МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра Геометрии

Свойства операций над бинарными отношениями

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 227 группы
направления 02.04.01 – Математика и компьютерные науки

механико-математического факультета

Приходько Софии Владиславовны

Научный руководитель
Профессор, д.ф.-м.н., профессор Д.А.Бредихин

Зав. кафедрой
д.ф.-м.н., доцент В.Б.Поплавский

Саратов 2026

Введение. Актуальность темы. Алгебры отношений представляют собой важный раздел универсальной алгебры, находящий применение в теории баз данных, логическом программировании и криптографии. Особый интерес вызывают примитивно-позитивные (диофантовы) и конъюнктивные операции, задаваемые формулами исчисления предикатов. Несмотря на длительную историю изучения алгебр отношений, многие вопросы, связанные с эквациональными теориями классов алгебр с такими операциями, остаются открытыми.

В частности, отсутствует полная классификация бинарных конъюнктивных операций и систематическое исследование выполнимости алгебраических тождеств на соответствующих классах. Решение этих задач необходимо как для развития самой теории универсальных алгебр, так и для практических приложений, например, для обобщения алгоритма Диффи-Хеллмана на неассоциативные структуры в криптографии.

Цель работы заключается в исследовании эквациональных теорий алгебр отношений с логическими операциями и классификации бинарных конъюнктивных операций ранга 6.

Для достижения цели поставлены следующие **задачи**:

1. Изучить основные понятия теории универсальных алгебр, бинарных отношений и алгебр отношений.
2. Исследовать критерий выполнимости тождеств на классах алгебр отношений с примитивно-позитивными операциями и обосновать разрешимость соответствующих эквациональных теорий.
3. Классифицировать все бинарные конъюнктивные операции ранга 6 с точностью до двойственности, сопряжения и инвертирования, а также проверить тождества на алгебрах отношений.
4. Разработать программу для численного исследования тождеств.

Материалы исследования базируются на методах универсальной алгебры (теория многообразий, клоны операций), алгебраической логики (исчисление предикатов первого порядка, примитивно-позитивные формулы) и элементах теории графов (ориентированные помеченные графы, двухполюсники, гомоморфизмы). Основой послужили результаты Д.А. Бредихина.

Структура работы состоит из введения, четырёх глав, заключения и списка литературы. В первой главе вводятся основные определения и вспомогательные сведения. Вторая глава, носящая реферативный характер, посвящена описанию эквациональных теорий алгебр отношений с примитивно-позитивными операциями. Третья глава содержит классификацию конъюнктивных операций ранга 6 и результаты проверки основных тождеств. Четвёртая глава (практическая часть) описывает программную реализацию алгоритма.

Научная новизна. В работе проведена полная классификация бинарных конъюнктивных операций ранга 6, выделены 11 классов эквивалентности. Для каждого класса установлены свойства ассоциативности, коммутативности, псевдо-идемпотентности (левой и правой), псевдо-коммутативности (левой и правой), псевдо-ассоциативности (левой и правой) и коммутативности квадратов. Разработан программный комплекс на языке *Python* для автоматической проверки основных алгебраических тождеств на группоидах отношений.

Научная значимость. Результаты углубляют понимание структуры группоидов отношений и их эквациональных теорий. Классификация конъюнктивных операций может быть использована при построении новых криптографических протоколов на неассоциативных группоидах.

Положения, выносимые на защиту:

1. Критерий выполнимости тождества $p = q$ (или $p \leqslant q$) на классе алгебр отношений с примитивно-позитивными операциями: тождество принадлежит эквациональной теории тогда и только тогда, когда существуют гомоморфизмы между соответствующими двухполюсниками.
2. Классификация всех бинарных конъюнктивных операций ранга 6: всего существует 11 классов эквивалентности относительно преобразований двойственности, обращения и сопряжения.
3. Результаты проверки девяти алгебраических тождеств для каждого из 11 классов группоидов.
4. Программная реализация на *Python*, позволяющая строить таблицу Кэли группоида по заданным битовым маскам операций и проверять выполнение тождеств.

Основное содержание работы. В **введении** объясняется значимость выбранной темы, формулируется цель работы и решаемые задачи.

В **первой части** вводятся необходимые обозначения из математической логики и теории множеств. Формально определяются бинарные отношения, операции над ними (умножение $\circ$, обращение $^{-1}$, пересечение $\cap$, объединение $\cup$). Приводятся классические свойства бинарных отношений:

Пусть $R \subset X \times X$.

1. R – рефлексивно, если $(x, x) \in R \; \forall x$ (граф рефлексивен, если у каждой точки есть дуга);
2. R – симметрично, если $(x, y) \in R \Rightarrow (y, x) \in R$;
3. R – транзитивно, если $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$;
4. R – антисимметрично, если $(x, y), (y, x) \in R \Rightarrow x = y$;
5. R – отношение эквивалентности, если оно рефлексивно, симметрично и транзитивно;
6. R – отношение порядка, если оно рефлексивно, транзитивно и антисимметрично.

Вводится понятие универсальной алгебры, группоида и, в частности, алгебры отношений. Отдельное внимание уделяется логическим операциям.

Определение 1. *Операция над отношениями называется диофантовой (в другой терминологии примитивно-позитивной, обобщенной композицией), если она может быть задана с помощью формулы, которая в своей префиксной нормальной форме содержит только лишь операции конъюнкции и кванторы существования.*

Частным случаем примитивно-позитивных операций являются операции, определяемые формулами без кванторов. Эти операции, естественно, называются конъюнктивными. Обратим внимание, что для случая унарных отношений (подмножеств) единственной бинарной конъюнктивной операцией является пересечение.

Далее излагаются основы алгебры термов и теории многообразий, формулируется теорема Биркгофа о структурной характеристике многообразий.

Теорема 1 (Биркгофа). *Непустой класс алгебр R сигнатуры Ω тогда и только тогда является многообразием, когда R замкнут относительно подалгебр, фактор-алгебр и декартовых произведений, т.е. класс R вместе с* *каждой алгеброй содержит любую ее подалгебру, фактор-алгебру, а также вместе с любым семейством алгебр содержит их декартово произведение.*

Вторая часть носит реферативный характер и основана на работе Д.А. Бредихина. Центральным является понятие двухполюсника.

Определение 2. *Двухполюсником называется помеченный граф с парой выделенных вершин, т.е. система 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.*

Теперь, когда у нас есть определение двухполюсника и диофантовой операции, перейдем к рассмотрению операций o, $^{-1}$, $\cap$ в графическом виде. Каждой диофантовой операции и каждому терму ставится в соответствие двухполюсник.

Операция произведения (композиции) отношений $\rho_1 \circ \rho_2 = \{(x_0, x_1) \mid \exists x_2 : (x_0, x_2) \in \rho_1 \wedge (x_2, x_1) \in \rho_2\}$ ставит в соответствие следующий двухполюсник:

$$in \bullet \xrightarrow{1} \bullet \xrightarrow{2} \bullet\ out$$

Эту операцию можно интерпретировать как склеивание конца графа операции ρ_1 с началом графа операции ρ_2, т.е. $out_{\rho_1} = in_{\rho_2}$.

Операция обращения $\rho^{-1} = \{(x_0, x_1) \mid (x_1, x_0) \in \rho\}$ ставит в соответствие следующий двухполюсник:

$$in \bullet \xleftarrow{1} \bullet\ out$$

Эту операцию можно интерпретировать как разворот графа операции ρ. Операция пересечения $\rho_1 \cap \rho_2 = \{(x_0, x_1) \mid (x_0, x_1) \in \rho_1 \wedge (x_0, x_1) \in \rho_2\}$ ставит в соответствие следующий двухполюсник:

$$\begin{tikzcd} in \bullet \arrow[r, bend left, "1"] \arrow[r, bend right, "2"'] & \bullet\ out \end{tikzcd}$$

После выполнения данной операции мы получаем множество помеченных графов из in в out с разными метками.

Далее вводится понятие гомоморфизма двухполюсников:

Определение 3. *Пусть* $G_1 = (V_1, E_1\,,\ in\ _1,\ out\ _1)$ *и* $G_2 = (V_2, E_2\,,\ in\ _2,$ $out\ _2)$ *– двухполюсники. Отображение* $f : V_2 \to V_1$ *называется гомоморфизмом* G_2 *в* G_1*, если* $f(\ in\ _2) = in\ _1, f(\ out\ _2) = out\ _1 (f(u), k, f(v)) \in E_1$ *для всякой тройки* $(u, k, v) \in E2$*.*

Доказывается основная теорема:

Теорема 2. *Пусть* Ω *– множество примитивно-позитивных операций. Тождество* $p = q$ *(соответственно* $p \leqslant q$*) принадлежит эквациональной теории* $E_q\{\Omega\}$ *(соответственно* $E_q\{\Omega, \subset\}$*) тогда и только тогда, когда существуют гомоморфизмы из* $G(q)$ *в* $G(p)$ *и из* $G(p)$ *в* $G(q)$ *(соответственно существует гомоморфизм из* $G(q)$ *в* $G(p)$*).* Следствием теоремы является разрешимость соответствующих эквациональных теорий.

Данная теорема сводит проверку тождеств на классах алгебр отношений с примитивно-позитивными операциями к анализу гомоморфизмов двухполюсников. Применительно к бинарным конъюнктивным операциям ранга 6 это означает, что перед проверкой конкретных тождеств необходимо сначала классифицировать сами операции с точностью до преобразований двойственности, инвертирования и сопряжения – поскольку эквивалентные операции дают одинаковые эквациональные теории. Этой классификации и посвящена следующая часть работы.

В третьей части рассматриваются группоиды отношений с одной бинарной конъюнктивной операцией. Для кодирования операций вводится восьмибитный двоичный код $\alpha = a_{00}a_{01}a_{10}a_{11}b_{00}b_{01}b_{10}b_{11}$, где $a_{ij}, b_{ij} \in \{0, 1\}$. Определяются преобразования:

Определение 4. *Операция* $F^*(\rho_1, \rho_2) = F(\rho_2, \rho_1)$ *называется двойственной к операции* F*.*

Определение 5. *Операция* $F^\star(\rho_1, \rho_2) = \big(F(\rho_1^{-1}, \rho_2^{-1})\big)^{-1}$*, где* $^{-1}$ *– операция реляционного обращения, называется инвертированной к операции* F*.*

Определение 6. *Операция* $F^{*\star}(\rho_1, \rho_2) = F^{\star *}(\rho_1, \rho_2) = \big(F(\rho_2^{-1}, \rho_1^{-1})\big)^{-1}$ *называется сопряжённой к операции* F*.*

Если исходная операция F имеет код $\alpha = a_{00}a_{01}a_{10}a_{11}b_{00}b_{01}b_{10}b_{11}$, то операции F^*, $F^\star$ и $F^{*\star} = F^{\star *}$ имеют соответственно коды:

$$\alpha^* = b_{00}b_{01}b_{10}b_{11}a_{00}a_{01}a_{10}a_{11}, \qquad \alpha^\star = a_{11}a_{01}a_{10}a_{00}b_{11}b_{01}b_{10}b_{00},$$

$$\alpha^{*\star} = \alpha^{\star *} = b_{11}b_{01}b_{10}b_{00}a_{11}a_{01}a_{10}a_{00}.$$

Операции $\{F, F^*, F^\star, F^{*\star}\}$ объединяются в один кластер. В зависимости от того, какие из этих операций совпадают, кластер может содержать один, два или четыре элемента. Возможны следующие типы кластеров:

1) тип A: один элемент $\{F = F^* = F^\star = F^{*\star}\}$;

2) тип B: два элемента $\{F = F^{*\star},\ F^\star = F^*\}$;

3) тип C: два элемента $\{F = F^*,\ F^\star = F^{*\star}\}$;

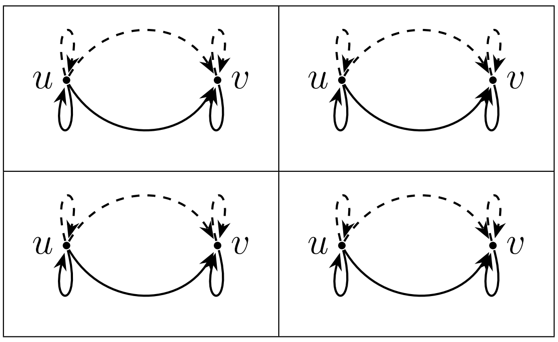
4) тип D: два элемента $\{F = F^\star,\ F^* = F^{*\star}\}$;

5) тип E: четыре элемента $\{F, F^*, F^\star, F^{*\star}\}$ (все операции попарно различны).

Проводится полная классификация конъюнктивных операций ранга 6, получаемых комбинациями графов ранга 2 с рангом 4 и ранга 3 с рангом 3. Выделено 11 классов эквивалентности. Для каждого класса указано графическое представление (двухполюсник) и количество операций в классе.

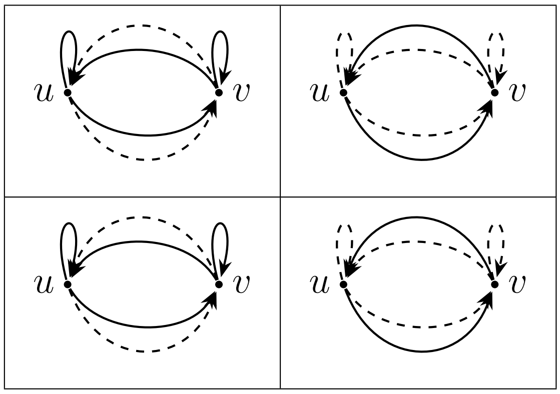
Пример класса с одной операцией:

$\mathrm{C}_1 + C_1$	$\mathrm{C}_1 + C_1$
$\mathrm{C}_1 + C_1$	$\mathrm{C}_1 + C_1$



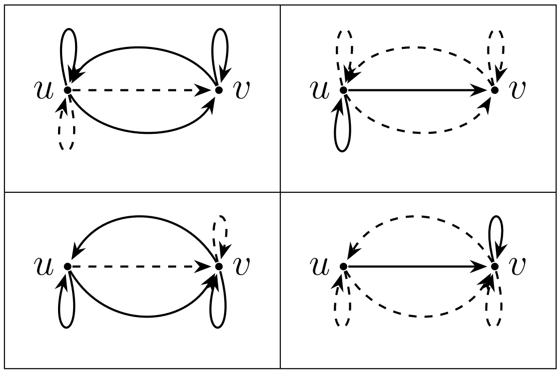
Пример класса с двумя операциями:

$\mathrm{B}_1 + D_1$	$\mathrm{D}_1 + B_1$
$\mathrm{B}_1 + D_1$	$\mathrm{D}_1 + B_1$



Пример класса с четырьмя операциями:

$\mathrm{B}_3 + D_1$	$\mathrm{D}_1 + B_3$
$\mathrm{B}_3^* + D_1$	$\mathrm{D}_1 + B_3^*$



Далее с помощью компьютерной программы проверяется выполнение девяти тождеств:

1. $(xy)z = x(yz)$ — ассоциативность;
2. $xy = yx$ — коммутативность;
3. $x^2y = xy$ — псевдо-идемпотентность слева;
4. $xy^2 = xy$ — псевдо-идемпотентность справа;
5. $(xy)z = (yx)z$ — псевдо-коммутативность слева;
6. $x(yz) = x(zy)$ — псевдо-коммутативность справа;
7. $((xy)z)w = (x(yz))w$ — псевдо-ассоциативность слева;
8. $x((yz)w) = x(y(zw))$ — псевдо-ассоциативность справа;
9. $x^2y^2 = y^2x^2$ — коммутативность квадратов.

Результаты сведены в следующую таблицу.

Класс	Элемент	1	2	3	4	5	6	7	8	9
1. B1 + D1	[0,1,1,0] + [1,1,1,1]	+	−	−	+	−	+	+	+	+
2. B2 + D1	[1,0,0,1] + [1,1,1,1]	+	−	+	+	+	−	+	+	−
3. B3 + D1	[1,1,0,0] + [1,1,1,1]	+	−	−	+	−	+	+	+	+
4. B4 + D1	[1,0,1,0] + [1,1,1,1]	−	−	−	+	−	+	−	+	+
5. C1 + C2	[1,1,0,1] + [1,0,1,1]	−	−	−	−	−	−	−	−	+
6. C1 + C3	[1,1,0,1] + [1,1,1,0]	−	−	−	−	−	+	+	+	+
7. C3 + C_3^*	[1,1,1,0] + [0,1,1,1]	−	−	−	−	+	+	+	+	+
8. C2 + C3	[1,0,1,1] + [1,1,1,0]	−	−	−	−	−	+	−	+	+
9. C1 + C1	[1,1,0,1] + [1,1,0,1]	+	+	+	+	+	+	+	+	+
10. C2 + C2	[1,0,1,1] + [1,0,1,1]	−	+	−	−	+	+	−	−	+
11. C3 + C3	[1,1,1,0] + [1,1,1,0]	−	+	−	−	+	+	+	+	+

Таблица 1 — проверка тождеств

Четвёртая часть посвящена численной реализаци. Для этого был разработан код на языке $Python$, использующий встроенные функции форматирования для перевода чисел в двоичное представление, целочисленные операции для обратного преобразования и многоуровневую систему вложенных циклов для перебора всех комбинаций элементов таблицы Кэли размером 16×16.

В качестве входных данных выступают четырёхбитные списки A и B (маски графов) для каждого из 11 классов, определяющие правило вычисления результата операции, а также девять функций проверки тождеств, каждая из которых реализует соответствующее алгебраическое соотношение.

Далее выполняются следующие действия:

1. Реализованы функции прямого и обратного преобразования между десятичными числами (от 0 до 15) и их четырёхбитным двоичным представлением.

2. Вспомогательная функция разбивает четырёхбитную строку на две двухбитовые подстроки. Другая вспомогательная функция проверяет, совпадают ли единичные биты матрицы A с соответствующими битами разбитого аргумента, используя два индекса для доступа к подстрокам.

3. Основная функция строит таблицу Кэли размером 16×16. Для четырёх комбинаций индексов вычисляются два логических условия (сравнение битов матриц с подстроками); формируется 4-битный вектор результата, где бит

равен 1, если оба условия истинны, и 0 в противном случае. Полученный вектор преобразуется в десятичное число и помещается в соответствующую ячейку таблицы.

4. Для каждого из 11 классов строится таблица Кэли, после чего последовательно вызываются девять функций проверки тождеств. Каждая такая функция перебирает все возможные значения переменных и сравнивает левую и правую части соответствующего алгебраического уравнения.

5. Результаты выводятся в двух форматах: подробный – для каждого класса отдельно с указанием используемых масок A и B и символами «+» (тождество выполняется) или «−» (не выполняется). Сводная таблица – все 11 классов в виде строк с результатами девяти проверок.

В конце программы приводится расшифровка каждого из девяти тождеств с их словесным описанием и алгебраической записью.

Заключение. В рамках данной магистерской работы было проведено исследование эквациональных теорий классов алгебр отношений с примитивно-позитивными операциями. Основной целью работы являлось изучение выполнимости тождеств и неравенств на таких классах, а также классификация бинарных конъюнктивных операций ранга 6 с последующей проверкой алгебраических тождеств.

В ходе выполнения магистерской работы получены следующие основные результаты:

1. Изучены фундаментальные понятия теории универсальных алгебр, бинарных отношений и алгебр отношений, необходимые для исследования эквациональных теорий.

2. Установлен критерий выполнимости тождеств и неравенств на классах алгебр отношений с примитивно-позитивными операциями, доказана разрешимость соответствующих эквациональных теорий.

3. Проведена полная классификация бинарных конъюнктивных операций ранга 6. Выделено 11 классов эквивалентности относительно преобразований двойственности, инвертирования и сопряжения. Для каждого класса приведено графическое представление (двухполюсник) и указано количество операций в классе (1, 2 или 4).

4. Выполнена проверка девяти алгебраических тождеств для всех классов.

Была разработана программа на языке *Python*, реализующая построение таблицы Кэли и автоматическую проверку тождеств. Программа может быть использована для дальнейшего исследования группоидов отношений, в том числе высших рангов.

В результате проведенного исследования получены новые результаты, касающиеся классификации бинарных конъюнктивных операций и разрешимости эквациональных теорий для классов алгебр отношений. Эти результаты углубляют понимание структуры алгебр отношений и их эквациональных свойств.

Магистерская работа вносит вклад в развитие теоретико-алгебраических методов исследования бинарных операций и может быть интересна специалистам в области универсальной алгебры, алгебраической логики, дискретной математики.

Кроме того, полученные результаты могут найти применение в криптографии при построении протоколов открытого распределения ключей на неассоциативных структурах.