3	1	(14)		(14)	(14)	
S_{21}	2	4	3	1	(124)			(124)	
S_{22}	3	4	2	1	(1324)				
S_{23}	4	3	2	1	(14)(23)				
					$G_4(S)$:	$H_4^1(S)$	$H_4^2(S)$	$H_4^3(S)$	$H_4^4(S)$

При всех стационарных образующих элементах равных n получаем единичную подгруппу

$$H_n^{1,2,\ldots,n}(S) = \{e\}. \quad (9)$$

Стационарными можно фиксировать от 1 до $n-2$ элементов, либо n образующих элементов, при фиксации $n-1$ элементов последний элемент автоматически становится стационарным, и мы получаем n стационарных элементов.

Таблица 4. Пример подгрупп при циклическом образовании подстановок
[Table 4. An example of subgroups in the cyclic formation of substitutions]

Цикл 3:		
1	e, S_4, S_3	e,(123),(132)
2	e, S_4, S_3	e,(132),(123)
3	e, S_{21}, S_{16}	e,(124),(142)
4	e, S_{16}, S_{21}	e,(142),(124)
5	e, S_{19}, S_9	e,(134),(143)
6	e, S_9, S_{19}	e,(143),(134)
7	e, S_{14}, S_7	e,(234),(243)
8	e, S_7, S_{14}	e,(243),(234)

Цикл 4:		
1	e, S_{18}, S_6	e,(1234),(1432)
2	e, S_6, S_{18}	e,(1432),(1234)
3	e, S_8, S_{15}	e,(1243),(1342)
4	e, S_{15}, S_8	e,(1342),(1243)
5	e, S_{13}, S_{22}	e,(1423),(1324)
6	e, S_{22}, S_{13}	e,(1324),(1423)

Стационарных подгрупп группы фиксирующие по два образующих элемента будет шесть, это подгруппы

$$\begin{aligned} H_4^{1,2}(S) &= \{e,(34)\}, \\ H_4^{1,3}(S) &= \{e,(24)\}, \\ H_4^{1,4}(S) &= \{e,(23)\}, \\ H_4^{2,3}(S) &= \{e,(14)\}, \\ H_4^{2,4}(S) &= \{e,(13)\}, \\ H_4^{3,4}(S) &= \{e,(12)\}. \end{aligned} \qquad (10)$$

Анализ табл. 2 и 3 показывает, что существуют подгруппы, включающие в свой состав только единичный элемент, прямую и обратную подстановки. Это позволяет нам ввести новый вид в классификации подгрупп. Назовем их подгруппами со структурой: e, S_i, S_i^{-1}. Для них: $eS^i = S^i$, $eS^{-i} = S^{-i}$, $S^i S^{-i} = e$, для единичного элемента умножение коммутативно.

В группе $G_3(S)$ такой структуре соответствует подгруппа

$$H_3(e, S, S^{-1}) = \{e, S_2, S_4\}. \qquad (11)$$

В группе $G_4(S)$ подгрупп со структурой: e, S_i, S_i^{-1} будет 14, половина из них отличается только порядком следования подстановок.

Аналогичные подгруппы существуют в группах, образованных подстановками всех последующих факториальных множеств.

Из табл. 3 и 4 видно, что пересечение подгрупп образует новые подгруппы. Новые подгруппы содержит те подстановки, которые есть в пересекающихся подгруппах, например:

$$(12),(12),e \quad (13),(13),e \quad (14),(14),e$$
$$(23),(23),e \quad (24),(24),e \quad (34),(34),e$$

Данное правило можно распространить на пересечение любого множества подгрупп некоторой группы. Оно подтверждает отмеченное ранее свойство отображения, что элементы группы, принадлежащие двум или большему числу подгрупп, образуют подгруппу и позволяет находить в любой группе наименьшую подгруппу, содержащую заранее заданные элементы группы. Элементы факториальных множеств - это конкретные подстановки.

Подгруппы образуют также и все подстановки любой выбранной группы при их возведении в степень [2–4]. Данные подгруппы обладают многими интересными особенностями, и их необходимо исследовать отдельно.

5. КЛАССИФИКАЦИЯ ПОДГРУПП ПО СПОСОБАМ ИХ ОБРАЗОВАНИЯ

В результате вышеизложенного можно сделать вывод, что подгруппы некоторой симметрической группы подстановок можно классифицировать по способам их образования, это:

1) тривиальные подгруппы:

– единичная подгруппа (e);

– группа, содержащая себя в качестве подгруппы;

2) группа предыдущего факториального множества;

3) знакопеременная подгруппа;

4) стационарные подгруппы:

– с одним стационарным образующим элементом;

– с числом стационарных образующих элементов >1 (при всех стационарных образующих элементах получаем единичную подгруппу);

5) подгруппы со структурой типа: e, S_i, S_i^{-1} (единичный элемент, прямая и обратная подстановки);

6) подгруппы пересечения любого множества подгрупп некоторой группы;

7) подгруппы объединения (в отличие от пересечения объединение подгрупп может быть подгруппой только в том случае, если одна из них полностью включает в свой состав другую);

8) циклические подгруппы.

Ряд подгрупп, отличных по способу образования, могут совпадать.

ЗАКЛЮЧЕНИЕ

В качестве отличительных свойств подгрупп можно рассматривать любой из способов их образования. Если отличительных свойств несколько, то каждое из них можно рассматривать в отдельности или в совокупности. Образуют подгруппу и те элементы, которые обладают полным набором выбранных отличительных свойств [6]. Данная классификация не является конечной. В ней рассмотрены подгруппы при анализе и классификации, которые не требуют более глубоких знаний алгебраической теории. При анализе факториальных множеств с большими номерами и циклических функций она может быть существенно дополнена.

Все рассмотренные подгруппы группы $G_4(S)$ факториального множества Φ_4 приведены в табл. 5.

Таблица 5. Подгруппы группы $G_4(S)$ факториального множества Φ_4
[Table 5. Group subgroups $G_4(S)$ factorial set Φ_4]

	Φ_4					группа	$G_4^i(S)$				Подгруппы с фиксацией двух элементов						Подгруппы типа: e, S_i, S_i^{-1}	Подгруппы типа: e, S_i, S_i^{-1}
S	**1**	**2**	**3**	**4**	S^{-1}		$i=1$	$i=2$	$i=3$	$i=4$	1,2	1,3	1,4	2,3	2,4	3,4		
P_0	1	2	3	4	P_0	e	e	e	e	e	e	e	e	e	e	e	e	e
P_1	2	1	3	4	P_1	(12)			(12)	(12)						(12)	e,(12)	(12),e
P_2	3	1	2	4	P_4	(132)				(132)							e,(132),(123)	(132),(123),e
P_3	1	3	2	4	P_3	(23)	(23)			(23)			(23)				e,(23)	(23),e
P_4	2	3	1	4	P_2	(123)				(123)							e,(123),(132)	(123),(132), e
P_5	3	2	1	4	P_5	(13)		(13)		(13)					(13)		e,(13)	(13),e
P_6	4	1	2	3	P_{18}	(1432)											e,(1432), (1234)	(1432),(13) (24),(1234), e
P_7	1	4	2	3	P_{14}	(243)	(243)										e,(243), (234)	(243),(234),e
P_8	2	4	1	3	P_{15}	(1243)											e,(1243), (1342)	(1243),(14) (23),(1342),e
P_9	4	2	1	3	P_{19}	(143)		(143)									e,(143), (134)	(143),(134),e
P_{10}	1	2	4	3	P_{10}	(34)	(34)	(34)			(34)						e,(34)	(34),e
P_{11}	2	1	4	3	P_{11}	(12)(34)											e,(12)(34)	(12)(34),e
P_{12}	3	4	1	2	P_{12}	(13)(24)											e,(13)(24)	(13)(24),e
P_{13}	4	3	1	2	P_{22}	(1423)											e,(1423), (1324)	(1423),(12) (34),(1324),e
P_{14}	1	3	4	2	P_7	(234)	(234)										e,(234), (243)	(234),(243),e
P_{15}	3	1	4	2	P_8	(1342)											e,(1342), (1243)	(1342),(14) (23),(1243),e
P_{16}	4	1	3	2	P_{21}	(142)			(142)								e,(142), (124)	(142),(124),e
P_{17}	1	4	3	2	P_{17}	(24)	(24)		(24)			(24)					e,(24)	(24),e
P_{18}	2	3	4	1	P_6	(1234)											e,(1234), (1432)	(1234),(13) (24),(1432),e
P_{19}	3	2	4	1	P_9	(134)		(134)									e,(134), (143)	(134),(143),e
P_{20}	4	2	3	1	P_{20}	(14)		(14)	(14)					(14)			e,(14)	(14),e
P_{21}	2	4	3	1	P_{16}	(124)			(124)								e,(124), (142)	(124),(142),e
P_{22}	3	4	2	1	P_{13}	(1324)											e,(1324), (1423)	(1324),(12) (34),(1423),e
P_{23}	4	3	2	1	P_{23}	(14)(23)											e,(14)(23)	(14)(23),e

КОНФЛИКТ ИНТЕРЕСОВ

Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Мартынов А. П.* Функции перестановки в системе счисления ряда факториальных множеств / А.П. Мартынов, И. А. Мартынова // Вестник ВГУ, Серия: Системный анализ и информационные технологии. – 2016. – № 3. – С. 42–49.

2. *Мартынов А. П.* Аксиоматические основы функций подстановки в системе счисления ряда факториальных множеств и их характеристики: монография / А. П. Мартынов, И. А. Мартынова, В. Н. Фомченко – Саров : ФГУП «РФЯЦ-ВНИИЭФ», 2019. – 210 с.

3. *Ван-дер-Варден Б. Л.* Алгебра. – М. : Мир, 1976. – 648 с.

4. *Винберг Э. Б.* Курс алгебры. – М. : МЦНМО, 2005. – 592 с.

5. Классы эквивалентности подстановок / А. П. Мартынов [и др.] // Сборник материалов XIV Всероссийской молодежной научно-инновационной школы «Математика и математическое моделирование». – 2020. – С. 151–152.

6. Свидетельство о государственной регистрации программы для ЭВМ № 2020613795. Программный комплекс анализа подстановок ряда факториальных множеств / Мартынов А. П., Николаев Д. Б., Сплюхин Д. В., Фомченко В. Н., Мартынова И. А. Зарег. 23.03.2020 г. – М. : Роспатент, 2020.

Мартынов Александр Петрович — д-р техн. наук, проф., начальник научно-исследовательского отдела ФГУП «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики»
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0002-8985-615X

Мартынова Инна Александровна — канд. физ.-мат. наук, старший научный сотрудник ФГБУН «Объединенный институт высоких температур Российской академии наук».
E-mail: webadmin@ihed.ras.ru
ORCID iD: https://orcid.org/0000-0003-2667-6669

Николаев Дмитрий Борисович — д-р техн. наук, доц., ведущий научный сотрудник ФГУП «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики».
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0003-2436-1532

Сплюхин Денис Валерьевич — аспирант, начальник научно-испытательной группы ФГУП «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики».
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0003-0240-5792

Фомченко Виктор Николаевич — д-р техн. наук, проф., главный конструктор – начальник конструкторского бюро ФГУП «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики».
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0002-4119-0870

DOI: https://doi.org/10.17308/sait.2021.1/3370 ISSN 1995-5499
Received 22.11.2020
Accepted 26.04.2021

SUBGROUPS OF SYMMETRIC GROUPS OF SUBSTITUTIONS OF A SERIES OF FACTORIAL SETS

© 2021 A. P. Martynov[1], I. A. Martynova[2], D. B. Nikolaev[1], D. V. Splyukhin✉[1], V. N. Fomchenko[1]

[1]Russian Federal Nuclear Center – All-Russian Research Institute of Experimental Physics
37, Mira Avenue, 607188, Sarov, Nizhny Novgorod Region, Russian Federation
[2]Federal State Budgetary Scientific Institution «Joint Institute for High Temperatures of the Russian Academy of Sciences»
13/2, Izhora Street, 000000 Moscow, Russian Federation

Annotation. Cryptographic algorithms and protocols are based on the simplest functions – permutations and substitutions of the elements of a given finite set. By combining and transforming these elements, we can form a structural element of information security, namely a mathematical transformation with a required degree of cryptographic strength. The main problem related to the development of such transformations is that when designing more powerful algorithms, developers use an increasing amount of data and computing power, while relying on the hardware capabilities of the information system. This increases resource consumption and limits the speed and confidentiality of applications. However, studying the mathematical aspects of the generation of permutations and the notation of series of factorial sets, we also need to investigate the problem of data accumulation in order to develop new algorithms that would reduce the models of hardware storage of a large number of permutations without limiting their capabilities.

The notation of series of factorial sets allows us to use the algorithm for the formation of any element of the factorial set without storing the permutations in the RAM. Thus, it is no longer necessary for cryptographic algorithms to store data in arrays, since this function can be replaced by the algorithm for forming permutations using the notation of a series of factorial sets.

The article considers axioms and methods of creating subgroups of symmetric substitution groups of a series of factorial sets. New concepts of a series of factorial sets and symmetric groups of substitutions of a series of factorial sets introduced in 2014, make it possible to expand the possibilities for the analyses of symmetric groups of substitutions. Namely, it is possible to number, identify, and structure these groups, and make the processes of group and individual transformation more visual. The article presents a classification of subgroups according to the formation method.

Keywords: a series of factorial sets, symmetric substitution group, transformation subgroups, group operation, formation methods, classification.

CONFLICT OF INTEREST

The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.

REFERENCE

1. *Martynov A. P., Martynova I. A.* (2016) Permutation functions in the number system of a number of factorial sets // Vestnik VSU, Series: System analysis and information technologies. – No. 3. P. 42–49.

2. *Martynov A. P., Martynova I. A., Fomchenko V. N.* (2019) Axiomatic foundations of substitution functions in the number system of a number of factorial sets and their characteristics: monograph. Sarov : FSUE RFNC-VNIIEF 210 p.

3. *Van der Waerden B. L.* (1976) Algebra. Moscow : Mir. 648 p.

4. *Vinberg E. B.* (2005) Course of algebra. Moscow : MTsNMO. 592 p.

✉ Splyukhin Denis V.
e-mail: staff@vniief.ru

5. *Martynov A. P. [et al.]* (2020) Classes of equivalence of substations-wok // Collection of materials of the XIV All-Russian Youth Scientific and Innovative School "Mathematics and Mathematical Modeling". P. 151–152.

6. *Martynov A. P., Nikolaev D. B., Splyukhin D. V., Fomchenko V. N., Martynova I. A.* (2020) Certificate of state registration of a computer program No. 2020613795. Software complex for the analysis of substitutions of a number of factorial sets. Registered. 03/23/2020 Moscow : Rospatent, 2020.

Martynov Alexander P. — DSc in Technical Sciences, Professor, Head of the Research Department of the Russian Federal Nuclear Center – All-Russian Research Institute of Experimental Physics.
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0002-8985-615X

Martynova Inna A. — PhD Physics and Mathematics, Senior Researcher of the Joint Institute for High Temperatures of the Russian Academy of Sciences.
E-mail: webadmin@ihed.ras.ru
ORCID: 0000-0003-2667-6669

Nikolaev Dmitry B. — DSc in Technical Sciences, Professor, leading researcher, Russian Federal Nuclear Center – All-Russian Research Institute of Experimental Physics.
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0003-2436-1532.

Splyukhin Denis V. — postgraduate student, Head of the Research and Experiments Group of the Russian Federal Nuclear Center – All-Russian Research Institute of Experimental Physics.
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0003-0240-5792

Fomchenko Viktor N. — DSc in Technical Sciences, Professor, Design Manager of the Design Bureau of the Russian Federal Nuclear Center – All-Russian Research Institute of Experimental Physics
E-mail: staff@vniief.ru
ORCID iD: https://orcid.org/0000-0002-4119-0870