 Научная статья

DOI: 10.18287/2541-7525-2020-26-2-23-49

УДК 512.531; 519.7

Дата: поступления статьи: 16.01.2020
после рецензирования: 30.01.2020
принятия статьи: 25.05.2020

В.П. Цветов
Самарский национальный исследовательский университет
имени академика С.П. Королева, г. Самара, Российская Федерация
E-mail: tsf-su@mail.ru. ORCID: https://orcid.org/0000-0001-6744-224X

ФРАКТАЛЬНЫЕ ГРУППОИДЫ И КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

АННОТАЦИЯ

В статье рассматриваются группоиды – простейшие алгебры с одной бинарной операцией. Предложены алгоритмы порождения шкал конечных группоидов на основе принципа самоподобия их таблиц Кэли. Каждый последующий порожденный группоид имеет мощность носителя в два раза большую по сравнению с порождающим его группоидом, а его таблица Кэли – блочную самоподобную структуру. В качестве примера приложения полученных результатов рассматриваются циклическая полугруппа бинарных операций, порожденная операцией конечного группоида с носителем небольшой мощности, и построенная на ее основе модификация протокола Диффи — Хелмана — Меркла открытого распределения ключей.

Ключевые слова: группоиды, полугруппы, таблицы Кэли, циклические полугруппы бинарных операций, криптография на группоидах, протокол Диффи — Хелмана — Меркла.

Цитирование. Цветов В.П. Фрактальные группоиды и криптография с открытым ключом // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 2. С. 23–49. DOI: http://doi.org/10.18287/2541-7525-2020-26-2-23-49.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

Информация об авторе: © *Цветов Виктор Петрович* — кандидат физико-математических наук, доцент кафедры безопасности информационных систем, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

1. Предварительные сведения

Напомним, что группоидом $\langle U, (*)\rangle$ называется множество (носитель) U с заданной на нем единственной бинарной операцией $*$, относительно свойств которой не делается никаких дополнительных предположений [1]. В англоязычной литературе за группоидами закреплен термин «магма», поэтому для обозначения группоидов мы будем использовать символ M. Заметим, что частный случай группоидов – квазигруппы – находят широкое применение в криптографии [2].

Конечные группоиды, т. е. группоиды с конечным носителем $U = \{u_1, \ldots, u_n\}$, полностью определяются таблицей Кэли, которая задает значения результата операции на значениях ее аргументов. Общий вид таблицы Кэли представлен в табл. 1.1.

Структура таблицы Кэли зависит от свойств операции, например, таблица Кэли коммутативной операции симметрична, а таблица Кэли квазигруппы — это латинский квадрат. Если операция обладает левым нейтральным элементом e_l (т.е. $e_l * u = u$ для любых $u \in U$), то в таблице Кэли ему будет соответствовать строка $u_1, u_2, \ldots, u_n$. То же самое относится и к правому нейтральному элементу и соответствующему ему столбцу.

В дальнейшем нам будет удобно представлять элементы носителей конечных группоидов значениями их индексов в некоторой нумерации. Нумерацию элементов будем начинать с единицы, т. е. вместо $U = \{u_1, \ldots, u_n\}$ будем записывать $1..n = \{1, \ldots, n\} \subset \mathbb{N}$.

Таблица 1.1

Общий вид таблицы Кэли

Table 1.1

General view of the Cayley table

$*$	u_1	$\dots$	u_j	$\dots$	u_n
u_1	$u_1 * u_1$	$\dots$	$u_1 * u_j$	$\dots$	$u_1 * u_n$
$\vdots$	$\vdots$	$\dots$	$\vdots$	$\dots$	$\vdots$
u_i	$u_i * u_1$	$\dots$	$u_i * u_j$	$\dots$	$u_i * u_n$
$\vdots$	$\vdots$	$\dots$	$\vdots$	$\dots$	$\vdots$
u_n	$u_n * u_1$	$\dots$	$u_n * u_j$	$\dots$	$u_n * u_n$

В свою очередь в таблице Кэли операции $*$ будем представлять целочисленной матрицей Кэли $A = (a_{i,j})$ порядка n с положительными элементами, определенными правилом

$$a_{i,j} = k,$$

где $u_k = u_i * u_j$, и $i, j, k \in 1..n \subset \mathbb{N}$.

Понятно, что если на множестве $1..n$ определить операцию $i \diamond j = a_{i,j}$, то группоиды $\langle U, (*)\rangle$ и $\langle 1..n, (\diamond)\rangle$ будут изоморфны.

Все последующие рассуждения имеют целью разработку математического аппарата для адаптации схемы открытого распределения ключа шифрования на основе протокола Диффи — Хелмана — Меркла (Diffie — Hellman — Merkle) [3; 4] применительно к группоидам.

2. Основные результаты

2.1. Фрактальные матрицы и шкалы фрактальных группоидов

Рассмотрим группоид $\langle 1..n, (\diamond)\rangle$ с матрицей Кэли A. Все дальнейшие построения опираются на «клонирование» матрицы Кэли операции исходного группоида в качестве подматриц матрицы Кэли операции группоида вдвое большей мощности.

Дадим следующие определения.

Определение 2.1.1. Диагональным расширением матрицы Кэли $A = (a_{i,j})$ порядка n будем называть матрицу $A^{(d)} = (a^{(d)}_{i,j})$ порядка $2n$, элементы которой определены правилом

$$a^{(d)}_{i,j} = \begin{cases} a_{i,j}\,, & i \in 1..n \wedge j \in 1..n \\ a_{i,j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ a_{i-n,j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ a_{i-n,j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.1}$$

Определение 2.1.2. Строковым расширением матрицы Кэли $A = (a_{i,j})$ порядка n будем называть матрицу $A^{(r)} = (a^{(r)}_{i,j})$ порядка $2n$, элементы которой определены правилом

$$a^{(r)}_{i,j} = \begin{cases} a_{i,j}\,, & i \in 1..n \wedge j \in 1..n \\ a_{i,j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ a_{i-n,j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ a_{i-n,j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.2}$$

Определение 2.1.3. Столбцевым расширением матрицы Кэли $A = (a_{i,j})$ порядка n будем называть матрицу $A^{(c)} = (a^{(c)}_{i,j})$ порядка $2n$, элементы которой определены правилом

$$a^{(c)}_{i,j} = \begin{cases} a_{i,j}\,, & i \in 1..n \wedge j \in 1..n \\ a_{i,j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ a_{i-n,j}\,, & i \in n+1..2n \wedge j \in 1..n \\ a_{i-n,j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.3}$$

Определение 2.1.4. Тривиальным расширением матрицы Кэли $A = (a_{i,j})$ порядка n будем называть матрицу $A^{(t)} = (a^{(t)}_{i,j})$ порядка $2n$, элементы которой определены правилом

$$a^{(t)}_{i,j} = \begin{cases} a_{i,j}\,, & i \in 1..n \wedge j \in 1..n \\ a_{i,j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ a_{i-n,j}\,, & i \in n+1..2n \wedge j \in 1..n \\ a_{i-n,j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.4}$$

Все определенные выше расширения матрицы Кэли будем называть фрактальными.

Определение 2.1.5. Фрактальным расширением группоида $\langle 1..n, (\diamond)\rangle$ с матрицей Кэли A будем называть любой из группоидов $\langle 1..2n, (\diamond^d)\rangle$, $\langle 1..2n, (\diamond^r)\rangle$, $\langle 1..2n, (\diamond^c)\rangle$, $\langle 1..2n, (\diamond^t)\rangle$, матрицы Кэли которых определены как $A^{(d)}$, $A^{(r)}$, $A^{(c)}$, $A^{(t)}$, соответственно. Сами операции $\diamond^d$, $\diamond^r$, $\diamond^c$, $\diamond^t$ будем называть фрактальным расширением операции $\diamond$. При необходимости уточнения конкретного типа расширения будем говорить о диагональных, строковых, столбцевых и тривиальных расширениях.

Замечание 2.1.1. В качестве примера рассмотрим фрактальное расширение мультипликативного группоида $\langle 1..2, (\cdot \bmod 3)\rangle$ с матрицей Кэли

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

до группоида $\langle 1..4, (\diamond^d)\rangle$ с матрицей Кэли

$$A^{(d)} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Заметим, что группоид $\langle 1..2, (\cdot \bmod 3)\rangle$ изоморфен группоиду $\langle 2^{\{1\}}, (\triangle)\rangle$, где $2^{\{1\}} = \{\emptyset, \{1\}\}$ — булеан над одноэлементным множеством, $\triangle$ — симметрическая разность множеств, и $1 \sim \emptyset$, $2 \sim \{1\}$.

Нетрудно понять, что группоид $\langle 1..4, (\diamond^d)\rangle$ изоморфен группоиду $\langle 2^{\{1,2\}}, (\triangle)\rangle$, где $2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ и $1 \sim \emptyset$, $2 \sim \{1\}$, $3 \sim \{2\}$, $4 \sim \{1,2\}$.

В силу определения, диагональное расширение коммутативного группоида будет коммутативным группоидом. Если в исходном группоиде имелись левые или/и правые нейтральные элементы, то они будут сохранять эти свойства и в диагональном расширении. Кроме того, если матрица Кэли исходного группоида являлась латинским квадратом, то латинским квадратом будет и матрица диагонального расширения.

Также понятно, что группоид $\langle 1..n, (\diamond)\rangle$ является подгруппоидом своего диагонального расширения $\langle 1..2n, (\diamond^d)\rangle$.

Замечание 2.1.2. Матрица Кэли строкового расширения группоида из примера предыдущего замечания 2.1.1 будет иметь вид

$$A^{(r)} = \begin{pmatrix} 1 & 2 & 1 & 2 \\ 2 & 1 & 2 & 1 \\ 3 & 4 & 3 & 4 \\ 4 & 3 & 4 & 3 \end{pmatrix}.$$

Строковое расширение группоида не может быть коммутативным. Свойство нейтрального элемента в строковом расширении будут сохранять только правые нейтральные элементы. Матрица строкового расширения не может быть латинским квадратом.

Понятно, что группоиды $\langle 1..n, (\diamond)\rangle$ и $\langle n{+}1..2n, (\diamond^r)\rangle$ являются подгруппоидами строкового расширения $\langle 1..2n, (\diamond^r)\rangle$.

Замечание 2.1.3. Матрица Кэли столбцевого расширения группоида из примера замечания 2.1.1 будет иметь вид

$$A^{(c)} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Столбцевое расширение группоида не может быть коммутативным. Свойство нейтрального элемента в столбцевом расширении будут сохранять только левые нейтральные элементы. Матрица столбцевого расширения не может быть латинским квадратом.

Понятно, что группоиды $\langle 1..n,(\diamond)\rangle$ и $\langle n+1..2n,(\diamond^c)\rangle$ являются подгруппоидами столбцевого расширения $\langle 1..2n,(\diamond^c)\rangle$.

Замечание 2.1.4. Матрица Кэли тривиального расширения группоида из примера замечания 2.1.1 будет иметь вид

$$A^{(t)}=\begin{pmatrix}1&2&1&2\\2&1&2&1\\1&2&1&2\\2&1&2&1\end{pmatrix}.$$

Тривиальное расширение коммутативного группоида будет коммутативным. Нейтральные элементы в тривиальном расширении будут отсутствовать. Матрица тривиального расширения не может быть латинским квадратом.

Понятно, что группоид $\langle 1..n,(\diamond)\rangle$ является подгруппоидом своего тривиального расширения $\langle 1..2n,(\diamond^t)\rangle$.

Определение 2.1.6. Однородной шкалой фрактальных группоидов $M_k^{(\sigma)}=\langle 1..n_k,(\diamond_k^\sigma)\rangle$ будем называть систему группоидов $S_\sigma=\{M_k^{(\sigma)}\}_{k=0}^\infty$, носители и матрицы Кэли A_k которых определены следующим условием:

$$\exists\sigma\forall k\ \sigma\in\{d,r,c,t\}\wedge k\in\mathbb{N}\wedge n_0\in\mathbb{N}\wedge n_k=2n_{k-1}\wedge A_k=A_{k-1}^{(\sigma)}.$$

Каждый из группоидов $M_k^{(\sigma)}$ при $k\in\mathbb{N}$ будем называть фрактальным, его индекс k — местом группоида в заданной шкале, а σ — типом расширения. Группоид $M_0^{(\sigma)}=\langle 1..n_k,(\diamond_0)\rangle$, его операцию $\diamond_0$ и матрицу Кэли A_0 будем называть базовыми в заданной шкале. Индексы 0 и σ в обозначениях базовых группоидов, матриц и операций обычно будем опускать. При необходимости уточнения конкретного типа шкалы будем говорить о диагональных, строковых, столбцевых или тривиальных шкалах.

В общем случае можно рассматривать смешанные шкалы, в которых тип расширений может изменяться в пределах шкалы. В данной статье смешанные шкалы не рассматриваются. Поэтому для простоты изложения однородные шкалы в дальнейшем будем называть просто шкалами.

Замечание 2.1.5. В силу определений каждая шкала $S_\sigma=\{M_k^{(\sigma)}\}_{k=0}^\infty$ с базовой матрицей Кэли A порождает при помощи сдвига места $h\in\mathbb{N}$ шкалу того же типа $S'_\sigma=\{M_{k-h}^{(\sigma)}\}_{k=h}^\infty$ с базовой матрицей Кэли A_h.

Рассмотрим последовательности из четырех первых матриц Кэли фрактальных шкал с базовым группоидом $M=\langle\{1\},(\diamond)\rangle$, где $1\diamond 1=1$.

1. Диагональные расширения (шкала S_d)

$$A=\begin{pmatrix}1\end{pmatrix},$$

$$A_1^{(d)}=\left(\begin{array}{cc|cc}\mathbf{1}&2&2&\\\hline 2&\mathbf{1}&&\end{array}\right),$$

$$A_2^{(d)}=\left(\begin{array}{cc|cc}\mathbf{1}&\mathbf{2}&3&4\\\mathbf{2}&\mathbf{1}&4&3\\\hline 3&4&\mathbf{1}&\mathbf{2}\\4&3&\mathbf{2}&\mathbf{1}\end{array}\right),$$

$$A_3^{(d)}=\left(\begin{array}{cccc|cccc}\mathbf{1}&\mathbf{2}&\mathbf{3}&\mathbf{4}&5&6&7&8\\\mathbf{2}&\mathbf{1}&\mathbf{4}&\mathbf{3}&6&5&8&7\\\mathbf{3}&\mathbf{4}&\mathbf{1}&\mathbf{2}&7&8&5&6\\\mathbf{4}&\mathbf{3}&\mathbf{2}&\mathbf{1}&8&7&6&5\\\hline 5&6&7&8&\mathbf{1}&\mathbf{2}&\mathbf{3}&\mathbf{4}\\6&5&8&7&\mathbf{2}&\mathbf{1}&\mathbf{4}&\mathbf{3}\\7&8&5&6&\mathbf{3}&\mathbf{4}&\mathbf{1}&\mathbf{2}\\8&7&6&5&\mathbf{4}&\mathbf{3}&\mathbf{2}&\mathbf{1}\end{array}\right).$$

Нетрудно проверить, что соответствующая шкала группоидов изоморфна шкале групп булеанов $\langle 2^{\{1\}},(\triangle)\rangle$, $\langle 2^{\{1,2\}},(\triangle)\rangle$, $\langle 2^{\{1,2,3\}},(\triangle)\rangle$ с операцией симметрической разности.

2. Строковые расширения (шкала S_r)

$$A=\begin{pmatrix}1\end{pmatrix},$$

$$A_1^{(r)}=\left(\begin{array}{cc|cc}\mathbf{1}&\mathbf{1}&&\\\hline 2&2&&\end{array}\right),$$

$$A_2^{(r)} = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ \hline 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \end{array}\right),$$

$$A_3^{(r)} = \left(\begin{array}{cccc|cccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} \\ \hline 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \end{array}\right).$$

Построенные расширения матриц Кэли определяют шкалу полугрупп левых нулей (правых единиц), операция которой $\wr$ определена правилом $u_i \wr u_j = u_i$.

3. Столбцевые расширения (шкала S_c)

$$A = \left(\begin{array}{c} 1 \end{array}\right),$$

$$A_1^{(c)} = \left(\begin{array}{cc} \mathbf{1} & 2 \\ \hline \mathbf{1} & 2 \end{array}\right),$$

$$A_2^{(c)} = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{2} & 3 & 4 \\ \mathbf{1} & \mathbf{2} & 3 & 4 \\ \hline \mathbf{1} & \mathbf{2} & 3 & 4 \\ \mathbf{1} & \mathbf{2} & 3 & 4 \end{array}\right),$$

$$A_3^{(c)} = \left(\begin{array}{cccc|cccc} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & 5 & 6 & 7 & 8 \end{array}\right).$$

Построенные расширения матриц Кэли определяют шкалу полугрупп правых нулей (левых единиц), операция которой $\wr\wr$ определена правилом $u_i \wr\wr u_j = u_j$.

4. Тривиальные расширения (шкала S_t)

$$A = \left(\begin{array}{c} 1 \end{array}\right),$$

$$A_1^{(r)} = \left(\begin{array}{cc} \mathbf{1} & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{1} \end{array}\right),$$

$$A_2^{(r)} = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{array}\right),$$

$$A_3^{(r)} = \left(\begin{array}{cccc|cccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{array}\right).$$

Построенные расширения матриц Кэли определяют шкалу полугрупп с нулевым умножением, операция которой $\dagger$ определена правилом $u_1 \dagger u_j = u_1$.

Замечание 2.1.6. Понятно, что, с одной стороны, каждый из группоидов M_k (матрица Кэли $A_k = ({}^k a_{i,j})$) однозначно определяется по своему месту и базовому группоиду M (матрице A) в заданной шкале. С другой стороны, для любых значений s, $i \in 1..n_s$, $j \in 1..n_s$ и $k \geqslant s$ имеет место равенство ${}^s a_{i,j} = {}^k a_{i,j}$. Это позволяет определять элементы матриц ${}^k a_{i,j}$, исходя только из значений их индексов и элементов базовой матрицы A.

Сказанное в замечании 2.1.6 позволяет сформулировать простые рекурсивные алгоритмы определения значений элементов матриц Кэли ${}^k a_{i,j}$ фрактальной шкалы в диагональных, строковых, столбцевых и тривиальных шкалах.

2.1.1. Алгоритм определения элемента матриц Кэли диагональных шкал по его индексам (диагональный алгоритм) DA(A, i, j)

Входные данные: базовая матрица $A = (a_{i,j})$; значения индексов i, j элементов фрактальной матрицы.

1. Вычислить порядок базовой матрицы A: $n := \mathrm{ord(A)}$.
2. Вычислить место наименьшего фрактального группоида, матрица Кэли которого содержит элемент с индексами i, j: $k := \lceil \max(\log(\frac{i}{n}), \log(\frac{j}{n})) \rceil$, где $\lceil x \rceil$ — потолок x — наименьшее целое, превосходящее или равное x.
3. Если $i \leqslant n \wedge j \leqslant n$, то
   3.1. Вывести $a_{i,j}$,

иначе
   3.2. Если $i \leqslant 2^{k-1}n \wedge j > 2^{k-1}n$, то
      3.2.1. Вывести $DA(A, i, j - 2^{k-1}n) + 2^{k-1}n$,
   иначе
      3.2.2. Если $i > 2^{k-1}n \wedge j \leqslant 2^{k-1}n$, то
         3.2.2.1. Вывести $DA(A, i - 2^{k-1}n, j) + 2^{k-1}n$,
      иначе
         3.2.2.2. Вывести $DA(A, i - 2^{k-1}n, j - 2^{k-1}n)$.
4. Завершить работу.

2.1.2. Алгоритм определения элемента матриц Кэли строковых шкал по его индексам (строковый алгоритм) RA(A, i, j)

Входные данные: базовая матрица $A = (a_{i,j})$; значения индексов i, j элементов фрактальной матрицы.

1. Вычислить порядок базовой матрицы A: $n := \mathrm{ord(A)}$.
2. Вычислить место наименьшего фрактального группоида, матрица Кэли которого содержит элемент с индексами i, j: $k := \lceil \max(\log(\frac{i}{n}), \log(\frac{j}{n})) \rceil$.
3. Если $i \leqslant n \wedge j \leqslant n$, то
   3.1. Вывести $a_{i,j}$,

иначе
   3.2. Если $i \leqslant 2^{k-1}n \wedge j > 2^{k-1}n$, то
      3.2.1. Вывести $RA(A, i, j - 2^{k-1}n)$,
   иначе
      3.2.2. Если $i > 2^{k-1}n \wedge j \leqslant 2^{k-1}n$, то
         3.2.2.1. Вывести $RA(A, i - 2^{k-1}n, j) + 2^{k-1}n$,
      иначе
         3.2.2.2. Вывести $RA(A, i - 2^{k-1}n, j - 2^{k-1}n) + 2^{k-1}n$.
4. Завершить работу.

2.1.3. Алгоритм определения элемента матриц Кэли столбцевых шкал по его индексам (столбцевой алгоритм) CA(A, i, j)

Входные данные: базовая матрица $A = (a_{i,j})$; значения индексов i, j элементов фрактальной матрицы.

1. Вычислить порядок базовой матрицы A: $n := \mathrm{ord(A)}$.
2. Вычислить место наименьшего фрактального группоида, матрица Кэли которого содержит элемент с индексами i, j: $k := \lceil \max(\log(\frac{i}{n}), \log(\frac{j}{n})) \rceil$.
3. Если $i \leqslant n \wedge j \leqslant n$, то
   3.1. Вывести $a_{i,j}$,

иначе

3.2. Если $i \leqslant 2^{k-1}n \wedge j > 2^{k-1}n$, то
3.2.1. Вывести $CA(A, i, j - 2^{k-1}n) + 2^{k-1}n$,
иначе
3.2.2. Если $i > 2^{k-1}n \wedge j \leqslant 2^{k-1}n$, то
3.2.2.1. Вывести $CA(A, i - 2^{k-1}n, j)$,
иначе
3.2.2.2. Вывести $CA(A, i - 2^{k-1}n, j - 2^{k-1}n) + 2^{k-1}n$.
4. Завершить работу.

2.1.4. Алгоритм определения элемента матриц Кэли тривиальных шкал по его индексам (тривиальный алгоритм) ТА(A, i, j)

Входные данные: базовая матрица $A = (a_{i,j})$; значения индексов i, j элементов фрактальной матрицы.

1. Вычислить порядок базовой матрицы A: $n := \mathrm{ord(A)}$.
2. Вычислить место наименьшего фрактального группоида, матрица Кэли которого содержит элемент с индексами i, j: $k := \lceil \max(\log(\frac{i}{n}), \log(\frac{j}{n})) \rceil$.
3. Если $i \leqslant n \wedge j \leqslant n$, то
3.1. Вывести $a_{i,j}$,
иначе
3.2. Если $i \leqslant 2^{k-1}n \wedge j > 2^{k-1}n$, то
3.2.1. Вывести $TA(A, i, j - 2^{k-1}n)$,
иначе
3.2.2. Если $i > 2^{k-1}n \wedge j \leqslant 2^{k-1}n$, то
3.2.2.1. Вывести $TA(A, i - 2^{k-1}n, j)$,
иначе
3.2.2.2. Вывести $TA(A, i - 2^{k-1}n, j - 2^{k-1}n)$.
4. Завершить работу.

2.2. Полугруппы бинарных операций и матриц Кэли

Для обозначения результатов бинарных операций на множестве U будем использовать как инфиксное $u_1 * u_2$, так и префиксное $\phi_*(u_1, u_2)$ обозначения. Множество бинарных операций будем обозначать U^{U^2}.

Следуя [5], дадим следующее

Определение 2.2.1. Композицией бинарных операций $\phi_*(u_1, u_2)$ и $\phi_\star(u_1, u_2)$ будем называть бинарную операцию $\phi_* \circ \phi_\star(u_1, u_2)$, определяемую правилом

$$u_3 = \phi_* \circ \phi_\star(u_1, u_2) = \phi_\star(\phi_*(u_1, u_2), u_2) = (u_1 * u_2) \star u_2.$$

В [5] было показано, что множество U^{U^2} замкнуто относительно операции $\circ$, а сама эта операция ассоциативна. Кроме того, она обладает нейтральным элементом — операцией полугруппы левых нулей (правых единиц) $\wr$, которая определена правилом $u_1 \wr u_2 = u_1$. Действительно,

$$(u_1 \wr u_2) * u_2 = u_1 * u_2 = (u_1 * u_2) \wr u_2.$$

Таким образом, алгебра $\langle U^{U^2}, (\circ) \rangle$ является полугруппой с единицей $\phi_\wr$, или моноидом.

Стандартным образом определим положительную степень $m \in \mathbb{N}$ бинарной операции ϕ_*

$$\begin{aligned} \phi_*^1 &= \phi_*, \\ \phi_*^{m+1} &= \phi_*^m \circ \phi_*. \end{aligned} \tag{2.5}$$

Рассмотрим пару группоидов $\langle 1..n, (\diamond) \rangle$ и $\langle 1..n, (\triangleright) \rangle$ с матрицами Кэли $A = (a_{i,j})$ и $B = (b_{i,j})$, соответственно.

Нетрудно понять, что т. к. $i \diamond j = a_{i,j}$ и $i \triangleright j = b_{i,j}$, то

$$\phi_\diamond \circ \phi_\triangleright(i, j) = \phi_\triangleright(\phi_\diamond(i, j), j) = (i \diamond j) \triangleright j = a_{i,j} \triangleright j = b_{a_{i,j},j},$$

т. е. элементы матрицы Кэли $C = (c_{i,j})$ композиции операций $\phi_\diamond(u_1, u_2)$ и $\phi_\triangleright(u_1, u_2)$ определяются правилом

$$c_{i,j} = b_{a_{i,j},j}. \tag{2.6}$$

В частности, элементы матрицы Кэли $A^2 = (a^2_{i,j})$ операции $\phi^2_\diamond$ — квадрата операции $\diamond$ — имеют вид

$$a^2_{i,j} = a_{a_{i,j},j}. \tag{2.7}$$

Определение 2.2.2. Произведением матриц Кэли $A = (a_{i,j})$ и $B = (b_{i,j})$ одного порядка n будем называть матрицу $C = (c_{i,j})$ порядка n, элементы которой определены в соответствии с (2.6). Произведение матриц будем обозначать $A \bullet B$. Стандартным образом определим положительную степень $m \in \mathbb{N}$ матрицы A

$$\begin{array}{l} A^1 = A, \\ A^{m+1} = A^m \bullet A. \end{array} \tag{2.8}$$

Замечание 2.2.1.
Обозначим множество бинарных операций на конечном множестве $1..n$ как $(1..n)^{(1..n)^2}$ и рассмотрим полугруппу $\langle (1..n)^{(1..n)^2}, (\circ) \rangle$.

Обозначим множество квадратных матриц (Кэли) $A = (a_{i,j})$ порядка n с элементами $a_{i,j} \in 1..n$ как $K(1..n)$ и рассмотрим полугруппу $\langle K(1..n), (\bullet) \rangle$.

Нетрудно понять, что полугруппы $\langle (1..n)^{(1..n)^2}, (\circ) \rangle$ и $\langle K(1..n), (\bullet) \rangle$ изоморфны.

2.3. Свойства фрактальных матриц

Рассмотрим две базовые матрицы Кэли $A = (a_{i,j})$ и $B = (b_{i,j})$ одного порядка n, а также их фрактальные расширения $A^{(d)}$, $A^{(r)}$, $A^{(c)}$, $A^{(t)}$, $B^{(d)}$, $B^{(r)}$, $B^{(c)}$, $B^{(t)}$.

2.3.1. Произведение расширений $\mathbf{A^{(d)} \bullet B^{(d)}}$

Рассмотрим произведение $A^{(d)} \bullet B^{(d)}$. В соответствии с (2.1), (2.6) и учетом того, что $a_{i,j}, b_{i,j} \in 1..n$ и $a_{i,j} + n, b_{i,j} + n \in n+1..2n$, при $i, j \in 1..n$, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(d)}_{i,j},j} = b^{(d)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(d)}_{i,j},j} = b^{(d)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n}.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(d)}_{i,j},j} = b^{(d)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j} + n.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(d)}_{i,j},j} = b^{(d)}_{a_{i-n,j-n},j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(d)} \bullet B^{(d)} = (a^{(d)} \bullet b^{(d)}{}_{i,j})$, где

$$a^{(d)} \bullet b^{(d)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.9}$$

2.3.2. Произведение расширений $\mathbf{A^{(d)} \bullet B^{(r)}}$

Рассмотрим произведение $A^{(d)} \bullet B^{(r)}$. В соответствии с (2.1), (2.2), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(d)}_{i,j},j} = b^{(r)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(d)}_{i,j},j} = b^{(r)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(d)}_{i,j},j} = b^{(r)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j} + n.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(d)}_{i,j},j} = b^{(r)}_{a_{i-n,j-n},j} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $A^{(d)} \bullet B^{(r)} = (a^{(d)} \bullet b^{(r)}{}_{i,j})$, где

$$a^{(d)} \bullet b^{(r)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.10}$$

2.3.3. Произведение расширений $\mathbf{A^{(r)} \bullet B^{(d)}}$

Рассмотрим произведение $A^{(r)} \bullet B^{(d)}$. В соответствии с (2.1), (2.2), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(r)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(r)}_{i,j},j} = b^{(d)}_{a_{i,j},j} = b_{a_{i,j},j}.$$
2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(r)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(r)}_{i,j},j} = b^{(d)}_{a_{i,j-n},j} = b_{a_{i,j-n},j-n} + n.$$
3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(r)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(r)}_{i,j},j} = b^{(d)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j} + n.$$
4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(r)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(r)}_{i,j},j} = b^{(d)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $A^{(r)} \bullet B^{(d)} = (a^{(r)} \bullet b^{(d)}{}_{i,j})$, где

$$a^{(r)} \bullet b^{(d)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.11}$$

2.3.4. Произведение расширений $\mathbf{A^{(d)} \bullet B^{(c)}}$

Рассмотрим произведение $A^{(d)} \bullet B^{(c)}$. В соответствии с (2.1), (2.3), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(d)}_{i,j},j} = b^{(c)}_{a_{i,j},j} = b_{a_{i,j},j}.$$
2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(d)}_{i,j},j} = b^{(c)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n} + n.$$
3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(d)}_{i,j},j} = b^{(c)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j}.$$
4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(d)}_{i,j},j} = b^{(c)}_{a_{i-n,j-n},j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(d)} \bullet B^{(c)} = (a^{(d)} \bullet b^{(c)}{}_{i,j})$, где

$$a^{(d)} \bullet b^{(c)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.12}$$

2.3.5. Произведение расширений $\mathbf{A^{(c)} \bullet B^{(d)}}$

Рассмотрим произведение $A^{(c)} \bullet B^{(d)}$. В соответствии с (2.1), (2.3), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(c)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(c)}_{i,j},j} = b^{(d)}_{a_{i,j},j} = b_{a_{i,j},j}.$$
2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(c)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(c)}_{i,j},j} = b^{(d)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n}.$$
3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(c)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(c)}_{i,j},j} = b^{(d)}_{a_{i-n,j},j} = b_{a_{i-n,j},j}.$$
4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(c)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(c)}_{i,j},j} = b^{(d)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $A^{(c)} \bullet B^{(d)} = (a^{(c)} \bullet b^{(d)}{}_{i,j})$, где

$$a^{(c)} \bullet b^{(d)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.13}$$

2.3.6. Произведение расширений $\mathbf{A^{(d)} \bullet B^{(t)}}$

Рассмотрим произведение $A^{(d)} \bullet B^{(r)}$. В соответствии с (2.1), (2.4), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(d)}_{i,j},j} = b^{(t)}_{a_{i,j},j} = b_{a_{i,j},j}.$$
2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(d)}_{i,j},j} = b^{(t)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n}.$$
3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(d)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(d)}_{i,j},j} = b^{(t)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j}.$$
4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(d)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(d)}_{i,j},j} = b^{(t)}_{a_{i-n,j-n},j} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $A^{(d)} \bullet B^{(t)} = (a^{(d)} \bullet b^{(t)}{}_{i,j})$, где

$$a^{(d)} \bullet b^{(t)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.14}$$

2.3.7. Произведение расширений $\mathbf{A^{(t)} \bullet B^{(d)}}$

Рассмотрим произведение $A^{(t)} \bullet B^{(d)}$. В соответствии с (2.1), (2.4), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(t)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(t)}_{i,j},j} = b^{(d)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a^{(t)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(t)}_{i,j},j} = b^{(d)}_{a_{i,j-n},j} = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a^{(t)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(t)}_{i,j},j} = b^{(d)}_{a_{i-n,j},j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a^{(t)} \bullet b^{(d)}{}_{i,j} = b^{(d)}_{a^{(t)}_{i,j},j} = b^{(d)}_{a_{i-n,j-n},j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(t)} \bullet B^{(d)} = (a^{(c)} \bullet b^{(d)}{}_{i,j})$, где

$$a^{(r)} \bullet b^{(d)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.15}$$

2.3.8. Произведение расширений $\mathbf{A^{(r)} \bullet B^{(r)}}$

Рассмотрим произведение $A^{(r)} \bullet B^{(r)}$. В соответствии с (2.2), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a^{(r)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(r)}_{i,j},j} = b^{(r)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a^{(r)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(r)}_{i,j},j} = b^{(r)}_{a_{i,j-n},j} = b_{a_{i,j-n},j-n}.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a^{(r)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(r)}_{i,j},j} = b^{(r)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j} + n.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a^{(r)} \bullet b^{(r)}{}_{i,j} = b^{(d)}_{a^{(r)}_{i,j},j} = b^{(r)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(r)} \bullet B^{(d)} = (a^{(r)} \bullet b^{(d)}{}_{i,j})$, где

$$a^{(r)} \bullet b^{(r)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.16}$$

2.3.9. Произведение расширений $\mathbf{A^{(r)} \bullet B^{(c)}}$

Рассмотрим произведение $A^{(r)} \bullet B^{(c)}$. В соответствии с (2.2), (2.3), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a^{(r)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(r)}_{i,j},j} = b^{(c)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a^{(r)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(r)}_{i,j},j} = b^{(c)}_{a_{i,j-n},j} = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a^{(r)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(r)}_{i,j},j} = b^{(c)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a^{(r)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(r)}_{i,j},j} = b^{(c)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(r)} \bullet B^{(c)} = (a^{(d)} \bullet b^{(c)}{}_{i,j})$, где

$$a^{(d)} \bullet b^{(c)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.17}$$

2.3.10. Произведение расширений $\mathbf{A^{(c)} \bullet B^{(r)}}$

Рассмотрим произведение $A^{(c)} \bullet B^{(r)}$. В соответствии с (2.2), (2.3), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a^{(c)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(c)}_{i,j},j} = b^{(r)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a^{(c)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(c)}_{i,j},j} = b^{(r)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a^{(c)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(c)}_{i,j},j} = b^{(r)}_{a_{i-n,j},j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a^{(c)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(c)}_{i,j},j} = b^{(r)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(c)} \bullet B^{(r)} = (a^{(c)} \bullet b^{(r)}{}_{i,j})$, где

$$a^{(c)} \bullet b^{(r)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.18}$$

2.3.11. Произведение расширений $\mathbf{A^{(r)} \bullet B^{(t)}}$

Рассмотрим произведение $A^{(r)} \bullet B^{(t)}$. В соответствии с (2.1), (2.4), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a^{(r)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(r)}_{i,j},j} = b^{(t)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a^{(r)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(r)}_{i,j},j} = b^{(t)}_{a_{i,j-n},j} = b_{a_{i,j-n},j-n}.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a^{(r)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(r)}_{i,j},j} = b^{(t)}_{a_{i-n,j}+n,j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a^{(r)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(r)}_{i,j},j} = b^{(t)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $A^{(d)} \bullet B^{(t)} = (a^{(d)} \bullet b^{(t)}{}_{i,j})$, где

$$a^{(r)} \bullet b^{(t)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.19}$$

2.3.12. Произведение расширений $\mathbf{A^{(t)} \bullet B^{(r)}}$

Рассмотрим произведение $A^{(t)} \bullet B^{(r)}$. В соответствии с (2.2), (2.4), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(t)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(t)}_{i,j},j} = b^{(r)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(t)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(t)}_{i,j},j} = b^{(r)}_{a_{i,j-n},j} = b_{a_{i,j-n},j-n}.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(t)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(t)}_{i,j},j} = b^{(r)}_{a_{i-n,j},j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(t)} \bullet b^{(r)}{}_{i,j} = b^{(r)}_{a^{(t)}_{i,j},j} = b^{(r)}_{a_{i-n,j-n},j} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $A^{(t)} \bullet B^{(r)} = (a^{(t)} \bullet b^{(r)}{}_{i,j})$, где

$$a^{(t)} \bullet b^{(r)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.20}$$

2.3.13. Произведение расширений $\mathbf{A^{(c)} \bullet B^{(c)}}$

Рассмотрим произведение $A^{(c)} \bullet B^{(c)}$. В соответствии с (2.3), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(c)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(c)}_{i,j},j} = b^{(c)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a^{(c)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(c)}_{i,j},j} = b^{(c)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a^{(c)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(c)}_{i,j},j} = b^{(c)}_{a_{i-n,j},j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a^{(c)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(c)}_{i,j},j} = b^{(c)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(c)} \bullet B^{(c)} = (a^{(c)} \bullet b^{(c)}{}_{i,j})$, где

$$a^{(c)} \bullet b^{(c)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.21}$$

2.3.14. Произведение расширений $\mathbf{A^{(c)} \bullet B^{(t)}}$

Рассмотрим произведение $A^{(c)} \bullet B^{(t)}$. В соответствии с (2.3), (2.4), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a^{(c)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(c)}_{i,j},j} = b^{(t)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a^{(c)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(c)}_{i,j},j} = b^{(t)}_{a_{i,j-n}+n,j} = b_{a_{i,j-n},j-n}.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a^{(c)} \bullet b^{(t)}{}_{i,j} = b^{(t)}_{a^{(c)}_{i,j},j} = b^{(t)}_{a_{i-n,j},j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a^{(c)} \bullet b^{(t)}{}_{i,j} = b^{(c)}_{a^{(c)}_{i,j},j} = b^{(t)}_{a_{i-n,j-n}+n,j} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $A^{(c)} \bullet B^{(t)} = (a^{(c)} \bullet b^{(t)}{}_{i,j})$, где

$$a^{(c)} \bullet b^{(t)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.22}$$

2.3.15. Произведение расширений $\mathbf{A^{(t)} \bullet B^{(c)}}$

Рассмотрим произведение $A^{(t)} \bullet B^{(c)}$. В соответствии с (2.3), (2.4), (2.6), как и ранее, получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a^{(t)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(t)}_{i,j},j} = b^{(c)}_{a_{i,j},j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a^{(t)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(t)}_{i,j},j} = b^{(c)}_{a_{i,j-n},j} = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a^{(t)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(t)}_{i,j},j} = b^{(c)}_{a_{i-n,j},j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a^{(t)} \bullet b^{(c)}{}_{i,j} = b^{(c)}_{a^{(t)}_{i,j},j} = b^{(c)}_{a_{i-n,j-n},j} = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $A^{(t)} \bullet B^{(c)} = (a^{(t)} \bullet b^{(c)}{}_{i,j})$, где

$$a^{(t)} \bullet b^{(c)}{}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.23}$$

2.3.16. Расширение произведения $\mathbf{(A \bullet B)^{(d)}}$

Рассмотрим диагональное расширение произведения матриц $(A \bullet B)^{(d)}$. В соответствии с (2.2) и (2.6), получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a \bullet b^{(d)}_{i,j} = a \bullet b_{i,j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a \bullet b^{(d)}_{i,j} = a \bullet b_{i,j-n} + n = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a \bullet b^{(d)}_{i,j} = a \bullet b_{i-n,j} + n = b_{a_{i-n,j},j} + n.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a \bullet b^{(d)}_{i,j} = a \bullet b_{i-n,j-n} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $(A \bullet B)^{(d)} = (a \bullet b^{(d)}_{i,j})$, где

$$a \bullet b^{(d)}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.24}$$

2.3.17. Расширение произведения $(\mathbf{A} \bullet \mathbf{B})^{(\mathbf{r})}$

Рассмотрим строковое расширение произведения матриц $(A \bullet B)^{(r)}$. В соответствии с (2.2) и (2.6), получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a \bullet b^{(r)}_{i,j} = a \bullet b_{i,j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a \bullet b^{(r)}_{i,j} = a \bullet b_{i,j-n} = b_{a_{i,j-n},j-n}.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a \bullet b^{(r)}_{i,j} = a \bullet b_{i-n,j} + n = b_{a_{i-n,j},j} + n.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a \bullet b^{(r)}_{i,j} = a \bullet b_{i-n,j-n} + n = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $(A \bullet B)^{(r)} = (a \bullet b^{(r)}_{i,j})$, где

$$a \bullet b^{(r)}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j} + n\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.25}$$

2.3.18. Расширение произведения $(\mathbf{A} \bullet \mathbf{B})^{(\mathbf{c})}$

Рассмотрим столбцевое расширение произведения матриц $(A \bullet B)^{(c)}$. В соответствии с (2.3) и (2.6), получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то

$$a \bullet b^{(c)}_{i,j} = a \bullet b_{i,j} = b_{a_{i,j},j}.$$

2. Если $i \in 1..n \wedge j \in n+1..2n$, то

$$a \bullet b^{(c)}_{i,j} = a \bullet b_{i,j-n} + n = b_{a_{i,j-n},j-n} + n.$$

3. Если $i \in n+1..2n \wedge j \in 1..n$, то

$$a \bullet b^{(c)}_{i,j} = a \bullet b_{i-n,j} = b_{a_{i-n,j},j}.$$

4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то

$$a \bullet b^{(c)}_{i,j} = a \bullet b_{i-n,j-n} + n = b_{a_{i-n,j-n},j-n} + n.$$

Таким образом, имеет место равенство $(A \bullet B)^{(c)} = (a \bullet b^{(c)}_{i,j})$, где

$$a \bullet b^{(c)}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n} + n\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n} + n\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.26}$$

2.3.19. Расширение произведения $(\mathbf{A \bullet B})^{(\mathbf{t})}$

Рассмотрим тривиальное расширение произведения матриц $(A \bullet B)^{(t)}$. В соответствии с (2.4) и (2.6), получаем следующее.

1. Если $i \in 1..n \wedge j \in 1..n$, то
$$a \bullet b^{(c)}_{i,j} = a \bullet b_{i,j} = b_{a_{i,j},j}.$$
2. Если $i \in 1..n \wedge j \in n+1..2n$, то
$$a \bullet b^{(t)}_{i,j} = a \bullet b_{i,j-n} = b_{a_{i,j-n},j-n}.$$
3. Если $i \in n+1..2n \wedge j \in 1..n$, то
$$a \bullet b^{(t)}_{i,j} = a \bullet b_{i-n,j} = b_{a_{i-n,j},j}.$$
4. Если $i \in n+1..2n \wedge j \in n+1..2n$, то
$$a \bullet b^{(t)}_{i,j} = a \bullet b_{i-n,j-n} = b_{a_{i-n,j-n},j-n}.$$

Таким образом, имеет место равенство $(A \bullet B)^{(t)} = (a \bullet b^{(t)}_{i,j})$, где

$$a \bullet b^{(t)}_{i,j} = \begin{cases} b_{a_{i,j},j}\,, & i \in 1..n \wedge j \in 1..n \\ b_{a_{i,j-n},j-n}\,, & i \in 1..n \wedge j \in n+1..2n \\ b_{a_{i-n,j},j}\,, & i \in n+1..2n \wedge j \in 1..n \\ b_{a_{i-n,j-n},j-n}\,, & i \in n+1..2n \wedge j \in n+1..2n. \end{cases} \tag{2.27}$$

Из (2.9) и (2.27) следует

Утверждение 2.3.1. Пусть $A = (a_{i,j})$ и $B = (b_{i,j})$ — матрицы Кэли одного порядка n. Тогда

$$\begin{array}{l} A^{(d)} \bullet B^{(d)} = A^{(r)} \bullet B^{(r)} = (A \bullet B)^{(r)}, \\ A^{(d)} \bullet B^{(r)} = A^{(r)} \bullet B^{(d)} = (A \bullet B)^{(d)}, \\ A^{(d)} \bullet B^{(c)} = A^{(t)} \bullet B^{(d)} = A^{(r)} \bullet B^{(c)} = A^{(c)} \bullet B^{(r)} = A^{(c)} \bullet B^{(c)} = A^{(t)} \bullet B^{(c)} = (A \bullet B)^{(c)}, \\ A^{(c)} \bullet B^{(d)} = A^{(d)} \bullet B^{(t)} = A^{(r)} \bullet B^{(t)} = A^{(t)} \bullet B^{(r)} = A^{(c)} \bullet B^{(t)} = (A \bullet B)^{(t)}. \end{array}$$

Из утверждения 2.3.1 следует

Утверждение 2.3.2. Пусть $A = (a_{i,j})$ — матрица Кэли и $m \in \mathbb{N}$. Тогда степени фрактальных расширений матрицы Кэли A удовлетворяют следующим равенствам:

$$\begin{array}{ll} (A^{(d)})^m = (A^m)^{(r)}, & m = 2s \wedge s \in \mathbb{N}; \\ (A^{(d)})^m = (A^m)^{(d)}, & m = 2s-1 \wedge s \in \mathbb{N}; \\ (A^{(r)})^m = (A^m)^{(r)}, & m \in \mathbb{N}; \\ (A^{(c)})^m = (A^m)^{(c)}, & m \in \mathbb{N}; \\ (A^{(t)})^m = (A^m)^{(t)}, & m \in \mathbb{N}. \end{array}$$

Из утверждений 2.3.1, 2.3.2 и замечания 2.1.5 следует

Утверждение 2.3.3. Пусть $S_\sigma = \{M^{(\sigma)}_k\}_{k=1}^{\infty}$– шкала фрактальных группоидов $M^{(\sigma)}_k = \langle 1..n_k, (\diamond_k)\rangle$ с матрицами Кэли A_k и базовой матрицей A. Тогда семейство группоидов $M^m_k = \langle 1..n_k, (\phi^m_{\diamond_k})\rangle$, при фиксированном значении $m \in \mathbb{N}$, образует шкалу группоидов $S^m_{\sigma'}$ с базовой матрицей A^m, при этом тип шкалы $S^m_{\sigma'}$ будет определяться следующими условиями:

$$\begin{array}{ll} \sigma' = r, & \sigma = d \wedge m = 2s \wedge s \in \mathbb{N}; \\ \sigma' = d, & \sigma = d \wedge m = 2s-1 \wedge s \in \mathbb{N}; \\ \sigma' = \sigma, & \sigma \in \{r, c, t\} \wedge m \in \mathbb{N}. \end{array}$$

Замечание 2.3.1.
Утверждение 2.3.3 фактически означает, что для представления матрицами Кэли степеней фрактальных расширений операции базового группоида нет необходимости вычислять степени матриц Кэли этих расширений, а достаточно вычислить соответствующую степень матрицы Кэли базовой операции и затем построить матрицу нужного расширения.

С учетом алгоритмов 2.1.1–2.1.4 это позволяет получить существенный выигрыш при вычислении результатов операций во фрактальных шкалах группоидов. Напомним, что порядок матрицы Кэли $A^{(\sigma)}_k$ фрактального группоида зависит от его места k в шкале и порядка $n = \mathrm{ord}(A)$ базовой матрицы Кэли,

как $2^k n$, т. е. экспоненциально от k. В свою очередь глубина рекурсии алгоритмов 2.1.1–2.1.4 не превышает k.

В качестве примера рассмотрим конечную последовательность степеней матриц Кэли $(A_k^{(\sigma)})^m$ фрактальных шкал, построенных для базового группоида со случайной матрицей Кэли

$$A = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 3 \\ 2 & 1 & 1 \end{pmatrix}.$$

1. Степени базовой матрицы $(A^m,\ m \in 1..4)$

$$A = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 3 \\ 2 & 1 & 1 \end{pmatrix}, \quad A^2 = \begin{pmatrix} 1 & 3 & 1 \\ 2 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

2. Степени диагонального расширения $((A_1^{(d)})^m,\ m \in 1..4)$

$$(A_1^{(d)}) = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & 5 & 5 & 4 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & 4 & 6 & 6 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \\ \hline 5 & 5 & 4 & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ 4 & 6 & 6 & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ 5 & 4 & 4 & \mathbf{2} & \mathbf{1} & \mathbf{1} \end{array}\right), \quad (A_1^{(d)})^2 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \hline 4 & 6 & 4 & 4 & 6 & 4 \\ 5 & 4 & 4 & 5 & 4 & 4 \\ 4 & 5 & 4 & 4 & 5 & 4 \end{array}\right),$$

$$(A_1^{(d)})^3 = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & 4 & 5 & 4 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & 5 & 6 & 4 \\ \hline 5 & 4 & 4 & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ 4 & 5 & 4 & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ 5 & 6 & 4 & \mathbf{2} & \mathbf{3} & \mathbf{1} \end{array}\right), \quad (A_1^{(d)})^4 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \hline 4 & 5 & 4 & 4 & 5 & 4 \\ 5 & 6 & 4 & 5 & 6 & 1 \\ 4 & 4 & 4 & 4 & 4 & 4 \end{array}\right).$$

3. Степени диагонального расширения $((A_2^{(d)})^m,\ m \in 1..4)$

$$(A_2^{(d)}) = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{5} & \mathbf{5} & \mathbf{4} & 8 & 8 & 7 & 11 & 11 & 10 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{6} & \mathbf{6} & 7 & 9 & 9 & 10 & 12 & 12 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{5} & \mathbf{5} & \mathbf{4} & \mathbf{2} & \mathbf{2} & \mathbf{1} & 11 & 11 & 10 & 8 & 8 & 7 \\ \mathbf{4} & \mathbf{6} & \mathbf{6} & \mathbf{1} & \mathbf{3} & \mathbf{3} & 10 & 12 & 12 & 7 & 9 & 9 \\ \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{2} & \mathbf{1} & \mathbf{1} & 11 & 10 & 10 & 8 & 7 & 7 \\ \hline 8 & 8 & 7 & 11 & 11 & 10 & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{5} & \mathbf{5} & \mathbf{4} \\ 7 & 9 & 9 & 10 & 12 & 12 & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{6} & \mathbf{6} \\ 8 & 7 & 7 & 11 & 10 & 10 & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} \\ 11 & 11 & 10 & 8 & 8 & 7 & \mathbf{5} & \mathbf{5} & \mathbf{4} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ 10 & 12 & 12 & 7 & 9 & 9 & \mathbf{4} & \mathbf{6} & \mathbf{6} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ 11 & 10 & 10 & 8 & 7 & 7 & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{2} & \mathbf{1} & \mathbf{1} \end{array}\right),$$

$$(A_2^{(d)})^2 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} \\ \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} \\ \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} \\ \hline 7 & 9 & 7 & 7 & 9 & 7 & 7 & 9 & 7 & 7 & 9 & 7 \\ 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 \\ 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 \\ 10 & 12 & 10 & 10 & 12 & 10 & 10 & 12 & 10 & 10 & 12 & 10 \\ 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 \\ 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 \end{array}\right),$$

$$(A_2^{(d)})^3 = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{2} & \mathbf{1} & \mathbf{1} & 11 & 10 & 10 & 8 & 7 & 7 \\ \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{1} & \mathbf{2} & \mathbf{1} & 10 & 11 & 10 & 7 & 8 & 7 \\ \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{2} & \mathbf{3} & \mathbf{1} & 11 & 12 & 10 & 8 & 9 & 7 \\ \hline 8 & 7 & 7 & 11 & 10 & 10 & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} \\ 7 & 8 & 7 & 10 & 11 & 10 & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} \\ 8 & 9 & 7 & 11 & 12 & 10 & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} \\ 11 & 10 & 10 & 8 & 7 & 7 & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ 10 & 11 & 10 & 7 & 8 & 7 & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ 11 & 12 & 10 & 8 & 9 & 7 & \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{2} & \mathbf{3} & \mathbf{1} \end{array}\right),$$

$$(A_2^{(d)})^4 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} \\ \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} \\ \hline 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 \\ 8 & 9 & 7 & 8 & 9 & 7 & 8 & 9 & 7 & 8 & 9 & 7 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 \\ 11 & 12 & 10 & 11 & 12 & 10 & 11 & 12 & 10 & 11 & 12 & 10 \\ 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \end{array}\right).$$

4. Степени строкового расширения $((A_1^{(r)})^m,\ m \in 1..4)$

$$(A_1^{(r)}) = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \hline 5 & 5 & 4 & 5 & 5 & 4 \\ 4 & 6 & 6 & 4 & 6 & 6 \\ 5 & 4 & 4 & 5 & 4 & 4 \end{array}\right), \quad (A_1^{(r)})^2 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \hline 4 & 6 & 4 & 4 & 6 & 4 \\ 5 & 4 & 4 & 5 & 4 & 4 \\ 4 & 5 & 4 & 4 & 5 & 4 \end{array}\right),$$

$$(A_1^{(r)})^3 = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \hline 5 & 4 & 4 & 5 & 4 & 4 \\ 4 & 5 & 4 & 5 & 4 & 4 \\ 5 & 6 & 4 & 5 & 6 & 4 \end{array}\right), \quad (A_1^{(r)})^4 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \hline 4 & 5 & 4 & 4 & 5 & 4 \\ 5 & 6 & 4 & 5 & 6 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 \end{array}\right).$$

5. Степени строкового расширения $((A_2^{(r)})^m,\ m \in 1..4)$

$$(A_2^{(r)}) = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{5} & \mathbf{5} & \mathbf{4} & \mathbf{5} & \mathbf{5} & \mathbf{4} & \mathbf{5} & \mathbf{5} & \mathbf{4} & \mathbf{5} & \mathbf{5} & \mathbf{4} \\ \mathbf{4} & \mathbf{6} & \mathbf{6} & \mathbf{4} & \mathbf{6} & \mathbf{6} & \mathbf{4} & \mathbf{6} & \mathbf{6} & \mathbf{4} & \mathbf{6} & \mathbf{6} \\ \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} \\ \hline 8 & 8 & 7 & 8 & 8 & 7 & 8 & 8 & 7 & 8 & 8 & 7 \\ 7 & 9 & 9 & 7 & 9 & 9 & 7 & 9 & 9 & 7 & 9 & 9 \\ 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 \\ 11 & 11 & 10 & 11 & 11 & 10 & 11 & 11 & 10 & 11 & 11 & 10 \\ 10 & 12 & 12 & 10 & 12 & 12 & 10 & 12 & 12 & 10 & 12 & 12 \\ 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 \end{array}\right),$$

$$(A_2^{(r)})^2 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} \\ \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} \\ \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} \\ \hline 7 & 9 & 7 & 7 & 9 & 7 & 7 & 9 & 7 & 7 & 9 & 7 \\ 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 \\ 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 \\ 10 & 12 & 10 & 10 & 12 & 10 & 10 & 12 & 10 & 10 & 12 & 10 \\ 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 \\ 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 \end{array}\right),$$

$$(A_2^{(r)})^3 = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} \\ \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} \\ \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} \\ \hline 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 \\ 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 \\ 8 & 9 & 7 & 8 & 9 & 7 & 8 & 9 & 7 & 8 & 9 & 7 \\ 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 \\ 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 \\ 11 & 12 & 10 & 11 & 12 & 10 & 11 & 12 & 10 & 11 & 12 & 10 \end{array}\right),$$

$$(A_2^{(r)})^4 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{4} \\ \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{4} \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} \\ \hline 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 & 7 & 8 & 7 \\ 8 & 9 & 7 & 8 & 9 & 7 & 8 & 9 & 7 & 8 & 9 & 7 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 & 10 & 11 & 10 \\ 11 & 12 & 10 & 11 & 12 & 10 & 11 & 12 & 10 & 11 & 12 & 10 \\ 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \end{array}\right).$$

6. Степени столбцевого расширения $((A_1^{(c)})^m,\ m \in 1..4)$

$$(A_1^{(c)}) = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & 5 & 5 & 4 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & 4 & 6 & 6 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \\ \hline \mathbf{2} & \mathbf{2} & \mathbf{1} & 5 & 5 & 4 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & 4 & 6 & 6 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \end{array}\right), \quad (A_1^{(c)})^2 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & 4 & 6 & 4 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & 4 & 5 & 4 \\ \hline \mathbf{1} & \mathbf{3} & \mathbf{1} & 4 & 6 & 4 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & 4 & 5 & 4 \end{array}\right),$$

$$(A_1^{(c)})^3 = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & 4 & 5 & 4 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & 5 & 6 & 4 \\ \hline \mathbf{2} & \mathbf{1} & \mathbf{1} & 5 & 4 & 4 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & 4 & 5 & 4 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & 5 & 6 & 4 \end{array}\right), \quad (A_1^{(c)})^4 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & 4 & 5 & 4 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & 5 & 6 & 4 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & 4 & 4 & 4 \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{1} & 4 & 5 & 4 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & 5 & 6 & 4 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & 4 & 4 & 4 \end{array}\right).$$

7. Степени столбцевого расширения $((A_2^{(t)})^m,\ m \in 1..4)$

$$(A_2^{(c)}) = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{5} & \mathbf{5} & \mathbf{4} & 8 & 8 & 7 & 11 & 11 & 10 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{6} & \mathbf{6} & 7 & 9 & 9 & 10 & 12 & 12 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{5} & \mathbf{5} & \mathbf{4} & 8 & 8 & 7 & 11 & 11 & 10 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{6} & \mathbf{6} & 7 & 9 & 9 & 10 & 12 & 12 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \hline \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{5} & \mathbf{5} & \mathbf{4} & 8 & 8 & 7 & 11 & 11 & 10 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{6} & \mathbf{6} & 7 & 9 & 9 & 10 & 12 & 12 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{5} & \mathbf{5} & \mathbf{4} & 8 & 8 & 7 & 11 & 11 & 10 \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{6} & \mathbf{6} & 7 & 9 & 9 & 10 & 12 & 12 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \end{array}\right),$$

$$(A_2^{(c)})^2 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{4} & \mathbf{6} & \mathbf{4} & 7 & 9 & 7 & 10 & 12 & 10 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{4} & \mathbf{6} & \mathbf{4} & 7 & 9 & 7 & 10 & 12 & 10 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \hline \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{4} & \mathbf{6} & \mathbf{4} & 7 & 9 & 7 & 10 & 12 & 10 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{4} & \mathbf{6} & \mathbf{4} & 7 & 9 & 7 & 10 & 12 & 10 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \end{array}\right),$$

$$(A_2^{(c)})^3 = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \hline \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{5} & \mathbf{4} & \mathbf{4} & 8 & 7 & 7 & 11 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \end{array}\right),$$

$$(A_2^{(c)})^4 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{4} & \mathbf{4} & \mathbf{4} & 7 & 7 & 7 & 10 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{4} & \mathbf{4} & \mathbf{4} & 7 & 7 & 7 & 10 & 10 & 10 \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{4} & \mathbf{4} & \mathbf{4} & 7 & 7 & 7 & 10 & 10 & 10 \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{5} & \mathbf{4} & 7 & 8 & 7 & 10 & 11 & 10 \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{6} & \mathbf{4} & 8 & 9 & 7 & 11 & 12 & 10 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{4} & \mathbf{4} & \mathbf{4} & 7 & 7 & 7 & 10 & 10 & 10 \end{array}\right).$$

8. Степени тривиального расширения $((A_1^{(t)})^m,\ m \in 1..4)$

$$(A_1^{(t)}) = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \end{array}\right), \quad (A_1^{(t)})^2 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \end{array}\right),$$

$$(A_1^{(t)})^3 = \left(\begin{array}{ccc|ccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \hline \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \end{array}\right), \quad (A_1^{(t)})^4 = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{array}\right).$$

9. Степени тривиального расширения $((A_2^{(t)})^m,\ m \in 1..4)$

$$(A_2^{(t)}) = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} & \mathbf{1} & \mathbf{3} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \end{array}\right),$$

$$(A_2^{(t)})^2 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \end{array}\right),$$

$$(A_2^{(t)})^3 = \left(\begin{array}{cccccc|cccccc} \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \hline \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \end{array}\right),$$

$$(A_2^{(t)})^4 = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{array}\right).$$

2.4. Циклические полугруппы фрактальных расширений и криптография с открытым ключом

Рассмотрим базовый группоид $M = \langle 1..n, (\diamond)\rangle$ с матрицей Кэли $A = (a_{i,j})$ и некоторую шкалу его фрактальных расширений $S_\sigma = \{M_k^{(\sigma)}\}_{k=0}^{\infty}$. Зафиксируем место k_0 в этой шкале и соответствующий ему группоид $M_{k_0}^{(\sigma)} = \langle 1..n_{k_0}, (\diamond_{k_0}^{\sigma})\rangle$. Для упрощения записи будем обозначать его как $M_* = \langle 1..N, (*)\rangle$, где $N = 2^{k_0}n$ и $\phi_* = \phi_{\diamond_{k_0}^{\sigma}}$. Матрицу Кэли операции $*$ обозначим как $\mathrm{A} = (\alpha_{i,j})$.

В дальнейшем нас будет интересовать циклическая полугруппа степеней операции $*$ — $\langle\{\phi_*^m\}_{m=1}^{\infty}, (\circ)\rangle \subset \langle U^{U^2}, (\circ)\rangle$.

В [5] была предложена следующая модификация протокола Диффи — Хелмана — Меркла (DHM) открытого распределения ключей шифрования на основе группоидов.

Протокол Диффи — Хелмана — Меркла на группоидах DHM-M

1. Опубликованные общедоступные значения: группоид $\langle U, (*)\rangle$; $p \in \mathbb{N}$; последовательность значений аргументов $\{(u_1^i, u_2^i)\}_{i=1}^p$, $u_1^i, u_2^i \in U$, $i \in 1..p$.

2. Вычисляемые значения на стороне A: операция $\phi_\star = \phi_*^m$– m-я степень операции $*$, последовательность значений результатов операции $\{\phi_\star(u_1^i, u_2^i)\}_{i=1}^p$. Значения, передаваемые по открытому каналу связи: $\{\phi_\star(u_1^i, u_2^i)\}_{i=1}^p$. Секретное значение: m.

3. Вычисляемые значения на стороне B: операция $\phi_{\star'} = \phi_*^{m'}$– m'-я степень операции $*$, последовательность значений результатов операции $\{\phi_{\star'}(u_1^i, u_2^i)\}_{i=1}^p$. Значения, передаваемые по открытому каналу связи: $\{\phi_{\star'}(u_1^i, u_2^i)\}_{i=1}^p$. Секретное значение: m'.

4. Вычисляемое значение секретного ключа на стороне A: $K = \{\phi_\star(\phi_{\star'}(u_1^i, u_2^i), u_2^i)\}_{i=1}^p$.

5. Вычисляемое значение секретного ключа на стороне B: $K = \{\phi_{\star'}(\phi_\star(u_1^i, u_2^i), u_2^i)\}_{i=1}^p$.

6. Значения, известные третьей стороне C: $\langle U, (*)\rangle$, p, $\{(u_1^i, u_2^i)\}_{i=1}^p$, $\{\phi_{\star_m}(u_1^i, u_2^i)\}_{i=1}^p$, $\{\phi_{\star_{m'}}(u_1^i, u_2^i)\}_{i=1}^p$.

Так как в силу ассоциативности операции $\circ$ имеет место правило степеней

$$\phi_\star \circ \phi_{\star'} = \phi_*^m \circ \phi_*^{m'} = \phi_*^{m+m'} = \phi_*^{m'} \circ \phi_*^m = \phi_{\star'} \circ \phi_\star,$$

то значения секретных ключей $\phi_\star(\phi_{\star'}(u_1^i, u_2^i), u_2^i) = \phi_{\star'} \circ \phi_\star(u_1, u_2)$ и $\phi_{\star'}(\phi_\star(u_1^i, u_2^i), u_2^i) = \phi_\star \circ \phi_{\star'}(u_1, u_2)$, вычисленные на сторонах A и B, совпадают.

Хорошо известно [6], что сложность вычисления операции $\phi_\star = \phi_*^m$ с применением быстрого алгоритма возведения в степень оценивается как $O(\log(m))$ полугрупповых операций $\circ$.

Возможности практического применения протокола DHM-M в первую очередь определяются потребностями в памяти для представления операций $\phi_\star = \phi_*^m$ и $\phi_{\star'} = \phi_*^{m'}$ на носителе большой мощности и вычислительной сложностью алгоритма построения секретного ключа.

В [5] рассматривался способ представления операции $\phi_\star = \phi_*^m$ индикатором ее графика, точнее, представлением индикатора в форме трехиндексного массива двоичных значений $r_{i,j,k}^m$, $i, j, k \in 1..N$, который в случае группоида $M_* = \langle 1..N, (*)\rangle$ определяется правилом

$$r_{i,j,k}^m = \begin{cases} 1\,, & \phi_*^m(i,j) = k \\ 0\,, & \phi_*^m(i,j) \neq k \end{cases}.$$

Нетрудно показать [5], что циклическая полугруппа $\langle\{\phi_*^m\}_{m=1}^\infty,(\circ)\rangle$ изоморфна полугруппе $\langle\{r_{i,j,k}^m\}_{m=1}^\infty,(\cdot)\rangle$, где

$$r_{i,j,s}^m\cdot r_{s,j,k}^n=\max\nolimits_{s\in 1..N}(\min(r_{i,j,s}^m,r_{s,j,k}^n)),$$

$$r_{i,j,k}=\begin{cases}1\,, & i*j=k\\ 0\,, & i*j\neq k\end{cases},$$

$$r_{i,j,k}^1=r_{i,j,k},$$

$$r_{i,j,k}^{m+1}=r_{i,j,s}^m\cdot r_{s,j,k},\ i,j,k\in 1..N,\ m\in\mathbb{N}.$$

При таком способе представления сложность реализации операции $\circ$ оценивается как $O(N^4)$ элементарных операций (взятия минимума и максимума из двоичных значений). Сложность нахождения результата операции $\phi_*^m(i,j)$ оценивается как $O(N)$ элементарных операций сравнения (двоичных значений). Грубые верхние оценки потребности в памяти и вычислительная сложность алгортима построения секретного ключа составляют $O(N^3)$ бит и $O(N^4)$ элементарных операций, соответственно. Таким образом, даже при мощности носителя группоида $N\sim 2^{20}$ потребности в памяти и вычислительная сложность будут весьма велики и составят $O(2^{60})$ и $O(2^{80})$ единиц измерения.

Изученные в предыдущих разделах фрактальные группоиды пригодны для снижения вычислительных затрат при реализации протокола DHM-M. В силу замечания 2.3.1 для вычисления результата операции $\phi_\star(i,j)=\phi_*^m(i,j)$ фрактального группоида $M_*=\langle 1..N,(*)\rangle$ потребуется хранение только матрицы Кэли $A=(a_{i,j})$ базового группоида $M=\langle 1..n,(\diamond)\rangle$, где $N=2^{k_0}n$, и применение к ней одного из алгоритмов 2.1.1–2.1.4, глубина рекурсии каждого из которых не превзойдет k_0.

Для более точных оценок рассмотрим пару матриц Кэли $A=(a_{i,j})$ и $B=(b_{i,j})$ порядка n и матричную операцию $\bullet$, определенную в соответствии с (2.6) как $A\bullet B=(b_{a_{i,j},j})$. Нетрудно понять, что реализация операции $\bullet$ потребует $2n^2$ операций последовательного доступа к элементам матриц A и B и одной операции записи итогового значения в результирующий массив. Последовательность этих трех операций будем считать элементарной операцией доступа. Таким образом, вычислительная сложность операции $\bullet$ может быть оценена как $2n^2$ элементарных операций доступа.

В силу замечания 2.2.1, циклические полугруппы $\langle\{\phi_\diamond^m\}_{m=1}^\infty,(\circ)\rangle$ и $\langle\{A^m\}_{m=1}^\infty,(\bullet)\rangle$ изоморфны, поэтому вычислительную сложность реализации операции $\phi_\diamond^m$ можно оценить как $O(mn^2)$ элементарных операций доступа.

Для представления $i\in 1..N$ потребуется не более $\log(N)+1=k_0+\log(n)+1$ бит. При этом потребности в памяти для представления операции $\phi_\diamond$ матрицей Кэли можно оценить как $O(n^2\log(n)$ бит.

Для оценки вычислительной сложности определения результата операции $\phi_\star(i,j)=\phi_*^m(i,j)$ достаточно проанализировать операции, выполняемые на шаге 3.2 каждого из алгоритмов 2.1.1–2.1.4. На каждом уровне рекурсии будет выполняться не более двух операций вычитания для индексов $i-n$, $j-n$, не более одной операции сложения для возвращаемого значения процедуры $D/R/C/TA+n$ и не более трех операций целочисленного сравнения. Таким образом, вычислительную сложность определения значения $\phi_\star(i,j)$ можно оценить как $O(k_0)$ арифметических операций и операций целочисленного сравнения.

Сформулируем протокол Диффи — Хелмана — Меркла для фрактальных группоидов.

Протокол Диффи — Хелмана — Меркла на группоидах DHM-FM

1. Опубликованные общедоступные значения: базовый группоид $\langle 1..n,(\diamond)\rangle$ (базовая матрица Кэли $A=(a_{i,j})$); тип расширения $\sigma\in\{d,r,c,t\}$, $p\in\mathbb{N}$; последовательность значений аргументов фрактальных группоидов $\{(i_s,j_s)\}_{s=1}^p$, $i_s,j_s\in 1..n_{k_s}$, $s\in 1..p$.

2. Вычисляемые значения на стороне A: операция $\phi_\diamond^m$ — m-я степень операции $\diamond$, последовательность значений результатов операции $\{\phi_\star(i_s,j_s)\}_{s=1}^p=\{\phi_{\diamond_{k_s}^\sigma}^m(i_s,j_s)\}_{s=1}^p$. Значения, передаваемые по открытому каналу связи: $\{\phi_\star(i_s,j_s)\}_{s=1}^p$. Секретное значение: m (для диагонального расширения – четное число).

3. Вычисляемые значения на стороне B: операция $\phi_\diamond^{m'}$ — m'-я степень операции $\diamond$, последовательность значений результатов операции $\{\phi_{\star'}(i_s,j_s)\}_{s=1}^p$, где $\phi_{\star'}(i_s,j_s)=\phi_{\diamond_{k_s}^\sigma}^{m'}(i_s,j_s)$. Значения, передаваемые по открытому каналу связи: $\{\phi_{\star'}(i_s,j_s)\}_{s=1}^p$. Секретное значение: m' (для диагонального расширения – четное число).

4. Вычисляемое значение секретного ключа на стороне A: $K=\{\phi_\star(\phi_{\star'}(i_s,j_s),j_s)\}_{s=1}^p$.

5. Вычисляемое значение секретного ключа на стороне B: $K = \{\phi_{\star'}(\phi_\star(i_s, j_s), j_s)\}_{s=1}^{p}$.

6. Значения, известные третьей стороне C: $\langle 1..n, (\diamond)\rangle$, p, $\{(i_s, j_s)\}_{s=1}^{p}$, $\{\phi_\star(i_s, j_s)\}_{s=1}^{p}$, $\{\phi_{\star'}(i_s, j_s)\}_{s=1}^{p}$.

Замечание 2.4.1

В силу замечания 2.1.6, можно считать, что целочисленные интервалы $1..n_{k_s}$ о которых идет речь в п. 1 протокола DHM-FM, являются наименьшими по включению из содержащих заданные значения $i_s, j_s \in 1..n_{k_s}$, т.е. $i_s, j_s \in 1..n_{k_s}$, и $i_s, j_s \notin 1..n_k$ для любого $n_k = 2^k n < n_{k_s} = 2^{k_s} n$.

Для вычисления значений результатов операции $\phi_{\star'}(i_s, j_s) = \phi^{m'}_{\diamond^\sigma_{k_s}}(i_s, j_s)$ в зависимости от типа расширения σ применяется один из алгоритмов 2.1.1–2.1.4.

В качестве примера приведем результаты численного эксперимента реализации протокола DHM-FM.

1. Опубликованные общедоступные значения: базовая матрица Кэли

$$A = \begin{pmatrix}
16 & 7 & 5 & 13 & 4 & 11 & 13 & 3 & 9 & 1 & 1 & 8 & 2 & 9 & 13 & 16 \\
9 & 6 & 16 & 7 & 13 & 13 & 16 & 1 & 6 & 10 & 15 & 8 & 6 & 9 & 12 & 14 \\
13 & 2 & 16 & 5 & 3 & 7 & 12 & 5 & 2 & 13 & 16 & 9 & 1 & 7 & 15 & 9 \\
14 & 14 & 8 & 5 & 5 & 1 & 9 & 9 & 8 & 5 & 11 & 5 & 2 & 7 & 2 & 12 \\
5 & 7 & 16 & 10 & 15 & 10 & 6 & 7 & 15 & 13 & 3 & 3 & 16 & 5 & 7 & 4 \\
8 & 2 & 6 & 3 & 12 & 11 & 6 & 2 & 13 & 10 & 10 & 9 & 9 & 7 & 11 & 13 \\
4 & 5 & 3 & 12 & 6 & 16 & 7 & 9 & 12 & 7 & 2 & 12 & 12 & 10 & 4 & 3 \\
11 & 15 & 9 & 12 & 13 & 4 & 16 & 14 & 8 & 16 & 14 & 2 & 1 & 10 & 7 & 2 \\
11 & 2 & 2 & 8 & 5 & 15 & 13 & 15 & 13 & 2 & 7 & 2 & 7 & 13 & 10 & 4 \\
11 & 5 & 2 & 16 & 8 & 1 & 10 & 2 & 4 & 14 & 6 & 1 & 7 & 10 & 14 & 11 \\
3 & 3 & 9 & 15 & 2 & 3 & 14 & 1 & 2 & 9 & 1 & 6 & 10 & 3 & 7 & 16 \\
9 & 9 & 1 & 9 & 12 & 8 & 9 & 16 & 7 & 7 & 7 & 16 & 8 & 6 & 13 & 4 \\
2 & 7 & 8 & 11 & 9 & 9 & 12 & 13 & 5 & 14 & 1 & 14 & 6 & 3 & 1 & 13 \\
10 & 14 & 3 & 15 & 10 & 15 & 6 & 12 & 7 & 16 & 4 & 12 & 10 & 16 & 16 & 14 \\
2 & 9 & 14 & 9 & 7 & 15 & 15 & 16 & 6 & 11 & 7 & 12 & 9 & 9 & 10 & 12 \\
5 & 15 & 7 & 11 & 7 & 16 & 1 & 6 & 11 & 2 & 4 & 15 & 8 & 10 & 16 & 1
\end{pmatrix},$$

тип расширения d — диагональное, длина последовательности значений аргументов 4, последовательность значений аргументов $\{(53, 6), (3273, 234), (11529, 2149), (434490, 39752)\}$,

2. Секретное значение на стороне A: показатель степени $m = 4$. Вычисляемые значения на стороне A: степень базовой матрицы Кэли

$$A^m = \begin{pmatrix}
5 & 5 & 3 & 9 & 7 & 16 & 13 & 9 & 15 & 1 & 1 & 2 & 7 & 7 & 1 & 1 \\
13 & 2 & 16 & 8 & 15 & 15 & 12 & 7 & 15 & 2 & 15 & 2 & 12 & 7 & 13 & 14 \\
11 & 6 & 16 & 11 & 3 & 16 & 12 & 15 & 5 & 2 & 1 & 2 & 9 & 10 & 16 & 4 \\
3 & 14 & 16 & 11 & 6 & 7 & 9 & 6 & 8 & 16 & 1 & 2 & 7 & 10 & 1 & 4 \\
5 & 5 & 16 & 15 & 12 & 3 & 6 & 16 & 5 & 2 & 11 & 8 & 2 & 5 & 12 & 12 \\
13 & 6 & 6 & 16 & 12 & 16 & 6 & 5 & 6 & 2 & 6 & 2 & 8 & 10 & 2 & 13 \\
11 & 7 & 3 & 12 & 12 & 16 & 7 & 6 & 7 & 7 & 2 & 12 & 2 & 10 & 13 & 12 \\
2 & 6 & 7 & 12 & 15 & 3 & 12 & 6 & 8 & 14 & 1 & 8 & 9 & 10 & 12 & 14 \\
2 & 6 & 3 & 8 & 6 & 15 & 13 & 2 & 6 & 16 & 7 & 8 & 1 & 10 & 16 & 12 \\
2 & 7 & 3 & 9 & 5 & 7 & 10 & 5 & 8 & 10 & 10 & 8 & 1 & 10 & 16 & 16 \\
9 & 2 & 7 & 12 & 5 & 16 & 6 & 7 & 5 & 14 & 1 & 8 & 8 & 10 & 12 & 1 \\
13 & 2 & 7 & 9 & 12 & 11 & 9 & 1 & 12 & 7 & 7 & 16 & 6 & 10 & 1 & 12 \\
3 & 5 & 16 & 8 & 7 & 15 & 12 & 13 & 13 & 10 & 1 & 15 & 12 & 10 & 13 & 13 \\
13 & 14 & 3 & 12 & 9 & 15 & 6 & 2 & 12 & 14 & 1 & 12 & 8 & 10 & 16 & 14 \\
3 & 2 & 7 & 9 & 12 & 15 & 15 & 1 & 15 & 10 & 7 & 12 & 8 & 7 & 16 & 4 \\
5 & 6 & 7 & 8 & 12 & 16 & 9 & 3 & 13 & 16 & 1 & 15 & 6 & 10 & 16 & 16
\end{pmatrix}.$$

Последовательность значений результатов операции, вычисленных при помощи алгоритма 2.1.1 и передаваемых по открытому каналу связи: $\{51, 3120, 9574, 408181\}$.

3. Секретное значение на стороне B: показатель степени $m' = 10$. Вычисляемые значения на стороне B: степень базовой матрицы Кэли

$$A^{m'} = \begin{pmatrix} 5 & 5 & 3 & 9 & 12 & 16 & 13 & 3 & 13 & 1 & 1 & 2 & 9 & 10 & 1 & 1 \\ 2 & 2 & 16 & 8 & 12 & 15 & 12 & 1 & 13 & 14 & 15 & 2 & 7 & 10 & 13 & 14 \\ 3 & 6 & 16 & 8 & 3 & 16 & 12 & 5 & 6 & 14 & 1 & 2 & 6 & 10 & 16 & 4 \\ 13 & 14 & 16 & 8 & 12 & 16 & 9 & 9 & 8 & 10 & 1 & 2 & 9 & 10 & 1 & 4 \\ 5 & 5 & 16 & 12 & 12 & 16 & 6 & 7 & 6 & 14 & 1 & 8 & 1 & 5 & 1 & 12 \\ 2 & 6 & 6 & 9 & 12 & 16 & 6 & 2 & 5 & 14 & 6 & 2 & 12 & 10 & 13 & 13 \\ 3 & 7 & 3 & 12 & 12 & 16 & 7 & 9 & 7 & 7 & 2 & 12 & 1 & 10 & 13 & 12 \\ 9 & 6 & 7 & 12 & 12 & 16 & 12 & 9 & 8 & 2 & 1 & 8 & 6 & 10 & 1 & 14 \\ 9 & 6 & 3 & 8 & 12 & 15 & 13 & 15 & 5 & 10 & 7 & 8 & 8 & 10 & 16 & 12 \\ 9 & 7 & 3 & 9 & 12 & 16 & 10 & 2 & 8 & 16 & 10 & 8 & 8 & 10 & 16 & 16 \\ 11 & 2 & 7 & 12 & 12 & 16 & 6 & 1 & 6 & 2 & 1 & 8 & 12 & 10 & 1 & 1 \\ 2 & 2 & 7 & 9 & 12 & 16 & 9 & 16 & 12 & 7 & 7 & 16 & 2 & 10 & 1 & 12 \\ 13 & 5 & 16 & 8 & 12 & 15 & 12 & 13 & 15 & 16 & 1 & 15 & 7 & 10 & 13 & 13 \\ 2 & 14 & 3 & 12 & 12 & 15 & 6 & 15 & 12 & 2 & 1 & 12 & 12 & 10 & 16 & 14 \\ 13 & 2 & 7 & 9 & 12 & 15 & 15 & 16 & 13 & 16 & 7 & 12 & 12 & 10 & 16 & 4 \\ 5 & 6 & 7 & 8 & 12 & 16 & 9 & 6 & 15 & 10 & 1 & 15 & 2 & 10 & 16 & 16 \end{pmatrix}.$$

Последовательность значений результатов операции, вычисленных при помощи алгоритма 2.1.1 и передаваемых по открытому каналу связи: $\{64, 3114, 9580, 408178\}$.

4. Вычисляемое при помощи алгоритма 2.1.1 значение секретного ключа на стороне A: $\{64, 3274, 11532, 434487\}$.

5. Вычисляемое при помощи алгоритма 2.1.1 значение секретного ключа на стороне B: $\{64, 3274, 11532, 434487\}$.

Выводы

В статье определены понятия фрактальных расширений конечных группоидов $M = \langle U, (*)\rangle$, а также связанные с ними понятия типов и шкал расширений. Конечный группоид полностью описывается своей таблицей Кэли, поэтому группоиды и таблицы Кэли их операций естественным образом отождествляются. Фрактальное расширение позволяет удваивать мощность носителя исходного (базового) группоида, определяя новую бинарную операцию путем «клонирования» базовой таблицы Кэли. При этом каждый группоид является подгруппоидом своего расширения. Для представления группоидов использовались целочисленные диапазоны $1..n$ и матрицы Кэли $A = (a_{i,j})$ с элементами $a_{i,j} \in 1..n$. Система последовательных расширений некоторого «базового» группоида $M = \langle 1..n, (\diamond)\rangle$ с матрицей $A = (a_{i,j})$ образует шкалу фрактальных расширений $S_\sigma = \{M_k^{(\sigma)}\}_{k=0}^{\infty}$ с фрактальными матрицами $A_k = ({}^k a_{i,j})$. Самоподобная структура матриц Кэли A_k позволяет сформулировать простые алгоритмы для вычисления результатов операций во фрактальных шкалах исключительно на основании базовой матрицы Кэли. Таким образом, несмотря на то что мощность носителей группоидов фрактальной шкалы возрастает экспоненциально как $2^k n$, для нахождения результатов их операций достаточно оперировать с элементами базовой матрицы порядка n, а не фрактальных матриц порядка $2^k n$. При этом сложность алгоритмов вычисления результатов оценивается как $O(k)$ целочисленных арифметических операций. Тем самым обеспечивается существенная экономия вычислительных ресурсов при расчетах.

Примечательным является тот факт, что фрактальные расширения сохраняют свойства фрактальности относительно композиции своих операций. Ранее было установлено [5], что композиция бинарных операций группоидов с общим носителем обладает свойством ассоциативности, что позволило использовать ее для модификации протокола протокола Диффи — Хелмана — Меркла открытого распределения ключей шифрования. Однако в случае произвольных группоидов данная модификация предъявляла весьма высокие требования к вычислительным ресурсам и памяти для своей реализации. Шкалы фрактальных группоидов позволяют снизить требуемые объемы вычислений до приемлемого уровня.

Все определяемые в статье понятия сопровождаются подробными примерами, также приведен пример результатов численного эксперимента по выработке общего ключа шифрования в асимметричной схеме с двумя участниками.

Литература

[1] Мальцев А.И. Алгебраические системы. Москва: Физматлит, 1970. 392 с. URL: http://inis.jinr.ru/sl/vol1/UH/_Ready/Mathematics/Mathematical%20logic/Mal'cev.%20Algebraicheskie%20sistemy%20(Nauka,%201970)%20(ru)(L)(197s).pdf.

[2] Глухов М.М. О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2 (2). С. 28–32. URL: http://www.mathnet.ru/links/5f23e5e82dc9870afaea3fef5dfd757a/pdm29.pdf; https://www.elibrary.ru/item.asp?id=12049756.

[3] Diffie W., Hellman M.E. New Directions in Cryptography // IEEE Transactions on Information Theory. 1976. V. IT-22. P. 644–654. DOI: http://doi.org/10.1109/TIT.1976.1055638.

[4] Merkle R.C. Secure Communications over Insecure Channels // Communications of the ACM. 1978. V. 21. No 4. P. 294–299.

[5] Цветов В.П. Полугруппы бинарых операций и криптосистемы на группоидах // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26. № 1. С. 23–51. DOI: http://doi.org/10.18287/2541-7525-2020-26-1-23-51.

[6] Graham R.L., Knuth D.E., Patashnik O. Concrete mathematics — A foundation for computer science. Advanced Book Program. Addison-Wesley, 1989. 625 p. URL: https://notendur.hi.is/pgg/(ebook-pdf)%20-%20Mathematics%20-%20Concrete%20Mathematics.pdf.

Scientific article

DOI: 10.18287/2541-7525-2020-26-2-23-49

Submited: 16.01.2020
Revised: 30.01.2020
Accepted: 25.05.2020

V.P. Tsvetov
Samara National Research University, Samara, Russian Federation
E-mail: tsf-su@mail.ru. ORCID: https://orcid.org/0000-0001-6744-224X

FRACTAL MAGMAS AND PUBLIC-KEY CRYPTOGRAPHY

ABSTRACT

In this paper, we deal with magmas – the simplest algebras with a single binary operation. The main result of our research is algorithms for generating chain of finite magmas based on the self-similarity principle of its Cayley tables. In this way the cardinality of a magma's domain is twice as large as the previous one for each magma in the chain, and its Cayley table has a block-like structure. As an example, we consider a cyclic semigroup of binary operations generated by a finite magma's operation with a low-cardinality domain, and a modify the Diffie-Hellman-Merkle key exchange protocol for this case.

Key words: magmas, semigroups, Cayley tables, cyclic semigroup of binary operations, magma-based cryptography, Diffie-Hellman-Merkle key exchange.

Citation. Tsvetov V.P. Fractal magmas and publec-key cryptography. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 2, pp. 23–49. DOI: http://doi.org/10.18287/2541-7525-2020-26-2-23-49. (In Russ.)

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

Information about the author: © *Tsvetov Victor Petrovich* — Candidate of Physical and Mathematical Sciences, assistant professor of the Department of Information Security, Samara National Research University, 34, Moskovskoye shosse, 443086, Russian Federation.

References

[1] Mal'cev A.I. Algebraic systems. Moscow: Fizmatlit, 1970, 392 p. Available at: http://inis.jinr.ru/sl/vol1/UH/_Ready/Mathematics/Mathematical%20logic/Mal'cev.%20Algebraicheskie%20sistemy%20(Nauka,%201970)%20(ru)(L)(197s).pdf. (In Russ.)

[2] Glukhov M.M. Some applications of quasigroups in cryptography. *Applied Discrete Mathematics*, 2008, no. 2 (2), pp. 28–32. Available at: http://www.mathnet.ru/links/5f23e5e82dc9870afaea3fef5dfd757a/pdm29.pdf; https://www.elibrary.ru/item.asp?id=12049756. (In Russ.)

[3] Diffie W., Hellman M.E. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 1976, V. IT-22, pp. 644–654. DOI: http://doi.org/10.1109/TIT.1976.1055638.

[4] Merkle R.C. Secure Communications over Insecure Channels. *Communications of the ACM*, 1978, vol. 21, no. 4, pp. 294–299. DOI: http://doi.org/10.1145/359460.359473.

[5] Tsvetov V.P. Semigroups of binary operations and magma-based cryptography. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 1, pp. 23–51. Available at: http://doi.org/10.18287/2541-7525-2020-26-1-23-51. (In Russ.)

[6] Graham R.L., Knuth D.E., Patashnik O. Concrete mathematics — A foundation for computer science. Advanced Book Program. Addison-Wesley, 1989, 625 p. Available at: https://notendur.hi.is/pgg/(ebook-pdf)%20-%20Mathematics %20-%20Concrete%20Mathematics.pdf.