МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

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

Кафедра Геометрии

Свойства конъюнктивных операций над бинарными отношениями

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студента 4 курса 421 группы

Направление 02.03.01 Математика и компьютерные науки

механико-математического факультета

Таванюка Максима Романовича

Научный руководитель
профессор, д. ф.-м. н., профессор ______________ Д.А. Бредихин
должность, уч. степень, звание

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

2025

Введение. Алгебра отношений предоставляет набор математических операций для эффективного управления и обработки данных в системах с базами данных, реализация таких операций происходит на языке SQL. При этом алгебра отношений играет важную роль в области криптографии, где она используется для разработки и анализа криптографических протоколов, обеспечивая безопасность передачи данных и коммуникаций. Применение алгебры отношений в этой области помогает обнаруживать уязвимости, разрабатывать надежные алгоритмы шифрования и дешифрования, а также анализировать и обеспечивать целостность систем безопасности. Таким образом, применение алгебры отношений играет ключевую роль в различных аспектах современной информационной технологии и науки, обеспечивая эффективное управление данными, разработку безопасных систем и обеспечение функциональности программ и алгоритмов.

Основное содержание работы. В первом разделе бакалаврской работы вводятся все необходимые определения и понятия, а так же перечислены математические символы и сокращения.

Определение 4. *Бинарным отношением (или просто отношением) на множестве U называется любое подмножество его декартова квадрата U^2. Принадлежность упорядоченной пары (x, y) отношению $R \subset U^2$ будем обозначать одним из следующих способов:*

- $(x, y) \in R$;
- xRy.

Множество всех отношений, заданных на U, будем обозначать как $\mathrm{Rel}(U)$. Отношение $\Delta = \{(x, x) \big| x \in U\}$ называется тождественным.

Бинарные отношения можно задать одним из следующих способов:

- Перечислением всех пар, связанных между собой отношением;
- Указать общие свойства, характеризующие данное отношение;
- Задание отношения в виде булевой матрицы;
- Задание отношения в виде графа.

Рассмотрим свойства бинарных отношений:

Пусть $R \subset X \times X$ (или же $R \subset X^2$).

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 называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно;
6. R называется отношением порядка, если оно рефлексивно, антисимметрично и транзитивно.

Так же существуют проекции и срезы отношений, а так же как определяются отношения в зависимости от их срезов.

Первой и второй проекцией отношения $R \subset U \times U$ называются подмножества U, которые задаются следующим образом:

$$\mathrm{pr}_1\, R = \{x : (\exists y : (x,\, y) \in R)\},\ \mathrm{pr}_2\, R = \{y : (\exists x : (x,\, y) \in R)\}.$$

Срез отношений $R \subset X \times X$ через элемент $x \in U$ (подмножество $X \subset U$) задается следующим образом:

$$R(x) = \{y : (x,\, y) \in R\},\ R(X) = \{y : (\exists x \in X : (x,\, y) \in R)\}.$$

На множестве $\mathrm{Rel}(U)$ определяются операции умножения ($\circ$) и обращения ($^{-1}$).

Определение 5. *Отношение $R \subset U \times U$ называется: полным, если $\mathrm{pr}_1\, R = U$; плотным, если $\mathrm{pr}_1\, R = \mathrm{pr}_2\, R = U$; симметричным, если $R^{-1} = R$; транзитивным, если $R \circ R \subset R$; проекционно-симметричным, если $\mathrm{pr}_1\, R = \mathrm{pr}_2\, R$; рефлексивным, если $\Delta \subset R$; антисимметричным, если $R \cap R^{-1} = \Delta$.*

В работе так же будут использоваться алгебры отношений, группоиды и упорядоченные группоиды, определния которым даны ниже:

Определение 8. *Под алгеброй (универсальной алгеброй) типа $\tau = \{n_j\}_{j \in J}$ мы понимаем пару $A = (A,\, \{f_j\}_{j \in J})$, где A - непустое множество, называемое носителем алгебры, $\{f_j\}_{j \in J}$ - семейство операций на A, причем арность* *операции f_j совпадает с n_j. Алгебры с конечным набором операций $f_1, \dots, f_n$ будем обозначать $(A, f_1, \dots, f_n)$.*

Определение 9. *Группоидом называется алгебра с одной бинарной операцией вида $(A, \cdot)$, где A - непустое множество, а под бинарной операцией $\cdot$ понимается правило, по которому можно найти результат операции для любых двух элементов из A.*

Определение 10. *Упорядоченным группоидом вида $(A, \cdot, \leq)$ называется группоид $(A, \cdot)$ с заданным на множестве A отношением порядка $\leq$, согласованным с операцией группоида. Это значит, что $x \leq y$ влечёт за собой $z \cdot x \leq z \cdot y$ и $x \cdot z \leq y \cdot z$.*

Определение 12. *Алгеброй отношений называется пара (Φ, Ω), где Φ - некоторое множество бинарных отношений, замкнутое относительно совокупности операций Ω над ним.*

Обозначим класс всех алгебр (упорядоченных алгебр) отношений с множеством операций Ω через $\mathrm{R}\{\Omega\}$ $(\mathrm{R}\{\Omega, \subset\})$.

Определение 13. *Операции над отношениями, задаваемые с помощью формул исчисления предикатов первого порядка, называются логическими операциями.*

Логические операции могут быть классифицированы в соответствии с формулами, которые их определяют. Операция над отношением называется диофантовой (в другой терминологии называется примитивно-позитивной или обобщенной композицией), если она может быть задана с помощью формулы, которая в префиксной нормальной форме содержит лишь операции конъюнкции и кванторы существования. Частным случаем примитивно-позитивных операций являются те операции, определяемые формулами без кванторов. Операции такого вида называются конъюнктивными. Стоит отметить, что для случаев унарных отношений (подмножеств) единственной бинарной конъюнктивной операцией является пересечение.

Следующий раздел описывает алгебру термов, как строятся термы и какими свойствами они обладают.

Термом в логике предикатов называют комбинацию функций, переменных и констант. Здесь переменные индивидные, т.е. принимают значения из некоторого универсума (т.е. множество, содержащее все объекты и все множества). Формула в логике предикатов составляется из атомарных формул (т.е. простейшая формула, которую нельзя разбить на подформулы), логических формул и кванторов. Терм имеет определённое значение, его можно вычислить, а формула имеет логическое значение: "да" или "нет". Если на место пропозициональных переменных в формуле логики высказываний подставить предикаты, зависящие от термов, то мы получим логическое выражение, истинность которого определяется зависимостью истинности формулы от переменных и значениями термов. Произвольная совокупность попарно различных символов (или же букв) $X = \{x_1, x_2, \ldots, x_n, \ldots\}$ называется алфавитом. Конечная последовательность символов (букв) в алфавите образует слово. Язык термов определяется индуктивно.

Термы не только являются средством задания функций над различными типами данных, но и сами используются как данные в ряде языков программирования (lisp, prolog и др.), а также в теоретических исследованиях. Благодаря рекурсивному построению, они позволяют легко образовывать и обрабатывать сложные динамические структуры данных (списки, деревья, формулы и пр.). Обычно используются алгебры термов. Носителем такой алгебры являются термы определённых сортов, а её операциями - функции, образующие сложные термы из более простых. Эти операции называются конструкторами.

Алфавит языка термов состоит из следующих символов:

1. Предметные символы (переменные) - T_0 (буквы $x, y, z, \ldots$ с индексами и без индексов);
2. Функциональные символы - F (буквы $f, g, \ldots$ с верхними индексами, обозначающие арность, и нижними символами. Если верхний индекс (арность) равен 0, то его можно не указывать.
3. Символы-разделители - левые и правые круглые скобки, а так же запятые.

Определение 14. *Сигнатурой называется совокупность символов* $\{f_j\}_{j \in J}$*, используемые для обозначений операций алгебры с указанием их арности* n_i.

Рассмотрим сигнатуру $\{f_i\}_{i \in I}$, где арность сигнатуры f_i совпадает с n_i. Рассмотрим множество T_0 состоящее из символов, которые называются переменными (или предметными переменными). Обозначим через Σ алфавит, который состоит из символов операций и символов переменных, и пусть $\mathrm{W}(\Sigma)$ - множество слов (так называемая последовательность символов) из алфавита Σ. Определим подмножество $T \subset \mathrm{W}(\Sigma)$, называемое множеством термов, следующим индуцированным образом:

Определение 15. *Термами называются слова, построенные по следующим правилам:*

1. *Все символы из T_0 - термы;*
2. *Если $t_1, t_2, \ldots, t_n$ - термы, то $f^n(t_1, t_2, \ldots, t_n)$ - терм. ($f^n \in F$, $n \geq 1$);*
3. *Термами являются только те слова, которые определены правилами 1 и 2.*

Далее идет раздел о многообразиях и квазимногообразиях, где формулируется теорема Биркгофа.

Определение 19. *Класс однотипных алгебр $\mathscr{K}$ называется многообразием (квазимногообразием), если существует такая система тождеств (квазитождеств) Σ, что для любой алгебры A (упорядоченной алгебры A), соответствующего типа, $A \in \mathscr{K}$ тогда и только тогда, когда A удовлетворяет системе тождеств (квазитождеств) Σ.*

Теорема 1 (Теорема Биркгофа)**.** *Непустой класс алгебр (упорядоченных алгебр) R сигнатуры Ω является многообразием тогда и только тогда, когда R замкнуто относительно взятия подалгебр, фактор-алгебр и декартовых произведений, то есть класс R вместе с каждой алгеброй (упорядоченной алгеброй) содержит любую её подалгебру, фактор-алгебру, а также вместе с любым семейством алгебр (упорядоченных алгебр) содержит их декартово произведение.*

Глава об эквациональной теории алгебр отношений несёт реферативный характер и основана на работе Д.А. Бредихина «Эквациональная теория алгебр отношений с позитивными операциями». Среди операций над отношениями особую роль играют логические операции, которые могут быть заданы с помощью формул исчисления предикатов первого порядка (т.е. логические выражения). Примитивно-позитивные (или же диофантовые) формулы задают так называемые примитивно-позитивные операции. К числу примитивно-позитивных операций относятся операции пересечения $\cap$, объединения $\cup$, произведения $\circ$ и обращения $^{-1}$ бинарных отношений.

Операции над отношениями, задаваемые с помощью формул исчисления предикатов первого порядка, называются логическими. Пусть $\phi(x, y, r_1, r_2, \ldots, r_n)$ исчисления предикатов первого порядка (т.е. логическая формула), содержащая две свободные индивидуальные переменные x и y, а так же бинарные предикатные символы $(r_1, \ldots, r_n)$, определяет операцию F_ϕ, задаваемую следующим образом:

$$F_\phi(\rho_1, \ldots, \rho_n) = \{(x, y) \mid \phi(x, y, r_1, \ldots, r_n)\}$$

где переменные x, y представляют собой элементы множества X, а бинарные предикатные символы $(r_1, \ldots, r_n)$ интерпретируются как бинарные отношения $(\rho_1, \ldots, \rho_n)$. Теперь когда у нас есть понятие логической операции над отношениями, можно дать определение диофантовой операции.

Определение 30. *Логическая операция называется диофантовой (в другой терминологии позитивно-примитивной), если она содержит в своей записи лишь кванторы существования и операции конъюнкции.*

К числу диофантовых операций можно отнести операции умножения $\circ$ и обращения $^{-1}$:

$$\rho \circ \sigma = \{(x, y) \mid \exists z :\ (x, z) \in \rho \wedge (y, z) \in \sigma\}$$

$$\rho^{-1} = \{(x, y) \mid (y, x) \in \rho\}$$

Помимо этого, операция пересечения $\cap$ являются диофантовой операций, тогда как операция объединения $\cup$ не является. Стоит отметить, что алгебра отношений называется диофантовой, если все её операции так же являются диофантовыми.

Логические операции так же очень удобно обозначать через двухполюсники. Двухполюсниками являются помеченные графы с выделенными вершинами, обычно это вход(in) и выход(out). Выделенные вершины при этом необязательно различны. Дадим более точные определения графам и двухполюсникам:

Определение 31. *Графом называется совокупность некоторых точек (объектов) и соединяющих их линий (связей). Точки графа называются его вершинами, а соединяющие их линии – дугами (рёбрами).*

Определение 32. *Помеченным ориентированным графом будем называть пару $G = (V, E)$, где $V = V(G)$ множество, называемое множеством вершин, и $E = E(G) \subset V \times \mathbb{N} \times V$ тернарным отношением, где $\mathbb{N}$ - множество натуральных чисел.*

Тройку $(u, k, v) \in E$ будем называть дугой с меткой $k \in \mathbb{N}$, соединяющей вершину $u \in V$ с вершиной $v \in V$. Таким образом E представляет собой множество помеченных ориентированных дуг, соединяющих любые две вершины с числовой меткой из $\mathbb{N}$. В графическом представлении это выглядит следующим образом:

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

Определение 34. *Двухполюсником называют помеченный граф с двумя выделенными вершинами, т.е. система вида $G = (V, E, in, out)$ представляет собой двухполюсник, где (V, E) - помеченный граф, а in и out - две выделенные вершины (необязательно различные), называемые входом и выходом двухполюсника соответственно.*

Определение 35. *Пусть F_ϕ - некоторая диофантовая операция, задаваемой формулой ϕ. Тогда такой операции может быть сопоставлен двухполюсник $G = G(\phi)$, который определяется следующим образом: $G =$*

(V, E, in, out), где множество вершин V совпадает со множеством логических переменных, входящих в формулу ϕ. Тройка $(x_i, k, x_j) \in E$ тогда и только тогда, когда атомарная формула $r_k(x_i, x_j) \in \phi$, где $(x_i, x_j) \in \rho_k$. Если формула $x_i = x_j \in \phi$, то индексы (или же вершины) x_i и x_j совпадают друг с другом. При этом $in = x_0$, $out = x_1$.

Теперь когда у нас есть определение двухполюсника, перейдем к рассмотрению операций $\circ$, $^{-1}$, $\cap$ над двухполюсниками и рассмотрим их в графическом виде.

Операция произведения $\rho_1 \circ \rho_2 = \{(x_0, x_1) \mid \exists x_2 : (x_0, x_2) \in \rho_1 \wedge (x_2, x_1) \in \rho_2\}$:

$$\mathrm{in} \cdot \xrightarrow{\quad 1 \quad} \cdot \xrightarrow{\quad 2 \quad} \cdot \mathrm{out}$$

Операция обращения $\rho^{-1} = \{(x_0, x_1) \mid (x_1, x_0) \in \rho\}$:

$$\mathrm{in} \cdot \xleftarrow{\quad 1 \quad} \cdot \mathrm{out}$$

Операция пересечения $\rho_1 \cap \rho_2 = \{(x_0, x_1) \mid (x_0, x_1) \in \rho_1 \ \wedge \ (x_0, x_1) \in \rho_2\}$:

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

В этом разделе присутствует и основная теорема, позволяющая определить принадлежность какого-либо тождества эквациональному классу, если между двухполюсниками существует гомоморфизм. Перед тем как будет сформулирована теорема, необходимо дать определение гомоморфизма двухполюсников.

Определение 37. *Пусть $G_1(V_1, E_1, in_1, out_1)$ и $G_2(V_2, E_2, in_2, out_2)$ - два двухполюсника. Отображение $f : V_2 \mapsto V_1$ называется гомоморфизмом двухполюсника G_2 в G_1, если $f(in_2) = in_1$, $f(out_2) = out_1$ и $(f(u), k, f(v)) \in E_1$ для любого ребра $(u, k, v) \in E_2$. Гомоморфизм из G_2 в G_1 обозначается* *через* $G_1 \prec G_2$. *Если же существует гомоморфизм из* G_2 *в* G_1 *и из* G_1 *в* G_2, *то оно обозначается через* $G_2 \cong G_1$. *Если граф* G_2 *является подграфом* G_1, *т.е.* $G_2 \subset G_1$, *то гомоморфизм из* G_2 *в* G_1 *всегда существует.*

Теорема 1. *Пусть* Ω *является множеством примитивно-позитивных операций. Тогда тождество* $p = q$ $(p \leq q)$ *принадлежит эквациональной теории* $E_q\{\Omega\}$ $(E_q\{\Omega, \subset\})$ *тогда и только тогда, когда существуют гомоморфизмы* $G(p) \to G(q)$ *и* $G(q) \to G(p)$ *(существует гомоморфизм* $G(q) \to G(p)$*).*

Доказательство данной теоремы описано в бакалаврской работе в разделе «Основная теорема».

Далее в работе происходит переход к практической части о классификации конъюнктивных операций. В практической части рассматриваются операции над алгебрами с одной бинарной операцией, т.е. над группоидами. Так же рассматриваются операции над упорядоченными группоидами, на которых задано отношение порядка. Операция группоида применяется к двум его элементам, отсюда и следует название "бинарная операция". Каждой такой операции над любыми двумя элементами из множества ставится в соответствии некоторый результат такой операции. Такие операции обычно задаются логическими формулами, их ещё называют логическими операциями. Как было сказано ранее, логические операции классифицируются в зависимости от определяемых их формулами. Операция называется примитивно-позитивной (или же диофантовой), если она может быть определена логической формулой первого порядка, содержащая только кванторы существования и операции конъюнкции. Если операция определена без кванторов существования, а лишь с использованием конъюнкций атомов (или же неразделимых формул/операций), то операция называется конъюнктивной.

Для какой-либо формулы исчисления предикатов первого порядка (т.е. без равенств или констант) вида $\phi(x_1, x_2, r_1, r_2)$, где x_1, x_2 - свободные переменные, а r_1, r_2 - бинарные символы предиката. Теперь мы можем задать операцию F над множеством $\mathrm{Rel}(U)$ следующим образом:

$$F(\rho_1, \rho_2) = \{(u, v) \in U^2 : \phi(u, v, \rho_1, \rho_2)\},$$

где $\phi(u, v, \rho_1, \rho_2)$ означает, что формула ϕ срабатывает каждый раз, когда x_1, x_2 интерпретируются как $u, v \in U$, а r_1, r_2 как отношения $\rho_1, \rho_2 \in \mathrm{Rel}(U)$. Мы говорим, что примитивно-позитивная операция F имеет ранг k, если она может быть определена такой формулой, которая содержит ровно k конъюнктивных элементов, и не может быть определена какой-либо другой формулой с меньшим числом конъюнктивных элементов.

Определение 40. *Операцию называют конъюнктивной, если она в своей пренексной нормальной форме содержит только операции конъюнкции.*

Определение 41. *Операция $F^d(\rho_1, \rho_2) = F(\rho_2, \rho_1)$ называется двойственной к операции F.*

Определение 42. *Операция $F^c(\rho_1, \rho_2) = (F(\rho_2^{-1}, \rho_1^{-1}))$, где $^{-1}$ - операция взятия обратного отношения, называется обратной к операции F.*

Определение 43. *Операция $F^f(\rho_1, \rho_2) = (F(\rho_2^{-1}, \rho_1^{-1}))^{-1}$ называется сопряженной к операции F. Заметим, что $F^f = F^{cd} = F^{dc}$.*

Стоит отметить, что отображение $f(\rho) = \rho^{-1}$ является изоморфизмом группоидов $\mathrm{Rel}(F)$ и $\mathrm{Rel}(F^f)$, а так же изоморфизмом группоидов $\mathrm{Rel}(F^c)$ и $\mathrm{Rel}(F^d)$. При классификации конъюнктивных операций мы их будем объединять в классы, состоящие из этих двухполюсников, располагая их в матрице следующего вида:

$$\boxed{\begin{array}{cc} F & F^d \\ F^f & F^c \end{array}}$$

Обозначение класса операций

Количество операций в этом классе зависит от того, являются ли они сопряженными и обратными. Некоторые операции не имеют сопряженных и обратных, поэтому в классах может быть присутствовать символ "$-$", что означает, что граф совпадает с графом, который находится выше (или напротив него в зависимости от знака "=").

В практической части идёт рассмотрение сначала конъюнктивных операций первого ранга, затем второго ранга, а затем строятся классы конъюнктивных операций, который состоят из комбинаций операций ранга 1 и 2 (или 2 и 1), а так же двойственные, сопряженные и обратные операции. Совокупность этих операций и формирует класс конъюнктивных операций.

Конъюнктивные операции ранга 1, 2 и 3 представлены в практической части бакалаврской работы.

Результатом практической части является программа на языке C++, которая по двум заданным конъюнктивным операциям ранга 1 и 2 строит таблицу Кэли для 16-ти элементного группоида, результатом бинарной операции которого над двумя элементами группоида является другой элемент, данная таблица применяется для проверки тождеств. Далее в программе строится матрица порядка для проверки квазитождеств. Добавочным результатом будет таблица, в которой для каждой операции стоит знак "+" или "-" в зависимости от результата проверки тождеств и квазитождеств, а так же четырехмерный булев куб для демонстрации отношений порядка.

Заключение. Итогами данной работы являются рассмотренные бинарные отношения с их свойствами и примеры бинарных отношений, алгебры термов, многообразия и квазимногообразия, множества тождеств и квазитождеств для алгебр и упорядоченных алгебр. Затем были рассмотрены логические операции, графы, помеченные графы и двухполюсники с графическими примерами самих двухполюсников и операций над ними. Была приведена основная теорема эквациональной теории алгебр отношений. В практической части были рассмотрены конъюнктивные операции, операции над ними и построение классов конъюнктивных операций ранга 3 из операций ранга 1 и 2. В конце была создана программа на языке C++ для проверки тождеств и квазитождеств на группоидах и упорядоченных группоидах.