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

Кафедра геометрии

Конъюнктивные операции над отношениями

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления 02.03.01 Математика и компьютерные науки

механико-математического факультета

Скупинского Романа Владимировича

Научный руководитель
профессор, д.ф.-м.н., профессор _____ Д.А. Бредихин
подпись, дата

Зав. кафедрой
к.ф.-м.н., доцент _____ С.В. Галаев
подпись, дата

Саратов 2023

Введение. Множество бинарных отношений, замкнутое относительно совокупности Ω операции над ними, называется алгеброй отношений. Одним из важнейших математиков, внесших вклад в развитие алгебр отношений, является Альфред Тарский. Он изложил формальную логику, основанную на разрешении количественного определения как элементов, так и отношений, а затем он обратился к более подробному изучению формул этой системы, не содержащих кванторов, которые включали только переменные отношения. После представления списка аксиом, которые содержались в алгебре отношений, он доказал, что эти аксиомы позволяют свести формулы уравнений без кванторов к уравнениям. Таким образом, его исчисление отношений стало изучением некоторой эквациональной теории, которая, как он отметил, имела такое же отношение к изучению всех бинарных отношений на множествах, что и эквациональная теория булевой алгебры для изучения всех подмножеств множеств.

Предметом исследования являются алгебры отношений с операциями, принадлежащими к числу операций алгебр отношений Тарского. 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 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.

Для любой совокупности Ω операций над отношениями обозначим через $\mathrm{Cl}_U(\Omega)$ клон операций на $\mathrm{Rel}(U)$, порожденный операциями из Ω. Алгебра отношений (Φ, Ω) называется подредуктом (соответственно обобщенным подредуктом) алгебры отношений Тарского, если $\Omega \subseteq \Omega_0$ (соответственно $\Omega \subseteq \mathrm{Cl}_U(\Omega_0)$). Классы обобщенных подредуктов алгебр отношений Тарского с одной бинарной диофантовой операцией называются классами группоидов отношений. Можно отметить возросший интерес к теории группоидов в связи с возможностью их применения в криптографии. Изучается возможность использования неассоциативных группоидов для реализации процедуры от-

крытого распределения ключей на основе алгоритма, обобщающего хорошо известный алгоритм Диффи-Хеллмана. Доказано существование неассоциативных группоидов, обладающих необходимым для этого свойством перестановочности степеней, и не являющихся группоидами с ассоциативными степенями.

Данная бакалаврская работа разделена на три раздела.

Первый раздел посвящен базовым определениям и обозначениям, связанными с алгеброй отношений с примитивно-позитивными и конъюнктивными операциями. Рассматриваются основные понятия общей алгебры, такие как определение алгебры (универсальной алгебры), алгебры отношений и другие. Приведены некоторые определения и обозначения общего характера.

Во втором вводится, занимающее центральное место в дальнейшем изложении, понятие примитивно-позитивной операции над отношениями. Рассматривается представление диофантовых с помощью графов, излагаются результаты. В этом разделе используется аппарат теории графов, находится эффективное описание эквациональных теорий алгебр отношений с позитивными операциями.

Третий раздел посвящен классификации конъюнктивных операции ранга 2 и ранга 3. Проверяются их свойства, используя двухполюсные графы. Разработаем программные код, которое будет проверять свойства конъюнктивных операции ранга 3.

Цель данной работы заключается в классификации конъюнктивных операции ранга 3 и проверки их свойств, что, в свою очередь, может быть использовано в сфере защиты информации.

Содержание. Сначала дадим основные определения из общей алгебры, алгебра термов, многообразия алгебр.

Определение 1.2.1 Бинарным отношением или просто отношением на множестве U называются любое подмножество его декартова квадрата. Принадлежность упорядоченной пары (x,y) отношению R $\subset U \times U$ будем обозначать одним из следующих способов: (x,y) $\in$ R, xRy, x $\equiv$ y(R). Множество всех отношений, заданных на U, будем обозначать *Rel(U)*.

Отношения $\Delta = (x, y) : x \in U$ и $U = U \times U$ называются соответственно тождественным и универсальным отношением на U. Отношения $\Delta_Y =$

$(x, y) : x \in Y$ называется частично-тождественным отношением, определяемым подмножеством $Y \subset U$.

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

Определение 1.2.4 Под алгеброй (универсальной алгеброй) типа $\tau = \{n_j\}_{j \in J}$ мы понимаем пару $A = (A, \{f_j\}_{j \in J})$, где A - множество, называемое носителем алгебры, и $\{f_j\}_{j \in J}$ - семейство операций на A, причем арность операции f_j совпадает с n_j. Алгебры с конечным набором операций $f_1, ..., f_n$ будем обозначать $(A, f_1, ..., f_n)$.

Универсальная алгебра с одной алгебраической операцией называется группоидом.

Определение 1.2.6 Алгеброй отношений называется пары (Φ, Ω), где Φ некоторое множество бинарных отношений, замкнутое относительно совокупности операции Ω над ними.

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

Определение 1.2.7 Операции над отношениями, задаваемые с помощью формул исчисления предикатов первого порядка, называются логическими операциями.

Определение 1.3.1 Термами называют слова, построенные по следующим правилам:

1) Все символы из T_0 — термы;
2) Если $t_1, t_2, ..., t_n$ – термы, то $f^n(t_1, t_2, ..., t_n)$ – терм $(f^n \in F, n \geq 1)$

3) Термами являются только те слова, которые определены правилами 1 и 2.

Определение 1.3.3 Тождеством назовем формальное выражение вида $p = q$, где p и q это термы в соответствующей сигнатуре. Будем говорить, что универсальная алгебра $\mathscr{A} = (A, \{f_i\}_{i \in I})$ удовлетворяет тождеству $p = q$, если для любой оценки α на множестве $A : p_\alpha = q_\alpha$

Определение 1.4.1 Класс $\mathscr{K}$ - однотипных алгебр называется многообразием, если существует такая система тождеств Σ, что для любой алгебры A, соответствующего типа, $A \in \mathscr{K}$ тогда и только тогда, когда A удовлетворяет системе тождеств Σ.

Определение 2.1.2 Логическая операция называется примитивно-позитивной (в другой терминологии диофантовой), если она содержит в своей записи лишь кванторы существования и операции конъюнкции.

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

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

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

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 выделенныевершины (не обязательно различные), называемые входом и выходом двухполюсника соответственно.

Определение 2.1.5 Пусть $G = (V, E, in, out)$ и $G_k = (V_k, E_k, in_k, out_k)$ $(k = 1, ..., m)$ — двухполюсники с попарно непересекающимися множествами вершин. Назовем композицией этих двухполюсников новый двухполюсник $G(G_1, ..., G_m)$, определяемый следующим образом: возьмем двухполюсник G и заменим каждое его ребро $(u, k, v) \in E$на двухполюсник G_k, отождествляя при этом вершину in_k с вершиной u и вершину out_k с вершиной v.

Определение 2.1.6 Пусть $G_1 = (V_1, E_1, in_1, out_1)$ и $G_2 = (V_2, E_2, in_2, out_2)$ — двухполюсники. Отображение $f : V_2 \mapsto V_1$ называется го-

моморфизмом 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 всякой тройки $(u, k, v) \in E2$.

Сформулируем основную теорему описывающую строение эквациональной теории алгебр отношений с примитивно-позитивными операциями.

Теорема 2.2.1 Пусть Ω - множество примитивно-позитивных операций. Тождество

$$p = q(p \leq q)$$

принадлежит эквациональной теории $E_q\{\Omega\}$ ($E_q\{\Omega, \subset\}$) тогда и только тогда, когда существуют гомоморфизмы из $G(q)$ в $G(p)$ и из $G(p)$ в $G(q)$ (существует гомоморфизм из $G(q)$ в $G(p)$).

Определение 3.1.1 Операция называется конъюнктивной, если она может быть определена формулой первого порядка, содержащей в своей пренексной нормальной форме только операции конъюнкции.

Определение 3.1.2 Операция $F^d(\rho_1, \rho_2) = F(\rho_1, \rho_2)$ называется двойственной по отношению к операции F.

Определение 3.1.3 Операция $F^c(\rho_1, \rho_2) = (F(\rho_2^{-1}, \rho_1^{-1}))^{-1}$, где $^{-1}$ - операция обратного отношения, называемая сопряженной с операцией F.

Обозначим через $Rel(U)$ множество всех отношений на U. Для любой формулы $\phi(z_0, z_1, r_1, r_2)$ исчисления предикатов первого порядка (без равенства и констант), содержащей две свободные переменные z_0, z_1 и два бинарных символа предиката r_1, r_2, мы можем задать бинарную операцию F над $Rel(U)$, определяемую следующим образом:

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

где $\phi(u, v, \rho_1, \rho_2)$ означает, что формула ϕ выполняется всякий раз, когда z_0, z_1 интерпретируются как u, v, а r_1, r_2 интерпретируются как отношения $\rho_1, \rho_2 \in Rel(U)$.

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.

Поскольку существует всего восемь атомов из двух символов-предикатов и двух отдельных переменных, легко увидеть, что общее число операций

равно двумстам двадцати трем. С помощью рутинных вычислений можно установить, что число конъюнктивных операций вплоть до двойственных и сопряженных равно девяноста семи. Мы сосредоточимся на тех из них, которые имеют второй ранг. Существует всего шесть таких операций, которые определяются следующим образом:

$$F_0(\rho_1, \rho_2) = \{(u, v) \in U \times U : (u, v) \in \rho_1 \wedge (u, v) \in \rho_2\};$$

$$F_1(\rho_1, \rho_2) = \{(u, v) \in U \times U : (v, u) \in \rho_1 \wedge (v, u) \in \rho_2\};$$

$$F_2(\rho_1, \rho_2) = \{(u, v) \in U \times U : (u, v) \in \rho_1 \wedge (v, u) \in \rho_2\};$$

$$F_3(\rho_1, \rho_2) = \{(u, v) \in U \times U : (u, u) \in \rho_1 \wedge (u, v) \in \rho_2\};$$

$$F_4(\rho_1, \rho_2) = \{(u, v) \in U \times U : (u, u) \in \rho_1 \wedge (v, u) \in \rho_2\};$$

$$F_5(\rho_1, \rho_2) = \{(u, v) \in U \times U : (u, u) \in \rho_1 \wedge (v, v) \in \rho_2\};$$

Определение 3.3.1 Частично упорядоченный группоид - это алгебраическая система $(A, \cdot, \leq)$, где $(A, \cdot)$ - группоид, т.е. алгебра с одной двоичной операцией, а $\leq$ - отношение частичного порядка на A, совместимое с умножением, т.е. $x \leq y$ подразумевает $xz \leq yz$ и $zx \leq zy$.

Далее, приведем конъюнктивные операции ранга 3. Существует всего сорок восемь таких операций.

Каждая операция строится методом комбинирования двух двухполюсных графов, которые, в свою очередь, представимы в виде бинарной матрицы. Первый граф состоит из одной дуги, второй из двух дуг. Таким образом, первый граф имеет 4 варианта представления, а второй 6 вариантов. Так получаем 48 операций.

Эти операции можно разделить на классы. В каждом классе две или четыре операции. Количество операций в классе зависит от результата сопряжения и обратности этих операций. Так как некоторые операции не имеют сопряженных и обратных. Так, к примеру, для операции $\{(u, v) \in U :$

$\times U(u,v) \in \rho_1 \wedge (u,v) \in \rho_2 \wedge (v,u) \in \rho_2\}$ нет сопряженной операции, а обратная будет совпадать с двойственной для $\{(u,v) \in U : \times U(u,v) \in \rho_1 \wedge (u,v) \in \rho_2 \wedge (v,u) \in \rho_2\}$, то есть с $\{(u,v) \in U \times U(u,v) \in \rho_2 \wedge (u,v) \in \rho_1 \wedge (v,u) \in \rho_1\}$.

Таким образом можно получить 16 классов:

Мы концентрируем наше внимание ассоциативной операции $*$ над $Rel(U)$,, которая определяется следующим образом: для любых соотношений ρ_1 и ρ_2 из $Rel(U)$, положим

$$\rho_1 * \rho_2 = \{(u,v) \in U \times U : (u,u) \in \rho_1 \wedge (v,v) \in \rho_1 \wedge (u,v) \in \rho_2\}.$$

Для этой операции выполняется теорема.

Теорема 3.3.1 Группоид $(A, \cdot)$ принадлежит многообразию $V\{*\}$ тогда и только тогда, когда он удовлетворяет тождествам:

$$x^2y = yx, \tag{3.1}$$

$$xyz = yxz, \tag{3.2}$$

$$xy \leq y, \tag{3.3}$$

$$x \leq yz \Rightarrow x \leq yx \tag{3.4}$$

Заключение.

Данная работа посвящена изучению конъюнктивных операций над отношениями. А именно, классификации конъюнктивных операций ранга 3. Для достижения поставленной цели использовались методы описания эквациональных теорий классов алгебр отношений с помощью двухполюсных графов.

В этой работе освешены базовые определениями и обозначениями, связанными с алгеброй отношений с примитивно-позитивными и конъюнктивным операциями. Рассматриваются основные понятия общей алгебры. Приведены некоторые определения и обозначения общего характера.

А также приведено понятие примитивно-позитивной операции над отношениями и рассмотрено представление диофантовых операций с помощью графов. Приводятся, полученные в статье Д.А. Бредихина «Эквациональная теория алгебр отношений с позитивными операциями», результаты.

Формулируется результат полученный в ходе самостоятельной работы. Были классифицированы конъюнктивных операций ранга 3 и проверены определённые тождества для них. Далее, доказывается теорема о принадлежности полугруппы $(A, \cdot, \leq)$ к классу $R\{*, \subset\}$. Доказательство основанно на доказательсте теоремы из работам Д. А. Бредихина «О полугруппах отношений с операцией рефлексивно-ограничительного умножения».

На основе полученных данных, был сделан вывод о выполнимости заданных тождеств для конъюнктивных операций ранга 3.