

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра геометрии

Тождество алгебр отношений с конъюнктивными операциями

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 227 группы

направления 02.04.01 Математика и компьютерные науки

механико-математического факультета

МАМЕДОВА БАХРУЗА ЭЛЬСЕВАН ОГЛЫ

Научный руководитель

Профессор, д.ф.-м.н., профессор

подпись, дата

Д.А. Бредихин

Зав. кафедрой

Д.ф.-м.н., доцент

подпись, дата

В.Б. Поплавский

Саратов 2025

Введение. Алгебры отношений могут быть классифицированы по виду формул, задающих их операции. Среди операций над отношениями особую роль играют логические операции, которые могут быть заданы с помощью формул исчисления предикатов 1-го порядка. Позитивные формулы задают так называемые позитивные операции. К числу последних относятся широко известные операции пересечения $\cap$, объединения $\cup$, произведения $\circ$ и обращения $^{-1}$ бинарных отношений. Важными классами логических операций являются классы примитивно-позитивных и конъюнктивных операций. Операция называется примитивно-позитивной, если она может быть задана с помощью формулы, которая в своей предваренной нормальной форме содержит лишь операцию конъюнкции и кванторы существования. Если формула содержит только операцию конъюнкции, то она называется конъюнктивной.

Теория группоидов находит применение в криптографии, особенно в областях, связанных с неассоциативными алгебраическими структурами и постквантовыми алгоритмами. Группоид — это множество с бинарной операцией, которая не обязательно обладает какими-либо дополнительными свойствами (ассоциативностью, коммутативностью или наличием нейтрального элемента). Эта гибкость позволяет конструировать криптографические протоколы, устойчивые к атакам с использованием классических и квантовых алгоритмов.

Данная бакалаврская работа разделена на три раздела.

Первый раздел посвящен базовым определениям и обозначениям, связанными с алгеброй отношений с примитивно-позитивными и конъюнктивными операциями. Второй раздел несёт реферативный характер. Вводится понятие примитивно-позитивной операции над отношениями. Рассматривается представление диофантовых операций с помощью графов. Излагаются, полученные в статье Д.А. Бредихина «Эквациональная теория алгебр отношений с позитивными операциями», результаты. В этом разделе используется аппарат теории графов, находится эффективное описание эквациональных теорий алгебр отношений с позитивными операциями. Третий раздел посвящен классификации конъюнктивных операций пятого ранга. Проверяются ключевые тождества и квазитождества для конъюнктивных операций, используя представление двухполюсных графов в виде матриц.

Цель данной работы заключается в классификации конъюнктивных операций ранга 5 и осуществление проверки тождеств и квазитожеств на алгебрах отношений с конъюнктивными операциями, что, в свою очередь, может быть использовано в сфере защиты информации.

Основное содержание работы. Операции над отношениями, задаваемые с помощью диофантовых формул, будем называть диофантовыми (примитивно-позитивными).

Алгебру отношений назовем диофантовой (примитивно-позитивной), если таковыми являются все ее операции. Нетрудно заметить, что отношение теоретико-множественного включения $\subset$ стабильно относительно диофантовых операций и, следовательно, всякая диофантова алгебра отношений (Φ, Ω) может быть рассмотрена как упорядоченная отношением включения $\subset$.

Удобным способом описания диофантовых операций над отношениями является представление их с помощью графов.

Обозначим через $\mathbb{N}$ множество всех натуральных чисел.

Определение 2.1.3. Помеченным ориентированным графом называется пара $G = (V, E)$, где $V = V(G)$ — множество, называемое множеством вершин, $E = E(G) \subset V \times \mathbb{N} \times V$ — тернарное отношение.

Тройку $(u, k, v) \in E$ будем называть ребром с меткой k , соединяющим вершину u с вершиной v , и графически изображать следующим образом:

$$u \cdot \xrightarrow{k} \cdot v$$

Множество $Lab(G) = \{k : (\exists u, v)(u, k, v) \in E\}$ назовем множеством меток графа G . Граф называется конечным, если множество его вершин и ребер являются конечным.

Будем говорить, что граф G' является подграфом графа G и писать $G' \subset G$ если, $V(G') \subset V(G)$, $E(G') \subset E(G)$. Граф $(V', E|V')$, где $E|V' = E \cap V' \times W \times V'$ назовем полным подграфом графа (V, E) на подмножестве $V' \subset V$.

Определение 2.1.4. Двухполюсником называется помеченный граф с парой выделенных вершин, т.е. систему вида $G = (V, E, in, out)$, где (V, E) — помеченный граф; in, out — две выделенные вершины (не обязательно различные), называемые входом и выходом двухполюсника соответственно.

Понятие изоморфизма помеченных графов и двухполюсников определяется естественным образом. В дальнейшем все графы будут рассматриваться с точностью до изоморфизма.

Пусть $F = F_\phi$ — диофантова операция, задаваемая формулой ϕ . С этой операцией может быть ассоциирован двухполюсник $G = G(\phi)$, определяемый следующим образом: $G = (V, E, in, out)$, где V — множество всех индексов индивидуальных переменных, входящих в формулу ϕ ; $in = 0$, $out = 1$; $(i, k, j) \in E$ тогда и только тогда, когда атомарная формула $r_k(z_i, z_j)$ входит в ϕ ; если формула $z_i = z_j$ входит в ϕ , то вершины i и j отождествляются.

Аналогично и обратное действие: всякому двухполюснику соответствует формула определяющая примитивно-позитивную операцию, которая строится следующим образом: $G = (V, E, in, out)$. Всякой вершине из V сопоставляется индуцированная логическая переменная, причем $in = z_0$, $out = z_1$. Формула начинается с кванторов существования по всем этим переменным, за исключением z_0, z_1 . Далее следует конъюнкция атомарных формул $r_k(z_i, z_j)((z_i, z_j) \in \rho_k)$ для всех дуг $(v_i, k, v_j) \in E$.

Мы говорим, что примитивно-позитивная операция F имеет ранг k , если она может быть определена формулой, содержащей k конъюнктивных элементов, и не может быть определена формулами с меньшим их числом.

Двухполюсник, соответствующий бинарной конъюнктивной операции F , можно представить как сумму 2 подграфов: $G(F) = G_1(F) + G_2(F)$, которые содержат ребра, помеченные 1 и 2 соответственно. Число ребер в первом графе $G_1(F)$ равна k_1 , а во втором графе $G_2(F)$ равна k_2 . Ясно, что $k = k_1 + k_2$. Каждому такому графу может быть сопоставлена булева матрица с размером 2×2 .

Определение 3.1.1. Операция $F^d(\rho_1, \rho_2) = F(\rho_1, \rho_2)$ называется двойственной по отношению к операции F .

Определение 3.1.2. Операция $F^c(\rho_1, \rho_2) = (F(\rho_2^{-1}, \rho_1^{-1}))^{-1}$, где $^{-1}$ — операция обратного отношения, называемая дуальной по отношению к операции F .

Определение 3.1.3. Операция $F^f(\rho_1, \rho_2) = (F(\rho_1^{-1}, \rho_2^{-1}))^{-1}$ называется инвертированной к операцией F .

Заметим, что $F^f = F^{cd} = F^{dc}$ является двойственной к дуальной и дуальная к двойственной.

При классификации конъюнктивных операций мы их будем объединять в непересекающиеся классы, состоящие из двухполюсников, располагая их в матрицы следующего вида:

F	F^d
F^c	F^f

Видим, что каждый класс наряду с рассматриваемой операцией также будет содержать двойственную, дуальную к двойственной и двойственную к дуальной. Опишем двухполюсники, содержащие m рёбер, при условии что $1 \leq m \leq 4$.

При $m = 1$ граф может иметь следующий вид:

$$A_1) u \cdot \longrightarrow \cdot v, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$A_2) u \cdot \longleftarrow \cdot v, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$A_3) \begin{array}{c} \text{---} \\ \cup \\ u \cdot \end{array} \cdot v, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$A_3^*) u \cdot \begin{array}{c} \cup \\ \text{---} \end{array} \cdot v, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

При $m = 2$ граф может иметь следующий вид:

$$B_1) \begin{array}{c} \text{---} \\ \curvearrowright \\ u \cdot \end{array} \begin{array}{c} \curvearrowleft \\ \text{---} \\ \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$B_2) \begin{array}{c} \text{---} \\ \cup \\ u \cdot \end{array} \begin{array}{c} \text{---} \\ \cup \\ \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$B_3) \begin{array}{c} \text{---} \\ \cup \\ u \cdot \end{array} \longrightarrow \cdot v, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$$B_3^*) u \cdot \longrightarrow \begin{array}{c} \text{---} \\ \cup \\ \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$B_4) \quad \begin{array}{c} \text{---} \circ \text{---} \\ | \\ u \cdot \longleftarrow \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

$$B_4^*) \quad \begin{array}{c} \text{---} \circ \text{---} \\ | \\ u \cdot \longleftarrow \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

При $m = 3$ граф может иметь следующий вид:

$$C_1) \quad \begin{array}{c} \text{---} \circ \text{---} \quad \text{---} \circ \text{---} \\ | \quad \quad | \\ u \cdot \longrightarrow \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$C_2) \quad \begin{array}{c} \text{---} \circ \text{---} \quad \text{---} \circ \text{---} \\ | \quad \quad | \\ u \cdot \longleftarrow \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$C_3) \quad \begin{array}{c} \text{---} \circ \text{---} \quad \text{---} \circ \text{---} \\ | \quad \quad | \\ u \cdot \quad \quad \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$C_3^*) \quad \begin{array}{c} \text{---} \circ \text{---} \quad \text{---} \circ \text{---} \\ | \quad \quad | \\ u \cdot \quad \quad \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

При $m = 4$ граф может иметь следующий вид:

$$D_1) \quad \begin{array}{c} \text{---} \circ \text{---} \quad \text{---} \circ \text{---} \\ | \quad \quad | \\ u \cdot \quad \quad \cdot v \end{array}, \text{ его представление в виде бинарной матрицы: } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

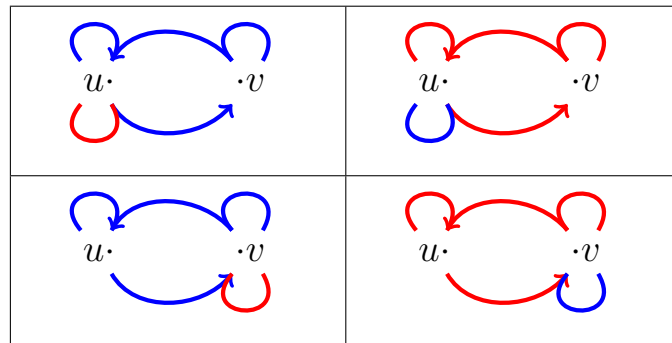
Теперь приведем конъюнктивные операции ранга 5. Мы ранее отмечали, что двухполюсник может быть представлен как сумма 2 подграфов. Ранг 5 может получиться комбинацией графа ранга 1 с графом рангом 4, а также графа ранга 2 с графом рангом 3. Также с комбинацией графов ранга 4 с графом рангом 1 и графа ранга 2 с графом рангом 3, но из-за свойства двойственности мы их опускаем.

Количество операций в каждом классе зависит от того, являются ли операции сопряженными и обратными. Некоторые операции не имеют сопряженных и обратных, поэтому в классах может быть присутствовать 1, 2, 3 или 4 операций.

Приведем пару классов, с соответствующим количеством операций в каждом классе. Отметим, что для исключения ошибок в каждом классе первый граф будет представлен красным цветом, а второй граф будет представлен синим цветом.

1)

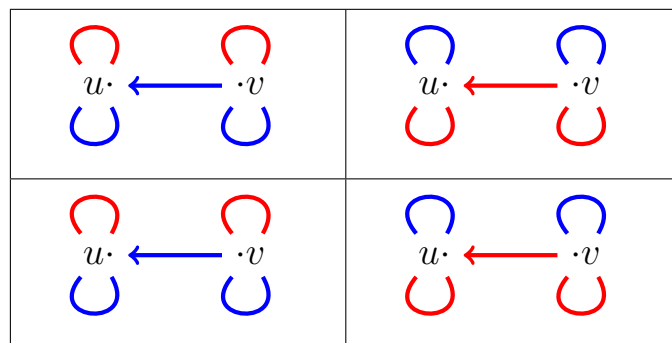
$A_3 + D_1$	$D_1 + A_3$
$A_3^* + D_1$	$D_1 + A_3^*$



Количество операций: 4

2)

$B_2 + C_2$	$C_2 + B_2$
$B_2 + C_2$	$C_2 + B_2$



Количество операций: 2

Получим в итоге 56 операций, из которых удалось выделить 17 различных классов.

Теперь для каждого элемента из каждого класса произведём проверку некоторый ряд тождеств и квазитожеств. Для этого необходимо построить группоид бинарных отношений на двухэлементном множестве. Этот группоид имеет важное значение, так как любое тождество, которое справедливо в

данном группоиде, будет справедливо и в любом другом группоиде, использующем бинарные операции для бинарных отношений.

Приведём список соответствующих тождеств и квазитожеств, которые необходимо проверить:

1. $(xy)z = x(yz)$ - ассоциативность.
2. $x^2y = xy$ - псевдо-идемпотентность слева.
3. $xy^2 = xy$ - псевдо-идемпотентность справа.
4. $(xy)z = (yx)z$ - псевдо-коммутативность слева.
5. $x(yz) = x(zx)$ - псевдо-коммутативность справа.
6. $((xy)z)w = (x(yz))w$ - псевдо-ассоциативность слева.
7. $x((yz)w) = x(y(zw))$ - псевдо-ассоциативность справа.
8. $xy = yx$ - коммутативность.
9. $x^2y^2 = y^2x^2$ - коммутативность квадратов.
10. $xy \leq x$;
11. $xy \leq y$;
12. $x \leq yz \implies x \leq xz$;
13. $x \leq yz \implies x \leq yx$;
14. $(x \leq yz \wedge x \leq uw) \implies x \leq yw$.

Результаты проверки будут представлены в виде таблицы (Таблица 3.1). Отметим, что в таблице 3.1 тождества будут обозначены в соответствии со своими нумерациями, приведенными ранее в виде списка.

Для выполнения расчетов используется программа на языке Python. В качестве входных данных программа принимает две матрицы, которые представляют ту или иную операцию. Далее строится таблица Кэли для нашего группоида $(A, \cdot)$. Построенная таблица Кэли используется в дальнейшей части работы для проверки тождеств и квазитожеств.

Класс	Элемент	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	$A_1 + D_1$	+	-	+	-	+	+	+	-	+	+	+	-	-	-
1	$D_1 + A_1$	+	+	-	+	-	+	+	-	+	+	+	-	-	-
2	$A_2 + D_1$	-	-	+	-	+	-	+	-	+	-	+	-	-	-

2	$D_1 + A_2$	-	+	-	+	-	+	-	-	+	+	-	-	-	-
3	$A_3 + D_1$	-	+	+	+	-	+	+	-	-	-	+	-	-	-
3	$D_1 + A_3$	-	+	+	-	-	+	+	-	-	+	-	-	-	-
3	$A_3^* + D_1$	-	+	+	+	-	+	+	-	-	-	+	-	-	-
3	$D_1 + A_3^*$	-	+	+	-	-	+	+	-	-	+	-	-	-	-
4	$B_1 + C_1$	+	-	-	-	-	+	+	-	+	-	-	-	-	-
4	$C_1 + B_1$	+	-	-	-	-	+	+	-	+	-	-	-	-	-
5	$B_2 + C_1$	+	+	+	+	-	+	+	-	-	-	+	-	-	-
5	$C_1 + B_2$	+	+	+	-	+	+	+	-	-	+	-	-	-	-
6	$B_3 + C_1$	+	-	+	-	+	+	+	-	+	-	-	-	-	-
6	$C_1 + B_3$	+	+	-	+	-	+	+	-	+	-	-	-	-	-
6	$B_3^* + C_1$	+	-	+	-	+	+	+	-	+	-	-	-	-	-
6	$C_1 + B_3^*$	+	+	-	+	-	+	+	-	+	-	-	-	-	-
7	$B_4 + C_1$	-	-	-	-	-	-	-	-	+	-	+	-	-	-
7	$C_1 + B_4$	-	-	-	-	-	-	-	-	+	+	-	-	-	-
7	$B_4^* + C_1$	-	-	-	-	-	-	-	-	+	-	+	-	-	-
7	$C_1 + B_4^*$	-	-	-	-	-	-	-	-	+	+	-	-	-	-
8	$B_1 + C_2$	-	-	-	-	-	+	-	-	+	+	-	-	-	-
8	$C_2 + B_1$	-	-	-	-	-	-	+	-	+	-	+	-	-	-
9	$B_2 + C_2$	-	+	-	+	-	+	-	-	-	+	+	-	-	-
9	$C_2 + B_2$	-	-	+	-	-	-	+	-	-	+	+	-	-	-
10	$B_3 + C_2$	-	-	-	-	+	-	-	-	+	+	-	-	-	-
10	$C_2 + B_3$	-	-	-	-	-	-	-	-	+	-	+	-	-	-
10	$B_3^* + C_2$	-	-	-	-	+	-	-	-	+	+	-	-	-	-
10	$C_2 + B_3^*$	-	-	-	-	-	-	-	-	+	-	+	-	-	-
11	$B_4 + C_2$	-	-	-	+	-	-	-	-	+	+	+	-	-	-
11	$C_2 + B_4$	-	-	-	+	-	-	-	-	+	+	+	-	-	-
11	$B_4^* + C_2$	-	-	-	+	-	-	-	-	+	+	+	-	-	-
11	$C_2 + B_4^*$	-	-	-	+	-	-	-	-	+	+	+	-	-	-
12	$B_1 + C_3$	-	-	-	-	-	+	+	-	+	-	-	-	-	-
12	$C_3 + B_1$	-	-	-	-	-	+	+	-	+	-	-	-	-	-

12	$B_1 + C_3^*$	—	—	—	—	—	+	+	—	+	—	—	—	—	—
12	$C_3^* + B_1$	—	—	—	—	—	+	+	—	+	—	—	—	—	—
13	$B_2 + C_3$	—	—	—	—	—	—	+	—	—	—	+	—	—	—
13	$C_3 + B_2$	—	—	—	+	—	+	—	—	—	+	—	—	—	—
13	$B_2 + C_3^*$	—	—	—	—	—	—	+	—	—	—	+	—	—	—
13	$C_3^* + B_2$	—	—	—	+	—	+	—	—	—	+	—	—	—	—
14	$B_3 + C_3$	—	—	—	—	+	—	+	—	—	—	—	—	—	—
14	$C_3 + B_3$	—	—	—	+	—	+	—	—	—	—	—	—	—	—
14	$B_3 + C_3^*$	—	—	—	—	+	—	+	—	—	—	—	—	—	—
14	$C_3^* + B_3$	—	—	—	+	—	+	—	—	—	—	—	—	—	—
15	$B_4 + C_3$	—	—	—	—	+	+	+	—	+	—	+	—	—	—
15	$C_3 + B_4$	—	—	—	+	—	+	+	—	+	+	—	—	—	—
15	$B_4^* + C_3^*$	—	—	—	—	+	+	+	—	+	—	+	—	—	—
15	$C_3^* + B_4^*$	—	—	—	+	—	+	+	—	+	+	—	—	—	—
16	$B_3^* + C_3$	—	—	—	—	—	—	+	—	+	—	+	—	—	—
16	$C_3 + B_3^*$	—	—	—	—	—	+	—	—	—	+	—	—	—	—
16	$B_3 + C_3^*$	—	—	—	—	—	—	+	—	+	—	—	—	—	—
16	$C_3^* + B_3$	—	—	—	—	—	+	—	—	+	—	—	—	—	—
17	$B_4^* + C_3$	—	—	—	—	—	—	+	—	+	—	+	—	—	—
17	$C_3 + B_4^*$	—	—	—	+	—	+	—	—	+	+	—	—	—	—
17	$B_4 + C_3^*$	—	—	—	—	—	—	+	—	+	—	+	—	—	—
17	$C_3^* + B_4$	—	—	—	+	—	+	—	—	+	+	—	—	—	—

Таблица 3.1 — Проверка тождеств

Ни одна из проверенных операций не удовлетворяет тождеству коммутативности и всем данным квазитождествам.

Заключение. Особый интерес представляет выявленная неоднородность свойств операций, что указывает на необходимость тщательного подхода при их использовании в алгебраических системах. Например, некоторые операции, несмотря на отсутствие стандартных свойств, могут оказаться полезными в специализированных областях, таких как теория графов, криптография или машинное обучение. Эти результаты не только вносят вклад в развитие

абстрактной алгебры, но и предоставляют ценные ориентиры для прикладных исследований, помогая выбирать оптимальные операции для решения конкретных математических и инженерных задач.

Таким образом, работа расширяет понимание структурных ограничений и возможностей алгебр отношений, предлагая новые направления для дальнейших теоретических и практических изысканий.