Научная статья
DOI: 10.18287/2541-7525-2020-26-1-23-51

УДК 512.531; 519.7

Дата: поступления статьи: 15.01.2020
после рецензирования: 17.02.2020
принятия статьи: 28.02.2020

***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

# ПОЛУГРУППЫ БИНАРНЫХ ОПЕРАЦИЙ И КРИПТОСИСТЕМЫ НА ГРУППОИДАХ

**АННОТАЦИЯ**

В статье изучаются частные случаи алгебр многоместных отношений, а именно алгебры бинарных операций, определенных на элементах конечных и бесконечных множеств. Инструментальную основу исследования составляют унарная и ассоциативная бинарная операции над 3-местными отношениями, которые индуцируются операциями взятия обратного и произведения над 2-местными отношениями. Это позволяет перенести основные понятия, связанные со свойствами функциональности, инъективности, сюръективности и тотальности 2-местных отношений, на 3-местные отношения и сформулировать критерии выполнения подобных свойств в терминах упорядоченных полугрупп. Возникающая при этом система последовательных вложенний моноида квазигрупповых операций в моноид бинарных операций, а затем в моноид 3-местных отношений соответствует последовательным вложениям моноидов биекций, функций и 2-местных отношений. Разработанный аппарат позволяет применять к бинарным операциям и соответствующим им конечным группоидам быстрые алгоритмы возведения в степень для построения элементов циклических полугрупп, которые используются в современной асимметричной криптографии. Возможное приложение полученных результатов демонстрируется на примере протокола Диффи — Хелмана — Меркла открытого распределения ключей.

**Ключевые слова:** алгебра многоместных отношений, алгебра индикаторов, группоиды, квазигруппы, полугруппы, циклические полугруппы бинарных операций, асимметричная криптография, протокол Диффи — Хелмана — Меркла.

**Цитирование.** 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.

**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

В статье рассматриваются бинарные операции как частный случай 3-местных отношений, заданных на множестве. Возможны два подхода к исследованию и конструктивной реализации операций– функциональный и объектный. В первом случае с операцией связывают алгоритм построения результирующего значения операции на наборе значений ее аргументов. При этом в момент времени начала исполнения алгоритма результат операции не определен и недоступен для использования. Во втором случае операцию задают при помощи графика или таблиц Кэли, указывая связи между наборами значений аргументов и результатом, причем в любой момент времени результат операции определен, а доступ к нему определяет «ключ»– наборы значений аргументов. Сложность реализации функционального подхода измеряют числом элементарных операций, исполняемых процессором при построении результата.

Сложность реализации объектного — числом элементарных ячеек памяти, которые требуются для хранения связей между аргументами и результатом. Эти меры в некотором смысле условны, т. к. для хранения инструкций, реализующих алгоритм, требуется определенный объем памяти, а для доступа к хранимому результату по набору аргументов необходим набор инструкций, осуществляющих этот доступ. Однако в сравнении с основными затратами на реализацию того или иного представления они считаются пренебрежимо малыми.

Функциональный и объектный подходы не являются взаимоисключающими уже хотя бы потому, что таблица Кэли «прошивается» в алгоритм, исполняемый процессором, в виде базовой «таблицы умножения», а для построения графика операции часто используются алгоритмы построения результата.

В дальнейшем изложении мы будем придерживаться объектного подхода, т. к. он позволяет при рассмотрении операций как объектов определять «операции над операциями» и использовать уже известные алгебраические методы при изучении самих операций и порождаемых ими алгебр.

В качестве прикладного примера мы рассмотрим направление асимметричной криптографии, связанное с созданием и реализацией протоколов безопасного распространения ключей шифрования в недоверенной среде. Оно опирается на идеи теории односторонних функций с секретом и существенно использует вычислительную сложность применяемых алгоритмов. Первой опубликованной и наиболее известной в этой области является работа У. Диффи и М. Хеллмана [1], в которой описывался протокол открытого распределения ключей. Статья была написана под влиянием идей Р. Меркла о распространении открытого ключа [2], а сам протокол получил название протокола Диффи — Хелмана DH (Diffie — Hellman) или Диффи — Хелмана — Меркла DHM (Diffie — Hellman — Merkle).

Протокол DHM формулировался в терминах мультипликативных групп конечных полей $GF(p)$. Одним из сновных условий, обеспечивающих криптостойкость протокола DHM, является ассоциативность операции умножения. Свойство ассоциативности позволяет построить эффективный алгоритм вычисления степени элемента $g$, который опирается на представление показателя степени $n$ в двоичной системе счисления

$$g^n = g^{2^r d_r + 2^{r-1} d_{r-1} \ldots d_0} = g^{2(\ldots 2(2(2d_r + d_{r-1}) + d_{r-1})\ldots) + d_0}.$$

Действительно, полагая $a_0 = g$ и выполняя последовательно $r$ вычислений $a_i = a_{i-1}^2 g^{d_i}$ при $i \in 1..r$, на завершающем шаге получим $g^n = a_{r-1}$. Нетрудно понять, что данный алгоритм имеет логарифмическую сложность $O(\log(n))$ групповых операций. Вместе с тем известные к настоящему времени алгоритмы логарифмирования, т. е. нахождения $n \in \mathbb{N}$ из уравнения $g^n = a$ при изветных $g$ и $a$, имеют корневую сложность $O(\sqrt{n})$.

Не менее известный протокол RSA (Rivest — Shamir — Adleman), опирается на схему Шамира [3], использующую интерполяционные полиномы Лагранжа в конечных полях для многостороннего разделения секрета при генерации ключей шифрования. В данном случае от алгебраических операций сложения и умножения, в терминах которых формулируется эта схема, требуется выполнение всех свойств операций поля.

Аналогичные требования к свойствам алгебраических операций предъявляет система HFE (Hidden Field Equations) [4; 5], пригодная для применения в рамках так называемой «постквантовой криптографии» [6; 7], или эллиптические и гиперэллиптические криптографические системы [8; 9].

Криптографические системы, основанные на целочисленных векторных решетках, в частности схема GGH (Goldreich–Goldwasser–Halevi), помимо полевых свойств операций используют евклидову метрику многомерных вещественных линейных векторных пространств [10; 11].

Приведенные примеры призваны продемонстрировать то обстоятельство, что, с одной стороны, подавляющее большинство современных криптографических схем опирается на весьма «богатые», в смысле набора свойств операций, алгебраические системы, что обеспечивает гибкую алгоритмическую базу при их вычислительной реализации.

С другой стороны, тот же арсенал алгоритмических приемов может применяться для атак на криптографические протоколы с целью их дискредитации. Поэтому в последнее время исследователи все чаще стали проявлять интерес к более «бедным» алгебраическим системам, таким, например, как полугруппы и полукольца [12; 13]. Этим же объясняется возрождение интереса к криптографии, основанной на квазигруппах [14–18], а также исследования в области $n$-арных квазигрупп и полугрупп [19].

Как было отмечено выше, одним из условий существования криптостойкого «доквантового» асимметричного протокола является свойство ассоциативности его базовой бинарной операции. Отказ от этого свойства является первым шагом на пути от полугрупп – алгебр с ассоциативной бинарной операцией, к группоидам – алгебрам, на бинарную операцию которых не накладывается никаких ограничений. В англоязычной литературе группоид часто называют магмой (magma), подчеркивая тем самым первичность и неструктурированность этого класса алгебр, из которого в результате дополнительных огра-

ничений на операции «выкристаллизовываются» более сложно организованные алгебрические системы: квазигруппы, полугруппы и группы.

Несмотря на то что дальнейшие рассуждения будут в основном относиться к произвольным, не обязательно ассоциативным, бинарным операциям, один класс полугрупп мы все же будем использовать постоянно – это полугруппы бинарных операций, определенных на некотором множестве.

Будем придерживаться следующей терминологии. Обозначим символом $\bigotimes_{i=1}^{n} U_i$ декартово произведение $n$ множеств $U_i$. Обозначим символом $2^U$ булеан над множеством $U$. Мощность множества $U$ будем обозначать символом $|U|$. Множество $R \subseteq \bigotimes_{i=1}^{n} U_i$ будем называть $n$-местным отношением на множествах $U_i$. В тех случаях, когда все множества $U_i$ совпадают, $R \subseteq U^n$ называют $n$-местным отношением на множестве $U$.

В дальнейшем нас в основном будут интересовать 3-местные отношения $R \subseteq U^3$. Мы будем рассматривать бинарные операции на $U$ как 3-местные отношения со специальным свойством функциональности. Такой подход позволит определить алгебры, сигнатура которых обобщает сигнатуру хорошо известной алгебры 2-местных (бинарных) отношений $\langle 2^{U^2}, (\cup, \cap, {}^{-}, \emptyset, U^2, \circ, {}^{-1}, \mathbb{I}_U)\rangle$. Хотя теория отношений восходит к теории множеств, теории порядковых типов [20; 21], математической логике и основаниям математики [22; 23], она имеет обширные приложения в дискретной математике [24; 25], теории графов [26], теоретической информатике и кибернетике [27].

Кратко приведем основные факты из теории 2-местных отношений и общей алгебры, которые потребуются нам в дальнейшем.

## 1.1. Общие сведения об алгебре 2-местных отношений

2-местные отношения $R \in 2^{U\times V}$ принято называть отношениями из множества $U$ в множество $V$. Если $U = V$, 2-местные отношения $R \in 2^{U\times U}$ принято называть отношениями на множестве $U$. Хорошо известно, что $|2^U| = 2^{|U|}$ и $|\bigotimes_{i=1}^{n} U_i| = \prod_{i=1}^{n} |U_i|$.

**Определение 1.1.** Обратным к 2-местному отношению $R \in 2^{U\times V}$ называется 2-местное отношение $R^{-1} \in 2^{V\times U}$, определяемое правилом

$$R^{-1} = \{(v, u) \mid u \in U \wedge v \in V \wedge (u, v) \in R\}.$$

**Определение 1.2.** Произведением (левой композицией) 2-местных отношений $R_1 \in 2^{U\times V}$ и $R_2 \in \in 2^{V\times W}$ называется 2-местное отношение $R_1 \bullet R_2 \in 2^{U\times W}$, определяемое правилом

$$R_1 \bullet R_2 = \{(u, w) \mid \ u \in U \wedge w \in W \wedge \exists v_0 \in V\, (u, v_0) \in R_1 \wedge (v_0, w) \in R_2\}.$$

Суперпозицией (правой композицией) 2-местных отношений $R_1 \in 2^{U\times V}$ и $R_2 \in 2^{V\times W}$ называется 2-местное отношение $R_2 \circ R_1 \in 2^{U\times W}$, определяемое правилом

$$R_2 \circ R_1 = R_1 \bullet R_2 = (R_2^{-1} \bullet R_1^{-1})^{-1}.$$

Определения операций произведения и суперпозиции симметричны и одинаково часто встречаются в литературе. Использование той или иной операции зависит от предпочтений авторов. Операция $\bullet$ более естественна для теории бинарных отношений и теории графов, а операция $\circ$ согласуется с операцией композиции функций. Мы будем в основном пользоваться операцией произведения. Все последующие результаты могут быть легко переформулированы в терминах суперпозиции.

**Определение 1.3.** Тождественным 2-местным отношением на множестве $U$ называется 2-местное отношение $\mathbb{I}_U \in 2^{U^2}$, определяемое правилом

$$\mathbb{I}_U = \{(u, u) \mid u \in U\}.$$

Вполне понятно, что $\mathbb{I}_U^{-1} = \mathbb{I}_U \bullet \mathbb{I}_U = \mathbb{I}_U \circ \mathbb{I}_U = \mathbb{I}_U$.

**Определение 1.4.** Областью определения 2-местного отношения $R \in 2^{U\times V}$ называется множество

$$D_R = \{u \mid u \in U \wedge \exists v_0 \in V\, (u, v_0) \in R\} \subseteq U.$$

**Определение 1.5.** Областью значений 2-местного отношения $R \in 2^{U\times V}$ называется множество

$$E_R = \{v \mid v \in V \wedge \exists u_0 \in U\, (u_0, v) \in R\} \subseteq V.$$

Вполне понятно, что $D_R = E_{R^{-1}}$ и $E_R = D_{R^{-1}}$.

**Утверждение 1.1.** Помимо свойств операций булевой алгебры $\langle 2^{U\times V}, (\cup, \cap, ^-, \emptyset, U\times V)\rangle$ справедливы следующие свойства операций $\bullet, ^{-1}$ для произвольных 2-местных отношений $R_1, \tilde{R}_1 \in 2^{U\times V}$, $R_2, \tilde{R}_2 \in \in 2^{V\times W}$, $R_3 \in 2^{W\times Q}$

**R1.** $R_1 \bullet (R_2 \bullet R_3) = (R_1 \bullet R_2) \bullet R_3$ — ассоциативность операции $\bullet$;

**R2.** $R_1 \bullet (R_2 \cup \tilde{R}_2) = (R_1 \bullet R_2) \cup (R_1 \bullet \tilde{R}_2)$ — дистрибутивность операции $\bullet$ относительно операции $\cup$;

**R3.** $R_1 \bullet (R_2 \cap \tilde{R}_2) \subseteq (R_1 \bullet R_2) \cap (R_1 \bullet \tilde{R}_2)$ — полудистрибутивность операции $\bullet$ относительно операции $\cap$;

**R4.** $R_1 \subseteq \tilde{R}_1 \wedge R_2 \subseteq \tilde{R}_2 \longrightarrow R_1 \bullet R_2 \subseteq \tilde{R}_1 \bullet \tilde{R}_2$ — монотонность операции $\bullet$;

**R5.** $\mathbb{I}_U \bullet R_1 = R_1 = R_1 \bullet \mathbb{I}_V$ — свойства нейтральных по операции $\bullet$;

**R6.** $(R_1^{-1})^{-1} = R_1$ — инволютивность операции $^{-1}$;

**R7.** $(R_1 \bullet R_2)^{-1} = R_2^{-1} \bullet R_1^{-1}$ — антидистрибутивность операции $^{-1}$ относительно операции $\bullet$;

**R8.** $(R_1 \cup \tilde{R}_1)^{-1} = R_1^{-1} \cup \tilde{R}_1^{-1}$ — дистрибутивность операции $^{-1}$ относительно операции $\cup$;

**R9.** $(R_1 \cap \tilde{R}_1)^{-1} = R_1^{-1} \cap \tilde{R}_1^{-1}$ — дистрибутивность операции $^{-1}$ относительно операции $\cup$;

**R10.** $R_1 \subseteq \tilde{R}_1 \longrightarrow R_1^{-1} \subseteq \tilde{R}_1^{-1}$ — монотонность операции $^{-1}$;

**R11.** $\mathbb{I}_{D_R} \subseteq R_1 \bullet R_1^{-1} = ker(R_1)$ — свойство ядра $R_1$;

**R12.** $\mathbb{I}_{E_R} \subseteq R_1^{-1} \bullet R_1 = ker(R_1^{-1})$ — свойство ядра $R_1^{-1}$.

**R13.** $D_{R_1 \bullet R_2} \subseteq D_{R_1}$ — свойство области определения $R_1 \bullet R_2$.

**R14.** $E_{R_1 \bullet R_2} \subseteq E_{R_2}$ — свойство области значений $R_1 \bullet R_2$.

**Определение 1.6.** Левым сужением 2-местного отношения $R \in 2^{U\times V}$ на множество $U_0 \subset U$ называется 2-местное отношение $R_{U_0} \in 2^{U'\times V}$, определяемое правилом

$$R_{U_0} = \{(u, v) \mid u \in U_0 \wedge v \in V \wedge (u, v) \in R\}.$$

**Определение 1.7.** Правым сужением 2-местного отношения $R \in 2^{U\times V}$ на множество $V_0 \subset V$ называется 2-местное отношение $R^{V_0} \in 2^{U\times V_0}$, определяемое правилом

$$R^{V_0} = \{(u, v) \mid u \in U \wedge v \in V_0 \wedge (u, v) \in R\}.$$

В тех случаях, когда это не приводит к недоразумениям, будем сохранять за сужениями $R_{U_0} \in 2^{U_0\times V}$ и $R^{V_0} \in 2^{U\times V_0}$ прежнее обозначение $R$.

Часто вместо записи $(u, v) \in R$ используют инфиксную запись $uRv$. В терминах операций над 2-местными отношениями удобно дать следующие определения.

**Определение 1.8.** Говорят, что 2-местное отношение $R \in 2^{U\times V}$ тотально (слева), если

$$D_R = U,$$

или, что то же самое,

$$\mathbb{I}_U \subseteq R \bullet R^{-1}.$$

**Определение 1.9.** Говорят, что 2-местное отношение $R \in 2^{U\times V}$ сюръективно (тотально справа), если

$$E_R = V,$$

или, что то же самое,

$$\mathbb{I}_V \subseteq R^{-1} \bullet R.$$

С учетом определения 1.1 можно утверждать, что 2-местное отношение сюръективно тогда и только тогда, когда обратное к нему тотально, и наоборот.

**Определение 1.10.** Говорят, что 2-местное отношение $R \in 2^{U\times V}$ функционально (функция из $U$ в $V$), если

$$\forall u \in U \forall v_1, v_2 \in V\ (u, v_1) \in R \wedge (u, v_2) \in R \longrightarrow v_1 = v_2,$$

или, что то же самое,

$$R^{-1} \bullet R \subseteq \mathbb{I}_V.$$

В подобных случаях принята запись $R : U \to V$, а вместо записей $(u, v) \in R$ или $uRv$ используют запись $v = R(u)$, при этом $u$ называют аргументом функции, а $v$ — значением функции на аргументе. Множество тотальных функций из $U$ в $V$ принято обозначать $V^U$. Хорошо известно, что $|V^U| = |V|^{|U|}$. Функция из $U$ в $U$ называется функцией на $U$. Тотальная функция на $U$ называется преобразованием $U$. Непосредственно из определений следует, что если $R_1 : U \to V$ и $R_2 : V \to W$, то $R_1 \bullet R_2 : U \to W$ и $R_1 \bullet R_2(u) = R_2(R_1(u)) = R_2 \circ R_1(u)$. В силу того что $\mathbb{I}_U^{-1} \bullet \mathbb{I}_U = \mathbb{I}_U \bullet \mathbb{I}_U^{-1} = \mathbb{I}_U \bullet \mathbb{I}_U = \mathbb{I}_U$, тождественное отношение $\mathbb{I}_U$ — преобразование $U$, причем $\mathbb{I}_U^{-1}(u) = \mathbb{I}_U(u) = u$.

**Определение 1.11.** Говорят, что 2-местное отношение $R \in 2^{U\times V}$ инъективно, если

$$\forall v \in V \forall u_1, u_2 \in U\ (u_1, v) \in R \wedge (u_2, v) \in R \longrightarrow u_1 = u_2,$$

или, что то же самое,

$$R \bullet R^{-1} \subseteq \mathbb{I}_U.$$

С учетом определения 1.1 можно утверждать, что 2-местное отношение инъективно тогда и только тогда, когда обратное к нему функционально, и наоборот. Таким образом, обратное к функциональному отношению $R \in 2^{U\times V}$ функционально тогда и только тогда, когда $R$ инъективно.

Инъективные функции принято называть инъекциями, а сюръективные — сюръекциями.

**Определение 1.12.** Говорят, что 2-местное отношение $R \in 2^{U\times V}$– тотальная биекция, если $R$ функционально, инъективно, сюръективно и тотально, или, что то же самое,

$$R \bullet R^{-1} = \mathbb{I}_U \wedge R^{-1} \bullet R = \mathbb{I}_V.$$

В силу симметричности определения относительно $R$ и $R^{-1}$, а также инволютивности операции $^{-1}$, можно утверждать, что $R$ — тотальная биекция тогда и только тогда, когда $R^{-1}$ — тотальная биекция.

Непосредственно из определений следует, что $R \bullet R^{-1}(u) = R^{-1}(R(u)) = \mathbb{I}_U(u) = u$ и $R^{-1} \bullet R(v) = R(R^{-1}(v)) = \mathbb{I}_V(v) = v$ для произвольных элементов $u \in U$ и $v \in V$. Если обозначить $v = R(u) \in V$, то $R^{-1}(R(u)) = R^{-1}(v) = \mathbb{I}_U(u) = u \in U$. Таким образом, для тотальных биекций $v = R(u)$ тогда и только тогда, когда $u = R^{-1}(v)$.

В силу свойств сюръективности и инъективности для каждого элемента $v \in V$ будет существовать единственный элемент $u \in U$ такой, что $v = R(u)$, а в силу свойств тотальности и функциональности для каждого элемента $u \in U$ будет существовать единственный элемент $v \in V$ такой, что $v = R^{-1}(u)$.

Тотальная биекция на $U$ называется подстановкой множества $U$. Множество подстановок будем обозначать $B_U$. Вполне понятно, что тождественное отношение $\mathbb{I}_U$ — подстановка множества $U$, которая называется тождественной подстановкой.

В дальнейшем будем обозначать функции символами $F, G, \Phi, \Psi,\ f, g, \phi, \psi$.

**Утверждение 1.2.** Пусть $F_1 : U \to V,\ F_2 : V \to W$, тогда

**F1.** $F_1 \bullet F_2 \in 2^{U\times W}$ — функция;

**F2.** Если $F_1,\ F_2$ — тотальны, то $F_1 \bullet F_2 : U \to W$ — тотальна;

**F3.** Если $F_1,\ F_2$ — сюръекции, то $F_1 \bullet F_2$ — сюръекция;

**F4.** Если $F_1,\ F_2$ — инъекции, то $F_1 \bullet F_2$ — инъекция;

**F5.** Если $F_1,\ F_2$ — тотальные биекции, то $F_1 \bullet F_2$ — тотальная биекция.

**Утверждение 1.3.** Пусть $F \in U^U$— инъекция (тотальная), и множество $U$ конечно, т. е. состоит из конечного числа элементов, тогда $F$— подстановка.

**Определение 1.13.** Функцией $F_R$, индуцированной 2-местным отношением $R \in 2^{U\times V}$, называется функция из $2^U$ в $2^V$, определяемая правилом

$$F_R(U_0) = \{v \mid v \in V \wedge u \in U_0 \subseteq U \wedge (u, v) \in R\} \subseteq V.$$

Значения индуцированной функции и само 2-местное отношение $R$ полностью определяются ее остовом (остовной функцией), т. е. значениями этой функции на одноэлементных подмножествах множества $U$

$$F_R(\{u\}) = \{v \mid v \in V \subseteq U(u, v) \in R\},$$

исходя из очевидных равенств,

$$F_R(U_0) = \bigcup_{u\in U_0} F_R(\{u\}),$$

$$R = \bigcup_{u\in U} F_R(\{u\}) \times \{u\}.$$

Обычно отождествляют элемент $u$ и одноэлементное подмножество $\{u\}$, понимая под остовной функцией функцию $F^0_R : U \to 2^V$, значения которой определены правилом $F^0_R(u) = F_R(\{u\})$.

**Определение 1.14.** Говорят, что 2-местное отношение $R \in 2^{U^2}$ рефлексивно, если

$$\forall u \in U\ (u, u) \in R,$$

или, что то же самое,

$$\mathbb{I}_U \subseteq R.$$

**Определение 1.15.** Говорят, что 2-местное отношение $R \in 2^{U^2}$ симметрично, если

$$\forall u_1, u_2 \in U\ (u_1, u_2) \in R \longrightarrow (u_2, u_1) \in R,$$

или, что то же самое,

$$R = R^{-1}.$$

**Определение 1.16.** Говорят, что 2-местное отношение $R \in 2^{U^2}$ транзитивно, если

$$\forall u_1, u_2, u_3 \in U\ (u_1, u_2) \in R \wedge (u_2, u_3) \in R \longrightarrow (u_1, u_3) \in R,$$

или, что то же самое,

$$R \bullet R \subseteq R.$$

**Определение 1.17.** 2-местное отношение $R \in 2^{U^2}$ называют отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

## 1.2. Общие сведения об алгебрах с бинарными операциями

Напомним, что $n$-арной операцией на множестве $U$ называется тотальная функция $\phi : U^n \to U$. Алгеброй называется множество $U$ с определенным на нем конечным набором операций $\phi_i : U^{n_i} \to U$. Множество $U$ называют носителем алгебры, набор операций $(\phi_1, \ldots, \phi_m)$ — сигнатурой алгебры, а набор арностей операций $(n_1, \ldots, n_m)$ — типом алгебры. Сигнатуру алгебры принято обозначать $\Sigma$, а сами алгебры $\mathcal{A} = \langle U, \Sigma\rangle$. Для того чтобы указать, что операция $\phi$ входит в сигнатуру $\Sigma$, будем записывать $\phi \in \Sigma$. Алгебра называется конечной, если множество $U$ состоит из конечного числа элементов.

Говорят, что подмножество $U_0 \subseteq U$ носителя алгебры $\mathcal{A} = \langle U, \Sigma\rangle$ типа $(n_1, \ldots, n_m)$ замкнуто относительно сигнатуры, если для любой операции $\phi_i \in \Sigma$ и любого набора ее аргументов $u_1, \ldots, u_{n_i} \in U_0$ следует, что $\phi_1(u_1, \ldots, u_{n_i}) \in U_0$. В таких случаях также говорят, что алгебра $\mathcal{A}_0 = \langle U_0, \Sigma_0\rangle$ является подалгеброй алгебры $\mathcal{A} = \langle U, \Sigma\rangle$. Здесь сигнатура $\Sigma_0$ образована сужениями операций $\phi_i \in \Sigma$ на множества ${U_0}^{n_i}$. Обычно за сигнатурой $\Sigma_0$ и ее операциями сохраняют прежние обозначения и записывают $\mathcal{A}_0 \subseteq \mathcal{A}$.

Тотальная функция $F : U \to V$ называется гомоморфизмом алгебр $\mathcal{A}_1 = \langle U, \Sigma_1\rangle$ и $\mathcal{A}_2 = \langle V, \Sigma_2\rangle$ одного и того же типа $(n_1, \ldots, n_m)$, если для любых пар операций $\phi_i \in \Sigma_1$, $\psi_i \in \Sigma_2$ и любого набора

аргументов $u_1, \ldots, u_{n_i} \in U$ выполняются равенства $F(\phi_i(u_1, \ldots, u_{n_i})) = \psi_i(F(u_1), \ldots, F(u_{n_i}))$. В таких случаях говорят, что алгебры $\mathcal{A}_1$ и $\mathcal{A}_2$ находятся в отношении гомоморфизма или гомоморфны.

Биективный гомоморфизм называют изоморфизмом, а алгебры алгебры $\mathcal{A}_1$ и $\mathcal{A}_2$ — изоморфными, при этом записывают $\mathcal{A}_1 \sim \mathcal{A}_2$. Отношение изоморфизма однотипных алгебр является отношением эквивалентности.

Понятно, что алгебры $\langle 2^{U^2}, (\cup, \cap, ^-, \emptyset, U^2, \bullet, ^{-1}, \mathbb{I})\rangle$ и $\langle 2^{U^2}, (\cup, \cap, ^-, \emptyset, U^2, \circ, ^{-1}, \mathbb{I})\rangle$ изоморфны, а изоморфизм устанавливает функция $F(R) = R^{-1}$.

Инъективный гомоморфизм называют мономорфизмом, при этом говорят, что алгебра $\mathcal{A}_1 = \langle U, \Sigma_1\rangle$ изоморфно вложима в алгебру $\mathcal{A}_2 = \langle V, \Sigma_2\rangle$, и записывают, $\mathcal{A}_1 \precsim \mathcal{A}_2$. Если $F : U \to V$ — мономорфизм, то $\tilde{\mathcal{A}}_2 = \langle E_F, \Sigma_2\rangle$ — подалгебра алгебры $\mathcal{A}_2$, а $F : U \to E_F$ — изоморфизм алгебр $\mathcal{A}_1$ и $\tilde{\mathcal{A}}_2$.

Вполне понятно, что любая $n$-арная операция на $U$, как тотальная функция $\phi : U^n \mapsto U$, является $n+1$-местным отношением на $U$. В этом случае $\phi \subseteq U^n \times U = U^{n+1}$, а условия тотальности и функциональности могут быть записаны в следующей форме:

$$\forall u_1, \ldots, u_n \in U \exists u_0 \in U\ (u_1, \ldots, u_n, u_0) \in \phi,$$

$$\forall u_1, \ldots, u_n, u_{n+1}, \tilde{u}_{n+1} \in U\ (u_1, \ldots, u_n, u_{n+1}) \in \phi \wedge (u_1, \ldots, u_n, \tilde{u}_{n+1}) \in \phi \longrightarrow u_{n+1} = \tilde{u}_{n+1}.$$

Простейший класс алгебр образуют алгебры с бинарными операциями. Обычно вместо префиксной записи результата операции $\phi(u_1, u_2)$ используют инфиксную запись $u_1 \phi u_2$. Бинарные операции принято обозначать символами $\cdot, +, -, *, \div, \star, \circ, \bullet, \odot, \oplus$, и т. п.

Операции $*$ и $\div$ называются взаимно обратными слева (справа), если $u_3 = u_1 * u_2$ тогда и только тогда, когда $u_2 = u_3 \div u_1$ $(u_1 = u_3 \div u_2)$, для произвольных элементов $u_1, u_2, u_3 \in U$.

Группоидом называется множество $U$ с определенной на нем бинарной операцией $*$. Группоиды принято обозначать $\langle U, (*)\rangle$.

При изучении группоидов обычно пользуются мультипликативной терминологией, трактуя операцию $*$ как умножение. Реже используется аддитивная терминология, когда операция $*$ трактуется как сложение. Мы будем придерживаться в основном мультипликативной терминологии.

Мощность носителя конечного группоида $|U|$ называют его порядком. Порядок бесконечных группоидов считается бесконечным.

Если $\langle U, (*)\rangle$– группоид, то определяют группоид $\langle 2^U, (*)\rangle$, полагая $U_1 * U_2 = \{u \mid u = u_1 * u_2 \wedge u_1 \in \in U_1 \wedge u_2 \in U_2\}$, для произвольных подмножеств $U_1, U_2 \subseteq U$. Если множество $U_1 = \{u\}$ $(U_2 = \{u\})$ одноэлементное, то вместо $\{u\} * U_2$ $(U_1 * \{u\})$ записывают $u * U_2$ $(U_1 * u)$. Если операция группоида $\langle U, (*)\rangle$ ассоциативна, то и операция группоида $\langle 2^U, (*)\rangle$ ассоциативна.

Непустое подмножество $U_1 \subseteq U$ называют левым (правым) идеалом группоида $\langle U, (*)\rangle$, если $U * U_1 \subseteq U_1$ $(U_1 * U \subseteq U_1)$. Подмножество, которое одновременно является и левым, и правым идеалом, называют двусторонним идеалом или просто идеалом. Группоид называется простым слева (справа), если $U$ является его единственным левым (правым) идеалом. Аналогично дается определение простого идеала. Группоид является простым слева (справа) тогда и только тогда, когда $U * u = U$ $(u * U = U)$, для произвольного элемента $u \in U$.

Если $\emptyset \neq U_1 \subseteq U$, то пересечение всех левых (правых) идеалов, содержащих $U_1$, называют левым (правым) идеалом группоида, порожденным $U_1$. Левый (правый) идеал, порожденный $U_1$, равен $U_1 \cup \cup U * U_1$ $(U_1 \cup U_1 * U)$. Идеал $L(u) = \{u\} \cup U * u$ $(\{u\} \cup u * U)$ называют левым (правым) главным идеалом группоида, порожденным $u$. В случае полугрупп двусторонний главный идеал, порожденный $u$, имеет вид $J(u) = \{u\} \cup U * u \cup u * U \cup U * u * U$.

В группоиде $\langle U, (*)\rangle$ определяется левая (правая) положительная степень элемента $u \in U$ по операции $*$, при этом полагают $u_l^1 = u_r^1 = u$, и $u_l^{n+1} = u * u_l^n$ $(u_r^{n+1} = u_r^n * u)$, для $n \in \mathbb{N}$. Иными словами,

$$u_l^n = \underbrace{u * (\ldots * (u * (u * u)) \ldots)}_{n},$$

$$u_r^n = \underbrace{(\ldots ((u * u) * u) * \ldots) * u}_{n}.$$

Если операция $*$ коммутативна, то $u_l^n = u_r^n$.

В случае аддитивной терминилогии степень элемента обозначают как $n$-кратную сумму $n \cdot u_l$ $(n \cdot u_r)$.

Определим $U_0^l = \{u_{0l}^n \mid u_0 \in U \wedge n \in \mathbb{N}\}$. Группоид $\langle U_0^l, (*)\rangle$ называется левым циклическим, порожденным элементом $u_0$.

Аналогично определяется правый циклический группоид $\langle U_0^r, (*)\rangle$, порожденный элементом $u_0$.

Если в группоиде существует элемент $u \in U$, обладающий свойством $u * u = u$, то он называется идемпотентом.

Элемент $e_l \in U$ ($e_r \in U$) называется левым (правым) нейтральным по операции $*$ (левой (правой) единицей в мультипликативной терминологии и нулем в аддитивной терминологии), если для любого элемента $u \in U$ выполняется равенство $e_l * u = u$ ($u * e_r = u$). Если в группоиде одновременно существуют левый и правый нейтральные элементы, то они совпадают, единственны, и в таком случае элемент $e = e_l = e_r$ называется нейтральным (единицей). Вполне понятно, что левые (правые) нейтральные элементы являются идемпотентами. Группоиды с (левым, правым) нейтральным элементом принято обозначать ($\langle U, (*, e_l)\rangle$, $\langle U, (*, e_r)\rangle$) $\langle U, (*, e)\rangle$.

Если в группоиде с левым (правым) нейтральным элементом для некоторого элемента $u \in U$ существует элемент $u'_l \in U$ ($u'_r \in U$), для которого выполняется равенство $u'_l * u = e_l$ ($u * u'_r = e_r$), то $u'_l$ ($u'_r$) называется левым (правым) обратным по операции $*$ к элементу $u$.

Элемент $\theta_l \in U$ ($\theta_r \in U$) называется левым (правым) поглощающим элементом по операции $*$ (левым (правым) нулем в мультипликативной терминологии), если для любого элемента $u \in U$ выполняется равенство $\theta_l * u = \theta_l$ ($u * \theta_r = \theta_r$). Если в группоиде одновременно существуют левый и правый поглощающие элементы, то они совпадают, единственны, и в таком случае элемент $\theta = \theta_l = \theta_r$ называется поглощающим (нулем). Вполне понятно, что левые (правые) поглощающие элементы являются идемпотентами.

Важный класс группоидов образуют группоиды с сокращением. Группоид $\langle U, (*)\rangle$ называется группоидом с левым (правым) сокращением, если для любых элементов $u_1, u_2, u_3 \in U$ из того, что $u_3 * u_1 = u_3 * u_2$ ($u_1 * u_3 = u_2 * u_3$), следует, что $u_1 = u_2$. Группоид с левым и правым сокращением называется группоидом с сокращением.

Группоид $\langle U, (*)\rangle$ называется группоидом с левым (правым) делением, если для любых элементов $u_1, u_3 \in U$ ($u_2, u_3 \in U$) существует такой элемент $u_0 \in U$, что $u_1 * u_0 = u_3$ ($u_0 * u_2 = u_3$). Группоид с левым и правым делением называется группоидом с делением.

Группоид $\langle U, (*)\rangle$ с левым (правым) сокращением и делением называется левой (правой) квазигруппой. Группоид, который является одновременно и левой, и правой квазигруппой, называют квазигруппой. Понятие квазигруппы непосредственно связано с понятием взаимно обратных операций. Квазигруппа (левая, правая) с нейтральным элементом называется лупой (левой, правой).

Если операция $*$ ассоциативна, то группоид называется полугруппой. В полугруппе $\langle U, (*)\rangle$ левые и правые положительные степени элемента $u \in U$ совпадают и обозначаются $u^{n+1} = u^n * u = u * u^n$, для $n \in \mathbb{N}$.

Для полугрупп справедливы следующие правила положительных степеней:

$$u^n * u^m = u^{n+m} = u^{m+n} = u^m * u^n, \tag{1.1}$$

$$(u^n)^m = u^{nm} = u^{mn} = (u^m)^n. \tag{1.2}$$

Правило (1.2) является прямым следствием правила (1.1).

В случае полугрупп рассматривают циклические полугруппы $\langle U_0, (*)\rangle$, порожденные элементом $u_0$. Любая циклическая полугруппа коммутативна.

Если для некоторого элемента $u_0 \in U$ группоида $\langle U, (*)\rangle$ выполняется правило левых (правых) положительных степеней

$$\begin{gathered} u_{0l}^n * u_{0l}^m = u_{0l}^{n+m} = u_{0l}^{m+n} = u_{0l}^m * u_{0l}^n, \\ u_{0r}^n * u_{0r}^m = u_{0r}^{n+m} = u_{0r}^{m+n} = u_{0r}^m * u_{0r}^n, \end{gathered} \tag{1.3}$$

то левый (правый) циклический группоид $\langle U_0^l, (*)\rangle$ ($\langle U_0^r, (*)\rangle$), порожденный этим элементом, является полугруппой, причем коммутативной. При этом правило

$$\begin{gathered} (u_{0l}^n)_{0l}^m = u_{0l}^{nm} = u_{0l}^{mn} = (u_{0l}^m)_l^n, \\ (u_{0r}^n)_{0r}^m = u_{0r}^{nm} = u_{0r}^{mn} = (u_{0r}^m)_r^n \end{gathered} \tag{1.4}$$

будет прямым следствием правила (1.3).

Так как в полугруппах левые и правые степени элемента совпадают, то выполнение одного из правил степеней (1.3) повлечет выполнение равенства $u_{0l}^n = u_{0r}^n$, из которого будет следовать равенство полугрупп $\langle U_0^l, (*)\rangle$ и $\langle U_0^r, (*)\rangle$.

Полугруппу с нейтральным элементом называют моноидом. В моноидах определяют нулевую степень элементов $u \in U$, полагая $u^0 = e$. В моноидах с сокращением не существует идемпотентов, отличных от нейтрального элемента. В моноидах правила степеней обобщаются на случай показателей $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Если в полугруппе одновременно существуют левый и правый обратные элементы для некоторого элемента $u \in U$, то они совпадают, единственны, и в таком случае элемент $u' = u'_l = u'_r$ называется

обратным по операции $*$ к элементу $u$, а сам элемент $u$ называется обратимым. Обратный элемент, очевидно, существует для нейтрального и совпадает с ним. Идемпотент, отличный от нейтрального, не обратим. Если в полугруппе для элементов $u_1, u_2 \in U$ существуют левые (правые) обратные $(u_1)'_l, (u_2)'_l$ ($(u_1)'_r, (u_2)'_r$), то существует и левый (правый) обратный к $u_1 * u_2$, причем $(u_1 * u_2)'_l = (u_2)'_l * (u_1)'_l$ ($(u_1 * u_2)'_r = (u_2)'_r * (u_1)'_r$).

Моноид, в котором для каждого элемента существует обратный, называется группой. В группах не существует идемпотентов, отличных от нейтрального элемента. В группах определяют отрицательные степени элементов $u \in U$, полагая $u^{-n} = (u')^n$, где $n \in \mathbb{N}$.

Правила неотрицательных степеней, справедливые для полугрупп, распространяются на целые показатели степеней в группах.

**Утверждение 1.4.** Алгебра 2-местных отношений $\langle 2^{U^2}, (\bullet, \mathbb{I}_U)\rangle$ является полугруппой с единицей (моноидом).

**Утверждение 1.5.** Алгебра преобразований $\langle U^U, (\bullet, \mathbb{I}_U)\rangle$ является подмоноидом моноида $\langle 2^{U^2}, (\bullet, \mathbb{I}_U)\rangle$.

**Утверждение 1.6.** Алгебра подстановок $\langle B_U, (\bullet, \mathbb{I}_U)\rangle$ является подгруппой моноида $\langle U^U, (\bullet, \mathbb{I}_U)\rangle$. При этом для произвольного $F \in B_U$ выполняются равенства $F \bullet F^{-1} = F^{-1} \bullet F = \mathbb{I}_U$.

Несмотря на то что алгебры $\langle 2^{U^2}, (\cup, \cap, {}^-, \emptyset, U^2, \bullet, {}^{-1}, \mathbb{I}_U)\rangle$ и $\langle 2^{U^2}, (\cup, \cap, {}^-, \emptyset, U^2, \circ, {}^{-1}, \mathbb{I}_U)\rangle$ изоморфны, моноиды $\langle U^U, (\bullet, \mathbb{I}_U)\rangle$ и $\langle U^U, (\circ, \mathbb{I}_U)\rangle$ в общем случае таковыми не являются. Дело в том, что множество преобразований $U^U \subset 2^{U^2}$ незамкнуто относительно операции ${}^{-1}$, при помощи которой задается изоморфизм $F(R) = R^{-1}$, если $|U| > 1$. Однако множество подстановок $B_U \subset U^U \subset 2^{U^2}$ уже обладает свойством замкнутости, и, следовательно, группы $\langle B_U, (\bullet, \mathbb{I}_U)\rangle$ и $\langle B_U, (\circ, \mathbb{I}_U)\rangle$ изоморфны. Эти группы принято называть симметрическими группами множества $U$.

**Утверждение 1.7.** Любая полугруппа (группоид) $\langle U, (\star)\rangle$ изоморфно вложима в моноид (группоид с единицей) $\langle U \cup \{e\}, (*, e)\rangle$, где $e \notin U$, и $\forall u_1, u_2 \in U\ u_1 * u_2 = u_1 \star u_2$, и $\forall u \in U \cup \{e\}\ e * u = u * e = u$.

**Утверждение 1.8. (Кэли)** Любой моноид $\langle U, (*, e)\rangle$ изоморфно вложим в моноид преобразований $\langle U^U, (\bullet, \mathbb{I}_U)\rangle$ с операцией произведения, причем мономорфизм этого вложения задает инъекция $F^* : U \to \to U^U$, где $f^*_{\tilde{u}} = F^*(\tilde{u})$, и $f^*_{\tilde{u}}(u) = u * \tilde{u}$. Аналогичное справедливо и для моноида $\langle U^U, (\circ, \mathbb{I}_U)\rangle$ с операцией суперпозиции, где $g^*_{\tilde{u}} = G^*(\tilde{u})$, и $g^*_{\tilde{u}}(u) = \tilde{u} * u$.

**Замечание 1.2.** В теории квазигрупп преобразование $u \mapsto u * \tilde{u}$ называют правой трансляцией группоида $\langle U, (*)\rangle$ относительно элемента $\tilde{u} \in U$, а преобразование $u \mapsto \tilde{u} * u$ — левой трансляцией.

**Утверждение 1.9.** Пусть $\langle U, (*)\rangle$ — конечная полугруппа, $\langle U_0, (*)\rangle$ — циклическая полугруппа, порожденная произвольным элементом $u_0 \in U$, тогда существует идемпотент $u \in U_0$. Если $\langle U, (*, e)\rangle$ — конечная группа, то такой идемпотент единственен и совпадает с нейтральным $e$, при этом $\langle U_0, (*, e)\rangle$ — циклическая подгруппа группы $\langle U, (*, e)\rangle$, порожденная элементом $u_0 \in U$.

**Замечание 1.1.** Минимальную степень $m \in \mathbb{N}$ элемента $u_0 \in U$ моноида $\langle U, (*, e)\rangle$, для которой $u_0^m = e$, называют порядком элемента $u_0$ (в моноиде) и обозначают $\mathrm{ord}(u_0) = m$. Если такой степени не существует, то $\mathrm{ord}(u_0) = \infty$. Если элемент $u_0$ имеет конечный порядок $m$, то он обратим, и $u'_0 = = u_0^{m-1}$. Только для нейтрального элемента справедливо равенство $\mathrm{ord}(u_0) = 1$, причем $e' = e^0 = e$. Вполне понятно, что $(u^k)' = (u')^k$ для любого обратимого элемента $u_0 \in U$ и любого $k \in \mathbb{N}$, т. е. любая степень обратимого элемента обратима.

Если $\langle U_0, (*)\rangle$ — циклическая полугруппа, порожденная произвольным элементом $u_0 \in U$ из носителя моноида, и порядок элемента $u_0$ в этом моноиде конечен, то $\langle U_0, (*, e)\rangle$ — конечная группа, и $|U_0| = = \mathrm{ord}(u_0)$.

Обратное утверждение не верно. Например, если в носителе моноида имеется идемпотент $u_0$, отличный от нейтрального элемента $e$, то $\mathrm{ord}(u_0) = \infty$, но $|U_0| = 1$.

В конечных группах порядок любого элемента делит порядок группы.

**Утверждение 1.10.** Пусть $\langle U,(*,e)\rangle$ — конечный моноид, $u_0 \in U$ обратим, тогда циклическая полугруппа, порожденная элементом $u_0$, является группой.

**Утверждение 1.11.** Для любой полугруппы $\langle U,(*)\rangle$ следующие условия эквивалентны:

**G1.** $\langle U,(*)\rangle$ — группа;

**G2.** Для любых $u_2,u_3 \in U$ каждое из уравнений $u_2 * u = u_3$ и $u * u_2 = u_3$ однозначно разрешимо относительно $u$;

**G3.** Для любых $u_2,u_3 \in U$ каждое из уравнений $u_2 * u = u_3$ и $u * u_2 = u_3$ разрешимо относительно $u$;

**G4.** $\langle U,(*)\rangle$ является простой слева и справа;

**G5.** Существует левый (правый) нейтральный элемент $e_l \in U$ ($e_r \in U$), относительно которого для каждого элемента $u \in U$ существует левый (правый) обратный элемент $u'_l$ ($u'_r$), т. е. такой, что $u'_l * u = e_l$ ($u * u'_r = e_r$).

**Утверждение 1.12.** Любая группа является моноидом и полугруппой с сокращением. Обратное верно только для конечных моноидов. Примером моноида с сокращением, который не является группой, может служить мультипликативный моноид натуральных чисел $\langle \mathbb{N},(\cdot,1)\rangle$.

# 2. Основные результаты

Прежде чем приступить к рассмотрению бинарных операций как элементов носителей полугрупп, установим несколько простых фактов, относящихся к самим полугруппам и 3-местным отношениям.

## 2.1. Полугруппы и алгебры 3-местных отношений

В дальнейшем мы будем существенно использовать утверждение 1.8, которое позволяет изучать полугруппы $\langle U,(*)\rangle$ в терминах тотальных функций с операцией произведения, т. е. в терминах подмоноидов моноида преобразований $\langle U^U,(\bullet,\mathbb{I}_U)\rangle$.

Сначала докажем три простых, не претендующих на новизну, утверждения.

**Утверждение 2.1.** Пусть $R \in 2^{U\times V}$, $R' \in 2^{V\times U}$, $R \bullet R' = \mathbb{I}_U$, и $R' \bullet R = \mathbb{I}_V$, тогда $R' = R^{-1}$.

**Доказательство.** Так как $D_{\mathbb{I}_U} = U$, то $D_{R\bullet R'} = D_{\mathbb{I}_U} = U$. В силу свойства R13 можем записать $U = D_{R\bullet R'} \subseteq D_R \subseteq U$. Откуда следует, что $D_R = U$. Аналогично из свойства R14 следует, что $E_{R'} = V$.

В силу предположения свойств R5, R12 и R4 можем записать $R' = \mathbb{I}_V \bullet R' \subseteq R^{-1} \bullet R \bullet R' = R^{-1} \bullet \mathbb{I}_U = R^{-1}$.

Аналогично предыдущему $R = R \bullet \mathbb{I}_V \subseteq R \bullet R' \bullet (R')^{-1} = \mathbb{I}_U \bullet (R')^{-1} = (R')^{-1}$. Откуда в силу свойств R6 и R9 следует, что $R^{-1} \subseteq R'$.

Из полученного следует равенство $R' = R^{-1}$.■

Из определения 1.12 и утверждения 2.1 следует

**Утверждение 2.2.** В моноиде $\langle 2^{U^2},(\bullet,\mathbb{I}_U)\rangle$ обратимы подстановки и только они.

**Замечание 2.1.** Утверждения 2.1 и 2.2 останутся справедливыми после соответствующих замен операции $\bullet$ на операцию $\circ$.

Докажем утверждение, равносильное утверждению 1.12 для конечных полугрупп.

**Утверждение 2.3.** Любая конечная полугруппа $\langle U,(*)\rangle$, изоморфно вложимая в группу, сама является группой.

**Доказательство.** В силу утверждения 1.9 в полугруппе $\langle U,(*)\rangle$ будет существовать идемпотент. Так как эта полугруппа изоморфно вложима в группу, то идемпотент должен обладать свойствами нейтрального элемента и быть единственным, в противном случае он будет необратим. Обозначим этот элемент $e \in U$ и перейдем к рассмотрению моноида $\langle U,(*,e)\rangle$.

В силу утверждения 1.8 $\langle U,(*,e)\rangle \precsim \langle U^U,(\bullet,\mathbb{I}_U)\rangle$, причем мономорфизм $F^* : U \to U^U$, устанавливающий вложение $\tilde{u} \mapsto f^*_{\tilde{u}}$, задается правилом $f^*_{\tilde{u}}(u) = u * \tilde{u}$.

Обозначим $E_{F^*} = \{f^*_{\tilde{u}} \mid \tilde{u} \in U \wedge f^*_{\tilde{u}}(u) = u*\tilde{u}\}$ — множество значений $F^*$, тогда $\langle U, (*, e)\rangle \sim \langle E_{F^*}, (\bullet, \mathbb{I}_U)\rangle$.

Пусть $\langle U, (*, e)\rangle \precsim \langle V, (\star, \varepsilon)\rangle$, где $\langle V, (\star, \varepsilon)\rangle$ — группа, и $F : U \to V$ — мономорфизм, устанавливающий вложение полугруппы в группу. Без ограничения общности будем считать, что $E_F = U \subseteq V$ и $u\star\tilde{u} = u*\tilde{u}$ для всех $u, \tilde{u} \in U$.

В силу утверждения 1.5 $\langle V, (\star, \varepsilon)\rangle \precsim \langle V^V, (\bullet, \mathbb{I}_V)\rangle$, причем мономорфизм $F^\star$, устанавливающий вложение $\tilde{v} \mapsto f^\star_{\tilde{v}}$, задается правилом $f^\star_{\tilde{v}}(v) = v \star \tilde{v}$.

Обозначим $E_{F^\star} = \{f^\star_{\tilde{v}} \mid \tilde{v} \in V \wedge f_{\tilde{v}}(v) = v*\tilde{v}\}$ — множество значений $F^\star$, тогда $\langle V, (\star, \varepsilon)\rangle \sim \langle E_{F^\star}, (\bullet, \mathbb{I}_V)\rangle$.

В силу того, что $\langle V, (\star, \varepsilon)\rangle$ является группой, то моноид $\langle E_{F^\star}, (\bullet, \mathbb{I}_V)\rangle$ должен быть подгруппой симметрической группы подстановок $\langle B_V, (\bullet, \mathbb{I}_V)\rangle$.

Рассмотрим произвольный элемент $\tilde{u} \in E_F = U \subseteq V$ и соответствующую ему подстановку $f^\star_{\tilde{u}} : V \to V$. По построению ее значения определяются правилом $f^\star_{\tilde{u}}(v) = v\star\tilde{u}$, причем для всех $\tilde{u} \in E_F = U$ справедливо равенство $f^\star_{\tilde{u}}(u) = u\star\tilde{u} = u*\tilde{u} = f^*_{\tilde{u}}(u)$. Таким образом, функция $f^*_{\tilde{u}}$ является сужением подстановки $f^\star_{\tilde{u}}$ на множество $U \subseteq V$ и, следовательно, является тотальной инъекцией.

В общем случае функция $f^*_{\tilde{u}}$ может не быть сюръекцией. Однако если множество $U$ конечно, то, в силу утверждения 1.3, $f^*_{\tilde{u}}$ — подстановка и поэтому обратима. Из утверждения 1.10 будет следовать, что $\langle E_{F^*}, (\bullet, \mathbb{I}_U)\rangle$ — группа, и изоморфный ей моноид $\langle U, (*, e)\rangle$ также будет группой. ■

**Замечание 2.2.** Свойство правого сокращения

$$\forall u_1, u_2, u_3 \in U\ u_1 * u_3 = u_2 * u_3 \longrightarrow u_1 = u_2$$

эквивалентно свойству инъективности функции $f^*_{u_3}(u) = u * u_3$, а свойство левого сокращения

$$\forall u_1, u_2, u_3 \in U\ u_3 * u_1 = u_3 * u_2 \longrightarrow u_1 = u_2$$

эквивалентно свойству инъективности функции $g^*_{u_3}(u) = u_3 * u$. Причем в случае конечного моноида выполнение одного из этих свойств, ввиду обратимости $f^*_{u_3}$ или $g^*_{u_3}$, влечет выполнение другого.

**Замечание 2.3.** Пусть $F^* : U \to U^U$ и $G^* : U \to U^U$ — мономорфизмы моноида $\langle U, (*, e)\rangle$ и моноидов $\langle U^U, (\bullet, \mathbb{I}_U)\rangle$ и $\langle U^U, (\circ, \mathbb{I}_U)\rangle$, соответственно. Моноиды $\langle E_{F^*}, (\bullet, \mathbb{I}_U)\rangle$ и $\langle E_{G^*}, (\circ, \mathbb{I}_U)\rangle$ изоморфны только в тех случаях, когда они являются группами.

Далее мы будем следовать статье [28], в которой определялись и изучались операции над многоместными отношениями на множестве $U$.

Рассмотрим множество 3-местных отношений на $U$ и по аналогии с определениями 1.1–1.3 дадим следующие определения.

**Определение 2.1.** $^{1|3}$Транспозицией (по первому и третьему аргументам) 3-местного отношения $R \in 2^{U^3}$ называется 3-местное отношение $R^t \in 2^{U^3}$, определяемое правилом

$$R^t = \{(u_3, u_2, u_1) \mid u_1, u_2, u_3 \in U \wedge (u_1, u_2, u_3) \in R\}.$$

**Определение 2.2.** $^{1|3}$Композицией (по первому и третьему аргументам) 3-местных отношений $R_1 \in \in 2^{U^3}$ и $R_2 \in 2^{U^3}$ называется 3-местное отношение $R_1 \odot R_2 \in 2^{U^3}$, определяемое правилом

$$R_1 \odot R_2 = \{(u_1, u_2, u_3) \mid u_1, u_2, u_3 \in U \wedge \exists u_0 \in U\ (u_1, u_2, u_0) \in R_1 \wedge (u_0, u_2, u_3) \in R_2\}.$$

**Определение 2.3.** $^{1|3}$Инвариантным (по первому и третьему аргументам) 3-местным отношением на множестве $U$ называется 3-местное отношение $\mathcal{I}_U \in 2^{U^3}$, определяемое правилом

$$\mathcal{I}_U = \{(u, u_2, u) \mid u, u_2 \in U\}.$$

**Замечание 2.4.** Аналогичные определения могут быть даны для $^{2|3}$операций (по второму и третьему аргументам). Все дальнейшие рассуждения, которые будут проводиться для $^{1|3}$операций, легко переносятся и на этот случай (при соответствующих заменах операции $\bullet$ на операцию $\circ$). Для простоты изложения мы будем опускать верхние индексы в названиях операций, отношений и свойств всюду, кроме их определений.

По аналогии с определением 1.13, для каждого 3-местного отношения $R \in 2^{U^3}$ определим остовную функцию $F^0_R : U \to 2^{U^2}$, положив

$$F^0_R(u_2) = \{(u_1, u_3) \mid u_1, u_2, u_3 \in U \wedge (u_1, u_2, u_3) \in R\},$$

или, что то же самое,

$$F^0_R = \{(u_2,(u_1,u_3)) \equiv (u_2,u_1,u_3) \mid u_1,u_2,u_3 \in U \wedge (u_1,u_2,u_3) \in R\}.$$

Понятно, что если для всех элементов $u_2 \in U$ имеют место равенства $F^0_{R_1}(u_2) = F^0_{R_2}(u_2)$, то $R_1 = R_2$.

В силу определения $F^0_R$ для произвольного элемента $u_2 \in U$ выполняются легко проверяемые равенства

$$F^0_{R_1 \cup R_2}(u_2) = F^0_{R_1}(u_2) \cup F^0_{R_2}(u_2),$$
$$F^0_{R_1 \cap R_2}(u_2) = F^0_{R_1}(u_2) \cap F^0_{R_2}(u_2),$$
$$F^0_{\overline{R}}(u_2) = \overline{F^0_R(u_2)},$$
$$F^0_{\emptyset}(u_2) = \emptyset,$$
$$F^0_{U^3}(u_2) = U^2,$$
$$F^0_{R^t}(u_2) = (F^0_R(u_2))^{-1},$$
$$F^0_{R_1 \bullet R_2}(u_2) = F^0_{R_1}(u_2) \odot F^0_{R_2}(u_2),$$
$$F^0_{\mathcal{I}_U}(u_2) = \mathbb{I}_U.$$

**Замечание 2.5.** Из сказанного следует, что для каждого $R \in 2^{U^3}$ выполняются равенства

$$\mathcal{I}_U \odot R = R \odot \mathcal{I}_U = R,$$

а также другие свойства, аналогичные свойствам R1–R14 для операций из сигнатуры алгебры $\langle 2^{U^3}, (\cup, \cap, ^-, \emptyset, U^3, \odot, ^t, \mathcal{I}_U)\rangle$, в т. ч. и ассоциативность операции $\odot$.

Кроме того, определения 1.4–1.12 допускают подходящую переформулировку для 3-местных отношений на множестве $U$.

**Определение 2.4.** $^{1|3}$Областью определения 3-местного отношения $R \in 2^{U^3}$ будем называть множество

$$D_R = \bigcap_{u_2 \in U} D_{F^0_R(u_2)} \subseteq U.$$

**Определение 2.5.** $^{1|3}$Областью значений 3-местного отношения $R \in 2^{U^3}$ будем называть множество

$$E_R = \bigcap_{u_2 \in U} E_{F^0_R(u_2)} \subseteq U.$$

**Определение 2.6.** Левым $^1$сужением (по первому месту) 3-местного отношения $R \in 2^{U^3}$ на множество $U_0 \subset U$ называется 3-местное отношение $R_{U_0} \in 2^{U_0 \times U^2}$, определяемое правилом

$$R_{U_0} = \{(u_1,u_2,u_3) \mid u_1 \in U_0 \wedge u_2,u_3 \in U \wedge (u_1,u_2,u_3) \in R\}.$$

**Определение 2.7.** Центральным $^2$сужением (по второму месту) 3-местного отношения $R \in 2^{U^3}$ на множество $U_0 \subset U$ называется 3-местное отношение $R_{U_0} \in 2^{U_0 \times U^2}$, определяемое правилом

$$R_{U_0} = \{(u_1,u_2,u_3) \mid u_2 \in U_0 \wedge u_2,u_3 \in U \wedge (u_1,u_2,u_3) \in R\}.$$

**Определение 2.8.** Правым $^3$сужением (по третьему месту) 3-местного отношения $R \in 2^{U^2 \times U_0}$ на множество $U_0 \subset U$ называется 3-местное отношение $R^{U_0} \in 2^{U^2 \times U_0}$, определяемое правилом

$$R^{U_0} = \{(u_1,u_2,u_3) \mid u_1,u_2 \in U \wedge u_3 \in U_0 \wedge (u_1,u_2,u_3) \in R\}.$$

В тех случаях, когда это не приводит к недоразумениям, будем сохранять за сужениями $R_{U_0} \in 2^{U_0 \times U^2}$ и $R^{U_0} \in 2^{U^2 \times U_0}$ прежнее обозначение $R$.

**Определение 2.9.** Будем говорить, что 3-местное отношение $R \in 2^{U^3}$ $^1$тотально, если

$$D_R = U,$$

или, что то же самое,

$$\mathcal{I}_U \subseteq R \odot R^t.$$

Заметим, что в силу определений

$$D_R = \bigcap_{u_2 \in U} D_{F_R(u_2)} = \bigcap_{u_2 \in U} \{u_1 \mid u_1 \in U \wedge \exists u_0 \in U\ (u_1, u_2, u_0) \in R\} =$$
$$= \{u_1 \mid u_1 \in U \wedge \forall u_2 \in U \exists u_0 \in U\ (u_1, u_2, u_0) \in R\},$$

и условие выполнение равенства $D_R = U$ равносильно условиям

$$\forall u_1, u_2 \in U \exists u_0 \in U\ (u_1, u_2, u_0) \in R,$$
$$\forall (u_1, u_2) \in U \exists u_0 \in U\ ((u_1, u_2), u_0) \in R.$$

Таким образом, данное определение совпадает с определением тотальности $R \in 2^{U^2} \equiv 2^{U^2 \times U}$ как 2-местного отношения из $U^2$ в $U$ с учетом общепринятого соглашения $(u_1, u_2, u_3) \equiv ((u_1, u_2), u_3)$. Заметим, что тождественное отношение $\mathcal{I}_U$ тотально.

**Определение 2.10.** Будем говорить, что 3-местное отношение $R \in 2^{U^3}$ $^3$сюръективно, если

$$E_R = V,$$

или, что то же самое,

$$\mathcal{I}_U \subseteq R^t \odot R.$$

С учетом определения 2.1 можно утверждать, что 3-местное отношение сюръективно тогда и только тогда, когда его транспозиция тотальна, и наоборот.

Аналогично предыдущему условие сюръективности равносильно условиям

$$\forall u_2, u_3 \in U \exists u_0 \in U\ (u_0, u_2, u_3) \in R,$$
$$\forall (u_2, u_3) \in U \exists u_0 \in U\ (u_0, (u_2, u_3)) \in R.$$

**Определение 2.11.** Будем говорить, что 3-местное отношение $R \in 2^{U^3}$ $^{1|3}$функционально, если

$$\forall u_1, u_2 \in U \forall u_3, \tilde{u}_3 \in U\ (u_1, u_2, u_3) \in R \wedge (u_1, u_2, \tilde{u}_3) \in R \longrightarrow u_3 = \tilde{u}_3,$$

или, что то же самое,

$$R^t \odot R \subseteq \mathcal{I}_U.$$

Заметим, что данное определение совпадает с определением функции $F : U^2 \to U$ с учетом общепринятого соглашения $(u_1, u_2, u_3) \equiv ((u_1, u_2), u_3)$.

Будем обозначать множество тотальных функциональных 3-местных отношений (множество тотальных функций) из $U^2$ в $U$, как $U^{U^2}$.

В силу того, что $\mathcal{I}_U^t \odot \mathcal{I}_U = \mathcal{I}_U \odot \mathcal{I}_U^t = \mathcal{I}_U \odot \mathcal{I}_U = \mathcal{I}_U$, тождественное отношение $\mathcal{I}_U$ функционально. С учетом того, что оно тотально, $\mathcal{I}_U$ определяет бинарную операцию $u_1 \wr u_2 = u_1$. Операция $\wr$ ассоциативна, и полугруппу $\langle U, (\wr) \rangle$ часто называют полугруппой левых нулей (правых единиц), т. к. каждый элемент из носителя полугруппы является левым нулем (правой единицей). Понятно, что полугруппа левых нулей (правых единиц) является полугруппой с правым сокращением. Наряду с полугруппой левых нулей рассматривают полугруппу правых нулей (левых единиц) $\langle U, (\wr\!\wr) \rangle$ с операцией $u_1 \wr\!\wr u_2 = u_2$, и полугруппу $\langle U, (\dagger) \rangle$ с нулевым умножением $u_1 \dagger u_2 = \theta \in U$.

**Определение 2.12.** Будем говорить, что 3-местное отношение $R \in 2^{U^3}$ $^{1|3}$инъективно, если

$$\forall u_2, u_3 \in U \forall u_1, \tilde{u}_1 \in U\ (u_1, u_2, u_3) \in R \wedge (\tilde{u}_1, u_2, u_3) \in R \longrightarrow u_1 = \tilde{u}_1,$$

или, что то же самое,

$$R \odot R^t \subseteq \mathcal{I}_U.$$

С учетом определения 2.1 можно утверждать, что 3-местное отношение инъективно тогда и только тогда, когда его транспозиция функциональна, и наоборот. Таким образом, транспозиция функционального отношения $R \in 2^{U^3}$ функциональна тогда и только тогда, когда $R$ инъективно. Понятно, что инвариантное отношение $\mathcal{I}_U$ инъективно.

**Определение 2.13.** Будем говорить, что 3-местное отношение $R \in 2^{U^3}$ $^{1|3}$тотально биективно, если $R$ функционально, инъективно, сюръективно и тотально, или, что то же самое,

$$R \odot R^t = \mathcal{I}_U \wedge R^t \odot R = \mathcal{I}_U.$$

В силу определений транспозиция тотально биективного отношения тотально биективна, и наоборот, причем $R' = R^t$ — обратное к тотально биективному отношению $R \in 2^{U^3}$ по операции $\odot$. Тем самым множество тотально биективных отношений замкнуто относительно операции транспозиции. В дальнейшем мы будем обозначать его $B_{U^2} \subseteq U^{U^2}$. Понятно, что инвариантное отношение $\mathcal{I}_U$ тотально биективно.

**Замечание 2.6.** Как и в случае замечания 2.5, будет выполняться аналог утверждения 1.2 для операции $\odot$ в смысле определений 2.9–2.13. Это означает замкнутость множеств $U^{U^2}$ и $B_{U^2}$ относительно операции композиции $\odot$, и множества $B_{U^2}$ относительно операции транспозиции $^t$. Таким образом, $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$ — моноид, а $\langle B_{U^2}, (\odot, \mathcal{I}_U)\rangle$ — группа. В моноиде $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$ обратимы только тотально биективные отношения.

## 2.2. Индикаторы 3-местных отношений и алгебра двоичных массивов

Обозначим $\mathbb{D} = \{0, 1\}$– двухэлементное множество и рассмотрим множество $\mathbb{D}^U$ тотальных функций $\chi : U \to \mathbb{D}$. На множестве $\mathbb{D}^U$ определим операции $\sqcup$, $\sqcap$, $\neg$.

$$\begin{array}{c}(\chi_1 \sqcup \chi_2)(u) = \max(\chi_1(u), \chi_2(u)),\\ (\chi_1 \sqcap \chi_2)(u) = \min(\chi_1(u), \chi_2(u)),\\ (\neg\chi)(u) = \left\{\begin{array}{ll} 1\,, & \chi(u) = 0,\\ 0\,, & \chi(u) = 1.\end{array}\right.\end{array} \tag{2.1}$$

Алгебра $\langle 2^U, (\cup, \cap, ^-, \emptyset, U)\rangle$ изоморфна алгебре $\langle \mathbb{D}^U, (\sqcup, \sqcap, \neg, 0_U, 1_U)\rangle$, где $0_U(u) = 0$, $1_U(u) = 1$ для всех $u \in U$, а изоморфизм устанавливает функция $F : 2^U \to \mathbb{D}^U$,

$$F(U_1) = \chi_{U_1}(u) = \left\{\begin{array}{ll} 1\,, & u \in U_1,\\ 0\,, & u \notin U_1,\end{array}\right.$$

где $U_1 \in 2^U$.

Функция $\chi_{U_1}$ называется индикатором подмножества $U_1$.

Следуя [28], рассмотрим множество 3-местных отношений $2^{U^3}$ и множество их индикаторов $\mathbb{D}^{U^3}$.

На множестве $\mathbb{D}^{U^3}$ дополнительно определим операции $\diamond$, $\tau$.

$$\begin{array}{c}\chi^\tau(u_1, u_2, u_3) = \chi(u_3, u_2, u_1),\\ (\chi_1 \diamond \chi_2)(u_1, u_2, u_3) = \left\{\begin{array}{ll} 1\,, & \exists u_0 \in U\ \chi_1(u_1, u_2, u_0) = 1 \wedge \chi_2(u_0, u_2, u_3) = 1,\\ 0\,, & \forall u_0 \in U\ \chi_1(u_1, u_2, u_0) = 0 \vee \chi_2(u_0, u_2, u_3) = 0.\end{array}\right.\end{array} \tag{2.2}$$

Аналогично предыдущему алгебра $\langle 2^{U^3}, (\cup, \cap, ^-, \emptyset, U^3, \odot, ^t, \mathcal{I}_U)\rangle$ изоморфна алгебре $\langle \mathbb{D}^{U^3}, (\sqcup, \sqcap, \neg, 0_{U^3}, 1_{U^3}, \diamond, ^\tau, \iota_U)\rangle$, где

$$\iota_U(u_1, u_2, u_3) = \left\{\begin{array}{ll} 1\,, & u_1, u_2, u_3 \in U \wedge u_1 = u_3,\\ 0\,, & u_1, u_2, u_3 \in U \wedge u_1 \neq u_3.\end{array}\right.$$

В случае конечного множества $U = \{u_1, \ldots, u_m\}$ удобно использовать представление индикаторов $\mathbb{D}^{U^3}$ 3-индексными двоичными (логическими) массивами.

Для этого определим нумерацию $\eta : 1..m \to U$, как обычно, будем обозначать $\eta(i)$, как $u_i$, и определим

$$r_{ijk} = \chi_R(u_i, u_j, u_k), \tag{2.3}$$

где $i, j, k \in 1..m$.

Множество определенных таким образом 3-индексных двоичных массивов будем обозначать $\mathbb{D}^{[1..m]^3}$.

Операции алгебры $\langle \mathbb{D}^{U^3}, (\sqcup, \sqcap, \neg, 0_{U^3}, 1_{U^3}, \diamond, ^\tau, \iota_U)\rangle$ индуцируют соответствующие операции на $\mathbb{D}^{[1..m]^3}$

$$\begin{array}{c} r^1_{ijk} \sqcup r^2_{i,j,k} = (\chi_{R_1} \sqcup \chi_{R_2})(u_i, u_j, u_k),\\ r^1_{ijk} \sqcap r^2_{i,j,k} = (\chi_{R_1} \sqcap \chi_{R_2})(u_i, u_j, u_k),\\ \neg r_{ijk} = (\neg\chi_R)(u_i, u_j, u_k),\\ r^\tau_{ijk} = \chi^\tau(u_1, u_2, u_3),\\ r^1_{ijs} \diamond r^2_{s,j,k} = \max_{s \in 1..m}(\min(r^1_{ijs}, r^2_{sjk})).\end{array} \tag{2.4}$$

Таким образом, в случае конечного множества $U = \{u_1, \dots, u_m\}$ алгебра $\langle 2^{U^3}, (\cup, \cap, ^-, \emptyset, U^3, \odot, ^t, \mathcal{I}_U)\rangle$ изоморфна алгебре $\langle \mathbb{D}^{[1..m]^3}, (\sqcup, \sqcap, \neg, 0_{ijk}, 1_{ijk}, \diamond, ^\tau, \iota_{ijk})\rangle$, где

$$0_{ijk} = 0,\ i,j,k \in 1..m,$$

$$1_{ijk} = 1,\ i,j,k \in 1..m,$$

$$\iota_{ijk} = \begin{cases} 1\,, & i,j,k \in 1..m \wedge i = k, \\ 0\,, & i,j,k \in 1..m \wedge i \neq k. \end{cases}$$

**Замечание 2.7.** Заметим, что для представления двоичного массива $r_{ijk}$, где $i,j,k \in 1..m$, потребуется $m^3$ бит. В случае линейного представления битовым потоком наиболее просто реализуются побитовые операции $\sqcup$, $\sqcap$, $\neg$, и скорость их выполнения будет определяться в основном разрядностью процессора, реализующего битовые логические операции (дизъюнкция, конъюнкция, отрицание). Сложность реализации операций $\sqcup$, $\sqcap$, $\neg$ можно оценить как $O(m^3)$ логических операций.

Реализация операций $\diamond$, $^\tau$ потребует выделения не более $2m^3$ и $m^3$ дополнительных бит оперативной памяти, соответственно, для формирования выходного потока. Заметим также, что эти операции легко поддаются распараллеливанию. Для определения значения каждого из $m^3$ бит результата операции $\diamond$ потребуется выполнение не более $m$ битовых логических операций (дизъюнкция, конъюнкция). С учетом сказанного, сложность реализации операции $\diamond$ можно оценить как $O(m^4)$ логических операций, а сложность реализации операции $^\tau$ как $O(m^3)$ операций копирования.

## 2.3. Полугруппы бинарных операций

Применим сказанное выше к бинарным операциям на множестве $U$. Для обозначения результатов бинарных операций будем использовать равноправные инфиксное $u_3 = u_1 * u_2$ и префиксное $u_3 = \phi_*(u_1, u_2)$, $(u_1, u_2, u_3) \in \phi_*$ обозначения. Любая бинарная операция по определению обладает свойствами тотальности и функциональности, т. е. является элементом носителя моноида $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$. Условия тотальности и функциональности в смысле определений 1.8 и 1.10 записываются в следующей форме:

$$\forall u_1, u_2 \in U \exists u_0 \in U\ (u_1, u_2, u_0) \in \phi_*,$$

$$\forall u_1, u_2, u_3, \tilde{u}_3\ (u_1, u_2, u_3) \in \phi_* \wedge (u_1, u_2, \tilde{u}_3) \in \phi_* \longrightarrow u_3 = \tilde{u}_3.$$

Выше мы отмечали, что определения 1.8 и 2.9 так же, как и определения 1.10 и 2.11, равносильны.

Если операция $\phi_* : U^2 \to U$ сюръективна, то выполняется дополнительное условие

$$\forall u_2, u_3 \in U \exists u_0 \in U\ (u_0, u_2, u_3) \in \phi_*.$$

Если операция $\phi_* : U^2 \to U$ инъективна, то выполняется дополнительное условие

$$\forall u_1, \tilde{u}_1, u_2, u_3,\ (u_1, u_2, u_3) \in \phi_* \wedge (\tilde{u}_1, u_2, u_3) \in \phi_* \longrightarrow u_1 = \tilde{u}_1.$$

Или в инфиксной форме

$$\forall u_1, u_2 \in U \exists u_0 \in U\ u_0 = u_1 * u_2,$$

$$\forall u_1, u_2, u_3, \tilde{u}_3\ u_3 = u_1 * u_2 \wedge \tilde{u}_3 = u_1 * u_2 \longrightarrow u_3 = \tilde{u}_3,$$

$$\forall u_2, u_3 \in U \exists u_0 \in U\ u_3 = u_0 * u_2,$$

$$\forall u_1, \tilde{u}_1, u_2, u_3,\ u_3 = u_1 * u_2 \wedge u_3 = \tilde{u}_1 * u_2 \longrightarrow u_1 = \tilde{u}_1.$$

Заметим, что значения остовной функции $F^0_{\phi_*} : U \to 2^{U^2}$ могут быть представлены в виде

$$F^0_{\phi_*}(u_2) = \{(u_1, u_3) \mid u_1, u_2, u_3 \in U \wedge u_3 = u_1 * u_2\} = f^*_{u_2},$$

где, как и ранее, $f^*_{u_2}(u_1) = u_1 * u_2 = u_3$.

**Замечание 2.8.** Нетрудно заметить, что если операция $\phi_*$ инъективна, то $\langle U, (*)\rangle$ — группоид с правым сокращением. Если операция $\phi_*$ сюръективна, то $\langle U, (*)\rangle$ — группоид с правым делением. Если операция $\phi_*$ и инъективна, и сюръективна, то $\langle U, (*)\rangle$ — правая квазигруппа.

Таким образом, любой группоид с тотально биективной операцией $\phi_* \in B_{U^2}$ является правой квазигруппой, и наоборот.

**Замечание 2.9.** Тотальность ассоциативной операции $\phi_*$ эквивалентна тотальности каждой функции $f^*_{u_2}$ в смысле определения 1.8. Сюръективность операции $\phi_*$ эквивалентна сюръективности каждой функции $f^*_{u_2}$ в смысле определения 1.9. Инъективность операции $\phi_*$ эквивалентна инъективности каждой функции $f^*_{u_2}$ в смысле определения 1.11. Тотальная биективность операции $\phi_*$ эквивалентна тому, что каждая функция $f^*_{u_2}$ является подстановкой, т. е. обратима относительно операции $\bullet$ как элемент носителя группы $\langle B_U, (\bullet, \mathbb{I}_U)\rangle$. Причем в силу утверждения 2.1 обратная функция $(f^*_{u_2})' = (f^*_{u_2})^{-1}$ в смысле определения 1.1. С учетом свойств остовной функции будет выполняться равенство $(f^*_{u_2})^{-1} = F^0_{\phi^t_*}(u_2)$.

Рассмотрим пару бинарных операций $\phi_*, \phi_\star \in U^{U^2}$ и их композицию

$$\phi_\star \odot \phi_* = \{(u_1, u_2, u_3) \mid u_1, u_2, u_3 \in U \wedge \exists u_0 \in U\ (u_1, u_2, u_0) \in \phi_\star \wedge (u_0, u_2, u_3) \in \phi_*\},$$

или, что то же самое,

$$u_3 = \phi_\star \odot \phi_*(u_1, u_2) = \phi_*(\phi_\star(u_1, u_2), u_2) = (u_1 \star u_2) * u_2. \tag{2.5}$$

Стандартным образом определим положительную степень

$$\phi^1_* = \phi_* \wedge \phi^{n+1}_* = \phi^n_* \odot \phi_* = \phi_* \odot \phi^n_*,$$

где $n \in \mathbb{N}$.

Тогда по определению

$$\begin{aligned} u_3 = \phi^n_*(u_1, u_2) = \phi_* \odot \phi^{n-1}_*(u_1, u_2) = \phi_*(\phi^{n-1}_*(u_1, u_2), u_2) = \phi^{n-1}_*(u_1, u_2) * u_2 = \\ = (\phi_*(\phi^{n-2}_*(u_1, u_2), u_2)) * u_2 = (\phi^{n-2}_*(u_1, u_2) * u_2) * u_2 = \ldots = \underbrace{(\ldots((u_1 * u_2) * u_2) * \ldots) * u_2}_{n}. \end{aligned} \tag{2.6}$$

Полагая в (2.6) $u_1 = u_2 = u$, получаем

$$\phi^n_*(u, u) = u^{n+1}_r. \tag{2.7}$$

Если существует левый нейтральный элемент $e_l$ относительно операции $\phi_*$, то, полагая в (2.6) $u_1 = e_l$ и $u_2 = u$, получаем

$$\phi^n_*(e_l, u) = u^n_r. \tag{2.8}$$

Заметим, что $\phi^n_*(u, e_r) = u$, т. е. правый нейтральный элемент относительно операции $\phi_*$ продолжает оставаться правым нейтральным относительно операции $\phi^n_*$.

Для ассоциативной операции $\phi_*$ можем записать

$$u_3 = \phi^n_*(u_1, u_2) = \phi_*(\phi^{n-1}_*(u_1, u_2), u_2) = \phi^{n-1}_*(u_1, u_2) * u_2 = u_1 * u^n_2. \tag{2.9}$$

Полагая в (2.7) $u_1 = u_2 = u$, получаем

$$\phi^n_*(u, u) = u^{n+1}. \tag{2.10}$$

По аналогии с (2.8) можем записать

$$\phi^n_*(e_l, u) = u^n. \tag{2.11}$$

## 2.4. Тотально биективные операции и правые квазигруппы

Предположим теперь, что бинарная операция $\phi_*$ тотально биективна, т. е. в силу замечания 2.8 $\langle U, (*)\rangle$ — правая квазигруппа.

В таком случае $\phi_* \in B_{U^2}$, и поэтому обратима как элемент группы $\langle B_{U^2}, (\odot, \mathcal{I}_U)\rangle$. Обратный к ней элемент в этой группе $\phi'_* = \phi^t_*$, следовательно,

$$\phi_* \odot \phi^t_* = \phi^t_* \odot \phi_* = \mathcal{I}_U,$$

$\phi^t_* \in B_{U^2}$ обладает свойством тотальной биективности, т. е. задает бинарную операцию на $U$. По определению график этой операции имеет вид

$$\phi^t_* = \{(u_3, u_2, u_1) \mid u_1, u_2, u_3 \in U \wedge (u_1, u_2, u_3) \in \phi_*\}.$$

Последнее означает, что

$$(u_3, u_2, u_1) \in \phi^t_* \iff (u_1, u_2, u_3) \in \phi_*,$$

или, что то же самое,

$$u_1 = u_3 *^t u_2 \iff u_3 = u_1 * u_2,$$

для произвольных элементов $u_1, u_2, u_3 \in U$. Следовательно, операции $\phi_*$ и $\phi_*^t$ взаимно обратны справа.

В дальнейшем будем обозначать $\phi_*^t$ как $\phi_\div$, таким образом,

$$\phi_* \odot \phi_\div = \phi_\div \odot \phi_* = \mathcal{I}_U, \tag{2.12}$$

где

$$u_1 = u_3 \div u_2 \Longleftrightarrow u_3 = u_1 * u_2. \tag{2.13}$$

**Замечание 2.10.** В силу того, что множество бинарных операций $U^{U^2}$ незамкнуто относительно операции транспозиции $^t$, транспозиция бинарной операции $\phi_* \in U^{U^2}$ может не обладать свойствами тотальности и функциональности, т. е. 3-местное отношение $\phi_*^t$ может не определять взаимно обратную с $\phi_*$ бинарную операцию на $U$. Например, в случае полугруппы с нулевым умножением $u_1 \dagger u_2 = \theta \in U$ транспозиция $\phi_\dagger^t$ не будет функциональной, если $|U| > 1$. Для аддитивной полугруппы $\langle \mathbb{N}, (+) \rangle$ транспозиция $\phi_+^t$ хотя и будет функциональной, но не будет тотальной. Заметим, что операция $\phi_\div = \phi_*^t$, взаимно обратная с операцией $\phi_* \in U^{U^2}$, существует тогда и только тогда, когда $\phi_* \in B_{U^2}$, т. е. тотально биективна. При этом $\phi_\div \in B_{U^2}$, т. е. тотально биективна. В частности, операция полугруппы левых нулей (правых единиц) $\langle U, (\wr) \rangle$ взаимно обратна справа с собой. С учетом замечания 2.2 $\langle U, (*) \rangle$ и $\langle U, (\div) \rangle$ — правые квазигруппы. Квазигруппу $\langle U, (\div) \rangle$ будем называть $^{1|3}$парастрофом квазигруппы $\langle U, (*) \rangle$.

С учетом (2.5) можем записать (2.12) в эквивалентной форме

$$u_1 \wr u_2 = u_1 = (u_1 * u_2) \div u_2 = (u_1 \div u_2) * u_2 \tag{2.14}$$

для любых элементов $u_1, u_2 \in U$.

**Определение 2.14.** Будем говорить, что операция $\div$ нейтрализует операцию $*$ справа, если

$$(u_1 * u_2) \div u_2 = u_1$$

для любых элементов $u_1, u_2 \in U$.

Таким образом, справедливо

**Утверждение 2.4.** Тотально биективные операции $*$ и $\div$ взаимно обратны справа тогда и только тогда, когда они взаимно нейтрализуют друг друга справа.

Допустим, что в правой квазигруппе $\langle U, (*) \rangle$ имеется левый нейтральный элемент $e_l \in U$, тогда, полагая в (2.14) $u_1 = e_l$, получаем

$$e_l = u_2 \div u_2 = (e_l \div u_2) * u_2.$$

Таким образом, $e_l \div u_2$ является левым обратным к $u_2$ в правой квазигруппе $\langle U, (*) \rangle$. Тем самым справедливо

**Утверждение 2.5.** Пусть $\langle U, (*, e_l) \rangle$ — правая квазигруппа с левым нейтральным элементом, тогда каждый элемент $u \in U$ имеет левый обратный $u'_l = e_l \div u$ по операции $*$, причем $e_l = u \div u$.

Допустим, что в правой квазигруппе $\langle U, (*) \rangle$ имеется правый нейтральный элемент $e_r \in U$, тогда, полагая в (2.14) $u_2 = e_r$, получаем:

$$u_1 = u_1 \div e_r.$$

Таким образом, $e_r$ — правый нейтральный элемент по операции $\div$. Тем самым справедливо

**Утверждение 2.6.** Пусть $\langle U, (*, e_r) \rangle$ — правая квазигруппа с правым нейтральным элементом, тогда ее парастроф $\langle U, (\div, e_r) \rangle$ — правая квазигруппа с правым нейтральным элементом.

Допустим, что в правой квазигруппе $\langle U, (*) \rangle$ имеется нейтральный элемент $e \in U$, тогда с учетом утверждений 2.5 и 2.6 для любого элемента $u \in U$ выполняются равенства:

$$u = u \div e,$$

$$e = u \div u = (e \div u) * u,$$

и тем самым справедливо

**Утверждение 2.7.** Пусть $\langle U, (*, e)\rangle$ — правая лупа, тогда ее парастроф $\langle U, (\div, \varepsilon_r)\rangle$ — правая квазигруппа с правым нейтральным элементом $\varepsilon_r = e$, каждый элемент $u \in U$ имеет левый обратный $u'_l = e \div u$ по операции $*$, и каждый элемент $u \in U$ является обратным к себе по операции $\div$.

Допустим теперь, что в правой квазигруппе $\langle U, (*)\rangle$ и ее парастрофе $\langle U, (\div)\rangle$ имеются нейтральные элементы $e \in U$ и $\varepsilon \in U$, соответственно. Тогда из утверждения 2.6 следует, что $\varepsilon = e$. Поэтому для всех элементов $u \in U$ должны выполняться равенства $u \div e = e \div u = u$. В силу определения операции $\div$, из последнего следует, что $u * u = e$. Кроме того, из утверждения 2.5 следует, что $u \div u = e$. Тем самым справедливо

**Утверждение 2.8.** Пусть $\langle U, (*, e)\rangle$ — правая лупа, и ее парастроф $\langle U, (\div)\rangle$ — правая лупа, тогда $\varepsilon = e$, и каждый элемент $u \in U$ является обратным к себе по операциям $*$ и $\div$.

Из утверждений 1.11 и 2.7 следует

**Утверждение 2.9.** Пусть $\langle U, (*, e)\rangle$ — правая лупа с ассоциативной операцией, тогда $\langle U, (*, e)\rangle$ — группа.

Справедливо и обратное

**Утверждение 2.10.** Пусть $\langle U, (*, e)\rangle$ — группа, тогда операция $*$ тотально биективна, причем взаимно обратная с ней справа операция $\div$ задается правилом $u_1 = u_3 \div u_2 = u_3 * u'_2$.

**Доказательство.** Операция $*$ тотальна и функциональна по своему определению. Сюръективность и инъективность этой операции следуют из обратимости элементов множества $U$.

По определению операции, взаимно обратной справа с операцией $*$, равенство

$$u_1 = u_3 \div u_2$$

равносильно равенству

$$u_3 = u_1 * u_2.$$

Из последнего равенства и обратимости элемента $u_2$ следует равносильность обоих равенств равенству

$$u_3 * u'_2 = u_1 * u_2 * u'_2 = u_1 * e = u_1,$$

т. е. равносильность равенств $u_1 = u_3 \div u_2$ и $u_1 = u_3 * u'_2$. Откуда следует равенство $u_3 \div u_2 = u_3 * u'_2$, для всех $u_2, u_3 \in U$, для которых определена правая часть $u_3 * u'_2$, т. е. в силу определения группы, для любых $u_2, u_3 \in U$.■

**Замечание 2.11.** Таким образом, любая правая лупа с ассоциативной операцией является группой, и наоборот. Однако, если в правой квазигруппе отсутствует нейтральный элемент, она может не допускать изоморфного вложения в группу, хотя и будет изоморфно вложима в моноид. Например, полугруппа с правым сокращением $\langle U, (\wr)\rangle$ не допускает изоморфного вложения в группу (если $|U| > 1$), хотя операция $\wr$ тотально биективна и взаимно обратна справа с собой.

Понятно, что операция, взаимно обратная справа с ассоциативной операцией, в общем случае не ассоциативна. Более того, справедливо следующее

**Утверждение 2.11.** Пусть $\langle U, (*, e)\rangle$ — моноид, в таком случае операция $\div$, взаимно обратная справа с операцией $*$, ассоциативна тогда и только тогда, когда $\langle U, (*, e)\rangle$ — группа, $u * u = e$, и $\phi_* = \phi_\div$.

**Доказательство.** Достаточность очевидна. Докажем необходимость. Пусть операция $\div$ ассоциативна, тогда

$$u_1 \div (u_2 \div u_3) = (u_1 \div u_2) \div u_3$$

для произвольных элементов $u_1, u_2, u_3 \in U$, или в префиксной форме:

$$\forall u_1, u_2, u_3 \exists u_0, \tilde{u}_0, u_4\ (u_1, u_0, u_4) \in \phi_\div \wedge (u_2, u_3, u_0) \in \phi_\div \wedge (u_1, u_2, \tilde{u}_0) \in \phi_\div \wedge (\tilde{u}_0, u_3, u_4) \in \phi_\div.$$

С учетом определения $\phi_{\div}$ получаем:

$$\forall u_1, u_2, u_3 \exists u_0, \tilde{u}_0, u_4\ (u_4, u_0, u_1) \in \phi_* \wedge (u_0, u_3, u_2) \in \phi_* \wedge (\tilde{u}_0, u_2, u_1) \in \phi_* \wedge (u_4, u_3, \tilde{u}_0) \in \phi_*,$$

или, что то же самое,

$$\forall u_1, u_2, u_3 \exists u_0, \tilde{u}_0, u_4\ (u_4 * u_0 = u_1 \wedge u_0 * u_3 = u_2) \wedge (\tilde{u}_0 * u_2 = u_1 \wedge u_4 * u_3 = \tilde{u}_0).$$

Из пар равенств, заключенных в скобки, следует, что

$$\forall u_1, u_2, u_3 \exists u_0, u_4\ (u_4 * u_2 = u_4 * u_0 * u_3 = u_1 * u_3) \wedge (u_4 * u_3 * u_2 = u_1),$$

поэтому

$$\forall u_1, u_2, u_3 \exists u_4\ (u_4 * u_2 = u_1 * u_3) \wedge (u_4 * u_3 * u_2 = u_1).$$

Полагая $u_1 = u_2 = e$, получаем

$$\forall u_3 \exists u_4\ (u_4 = u_3) \wedge (u_4 * u_3 = e).$$

Следовательно,

$$\forall u_3\ u_3 * u_3 = e.$$

Таким образом, каждый элемент $u \in U$ является обратным к самому себе по операции $*$, т. е. $\langle U, (*, e)\rangle$ — группа, и $u' = u$. В силу утверждения 2.10 это означает справедливость равенства $u_1 \div u_2 = u_1 * u_2' = u_1 * u_2$ для любых $u_1, u_2 \in U$, т. е. $\phi_* = \phi_{\div}$.■

## 2.5. Циклические полугруппы бинарных операций

Рассмотрим группоид $\langle U, (*)\rangle$ и циклическую полугруппу $\langle \Phi_*, (\odot)\rangle$, порожденную операцией $*$. Здесь $\Phi_* = \{\phi_*^n \mid \phi_*^1 = \phi_* \wedge \phi_*^n = \phi_*^{n-1} \odot \phi_* \wedge n \in \mathbb{N}\}$.

Будем считать, что группоид конечен, т. е. $U = \{u_1, \ldots, u_m\}$. Так как $\Phi_* \subseteq U^{U^2}$, то $|\Phi_*| \leqslant |U|^{|U|^2} = m^{m^2}$, носитель полугруппы $\Phi_*$ также конечен, и в силу утверждения 1.9 в полугруппе $\langle \Phi_*, (\odot)\rangle$ будет существовать идемпотент $\phi_*^s \in \Phi_*$, т. е. такая операция, что $\phi_*^s \odot \phi_*^s = \phi_*^{2s} = \phi_*^s$, или, что то же самое

$$\phi_*^s \odot \phi_*^s(u_1, u_2) = \phi_*^s(\phi_*^s(u_1, u_2), u_2) = \phi_*^{2s}(u_1, u_2) = \phi_*^s(u_1, u_2),$$

сразу для всех элементов $u_1, u_2 \in U$.

Пользуясь представлением (2.7), заключаем, что существует такой показатель правой степени $s \in \mathbb{N}$, что

$$\phi_*^{2s}(u, u) = u_r^{2s+1} = u_r^{s+1} = \phi_*^s(u, u),$$

сразу для всех элементов $u \in U$. Для группоидов с левой единицей из (2.8) будет следовать равенство

$$\phi_*^{2s}(e_l, u) = u_r^{2s} = u_r^s = \phi_*^s(e_l, u).$$

Пусть теперь $\langle U, (*)\rangle$ — правая квазигруппа (не обязательно конечная). Тогда $\langle \Phi_* \cup \Phi_{\div} \cup \{\mathcal{I}_U\}, (\odot, \mathcal{I}_U)\rangle$ — подгруппа группы $\langle B_{U^2}, (\odot, \mathcal{I}_U)\rangle$. Здесь $\Phi_{\div} = \{\phi_{\div}^n \mid \phi_{\div}^1 = \phi_{\div} \wedge \phi_{\div}^n = \phi_{\div}^{n-1} \odot \phi_{\div} \wedge n \in \mathbb{N}\}$.

Если множество $U$ конечно, то из утверждения 2.3 следует, что $\langle \Phi_*, (\odot, \mathcal{I}_U)\rangle$ — циклическая группа, и ее порядок $|\Phi_*|$, в силу замечания 1.2, равен порядку элемента $\phi_*$ в группе $\langle B_{U^2}, (\odot, \mathcal{I}_U)\rangle$. Таким образом, $|\Phi_*| = \operatorname{ord}(\phi_*)$. Обозначим $s = \operatorname{ord}(\phi_*)$, тогда

$$\phi_*^s = \mathcal{I}_U,$$

или, что то же самое,

$$\phi_*^s(u_1, u_2) = \underbrace{(\ldots((u_1 * u_2) * u_2) * \ldots) * u_2}_{s} = u_1 = u_1 \wr u_2$$

для любых $u_1, u_2 \in U$.

Из (2.7) получаем, что

$$\phi_*^s(u, u) = u_r^{s+1} = u$$

сразу для всех элементов $u \in U$.

Если $\langle U, (*, e_l)\rangle$ — левая лупа, то из (2.7) получаем, что

$$\phi_*^s(e_l, u) = u_r^s = e_l,$$

и если $\langle U, (*, e)\rangle$ — лупа, то

$$\phi_*^s(e, u) = u_r^s = e.$$

Если дополнительно предположить ассоциативность квазигрупповой операции $*$, то

$$u^s = e$$

сразу для всех элементов $u \in U$. Напомним, что в этом случае $\langle U, (*, e)\rangle$ — правая лупа, т. е. в силу утверждения 2.9 является группой.

Таким образом, порядок любого элемента конечной группы $\langle U, (*, e)\rangle$ делит порядок циклической группы $\langle \Phi_*, (\odot, \mathcal{I}_U)\rangle$.

На самом деле несложно выразить порядок $|\Phi_*|$ через порядки элементов конечной группы $\langle U, (*, e)\rangle$.

Действительно, пусть $U = \{u_1, \dots, u_m\}$ и $k_i = \mathrm{ord}(u_i)$, $i \in 1..m$. Положим $\tilde{s} = \mathrm{НОК}(k_1, \dots k_m)$ и обозначим $s_i = \tilde{s}/k_i$. Понятно, что

$$u_i^s = u_i^{k_i s_i} = (u_i^{k_i})^{s_i} = e^{s_i} = e$$

сразу для всех элементов $u_i \in U$. Откуда следует, что

$$\phi_*^{\tilde{s}} = \mathcal{I}_U,$$

т. е. $\tilde{s} \geqslant \mathrm{ord}(\phi_*) = s$.

Если предположить, что $\tilde{s} > s$, то в этом случае найдется элемент $u_i \in U$, порядок которого $k_i < s$ не делит $s$, и одновременно

$$e = u_i^s = u_i^{qk_i + r} = (u_i^{k_i})^q * u_i^r = e^q * u_i^r = e * u_i^r = u_i^r,$$

где $0 < r < k_i = \mathrm{ord}(u_i)$. Последнее противоречит определению $\mathrm{ord}(u_i)$, и поэтому $s = \tilde{s} = \mathrm{НОК}(k_1, \dots k_m)$.

Тем самым справедливо

**Утверждение 2.12.** Пусть $\langle U, (*, e)\rangle$ — конечная группа, где $U = \{u_1, \dots, u_m\}$ и $k_i = \mathrm{ord}(u_i)$, $i \in 1..m$. Тогда порядок циклической группы $\langle \Phi_*, (\odot, \mathcal{I}_U)\rangle$ равен $\mathrm{НОК}(k_1, \dots k_m)$.

Теперь рассмотрим пару группоидов $\langle U, (\star)\rangle$, $\langle U, (*)\rangle$ и определим композицию их операций $\phi_\otimes = \phi_\star \odot \phi_*$. Учитывая представление (2.5), можем записать

$$u_3 = u_1 \otimes u_2 = \phi_\otimes(u_1, u_2) = \phi_\star \odot \phi_*(u_1, u_2) = \phi_*(\phi_\star(u_1, u_2), u_2) = (u_1 \star u_2) * u_2$$

сразу для всех элементов $u_1, u_2 \in U$.

Отметим несколько очевидных свойств операции $\otimes$, которые определяются свойствами операций $\star$ и $*$.

1. Если операция $*$ нейтрализует операцию $\star$ справа, то

   $$u_1 \otimes u_2 = (u_1 \star u_2) * u_2 = u_1 = u_1 \wr u_2$$

   сразу для всех элементов $u_1, u_2 \in U$. Поэтому группоид $\langle U, (\otimes)\rangle$ есть не что иное, как полугруппа $\langle U, (\wr)\rangle$ левых нулей (правых единиц), и имеет место равенство

   $$\phi_\star \odot \phi_* = \mathcal{I}_U.$$

   Это означает, что $\phi_\star$– левый обратный элемент к $\phi_*$, а $\phi_*$– правый обратный элемент к $\phi_\star$ в моноиде $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$.

   Если операции $*$ и $\star$ взаимно нейтрализуют друг друга справа, то они обратны друг к другу как элементы моноида $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$, т. е.

   $$\phi_\star \odot \phi_* = \phi_* \odot \phi_\star = \mathcal{I}_U.$$

   Так как в моноиде $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$ обратимы только тотально биективные операции, то операции $\phi_\star, \phi_* \in B_{U^2}$ взаимно обратны, и $\langle U, (\star)\rangle$, $\langle U, (*)\rangle$ — квазигруппы.

   Понятно, что в этом случае порядок циклической полугруппы $\langle \Phi_\wr, (\odot)\rangle$, порожденной операцией $\wr$, равен 1.

2. Если операция $*$ поглощает операцию $\star$ справа, то

   $$u_1 \otimes u_2 = (u_1 \star u_2) * u_2 = u_2 = u_1 \wr\!\!\wr u_2,$$

сразу для всех элементов $u_1, u_2 \in U$. Поэтому группоид $\langle U, (\otimes)\rangle$ есть не что иное, как полугруппа правых нулей (левых единиц) $\langle U, (\wr)\rangle$, и имеет место равенство

$$\phi_\star \odot \phi_* = \phi_\wr.$$

Нетрудно понять, что операция $\phi_\wr$ — идемпотент моноида $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$, поэтому порядок циклической полугруппы $\langle \Phi_\wr, (\odot)\rangle$, порожденной операцией $\wr$, равен 1.

3. Если операция $*$ дистрибутивна относительно операции $\star$ справа, то

$$u_1 \otimes u_2 = (u_1 \star u_2) * u_2 = (u_1 * u_2) \star (u_1 * u_2).$$

Сейчас будет удобно воспользоваться аддитивно-мультипликативной терминологией. Назовем операцию $\star$ сложением и обозначим $+$, а операцию $*$ — умножением и обозначим $\cdot$, придерживаясь принятых в подобных случаях соглашений о старшинстве операций и записи степеней. Итак, будем считать, что

$$u \otimes v = (u + v) \cdot v = u \cdot v + v_r^2.$$

Учитывая (2.6), можем записать

$$\begin{aligned} &\phi_\otimes^n(u,v) = \phi_\otimes(\phi_\otimes^{n-1}(u,v), v) = \phi_\otimes^{n-1}(u,v) \cdot v + v_r^2 = (\phi_\otimes(\phi_\otimes^{n-2}(u,v)) \cdot v + v_r^2 = \dots \\ &= (\phi_\otimes^{n-2}(u,v) \cdot v + v_r^2) \cdot v + v_r^2 = \dots = \underbrace{(\dots((u \cdot v + v_r^2) \cdot v + v_r^2) \cdot v + v_r^2) \dots) \cdot v + v_r^2}_{n} = \\ &= \underbrace{(\dots((u \cdot v_r^n + v_r^{n+1}) + v_r^n) + v_r^{n-1}) \dots) + v_r^2}_{n}. \end{aligned} \tag{2.15}$$

С целью упрощения записей будем считать операцию $+$ ассоциативной и перепишем (2.15) в виде

$$\phi_\otimes^n(u,v) = u \cdot v_r^n + v_r^{n+1} + v_r^n + v_r^{n-1} + \dots + v_r^2. \tag{2.16}$$

По аналогии с предыдущим рассмотрим группоид $\langle U, (\otimes)\rangle$ и циклическую полугруппу $\langle \Phi_\otimes, (\odot)\rangle$, порожденную операцией $\diamond$.

Предположим, что группоид конечен, из чего, как это уже было отмечено выше, следует существование идемпотента $\phi_\otimes^s \in \Phi_\otimes$ такого, что

$$\phi_\otimes^s \odot \phi_\otimes^s(u,v) = \phi_\otimes^{2s}(u,v) = \phi_*^s(\phi_*^s(u_1,u_2),u_2) = \phi_\otimes^s(u,v) \tag{2.17}$$

сразу для всех элементов $u, v \in U$.

Откуда с учетом (2.16) получим равенство

$$u \cdot v_r^{2s} + v_r^{2s+1} + v_r^{2s} + v_r^{2s-1} + \dots + v_r^{s+2} + v_r^{s+1} + \dots + v_r^2 = u \cdot v_r^s + v_r^{s+1} + v_r^s + v_r^{s-1} + \dots + v_r^2 \tag{2.18}$$

сразу для всех элементов $u, v \in U$.

Понятно, что если операция $\cdot$ идемпотентна, то (2.18) вырождается в тривиальное равенство $u \cdot v + v = u \cdot v + v$. Если вдобавок операция $+$ поглощает операцию $\cdot$, то (2.18) сведется к равенству $u = u$.

Пусть $\langle U, (\star)\rangle$, $\langle U, (*)\rangle$– квазигруппы, а $\langle U, (-)\rangle$, $\langle U, (\div)\rangle$– их парастрофы.
Определим композиции

$$u_3 = u_1 \triangleright u_2 = \phi_\triangleright(u_1,u_2) = \phi_\star \odot \phi_\div(u_1,u_2) = \phi_\div(\phi_\star(u_1,u_2),u_2) = (u_1 \star u_2) \div u_2,$$

$$u_3 = u_1 \triangleleft u_2 = \phi_\triangleleft(u_1,u_2) = \phi_* \odot \phi_-(u_1,u_2) = \phi_-(\phi_*(u_1,u_2),u_2) = (u_1 * u_2) - u_2,$$

$$u_3 = u_1 \triangle u_2 = \phi_\triangle(u_1,u_2) = \phi_\triangleleft \odot \phi_\triangleright(u_1,u_2) = \phi_\triangleright(\phi_\triangleleft(u_1,u_2),u_2) = (((u_1 * u_2) - u_2) \star u_2) \div u_2,$$

$$u_3 = u_1 \bigtriangledown u_2 = \phi_\bigtriangledown(u_1,u_2) = \phi_\triangleright \odot \phi_\triangleleft(u_1,u_2) = \phi_\triangleleft(\phi_\triangleright(u_1,u_2),u_2) = (((u_1 \star u_2) \div u_2) * u_2) - u_2.$$

В силу замечания 2.6 $\langle U, (\triangleright)\rangle$, $\langle U, (\triangleleft)\rangle$, $\langle U, (\triangle)\rangle$, $\langle U, (\bigtriangledown)\rangle$ — квазигруппы.

Понятно, что если сложность реализации операции $\phi_\star$ равна $N$, а сложность реализации операции $\phi_*$ равна $M$, то сложность реализации операций $\phi_\star \odot \phi_*$ и $\phi_* \odot \phi_\star$ равна $N + M$.

**Замечание 2.12.** Способ определения операций $\triangleright$, $\triangleleft$, $\triangle$, $\bigtriangledown$ задает схему порождения квазигрупп на основе их некоторого базового набора.

## 2.6. Криптосистемы на группоидах

Рассмотрим протокол DHM открытого распространения ключей. Основой протокола является вычисление значения секретного ключа $(u_0^n)^m = (u_0^m)^n = u_0^{nm}$ в циклической группе $\langle U_0, (*, e)\rangle$, порожденной элементом $u_0 \in U$ некоторой группы $\langle U, (*, e)\rangle$. Криптостойкость протокола обеспечивается существованием эффективного алгоритма вычисления степени элемента, который опирается на представление показателя степени $n$ в двоичной системе счисления

$$u^n = u^{2^r d_r + 2^{r-1} d_{r-1} \ldots d_0} = u^{2(\ldots 2(2(2d_r + d_{r-1}) + d_{r-1})\ldots) + d_0}$$

и имеет логарифмическую сложность $O(\log(n))$, в то время как известные к настоящему времени алгоритмы логарифмирования имеют корневую сложность $O(\sqrt{n})$ групповых операций.

Этот протокол, очевидно, применим к любой циклической подполугруппе $\langle U_0, (*)\rangle$ полугруппы $\langle U, (*)\rangle$, т. к. в ней справедливы правила положительных степеней (1.1) и (1.2).

В терминах полугрупповой (групповой) операции $*$ протокол DHM с двумя участниками описывается следующей схемой.

**Протокол DHM-1**

1. Опубликованные общедоступные значения: полугруппа $\langle U, (*)\rangle$; элемент $u_0 \in U$.
2. Вычисляемые значения на стороне A: $u_0^n \in U$. Значения, передаваемые по открытому каналу связи: $u_0^n$. Секретное значение: $n$.
3. Вычисляемые значения на стороне B: $u_0^m \in U$. Значения, передаваемые по открытому каналу связи: $u_0^m$. Секретное значение: $m$.
4. Вычисляемое значение секретного ключа на стороне A: $K = (u_0^m)^n = u_0^{mn}$.
5. Вычисляемое значение секретного ключа на стороне B: $K = (u_0^n)^m = u_0^{nm} = u_0^{mn}$.
6. Значения, известные третьей стороне C: $\langle U, (*)\rangle,\ u_0 \in U,\ u_0^n,\ u_0^m$.

Естественными требованиями, предъявляемыми к полугруппе, будут наличие эффективной вычислительной реализации полугрупповой операции $*$ для вычисления секретного ключа за приемлемое время, компактного способа представления ее элементов, а также достаточно большой или бесконечный порядок ее циклических подполугрупп $\langle U_0, (*)\rangle$.

Протокол DHM-1 можно переписать в терминах степеней полугрупповой операции $\phi_*^n(u_1, u_2)$, определенной в соответствии с (2.9) как степень $n > 1$ операции $*$ в моноиде $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$.

**Протокол DHM-2**

1. Опубликованные общедоступные значения: полугруппа $\langle U, (*)\rangle$; элемент $u_0 \in U$.
2. Вычисляемые значения на стороне A: $\phi_*^{n-1}(u_0, u_0) = u_0^n \in U$. Значения, передаваемые по открытому каналу связи: $\phi_*^{n-1}(u_0, u_0)$. Секретное значение: $n$.
3. Вычисляемые значения на стороне B: $\phi_*^{m-1}(u_0, u_0) = u_0^m \in U$. Значения, передаваемые по открытому каналу связи: $\phi_*^{m-1}(u_0, u_0)$. Секретное значение: $m$.
4. Вычисляемое значение секретного ключа на стороне A: $K = \phi_*^n(u_0, \phi_*^{m-1}(u_0, u_0)) = u_0 * (u_0^m)^n = = u_0^{mn+1}$.
5. Вычисляемое значение секретного ключа на стороне B: $K = \phi_*^m(u_0, \phi_*^{n-1}(u_0, u_0)) = u_0 * (u_0^n)^m = = u_0^{nm+1} = u_0^{mn+1}$.
6. Значения, известные третьей стороне C: $\langle U, (*)\rangle,\ u_0 \in U,\ u_0^n,\ u_0^m$.

**Замечание 2.13.** Вполне понятно, что требование ассоциативности операции $*$ не является определяющим для возможности построения на ее основе протокола DHM. Он может быть реализован на некотором циклическом группоиде, порожденном элементом $u_0 \in U$, для которого выполняется одно из

правил левых (правых) степеней (1.3). Действительно, если выполняется хотя бы одно из правил (1.3), то соответствующий циклический группоид $\langle U_0^l, (*)\rangle$, или что то же самое $\langle U_0^r, (*)\rangle$, является полугруппой, на которую легко переносится схема протокола DHM-1.

Как уже отмечалось выше, правило левых (правых) степеней (1.4) является следствием правила (1.3). Однако для реализации протокола DHM не требуется выполнение равенств

$$\begin{gathered}(u_{0l}^n)_{0l}^m = u_{0l}^{nm},\\ (u_{0r}^n)_{0r}^m = u_{0r}^{nm},\end{gathered} \tag{2.19}$$

а требуется лишь перестановочность степеней

$$\begin{gathered}(u_{0l}^n)_{0l}^m = (u_{0l}^m)_l^n,\\ (u_{0r}^n)_{0r}^m = (u_{0r}^m)_r^n,\end{gathered} \tag{2.20}$$

и эффективность их вычислительной реализации (по сравнению с операцией логарифмирования), которые могут иметь место независимо от (2.19).

Поясним сказанное на примере. В соответствии с (2.9) определим семейство операций $\{\star_s\}_{s=1}^{\infty}$, как степени $s \in \mathbb{N}$ ассоциативной операции $*$ в моноиде $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$

$$\phi_{\star_s}(u_1, u_2) = \phi_*^s(u_1, u_2) = \phi_*(\phi_*^{s-1}(u_1, u_2), u_2) = \phi_*^{s-1}(u_1, u_2) * u_2 = \ldots = u_1 * u_2^s. \tag{2.21}$$

В дальнейшем будем опускать индекс $s$ в обозначении операции $\star_s$, при необходимости обозначая $\star_{s'}$ как $\star'$.

Операции $\star$ в общем случае не ассоциативны. Действительно,

$$(u_1 \star u_2) \star u_3 = (u_1 * u_2^s) \star u_3 = u_1 * u_2^s * u_3^s,$$

$$u_1 \star (u_2 \star u_3) = u_1 \star (u_2 * u_3^s) = u_1 * (u_2 * u_3^s)^s,$$

и одновременно

$$\begin{gathered}u_{\star r}^n = u_*^{(n-1)s+1},\\ u_{\star l}^n = u_*^{\frac{s^n-1}{s-1}}.\end{gathered}$$

Здесь символами $u_{\star r}^k$, $u_{\star l}^k$ обозначены правые и левые степени элемента $u \in U$ по операции $\star$, а символом $u_*^k$ — степень этого элемента по операции $*$.

Таким образом, в общем случае $\langle U, (\star)\rangle$ – группоиды.

Понятно, что выполняется перестановочность степеней (2.20) для каждой операции семейства $\star$

$$(u_{\star r}^m)_{\star r}^n = (u_{\star r}^m)_*^{(n-1)s+1} = (u_*^{(m-1)s+1})_*^{(n-1)s+1} = u_*^{((m-1)s+1)((n-1)s+1)} = u_*^{((n-1)s+1)((m-1)s+1)} = (u_{\star r}^n)_{\star r}^m,$$

$$(u_{\star l}^m)_{\star l}^n = u_*^{\frac{(s^m-1)(s^n-1)}{(s-1)^2}} = (u_{\star l}^n)_{\star l}^m,$$

однако для них могут не выполняться равенства (2.19), т. к.

$$\begin{gathered}u_{\star r}^{mn} = u_*^{(mn-1)s+1},\\ u_{\star l}^{mn} = u_*^{\frac{s^{mn}-1}{s-1}}.\end{gathered}$$

Также имеет место взаимная перестановочность левых и правых степеней

$$(u_{\star r}^m)_{\star l}^n = u_*^{\frac{((m-1)s+1)(s^n-1)}{s-1}} = (u_{\star l}^n)_{\star r}^m.$$

Более того, любая пара степеней по операциям $\star$ и $\star'$ перестановочна

$$\begin{gathered}(u_{\star r}^m)_{\star' r}^n = (u_{\star' r}^n)_{\star r}^m,\\ (u_{\star l}^m)_{\star' l}^n = (u_{\star' l}^n)_{\star l}^m,\\ (u_{\star r}^m)_{\star' l}^n = (u_{\star' l}^n)_{\star r}^m,\\ (u_{\star l}^m)_{\star' r}^n = (u_{\star' r}^n)_{\star l}^m.\end{gathered}$$

С учетом ассоциативности операции $*$ можно оценить сложности вычисления значений операций $u_{\star r}^k$ и $u_{\star l}^k$ как $O(\log(ks))$ и $O(k\log(s))$ полугрупповых операций $*$, соответственно.

Таким образом, группоиды $\langle U,(\star)\rangle$ могут оказаться пригодными для реализации протокола DHM. С учетом взаимной перестановочности правых и левых степеней по операциям $\star$ и $\star'$ не будем указывать нижние индексы $_r$ и $_l$ в их обозначении, понимая под $u^k_\star$ одну из степеней $u^k_{\star r}$ или $u^k_{\star l}$.

Опишем схему протокола DHM для группоида $\langle U,(\star)\rangle$.

**Протокол DHM-3**

1. Опубликованные общедоступные значения: полугруппа $\langle U,(*)\rangle$; элемент $u\in U$.
2. Вычисляемые значения на стороне A: $u^n_\star\in U$. Значения, передаваемые по открытому каналу связи: $u^n_\star$. Секретные значения: $n$, $\star$.
3. Вычисляемые значения на стороне B: $u^m_{\star'}\in U$. Значения, передаваемые по открытому каналу связи: $u^m_{\star'}$. Секретные значения: $m$, $\star'$.
4. Вычисляемое значение секретного ключа на стороне A: $K=(u^m_{\star'})^n_\star$.
5. Вычисляемое значение секретного ключа на стороне B: $K=(u^n_\star)^m_{\star'}=(u^m_{\star'})^n_\star$.
6. Значения, известные третьей стороне C: $\langle U,(*)\rangle$, $u_0\in U$, $u^n_\star$, $u^m_{\star'}$.

Рассмотрим еще одну модификацию протокола DHM, отказавшись от требования ассоциативности операции $*$. По аналогии с предыдущим и в соответствии с (2.6) определим семейство операций $\{\star_s\}_{s=1}^\infty$ как степени $s\in\mathbb{N}$ неассоциативной операции $*$ в моноиде $\langle U^{U^2},(\odot,\mathcal{I}_U)\rangle$

$$\phi_{\star_s}(u_1,u_2)=\phi^s_*(u_1,u_2)=\phi_*(\phi^{s-1}_*(u_1,u_2),u_2)=\phi^{s-1}_*(u_1,u_2)*u_2=\ldots=\underbrace{(\ldots((u_1*u_2)*u_2)*\ldots)*u_2}_{n}. \tag{2.22}$$

В силу ассоциативности операции $\odot$ имеют место равенства

$$\begin{aligned}&\phi_{\star_s}\odot\phi_{\star_{s'}}(u_1,u_2)=\phi_{\star_s}(\phi_{\star_{s'}}(u_1,u_2),u_2)=\phi^s_*(\phi^{s'}_*(u_1,u_2),u_2)=\\&=\phi^s_*(\underbrace{(\ldots((u_1*u_2)*u_2)*\ldots)*u_2}_{s'},u_2)=(\underbrace{(\ldots((u_1*u_2)*u_2)*\ldots)*u_2}_{s})\underbrace{*u_2)*\ldots)*u_2}_{s'}=\\&.=(\underbrace{(\ldots((u_1*u_2)*\ldots)*u_2}_{s'})\underbrace{*u_2)*u_2)*\ldots)*u_2}_{s}=\phi^{s'}_*(\underbrace{(\ldots((u_1*u_2)*u_2)*\ldots)*u_2}_{s},u_2)=\\&=\phi^{s'}_*(\phi^s_*(u_1,u_2),u_2)=\phi_{\star_{s'}}(\phi_{\star_s}(u_1,u_2),u_2)=\phi_{\star_{s'}}\odot\phi_{\star_s}(u_1,u_2)=\phi_{\star_{s+s'}}(u_1,u_2).\end{aligned} \tag{2.23}$$

С учетом ассоциативности операции $\odot$ можно оценить сложность вычисления операции $\phi_{\star_s}=\phi^s_*$ как $O(\log(s))$ полугрупповых операций $\odot$.

Если для представления операций $\phi_*$ и $\phi_{\star_s}=\phi^s_*$ на конечном множестве $U$ используются двоичные массивы $r^*_{ijk}$ и $r^{\star_s}_{ijk}$, то, с учетом замечания 2.7, можно оценить сложность реализации операции $\odot$ как $O(|U|^4)$. Потребности в памяти для реализации операции $\odot$ оцениваются как $2|U|^3$. Потребности в памяти для представления каждой из операций $\phi_*$ и $\phi_{\star_s}$ оцениваются как $|U|^3$.

Если для представления элемента $u_i$ конечного множества $U$ используется его номер $i$ в двоичной системе счисления, то потребности в памяти для представления $u_i\in U$ оцениваются как $\log(|U|)+1$. При этом потребности в памяти для представления операции $\phi_*$ таблицей Кэли можно оценить как $|U|^2(\log(|U|+1))$.

Заметим, что если элементы $u_i\in U$ и $u_j\in U$ представлены своими номерами $i$ и $j$, то для определения номера результирующего значения операции $u_k=\phi_{\star_s}(u_i,u_j)$ достаточно найти единственное значение индекса $k\in 1..|U|$ (при фиксированных значениях $i$ и $j$), для которого $r^{\star_s}_{ijk}=1$. Таким образом, сложность нахождения результата операции на аргументах можно оценить как $O(|U|)$ операций сравнения.

Опишем схему протокола DHM для группоида $\langle U,(*)\rangle$.

**Протокол DHM-4**

1. Опубликованные общедоступные значения: группоид $\langle U,(*)\rangle$; $k\in\mathbb{N}$; последовательность значений аргументов $\{(u^i_1,u^i_2)\}_{i=1}^k$, $u^i_1,u^i_2\in U$, $i\in 1..k$.

2. Вычисляемые значения на стороне A: операция $\phi_{\star_s} = \phi_*^s$, последовательность значений результатов операции $\{\phi_{\star_s}(u_1^i, u_2^i)\}_{i=1}^k$. Значения, передаваемые по открытому каналу связи: $\{\phi_{\star_s}(u_1^i, u_2^i)\}_{i=1}^k$. Секретное значение: $s$.

3. Вычисляемые значения на стороне B: операция $\phi_{\star_{s'}} = \phi_*^{s'}$, последовательность значений результатов операции $\{\phi_{\star_{s'}}(u_1^i, u_2^i)\}_{i=1}^k$. Значения, передаваемые по открытому каналу связи: $\{\phi_{\star_{s'}}(u_1^i, u_2^i)\}_{i=1}^k$. Секретное значение: $s'$.

4. Вычисляемое значение секретного ключа на стороне A: $K = \{\phi_{\star_s}(\phi_{\star_{s'}}(u_1^i, u_2^i), u_2^i)\}_{i=1}^k = \{\phi_{\star_{s+s'}}(u_1, u_2)\}_{i=1}^k$.

5. Вычисляемое значение секретного ключа на стороне B: $K = \{\phi_{\star_{s'}}(\phi_{\star_s}(u_1^i, u_2^i), u_2^i)\}_{i=1}^k = \{\phi_{\star_{s+s'}}(u_1, u_2)\}_{i=1}^k$.

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

Понятно, что криптографическая стойкость предложенного протокола определяется свойствами конкретного группоида. Например, протокол будет абсолютно ненадежен в случае его реализации на полугруппе идемпотентов. Помимо всего прочего, степень уязвимости протокола зависит от порядка носителя группоида $|U|$, при этом, как было отмечено выше, грубые верхние оценки потребности в памяти и вычислительная сложность алгортима построения секретного ключа, в случае представления операции двоичным массивом ее графика, оценивается как $O(|U|^3)$ бит и $O(|U|^4)$ битовых логических операций (дизъюнкция, конъюнкция), соответственно.

Таким образом, вопрос о практической реализации протокола DHM-4 требует отдельного и глубокого анализа.

## Выводы

В статье предложен метод изучения бинарных операций как элементов носителей подполугрупп полугруппы 3-местных отношений. Метод развивает подход, разработанный в [28], который опирается на определение операции $\odot$ над 3-местными отношениями, индуцированной операцией произведения $\bullet$ над 2-местными отношениями. Такой подход приводит к естественной классификации бинарных операций в терминах вложений полугрупп $\langle B_{U^2}, (\odot, \mathcal{I}_U)\rangle \subseteq \langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle \subseteq \langle 2^{U^3}, (\odot, \mathcal{I}_U)\rangle$, где $2^{U^3}$ — множество 3-местных отношений, $U^{U^2}$ — множество бинарных операций, $B_{U^2}$ — множество операций правых квазигрупп, которые определены на множестве $U$. Отмечена очевидная связь данных вложений и вложений $\langle B_U, (\bullet, \mathbb{I}_U)\rangle \subseteq \langle U^U, (\bullet, \mathbb{I}_U)\rangle \subseteq \langle 2^{U^2}, (\bullet, \mathbb{I}_U)\rangle$, где $2^{U^2}$ — множество 2-местных отношений, $U^U$ — множество тотальных функций, $B_U$ — множество подстановок, которые определены на множестве $U$. Напомним, что $\langle B_U, (\bullet, \mathbb{I}_U)\rangle$ и $\langle B_{U^2}, (\odot, \mathcal{I}_U)\rangle$ — группы.

Аналогичные результаты, но уже для операций левых квазигрупп получаются простой заменой операции произведения $\bullet$ на операцию суперпозиции $\circ$. Множество квазигрупповых операций очевидным образом описываются, как пересечение носителей соответствующих групп.

В терминах полугрупповой операции $\odot$ оказалось удобно описывать свойства правой нейтрализации и правого поглощения операцией $*$ операции $\star$

$$(u_1 \star u_2) * u_2 = u_1,$$
$$(u_1 \star u_2) * u_2 = u_2.$$

Нетрудно убедиться, что последние равенства эквивалентны равенствам

$$\phi_\star \odot \phi_* = \phi_\wr = \mathcal{I}_U,$$
$$\phi_\star \odot \phi_* = \phi_{\wr\wr},$$

где $\langle U, (\wr)\rangle$– полугруппа левых нулей (правых единиц), а $\langle U, (\wr\wr)\rangle$ – полугруппа правых нулей (левых единиц).

Прикладной интерес представляют циклические подполугруппы полугруппы $\langle U^{U^2}, (\odot, \mathcal{I}_U)\rangle$. Операции $\phi_*^n \in \Phi_*$ носителя циклической полугруппы $\langle \Phi_*, (\odot)\rangle$, порожденной бинарной операцией $*$, имеют вид

$$\phi_*^n(u_1, u_2) = \underbrace{(\ldots((u_1 * u_2) * u_2) * \ldots) * u_2}_{n}.$$

Полугруппы $\langle \Phi_*, (\odot)\rangle$ использовались в статье для построения аналога протокола Диффи — Хелмана — Меркла на группоидах.

Проанализирована схема реализации протокола, оперирующая с представлением операции в виде двоичного массива ее графика. Для подобного способа представления грубые верхние оценки потребности в памяти и вычислительных ресурсах при реализации алгортима построения секретного ключа оцениваются как $O(|U|^3)$ бит и $O(|U|^4)$ битовых логических операций (дизъюнкция, конъюнкция), соответственно.

Вопрос о подходах к практической реализации предложенного протокола требует отдельного изучения.

# Литература

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

[2] Merkle R.C. Secure Communications over Insecure Channels // Communications of the ACM. 1978. V. 21. No 4. P. 294–299. URL: https://nakamotoinstitute.org/static/docs/secure-communications-insecure-channels.pdf.

[3] Shamir A. How to share a secret // Communications of the ACM. 1979. V. 22. Iss. 11. P. 612–613. DOI: https://doi.org/10.1145/359168.359176.

[4] Matsumoto T., Imai H. Public Quadratic Polynomial-tuples for effcient signature-verification and message-encryption // In: Barstow D. et al. (eds) Advances in Cryptology — EUROCRYPT '88. EUROCRYPT 1988. Lecture Notes in Computer Science. V. 330. Springer, Berlin, Heidelberg, pp. 419–453. DOI: https://doi.org/10.1007/3-540-45961-8_39.

[5] Patarin J. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms // Maurer U. (eds) Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science. V. 1070. Springer, Berlin, Heidelberg, pp. 33–48. DOI: https://doi.org/10.1007/3-540-68339-9_4.

[6] Shor P. Algorithms for quantum computation: discrete logarithms and factorings // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134. DOI: http://doi.org/10.1109/SFCS.1994.365700.

[7] Bernstein J.D., Buchmann J., Dahmen E. (Eds.) Post-quantum cryptography. Springer, Berlin, 2009, 245 p. DOI: http://doi.org/10.1007/978-3-540-88702-7.

[8] Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation. 1987. V. 48. No 177. P. 203–209. URL: https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf.

[9] Koblitz N. Hyperelliptic Cryptosystems // Journal of cryptology. 1989. V. 1. No 3. P. 139–150. DOI: http://doi.org/10.1007/BF02252872.

[10] Goldreich O., Goldwasser S., Halevi S. Public-key cryptosystems from lattice reduction problems // Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 97). 1997. P. 112–131. DOI: https://doi.org/10.1007/BFb0052231.

[11] Regev O. Lattice-based cryptography. // In: Dwork C. (eds) Advances in Cryptology - CRYPTO 2006. CRYPTO 2006. Lecture Notes in Computer Science. V. 4117. Springer, Berlin, Heidelberg, pp. 131–141. DOI: https://doi.org/10.1007/11818175_8.

[12] Maze G., Monico C., Rosenthal J. Public key cryptography based on semigroup actions // Advances in Mathematics of Communications. 2007. V. 1, No 4. P. 489–507. DOI: http://doi.org/10.3934/amc.2007.1.489.

[13] Ebrahimi Atani R., Ebrahimi Atani S., Mirzakuchaki S. Public key cryptography using semigroup actions and semirings // Journal of Discrete Mathematical Sciences & Cryptography. 2008. V. 4.

[14] Carter S., Wegman M.N. Universal Class of Hash Function // J. Computer and System Sciences. 1979. V. 18. No. 2. P. 143–154. URL: https://www.cs.princeton.edu/courses/archive/fall09/cos521/Handouts/universalclasses.pdf.

[15] Denes J., Keedwell A.D. Latin Squares. New Developments in the Theory and Applications. Amsterdam: Nord-Holland Publishing Co., 1981, 469 p. URL: http://lib.mexmat.ru/books/191480.

[16] Bakhtiari S., Safavi-Naini R., Pieprzyk J. A message Authentication Code based on Latin Squares // Proc. Australasian on Information Security and Privacy. 1997. P. 194–203. DOI: http://doi.org/10.1007/BFb0027926.

[17] Dawson E., Donovan D., Offer A. Quasigrops, isotopism and authentication schemes // Australasian Journal of Combinatorics. 1996. V. 13. P. 75–88.

[18] Глухов М.М. О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. No 2. С. 28–32. URL: http://www.mathnet.ru/links/f859b1b745b65468d900eab5fbd7ebde/pdm29.pdf.

[19] Cheremushkin A.V. Partially invertible strongly dependent n-ary operations // Sbornik: Mathematics. 2020. V. 211. No 2. P. 291–308. DOI: https://doi.org/10.4213/sm9204.

[20] Hessenberg G. Grundbegriffe der Mengenlehre // Abhandlungen der Friesschen Schule. 1906. V. 1. No. 4. P. 478–706. Available at: https://archive.org/details/grundbegriffede00hessgoog/page/n1/mode/2up.

[21] Hausdorff F. Grundzlige der Mengenlehre. Leipzig: Verlag von Veit & Comp., 1914, 500 p. URL: https://archive.org/details/grundzgedermen00hausuoft.

[22] Tarski A. On the calculus of relations // Journal of Symbolic Logic. 1941. V. 6. No 3. P. 73–89.

[23] Fraisse R. Theory of Relations // Studies in Logic and the Foundations of Mathematics. Elsevier, 2011, 410 p. URL: https://readli.net/theory-of-relations/.

[24] Biggs N.L. Discrete Mathematics. Oxford: Oxford University Press, 2002. 425 p. URL: https://archive.org/details/discretemathemat00norm_0/mode/2up.

[25] Schein B.M. Relation algebras and function semigroups // Semigroup Forum. 1970. V. 1. No. 1. P. 1–62. DOI: http://doi.org/10.1007/BF02573019.

[26] Bruijn N., Erdos P. A colour problem for infinite graphs and a problem in the theory of relations // Nederl. Akad. Wetensch. Proc. Indag. Math. Ser. A. 1951. V. 54, issue 5, pp. 371–373. URL: https://research.tue.nl/files/4237754/597497.pdf.

[27] 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.

[28] Tsvetov V.P. Algebras of finitary relations // CEUR Workshop Proceedings. 2019. V. 2416. P. 119–125. DOI: https://doi.org/10.18287/1613-0073-2019-2416-119-125.

Scientific article

DOI: 10.18287/2541-7525-2020-26-1-23-51

Submited: 15.01.2020
Revised: 17.02.2020
Accepted: 28.02.2020

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

# SEMIGROUPS OF BINARY OPERATIONS AND MAGMA-BASED CRYPTOGRAPHY

**ABSTRACT**

In this article, algebras of binary operations as a special case of finitary homogeneous relations algebras are investigated. The tools of our study are based on unary and associative binary operations acting on the set of ternary relations. These operations are generated by the converse operation and the left-composition of binary relations. Using these tools, we are going to define special kinds of ternary relations that correspond to functions, injections, right- and left-total binary relations. Then we obtain criteria for these properties in terms of ordered semigroups. Note, that there is an embedding of the semigroup of quasigroups operations in the semigroup of magmas operation and further in the semigroup of ternary relations. This is similar to embedding the semigroup of bijections in the semigroup of functions and then in the semigroup of binary relations. Taking a binary operation as the generator of a cyclic semigroup, we can apply an exponential squaring method for the fast computation of its positive integer powers. Given that this is the main method of public key cryptography, we are adapting the Diffie-Hellman-Merkle key exchange algorithm for magmas as a result.

**Key words:** algebra of finitary relations, algebra of indicator function, magmas, quasigroups, semigroups, cyclic semigroup of binary operations, public key cryptography, Diffie-Hellman-Merkle key exchange.

**Citation.** 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. DOI: http://doi.org/10.18287/2541-7525-2020-26-1-23-51. (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] Diffie W., Hellman M.E. New Directions in Cryptographyю *IEEE Transactions on Information Theory*, 1976, vol. IT-22, pp. 644–654. DOI: https://doi.org/10.1109/TIT.1976.1055638.

[2] Merkle R.C. Secure Communications over Insecure Channels. *Communications of the ACM*, 1978, vol. 21, no 4, pp. 294–299. Available at: https://nakamotoinstitute.org/static/docs/secure-communications-insecure-channels.pdf.

[3] Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, issue 11, pp. 612–613. DOI: https://doi.org/10.1145/359168.359176.

[4] Matsumoto T., Imai H. Public Quadratic Polynomial-tuples for effcient signature-verification and message-encryption. In: Barstow D. et al. (eds) Advances in Cryptology — EUROCRYPT '88. EUROCRYPT 1988. Lecture Notes in Computer Science, vol 330. Springer, Berlin, Heidelberg, pp. 419–453. DOI: https://doi.org/10.1007/3-540-45961-8_39.

[5] Patarin J. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer U. (eds) Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg, pp. 33–48. DOI: https://doi.org/10.1007/3-540-68339-9_4.

[6] Shor P. Algorithms for quantum computation: discrete logarithms and factorings. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[7] Bernstein J.D., Buchmann J., Dahmen E. (Eds.) Post-quantum cryptography. Springer, Berlin, 2009, 245 p. DOI: http://doi.org/10.1007/978-3-540-88702-7.

[8] Koblitz N. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 1987, vol. 48, no. 177, pp. 203–209. Available at: https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf.

[9] Koblitz N. Hyperelliptic Cryptosystems. *Journal of cryptology*, 1989, vol. 1, no 3, pp. 139–150. DOI: http://doi.org/10.1007/BF02252872.

[10] Goldreich O., Goldwasser S., Halevi S. Public-key cryptosystems from lattice reduction problems. In: Kaliski B.S. (eds) Advances in Cryptology — CRYPTO '97. CRYPTO 1997. Lecture Notes in Computer Science, vol. 1294. Springer, Berlin, Heidelberg, pp. 112–131. DOI: https://doi.org/10.1007/BFb0052231.

[11] Regev O. Lattice-based cryptography. In: Dwork C. (eds) Advances in Cryptology - CRYPTO 2006. CRYPTO 2006. Lecture Notes in Computer Science, vol 4117. Springer, Berlin, Heidelberg, pp. 131–141. DOI: https://doi.org/10.1007/11818175_8.

[12] Maze G., Monico C., Rosenthal J. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, 2007, vol. 1, no 4, pp. 489–507. DOI: http://doi.org/10.3934/amc.2007.1.489.

[13] Ebrahimi Atani R., Ebrahimi Atani S., Mirzakuchaki S. Public key cryptography using semigroup actions and semirings. *Journal of Discrete Mathematical Sciences & Cryptography*, 2008, vol. 4. DOI: DOI: http://doi.org/10.1080/09720529.2008.10698195.

[14] Carter S., Wegman M.N. Universal Class of Hash Function. *Journal of Computer and System Sciences*, 1979, vol. 18, no. 2, pp. 143–154. Available at: https://www.cs.princeton.edu/courses/archive/fall09/cos521/Handouts/universalclasses.pdf.

[15] Denes J., Keedwell A.D. Latin Squares. New Developments in the Theory and Applications. Amsterdam: Nord-Holland Publishing Co., 1981, 469 p. Available at: http://lib.mexmat.ru/books/191480.

[16] Bakhtiari S., Safavi-Naini R., Pieprzyk J. A message Authentication Code based on Latin Squares. *Proc. Australasian on Information Security and Privacy*, 1997, pp. 194–203. DOI: 10.1007/BFb0027926.

[17] Dawson E., Donovan D., Offer A. Quasigroups, isotopism and authentication schemes. *Australasian Journal of Combinatorics*, 1996, vol. 13, pp. 75–88.

[18] Glukhov M.M. Some application of quasigroups in cryptography. *Prikladnaya Diskretnaya Matematika*, 2008, no 2, pp. 28–32. Available at: http://www.mathnet.ru/links/f859b1b745b65468d900eab5fbd7ebde/pdm29.pdf. (in Russ.)

[19] Cheremushkin A.V. Partially invertible strongly dependent n-ary operations. *Sbornik: Mathematics*, 2020, vol. 211, no 2, pp. 291—308. DOI: https://doi.org/10.4213/sm9204.

[20] Hessenberg G. Grundbegriffe der Mengenlehre. In: Abhandlungen der Friesschen Schule, 1906, bd. 1, hft. 4, pp. 478–706. Available at: https://archive.org/details/grundbegriffede00hessgoog/page/n1/mode/2up.

[21] Hausdorff F. Grundzlige der Mengenlehre. Leipzig: Verlag von Veit & Comp., 1914, 500 s. Available at: https://archive.org/details/grundzgedermen00hausuoft.

[22] Tarski A. On the calculus of relations. *Journal of Symbolic Logic*, 1941, vol. 6, no. 3, pp. 73–89. DOI: http://doi.org/10.2307/2268577.

[23] Fraisse R. Theory of Relations. In: Studies in Logic and the Foundations of Mathematics. Elsevier, 2011, 410 p. Available at: https://readli.net/theory-of-relations/.

[24] Biggs N.L. Discrete Mathematics. Oxford: Oxford University Press, 2002, 425 p. Available at: https://archive.org/details/discretemathemat00norm_0/mode/2up.

[25] Schein B.M. Relation algebras and function semigroups. *Semigroup Forum*, 1970, vol. 1, no. 1, pp. 1–62. DOI: http://doi.org/10.1007/BF02573019.

[26] Bruijn N., Erdos P. A colour problem for infinite graphs and a problem in the theory of relations. *Nederl. Akad. Wetensch. Proc. Indag. Math. Ser. A.*, 1951, vol. 54, issue 5, pp. 371–373. Available at: https://research.tue.nl/files/4237754/597497.pdf.

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

[28] Tsvetov V.P. Algebras of finitary relations. *CEUR Workshop Proceedings*, 2019, vol. 2416, pp. 119–125. DOI: https://doi.org/10.18287/1613-0073-2019-2416-119-125.