

Министерство образования и науки Российской Федерации
Санкт-Петербургский государственный политехнический университет

Конспект лекций по курсу

«Дискретная математика».

Для подготовки студентов по направлениям

**«Информатика и вычислительная техника» и
«Программная инженерия»**

Разработал доцент кафедры
«Информационные и управляющие системы»,
к.т.н. А.И.Тышкевич

Содержание

Тема 1. ВВЕДЕНИЕ В ДИСКРЕТНУЮ МАТЕМАТИКУ И ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ

Тема 2. Бинарные предикаты. Бинарные отношения. Прямые произведения множеств. Бинарные отношения и функции. Типы функциональных отношений. Взаимнооднозначные соответствия. Эквивалентность (равномощность) множеств.

Тема 3. Специальные виды операций над бинарными отношениями. Обращение и композиции. Степень бинарного отношения. Отношение достижимости. Особенности последовательности степеней бинарного отношения на конечном множестве.

Тема 4. Ряд натуральных чисел. Рекуррентные формулы и функция следования. Принцип индукции. Примеры доказательств в формальной арифметике.

Тема 5. Специальные виды бинарных отношений. Отношения эквивалентности. Классы эквивалентности. Разбиения. Примеры отношений эквивалентности.

Тема 6. Специальные виды бинарных отношений: отношения порядка. Отрезки. Диаграммы Хассе.

Тема 7. Модели теории графов. Определение простого графа. Способы задания простых графов. Отношения и матрицы смежности и инцидентности. Степень вершин простого графа и её свойства.

Тема 8. Маршруты и циклы в простом графе. Отношение связности и компоненты связности.

Тема 9. Размеченные графы. Вес рёбер и вес маршрута. Требования. Задача поиска кратчайшего маршрута. Алгоритм Флойда-Уоршалла.

Тема 10. Планырные графы. Грани. Формула Эйлера. Полный граф. Двудольный граф. Полный двудольный граф. Необходимые и достаточные условия планарности.

Тема 11. Бинарные алгебры с одной операцией: Отношение изоморфизма для бинарных алгебр.

Тема 12. Бинарные алгебры с одной операцией: специальные свойства операций и специальные элементы.

Тема 13. Моноиды. Степени элементов. Обратимость и сократимость. Особенности конечных моноидов.

Тема 14. Алгебраические группы. Определение и свойства. Подгруппы. Конечные группы и циклические подгруппы степеней элементов.

Тема 15. Циклические группы. Изоморфизм циклических групп и сложения классов вычетов по модулю n . Смежные классы элементов по подмножествам-подгруппам. Разбиения множества элементов группы на смежные классы по подгруппам.

Тема 16. Двоичные групповые коды: постановка задачи повышения достоверности при передаче дискретной информации по ненадёжному каналу. Блочное кодирование.

Тема 17. Двоичные групповые коды: матричное кодирование, групповые свойства и таблица стандартной расстановки. Исправление ошибок.

Тема 18. Алгебры с двумя бинарными операциями: классификация, кольца, области целостности и поля, свойства элементов.

Тема 19. Конечные области целостности и поля. Поля простого порядка. Элементы, кратные единице. Характеристика поля. Векторное представление элементов поля. Характеристика и размерность.

Тема 20. Кольцо многочленов с коэффициентами из поля. Операции над многочленами. Конечные поля: построение путём разложения на классы вычетов по модулю неприводимого многочлена.

Тема 1. ВВЕДЕНИЕ В ДИСКРЕТНУЮ МАТЕМАТИКУ И ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ

Современную структуру научного знания можно представить разделенной на два основных направления – естественно-научное и прикладное. Естественно-научные дисциплины (компоненты структуры знания), такие как физика, биология, характеризуются прежде всего тем, что предмет их исследования объективно существует и исследователь, выстраивая свои модельные представления имеет возможность сопоставлять их адекватность действительности: ставить эксперименты, анализировать статистику и т.д. В этом смысле можно говорить, что модельные представления в естественных науках вторичны по отношению к предмету исследования в типовом «жизненном цикле» научных теорий: модель выстраивается по уже имеющемуся предмету исследования, затем проверяется адекватность модели. Для удачных решений на основе принятых представлений разрабатываются способы использования изучаемых явлений в практической деятельности: разрабатываются технологические процессы, изготавливаются механизмы, приспособления.

В прикладных дисциплинах, таких как математика, в частности, дискретная математика, чаще наоборот, модельные представления и способы работы с моделями разрабатываются в отрыве от конкретных областей применения. Особо это касается информационных систем, когда нельзя сказать, что разрабатываемая математическая модель отражает поведения чего-либо реально существующего: информационная система не может заранее существовать как предмет исследования, так как ни одна из существующих (по крайней мере искусственно создаваемых систем), так как для ее функционирования как раз и не хватает тех свойств, которыми призвано наделить ее применение разрабатываемых методов. В этом смысле можно сказать, что модельные представления в данном случае первичны по отношению к остальной деятельности.

Например, разрабатываемые системы защиты информации или повышения достоверности с требуемыми свойствами первоначально ни в каком виде не существуют, пока необходимые математические методы не будут разработаны. Маловероятно найти их природный аналог.

Отсутствие естественных аналогов, невозможность представить предмет исследования в «осознаваемом» виде могут создавать сложности при изучении прикладных математических дисциплин. Имеющиеся общематематические знания у изучающих дискретную математику студентов мало помогают, так как обычно формируются еще в курсе начальной школы, когда о полном жизненном цикле научного знания представлений у обучающихся еще нет. Соответственно использование абстрактных моделей очень трудно для восприятия.

Этим же обусловлены возможные трудности в изучении предмета связанные с тем, что для проверки адекватности моделей в естественно-научных дисциплинах, придания уверенности, что изучение идет в верном направлении, можно применять такие приемы, как натурные эксперименты, аналогии, ссылки на опыт изучающих дисциплину. В математике для достижения данных целей приходится применять совсем другие приемы: доказательства, вычисления. А они тоже основываются на прикладных математических методах. Соответственно при изучении дискретной математики приходится в параллель с «предметно-ориентированными» моделями (графами, алгебрами, кодами), на основе которых в дальнейшем можно принимать технические решения (алгоритмы, структурные схемы) при разработке информационных систем, изучать и «внутренние» модели (математическую логику, исчисления, теорию доказательств), которые являются еще более абстрактными. Впрочем, термин «внутренняя модель» здесь условен: при разработке таких информационных систем, как базы знаний, логические анализаторы методы математической логики становятся вполне предметными.

В связи с этим предлагаемый курс лекций предлагается организовать следующим образом:

Сначала уделить внимание «внутренним» моделям – математической логике, исчислениям, теории множеств с моделями функций, отношений и их представлениям, а затем перейти к «предметным» моделям – графам, алгебрам, элементам теории кодирования.

Предметом дискретной математики являются дискретные модели, то есть такие, которые можно представить в символьной форме: текстом, формулами, символьными разметками диаграмм. В этом смысле можно сказать, что существенную долю общематематических знаний можно отнести также к дискретной математике, так как она основывается на символьной (в виде формул) формой представления моделей и методов работы с моделями: методы доказательств на основе определенных исчислений. Несмотря на то, что основным предметом в «традиционной» математике являются непрерывные величины и их функции, ее «внутренние» методы можно отнести уже к математике дискретной.

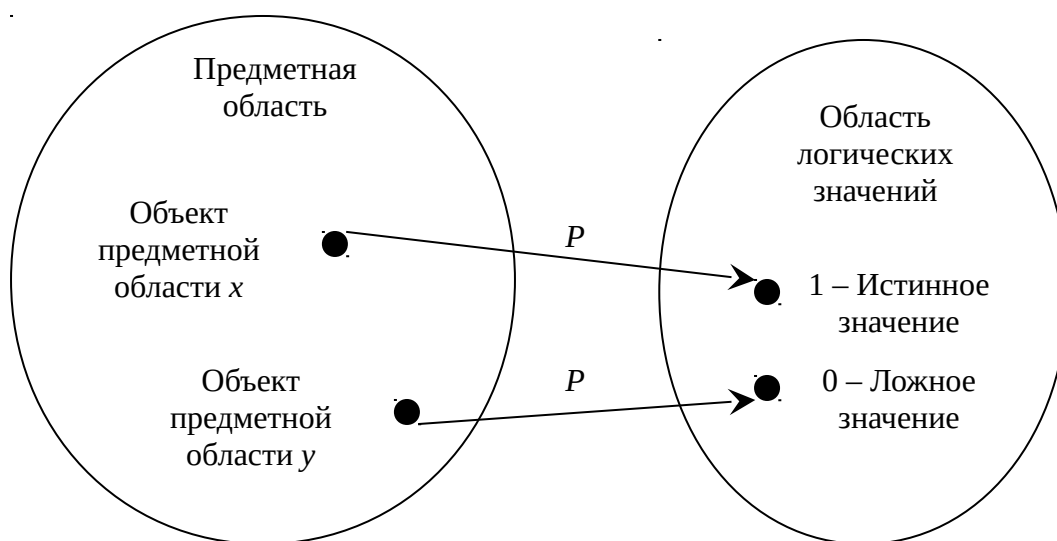
В области информационных систем как правило и «внутренние» и «предметные» модели дискретны: обрабатываемая информация рассматривается как правило в символьной форме (символы текстов сообщений, дискретные сигналы).

Раздел дискретной математики, с которого начинается ее рассмотрение в данном курсе – математическая логика – как «внутренняя» модель достаточно универсальна – она может быть «внутренней» моделью различных дисциплин, использующих символьные методы представления суждений о предметной области (доказательства, рассуждения и их формы представления).

Высказывания, предикаты, двоичные функции. Множества, теоретико-множественные операции и отношения между множествами. Взаимосвязь между логикой высказываний, алгеброй логики и теорией множеств.

Почти во всех областях знаний исследователь, описывая свою предметную область, выделяет в ней некоторые *объекты*, группирует их, приписывает им какие-либо *свойства*. То есть пытается как-то дифференцировать предметную область, не делая ее однородной, бесструктурной. Построение описания, выбор определяющих свойств, введение классификаций является одним из важных этапов в процессе познания с использованием модельных представлений. Конечно, за этим следует еще большая работа по выработке правил действий с самой моделью, получения результатов, сопоставление их с реальными объектами или внедрение результатов в практическую деятельность. Но уже на этом начальном этапе рассмотрения следует отметить некоторые общие черты процесса.

Приписывание свойств может быть схематично представлено следующей диаграммой:



Здесь иллюстрируется, что при рассмотрении предметной области в ней выделен некоторый объект, ему приписано имя или обозначение x , и отмечено, что для него выполняется некоторое свойство, названное или обозначенное символом P . То, что свойство для объекта x имеет место, на рисунке изображено в виде направленной линии (стрелки) от точки внутри предметной области к точке внутри области логических значений, обозначенной символом 1, интерпретируемым как истинное значение. Также для большей ясности схемы в предметной области другой точкой представлен еще один объект, от которого также проведена направленная линия в область логических значений, но к другой точке, подписанной символом 0, интерпретируемым как ложное значение. Само название свойства (символ P) приведено на рисунке с учетом того, что, как правило, разных названий рассматриваемых свойств может быть несколько и если возникнет необходимость проиллюстрировать их такими диаграммами, их нужно как-то различать.

Символы для обозначения логических значений могут выбираться произвольно. Отметим только, что в данной схеме они вынесены из предметной области. То есть в данном примере мы не рассматриваем саму логику в качестве объекта исследования, считая ее существенно проще предметной области. Ведь всякое модельное представление потому и является полезным инструментом в познании, что представляет собой некоторое упрощение для рассматриваемой ситуации. В данном случае одно из упрощений

заключается в том, что предметная область возможно очень сложна, в ней можно выделить большое число объектов (можно даже себе представить, что его вообще нельзя выразить конечным числом). А вот область логических значений относительно проста: в ней всего два объекта.

Изображенную ситуацию можно более компактно представить и не прибегая к рисункам, записав вышесказанное в символьной форме:

$$P(x) = 1$$

$$P(y) = 0$$

То есть выделение объектов и приписывание им свойств может рассматриваться так, как если бы была задана некоторая *функция*, аргументами которой могли бы быть любые объекты предметной области, а результатом ее вычисления были бы логические значения.

Уточнение понятия функции будет рассмотрено несколько позднее. На данном этапе вполне достаточно обычных представлений из области математики. А именно, считается, что для любого значения аргумента (в данном случае – обозначения объекта предметной области) определено единственное (то есть либо истинное, либо ложное) значение.

Предметом рассмотрения математической логики являются предложения языка, используемого для формулировки суждений о произвольной предметной области. Вообще язык описания предметной области может быть очень разнообразным, специфичным для разных областей знаний – естественнонаучных (физика, химия, электротехника, и т.д.) и прикладных дисциплин (математика, теория алгоритмов, математическая лингвистика и т.д.). В математической логике делается попытка найти нечто общее в этом многообразии и выделить некоторые общие приемы как для этапа построения описания (начальный этап, *абстрагирование* от области исследования, построение моделей), так и для последующих этапов (работа с построенными моделями, получение новых знаний для упрощенной модели). Эти последующие этапы с точки зрения математической логики могут рассматриваться как преобразования текстов формул, отражающих рассматриваемые предложения.

В математической логике функции, ставящие в соответствие некоторому значению произвольного типа логическое значение, называют *предикатами*. Сами фрагменты фраз анализируемого языка, которым можно сопоставить описанным образом логическое значение, называют *высказываниями*.

Еще раз отметим: высказывание это то, о чем можно сказать, что оно может быть истинным или ложным.

Рассмотрим примеры фрагментов предложений из различных дисциплин с позиций такого анализа.

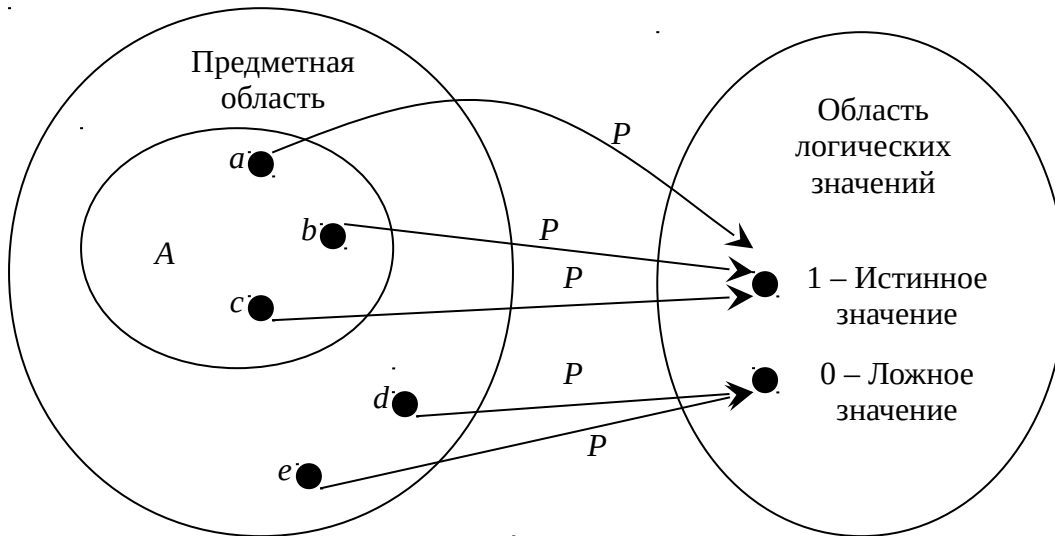
Математика: «Семь – простое число». В целом это предложение является высказыванием, так как ему можно сопоставить логическое значение (истинное в данном примере). «Семь» это название конкретного объекта предметной области (например, натуральных чисел). «Простое число» это предикат, так как является свойством, использованным для построения высказывания. Сами по себе фрагменты «Семь» и «простое число» высказываниями не являются, им не приписывается логических значений. Фрагмент «семь» не является также и предикатом, в нем нельзя выделить аргумента и сопоставляемого логического значения.

Химия: «Натрий является металлом». Аналогично, предложение является высказыванием (истинным).

Высказывание не обязательно должно быть истинным. Наоборот, именно наличие хоть и двух, но различных значений позволяет сохранить некоторое разнообразие суждений, всем возможным набором комбинаций значений высказывания что-то

высказать о предметной области в целом. Например, в математике высказывание «семь является четным числом» является ложным.

Рассматривая высказывания о значении предикатов по всей предметной области можно также сформировать представление о том, что предикаты выделяют в предметной области некоторые меньшие (лежащие целиком внутри) области. Следующая схема иллюстрирует это представление.



В примере предметная область состоит из литер a, b, c, d, e . При этом $P(a)=1$, $P(b)=1$, $P(c)=1$, $P(d)=0$, $P(e)=0$. Тогда говорят, что предикат P выделяет множество объектов a, b, c , на которых он принимает истинное значение. На рисунке это множество можно представить как лежащую внутри предметной области обведенную область. Таким областям тоже можно давать имена (названия). На рисунке эта область обозначена символом A . Такое выделение дает представление о *множестве*. В виде формулы для обозначения такого выделения и именования используется запись

$$A = \{ x \mid P(x) \}$$

Такая формула как бы отражает некоторую процедуру построения множества: перебираем все объекты предметной области и вычисляем для них значение предиката. Про объекты, для которых значения предиката окажутся истинными говорят, что они являются *элементами* множества. При этом в записи символ x является *подстановочным символом*. Он обозначает не имя или название конкретного объекта, а является ссылкой на такие объекты для словесной (формальной) записи некоторой процедуры. Имя подстановочного символа само по себе не несет смыслового значения. Единственное требование к нему – не допускать конфликта имен с конкретными названиями объектов предметной области и других вспомогательных объектов. Например, запись $A = \{ y \mid P(y) \}$ имеет в точности такой же смысл, как и приведенная выше формула, если ничего не обозначено символом y рассматриваемых областях. Еще удобнее пользоваться соглашением, что с каждым символом связана некоторая *область видимости*. В данном примере – часть формулы между фигурными скобками. Тогда удобнее считать, что символ используется как местный, локальный, для данной формулы, даже если вне неё он еще что-либо обозначает. В противном случае могут возникнуть сложности из-за нехватки коротких и ясных обозначений. Для уяснения этого соглашения рассмотрите обычные математические формулы, например, в записи для суммы ряда

$$s = \sum_{i=1}^{\infty} a_i$$

символ i является локальным подстановочным символом, не имеющим смысла вне формулы (или имеет, например, в математике он может означать мнимую единицу, но при прочтении формулы об этом можно «забыть») Внутри же он обозначает индекс элемента ряда.

Кроме того, формула $A = \{ x \mid P(x) \}$ используется для задания имени (названия) множеству. В данном случае множество названо A . При помощи этого имени в дальнейшем ссылаются на данное множество. При этом часто предикат в правой части формулы записывается средствами, принятыми в той или иной области знаний (формулы, специальные знаки и т.д.).

Предложение « x является элементом множества A » также является высказыванием в указанных обозначениях. Для его краткого обозначения используется формула (читается «элемент x принадлежит множеству A »)

$$x \in A$$

Её можно рассматривать как высказывание о значении предиката, отражающего «свойство» «принадлежать множеству A ». Только в отличие от рассмотренной ранее формы записи, этому предикату не дано явного имени. Само же высказывание принимает логическое значение, например, для ситуации на рисунке можно написать

$$\begin{aligned} b \in A &= 1 \\ e \in A &= 0 \end{aligned}$$

Если некоторый предикат все же полагать истинным повсюду в предметной области, будем говорить, что он выделяет *универсальное множество* (иногда используют термин *вселенная рассмотрения*). В принятых обозначениях его легко определить следующей формулой

$$U = \{ x \mid 1 \}$$

Фактически эта запись означает, что предикат для любого своего значения аргумента дает истинное значение, потому в правой части формулы подстановочный символ отсутствует: не нужно знать его значение для вычисления логического значения предиката. Обычно такое универсальное множество обозначают символом U .

Аналогично определяется и *пустое множество*. Только в этом случае предикат везде вычисляется как логически ложное значение. Пустое множество обозначают символом \emptyset .

$$\emptyset = \{ x \mid 0 \}$$

Многие свойства предметной области строятся (определяются) как комбинации некоторых ранее оговоренных (определенных) свойств при помощи так называемых *логических связок*. Например, рассмотрим определение «целое неотрицательное число это натуральное число или число ноль». Здесь два предиката «натуральное число» и «число ноль» объединяются при помощи логической связки, отраженной в естественном языке союзным словом «или». Можно сказать, что в этом предложении два высказывания связываются в новое составное высказывание. То есть имеется некоторое соглашение (оно и выражено союзным словом) как, имея вычисленные логические значения двух высказываний, вычислить значение составного высказывания. Пусть предикат P обозначает свойство «быть натуральным числом», а предикат Q обозначает свойство «быть числом ноль». Соответствующие множества можно обозначить символами A и B и записать

$$A = \{ x \mid P(x) \}$$

$$B = \{ x \mid Q(x) \}$$

Комбинирование высказываний для получения нового свойства можно отразить следующей формулой, в примере интерпретируемой как «множество целых неотрицательных чисел»:

$$C = \{ x \mid P(x) \vee Q(x) \}$$

Здесь символ \vee обозначает комбинацию двух логических значений для получения третьего значения так, чтобы эта комбинация отражала желаемое поведение в этом отношении союзного слова «или». Его можно рассматривать как некоторую операцию над логическими значениями, подобно тому, как символ $+$ может обозначать операцию сложения для числовых значений в математике. Но в отличие от математики, где многие свойства операций и способы их задания довольно сложны из-за потенциальной неограниченности предметной области, в логической области задать значения для всех возможных комбинаций *операндов* определяемой операции очень просто: надо перечислить все эти комбинации и указать значения для вычисления результата операции для каждой из них. Это задание можно оформить в виде таблицы или списка. Например, рассматриваемую операцию, назовем её *ЛОГИЧЕСКОЕ ИЛИ*, можно задать двумерной таблицей

		Правые операнды	
		\vee	
Левые операнды		0	1
	0	0	1
	1	1	1

Операцию ЛОГИЧЕСКОЕ ИЛИ называют также *ДИЗЬЮНКЦИЕЙ*.

Еще одной формой таблицы может быть одномерная, когда все комбинации аргументов выписаны в столбце заголовков:

u	v	$u \vee v$
0	0	0
0	1	1
1	0	1
1	1	1

То есть $0 \vee 0 = 0$, $0 \vee 1 = 1$, $1 \vee 0 = 1$, $1 \vee 1 = 1$. Имеются всего четыре комбинации значения аргументов, они все перечислены и для каждой комбинации указано значение. Отметим, что операция для двух операндов называется *бинарной операцией*. Она может также рассматриваться как функция двух аргументов. Но выражения легче воспринимаются, если символ операции ставить между двух операндов для обозначения вычисления логического значения в виде формулы. Такая форма записи называется *инфиксной записью*. В этом случае говорят о левых и правых её операндах.

Таким образом, бинарным логическим связкам соответствуют бинарные логические операции. Можно сказать, что это операции или функции двух аргументов на логической области.

Кроме логических операций, можно рассматривать построение сложных высказываний из простых как результат некоторой операции над множествами, заданными соответствующими предикатами. Например, рассмотренная выше логическая связка задает объединение множеств. Эта операция обозначается символом \cup . Пишут

$$C = A \cup B$$

При этом для операции объединения в рассмотренных обозначениях можно дать следующее определение:

$$A \cup B = \{ x \mid x \in A \vee x \in B \}$$

Здесь предикаты, определяющие принадлежность элементов множеств, не имеют явного имени. Еще раз обратите внимание, что x здесь просто подстановочный символ, не имеющий смысла вне формулы.

Операции над множествами, определяемые при помощи логических связок над предикатами, определяющими принадлежность элементов множеств-операндам, называют теоретико-множественными операциями.

Еще проще рассмотреть так называемую унарную связку – ЛОГИЧЕСКОЕ ОТРИЦАНИЕ. Еще раз посмотрите на пример с множеством из трех литер a, b, c в области из пяти литер a, b, c, d, e . Можно заметить, что не только предикат P своим логически истинным значением выделяет некоторое множество A , но и литеры, на которых предикат принимает ложное значение тоже можно представить как множество. Для этого надо представить предикат Q с логическими значениями, противоположными значениям предиката P : где $P(x) = 1$ там $Q(x) = 0$ и наоборот, где $P(x) = 0$ там $Q(x) = 1$. Это и определяет унарную связку ЛОГИЧЕСКОЕ ОТРИЦАНИЕ, которой соответствует приведенная ниже таблица и символ для обозначения в логических формулах \neg .

x	$\neg x$
0	1
1	0

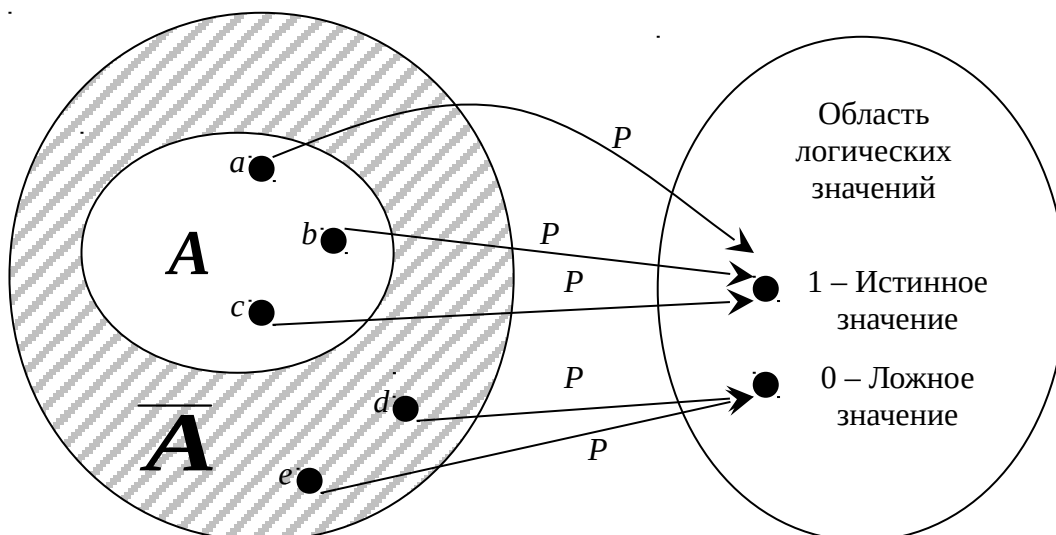
Здесь \neg – префиксный символ (т.е. относится к ближайшему стоящему от него справа высказыванию, например, можно написать $Q(x) = \neg P(x)$). Эту связку также называют связкой НЕ, так как при «переводе» предложений с естественного для предметной области языка на формульную запись в математической логике этой связке соответствуют фразы вида «неверно что ...».

Выделяемое таким образом множество и соответствующая теоретико-множественная операция называется дополнением. Она определяется следующим образом:

$$\overline{A} = \{ x \mid \neg x \in A \}$$

Обозначением для этой операции служит черта над множеством-операндом. Иногда употребляют также знак минус слева: $-A = \{ x \mid \neg x \in A \}$.

Дополнение можно наглядно представить как внешнюю область по отношению к выделенному множеству на схеме, использованной в примере (на рисунке выделено наклонной штриховкой).



Вообще можно составить четыре различные унарные логические операции (логические функции одного аргумента), так как есть две возможности для значения операнда и для каждого из этих двух значений можно выбрать значение результата двумя способами. В таблице показаны все возможные способы.

Аргумент	Возможные функции			
x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1

Функции f_1 и f_4 неинтересны, являются константами. Будем говорить, что их аргумент *фиктивен*. Остальные две имеют *существенную* зависимость от аргумента, необходимо знать его значение для вычисления значения функции. Но функция f_2 мало полезна, так как не вносит никаких изменений в логическое значение, всегда выполняется условие $f_2(x) = x$. Оставшаяся функция f_3 реализует поведение логической связки НЕ: всегда $f_3(x) = \neg x$. Поэтому не вводится каких-либо других унарных связок.

Рассмотрим теперь бинарные связки (логические функции двух аргументов) с позиции наличия или отсутствия у них фиктивных аргументов. Всего возможно 16 бинарных логических операций – имеется 4 комбинации значений аргументов и для каждой комбинации можно задать значение операции двумя способами (и вообще для n аргументов возможно 2^{2^n} операций). Если их все свести в одну таблицу, будем иметь:

	Номера возможных функций двух аргументов u и v															
$u \ v$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0 0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0 1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1 0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1 1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

При таком заполнении таблицы функции-константы располагаются в столбцах 1 и 16. В столбцах 11 и 13 располагаются функции, повторяющие значения одного из своих

аргументов, а в столбцах 4 и 6 – вычисляющие значение отрицания одного из аргументов. При этом оставшийся аргумент является фиктивным. Если исключить из рассмотрения указанные случаи, останется 10 функций, существенно зависящих от обоих аргументов. Можно сказать, они заслуживают того, чтобы дать им названия и инфиксные символы, чтобы компактно представлять различные бинарные связи в формулах. Приведем сначала таблицу инфиксных обозначений для операций с операндами u и v .

$u \ v$	$\&$	\vee	\oplus	$ $	\downarrow	\leftrightarrow	\rightarrow	\leftarrow	\Rightarrow	\Leftarrow
0 0	0	0	0	1	1	1	1	1	0	0
0 1	0	1	1	1	0	0	1	0	0	1
1 0	0	1	1	1	0	0	0	1	1	0
1 1	1	1	0	0	0	1	1	1	0	0

Символ $\&$ обозначает связку **ЛОГИЧЕСКОЕ И** (называемая также **КОНЪЮНКЦИЕЙ**). Назначение понятно из названия: необходимо выполнение одновременно двух свойств для того, чтобы составное высказывание считать истинным. Соответственно, в естественном языке этому соответствует союзное слово «и». Операция \vee (**ЛОГИЧЕСКОЕ ИЛИ, ДИЗЪЮНКЦИЯ**) уже рассмотрена на примере.

Далее следует связка **ИСКЛЮЧАЮЩЕЕ ИЛИ** (символ \oplus). Она может использоваться для представления суждений вида «только одно из двух». Обратите также внимание, что для того, чтобы значение составного высказывания было истинным нужно, чтобы значения высказываний-операндов были различны. Поэтому другая интерпретация операции – представление логического отношения «не равно» (может использоваться наравне с символом \neq между логическими выражениями).

Следующие три операции могут быть рассмотрены как отрицания первых трех. Операция, обозначенная символом $|$, называется **ШТРИХ ШЕФФЕРА** и представляет выражения вида «неверно, что u и v ». Сокращенно её можно назвать **НЕ-И**. Аналогично операция \downarrow представляет выражения вида «неверно, что u или v » и называется **СТРЕЛКА ПИРСА** (или сокращенно **НЕ-ИЛИ**). Далее идет операция отрицания от **ИСКЛЮЧАЮЩЕГО ИЛИ** называемая **ЛОГИЧЕСКАЯ ЭКВИВАЛЕНТНОСТЬ** (символ \leftrightarrow). То есть её можно использовать наряду с символом $=$ в логических формулах, результат будет истинным, когда значения аргументов одинаковые. Также её можно использовать для представления высказываний вида « u тогда и только тогда, когда v ».

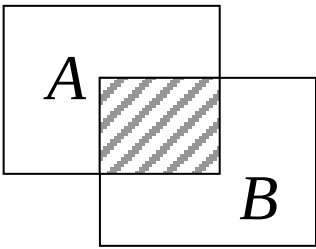
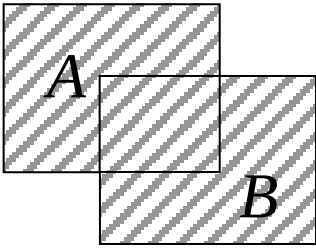
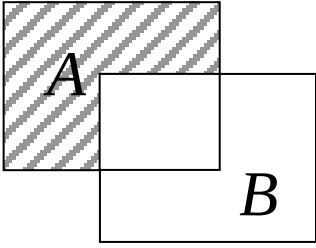
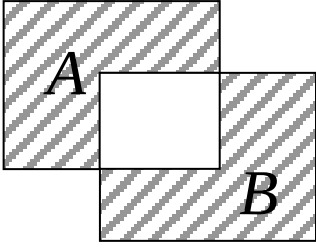
Первые шесть из приведенных операций **коммутативные**, то есть не зависят от порядка высказываний (логических аргументов) в формуле. Если их представить двумерными таблицами, как это сделано выше для \vee , таблицы окажутся симметричными относительно диагонали. Оставшиеся четыре операции не являются коммутативными.

Операция, обозначенная символом \rightarrow , называется **ИМПЛИКАЦИЯ**. Она представляет суждения вида «если u то v ». То есть единственной комбинацией значений операндов, на которых значение выражения будет ложным, является комбинация $u=1$ и $v=0$. Эта операция чувствительна к порядку следования операндов.

Остальные три операции могут быть получены из импликации путем перемены мест операндов и добавления отрицания перед высказыванием. Не будем давать им имена. И обозначения в таблице не являются общеупотребительными, так как соответствующие им фразы, во-первых, достаточно редкие, и, во-вторых, могут быть переформулированы с использованием приведенных ранее связок, например, можно выразить связку \Rightarrow через связки $\&$ и \neg : $u \Rightarrow v = u \& \neg v$. В том, что формулы $u \Rightarrow v$ и $u \& \neg v$ эквивалентны, можно убедиться, непосредственно вычислив их для всех возможных значений u и v . В таблице они приведены для полноты как удовлетворяющие критерию отсутствия фиктивных аргументов.

Замечание: ранее приведенные связки тоже могут быть выражены друг через друга. Подробнее этот вопрос обсуждается позднее.

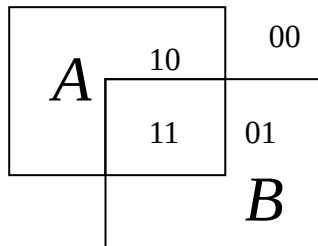
С использованием перечисленных логических связок определяются теоретико-множественные операции. Бинарных теоретико-множественных операций можно определить столько же, сколько и логических, и между ними будет *взаимнооднозначное соответствие*. Но общеупотребительных операций над множествами еще меньше, чем логических. Приведем их в виде таблицы.

Обозначение и название		Соответствующая логическая связка	Определение и иллюстрирующая диаграмма
\cap	Пересечение	$\&$	$A \cap B = \{ x \mid x \in A \& x \in B \}$ 
\cup	Объединение	\vee	$A \cup B = \{ x \mid x \in A \vee x \in B \}$ 
\setminus	Разность	\nrightarrow	$A \setminus B = \{ x \mid x \in A \nrightarrow x \in B \}$ 
$\dot{-}$	Симметрическая разность	\oplus	$A \dot{-} B = \{ x \mid x \in A \oplus x \in B \}$ 

Замечание: так как для связки \nrightarrow нет общеупотребительного названия, определение для разности обычно пишут в виде $A \setminus B = \{ x \mid x \in A \& \neg x \in B \}$.

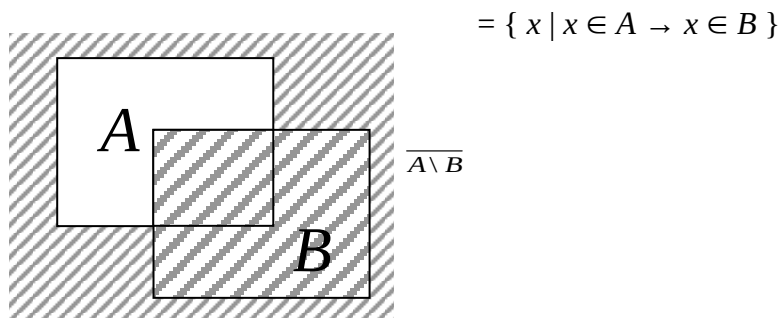
Приведенные диаграммы, иллюстрирующие определения, называются *диаграммами Венна*. Их можно представить сокращенным вариантом рассмотренных ранее графических схем представления суждений о множествах на воображаемой предметной области. Оставлены только области, представляющие сами множества (в

данном случае прямоугольниками, чаще рисуют круги). Область, соответствующая результату, отмечена штриховкой. Важно обратить внимание, что такая диаграмма представляет все четыре возможные комбинации логических значений аргументов логической операции-связки – значений высказываний $x \in A$ и $x \in B$ – 00, 01, 10, 11. Две пересекающиеся области разбивают плоскость на четыре части. Значения комбинаций для выбранной формы диаграммы могут быть нанесены на нее так:

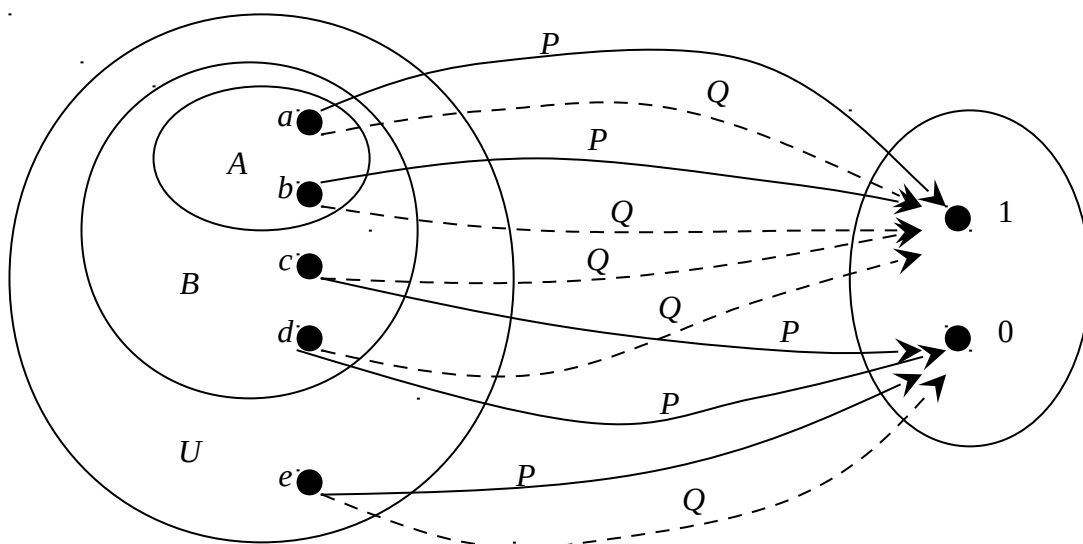


Область для комбинации 00 лежит вне обведенных областей-множеств. Только когда все возможные комбинации представимы, диаграмма Венна может использоваться для иллюстрации операции с множествами или представления некоторого суждения. В общем случае для n высказываний (а не двух, как для бинарных операций) требуется изобразить разбиение плоскости на 2^n частей и диаграммы теряют наглядность.

Может возникнуть потребность представить также операции, для которых определяющая связка принимает истинное значение в области, где все высказывания-операнды являются ложными. В этом случае будем штриховать внешнюю область вплоть до некоторой воображаемой границы (границы предметной области). Например, если захотим представить множество, определяемое связкой \rightarrow , будем изображать это так:



Собственно кроме высказываний самих по себе, приходится иметь дело с суждениями о высказываниях по отношению друг к другу. Рассмотрим следующую диаграмму:



Допустим, предметная область состоит из объектов – литер a, b, c, d, e . На ней задано сразу два свойства, представленных предикатами P и Q . При этом значения предикатов, соответственно рисунку, можно свести в таблицу

X	$P(x)$	$Q(x)$	$P(x) \rightarrow Q(x)$
A	1	1	1
B	1	1	1
C	0	1	1
D	0	1	1
E	0	0	1
Итог по &			1

В таблице также приведено значение логического выражения $P(x) \rightarrow Q(x)$ для всех возможных значений аргументов предикатов. Это все интерпретации данного выражения в предметной области (в универсальном множестве U). В таблице показано, что во всех интерпретациях это выражение оказывается логически истинным (=1). На естественном языке такое взаимное свойство высказываний можно выразить фразой «всегда, когда P тогда и Q ». В логике для краткой записи этого факта применяют специальную символическую формулу (читается «для любого x если $P(x)$ то $Q(x)$ »):

$$\forall x (P(x) \rightarrow Q(x))$$

Она подчёркивает, какой из символов является подстановочным для формулы в том смысле, что на его место можно подставить любой символ, обозначающий конкретный объект из предметной области и получить истинное высказывание, вычислив значения предикатов для данного символа. Например:

$$P(a) \rightarrow Q(a) (1 \rightarrow 1=1),$$

$$P(c) \rightarrow Q(c) (0 \rightarrow 1=1),$$

$$P(e) \rightarrow Q(e) (0 \rightarrow 0=1).$$

Символ \forall , предвещающий формулу, называется *квантором всеобщности*. В целом формула тоже является высказыванием (принимает логическое значение). Чтобы его наглядно представить, обычно записывают символическое определение для данного квантора:

$$\forall x \Phi(x) = \bigwedge_{x \in U} \Phi(x)$$

То есть если некоторая формула Φ , в которую символ x входит в виде аргументов предикатов, предварена квантором всеобщности, после которого следует этот же символ x , она понимается как «объединение» по логической связке «И» всех способов записи этой формулы с подстановкой на место этого символа обозначений объектов предметной области. Так как такая формула может быть достаточно сложной, обычно используются скобки для указания ее границ. В пределах такой формулы символ x следует рассматривать как локальный подстановочный символ в соответствии с оговоренными соглашениями о записи формул.

В таблице выполнимость формулы на всех интерпретациях отмечено в последней строке (Итог по &). Такое взаимное отношение двух высказываний называют *логическим следованием*. Можно также сказать, что выполнение свойства P влечёт за собой выполнение свойства Q . Выполнимость на всех интерпретациях (на предметной области) некоторой формулы (в данном случае формулы $P(x) \rightarrow Q(x)$) называется *общезначимостью*. В случае, если две формулы, представляющей собой высказывание, объединены в одну через связку \rightarrow , и такая формула общезначима, будем говорить, что вторая формула является *логическим следствием* первой. Для этого будем использовать следующее обозначение:

$$\Phi_1 \Rightarrow \Phi_2$$

Здесь Φ_1 и Φ_2 – формулы, являющиеся высказываниями, и при этом формула $\Phi_1 \rightarrow \Phi_2$ общезначима. Это значит, что в их состав входят некоторое множество литер, которые могут рассматриваться как подстановочные символы, и для всех возможных их комбинаций формула $\Phi_1 \rightarrow \Phi_2$ тождественно равна 1 (истинному значению). Встречается также запись вида $\Phi_1 \rightarrow \Phi_2 \equiv 1$.

На диаграмме также показаны выделенные данными предикатами области – множества $A = \{ x \mid P(x) \}$ и $B = \{ x \mid Q(x) \}$. Обратите внимание, что при таких значениях предикатов область для множества A целиком лежит внутри области для множества B . Тогда будем говорить, что множество A *содержится* во множестве B , или что A *включается* в B или что A является *подмножеством* в B . Будем обозначать это в виде формулы символом \subseteq .

$$A \subseteq B = \forall x (x \in A \rightarrow x \in B)$$

Можно также написать $(A \subseteq B) = (x \in A \Rightarrow x \in B)$. Здесь имеется в виду, что подстановочным символом является только x . В этом смысле использование формул с квантором всеобщности предпочтительнее, так как они явно указывают, какие символы являются подстановочными.

Кроме выполнимости на всех интерпретациях формулы со связкой \rightarrow , рассмотрим общезначимость формулы со связкой \leftrightarrow , то есть формулы вида $\Phi_1 \leftrightarrow \Phi_2$. Тогда говорят, что задаваемые формулами Φ_1 и Φ_2 высказывания логически эквивалентны или *равносильны*. Если эти формулы есть предикаты, определяющие множества, то такие множества называют *равными*. Можно записать

$$(A = B) = \forall x (x \in A \leftrightarrow x \in B)$$

$$\text{или } (A = B) \Leftrightarrow (x \in A \Leftrightarrow x \in B).$$

Общезначимость логических формул и доказательства свойств теоретико-множественных операций. Таблицы истинности и диаграммы Венна. Методики доказательств.

Логическое следствие и равносильность высказываний очень часто встречается в различных областях знаний, как при построении формализованных описаний, так и в процессе работы с моделями. Пример: рассмотрим фразу «если вещество является металлом, то оно электропроводно». Здесь два свойства (предиката, а также множества), одно «быть металлом» другое «быть электропроводным». По своему строению она соответствует схеме $P(x) \rightarrow Q(x)$. Слово «вещество» и местоимение «оно» играют роль подстановочного символа. Можно также построить фразу «любое вещество, если является металлом, является электропроводным». Здесь еще указывается, что формула общезначима (на предметной области веществ – химических элементов). То есть формула имеет вид $\forall x (P(x) \rightarrow Q(x))$. Является ли эта формула истинным высказыванием? Ответить на этот вопрос сложно, не разбираясь во внутренних понятиях соответствующей области знаний (в данном примере – физической химии).

А вот пример другого вида. Рассмотрим высказывание

$$\forall x ((P(x) \vee (Q(x) \& R(x))) \leftrightarrow ((P(x) \vee Q(x)) \& (P(x) \vee R(x))))$$

При этом не будем оговаривать предметную область, и задавать на ней значения предикатов P , Q и R . Тем не менее, можно утверждать, что какова бы ни была эта предметная область с заданными на ней предикатами, данная формула будет общезначимой. Чтобы понять это, обозначим все вхождения высказываний $P(x)$, $Q(x)$ и $R(x)$ символами a , b и c соответственно. При такой замене формула, стоящая под квантором всеобщности, приобретет вид

$$(a \vee (b \& c)) \leftrightarrow ((a \vee b) \& (a \vee c))$$

Можно себе представить, что символы a , b и c представляют логические значения соответствующих предикатов для некоторого значения их аргументов. Независимо от поведения предикатов, максимально возможно получить до 8 комбинаций их логических значений (3 символа по 2 возможных значения для каждого). При этом общая формула для любой из этих комбинаций будет логически истинной. Это можно проверить непосредственным вычислением по таблице.

a	b	c	$b \& c$	$a \vee b$	$a \vee c$	$a \vee (b \& c)$	$(a \vee b) \& (a \vee c)$	Л.Ч. \leftrightarrow П.Ч.
0	0	0	0	0	0	0	0	1
0	0	1	0	0	1	0	0	1
0	1	0	0	1	0	0	0	1
0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	1	1	1	1	1	1	1	1
Итог по $\&$								1

Здесь сокращение Л.Ч. обозначает часть формулы слева от связки \leftrightarrow , а сокращение П.Ч. – правую. Можно сказать, в данном случае формула является общезначимой в силу своей структуры, а не в силу определенного поведения входящих в неё предикатов (фактически мы упростили её до вида $\forall x (1)$). Ситуация здесь упрощается за счёт того,

что в рассмотренной формуле были выделены отдельные высказывания, многократно входящие в неё. При этом внутренняя структура высказываний не анализируется. Они рассматриваются как неделимые – *атомарные* высказывания. Это наиболее простая ситуация в математической логике. Формулы, которые можно представить как набор атомарных высказываний, связанных логическими связками, относят к классу формул *логики высказываний*. Общезначимость формул в логике высказываний всегда можно проверить перебором всех способов задания логических значений атомарным высказываниям и вычислением значения формулы для всех этих комбинаций логических значений.

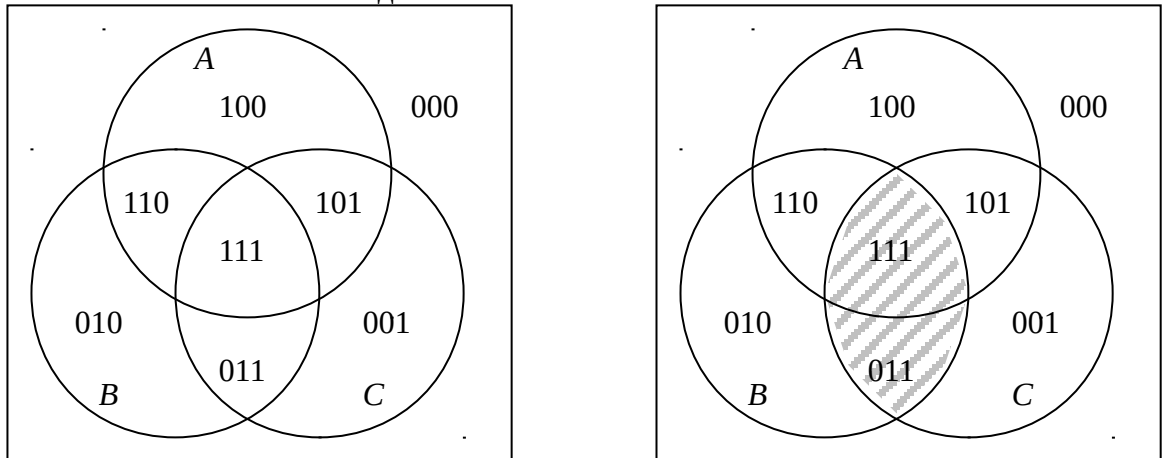
Рассмотренное логическое тождество $(a \vee (b \wedge c)) \leftrightarrow ((a \vee b) \wedge (a \vee c))$ может быть выражено и в терминах теоретико-множественных операций (в соответствии с определениями для операций над множествами):

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

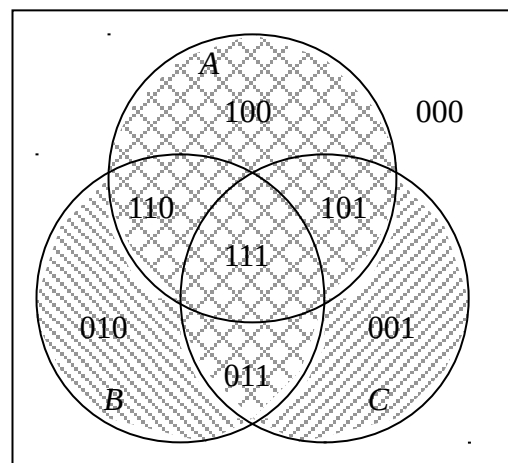
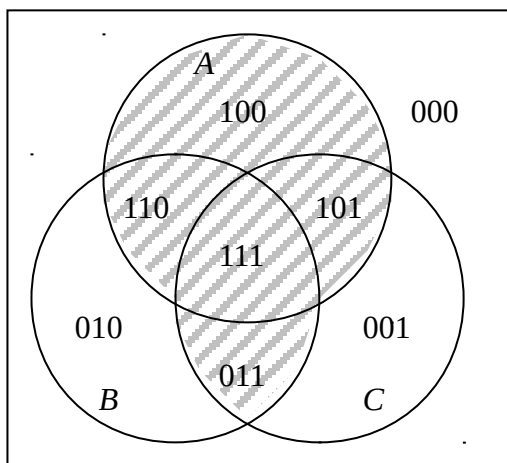
Эта формула соответствует такому сопоставлению высказываний: $a=x \in A$, $b=x \in B$, $c=x \in C$, в выражении $x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$, которое может быть преобразовано по определениям \cup и \cap как

$$\forall x ((x \in A \vee (x \in B \wedge x \in C)) \leftrightarrow ((x \in A \vee x \in C) \wedge (x \in A \vee x \in B)))$$

Приведём диаграмму Венна, иллюстрирующую это свойство. Для трёх множеств потребуется разбить плоскость на 8 областей взаимным расположением областей для множеств A , B и C . 8 областей подписаны значениями истинности высказываний a , b , c . В порядке скобок в левой части тождества отметим область $B \cap C$.



Теперь объединим область $B \cap C$ с областью A . Получим представление для выражения $A \cup (B \cap C)$. Для правой части отметим области $A \cup B$ и $A \cup C$ штриховкой различных направлений. Область пересечения штриховок дает наглядное представление об области $(A \cup B) \cap (A \cup C)$ и сравнение её с предыдущей картинкой демонстрирует равенство множеств.



Далее приводится набор наиболее употребительных тождеств для операций с множествами и соответствующих им тождеств для логических операций. Все они могут непосредственно доказаны при помощи таблиц или диаграмм Венна.

<i>Идемпотентность</i>	
$A \cap A = A$ $A \cup A = A$	$a \& a = a$ $a \vee a = a$
Двойное дополнение	Двойное отрицание
$\overline{(\overline{A})} = A$	$\neg(\neg a) = a$
<i>Формулы де Моргана</i>	
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	$\neg(a \vee b) = \neg a \& \neg b$ $\neg(a \& b) = \neg a \vee \neg b$
<i>Коммутативность (переместительный закон)</i>	
$A \cap B = B \cap A$ $A \cup B = B \cup A$ $A \div B = B \div A$	$a \& b = b \& a$ $a \vee b = b \vee a$ $a \oplus b = b \oplus a$
<i>Ассоциативность (сочетательный закон)</i>	
$A \cap (B \cap C) = (A \cap B) \cap C$ $A \cup (B \cup C) = (A \cup B) \cup C$ $A \div (B \div C) = (A \div B) \div C$	$a \& (b \& c) = (a \& b) \& c$ $a \vee (b \vee c) = (a \vee b) \vee c$ $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
<i>Дистрибутивность (распределительный закон)</i>	
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \div C) = (A \cap B) \div (A \cap C)$	$a \& (b \vee c) = (a \& b) \vee (a \& c)$ $a \vee (b \& c) = (a \vee b) \& (a \vee c)$ $a \& (b \oplus c) = (a \& b) \oplus (a \& c)$

Кроме метода непосредственной проверки, в математической логике рассматриваются и другие методы. Во-первых, большинство реальных задач не укладываются в рассмотренную схему формул логики высказываний – необходимо учитывать способы подстановки аргументов предикатов в формулы, предваряемые кванторами. Во-вторых, даже в логике высказываний с ростом числа атомарных высказываний перебор всех возможных комбинаций имеет экспоненциальную сложность (два в степени числа высказываний). Поэтому представляет интерес изучение методов, не использующих непосредственный перебор логических значений, а основанных на введении определённых правил преобразования текста формул – *правил логического вывода*. Развитой системой в математической логике является *логика предикатов* и соответствующее ей *исчисление предикатов*. Рассмотренные выше формулы укладываются в её схемы. Кроме того, в логике предикатов наряду с квантором всеобщности рассматривается также *квантор существования*, используемый для представления высказываний, утверждающих выполнимость формулы не на всей предметной области, а только на некотором её непустом подмножестве (не оговариваемом). Наиболее частая формулировка имеет вид «существует x такой, что для него выполняется свойство P ». Для представления таких высказываний формулами используется следующая запись

$$\exists x P(x)$$

Аналогично тому, как квантор всеобщности можно представить определяемым через связку $\&$ по предметной области, для квантора существования дают аналогичное «определение»:

$$\exists x \Phi(x) = \bigvee_{x \in U} \Phi(x)$$

Но с учетом того, что связку \vee можно выразить через связки $\&$ и \neg : $u \vee v = \neg(\neg u \& \neg v)$ можно и квантор \exists выразить через \forall :

$$\exists x P(x) = \bigvee_{x \in U} P(x) = \neg(\&_{x \in U} (\neg P(x))) = \neg(\forall x (\neg P(x)))$$

Вообще символами объединения и пересечения по некоторому *семейству множеств* (множеству S , элементами которого являются другие множества) обозначается следующее:

$$\bigcup_{B \in S} B = \{ x \mid \exists B (B \in S \& x \in B) \}$$

$$\bigcap_{B \in S} B = \{ x \mid \forall B (B \in S \rightarrow x \in B) \}$$

Обычно для выбора множества из семейства используется некоторая функция, например, индексация по множеству номеров (натуральных чисел): $B_i = f(i)$. В таком случае будем писать

$$\bigcup_{i \in \mathbb{N}} B_i = \bigcup_{B \in \{ A \mid \exists i (i \in \mathbb{N} \& A = B_i) \}}$$

Семейству $\{ A \mid \exists i (i \in \mathbb{N} \& A = B_i) \}$ в этом случае иногда не дают явного имени.

Различные методы доказательств, как приведенные здесь, так и другие, основанные на исчислениях высказываний, и построенные в соответствии с рассмотренными алгебраическими свойствами логических операций рассматриваются в ходе практических занятий по данной теме.

Рассмотрим в качестве примера метод проверки общезначимости формул, основанный на представлении структур высказываний – двоичных функций своих компонентов – так называемыми конъюнктивными формами.

Конъюнктивной формой называют формулы определенной структуры, содержащие только символы операций $\&$, \vee и \neg в произвольном количестве над некоторым множеством операндов, представляемых в формуле символами-литерами. В качестве литер используются буквы некоторого алфавита, например, латинского (что удобно при «ручной работе») или индексированные символы (что удобнее для более строго задания структуры таких формул). Структура конъюнктивной формы определяется следующим порядком или лучше сказать иерархией расположения операций:

- Отрицания \neg применяются только к литерам.
- Литеры и/или их отрицания соединяются при помощи символа операции \vee в части формул, называемые *термами*. Допускается также наличие всего одной литеры в терме (с отрицанием или без). В таком случае данный терм не содержит символа \vee .
- Термы (обычно для удобства понимания порядка применения операций взятые в скобки) соединяются при помощи символа операции $\&$ в формулу. Допускается формула, состоящая из единственного терма. В этом случае она не содержит символа $\&$.

Таким образом, если рассматривать структуру таких формул «снизу вверх», получается следующая иерархия символов операций:

- Нижний уровень: ЛОГИЧЕСКОЕ ОТРИЦАНИЕ, НЕ (символ \neg)
- Средний уровень: ЛОГИЧЕСКОЕ ИЛИ, ДИЗЬЮНКЦИЯ (символ \vee)
- Верхний уровень: ЛОГИЧЕСКОЕ И, КОНЪЮНКЦИЯ (символ $\&$)

Рассмотрим примеры конъюнктивных форм над литерами a, b, c, d .

(a)

В этом терме присутствует единственная литера без отрицания, и формула состоит из одного терма. Поэтому такая формула является конъюнктивной формой.

($\neg a$)

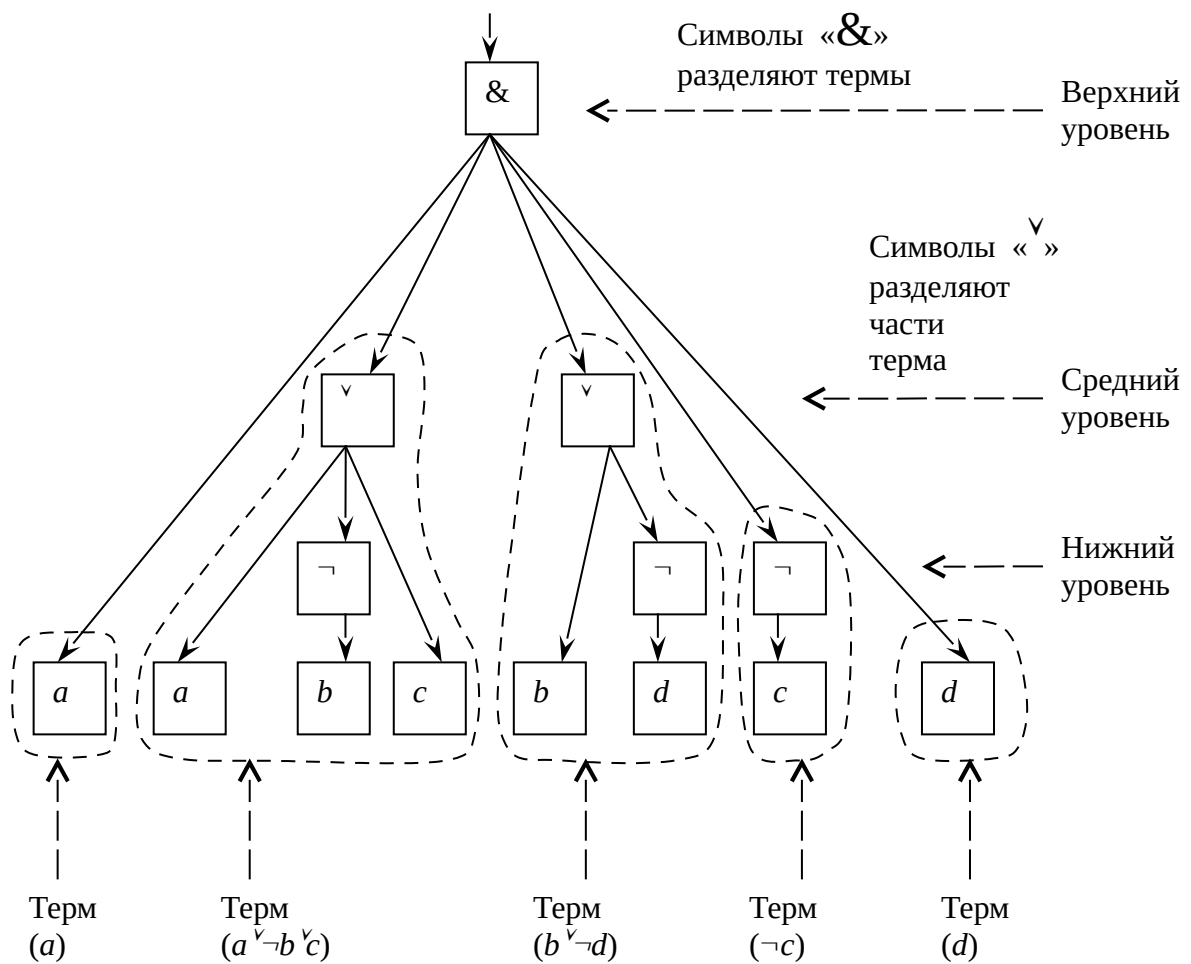
Это тоже конъюнктивная форма с одним термом из одной литерой с отрицанием.

($a \vee \neg b \vee c$)

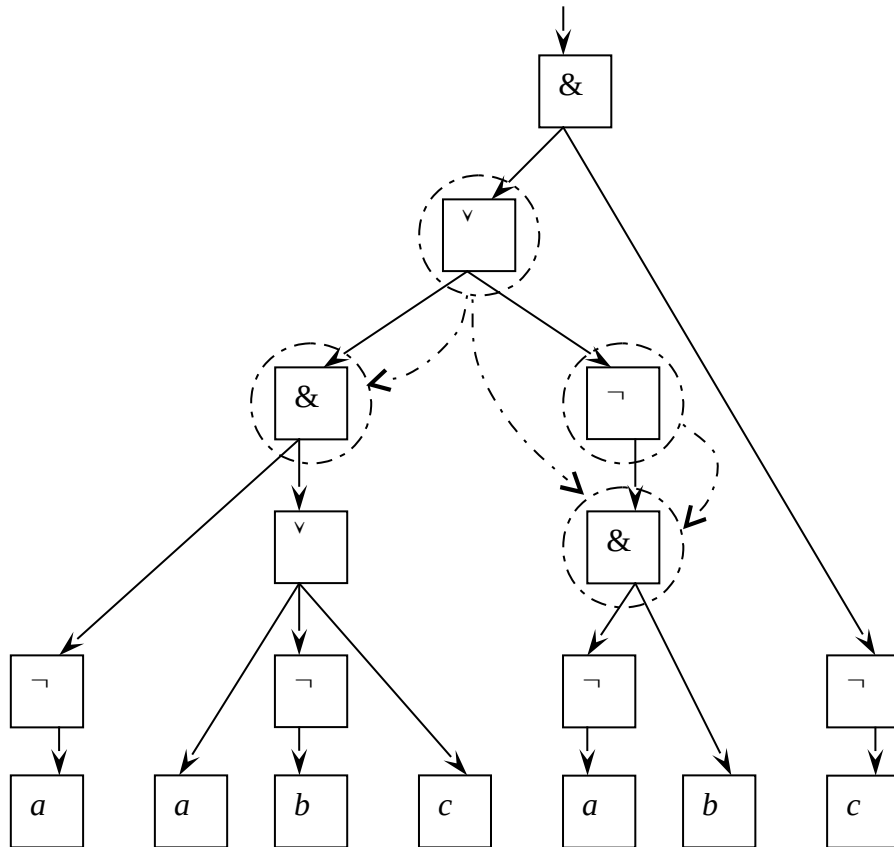
Это терм с тремя литерами a, b, c . Причем литера b входит в него с отрицанием. Он тоже является конъюнктивной формой.

(a) $\&$ ($a \vee \neg b \vee c$) $\&$ ($b \vee \neg d$) $\&$ ($\neg c$) $\&$ (d)

Это конъюнктивная форма из пяти термов. Отобразим в виде диаграммы структуру этой формулы.



Формула $((\neg a) \& (a \vee \neg b \vee c)) \vee \neg(\neg a \& b) \& (\neg c)$ вообще конъюнктивной формой не является, так как нарушает указанную иерархию символов операций. Следующая диаграмма поясняет, где нарушается иерархия.



Здесь штрихпунктирными линиями показано нарушение иерархии следования символов операций: двигаясь сверху вниз по стрелкам из некоторых узлов диаграммы, помеченных символами \vee или \neg , можно достичь узлы, помеченные символом $\&$.

Соответствующие места в тексте формулы отмечены стрелками на следующем рисунке.

$$(((\neg a) \& (a^{\vee} \neg b^{\vee} c))^{\vee} \neg (\neg a \& b)) \& (\neg c)$$

Символ \vee выше, чем $\&$
Символ \neg выше, чем $\&$

Оказывается, для любой формулы, в которой любые две части (взятые в скобки или являющиеся одиночными литерами и, возможно, предваряемые унарным символом \neg) разделяются любыми рассмотренными бинарными символами ($\&$, \vee , \oplus , \mid , \downarrow , \leftrightarrow , \rightarrow , \leftarrow , \Rightarrow , \Leftarrow), существует эквивалентная ей конъюнктивная форма над теми же литерами.

Под их эквивалентностью понимается общезначимость по всем возможным подстановкам логических значений литер в формулу из операции \leftrightarrow между исходной формулой и ее конъюнктивной формой, что обозначается знаком $=$. При этом следует учесть, что символы разделителей $\&$ и \vee отражают ассоциативные операции. Поэтому порядок вычисления \vee между частями терма и $\&$ между термами несущественен и не указывается расстановкой скобок.

Чтобы показать это, сначала приведем для каждой из рассмотренных бинарных связок их конъюнктивные формы над двумя литерами. При этом некоторые из исходных формул изначально удовлетворяют требованиям на состав и порядок операций и, таким образом, совпадают со своими конъюнктивными формами.

Исходная формула с бинарной операцией над двумя литерами	Ее конъюнктивная форма
$u \& v$	$(u) \& (v)$
$u \vee v$	$(u \vee v)$
$u \oplus v$	$(\neg u \vee \neg v) \& (u \vee v)$
$u \mid v$	$(\neg u \vee \neg v)$
$u \downarrow v$	$(\neg u) \& (\neg v)$
$u \leftrightarrow v$	$(\neg u \vee v) \& (u \vee \neg v)$
$u \rightarrow v$	$(\neg u \vee v)$
$u \leftarrow v$	$(u \vee \neg v)$
$u \nrightarrow v$	$(u) \& (\neg v)$
$u \nleftarrow v$	$(\neg u) \& (v)$

Эквивалентность исходных формул с их соответствующими конъюнктивными формами проверяется непосредственным вычислением по четырем возможным интерпретациям значений литер. Например:

u	v	$u \downarrow v$	$(\neg u) \& (\neg v)$	$(u \downarrow v) \leftrightarrow ((\neg u) \& (\neg v))$
0	0	1	1	1
0	1	0	0	1
1	0	0	0	1
1	1	0	0	1
Итог по $\&$:				1

Можно заметить, что рассмотренные конъюнктивные формы бинарных операций не определяются однозначно. Например, формулу $u \downarrow v$ можно также представить эквивалентной конъюнктивной формой $(\neg u \vee v) \& (u \vee \neg v) \& (\neg u \vee \neg v)$:

u	v	$u \downarrow v$	$\neg u \vee v$	$u \vee \neg v$	$\neg u \vee \neg v$	$(\neg u \vee v) \& (u \vee \neg v) \& (\neg u \vee \neg v)$	$(u \downarrow v) \leftrightarrow ((\neg u \vee v) \& (u \vee \neg v) \& (\neg u \vee \neg v))$
0	0	1	1	1	1	1	1
0	1	0	1	0	1	0	1
1	0	0	0	1	1	0	1
1	1	0	1	1	0	0	1
Итог по $\&$:							1

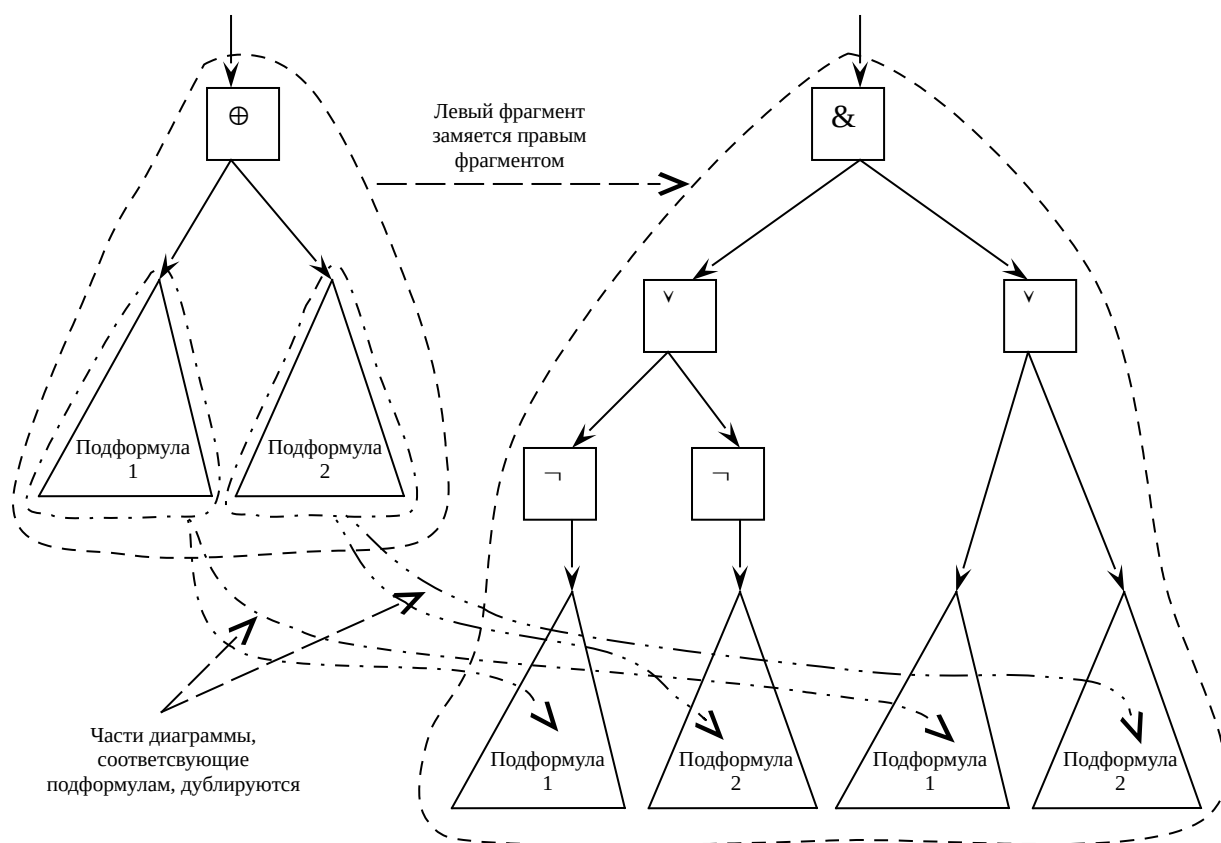
Вообще, если не накладывать дополнительных ограничений в определении структуры и состава конъюнктивной формы, у каждой из рассмотренных формул будет бесчисленное множество конъюнктивных форм, так как повторение текста терма или присоединение терма, тождественно равного 1 (например $(v \vee \neg v)$) сохраняет рассмотренную эквивалентность формул. Эквивалентность формул сохраняется также при перестановке термов и/или частей терма ввиду коммутативности $\&$ и \vee . В таблице выше были приведены минимальные по сложности конъюнктивные формы бинарных операций.

Имея представления для всех бинарных операций, покажем, что любую формулу над некоторым множеством литер, построенную только при помощи символов бинарных и унарных операций и скобок, привести к эквивалентной формуле, построенной только при помощи символов $\&$, \vee и \neg . Для этого нужно заменить вхождения символов операций,

отличных от $\&$, \vee и \neg на их представления через $\&$, \vee и \neg по формулам из таблицы. Обратите внимание, что при этом сложность формулы может возрасти, так как некоторые операции (а именно, \oplus и \leftrightarrow) представляются в виде конъюнкции двух термов, в каждый из которых входят по две подформулы исходной формулы. То есть, для них производят замену по схеме (на примере \oplus)

$$\begin{aligned} &(\text{Подформула1}) \oplus (\text{Подформула2}) = \\ &= (\neg(\text{Подформула1}) \vee \neg(\text{Подформула2})) \& ((\text{Подформула1}) \vee (\text{Подформула2})). \end{aligned}$$

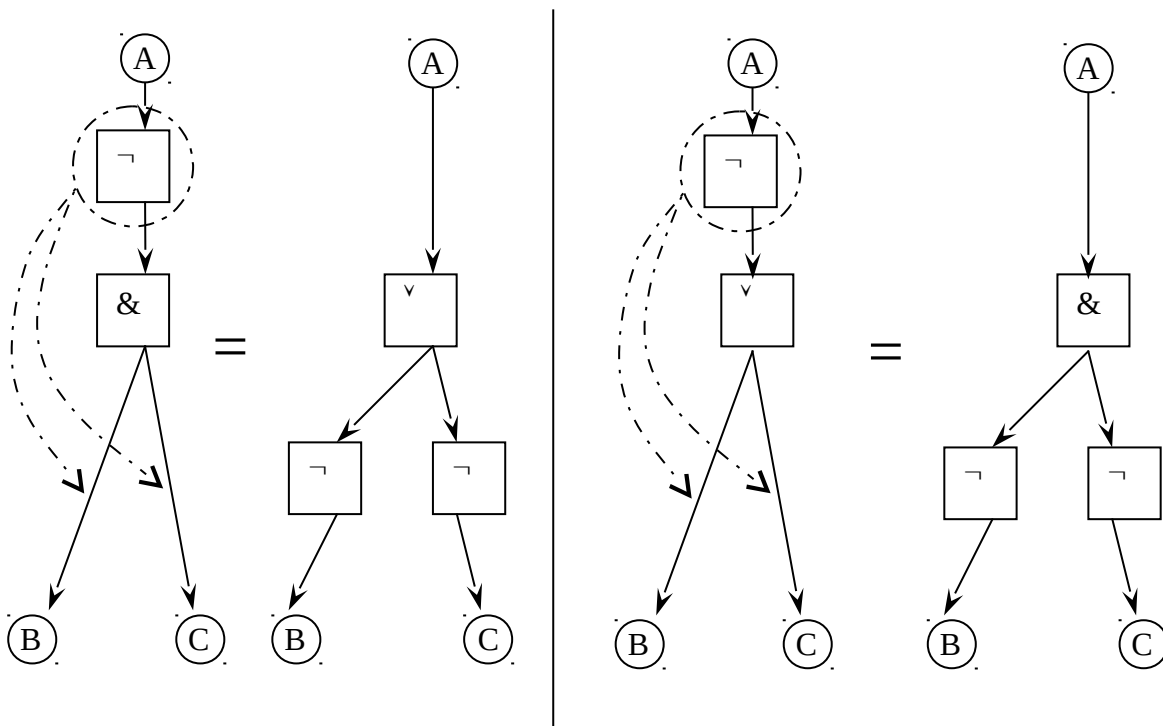
Фактически это приводит к удвоению длины текста, представляющего некоторую часть исходной формулы. То же касается и представления формулы диаграммой.



После получения формулы, содержащий только символы операций $\&$, \vee и \neg , следует получить эквивалентную ей формулу, в которой операции применяются только к литерам, а не к подформулам, содержащим символы операций. Для этого воспользуемся следующими уже известными свойствами:

$$\begin{aligned} \neg(a \vee b) &= \neg a \& \neg b \\ \neg(a \& b) &= \neg a \vee \neg b \\ \neg(\neg a) &= a \end{aligned}$$

Первые две формулы, называемые формулами Де-Моргана, позволяют опускать отрицания сквозь узлы по диаграмме. И при этом символы бинарных операций претерпевают замену: $\&$ меняется на \vee и наоборот, \vee меняется на $\&$. Следующая диаграмма иллюстрирует процесс опускания отрицаний.

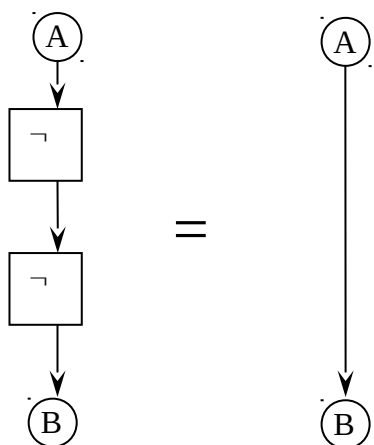


Аналогично следует поступать и когда в подформуле более двух частей разделяются символом $\&$ или \vee .

$$\neg(a \vee b \vee c \vee \dots \vee e) = \neg a \& \neg b \& \neg c \dots \& \neg e$$

$$\neg(a \& b \& c \& \dots \& e) = \neg a \vee \neg b \vee \neg c \dots \vee \neg e$$

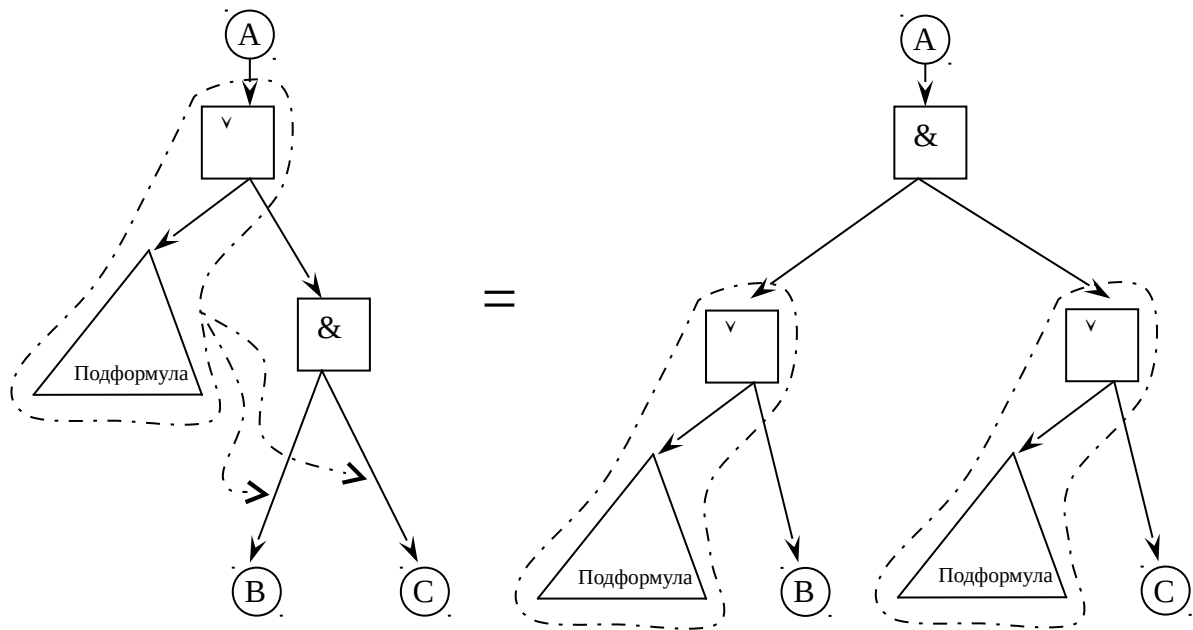
При опускании отрицаний возможно, что они войдут в непосредственный контакт в формуле или диаграмме. В этом случае необходимо воспользоваться формулой двойного отрицания $\neg(\neg a) = a$ и устранить их.



Эти этапы преобразований выполняют до тех пор, пока отрицания не займут самый нижний уровень в формуле. После этого следует приступить к упорядочению иерархии только операций $\&$ и \vee . Для этого воспользуемся дистрибутивным свойством (распределительным законом) \vee относительно $\&$.

$$a \vee (b \& c) = (a \vee b) \& (a \vee c)$$

На этом этапе сложность формулы опять может возрасти, так как применение этой формулы опять приводит к дублированию ее частей. Зато символы \vee опускаются ниже символов $\&$ (и символы $\&$ поднимаются над \vee).



Аналогично формулам Де-Моргана, распределительный закон можно применять и к формулам с более чем двумя частями, разделяемыми символом $\&$:

$$a \vee (b \& c \& \dots \& e) = (a \vee b) \& (a \vee c) \& \dots \& (a \vee e)$$

Этот этап выполняется до тех пор, пока возможно применение данного правила преобразования. После этого полученная формула будет конъюнктивной формой. Тем самым показано, что эквивалентная конъюнктивная форма существует у любой логической формулы.

Полученный результат можно несколько упростить, если воспользоваться свойством идемпотентности для операции \vee для литер или их отрицаний.

$$\begin{aligned} a \vee a &= a \\ \neg a \vee \neg a &= \neg a \end{aligned}$$

А с учетом идемпотентности $\&$ ($a \& a = a$), можно исключить дублирование идентичных по составу литер термов.

Пример:

Построим конъюнктивную формулу для формулы $\neg(a \rightarrow ((b \& \neg d) \oplus c)) \vee (c \leftrightarrow d)$.

Этап 1. Выражаем \rightarrow , \oplus и \leftrightarrow через $\&$, \vee и \neg .

$$\begin{aligned} \neg(a \rightarrow ((b \& \neg d) \oplus c)) \vee (c \leftrightarrow d) &= \\ = \neg(\neg a \vee ((\neg(b \& \neg d) \vee \neg c) \& ((b \& \neg d) \vee c))) \vee ((\neg c \vee d) \& (c \vee \neg d)) \end{aligned}$$

Этап 2. Опускаем отрицания до литер формулы.

$$\begin{aligned}
& \neg(\neg a^{\vee}((\neg(b \& \neg d)^{\vee} \neg c) \& ((b \& \neg d)^{\vee} c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (\neg \neg a \& \neg((\neg b^{\vee} \neg \neg d^{\vee} \neg c) \& ((b \& \neg d)^{\vee} c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (a \& \neg((\neg b^{\vee} d^{\vee} \neg c) \& ((b \& \neg d)^{\vee} c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (a \& (\neg(\neg b^{\vee} d^{\vee} \neg c)^{\vee} \neg((b \& \neg d)^{\vee} c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (a \& ((\neg \neg b \& \neg d \& \neg \neg c)^{\vee} (\neg(b \& \neg d) \& \neg c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (a \& ((b \& \neg d \& c)^{\vee} (\neg(b \& \neg d) \& \neg c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (a \& ((b \& \neg d \& c)^{\vee} (\neg b^{\vee} \neg \neg d) \& \neg c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (a \& ((b \& \neg d \& c)^{\vee} (\neg b^{\vee} d) \& \neg c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d))
\end{aligned}$$

Этап 3. Опускаем дизъюнкции ниже конъюнкций (раскрываем скобки).

$$\begin{aligned}
& (a \& ((b \& \neg d \& c)^{\vee} (\neg b^{\vee} d) \& \neg c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = (a \& (((b \& \neg d \& c)^{\vee} (\neg b^{\vee} d)) \& ((b \& \neg d \& c)^{\vee} c)))^{\vee}((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = \quad a \& (b^{\vee} \neg b^{\vee} d) \& (\neg d^{\vee} \neg b^{\vee} d) \& (c^{\vee} \neg b^{\vee} d) \& (b^{\vee} \neg c) \& (\neg d^{\vee} \neg c) \& (c^{\vee} \neg c))^{\vee} \\
& \quad \vee ((\neg c^{\vee} d) \& (c^{\vee} \neg d)) = \\
& = \quad (a^{\vee} ((\neg c^{\vee} d) \& (c^{\vee} \neg d))) \& \\
& \quad \& (b^{\vee} \neg b^{\vee} d^{\vee} ((\neg c^{\vee} d) \& (c^{\vee} \neg d))) \& \\
& \quad \& (\neg d^{\vee} \neg b^{\vee} d^{\vee} ((\neg c^{\vee} d) \& (c^{\vee} \neg d))) \& \\
& \quad \& (c^{\vee} \neg b^{\vee} d^{\vee} ((\neg c^{\vee} d) \& (c^{\vee} \neg d))) \& \\
& \quad \& (b^{\vee} \neg c^{\vee} ((\neg c^{\vee} d) \& (c^{\vee} \neg d))) \& \\
& \quad \& (\neg d^{\vee} \neg c^{\vee} ((\neg c^{\vee} d) \& (c^{\vee} \neg d))) \& \\
& \quad \& (c^{\vee} \neg c^{\vee} ((\neg c^{\vee} d) \& (c^{\vee} \neg d))) = \\
& = \quad (a^{\vee} \neg c^{\vee} d) \& \\
& \quad \& (a^{\vee} c^{\vee} \neg d) \& \\
& \quad \& (b^{\vee} \neg b^{\vee} d^{\vee} \neg c^{\vee} d) \& \\
& \quad \& (b^{\vee} \neg b^{\vee} d^{\vee} c^{\vee} \neg d) \& \\
& \quad \& (\neg d^{\vee} \neg b^{\vee} d^{\vee} \neg c^{\vee} d) \& \\
& \quad \& (\neg d^{\vee} \neg b^{\vee} d^{\vee} c^{\vee} \neg d) \& \\
& \quad \& (c^{\vee} \neg b^{\vee} d^{\vee} \neg c^{\vee} d) \& \\
& \quad \& (c^{\vee} \neg b^{\vee} d^{\vee} c^{\vee} \neg d) \& \\
& \quad \& (b^{\vee} \neg c^{\vee} \neg c^{\vee} d) \& \\
& \quad \& (b^{\vee} \neg c^{\vee} c^{\vee} \neg d) \& \\
& \quad \& (\neg d^{\vee} \neg c^{\vee} \neg c^{\vee} d) \& \\
& \quad \& (\neg d^{\vee} \neg c^{\vee} c^{\vee} \neg d) \& \\
& \quad \& (c^{\vee} \neg c^{\vee} \neg c^{\vee} d) \& \\
& \quad \& (c^{\vee} \neg c^{\vee} c^{\vee} \neg d)
\end{aligned}$$

Полученный результат очень громоздкий. Его можно существенно упростить. Во-первых, как указывалось, достаточно привести только по одному вхождению каждой литеры в терм. Например, вместо $b^{\vee} \neg c^{\vee} \neg c^{\vee} d$ достаточно записать $b^{\vee} \neg c^{\vee} d$.

Во-вторых, термы, содержащие одну и ту же литеру с отрицанием и без отрицания как подформулы эквивалентны константе 1. Например, терм $b^{\vee} \neg c^{\vee} c^{\vee} \neg d = 1$. Зная, что имеет место свойство $\forall x \ x \ \& \ 1 = 1$, такие термы можно исключить из конъюнктивной формы. Тогда от полученного результата можно оставить только следующие термы:

$$(a^{\vee} \neg c^{\vee} d) \& (a^{\vee} c^{\vee} \neg d) \& (b^{\vee} \neg c^{\vee} d)$$

Проверим непосредственным вычислением эквивалентность исходной формулы и

полученной конъюнктивной формы:

a	b	c	d	$\neg(a \rightarrow ((b \& \neg d) \oplus c))^{\vee}(c \leftrightarrow d)$	$(a^{\vee} \neg c^{\vee} d) \& (a^{\vee} c^{\vee} \neg d) \& (b^{\vee} \neg c^{\vee} d)$
0	0	0	0	1	1
0	0	0	1	0	0
0	0	1	0	0	0
0	0	1	1	1	1
0	1	0	0	1	1
0	1	0	1	0	0
0	1	1	0	0	0
0	1	1	1	1	1
1	0	0	0	1	1
1	0	0	1	1	1
1	0	1	0	0	0
1	0	1	1	1	1
1	1	0	0	1	1
1	1	0	1	1	1
1	1	1	0	1	1
1	1	1	1	1	1

Что произойдет при попытке упрощения с конъюнктивной формы, если все термы содержат одновременно и некоторую литеру и ее отрицание? В соответствии с описанной ранее процедурой упрощения такие термы можно исключить из формулы, но тогда в формуле не останется ни одного терма и она фактически превратится в пустую строку. Ее можно назвать пустой формулой. Следует ли считать пустую формулу конъюнктивной формой? Может быть и да, если принять некоторое соглашение о ее интерпретации. По идее пустую формулу в качестве конъюнктивной формы следует считать формулой, эквивалентной некоторой общезначимой формуле, так как она явно получается в результате упрощения, например формулы $(a^{\vee} \neg a)$ и которой должна быть эквивалентна. Но ведь совершенно аналогично можно было ввести в рассмотрение другой класс формул (называемых *дизъюнктивными формами*), представляющих собой дизъюнкцию термов, где каждый терм есть конъюнкция литер и их отрицаний. Примером дизъюнктивной формы может служить формула

$$(a \& \neg b)^{\vee} (a \& \neg c \& d)^{\vee} (b \& \neg d)$$

Для таких формул с учетом свойств $\forall x (x \& \neg x) = 0$ и $\forall x (x^{\vee} 0) = x$ при их упрощении аналогично следует исключать термы с литерами и их отрицаниями. При этом, пустую дизъюнктивную форму следует читать эквивалентной 0. Заметим, что относительно некоторой формулы высказывания о том, является ли она конъюнктивной или дизъюнктивной формой не являются взаимоисключающими. Например

Формула	Является конъюнктивной формой	Является дизъюнктивной формой
$(a^{\vee} \neg c^{\vee} d) \& (a^{\vee} c^{\vee} \neg d) \& (b^{\vee} \neg c^{\vee} d)$	Да	Нет
$(a \& \neg b)^{\vee} (a \& \neg c \& d)^{\vee} (b \& \neg d)$	Нет	Да
$((\neg a) \& (a^{\vee} \neg b^{\vee} c))^{\vee} \neg(\neg a \& b) \& (\neg c)$	Нет	Нет
$a \& b \& c$	Да	Да
$a^{\vee} b^{\vee} c$	Да	Да

Последние две формулы попадают одновременно в оба класса, так как формулу $a \& b \& c$ можно рассматривать и как три однолитерных терма конъюнктивной формы и как один трехлитерный терм дизъюнктивной формы, а формулу $a^{\vee} b^{\vee} c$, соответственно,

наоборот как три однолитерных терма дизъюнктивной формы и как один трехлитерный терм конъюнктивной формы.

Поэтому, если расширить одновременно определения и конъюнктивной и дизъюнктивной форм, считая пустую формулу относящейся к обоим классам, мы получим противоречие: пустая формула одновременно в качестве конъюнктивной формы эквивалента 1 и в качестве дизъюнктивной формы эквивалента 0.

Это оставляет нам следующие возможности:

1. Пустая формула является конъюнктивной формой, по определению эквивалентной 1, но не является дизъюнктивной формой.
2. Пустая формула является дизъюнктивной формой, по определению эквивалентной 0, но не является конъюнктивной формой.
3. Пустые формулы не соответствуют структурам высказываний, не имеют логических значений и не являются ни конъюнктивными ни дизъюнктивными формами.

По-видимому, последний вариант более симметричный по отношению к обоим формам, хотя с точки зрения компактности записи варианты 1 и 2 иногда применяются. При этом для ясности лучше делать оговорку, явно указывая как интерпретируется пустая формула.

С учетом этого, будем рассматривать конъюнктивные формы с точностью до состава термов и структуры наличия или отсутствия символов отрицания у литер без учета их порядка записи и возможных повторов следующим образом.

Можно заметить, что по отношению к каждому терму каждая литера может входить или не входить в него четырьмя способами:

- 1) Литера не входит в состав терма.
- 2) Литера входит в состав терма без символа отрицания.
- 3) Литера входит в состав терма с символом отрицания.
- 4) Литера входит в состав терма и с символом отрицания и без символа отрицания.

Поэтому, можно сказать, что состав каждого терма однозначно определяется двумя множествами:

- 1) Множество литер, которые входят в данный терм без символа отрицания. Назовем это множество множеством положительных (не отрицаемых) литер терма.
- 2) Множество литер, которые входят в данный терм с символами отрицания. Назовем это множество множеством отрицаемых литер терма.

Эти множества могут пересекаться и некоторые, но не оба сразу, могут быть пустыми.

Для сжатой записи структуры и состава термов конъюнктивной формы удобнее воспользоваться индексированной формой записи следующим образом.

Пусть T^K – множество термов конъюнктивной формы K над множеством литер L и каждому терму однозначно сопоставлен индекс из множества индексов термов I^K . Здесь верхний индекс используется просто как напоминание, что символы относятся к представлению некоторой конъюнктивной формы K . Обозначим символом T_i^K терм, сопоставленный индексу i из множества индексов термов.

Структуру всей конъюнктивной формы будем записывать в виде

$$K = \bigwedge_{i \in I^K} T_i^K$$

Эта формула отражает, что вся конъюнктивная форма K является конъюнкцией

своих термов. Каждой литере a из множества L^K также сопоставим индекс j из множества индексов литер J^K . То есть $\forall a \in L^K \exists j \in J^K x_j = a$. Множества положительных и отрицаемых литер терма с индексом i обозначим P_i^K и N_i^K соответственно. Тогда структуру каждого терма будем записывать в виде формулы

$$T_i^K = (\bigvee_{j \in P_i^K} x_j)^\vee (\bigvee_{j \in N_i^K} \neg x_j)$$

При этом $\forall i \in I^K \quad P_i^K \cup N_i^K \neq \emptyset$.

Итого

$$K = \bigwedge_{i \in I^K} ((\bigvee_{j \in P_i^K} x_j)^\vee (\bigvee_{j \in N_i^K} \neg x_j))$$

Пример.

Найдем множества положительных и отрицаемых литер полученной ранее конъюнктивной формы. Для этого занумеруем литеры (их 4) и термы (их 14):

$$L^K = \{a, b, c, d\}, J^K = \{1, 2, 3, 4\}$$

$$x_1 = a, x_2 = b, x_3 = c, x_4 = d$$

$$I^K = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$$

i	T_i^K	Множество P_i^K	Множество N_i^K	$P_i^K \cap N_i^K$
1	$T_1^K = (a^\vee \neg c^\vee d)$	$\{1, 4\}$	$\{3\}$	\emptyset
2	$T_2^K = (a^\vee c^\vee \neg d)$	$\{1, 2\}$	$\{4\}$	\emptyset
3	$T_3^K = (b^\vee \neg b^\vee d^\vee \neg c^\vee d)$	$\{2, 4\}$	$\{2, 3\}$	$\{2\}$
4	$T_4^K = (b^\vee \neg b^\vee d^\vee c^\vee \neg d)$	$\{2, 3, 4\}$	$\{2, 4\}$	$\{2, 4\}$
5	$T_5^K = (\neg d^\vee \neg b^\vee d^\vee \neg c^\vee d)$	$\{4\}$	$\{2, 3, 4\}$	$\{4\}$
6	$T_6^K = (\neg d^\vee \neg b^\vee d^\vee c^\vee \neg d)$	$\{3, 4\}$	$\{2, 4\}$	$\{4\}$
7	$T_7^K = (c^\vee \neg b^\vee d^\vee \neg c^\vee d)$	$\{3, 4\}$	$\{2, 3\}$	$\{3\}$
8	$T_8^K = (c^\vee \neg b^\vee d^\vee c^\vee \neg d)$	$\{3, 4\}$	$\{2, 4\}$	$\{4\}$
9	$T_9^K = (b^\vee \neg c^\vee \neg c^\vee d)$	$\{2, 4\}$	$\{3\}$	\emptyset
10	$T_{10}^K = (b^\vee \neg c^\vee c^\vee \neg d)$	$\{2, 3\}$	$\{3, 4\}$	$\{3\}$
11	$T_{11}^K = (\neg d^\vee \neg c^\vee \neg c^\vee d)$	$\{4\}$	$\{3, 4\}$	$\{4\}$
12	$T_{12}^K = (\neg d^\vee \neg c^\vee c^\vee \neg d)$	$\{3\}$	$\{3, 4\}$	$\{3\}$
13	$T_{13}^K = (c^\vee \neg c^\vee \neg c^\vee d)$	$\{3, 4\}$	$\{3\}$	$\{3\}$
14	$T_{14}^K = (c^\vee \neg c^\vee c^\vee \neg d)$	$\{3\}$	$\{3, 4\}$	$\{3\}$

Отсюда сразу можно увидеть необходимые и достаточные условия общезначимости формулы, представленной эквивалентной ей конъюнктивной формой:

Формула является общезначимой тогда и только тогда, когда в составе каждого терма ее эквивалентной конъюнктивной формы имеется пересечение множеств положительных и отрицаемых литер:

$$K=1 \Leftrightarrow \forall i \in I^K P_i^K \cap N_i^K \neq \emptyset$$

Это обосновывается тем, что если в составе некоторого терма T_i $P_i^K \cap N_i^K = \emptyset$, то существует подстановка значений литер, на которой терм T_i как функция своих литер примет значение 0. При этом и вся конъюнктивная форма тоже примет значение 0 как конъюнкция своих термов. А именно, чтобы значение такого терма было 0, достаточно подставить в качестве значений положительных литер значение 0, а в качестве значения отрицаемых литер значение 1.

Например, рассмотренная ранее конъюнктивная форма не является общезначимой, то есть существуют интерпретации, в которых она принимает логически ложные значения, так как среди ее термов есть три, в которых $P_i^K \cap N_i^K \neq \emptyset$:

$$T_1^K = (a^{\vee} \neg c^{\vee} d), T_2^K = (a^{\vee} c^{\vee} \neg d), T_9^K = (b^{\vee} \neg c^{\vee} d).$$

Для $T_1^K = (a^{\vee} \neg c^{\vee} d)$ такой интерпретацией является подстановка $a=0, c=1, d=0$ при любом значении b . Обратите внимание, что мы нашли такую интерпретацию без вычисления исходной формулы. Таблица ее значений была приведена только для самоконтроля нашего построения конъюнктивной формы (лучше сказать: для контроля неединичных термов, так как правильность термов, где $P_i^K \cap N_i^K = \emptyset$ невозможно проверить по таблице значений – в смысле таблицы значений формулы любые такие термы правильны).

Это очень важный результат. Мы нашли способ проверки общезначимости формул с произвольным составом литер и операций и произвольной структуры (указываемой скобками), **не требующий вычисления** ее значений для всех возможных интерпретаций.

Для формул с небольшим числом литер при ручном выполнении операций приведения к конъюнктивной форме промежуточные результаты и объем работы может показаться громоздким по сравнению с непосредственным расчетом. Но число интерпретаций **растет экспоненциально** с ростом числа литер формулы (для формулы с n литерами 2^n интерпретаций). Поэтому для формул с большим числом литер проверка общезначимости без вычисления (например, за счет приведения к конъюнктивной форме, хотя существуют и другие способы) может оказаться предпочтительнее.

Кстати, в данной форме записи пустые формулы можно допустить с однозначной интерпретацией. Действительно, если допустить пустые формулы, интерпретируя их как конъюнктивные формы, то их множества индексов их термов будут пустыми: $I^K = \emptyset$. Тогда представлением всей такой конъюнктивной формы будет формула

$$K = \bigwedge_{i \in I^K} T_i^K = \bigwedge_{i \in \emptyset} f(i) = 1,$$

где f – некоторая функция, ставящая в соответствие индексу i некоторую произвольную формулу, содержание которой несущественно. Такую запись можно считать эквивалентной соглашению в математике, когда знак суммирования по пустому множеству значений индекса трактуется как число 0: $\sum_{i \in \emptyset} a_i = 0$. Аналогично для дизъюнктивных форм можно было бы определить $\bigvee_{i \in \emptyset} f(i) = 0$. В таких обозначениях условие $K=1 \Leftrightarrow \forall i \in I^K P_i^K \cap N_i^K \neq \emptyset$ для формулы с пустым множеством термов также выполняется, так как если $I^K = \emptyset$, его правая часть примет вид $\forall i \in \emptyset P(i)$, где P – некоторый произвольный предикат, значения которого несущественны, так как высказывание $\forall i \in \emptyset P(i)$ имеет истинное логическое значение независимо от P ввиду

ложности условия $i \in \emptyset$. Вспомним, что $\forall i \in \emptyset P(i)$ является сокращенной записью для $\forall i (i \in \emptyset) \rightarrow P(i)$, и что по определению $\emptyset = \{x \mid 0\}$ даст $\forall i 0 \rightarrow P(i)$, а по определению операции \rightarrow формула $0 \rightarrow x$ общезначима: $0 \rightarrow 0 = 1$ и $0 \rightarrow 1 = 1$.

В качестве примера докажем следующую формулу над тремя литерами (известную в логике как правило резолюции), не вычисляя ее на всех интерпретациях (их 8):

$$((a \vee b) \& (\neg a \vee c)) \Rightarrow (b \vee c)$$

Нам нужно показать общезначимость формулы $((a \vee b) \& (\neg a \vee c)) \rightarrow (b \vee c)$. Для этого приведем ее к конъюнктивной форме.

$$\begin{aligned} & ((a \vee b) \& (\neg a \vee c)) \rightarrow (b \vee c) = \\ & = \neg((a \vee b) \& (\neg a \vee c)) \vee (b \vee c) = \\ & = (\neg(a \vee b) \vee \neg(\neg a \vee c)) \vee (b \vee c) = \\ & = (\neg a \& \neg b) \vee (\neg \neg a \& \neg c) \vee (b \vee c) = \\ & = (\neg a \& \neg b) \vee (a \& \neg c) \vee (b \vee c) = \\ & = (\neg a \vee (a \& \neg c)) \vee (b \vee c) \& (\neg b \vee (a \& \neg c)) \vee (b \vee c) = \\ & = (((\neg a \vee a) \& (\neg a \vee \neg c)) \vee (b \vee c)) \& ((\neg b \vee a) \& (\neg b \vee \neg c)) \vee (b \vee c) = \\ & = (\neg a \vee a \vee b \vee c) \& (\neg a \vee \neg c \vee b \vee c) \& (\neg b \vee a \vee b \vee c) \& (\neg b \vee \neg c \vee b \vee c) \end{aligned}$$

Множества пересечений положительных и отрицательных литер для термов $(\neg a \vee a \vee b \vee c)$, $(\neg a \vee \neg c \vee b \vee c)$, $(\neg b \vee a \vee b \vee c)$ и $(\neg b \vee \neg c \vee b \vee c)$ будут соответственно $\{a\}$, $\{c\}$, $\{b\}$ и $\{b, c\}$. Термов с пустым пересечением нет. Следовательно, формула общезначима.

Замечание:

В ходе рассмотрения данного метода (сведение формулы к конъюнктивной формы) было введено определенное исчисление логических формул – преобразование по определенным правилам текста, представляющего формулы. В качестве правил использовались формулы Де-Моргана, закон двойного отрицания и распределительный закон. Все эти правила были интерпретированы также как определенные трансформации диаграмм, представляющих структуры формул. То есть в параллель с исчислением формул можно также рассматривать исчисление диаграмм (размеченных символами операций и операндов). В дискретной математике размеченные диаграммы рассматриваются как одна из моделей теории графов.

Тема 2. Бинарные предикаты. Бинарные отношения. Прямые произведения множеств. Бинарные отношения и функции. Типы функциональных отношений. Взаимнооднозначные соответствия. Эквивалентность (равномощность) множеств.

Кроме высказываний о свойствах отдельных объектов при анализе суждений можно встретиться с ситуацией, когда суждение можно рассматривать, как относящееся к нескольким объектам сразу. Например, в предложении из области математики «число двенадцать делится на число три» можно усмотреть некоторое высказывание (есть возможность задать логическое значение) сразу для двух объектов: числа двенадцать и числа три. То же касается всяческих сравнений, например, из области физики «жидкая вода плотнее льда», из области математики «пять больше трех» и т.д. Для описания таких высказываний можно поступить двумя способами.

Способ 1. Рассматривать такие предложения как высказывания о *бинарных предикатах*. То есть как функции с двумя аргументами произвольного типа (из предметной области) с логическим значением.

Способ 2. Ввести новую предметную область, представив её как бы состоящей из *всех возможных сочетаний* интересующих объектов исходной предметной области в *упорядоченные пары*. Эти упорядоченные пары в дальнейшем рассматривать как составные, *структурированные объекты*, которые могут далее рассматриваться как возможные значения аргументов предиката на новой предметной области.

С точки зрения записи высказывания при помощи именованного предиката разница между этими способами несущественна. И в том и в другом способе она будет состоять из названия предиката и двух его аргументов: либо отдельных, либо как частей пары. Но для второго способа появляется возможность говорить о выделяемом таким предикатом множестве. Это будет множество всех возможных сочетаний объектов в упорядоченную пару, так, чтобы значение предиката на такой паре было истинным. Такое множество называют *бинарным отношением*.

Связь между этими способами можно схематично представить следующей формулой:

$$\alpha = \{ (x, y) \mid P(x, y) \}$$

Здесь P – бинарный предикат, α – бинарное отношение (множество из упорядоченных пар), (x, y) – подстановочный символ для представления упорядоченной пары, рассматриваемой как *структурированный объект*.

Если U – некоторое универсальное множество, множество всех возможных пар на нем обозначим $U \times U$ как результат некоторой новой бинарной операции между множествами.

Вообще, если A и B некоторые множества, то обозначим через $A \times B$ следующее множество, называемое *прямым произведением множеств* (его также называют *декартовым произведением*):

$$A \times B = \{ (x, y) \mid x \in A \ \& \ y \in B \}$$

То есть это есть множество всех возможных упорядоченных пар, первый компонент которых принадлежит первому множеству, а второй компонент – второму. Такое определение существенно отличается от определений теоретико-множественных операций за счет того, что здесь вводится представление об упорядоченной паре как о *цельном объекте*.

Если бинарное отношение задано на некоторой предметной области U будем записывать это в виде формулы:

$$\alpha \subseteq U \times U$$

так как формула $P(x, y) \rightarrow 1$ общезначима.

Часто встречается ситуация, когда бинарное отношение устанавливается между разными множествами. Обыденным примером может являться отношение «быть женатым». В этом случае первый компонент в упорядоченной паре обычно относят к «множеству лиц мужского пола», а второй компонент к «множеству лиц женского пола». В подобных случаях будем называть такие отношения *между* множествами. Например, скажем, что α есть отношение между множествами A и B . В виде формулы это записывается как

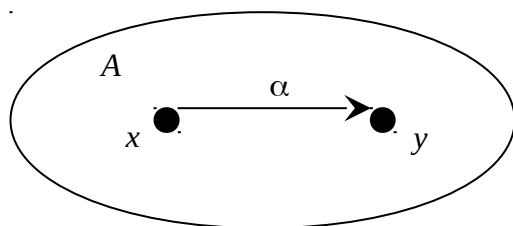
$$\alpha \subseteq A \times B$$

Или, если A и B совпадают, будем записывать

$$\alpha \subseteq A \times A$$

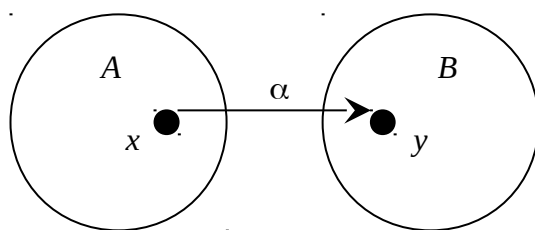
и называть α отношением *на* множестве A . То есть, выделена часть предметной области и уже на ней рассматривается отношение. Например, на множестве целых чисел рассматривается отношение делимости $\alpha = \{ (x, y) \mid \text{целое число } x \text{ делит целое число } y \}$

Отношение на множестве иногда удобно изобразить в виде *ориентированного графа*. Его можно представить в виде картинке на плоскости, где *вершины* представляют элементы множества, а направленные стрелки (*рёбра*) проведены между теми узлами, для которых пара, упорядоченная по направлению стрелки, является элементом отношения (бинарный предикат, задающий отношение, является истинным на такой паре аргументов). Пример возможного изображения такого графа показан на рисунке:



Здесь $\alpha \subseteq A \times A$, $(x, y) \in \alpha$ и $\neg (y, x) \in \alpha$. Поэтому стрелка от x к y проведена, а от y к x – нет. Над стрелкой, изображающей ребро графа, будем подписывать название отношения (α) на тот случай, если возникнет необходимость на одном наборе вершин представить несколько отношений.

Аналогично отношения между двумя множествами будем изображать в виде ориентированных графов, у которых вершины разделены на два множества, так, что стрелки, изображающие ребра, могут начинаться только в первом множестве, а заканчиваться только во втором. Пример для $\alpha \subseteq A \times B$:



Обратите внимание, что некоторые из введенных символов сами могут рассматриваться как бинарные отношения:

\in – отношение принадлежности между элементами и множествами некоторой предметной области. Множество всех подмножеств или булеан некоторого подмножества обозначается как $\wp(A) = \{X \mid X \subseteq A\}$. Принадлежность можно рассматривать как бинарное отношение между U и $\wp(U)$.

\subseteq и $=$ – отношения включения и равенства множеств как отношения на $\wp(U)$.

\Rightarrow и \Leftrightarrow – отношения логического следования и логической равносильности на множестве всех возможных высказываний математической логики вообще либо некоторого множества формул, например, на множестве формул логики высказываний.

Любая из бинарных логических операций может рассматриваться как бинарное отношение на логической области. В частности, обозначаемое также символом $=$ равенство логических значений (определяется операцией \leftrightarrow).

Во всех этих случаях используется инфиксная форма записи для высказывания об упорядоченной паре: они все имеют вид $x * y$, где $*$ – некоторый инфиксный символ для обозначения отношения. То есть высказывание $x * y = ((x, y) \in \alpha)$. Аналогично в этом случае $\alpha = \{(x, y) \mid x * y\}$. Иногда также просто пишут $x \alpha y$, то есть само название отношения используют как инфиксный символ.

Также заметьте, что символ $=$ использовался тремя различными способами:

- 1) Для задания определений, например $A \cap B = \{x \mid x \in A \ \& \ x \in B\}$.
- 2) Для обозначения отношения равенства логических значений высказываний, например, $u \checkmark v = \neg(\neg u \ \& \ \neg v)$.
- 3) Для обозначения отношения равенства множеств, например, $(A = B) \Leftrightarrow (x \in A \Leftrightarrow x \in B)$.

Первую формулу лучше вообще как высказывание не рассматривать. Это скорее предписание для читающих данный текст, как интерпретировать ту или иную формулу. То есть, встретив в тексте, например, фрагмент $A \cap B$ можно заменить его на $\{x \mid x \in A \ \& \ x \in B\}$. Поэтому иногда для записи определений используют отличимый от знака $=$ символ, например, $\stackrel{\text{def}}{=}$ или $\stackrel{\Delta}{=}$ (читается «равно по определению»). Пишут

$$A \cap B \stackrel{\text{def}}{=} \{x \mid x \in A \ \& \ x \in B\}$$

Остальные два случая различимы по типу выражений, стоящих слева и справа от знака $=$. Для высказываний также используется символ \leftrightarrow .

При рассмотрении конкретных предметных областей обычно также вводится некоторое отношение равенства элементов предметной области и для его обозначения также используется символ $=$. В каждом конкретном случае мы будем иметь дело с разными областями, и отношение равенства может пониматься по-разному. Например, в математике при рассмотрении выражений обычно используют символ $=$ для указания, что две формулы могут быть вычислены до одинаковых значений, например, пишут $a+b = b+a$. В другом случае при рассмотрении множеств многочленов от некоторой переменной интересуются составом коэффициентов при одинаковых степенях, например, под записью $\sum a_i X^i = \sum b_i X^i$ подразумевают, что $\forall i \ a_i = b_i$.

Чтобы абстрагироваться от этого многообразия, будем считать, что равенство элементов множеств есть просто некоторое бинарное отношение на предметной области. На него, однако, наложим определённые ограничения. Допустим, инфиксному символу $=$ для обозначения этого отношения соответствует множество $\alpha = \{ (x, y) \mid x = y \}$. При этом, предикат E , определяющий это отношение как множество пар $\alpha = \{ (x, y) \mid E(x, y) \}$ удовлетворяет следующим условиям:

- 1) $\forall x E(x, x)$
- 2) $\forall x \forall y (E(x, y) \rightarrow E(y, x))$
- 3) $\forall x \forall y \forall z ((E(x, y) \& E(y, z)) \rightarrow E(x, z))$

Свойство (1) называют рефлексивностью, то есть α – рефлексивное отношение. Свойство (2) называют симметричностью, то есть α – симметричное отношение. Свойство (3) называют транзитивностью, то есть α – транзитивное отношение.

В терминах множеств упорядоченных пар эти свойства могут быть записаны так:

- 1) $\forall x ((x, x) \in \alpha)$
- 2) $\forall x \forall y ((x, y) \in \alpha \rightarrow (y, x) \in \alpha)$
- 3) $\forall x \forall y \forall z ((x, y) \in \alpha \& (y, z) \in \alpha) \rightarrow (x, z) \in \alpha$

В инфиксной форме они приобретают вид

- 1) $\forall x (x = x)$
- 2) $\forall x \forall y ((x = y) \rightarrow (y = x))$
- 3) $\forall x \forall y \forall z ((x = y) \& (y = z) \rightarrow (x = z))$

Свойство транзитивности позволяет выписывать равенства в цепочки:
 $a = b = c$ есть сокращённая форма записи для $((a = b) \& (b = c)) \Rightarrow (a = c)$.

Любое бинарное отношение, удовлетворяющее свойствам (1), (2) и (3) называют отношением эквивалентности.

В частности, рассмотренные ранее отношения, для которых употреблялся символ $=$, являются отношениями эквивалентности на соответствующих множествах.

Теперь, после того, как было оговорено, что будет пониматься под равенством элементов множеств, можно ввести ещё некоторые общеупотребительные обозначения.

Во-первых, в приведенных примерах мы имели дело с конечными множествами, заданными списками элементов (неупорядоченными). Например, вместо словесной формулировки «множество A состоит из элементов a, b, c » будем писать формулу

$$A = \{ a, b, c \}$$

Её можно представить как задание множества предикатом

$$A = \{ x \mid x=a \vee x=b \vee x=c \}$$

В частности, для логической области как множества будет использоваться символ $\mathcal{B} = \{ 0, 1 \}$. При этом на \mathcal{B} равенство это связка \leftrightarrow .

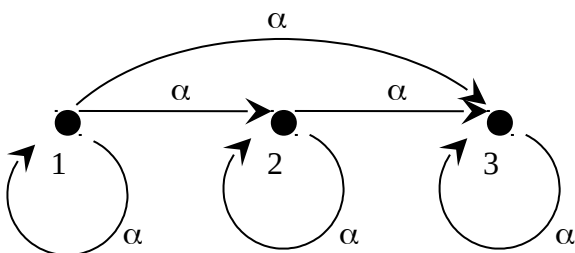
Во-вторых, аналогично конечным множествам, конечные бинарные отношения тоже можно задать списком пар. Например, рассмотрим множество чисел $A = \{1, 2, 3\}$ с отношением \leq (меньше или равно). Оно установлено для следующих упорядоченных пар:

$$1 \leq 1, 1 \leq 2, 1 \leq 3, 2 \leq 2, 2 \leq 3, 3 \leq 3.$$

Тогда будем записывать для $\alpha \subseteq A \times A$

$$\alpha = \{ (x, y) \mid x \leq y \} = \{ (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3) \}$$

Графически оно может быть представлено следующим образом:



Так как в отношении присутствуют пары одинаково обозначенных элементов, на графе присутствуют петли. Для интерпретации списка пар, естественно, требуется задать и отношение равенства между парами. Будем считать, что если $=$ означает некоторое отношение эквивалентности на U , то для множества всех упорядоченных пар символ $=$ означает их покомпонентное равенство:

$$((x, y) = (p, q)) \Leftrightarrow ((x=p) \& (y=q))$$

Это уже отношение на $U \times U$. Оно тоже является эквивалентностью.

В третьих, имея отношение равенства на предметной области, рассмотрим еще одну часто употребительную форму построения высказываний: утверждение о единственности элемента с некоторым свойством. Примером может служить сформулированное во введении свойство для функций: «каждому значению аргумента сопоставляется единственное значение». Формула, отражающая, что некоторое свойство P выполняется только для одного объекта в предметной области, записывается так:

$$\exists! x P(x)$$

Читается «Существует единственный x такой, что $P(x)$ ». Это сложное высказывание, его проще понять как состоящее из двух:

- 1) Утверждение, что объект с данным свойством существует.
- 2) Утверждение о единственности такого объекта.

Поэтому запишем его в таком виде:

$$\exists! x P(x) = (\exists x P(x)) \& (\forall x \forall y (P(x) \& P(y)) \rightarrow (x=y))$$

Также будем использовать сокращения

$$\forall x \in A \Phi(x) \text{ для формулы } \forall x ((x \in A) \rightarrow \Phi(x))$$

$$\exists x \in A \Phi(x) \text{ для формулы } \exists x ((x \in A) \& \Phi(x))$$

$$\exists! x \in A \Phi(x) \text{ для формулы } \exists! x ((x \in A) \& \Phi(x))$$

где $\Phi(x)$ – некоторая формула, содержащая символ x .

ФУНКЦИОНАЛЬНЫЕ ОТНОШЕНИЯ.

С использованием введённых обозначений и представлений, введём определение для функции, действующей из одного множества в другое.

Множество $B^A = \{ f \mid f \subseteq A \times B \ \& \ (\forall x \in A \ \exists! y \in B \ (x, y) \in f) \}$ называется множеством всех функций (или функциональных отношений), действующих из множества A в множество B .

Здесь для элементов этого множества (для функций) отмечены следующие свойства

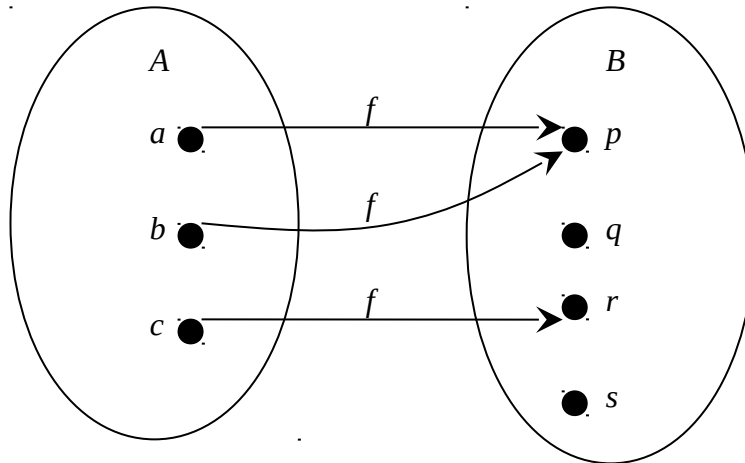
- 1) $f \subseteq A \times B$ означает, что функция рассматривается как бинарное отношение между множествами (она связывает аргументы в A с результатами в B в упорядоченные пары).
- 2) $\forall x \in A \ \exists! y \in B \ (x, y) \in f$ говорит о том, что каждому элементу в A (аргументу) сопоставляется единственный элемент в B (результат). Само понятие о единственности результата подразумевает, что на множестве B установлено некоторое отношение равенства. При этом более привычная форма записи сопоставления аргументу результата $y = f(x)$ будем считать синонимом для записи $(x, y) \in f$. Просто выражение $f(x)$ будет являться обозначением результата функции на аргументе x .

В дальнейшем для указания, что некоторый символ f обозначает функцию из множества A во множество B , будем использовать запись $f \in B^A$. Обозначение B^A связано с подсчётом количества способов установить функциональное отношение из множества A в множество B . Если в A – n элементов, а в B – m элементов, то установить функциональное отношение из A в B можно m^n способами. В этом случае наглядное представление о функции дает следующая таблица:

x	$f(x)$
n строк $\left\{ \begin{array}{l} a_1 \\ a_2 \\ \vdots \\ a_n \end{array} \right.$	$\left\{ \begin{array}{l} f(a_1) \\ f(a_2) \\ \vdots \\ f(a_n) \end{array} \right.$

Имеется n строк, представляющих все значения аргументов, для которых надо задать значения результатов. Для каждой строки имеется m вариантов выбора значения функции для данного значения аргумента. То есть n раз делается выбор из m возможностей. Это можно сделать m^n способами.

Также функции будем изображать ориентированными графами. Например, так:



Здесь $A = \{ a, b, c \}$, $B = \{ p, q, r, s \}$, $f = \{ (a, p), (b, p), (c, r) \}$, $f \in B^A$.

Функции двух аргументов можно представить как функции, действующие из прямого произведения соответствующих множеств. Например, рассмотренное ранее множество бинарных логических операций (состоящее из 16 функций) можно в данных обозначениях представить как $B^{B \times B}$.

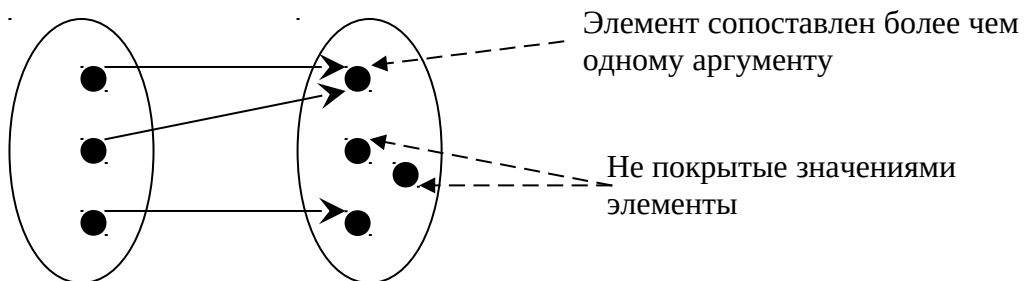
Рассмотрим следующие классификационные признаки, вводимые для функций:

- 1) Функция $f \in B^A$ называется *сюрьективной*, если $\forall y \in B \exists x \in A y = f(x)$. В этом случае множество B полностью покрыто значениями функции.
- 2) Функция $f \in B^A$ называется *инъективной*, если разным аргументам она ставит в соответствие разные результаты. По иному это можно сформулировать так: из равенства результатов логически следует равенство аргументов: $(f(x)=f(y)) \Rightarrow (x=y)$.

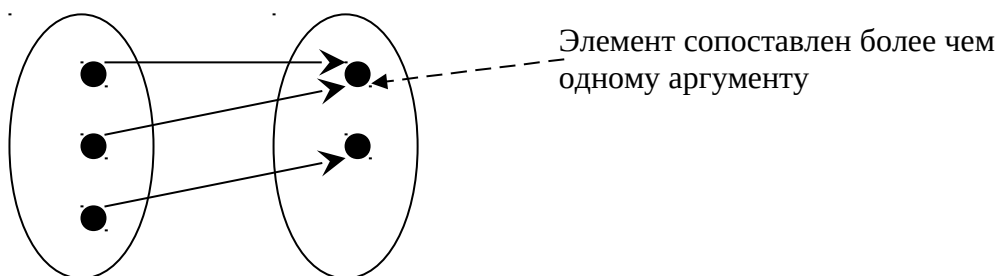
В определении инъективной функции, таким образом, полагается заданным равенство на обоих множествах, A и B .

Проиллюстрируем эти свойства диаграммами с ориентированными графами. Введено два признака, поэтому с учетом их сочетаний, возможно четыре случая:

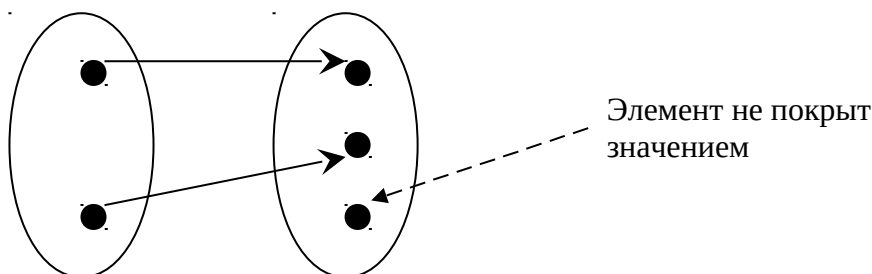
Не инъективная и не сюрьективная:



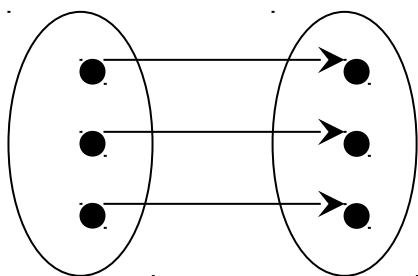
Сюрьективная, но не инъективная:



Инъективная, но не сюръективная:



Сюръективная и инъективная:



Функция, являющаяся одновременно инъективной и сюръективной, называется биективной.

Биективная функция $f \in B^A$ устанавливает *взаимнооднозначное соответствие* между множествами A и B : $(\forall x \in A \exists! y \in B (x, y) \in f) \& (\forall y \in B \exists! x \in A (x, y) \in f)$.

Для функций из B^A с введённой классификацией и конечных множеств A и B следует отметить следующие свойства (иллюстрируются теми же графами):

Сюръективная функция существует тогда и только тогда, когда в A элементов больше или равно, чем в B .

Инъективная функция существует тогда и только тогда, когда в B элементов больше или равно, чем в A .

Биективная функция существует тогда и только тогда, когда число элементов во множествах A и B совпадает.

В рассмотренных представлениях отношения и функции представлены множествами из упорядоченных пар. Как ко всяким множествам, к ним применимы теоретико-множественные операции, например, пересечения, объединения, разности, дополнения.

Допустим, $\alpha \subseteq U \times U$. Тогда его дополнение, $\overline{\alpha} = \{ (x, y) \mid \neg((x, y) \in \alpha) \}$ может означать некоторое противоположное отношение, как, например, «не равно» является

противоположным для отношения «равно». Обычно инфиксный символ для представления такого противоположного отношения берут такой же, как и для исходного отношения, но перечеркивают. Пишут, например, $a \neq b$, $x \notin A$, $A \not\subseteq B$.

Если $\alpha \subseteq A \times B$, то обычно под дополнением $\bar{\alpha}$ имеют в виду дополнение до полного отношения. Полным отношением называют само множество всех возможных пар $A \times B$. Тогда, если не оговорено иное, будем считать, что

$$\bar{\alpha} = (A \times B) \setminus \alpha.$$

Полезным свойством такого дополнения является то, что и $\alpha \subseteq A \times B$ и $\bar{\alpha} \subseteq A \times B$. Получается некоторая замкнутая на $A \times B$ система теоретико-множественных операций.

Кроме теоретико-множественных операций для бинарных отношений и функций введём ещё две операции: обращение и композицию.

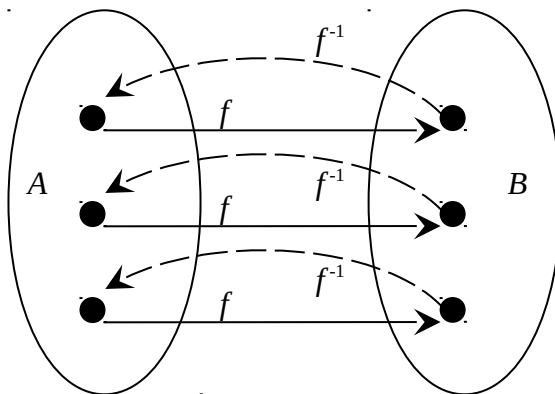
Обращение бинарного отношения определяется как

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

Операция обращения отношения заключается в смене направлений установленных связей. В рассматривавшемся ранее примере $\alpha = \{ (x, y) \mid x \leq y \}$ обратное отношение по смыслу будет $\alpha^{-1} = \{ (x, y) \mid x \geq y \}$. Обращение следует отличать от дополнения, которое в этом примере означало бы $\bar{\alpha} = \{ (x, y) \mid x > y \}$. Если $\alpha \subseteq A \times B$ то $\alpha^{-1} \subseteq B \times A$.

Для функций обратное отношение в общем случае не будет функцией. Если функция не инъективная, то обратное к ней отношение ставит в соответствие одному значению сразу несколько. Если функция не сюръективная, то обратное к ней отношение некоторым значениям вообще не сопоставляет значений. Приведенные примеры графов функций позволяют это понять. Обратное отношение будет функцией тогда и только тогда, когда она биективная.

В примере это выглядит так (сплошные линии показывают исходную биективную функцию, штриховые – обратное отношение) $f \in B^A$ & $f^{-1} \in A^B$:



Видно, что формула эквивалентна условию взаимнооднозначного соответствия:

$$(f \in B^A \text{ \& } f^{-1} \in A^B) \Leftrightarrow (\forall x \in A \exists! y \in B (x, y) \in f) \text{ \& } (\forall y \in B \exists! x \in A (x, y) \in f)$$

Множества A и B называют эквивалентными или равномошными, если между ними можно установить взаимнооднозначное соответствие. Это, как будет показано

далее, является отношением эквивалентности между множествами. Используется следующее обозначение:

$$A \sim B \Leftrightarrow (\exists f \in B^A \ (f^{-1} \in A^B))$$

В конечном случае это отношение проще всего представить как свойство «иметь одинаковое число элементов».

В дальнейшем будет удобно также использовать обозначение $A \overset{f}{\sim} B$ для описания ситуации, когда множества A и B эквивалентны и функция f устанавливает их взаимнооднозначное соответствие.

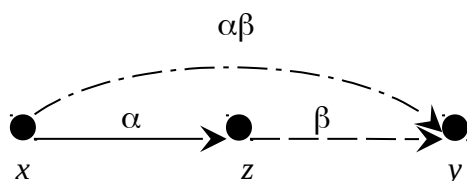
Тема 3. СПЕЦИАЛЬНЫЕ ВИДЫ ОПЕРАЦИЙ НАД БИНАРНЫМИ ОТНОШЕНИЯМИ. ОБРАЩЕНИЕ И КОМПОЗИЦИИ. СТЕПЕНЬ БИНАРНОГО ОТНОШЕНИЯ. ОТНОШЕНИЕ ДОСТИЖИМОСТИ. ОСОБЕННОСТИ ПОСЛЕДОВАТЕЛЬНОСТИ СТЕПЕНЕЙ БИНАРНОГО ОТНОШЕНИЯ НА КОНЕЧНОМ МНОЖЕСТВЕ.

Обращение бинарных отношений как специальная операция над отношениями уже была упомянута при рассмотрении биективных функций. В этом разделе будет введена еще одна операция, называемая композицией.

Композиция бинарных отношений определяется как

$$\alpha \circ \beta = \{ (x, y) \mid \exists z (x, z) \in \alpha \ \& \ (z, y) \in \beta \}$$

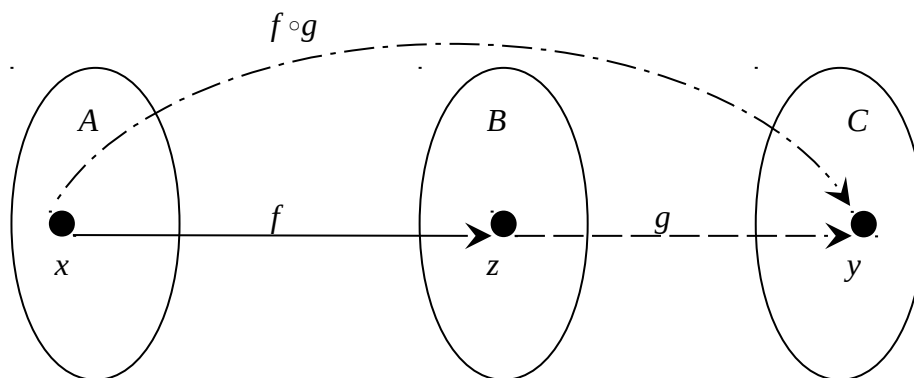
Эта бинарная операция между отношениями: она по двум отношениям α и β строит третье $\alpha \circ \beta$. Смысл этой операции лучше всего пояснить графически.



Композицию можно представить в виде множества всех возможностей проложить пути так, чтобы первый шаг делать по стрелкам, размеченным символом α , а второй шаг – по стрелкам, размеченным символом β . Для того, чтобы из x можно было так перейти в y , должна быть хотя бы одна промежуточная вершина (в примере обозначена как z), связанная по α с x (от x к z) и по β с y (от z к y).

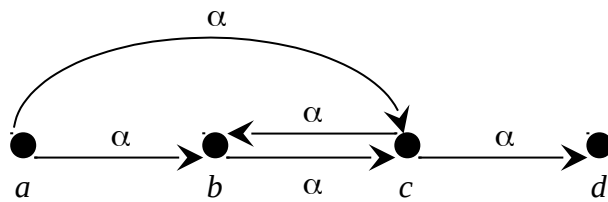
Если $\alpha \subseteq A \times B$ и $\beta \subseteq B \times C$ то $\alpha \circ \beta \subseteq A \times C$

Для функций композиция означает последовательное их применение к аргументу: Если $f \in B^A$ и $g \in C^B$ то $f \circ g \in C^A$.

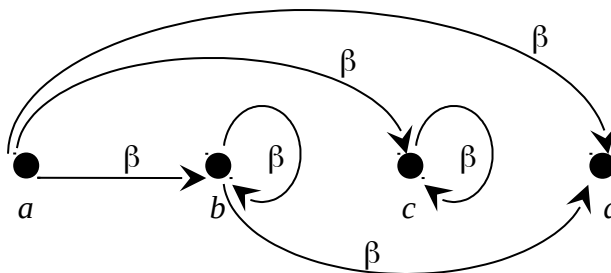


В примере $z = f(x)$, $y = g(z)$, то можно представить, что $y = g(f(x))$.

Особо рассмотрим случай, когда имеется только одно отношение α на некотором множестве A : $\alpha \subseteq A \times A$. Изображением такого отношения является диаграмма ориентированного графа. Пример такого графа (для $A = \{a, b, c, d\}$) приведен на следующем рисунке:



Какой смысл в этом случае будет у отношения $\beta = \alpha \circ \alpha$? Это отношение будет связывать те вершины графа, между которыми существует путь, состоящий ровно из двух шагов по направленным стрелкам. Если их отследить для приведенного примера отношения и построить граф отношения β , получится следующая конфигурация связей:



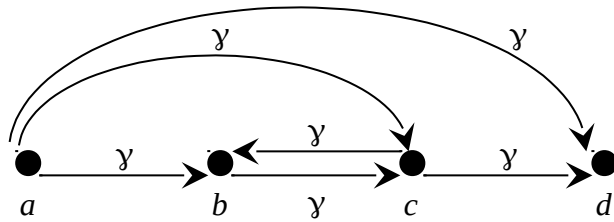
Например, в исходном отношении были связи (b, c) и (c, d) . Поэтому существует путь длиной ровно за два шага из вершины b в вершину d – упорядоченная пара $(b, d) \in \beta$. По этой же причине в графе для отношения β появляются петли в вершинах b и c , например,

$$(b, c) \in \alpha \ \& \ (c, b) \in \alpha \Rightarrow (b, b) \in \beta.$$

А вот пути ровно за два шага из c в d нет. Поэтому хотя $(c, d) \in \alpha$, но $(c, d) \notin \beta$.

Переходы за три шага можно вычислить следующими способами

- 1) Отследить их по изначально заданному графу для α , например, есть путь из a в b , затем через c в d . Это сложный способ, так как с увеличением длины путей необходимо учитывать все возможности для промежуточных узлов
- 2) Воспользоваться предварительно вычисленными связями, отражающими переходы в два шага (β) и рассмотреть все возможности продлить их еще на один шаг: например, если $(a, c) \in \beta$ & $(c, d) \in \alpha$, то есть путь ровно за три шага из a в d . Фактически, так вычисляется еще одно отношение (назовём его γ), отражающее все такие пути. Оно является композицией β и α : $\gamma = \beta \circ \alpha$. Так можно вычислять пути и больших длин: если есть результат по путям некоторой длины, всегда можно рассмотреть варианты его удлинения еще на один шаг.
- 3) Можно поступить и наоборот, имея предварительно вычисленные результаты для путей меньшей длины, можно их рассматривать как продолжение путей длиной в один шаг, в данном примере этому соответствует отношение $\alpha \circ \beta$. Оказывается, результат будет совпадать с результатами первых двух способов. Результат вычисления $\gamma = \beta \circ \alpha = \alpha \circ \beta$ соответствует следующему графу:



Дело в том, что $\alpha \circ \beta$, с учётом того, что $\beta = \alpha \circ \alpha$, может быть представлено в виде $\alpha \circ (\alpha \circ \alpha)$. А $\beta \circ \alpha$ может быть представлено как $(\alpha \circ \alpha) \circ \alpha$. Равенство же

$$\alpha \circ (\alpha \circ \alpha) = (\alpha \circ \alpha) \circ \alpha$$

обусловлено тем, что **композиция – ассоциативная операция**. Для неё выполняется **сочетательный закон**. То есть для произвольных трёх отношений имеет место следующее свойство:

$$p \circ (q \circ r) = (p \circ q) \circ r$$

Докажем это свойство, используя определения для бинарной операции \circ . Целевое утверждение представляет равенство множеств, и элементами этих множеств являются упорядоченные пары. Поэтому, в соответствии с определением равенства множеств $(A = B) \Leftrightarrow (x \in A \Leftrightarrow x \in B)$, в данном случае необходимо доказать что

$$(x, y) \in p \circ (q \circ r) \Leftrightarrow (x, y) \in (p \circ q) \circ r$$

Имеем по определению \circ :

$$(x, y) \in p \circ (q \circ r) \Leftrightarrow \exists z ((x, z) \in p \ \& \ (z, y) \in (q \circ r))$$

Еще раз применяем определение \circ для раскрытия условия $(z, y) \in (q \circ r)$:

$$\exists z ((x, z) \in p \ \& \ (z, y) \in (q \circ r)) \Leftrightarrow \exists z ((x, z) \in p \ \& \ \exists t ((z, t) \in q \ \& \ (t, y) \in r))$$

Обратите внимание, что во внутренней формуле с квантором связан символ t , но и символ z , связанный с внешним квантором, тоже присутствует: $\exists t ((z, t) \in q \ \& \ (t, y) \in r)$. Именно поэтому при повторном применении подстановки определения \circ использован другой подстановочный символ. Правая часть целевой формулы $(x, y) \in (p \circ q) \circ r$ раскрывается аналогично: два раза применяется подстановка по определению \circ . Используем для этого еще два подстановочных символа, связанных с кванторами \exists . Из-за иного порядка скобок эта формула несколько отличается от формулы для левой части:

$$(x, y) \in (p \circ q) \circ r \Leftrightarrow \exists u ((x, z) \in (p \circ q) \ \& \ (z, y) \in r)$$

$$\exists u ((x, u) \in (p \circ q) \ \& \ (u, y) \in r) \Leftrightarrow \exists u (\exists v ((x, v) \in p \ \& \ (v, u) \in q) \ \& \ (u, y) \in r)$$

Имеем две формулы, равносильность которых необходимо проверить:

$$\exists z ((x, z) \in p \ \& \ \exists t ((z, t) \in q \ \& \ (t, y) \in r))$$

$$\exists u (\exists v ((x, v) \in p \ \& \ (v, u) \in q) \ \& \ (u, y) \in r)$$

Для этого заметим, что формула вида $a \ \& \ (\exists x P(x))$ равносильна формуле $\exists x (a \ \& \ P(x))$, где a – некоторое высказывание. Чтобы понять это, вспомним определение квантора \exists как дизъюнкцию по предметной области $\exists x \Phi(x) = \bigvee_{x \in U} \Phi(x)$ и свойство дистрибутивности (распределительный закон) для логических операций $\&$ и \vee :

$$a \ \& \ (b \vee c) = (a \ \& \ b) \vee (a \ \& \ c)$$

Получаем $a \& (\exists x \Phi(x)) = a \& (\bigvee_{x \in U} \Phi(x)) = \bigvee_{x \in U} (a \& \Phi(x)) = \exists x (a \& \Phi(x))$.

Это свойство позволяет преобразовывать формулы с квантором \exists , вынося его из-под логической связки $\&$. Такие формы, когда все кванторы вынесены из-под логических связок, называют *предварёнными*. В нашем случае предварённые формы для рассматриваемых формул будут (очерёдность подряд записанных кванторов \exists безразлична, $\exists v \exists u \dots = \exists v \exists u \dots$ по коммутативности ЛОГИЧЕСКОГО ИЛИ):

$$\begin{aligned} \exists z \exists t ((x, z) \in p \& (z, t) \in q \& (t, y) \in r) \\ \exists v \exists u ((x, v) \in p \& (v, u) \in q \& (u, y) \in r) \end{aligned}$$

Видно, что эти формулы отличаются только обозначениями подстановочных символов (v вместо z и u вместо t) и потому эквивалентны. Что и доказывает свойство ассоциативности композиции.

Замечание.

В отличие от формул, представляющих высказывания, построенные из атомарных (рассматриваемых как неделимые части) подформул и потому моделируемых формулами исчисления высказываний, кванторные формулы из этого примера не могут быть разложены на атомарные части, соединенные только связками-логическими операциями. Приведенные формулы при проведении преобразований требуют учета обозначений подстановочных символов – аргументов предикатов. Правила таких преобразований, ведущие к эквивалентным формулам устанавливаются на основе раздела дискретной математике – исчисления предикатов. В общем случае не существует стратегии применения таких правил, позволяющей за конечное число шагов установить такие свойства формул логики предикатов, как общезначимость, выполнимость, эквивалентность, отношение следования.

СТЕПЕНЬ БИНАРНОГО ОТНОШЕНИЯ ПО КОМПОЗИЦИИ.

Рассматривая отношения достижимости вершин за некоторое количество шагов и способы их вычислений, приходим к потребности ввести понятие о степени отношения, подобно тому, как в арифметике определяют степень исходя из многократного выполнения умножения чисел. В арифметике k степенью числа называют результат k раз выполненного умножения числа на себя ($a^k = \underbrace{a \cdot a \cdot \dots \cdot a}_{k \text{ раз}}$). Аналогично для бинарных отношений k степенью бинарного отношения α назовём k раз выполненное вычисление композиции с самим этим отношением: $\alpha^k = \underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{k \text{ раз}}$. При этом, ввиду ассоциативности операции \circ , все равно, как расставлять скобки в выражении

$$(((\alpha \circ \alpha) \circ \alpha) \circ \dots) \circ \alpha = \alpha \circ (\dots (\alpha \circ (\alpha \circ \alpha)))$$

Для ассоциативных операций скобки вообще можно опускать из формул и просто записывать $\alpha \circ \alpha \circ \dots \circ \alpha$.

Определение вида $\alpha^k = \underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{k \text{ раз}}$ не является хорошо формализованным, хотя и является достаточно наглядным, для его записи приходится применять специальные пояснения. Им не очень удобно пользоваться в доказательствах. Удобнее дать определение, имитирующее сам алгоритм вычисления α^k в виде рекуррентного соотношения и начальных условий:

$$\alpha^1 = \alpha$$

$$\alpha^{k+1} = \alpha^k \circ \alpha$$

С учётом ассоциативности \circ можно второе соотношение записать и так: $\alpha^{k+1} = \alpha \circ \alpha^k$.

Степень отношения, таким образом, может рассматриваться как функция, ставящая в соответствие показателю – *натуральному числу* некоторое бинарное отношение. Результат применения этого алгоритма для первых четырёх степеней будет следующим:

$$\alpha^1 = \alpha$$

$$\alpha^2 = \alpha^1 \circ \alpha = \alpha \circ \alpha$$

$$\alpha^3 = \alpha^2 \circ \alpha = (\alpha \circ \alpha) \circ \alpha$$

$$\alpha^4 = \alpha^3 \circ \alpha = ((\alpha \circ \alpha) \circ \alpha) \circ \alpha$$

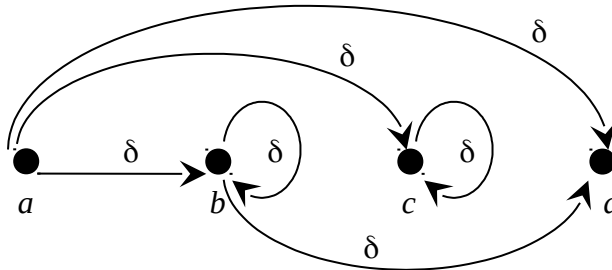
...

Можно тогда объединить все степени некоторого отношения α в некоторое множество $B_\alpha = \{x \mid \exists k x = \alpha^k\}$. В соответствии с рекуррентным соотношением оно строится следующим образом: Отправной точкой в построении берется элемент $\alpha \in B_\alpha$. Определим на B_α функцию, ставящую некоторой степени α в соответствие следующую за ней степень. Эту функцию естественно назвать *функцией следования*. Обозначим её символом s_α :

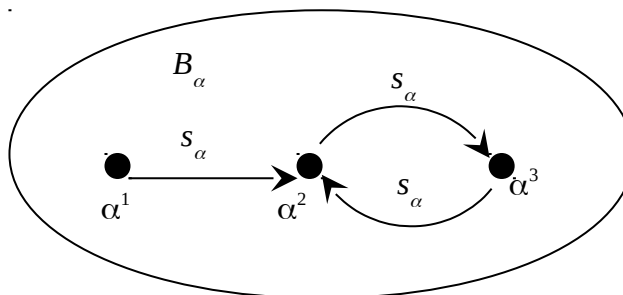
$$\forall x \in B_\alpha \quad s_\alpha(x) = x \circ \alpha, \text{ при этом } s_\alpha \in B_\alpha^{B_\alpha}$$

Тогда элементы B_α могут быть все получены последовательным применением этой функции сначала к α , затем к $s_\alpha(\alpha)$, затем к $s_\alpha(s_\alpha(\alpha))$ и так далее.

В продолжение примера с ориентированным графом на четырёх узлах, посмотрим построение множества B_α . У нас уже вычислены в виде графов $\alpha^1 = \alpha$, $\alpha^2 = s_\alpha(\alpha) = \alpha \circ \alpha = \beta$, $\alpha^3 = s_\alpha(s_\alpha(\alpha)) = (\alpha \circ \alpha) \circ \alpha = \beta \circ \alpha = \gamma$. Следующая степень, $\alpha^4 = s_\alpha(s_\alpha(s_\alpha(\alpha))) = ((\alpha \circ \alpha) \circ \alpha) \circ \alpha = \gamma \circ \alpha = \delta$ для данного начального расположения связей в графе даст ту же картину, что и $\alpha^2 = \beta$ ($\delta = \beta$):



Это означает, что если продолжить построение множества B_α по рекуррентной формуле, мы не получим новых значений элементов: $\alpha^4 = \alpha^2 \Rightarrow \alpha^5 = \alpha^4 \circ \alpha = \alpha^2 \circ \alpha = \alpha^3$. Можно представить графически поведение функции следования s_α на множестве B_α :



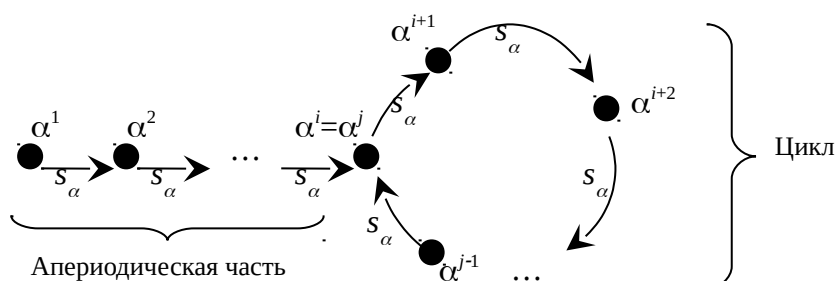
Эта функция не сюръективная – ни одна стрелка не входит в вершину α^1 , и не инъективная – в вершину α^2 входят сразу две стрелки (из α^1 и из α^3). И множество B_α получается конечным: $B_\alpha = \{\alpha^1, \alpha^2, \alpha^3\} = \{\alpha, \beta, \gamma\}$.

ОСОБЕННОСТИ ПОСЛЕДОВАТЕЛЬНОСТИ СТЕПЕНЕЙ БИНАРНОГО ОТНОШЕНИЯ НА КОНЕЧНОМ МНОЖЕСТВЕ

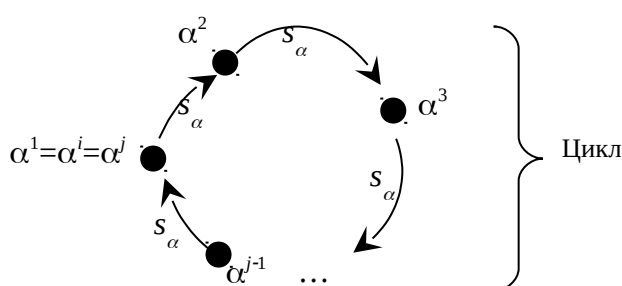
Оказывается, для любых отношений на конечных множествах множества значений степеней тоже будут конечными, а функция следования на них иметь (необязательную) аperiодическую часть и цикл (возможно из одного значения). Такая функция следования может быть инъективной тогда и только тогда, когда цикл проходит через первую степень.

Возможные поведения функции следования на конечном множестве можно схематично изобразить так:

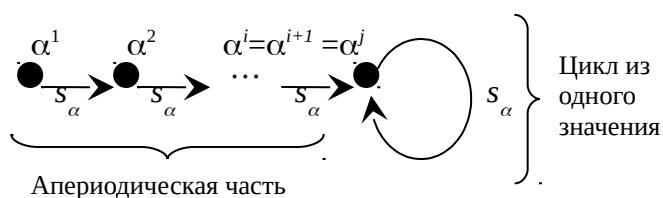
Аperiодическая часть и цикл



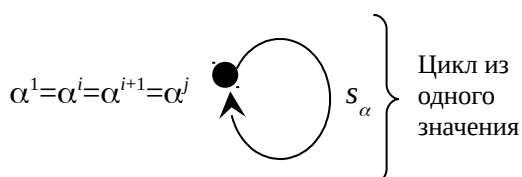
Цикл, проходящий через α^1



Аperiодическая часть, затем цикл из одного значения



Цикл из одного значения, $B_\alpha = \{\alpha^1\}$



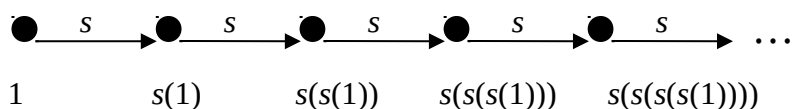
Если отношение $\alpha \subseteq A \times A$ и A состоит из n элементов, то, так как возможно составить n^2 упорядоченных пар, и каждая пара может быть либо представлена, либо не представлена в некотором отношении на A , разных степеней α не более 2^{n^2} . Поэтому можно выбрать такие минимальные показатели степеней i и $j > i$ что $\alpha^i = \alpha^j$. При этом длина цикла будет $j-i$.

Тема 4. Ряд натуральных чисел. РЕКУРРЕНТНЫЕ ФОРМУЛЫ И ФУНКЦИЯ СЛЕДОВАНИЯ. ПРИНЦИП ИНДУКЦИИ. ПРИМЕРЫ ДОКАЗАТЕЛЬСТВ В ФОРМАЛЬНОЙ АРИФМЕТИКЕ.

Интересно, что и ряд натуральных чисел может быть описан образом аналогичным тому, как описывается множество всех степеней некоторого отношения по композиции. Положим, на некотором множестве N задана функция $s \in N^N$ (и соответствующее отношение равенства, обозначаемое символом $=$, требуемое для указания его свойства функциональности). Также положим наличие элемента $1 \in N$, с которого начнём построение ряда, используя s в качестве функции следования. На неё наложим следующие ограничения:

- 1) s – инъективная функция: $\forall x \in N \forall y \in N ((s(x)=s(y)) \rightarrow (x=y))$
- 2) Элемент 1 не покрыт значениями s : $\neg \exists x \in N (s(x)=1)$

В этом случае $s(1) \neq 1$ по свойству (2). То есть уже имеем два разных элемента. $s(s(1)) \neq 1$ также по свойству (2). Но $s(s(1)) \neq s(1)$ по свойству (1), иначе бы $s(1)$ был сопоставлен сразу, как уже показано, разным аргументам 1 и $s(1)$. Рассуждая аналогично, можно показать, что и другие элементы ряда все различны. Начало графа такой функции выглядит так:



Собственно такой ряд отражает (моделирует) процесс счета. Он подобен унарной системе записи: число «один» обозначается как 1, число «два» обозначается как $s(1)$, число «три» как $s(s(1))$ и так далее. То есть основной формой представления чисел здесь является их выражение через элемент 1 и функцию следования s . Каждому числу соответствует единственная такая формула.

На этом ряду далее можно определить арифметические операции рекуррентными соотношениями, подобно тому, как ранее была определена степень для бинарных отношений. Покажем, как определить бинарную операцию сложения, обозначаемую символом $+$. Задаются начальные условия (А) – что означает прибавление 1 (переход к следующему в ряду элементу) и рекуррентная формула (В) – как, зная как прибавить некоторое число, прибавить следующее (это будет следующее за суммой):

- (правило А) $x+1 = s(x)$
 (правило В) $x+s(y) = s(x+y)$

Покажем, как применять эти правила для вычисления результата операции $+$. Вычислим результат сложения чисел «два» и «три». Необходимо найти представление для выражения $s(1)+s(s(1))$ только через символы 1 и s , применяя правила (А) и (В):

$$s(1) + s(s(1)) \overset{B}{=} s(s(1) + s(1)) \overset{B}{=} s(s(s(1) + 1)) \overset{A}{=} s(s(s(s(1))))$$

Над знаками $=$ надписаны названия правил, по которым производится замена: если справа от символа $+$ стоит формула вида $s(...)$, применяется правило (В), если справа от

символа + стоит символ 1, применяется правило (А). Процесс заканчивается, когда в формуле остаются только символы 1 и s. В данном примере $s(s(s(s(1))))$ является представлением для числа «пять», единственным в данной системе записи. Сам термин «формальная арифметика» используется для данной модели счета именно потому, что элементы множества натуральных чисел представлены в виде правильно построенных формул с предметной константой 1 и одноместным функциональным символом s.

Конечно, такой способ вычислений (в унарном коде) неэффективен. Использование привычной позиционной системы (десятичной или двоичной) существенно выгоднее. Но такая унарная форма с рекуррентными определениями операций позволяет доказывать многие свойства существенно проще, а главное, с минимальным набором первичных представлений.

Доказательства утверждений о произвольных таких натуральных числах (формул вида $\forall x \in N P(x)$) невозможно выполнить просто перебирая все элементы, строя их по рекуррентной формуле (в отличие от рассматривавшихся ранее конечных множеств, например, логических значений). Видно, что процесс построения всех натуральных чисел (формул вида $s(s(s(...)))$) не может быть закончен за конечное число шагов – натуральный ряд не может иметь точек повторения, аналогичных $\alpha^i = \alpha^j$. Поэтому, если формулу не удаётся доказать методами вывода логических исчислений (найти конечную цепочку подстановок по некоторым правилам, переводящим одну формулу в другую), прибегают к выводу на основе принципа индукции.

Допустим, необходимо доказать истинность высказывания вида $\forall x \in N P(x)$. Здесь P – некоторое свойство для натурального числа. Формулу $\forall x \in N P(x)$ считаем доказанной, если возможно доказать истинности следующих утверждений:

- 1) База индукции: $P(1)$
- 2) Шаг индукции (индукционный переход): $\forall x \in N (P(x) \rightarrow P(s(x)))$

То есть, мы как бы добавили новое правило вывода

$$(P(1) \& (\forall x \in N (P(x) \rightarrow P(s(x))))) \Rightarrow (\forall x \in N P(x))$$

Само утверждение $P(x)$ на шаге индукции называют индукционным предположением.

Докажем, например, что определённая выше операция сложения натуральных чисел + является ассоциативной: $(a+b)+c=a+(b+c)$. Сформулируем задачу так, чтобы увидеть, в чем заключается в данном случае свойство P . Определим предикат P следующим образом:

$$P(x) = ((a+b)+x=a+(b+x))$$

Тогда база индукции превратится в $P(1) = ((a+b)+1=a+(b+1))$, а шаг индукции будет иметь вид:

$$(P(x) \Rightarrow P(s(x))) = ((a+b)+x=a+(b+x) \Rightarrow (a+b)+s(x)=a+(b+s(x)))$$

Докажем сначала первое утверждение $(a+b)+1=a+(b+1)$, используя правила, определяющие операцию +:

$$\text{По правилу (A) } (a+b)+1 = s(a+b).$$

$$\text{По правилу (A) } a+(b+1) = a+s(b).$$

$$\text{По правилу (B) } a+s(b) = s(a+b).$$

Получили, что и левая и правая части равенства равны $s(a+b)$.

Теперь аналогично докажем второе утверждение

$$(a+b)+x=a+(b+x) \Rightarrow (a+b)+s(x)=a+(b+s(x))$$

Для левой части получаем (над символами = надписаны названия правил, по которым производится замена текста в формулах): $(a + b) + s(x) \stackrel{B}{=} s((a + b) + x)$.

Для правой части $a + (b + s(x)) \stackrel{B}{=} a + s(b + x) \stackrel{B}{=} s(a + (b + x))$.

Но аргументы s в левой и правой частях равны по индукционному предположению: $(a+b)+x=a+(b+x)$. Следовательно, должны быть равны и результаты: $s((a+b)+x)=s(a+(b+x))$.

Тем самым доказана формула $\forall x \in N P(x) = \forall x \in N ((a+b)+x=a+(b+x))$.

Аналогично можно дать рекуррентное определение для умножения как многократного сложения и для возведения в степень, как многократного умножения:

$$\begin{aligned} x \cdot 1 &= x \\ x \cdot s(y) &= (x \cdot y) + x \end{aligned}$$

$$\begin{aligned} x^1 &= x \\ x^{s(y)} &= x^y \cdot x \end{aligned}$$

Положенные в основу данной модели счета свойства функции следования совместно с рекуррентным заданием правил выполнения операций над формулами и принципом индукции известны в математике как *система аксиом Пеано для формальной арифметики*.

Принцип индукции в математике трактуется двояко: если в системе рассуждений принято говорить о таких бесконечных объектах, как, например, рассмотренный ряд натуральных чисел, как о готовых объектах (хотя ясно, что его невозможно построить за конечное число шагов), его можно рассматривать как дополнительное правило вывода к логическим исчислениям. Такой подход известен как *абстракция актуальной бесконечности*. Другая трактовка может быть пояснена так: несмотря на то, что мы не можем построить подобное бесконечное множество целиком, укажем, как выполнять те или иные действия для их произвольных элементов. Например, приведённое доказательство по индукции для свойства ассоциативности можно рассматривать как набор правил для выписывания доказательства в виде конечного набора подстановок для любого числа c , представленного в указанной форме (через 1 и s). Для $c=s(1)$ будем иметь

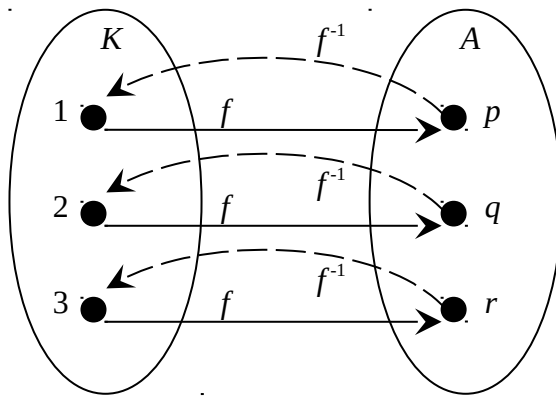
$$\begin{aligned} (a + b) + s(s(1)) &\stackrel{B}{=} s((a + b) + s(1)) \stackrel{B}{=} s(s((a + b) + 1)) \\ a + (b + s(s(1))) &\stackrel{B}{=} a + s(b + s(1)) \stackrel{B}{=} s(a + (b + s(1))) \stackrel{B}{=} s(a + s(b + 1)) \stackrel{B}{=} s(s(a + (b + 1))) \end{aligned}$$

Неважно, что мы не можем выписать все такие цепочки формул для всех элементов натурального ряда. Зато у нас есть *алгоритм* выписывания их для любого конкретного элемента. Такой подход известен как *абстракция потенциальной бесконечности*.

Множество натуральных чисел в дальнейшем будем обозначать символом \mathbb{N} , а его элементы в любой удобной системе счисления, позиционной или унарной.

ИСПОЛЬЗОВАНИЕ МАТРИЦ БИНАРНЫХ ОТНОШЕНИЙ ДЛЯ ВЫЧИСЛЕНИЯ КОМПОЗИЦИИ БИНАРНЫХ ОТНОШЕНИЙ

Вернёмся теперь к конечным множествам и отношениям на них. Конечное множество можно представить как множество, эквивалентное некоторому отрезку натурального ряда от начального элемента 1 до некоторого конечного числа. Под эквивалентностью множеств имеется в виду возможность построить взаимнооднозначное соответствие (биективную функцию) из одного множества в другое (и обратно). Будем в этом случае говорить, что множество *занумеровано*. Его элементы будем тогда символически обозначать в виде символа с нижним индексом. Фактически это есть просто форма представления той самой функции, взаимнооднозначно ставящей в соответствие натуральному числу элемент конечного множества. Следующая схема поясняет это представление:



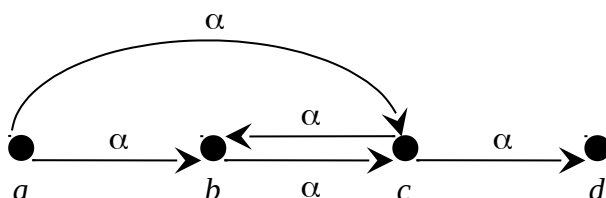
Здесь в A – три элемента. Числам 1, 2, 3 взаимнооднозначно сопоставлены элементы множества A . Пусть для индексации элементов множества выбран символ a . Тогда для данной функции f , нумерующей элементы множеств, обозначим $a_i = f(i)$. То есть $a_1 = p$, $a_2 = q$, $a_3 = r$. $K = \{1, 2, 3\}$ здесь множество индексов, $K \subseteq \mathbb{N}$, $f \in A^K$, $A \sim K$. Будем также записывать $A = \{a_1, a_2, a_3\}$. Для конечного, но не оговоренного числа элементов n будем записывать $A = \{a_1, a_2, \dots, a_n\}$ и говорить, множество A содержит n элементов.

На основе такого приписывания индексов элементам множеств рассмотрим ещё одну удобную форму представления бинарных отношений (и, соответственно, ориентированных графов) – представление при помощи матриц. Пусть $\alpha \subseteq A \times B$ и $A = \{a_1, a_2, \dots, a_n\}$ и $B = \{b_1, b_2, \dots, b_m\}$. Матрицей отношения α называется прямоугольная матрица из n строк и m столбцов из логических значений высказываний вида $(a_i, b_j) \in \alpha$ в строке i и столбце j . Матрицу отношения α будем обозначать символом C^α :

$$C_{ij}^\alpha = (a_i, b_j) \in \alpha$$

Номера строк соответствуют элементам множества A . Номера столбцов соответствуют элементам множества B . Если $\alpha \subseteq A \times A$, то матрица будет квадратной.

Например, для уже рассматривавшегося примера отношения, заданного ориентированным графом



при нумерации элементов $A=\{a_1, a_2, a_3, a_4\}$, $a_1=a, a_2=b, a_3=c, a_4=d$, матрица отношения будет

$$C^\alpha = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

В матричной форме удобно выполнять рассмотренные операции над отношениями.

Теоретико-множественные операции над отношениями на одних и тех же множествах выполняются покомпонентно:

$$C_{ij}^{\bar{\alpha}} = \neg C_{ij}^{\alpha}, \quad C_{ij}^{\alpha \& \beta} = C_{ij}^{\alpha} \& C_{ij}^{\beta}, \quad C_{ij}^{\alpha \vee \beta} = C_{ij}^{\alpha} \vee C_{ij}^{\beta} \text{ и т.д.}$$

Обращение заключается в *транспонировании* матрицы (замена строк на столбцы)

$$C_{ij}^{\alpha^{-1}} = C_{ji}^{\alpha} \text{ или более кратко } C^{\alpha^{-1}} = (C^{\alpha})^T$$

Вычисление композиции заключается в *логическом умножении* матриц. Обозначим эту операцию символом \bullet и определим ее следующим образом:

$$(C^{\alpha} \bullet C^{\beta})_{ij} = \bigvee_k C_{ik}^{\alpha} \& C_{kj}^{\beta}$$

Тогда матрица для композиции будет строиться так:

$$C^{\alpha \circ \beta} = C^{\alpha} \bullet C^{\beta}$$

Смысл этой операции в том, что перебираются все элементы общего для данных отношений множества и проверяется, может ли такой элемент k быть промежуточным на пути из двух шагов от элемента i к элементу j .

Вычислим степенной ряд для отношения из примера, используя матричную форму:

$$C^{\alpha^2} = C^{\alpha} \bullet C^{\alpha} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$C^{\alpha^3} = C^{\alpha^2} \bullet C^{\alpha} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$C^{\alpha^4} = C^{\alpha^3} \bullet C^{\alpha} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = C^{\alpha^2}$$

Степени отношений выражают возможность достичь одну вершину из другой ровно за определенное число шагов. Чаще интереснее узнать, можно ли вообще за какое-либо число шагов перейти из одной вершины в другую. Запишем условие такого перехода из вершины x в вершину y :

$$(x, y) \in \alpha^1 \vee (x, y) \in \alpha^2 \vee (x, y) \in \alpha^3 \vee \dots$$

То есть по всем возможным k необходимо объединить по операции ЛОГИЧЕСКОЕ ИЛИ k степени отношения α . Это есть представление фразы «достижимо за 1 шаг ИЛИ достижимо за 2 шага ИЛИ достижимо за 3 шага ИЛИ ...». Соединению высказываний через связку \vee соответствует объединение соответствующих множеств – степеней отношения. Объединение ведется по всем возможным степеням – натуральным числам. Результат можно назвать отношением *достижимости*, обозначается символом $\hat{\alpha}$ над обозначением отношения. По определению

$$\hat{\alpha} = \bigcup_{k \in \mathbb{N}} \alpha^k$$

Но перебирать все натуральные числа невозможно, а достижимость надо вычислять. Оказывается для конечных множеств A из n элементов, на которых задано отношение α ($\alpha \subseteq A \times A$) достаточно объединить первые n степеней. Символически будем записывать это так:

$$\hat{\alpha} = \bigcup_{k=1}^n \alpha^k$$

Это объясняется тем, что если между вершинами есть путь за сколько-нибудь шагов, и этот путь длиннее числа вершин, то промежуточные вершины вместе с конечной вершиной не могут все быть различными. Это означает наличие цикла в маршруте и путь можно сократить на длину указанного цикла. Новый, эквивалентный путь, если он окажется длиннее числа вершин можно аналогично сократить. Иначе мы уже нашли путь длины не более n . Процедуру же сокращения можно выполнять, пока длина пути не перестанет превосходить n .

Более формально,

$$(x, y) \in \hat{\alpha} \Rightarrow \exists k (x, y) \in \alpha^k$$

$$\text{Если } k \leq n \text{ то условие выполнено, } (x, y) \in \bigcup_{k=1}^n \alpha^k$$

Иначе для $k > n$ выписываем условие наличия пути длиной k

$$(x, y) \in \alpha^k \Rightarrow \exists u_1 \exists u_2 \dots \exists u_{k-1} (x, u_1) \in \alpha \ \& \ (u_1, u_2) \in \alpha \ \& \ \dots \ \& \ (u_{k-1}, y) \in \alpha.$$

Обозначим $u_k = y$. Тогда $\exists i \exists j > i \ u_i = u_j$. Получаем новый путь

$$(x, u_1) \in \alpha \ \& \ (u_1, u_2) \in \alpha \ \& \ \dots \ \& \ (u_{i-1}, \underline{u_i}) \in \alpha \ \& \ (\underline{u_i}, u_{j+1}) \in \alpha \ \& \ \dots \ \& \ (u_{k-1}, y) \in \alpha.$$

Место, где удалён цикл, подчеркнуто.

$$\text{Длина этого цикла } k' = k - (j - i) < k. \Rightarrow (x, y) \in \alpha^{k'}.$$

Продолжая эту процедуру необходимое число раз, можно показать, что

$$\exists m \leq n (x, y) \in \alpha^m \Rightarrow (x, y) \in \bigcup_{k=1}^n \alpha^k$$

Для вычисления достижимости в матричной форме используется сочетание матричного произведения для вычисления степеней и объединения результатов при помощи поэлементного ЛОГИЧЕСКОГО ИЛИ.

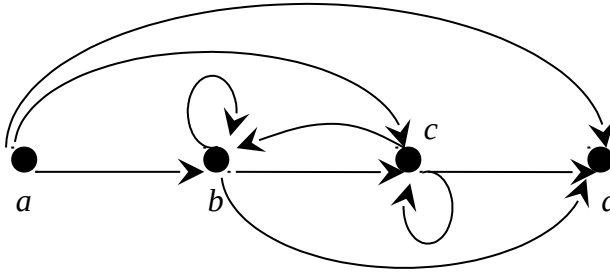
$$C_{ij}^{\hat{\alpha}} = \bigvee_{k=1}^n C_{ij}^{\alpha^k}$$

Обратите внимание, что это существенно меньше действий, чем верхняя оценка для числа разных значений степени (2^{n^2}). Конечно, реальные длины рядов степеней короче, может быть даже меньше n . В рассмотренном примере при $n=4$ было только три разных степени. В примере, где $\alpha^4=\alpha^2$, можно вычислить $\hat{\alpha}$ как $\hat{\alpha}=\alpha^1\cup\alpha^2\cup\alpha^3$.

В матричной форме для рассмотренного примера получим

$$C^{\hat{\alpha}} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Граф для этого отношения будет иметь вид



Для натуральных чисел достижимость по функции следования представляет собой отношение «меньше»:

$$\hat{S} = \{(x, y) \mid x \in \mathbb{N} \ \& \ y \in \mathbb{N} \ \& \ x < y\}$$

Фактически, это могло бы быть определением для отношения $<$ на \mathbb{N} :

$$x < y \Leftrightarrow (x, y) \in \hat{S}$$

Пример ($2 < 4$):

$$(s(1), s(s(1))) \in s \ \& \ (s(s(1)), s(s(s(1)))) \in s \Rightarrow (s(1), s(s(s(1)))) \in s \circ s \Rightarrow (s(1), s(s(s(1)))) \in \hat{S}.$$

Так можно формализовать конечное множество натуральных чисел, меньших или равных заданного числа x (например, множество индексов для нумерации):

$$K_x = \{ y \mid y \in \mathbb{N} \ \& \ ((y, x) \in \hat{S} \vee (x=y)) \}$$

Можно тогда сказать, «множество A имеет n элементов» как $A \sim K_n$ (множество A эквивалентно множеству K_n).

В параллель с рекуррентно определяемыми операциями (степень, сумма, произведение) можно говорить и о рекуррентно определяемых предикатах (свойствах). Например, имея функциональное отношение следования s с соответствующим двухместным предикатом $S(x, y) = (y=s(x))$ рекуррентно определим свойство «быть натуральным числом» $N(x) = (x \in \mathbb{N})$:

$$N(1) \ \& \ \forall x \forall y ((N(x) \ \& \ S(x, y)) \rightarrow N(y))$$

То есть $N(y) = (y=1) \vee (y=s(x) \ \& \ N(x))$ или

Правило 1: $N(1)=1$

Правило 2: $N(s(x))=N(x)$

Тогда вычислим, например $N(s(s(1)))$:

$$N(s(s(1))) = N(s(1)) = N(1) = 1$$

Тема 5. СПЕЦИАЛЬНЫЕ ВИДЫ БИНАРНЫХ ОТНОШЕНИЙ. ОТНОШЕНИЯ ЭКВИВАЛЕНТНОСТИ. КЛАССЫ ЭКВИВАЛЕНТНОСТИ. РАЗБИЕНИЯ. ПРИМЕРЫ ОТНОШЕНИЙ ЭКВИВАЛЕНТНОСТИ.

Рассмотрим теперь некоторые специальные бинарные отношения, используя введенные обозначения и представления, а также дадим некоторые новые определения.

Назовём отношение $\Delta_A = \{(x, x) \mid x \in A\}$ *диагональным* отношением множества A . Это самый узкий класс эквивалентностей, возможный в некоторой системе обозначений. Обычно это просто отношение равенства на A : $\Delta_A = \{(x, y) \mid x \in A \text{ \& } y \in A \text{ \& } x=y\}$. Графически ему соответствует набор вершин с петлями без рёбер между вершинами. Матрица такого отношения будет диагональной (единичной) логической матрицей. Отсюда название.

$$C^{\Delta_A} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Рассматривавшееся свойство рефлексивности может тогда быть выражено формулой $\Delta_A \subseteq \alpha$.

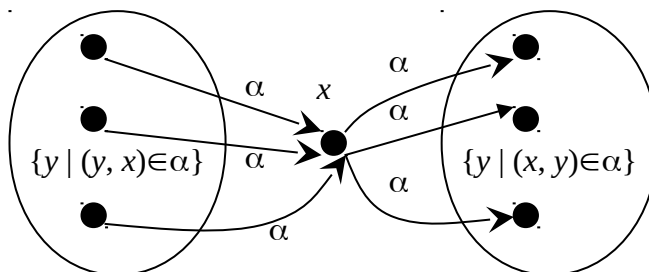
Симметричность можно выразить формулой $\alpha^{-1} = \alpha$.

Транзитивность можно выразить формулой $\alpha \circ \alpha \subseteq \alpha$. (можно написать и $\alpha^2 \subseteq \alpha$)

Таким образом, получаем определение для отношения эквивалентности

α - эквивалентность на множестве $A \Leftrightarrow (\Delta_A \subseteq \alpha \text{ \& } \alpha^{-1} = \alpha \text{ \& } \alpha \circ \alpha \subseteq \alpha)$.

Если α - некоторое бинарное отношение ($\alpha \subseteq A \times A$), а x – некоторый элемент ($x \in A$), то для этого элемента можно указать множества элементов, связанных с ним по α так, что он будет являться первым элементом в упорядоченной паре $\{y \mid (x, y) \in \alpha\}$. Графически это можно представить как все вершины, куда можно попасть из x за один шаг:



Аналогично можно указать и множество $\{y \mid (y, x) \in \alpha\}$, вершин, где начинаются стрелки, идущие в x .

Но если $\alpha^{-1} = \alpha$ то $\{y \mid (x, y) \in \alpha\} = \{y \mid (y, x) \in \alpha\}$. Для симметричных отношений обозначим такое множество как

$$[x]_\alpha = \{y \mid (x, y) \in \alpha\} = \{y \mid (y, x) \in \alpha\}$$

Если α это эквивалентность, то будем называть $[x]_\alpha$ *классом эквивалентности* элемента x по отношению α . Это есть просто **множество элементов, эквивалентных x** . При этом элемент x называют *образующим* класса $[x]_\alpha$.

Для классов эквивалентности некоторого $\alpha \subseteq A \times A$ следует отметить следующие свойства.

1) Каждый элемент принадлежит своему классу эквивалентности.

$$\forall x \in A \quad x \in [x]_\alpha$$

Это свойство следует из рефлексивности α :

$$\Delta_A \subseteq \alpha \Rightarrow \forall x \in A \quad (x, x) \in \alpha \Rightarrow \forall x \in A \quad x \in [x]_\alpha$$

2) Каждый элемент из класса образует в точности тот же самый класс.

$$y \in [x]_\alpha \Rightarrow [y]_\alpha = [x]_\alpha$$

Для обоснования необходимо использовать и свойство симметричности, и свойство транзитивности:

$$y \in [x]_\alpha \Rightarrow (y, x) \in \alpha \ \& \ (x, y) \in \alpha \text{ по определению } [x]_\alpha \text{ и симметричности } \alpha$$

Покажем что $[y]_\alpha \subseteq [x]_\alpha$, то есть, что $z \in [y]_\alpha \Rightarrow z \in [x]_\alpha$

$$z \in [y]_\alpha \Rightarrow (z, y) \in \alpha \ \& \ (y, z) \in \alpha \text{ по определению } [y]_\alpha \text{ и симметричности } \alpha.$$

$$\text{Имеем } (z, y) \in \alpha \ \& \ (y, x) \in \alpha$$

$$\text{По транзитивности } \alpha \text{ и определению } [x]_\alpha \text{ получаем } (z, x) \in \alpha \Rightarrow z \in [x]_\alpha$$

Аналогично покажем $[x]_\alpha \subseteq [y]_\alpha$, то есть, что $z \in [x]_\alpha \Rightarrow z \in [y]_\alpha$

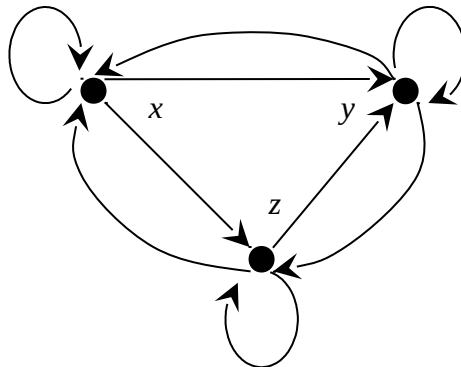
$$z \in [x]_\alpha \Rightarrow (z, x) \in \alpha \ \& \ (x, z) \in \alpha \text{ по определению } [x]_\alpha \text{ и симметричности } \alpha.$$

$$\text{Имеем } (z, x) \in \alpha \ \& \ (x, y) \in \alpha$$

$$\text{По транзитивности } \alpha \text{ и определению } [y]_\alpha \text{ получаем } (z, y) \in \alpha \Rightarrow z \in [y]_\alpha$$

$$\text{Из } [y]_\alpha \subseteq [x]_\alpha \text{ и } [x]_\alpha \subseteq [y]_\alpha \text{ получаем } [y]_\alpha = [x]_\alpha$$

Следующий возможный фрагмент графа поясняет эти 4 связи (рефлексивность непосредственно не используется для доказательства, но петли на графе приведены для иллюстративных целей, α – это эквивалентность):



То есть, если z эквивалентен x , а x и y эквивалентны между собой, то z эквивалентен каждому из них. Фактически, класс $[z]_\alpha$ совпадает с $[x]_\alpha$ и $[y]_\alpha$.

Рассмотренное свойство можно сформулировать и в виде следующей фразы:

3) Каждый класс эквивалентности представляет собой в точности множество всех своих образующих элементов.

4) Два класса либо не имеют общих элементов, либо полностью совпадают.

Возможные формулировки:

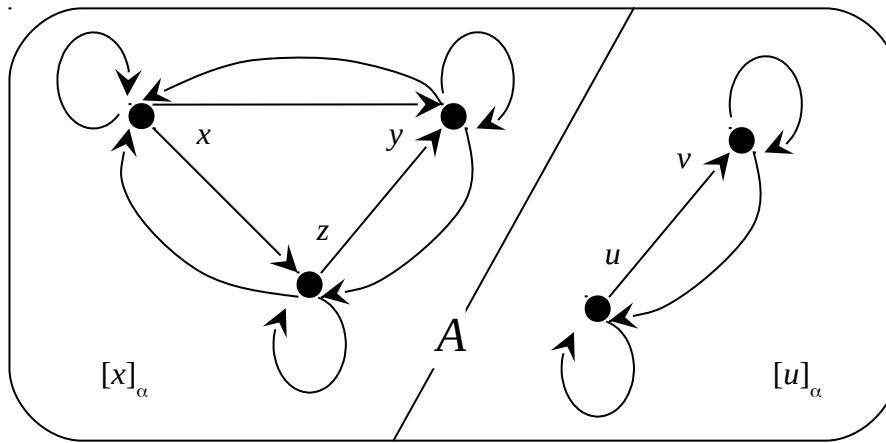
$$\forall x \in A \quad \forall y \in A \quad ([x]_\alpha \cap [y]_\alpha = \emptyset) \oplus ([x]_\alpha = [y]_\alpha)$$

или

$$([x]_\alpha \cap [y]_\alpha \neq \emptyset) \Rightarrow ([x]_\alpha = [y]_\alpha)$$

$$([x]_\alpha \neq [y]_\alpha) \Rightarrow ([x]_\alpha \cap [y]_\alpha = \emptyset)$$

Таким образом, каждый класс эквивалентности представляет собой полносвязное по α множество, а между разными классами связей α нет. Пример фрагмента графа, удовлетворяющего этому условию, показан на рисунке.



В множестве A выделено два класса эквивалентности $[x]_\alpha = [y]_\alpha = [z]_\alpha = \{x, y, z\}$ и $[u]_\alpha = [v]_\alpha = \{u, v\}$. Эти классы образуют разбиение множества A . Это множество (множество классов) называется фактормножеством. Для него используется следующее обозначение:

$$A /_\alpha = \{ [x]_\alpha \mid x \in A \}$$

В данном примере $A /_\alpha = \{ \{x, y, z\}, \{u, v\} \}$

Вообще **разбиением** некоторого множества A называют семейство множеств (множество S из множеств C), таких, что они

- 1) не пустые
- 2) в объединении покрывают всё множество A
- 3) попарно либо не пересекаются, либо полностью совпадают

$$(\forall C \in S \quad C \neq \emptyset) \ \& \ A = \bigcup_{C \in S} C \ \& \ (\forall C_1 \in S \quad \forall C_2 \in S \quad ((C_1 \cap C_2 = \emptyset) \oplus (C_1 = C_2)))$$

При этом сами множества из семейства называют *классами разбиений*.

Покажем, что любое такое разбиение порождает некоторое отношение эквивалентности α , которое можно охарактеризовать как свойство «принадлежать одному классу разбиения»:

$$\alpha = \{ (x, y) \mid \exists C \in S \quad x \in C \ \& \ y \in C \}$$

Рефлексивность: $x \in A \ \& \ A = \bigcup_{C \in S} C \Rightarrow \exists C \in S \ x \in C \Rightarrow (x, x) \in \alpha$.

Симметричность: Следует из коммутативности связки $\&$ в определении α .

Транзитивность:

$(x, y) \in \alpha \ \& \ (y, z) \in \alpha \Rightarrow (\exists C_1 \in S \ x \in C_1 \ \& \ y \in C_1) \ \& \ (\exists C_2 \in S \ y \in C_2 \ \& \ z \in C_2) \Rightarrow$
 $(\exists C_1 \in S \ \exists C_2 \in S \ x \in C_1 \ \& \ y \in C_1 \ \& \ y \in C_2 \ \& \ z \in C_2 \ \& \ C_1 \cap C_2 \neq \emptyset \ \& \ C_1 = C_2) \Rightarrow$
 $(\exists C \in S \ x \in C \ \& \ z \in C) \Rightarrow (x, z) \in \alpha$

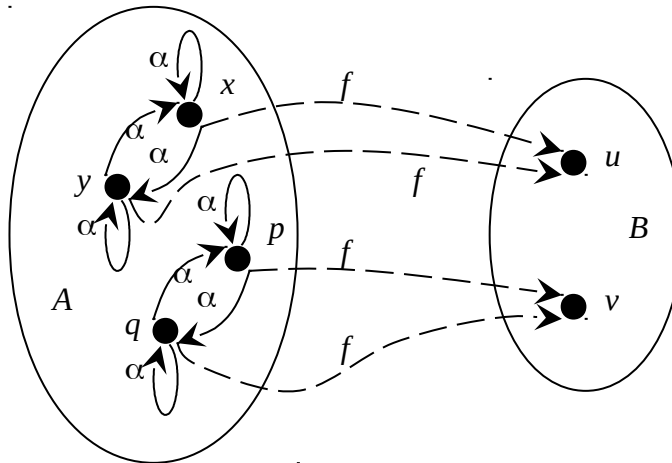
Важным примером отношений эквивалентности являются отношения, получаемые при функциональном отображении одного множества на другое. Допустим, $f \in B^A$. Построим отношение $\alpha \subseteq A \times A$ следующим образом:

$$\alpha = \{(x, y) \mid f(x) = f(y)\}$$

Тогда оно будет являться отношением эквивалентности. Эквивалентными будут элементы, которым функция f ставит в соответствие одинаковые значения (в смысле некоторого отношения равенства на множестве B). При этом классом эквивалентности будут множества всех тех элементов в A , для которых значения функции равны:

$$[x]_\alpha = \{y \mid f(x) = f(y)\}$$

Следующая диаграмма показывает пример такого отношения:



То, что данное отношение действительно является эквивалентностью, непосредственно следует из аналогичных свойств отношения $=$ на множестве B .

ПРИМЕРЫ ОТНОШЕНИЙ ЭКВИВАЛЕНТНОСТИ: СРАВНИМОСТЬ. КОНГРУЭНЦИЯ.

В теории чисел часто рассматривается следующее отношение эквивалентности. По некоторому натуральному числу n любое целое число x можно единственным образом представить в виде $x=a \cdot n+b$ так, чтобы $0 \leq b$ и $b < n$. Тогда b называют остатком от деления x на n . При фиксированном n b можно рассматривать в качестве результата вычисления некоторой функции: $b=R_n(x)$. Определяя по рассмотренной схеме для этой функции отношение эквивалентности, получаем отношение «иметь одинаковые остатки от деления на n »: $\alpha_n = \{(x, y) \mid R_n(x)=R_n(y)\}$. Такое отношение называется *сравнением по модулю n* . Для него в математике используется специальное обозначение

$$x \equiv y \pmod{n}$$

Читается: « x сравнимо с y по модулю n ».

Каждый класс эквивалентности для этого отношения представляет собой множество чисел, дающих определённый остаток от деления на n , и называется *классом вычетов по модулю n* . Обозначаются эти классы обычно просто символами квадратных скобок вокруг числа, выбранного образующим элементом класса. Обычно число n ясно из контекста. Образующими обычно берут минимальные неотрицательные элементы классов.

Пример для $n=3$. Возможны три вида остатков: 0, 1, 2. Множество всех классов вычетов по модулю 3 будет $\{[0], [1], [2]\}$. Число 7 и число 13 оба дают остаток от деления на 3, равный 1. Поэтому пишут $7 \equiv 13 \pmod{3}$, при этом $7 \in [1]$ и $13 \in [1]$.

Множество всех целых чисел обычно обозначают символом \mathbb{Z} , а множество всех классов вычетов по модулю n обозначают \mathbb{Z}_n . Например, $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

Для операции сложения целых чисел $+$ такое разбиение на классы эквивалентности обладает важным свойством:

$$a \equiv b \pmod{n} \text{ \& } c \equiv d \pmod{n} \Rightarrow a+c \equiv b+d \pmod{n}$$

Получается, что данное отношение эквивалентности «согласовано» с некоторой операцией на разбиваемом множестве.

Отношение эквивалентности, согласованное с некоторой ассоциативной операцией на разбиваемом им на классы множестве, называется конгруэнцией:

$$(a, b) \in \alpha \text{ \& } (c, d) \in \alpha \Rightarrow (a * c, b * d) \in \alpha,$$

где $*$ – некоторая ассоциативная бинарная операция.

Таким же свойством сравнение по модулю n обладает и по отношению к умножению целых чисел: $a \equiv b \pmod{n} \text{ \& } c \equiv d \pmod{n} \Rightarrow a \cdot c \equiv b \cdot d \pmod{n}$.

Конгруэнция – основной способ получения конечных алгебр (особенно не двоичных) из бесконечных. Она позволяет определять операции между классами на основе операций между образующими элементами.

Операцией между классами называют множество возможных значений результатов операции между элементами классов:

$$[x]_\alpha * [y]_\alpha = \{ u * v \mid u \in [x]_\alpha \text{ \& } v \in [y]_\alpha \}$$

Для конгруэнции имеет место следующее представление:

$$[x]_\alpha * [y]_\alpha = [x * y]_\alpha$$

Для рассмотренного примера сравнения по модулю 3 можно построить следующие алгебры сложения и умножения классов:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Такая алгебра классов с операциями + и · называется кольцом классов вычетов по модулю 3. Например, выражение $[2]+[2]=[1]$ означает, что если сложить любые два числа, дающие остаток от деления на 3 равный 2, то получится число, дающее остаток от деления на 3 равный 1.

ПРИМЕРЫ ОТНОШЕНИЙ ЭКВИВАЛЕНТНОСТИ: ЭКВИВАЛЕНТНОСТЬ (РАВНОМОЩНОСТЬ) МНОЖЕСТВ. МОЩНОСТЬ МНОЖЕСТВА. СЧЁТНЫЕ И НЕСЧЁТНЫЕ МНОЖЕСТВА.

Еще одним примером отношения эквивалентности является уже упомянутая эквивалентность (равномощность) множеств: $A \sim B \Leftrightarrow (\exists f \in B^A (f^{-1} \in A^B))$. То, что это действительно отношение эквивалентности, следует из следующего:

1. Рефлексивность. Каждое множество равномощно самому себе. Рассматривая отношение Δ_A как функцию, ставящую каждому элементу множества A его самого, $\Delta_A \in A^A$, $\forall x \in A \Delta_A(x) = x$ (эта функция биективная, так как $(\Delta_A)^{-1} = \Delta_A$) видим, что $A \sim A$. То, что некоторая функция устанавливает равномощность, удобно обозначать, надписывая её обозначение над символом \sim : $A \overset{\Delta_A}{\sim} A$.
2. Симметричность. $A \overset{f}{\sim} B \Rightarrow B \overset{f^{-1}}{\sim} A$.
3. Транзитивность. $A \overset{f}{\sim} B \& B \overset{g}{\sim} C \Rightarrow A \overset{f \circ g}{\sim} C$

Классы эквивалентности отношения \sim представляют собой множества из всех множеств, равномощных некоторому образующему элементу (множеству). Обозначаются они обычно вертикальными чертами с обеих сторон от выбранного образующего элемента (множества) – представителя класса:

$$|A| = \{ B \mid A \sim B \}$$

Такой класс эквивалентности называют мощностью множества. Для конечных множеств представление о таких классах можно считать отвлечённым представлением о числе, возникающим при рассматривании разнородных наборов предметов, общим для которых является именно количество предметов в наборах. Для бесконечных множеств их мощности представляют дальнейшее развитие понятия числа. **Мощности произвольных множеств называют кардинальными числами. Множества, равномощные множеству натуральных чисел \mathbb{N} , называют счётными множествами.** В математике известны примеры построенных определений для бесконечных множеств, не являющихся счётными, например множество всех функций $\mathcal{B}^{\mathbb{N}}$ ($\mathcal{B} = \{0, 1\}$) не является счётным. Это множество можно представить как множество всех бесконечных двоичных последовательностей. В каждой последовательности на позиции с номером $j \in \mathbb{N}$ записано одно из двух возможных значений 0 или 1 (как функция от номера позиции). Если бы всё множество таких последовательностей было счётным (каждой последовательности был бы назначен номер $i \in \mathbb{N}$), последовательности можно было бы представить в виде a_{ij} , где i – номер последовательности, j – номер позиции. Но тогда можно построить новую последовательность, не совпадающую ни с одной из перечисленных по формуле

$$\forall j \in \mathbb{N} \quad b_j = \neg a_{jj}$$

Эта последовательность, на каждой позиции которой с номером j записано значение b_j , отличается от всех последовательностей, которые можно данным образом занумеровать (от каждой занумерованной последовательности она отличается, по крайней мере, в позиции, равной номеру последовательности). С другой стороны, она также (как функция от номера позиции) является элементом множества $\mathcal{B}^{\mathbb{N}}$. То есть, каково бы ни было отображение из \mathbb{N} в $\mathcal{B}^{\mathbb{N}}$, в $\mathcal{B}^{\mathbb{N}}$ останутся незанумерованные элементы (функции), что и показывает несчётность $\mathcal{B}^{\mathbb{N}}$.

Для конечных множеств само число элементов выбирают в качестве обозначений их мощности, пишут $|A| = n$, имея в виду, что каждому натуральному числу $n \in \mathbb{N}$

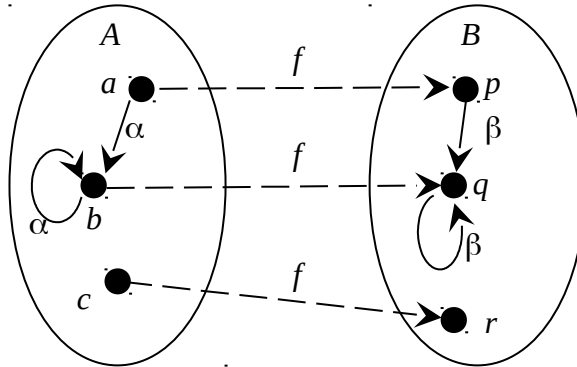
взаимнооднозначно сопоставлен некоторый класс множеств, равномоощных K_n – множеству натуральных чисел от 1 до n . Мощнось самого множества \mathbb{N} традиционно обозначают $|\mathbb{N}|=\aleph_0$ (древнееврейская буква алеф с индексом 0, обычно произноят «алеф-ноль», индексирование используется для указания порядковых типов множеств, здесь не рассматривается). Мощнось множества $\mathcal{B}^{\mathbb{N}}$ обозначают как $|\mathcal{B}^{\mathbb{N}}|=\aleph$ (алеф без индекса) или готической буквой \mathfrak{c} , и называют *мощносью континуума*.

ПРИМЕРЫ ОТНОШЕНИЙ ЭКВИВАЛЕНТНОСТИ: ПОДОБИЕ (ИЗОМОРФИЗМ) БИНАРНЫХ ОТНОШЕНИЙ (ОРИЕНТИРОВАННЫХ ГРАФОВ).

Следующий пример связан непосредственно с самим предметом рассмотрения – бинарными отношениями. Допустим, задано два бинарных отношения, каждое на своем множестве: $\alpha \subseteq A \times A$ и $\beta \subseteq B \times B$ и имеется биективная функция со следующим свойством:

$$f \in B^A \ \& \ f^{-1} \in A^B \ \& \ (\forall x \in A \ \forall y \in A \ ((x, y) \in \alpha \leftrightarrow (f(x), f(y)) \in \beta))$$

Следующий рисунок иллюстрирует пример такого отображения.



Везде, где есть связь по отношению α в A , есть связь между соответствующими отображениями по функции f в B по β . И наоборот, если нет связи в A между некоторыми элементами, то нет и связи между их отображениями в B . Например, $(a, b) \in \alpha$, $f(a) = p$, $f(b) = q$ и $(p, q) \in \beta$. Где есть петля в графе α , есть петля в графе β в вершине, соответствующей вершине с петлей в α по функции f .

Отношения, между которыми можно установить такие отображения, называются подобными.

Возможность установить такое отображение называется отношением подобия. Отношение подобия обозначим инфиксным символом \cong .

$$\alpha \cong \beta \Leftrightarrow \alpha \subseteq A \times A \ \& \ \beta \subseteq B \times B \ \& \ (\exists f \in B^A \ (f^{-1} \in A^B) \ \& \ (\forall x \in A \ \forall y \in A \ ((x, y) \in \alpha \leftrightarrow (f(x), f(y)) \in \beta)))$$

Как и с равномощностью множеств, для удобства будем надписывать над символом \cong обозначение функции, устанавливающей данное соответствие.

Покажем, что подобие отношений является отношением эквивалентности.

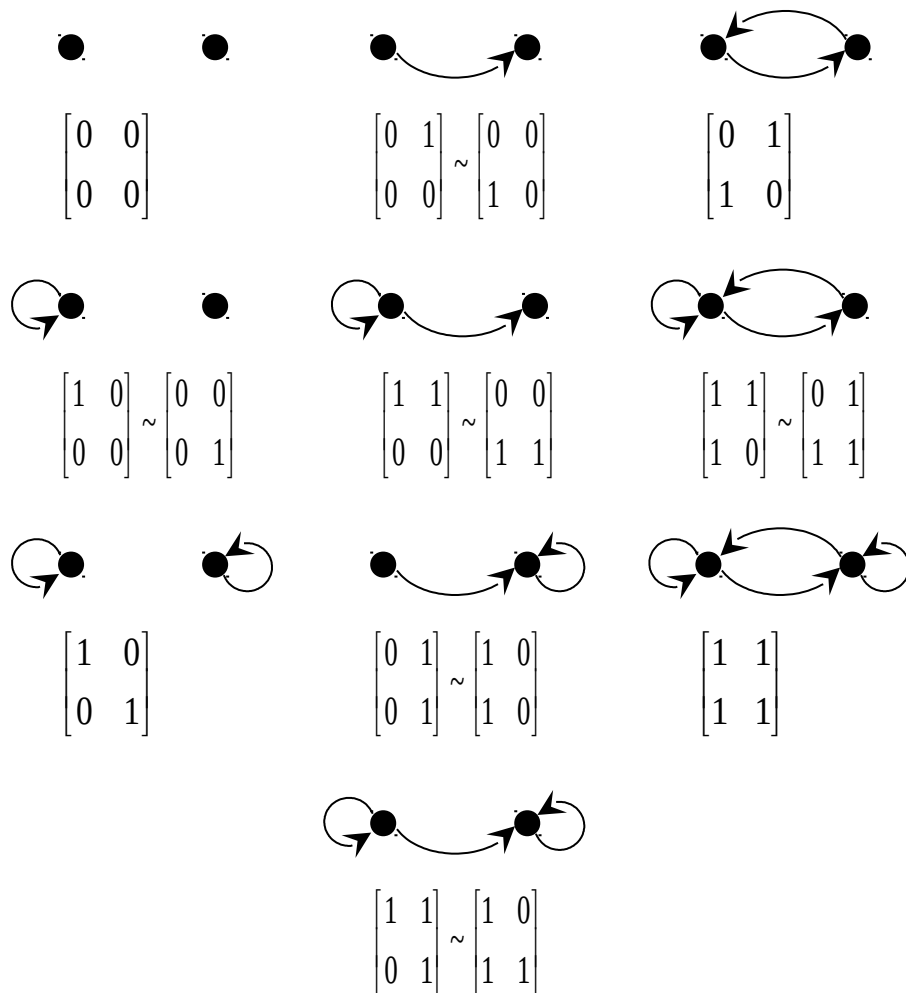
1. Рефлексивность. $\alpha \stackrel{\Delta_A}{\cong} \alpha$
2. Симметричность. $\alpha \stackrel{f}{\cong} \beta \Rightarrow \beta \stackrel{f^{-1}}{\cong} \alpha$
3. Транзитивность. $\alpha \stackrel{f}{\cong} \beta \ \& \ \beta \stackrel{g}{\cong} \gamma \Rightarrow \alpha \stackrel{f \circ g}{\cong} \gamma$

Классы эквивалентностей отношения подобия представляют собой множество всех отношений, имеющих определенную структуру связей между элементами без учета названий элементов и отношений. С точки зрения рассмотрения графов подобных отношений, подобие – это свойство иметь одинаковую форму графа. В рассмотренном примере оба графа могут быть описаны словами «три вершины, одна стрелка и петля в вершине, куда входит стрелка». Такие классы эквивалентностей можно назвать *абстрактными отношениями*. Их можно изображать графами, не подписывая узлов.

Важно, что все свойства отношений, рассматриваемые здесь, не зависят от названий отношений, названий элементов и интерпретации отношения в предметной области. С другой стороны, изучив свойства какого-либо конкретного отношения, фактически мы изучили свойства всех отношений данного класса. Для рассмотренного примера граф абстрактного отношения выглядит так:



Число различных классов отношений вообще-то меньше, чем самих отношений. Например, для двоичного множества все отношения могут быть представлены логическими матрицами 2×2 . Таких матриц 16. Некоторые из них будут представлять подобные отношения. Разбиение множества таких матриц на классы эквивалентности по подобию соответствующих им отношений представим ориентированными графами и укажем матрицы, реализующие эти отношения. Видно, что число классов (форм конфигураций связей) будет 10. Некоторые классы имеют по две реализации.



Тема 6. СПЕЦИАЛЬНЫЕ ВИДЫ БИНАРНЫХ ОТНОШЕНИЙ: ОТНОШЕНИЯ ПОРЯДКА. ОТРЕЗКИ. ДИАГРАММЫ ХАССЕ.

Введём еще одно определяющее свойство бинарных отношений: **антисимметричность**. **Отношение называют антисимметричным, если в его составе нет одновременно пар вида (x, y) и (y, x) для различных (не равных) x и y** . Пары вида (x, x) допускаются. Алгебраически это условие для $\alpha \subseteq A \times A$ выглядит так:

$$\alpha \cap \alpha^{-1} \subseteq \Delta_A$$

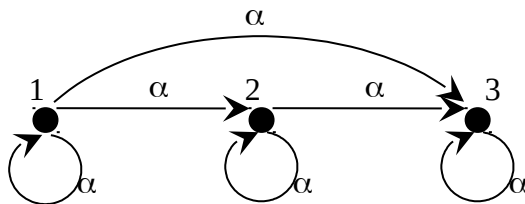
Полагая $\Delta_A = \{(x, y) \mid x \in A \ \& \ y \in A \ \& \ x=y\}$, эту формулу можно прочесть как:

$$(x, y) \in \alpha \ \& \ (y, x) \in \alpha \Rightarrow (x=y)$$

Отношение одновременно рефлексивное, антисимметричное и транзитивное называется отношением порядка.

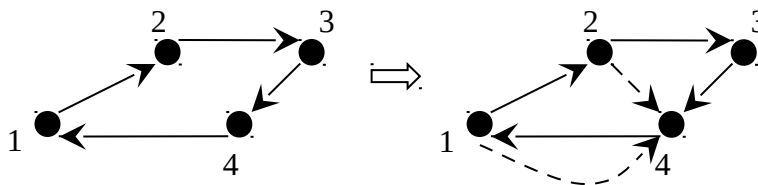
$$\alpha - \text{порядок} \Leftrightarrow (\Delta_A \subseteq \alpha) \ \& \ (\alpha \cap \alpha^{-1} \subseteq \Delta_A) \ \& \ (\alpha \circ \alpha \subseteq \alpha).$$

Примером отношения порядка может быть рассмотренное ранее отношение $\alpha = \{(x, y) \mid x \leq y\} = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$



Транзитивность здесь проявляется, например, в том, что $1 \leq 2 \ \& \ 2 \leq 3 \Rightarrow 1 \leq 3$. Антисимметричность заключается в однонаправленных связях между различными элементами.

Важным свойством для графов отношения порядка является отсутствие циклов. Если в графе транзитивного отношения есть цикл, отличный от петли в вершине, то отношение уже не может быть антисимметричным. Это поясняется следующим рисунком:



Допустим, есть цикл $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1$. По транзитивности для перехода за два шага $2 \rightarrow 3 \rightarrow 4$ должен быть и переход за один шаг $2 \rightarrow 4$. Виден переход за два шага $1 \rightarrow 2 \rightarrow 4$. Тогда должен быть переход за один шаг $1 \rightarrow 4$. Но это противоречит антисимметричности, так как переход $4 \rightarrow 1$ тоже есть.

Данный пример основывается на том, что если некоторое отношение α является транзитивным, то и любая степень α , и отношение достижимости $\hat{\alpha}$ целиком содержатся в самом α :

$$\alpha^2 \subseteq \alpha \Rightarrow \forall k \in \mathbb{N} \alpha^k \subseteq \alpha \Rightarrow \hat{\alpha} \subseteq \alpha$$

Для доказательства этого утверждения потребуется воспользоваться принципом индукции, так как степени определены рекуррентно:

База индукции: $\alpha^1 \subseteq \alpha$ (по определению $\alpha^1 = \alpha \Rightarrow \alpha^1 \subseteq \alpha$).

Индукционный переход: Предположим $\alpha^k \subseteq \alpha$. Покажем $\alpha^{k+1} \subseteq \alpha$.

Сначала покажем, что $p \subseteq q \Rightarrow \forall r (p \circ r \subseteq q \circ r)$:

$$(x, y) \in p \circ r \Rightarrow \exists z ((x, z) \in p \ \& \ (z, y) \in r) \Rightarrow \exists z ((x, z) \in q \ \& \ (z, y) \in r) \Rightarrow (x, y) \in q \circ r$$

Переход возможен, так как $p \subseteq q \Rightarrow ((x, z) \in p \Rightarrow (x, z) \in q)$.

Теперь, на основании доказанного, видим, что $\alpha^k \subseteq \alpha \Rightarrow \alpha^k \circ \alpha \subseteq \alpha \circ \alpha$.

Но $\alpha^k \circ \alpha = \alpha^{k+1}$ & $\alpha \circ \alpha = \alpha^2$ & $\alpha^2 \subseteq \alpha \Rightarrow \alpha^{k+1} \subseteq \alpha$.

Отношения прядка в определённом смысле похожи на отношение \leq между числами. Рассматриваемые далее свойства легче воспринять, если для отношений порядка использовать инфиксную запись. Обычно для этих целей используется символ \leqslant_α . Далее будем использовать его как синоним для $\alpha = \{ (x, y) \mid x \leqslant_\alpha y \}$.

Отношения порядка разделяются на два типа по следующему признаку. Назовём элементы x и y *сравнимыми* по α , если хотя бы одна пара, (x, y) или (y, x) присутствует в данном отношении α . Это новое бинарное отношение сравнимости обозначим инфиксным символом \leqslant_α :

$$x \leqslant_\alpha y \Leftrightarrow (x \leqslant_\alpha y) \vee (y \leqslant_\alpha x)$$

Иначе будем записывать

$$x \not\leqslant_\alpha y \Leftrightarrow \neg(x \leqslant_\alpha y) \Leftrightarrow \neg(x \leqslant_\alpha y) \ \& \ \neg(y \leqslant_\alpha x)$$

Такие элементы называют *несравнимыми* по α .

Отношения порядка α , где все элементы сравнимы, называют *линейным порядком* (на некотором множестве A).

$$\alpha \text{ – линейный порядок на } A \Leftrightarrow \forall x \in A \ \forall y \in A \ x \leqslant_\alpha y$$

Отношения порядка α , где существует хотя бы одна пара несравнимых элементов, называют *частичным порядком* (на некотором множестве A).

$$\alpha \text{ – частичный порядок на } A \Leftrightarrow \exists x \in A \ \exists y \in A \ x \not\leqslant_\alpha y$$

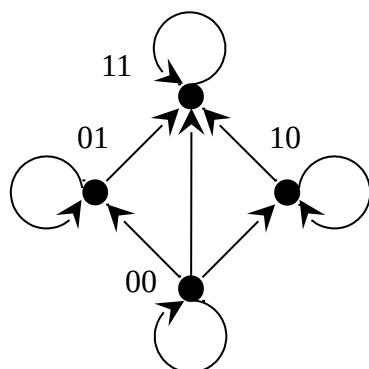
Приведём пример частичного порядка на $\alpha \subseteq A \times A$, $A = \mathcal{B} \times \mathcal{B}$. Рассмотрим отношение между парами двоичных символов (двоичными векторами размерности 2):

$$(x_1, x_2) \leqslant (y_1, y_2) \Leftrightarrow ((x_1 \rightarrow y_1) \ \& \ (x_2 \rightarrow y_2))$$

Всего есть 4 пары: 00, 01, 10, 11 (для удобства записи скобки вокруг пар опущены). Отношение установлено между следующими парами:

$$00 \leqslant 00, 00 \leqslant 01, 00 \leqslant 10, 00 \leqslant 11, 01 \leqslant 01, 01 \leqslant 11, 10 \leqslant 10, 10 \leqslant 11, 11 \leqslant 11.$$

Графическое представление этого отношения будет таким:



Здесь все определяющие свойства для отношения порядка выполняются. Но пары 01 и 10 не являются сравнимыми. Ни одна из них не упорядочена по отношению к другой.

Так же, как отношение эквивалентности однозначно определяется своим семейством классов эквивалентности (разбиением множества), так и для отношений порядка существует более простая форма представления, чем полное перечисление всех упорядоченных пар.

Назовем множество

$$[a, b]_{\alpha} = \{ x \mid a \leq_{\alpha} x \text{ \& } x \leq_{\alpha} b \}$$

отрезком (сегментом), выделяемым *границами* a и b по отношению α . Это определение аналогично тому, как на числовой прямой определяются отрезки (закрытые интервалы): $a \leq x \leq b$. Но теперь в качестве отношения α берётся произвольное отношение порядка (не обязательно линейного). Элементы отрезка $[a, b]_{\alpha}$ отличные от a и b называются *внутренними точками* отрезка. В примере пары 01 и 10 – внутренние точки отрезка $[00, 11]_{\leq}$.

Справедливы следующие свойства отрезков по отношениям порядка:

- 1) **Если границы упорядочены по рассматриваемому отношению, то отрезок не является пустым.**

$$a \leq_{\alpha} b \Rightarrow [a, b]_{\alpha} \neq \emptyset$$

Действительно, $a \leq_{\alpha} b \Rightarrow a \in [a, b]_{\alpha}$ так как $a \leq_{\alpha} a \text{ \& } a \leq_{\alpha} b \Rightarrow [a, b]_{\alpha} \neq \emptyset$. $a \leq_{\alpha} a$ следует из рефлексивности α .

Аналогично заметим, что и вторая граница тоже принадлежит отрезку:

$$a \leq_{\alpha} b \text{ \& } b \leq_{\alpha} b \Rightarrow b \in [a, b]_{\alpha}$$

Отсюда получаем следующее свойство:

- 2) **Если границы упорядочены по рассматриваемому отношению, то обе границы принадлежат отрезку.**

$$a \leq_{\alpha} b \Rightarrow a \in [a, b]_{\alpha} \text{ \& } b \in [a, b]_{\alpha}$$

Отрезок называется простым отрезком, если он содержит только свои границы (не имеет внутренних точек).

$$[a, b]_{\alpha} \text{ – простой отрезок } \Leftrightarrow [a, b]_{\alpha} = \{a, b\}$$

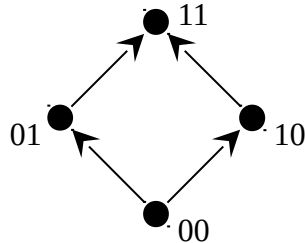
Петля тоже является простым отрезком (по рефлексивности и отсутствию циклов): $[a, a]_{\alpha} = \{a\}$.

Построим по отношению порядка новое отношение, отражающее свойство «быть концами простого отрезка» и исключим из него петли:

$$\tau_\alpha = \{ (a, b) \mid [a, b]_\alpha = \{a, b\} \} \setminus \Delta_A = \{ (a, b) \mid [a, b]_\alpha = \{a, b\} \ \& \ (a \neq b) \}$$

В примере для отношения \leq простыми отрезками, но не петлями будут $[00, 01]_\leq$, $[00, 10]_\leq$, $[01, 11]_\leq$, $[10, 11]_\leq$. Соответственно, $\tau_\leq = \{(00, 01), (00, 10), (01, 11), (10, 11)\}$.

Граф τ_\leq показан на рисунке.



Граф отношения «быть концами простого отрезка» (без петель) называют *диаграммой Хассе*. Это отношение однозначно определяет представляемое им отношение порядка. Упорядоченность по α представляет собой достижимость по τ_α . Для восстановления α по τ_α следует использовать формулу

$$\alpha = \hat{\tau}_\alpha \cup \Delta_A$$

Диаграмма Хассе также не должна иметь циклов, так как получаемое по ней отношение достижимости является транзитивным. Вообще всегда имеет место свойство $\forall \tau \ (\tau \subseteq A \times A \Rightarrow (\hat{\tau})^2 \subseteq \hat{\tau})$. То есть достижимость любого бинарного отношения транзитивна.

Диаграмма Хассе для отношения линейного порядка представляет собой цепь связей между разветвлений и слияний. Потому все отношения линейного порядка на конечных множествах подобны (для любого числа элементов есть только один класс линейного порядка).

Тема 7. МОДЕЛИ ТЕОРИИ ГРАФОВ. ОПРЕДЕЛЕНИЕ ПРОСТОГО ГРАФА. СПОСОБЫ ЗАДАНИЯ ПРОСТЫХ ГРАФОВ. ОТНОШЕНИЯ И МАТРИЦЫ СМЕЖНОСТИ И ИНЦИДЕНТНОСТИ. СТЕПЕНЬ ВЕРШИН ПРОСТОГО ГРАФА И ЕЁ СВОЙСТВА.

Рассматривавшиеся ранее графы, при помощи которых иллюстрировались функциональные связи и бинарные отношения являлись частным случаем более широкого класса дискретных структур, моделирующих не только бинарные отношения (и, соответственно, предикаты в математической логике), но в большей степени непосредственно (то есть без промежуточной модели логических высказываний) исследуемые объекты. Примерами таких объектов могут быть структуры данных в алгоритмах обработки информации, структурные схемы технических систем, анализ состояний объекта или системы во временной области, некоторые модели в математической лингвистике, транспортные или коммуникационные сети.

Рассматриваемый класс дискретных моделей, называемых графами, включает в себя такие понятия, как:

- *Ориентированный граф* – уже знакомое понятие: задаётся множеством *вершин* (для ориентированных графов их чаще называют *узлами*) и множеством упорядоченных пар вершин – *рёбер* (называемых в этом случае *дугами*).
- *Простой граф*. В данной модели существенным является указание наличия связи между двумя вершинами – симметричное бинарное отношение смежности вершин. Задаётся возможностью ответа на вопрос, «связаны данные (разные) вершины или нет?». Обычная форма задания – множество вершин и множество двухэлементных подмножеств вершин – множество *рёбер*. В данной модели не рассматривается возможность кратных связей между вершинами (связь либо есть, либо её нет) и связи вершины с собой: ребро всегда двухэлементное множество, потому в простом графе нет петель.
- *Граф с петлями*. Аналогично простому графу, но петли допускаются. Рёбра не только двухэлементные, но и одноэлементные. Можно рассматривать и как ориентированный граф, но с симметричным определяющим отношением.
- *Мультиграф*. Более широкая модель, чем простой граф, допускающая более одного ребра между разными вершинами. Для задания потребуется ввести отдельное множество рёбер (например, задав его списком именованных элементов, так как простое перечисление двухэлементных множеств вершин не отражает кратных связей) и *отношение инцидентности* – отношение между множеством вершин и множеством рёбер – для ответа на вопрос, какие вершины соединяет данное ребро. При этом каждое отдельное ребро всё равно соединяет ровно две вершины. Такое отношение может быть полезно и при рассмотрении простого графа, но с ограничением – каждая пара вершин соединяется не более чем одним ребром.
- *Гиперграф*. Аналогично простому графу, но связующие элементы между вершинами не обязательно двухэлементные множества – могут соединять сразу произвольное число вершин. Такие связующие элементы называют *гипердугами*.

Могут рассматриваться и другие модели (ориентированный мультиграф, мультиграф с петлями и т.д.). Общим и самым существенным здесь является наличие двух множеств – множества вершин (или узлов) и множества рёбер (или дуг). Обычно, но не обязательно, под термином *граф* имеют в виду простой граф.

Размеченный граф. В дополнение к отражению наличия связей, указываются функции, ставящие в соответствие вершинам и дугам значения из некоторого множества меток. Соответственно можно указать разметку вершин (узлов) и разметку рёбер (дуг).

Метки могут быть даже действительными числами, представляющими такие понятия, как расстояния между узлами или пропускную способность в транспортных сетях, вероятности изменения состояний объекта или затраты чего-либо (времени, материалов...) для осуществления некоторой операции. Имеется очень широкий круг задач, использующих данную модель. Особенно следует отметить задачи оптимизации, например поиск кратчайшего пути, планирование работ. Разметки символами используются в математической лингвистике.

Использование графов как модели является мощным средством исследования по следующим причинам:

- На этапе абстрагирования наглядная форма представления графа позволяет удобно построить такую модель – усмотреть, что в предметной области может быть вершинами, рёбрами (и, возможно, разметкой).
- На этапе работы с моделью преобразования опираются на методы дискретной математики, часто сводится к уже решённым задачам.
- На этапе практического применения могут применяться уже разработанные алгоритмы с незначительными изменениями и соответствующее представление обрабатываемой информации подходящими структурами данных.

Рассмотрим более подробно сначала простые графы (но многие результаты могут быть применимы и к другим моделям).

Простой граф – упорядоченная пара $\langle V, E \rangle$, где V – множество вершин, $E \subseteq \wp(V)$ – множество двухэлементных подмножеств V – множество рёбер (семейство двухэлементных множеств). Граф (упорядоченная пара) обозначается обычно как $G(V, E)$:

$$G(V, E) = \langle V, E \rangle \Leftrightarrow E \subseteq \wp(V) \ \& \ \forall e \in E \ |e|=2$$

Здесь $\wp(V)$ – множество всех подмножеств V , $\wp(V) = \{X \mid X \subseteq V\}$.

$|e|=2$ означает, что каждое ребро равномощно двухэлементному множеству. Можно также записать $e \sim \mathcal{B}$, $\mathcal{B} = \{0, 1\}$.

Множество вершин обычно обозначают буквой V – от английского термина для вершины – “vertex”. Множество ребер обычно обозначают буквой E – от английского термина для ребра – “edge”.

Пример простого графа.

$$V = \{a, b, c, d, e\}$$

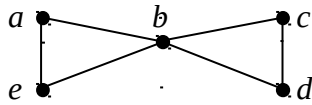
$$E = \{\{a, b\}, \{a, e\}, \{b, e\}, \{b, d\}, \{b, c\}, \{c, d\}\}$$

Можно подумать, что такое определение простого графа избыточно, так как вроде бы по заданному списку множеству E множество V можно восстановить как $V = \{x \mid \exists u \in E \ x \in u\}$. Но на самом деле к простым графам относят также случаи, когда имеются «изолированные» вершины, не инцидентные ни одному ребру. В таких графах $V \neq \{x \mid \exists u \in E \ x \in u\}$.

Как и ориентированные графы, простые графы (и все другие варианты графов) удобно изображать диаграммами. В этом основное преимущество данного класса моделей. Именно оно даёт им наглядность. Вершины на диаграммах изображают точками или кружками, рёбра – линиями между ними. Вершины подписывают символами их элементов в множестве E . В простом графе рёбрам, в отличие от вершин, названий обычно не дают – называют и обозначают их по названиям тех вершин, которые они

соединяют. В примере – ребро $\{a, b\}$, ребро $\{b, c\}$. Порядок названий вершин в обозначении ребра роли не играет. Можно ребро $\{a, b\}$ назвать и ребром $\{b, a\}$. Для размеченных графов рядом с объектами изображают значения функций разметки вершин и рёбер.

Для рассмотренного примера диаграмма может быть изображена следующим образом



Для простого графа на множестве вершин вводится бинарное отношение (в данном случае симметричное и *иррефлексивное*) смежности вершин.

$$\alpha_{G(V, E)} \subseteq V \times V$$

$$(x, y) \in \alpha_{G(V, E)} \Leftrightarrow \{x, y\} \in E$$

(Иррефлексивным называют отношение, по которому элементы не сопоставляются сами себе: $\forall x (x, x) \notin \alpha_{G(V, E)}$)

Две вершины называют смежными, если существует соединяющее их ребро.

Для ориентированного графа отношением смежности называют соответствующее ему бинарное отношение. Это представление уже рассматривалось при изучении бинарных отношений. Для ориентированных графов отношение смежности может не быть симметричным.

Матрица отношения смежности называется матрицей смежности.

$$G(V, E) = \langle V, E \rangle \Rightarrow (A - \text{матрица смежности } G(V, E) \Leftrightarrow A = C^{\alpha_{G(V, E)}}).$$

То есть, если множество V графа $G(V, E)$ занумеровано как $V = \{v_1, v_2, \dots, v_n\}$, то $A_{ij} = A_{ji} = 1$ ($\{v_i, v_j\} \in E$). Будем обозначать матрицу смежности символом A от английского названия “adjacency matrix”.

В простом графе матрица смежности симметричная и на диагонали стоят нули. Для представления графа $G(V, E)$ матрицей смежности необходимо задать нумерацию множества вершин. Так как это можно сделать числом способов, равным числу перестановок элементов множества V , у каждого графа есть $|V|!$ матриц смежности. Они отличаются только перестановкой строк и столбцов.

Для примера $V = \{a, b, c, d, e\}$ и $E = \{\{a, b\}, \{a, e\}, \{b, e\}, \{b, d\}, \{b, c\}, \{c, d\}\}$ зададим нумерацию вершин $v_1=a, v_2=b, v_3=c, v_4=d, v_5=e$. Тогда матрица смежности A будет

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Матрица смежности полностью определяет простой граф (и ориентированный граф) при заданной нумерации вершин (узлов).

Также как отношение подобия бинарных отношений \cong является отношением эквивалентности, выражающим свойство для ориентированных графов «иметь одинаковую форму без учёта обозначений элементов», аналогичное отношение вводят и для других типов графов. Такое отношение называют *изоморфизмом графов*, а сами эквивалентные графы называют *изоморфными*.

Два графа изоморфны тогда и только тогда, когда существует взаимнооднозначное соответствие между их множествами вершин, сохраняющее отношение смежности. Отношения смежности таких графов подобны.

$$\begin{aligned} G(V_1, E_1) \sim G(V_2, E_2) &\Leftrightarrow \alpha_{G(V_1, E_1)} \cong \alpha_{G(V_2, E_2)} \\ &\Leftrightarrow \exists f \in V_2^V, f^1 \in V_1^V, \& (\{x, y\} \in E_1 \Leftrightarrow \{f(x), f(y)\} \in E_2) \end{aligned}$$

Матрицы смежности изоморфных графов либо равны, либо отличаются только перестановкой строк и столбцов.

Изоморфизм графов является отношением эквивалентности (следует из аналогичного свойства для отношения подобия соответствующих отношений смежности).

Для простых графов отношение смежности (и, следовательно, сам граф) можно задать, перечислив для каждой вершины множества смежных с ней вершин.

Множество вершин, смежных с вершиной x в графе $G(V, E)$, обозначается

$$\Gamma_{G(V, E)}(x) = \{y \mid \{x, y\} \in E\}$$

Очевидно, $\Gamma_{G(V, E)}(x) \subseteq V$ и $\Gamma_{G(V, E)}(x) = [x]_{\alpha_{G(V, E)}}$ (в простом графе отношение смежности симметрично и $[x]_{\alpha_{G(V, E)}} = \{y \mid (x, y) \in \alpha_{G(V, E)}\} = \{y \mid (y, x) \in \alpha_{G(V, E)}\}$).

Если рассматривается определённый граф с уже оговоренными множествами V и E , индекс обозначения графа будем опускать. В примере $\Gamma(a) = \{b, e\}$, $\Gamma(b) = \{a, c, d, e\}$, $\Gamma(c) = \{b, d\}$, $\Gamma(d) = \{b, c\}$ и $\Gamma(e) = \{a, b\}$.

Если ребер в графе не очень много, но много вершин, то множества смежности $\{\Gamma_{G(V, E)}(x) \mid x \in V\}$ могут оказаться более компактной формой задания графа, чем матричная.

Простой граф $G(V, E)$ можно задать еще одним видом матрицы, называемой *матрицей инцидентности*. Для данного способа задания графа, в дополнение к нумерации вершин ($|V|!$ способов), необходимо ввести также нумерацию рёбер ($|E|!$ способов). **Элемент матрицы инцидентности в строке i и в столбце j равен 1, если вершина v_i инцидентна ребру e_j (ребро e_j соединяет вершину v_i с какой-либо еще вершиной), иначе этот элемент равен 0.** То есть, если $V = \{v_1, v_2, \dots, v_n\}$ и $E = \{e_1, e_2, \dots, e_m\}$, то матрица инцидентности \mathbf{I} будет иметь n строк и m столбцов, и её элементы заполняются по условию $\mathbf{I}_{ij} = (v_i \in e_j)$. Будем обозначать эту матрицу символом \mathbf{I} от английского названия “incidence matrix”.

В примере $G(V, E)$ графа с $V = \{a, b, c, d, e\}$ и $E = \{\{a, b\}, \{a, e\}, \{b, e\}, \{b, d\}, \{b, c\}, \{c, d\}\}$ в дополнение к нумерации вершин $v_1=a, v_2=b, v_3=c, v_4=d, v_5=e$ зададим нумерацию рёбер $e_1=\{a, b\}, e_2=\{a, e\}, e_3=\{b, e\}, e_4=\{b, d\}, e_5=\{b, c\}, e_6=\{c, d\}$. Тогда матрица инцидентности будет

$$\mathbf{I} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Соответственно, для графа $G(V, E)$ отношение инцидентности $\beta_{G(V, E)} \subseteq V \times E$ это бинарное отношение между множеством вершин V и множеством рёбер E .

$$\beta_{G(V, E)} = \{(x, y) \mid x \in V \ \& \ y \in E \ \& \ x \in y\}$$

Выражение $(x, y) \in \beta_{G(V, E)}$ читается «вершина x инцидентна ребру y ». Можно сказать и наоборот, «ребро y инцидентно вершине x ». Эта фраза представляет обратное для $\beta_{G(V, E)}$ отношение между рёбрами и вершинами $\beta_{G(V, E)}^{-1}$.

В примере $\beta = \{(a, \{a, b\}), (a, \{a, e\}), (b, \{a, b\}), (b, \{b, c\}), (b, \{b, d\}), (b, \{b, e\}), (c, \{b, c\}), (c, \{c, d\}), (d, \{b, d\}), (d, \{c, d\}), (e, \{a, e\}), (e, \{b, e\})\}$, что, с учётом введённой нумерации будет $\{(1, 1), (1, 2), (2, 1), (2, 3), (2, 4), (2, 5), (3, 5), (3, 6), (4, 4), (4, 6), (5, 2), (5, 3)\}$. Здесь парой (i, j) обозначено наличие пары (v_i, e_j) в отношении инцидентности. Это в точности те индексы матрицы инцидентности, для которых элементы матрицы равны 1.

Матрица инцидентности I графа $G(V, E)$ это матрица данного бинарного отношения $I = C^{\beta_{G(V, E)}}$.

Простой граф однозначно определяется своей матрицей инцидентности (при заданной нумерации вершин и рёбер).

Можно даже простой граф задать ориентированным графом его отношения инцидентности.

В графе $G(V, E)$ с каждой вершиной x можно связать множество инцидентных ей рёбер $I_{G(V, E)}(x) = \{y \mid y \in E \ \& \ x \in y\} = \{y \mid (x, y) \in \beta_{G(V, E)}\}$, в примере:

$$I(a) = \{\{a, b\}, \{a, e\}\},$$

$$I(b) = \{\{a, b\}, \{b, c\}, \{b, d\}, \{b, e\}\},$$

$$I(c) = \{\{b, c\}, \{c, d\}\},$$

$$I(d) = \{\{b, d\}, \{c, d\}\},$$

$$I(e) = \{\{a, e\}, \{b, e\}\}.$$

Семейство таких множеств $\{I(x) \mid x \in V\}$ тоже однозначно определяет простой граф. Заметьте, что в отличие от $\Gamma_{G(V, E)}(x) \subseteq V$, $I_{G(V, E)}(x) \subseteq E$.

Таким образом, простые графы допускают большое разнообразие форм представления, эквивалентных в том смысле, что они определяют один и тот же граф, но имеющих определённые преимущества или недостатки, в зависимости от цели решаемой задачи.

Итог по основным способам задания простого графа.

- 1) Множество вершин и рёбер в виде списка неупорядоченных пар (двухэлементных множеств).
- 2) Множество вершин и семейство множеств смежных вершин для каждой вершины.
- 3) Нумерованное множество вершин и матрица смежности.
- 4) Нумерованное множество вершин, матрица инцидентности и нумерация рёбер.
- 5) Множество вершин и семейство множеств инцидентных рёбер для каждой вершины.

Так как в простом графе каждое ребро соединяет некоторую вершину со смежными (но не равными ей) вершинами, множества $I_{G(V, E)}(x)$ и $\Gamma_{G(V, E)}(x)$ должны быть равномощными:

$$\forall x \in V |I_{G(V,E)}(x)| = |\Gamma_{G(V,E)}(x)|$$

Количество рёбер, инцидентных некоторой вершине v , называют *степенью вершины* и обозначают $\deg(v)$ (обозначение происходит от английского термина “degree”, его часто сокращают до обозначения $d(v)$).

$$\deg(v) = |I(v)|$$

В простом графе степень вершины также равна числу смежных с ней вершин:

$$\deg(v) = |I(v)| = |\Gamma(v)|.$$

Степень вершины равна сумме числа элементов строки матрицы инцидентности, соответствующей данной вершине.

$$\deg(v_i) = \sum_{j: I_{ij} = 1} 1$$

Хотя формально элементы матрицы I являются логическими значениями, их также можно рассматривать как целые числа и написать $\deg(v_i) = \sum_j I_{ij}$.

Сумма степеней вершин простого графа равна удвоенному числу рёбер (и поэтому всегда чётная):

$$\sum_{v \in V} \deg(v) = 2 \cdot |E|,$$

$$\sum_{v \in V} \deg(v) \text{ чётно.}$$

Это объясняется тем, что каждому ребру в простом графе инцидентны ровно две вершины. Сумма степеней вершин это сумма всех элементов матрицы инцидентности ($\sum_{v \in V} \deg(v) = \sum_i \sum_j I_{ij}$). То, что каждому ребру инцидентны ровно две вершины, в терминах матрицы инцидентности означает, что в каждом столбце имеются ровно две единицы.

Отсюда следует также, что **число вершин нечётной степени чётно.**

Вершину степени 0 называют *изолированной*, вершину степени 1 – *висячей*.

Тема 8. МАРШРУТЫ И ЦИКЛЫ В ПРОСТОМ ГРАФЕ.
ОТНОШЕНИЕ СВЯЗНОСТИ И КОМПОНЕНТЫ СВЯЗНОСТИ.

Рассмотрим далее понятия, необходимые для анализа некоторых полезных свойств графов.

Для графов различных видов обычно определяют **маршрут** как **последовательность чередующихся вершин и рёбер**

$$v_0, e_1, v_1, e_2, v_2, e_3, \dots, e_k, v_k,$$

где $v_i \in V$ & $e_i \in E$ и соседние элементы последовательности инцидентны:

$$(v_i, e_{i+1}) \in \beta \text{ \& } (e_i, v_i) \in \beta^{-1}.$$

Такое представление полезно для мультиграфов, когда вершины могут соединяться более чем одним ребром (названия e_i указывают, по какому именно ребру проходит маршрут). Для простых графов такое представление избыточно. Достаточно указать только последовательность вершин. Вершины при этом должны быть смежными:

S – маршрут длины k в простом графе $G(V, E) \Leftrightarrow$

$$S = (v_0, v_1, v_2, \dots, v_k) \text{ \& } \forall i (0 \leq i < k \rightarrow \{v_i, v_{i+1}\} \in E) \text{ \& } v_k \in V$$

При этом $e_{i+1} = \{v_i, v_{i+1}\} \in E$ называют ребром маршрута S . Элементы последовательности обычно нумеруют от числа 0, так чтобы номер последнего элемента совпадал с количеством рёбер в маршруте. Это число называют *длиной маршрута*.

Последовательность только из одной вершины называется маршрутом нулевой длины.

Маршрут в простом графе можно представить как функцию $f(i) = v_i$ из множества номеров элементов последовательности вершин в множество вершин, на которую наложено ограничение $(f(i), f(i+1)) \in \alpha$ – отношению смежности графа.

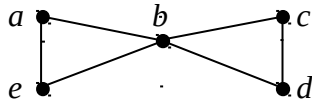
Нумерацию элементов последовательности $S = (v_0, v_1, v_2, \dots, v_k)$ следует отличать от нумерации элементов конечного множества $A = \{a_1, a_2, \dots, a_k\}$. При нумерации множества задаётся взаимнооднозначное соответствие номеров (индексов) и элементов. В этом случае можно также говорить и о последовательности элементов множества (a_1, a_2, \dots, a_k) – упорядоченного набора или вектора. Обратное не верно. Функция, задающая последовательность S , не обязательно инъективна – в ней могут быть повторения. При рассмотрении графов повторения означают, что маршрут несколько раз проходит через некоторую вершину.

Если в маршруте нет повторяющихся вершин (то есть S инъективна), то маршрут называют *простым маршрутом*.

Маршрут ненулевой длины, соединяющий вершину саму с собой ($v_0 = v_k$) и не содержащий повторяющихся ребер называется *циклом*.

Цикл без повторяющихся вершин, кроме начальной и одновременно конечной вершины ($v_0 = v_k$) называется *простым циклом*.

Рассмотрим тот же пример, на котором иллюстрировались способы задания графа (приведём как напоминание только диаграмму):



Здесь маршрут $abcdbe$ не является простым маршрутом, так как два раза проходит через вершину b .

Маршрут abc является простым маршрутом.

Последовательность cde вообще не является маршрутом (вершины d и e не смежные).

Последовательность $abcdbea$ является циклом, но не является простым циклом (есть повторение b , отличное от начальной и конечной вершины a).

Цикл $bcdbeab$ также не будет простым циклом. Здесь вершина b повторяется не только в начале и в конце, но и в середине маршрута.

Цикл $abea$ будет простым циклом.

Маршрут aba не будет циклом, так как, несмотря на то, что единственное повторение здесь это начало и конец маршрута, в маршруте имеется повтор рёбер (ребро $\{a, b\}$ присутствует дважды: $e_1=e_2=\{a, b\}$).

Маршрут a циклом не является – имеет нулевую длину.

Две вершины в простом графе $G(V, E)$ x и y называются связанными, если между ними существует маршрут $S=(v_0, v_1, v_2, \dots, v_k)$, такой, что $v_0=x$ & $v_k=y$.

Отношение связности вершин $\sigma \subseteq E \times E$ является бинарным отношением на множестве вершин простого графа. Его можно вычислить, объединив все степени отношения смежности и дополнив его до рефлексивного отношения:

$\sigma = \hat{\alpha} \cup \Delta_V$, где $\alpha = \{(x, y) \mid \{x, y\} \in E\}$ – отношение смежности, $\hat{\alpha} = \bigcup_i \alpha^i$ – отношение достижимости по α – объединение степеней.

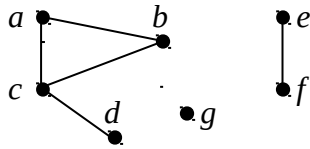
Добавление Δ_V необходимо, чтобы учесть пути нулевой длины. Ранее мы рассматривали только натуральные степени для бинарных отношений. Чтобы записывать формулу вида $\sigma = \hat{\alpha} \cup \Delta_V$, где $\hat{\alpha} = \bigcup_i \alpha^i$, более компактно, иногда определяют и нулевую степень отношения как диагональное отношение (в данном случае можно написать $\alpha^0 = \Delta_V$). В таком случае считают, что $\Delta_V \subseteq \hat{\alpha}$ и $\sigma = \hat{\alpha} = \Delta_V \cup \alpha^1 \cup \alpha^2 \cup \alpha^3 \cup \dots$.

Отношение связности вершин является отношением эквивалентности. Действительно, $\sigma = \hat{\alpha} \cup \Delta_V \Rightarrow \Delta_V \subseteq \sigma \Rightarrow \sigma$ рефлексивно. $\alpha = \alpha^{-1}$ & $\Delta_V = (\Delta_V)^{-1} \Rightarrow \forall i (\alpha^i)^{-1} = \alpha^i \Rightarrow \sigma^{-1} = \sigma \Rightarrow \sigma$ симметрично. $(\hat{\alpha} \cup \Delta_V)^2 \subseteq \hat{\alpha} \cup \Delta_V \Rightarrow \sigma^2 \subseteq \sigma \Rightarrow \sigma$ транзитивно.

Классы эквивалентности по отношению связности вершин называют компонентами связности графа.

В пределах такого класса $[x]_\sigma = \{y \mid (x, y) \in \sigma\}$ между всеми вершинами существуют маршруты. Между вершинами разных классов маршрутов нет.

Следующая диаграмма дает пример графа с тремя компонентами связности $V/\sigma = \{\{a, b, c, d\}, \{e, f\}, \{g\}\}$.



Каждый класс эквивалентности (компонент связности) может рассматриваться в качестве отдельного графа. Поэтому часто при рассмотрении графов рассматривают только *связные* графы. **Граф называют связным, если для каждой пары вершин существует маршрут между ними** ($\forall x \in V \forall y \in V (x, y) \in \sigma$). В этом случае отношение связности – полное отношение $\sigma = V \times V$.

Выделить компонент связности из несвязного графа в отдельный граф можно, если в качестве множества вершин взять выделяющий класс эквивалентности, а множества рёбер – множество рёбер, инцидентных выбранным вершинам: $G([x]_\sigma, \bigcup_{y \in [x]_\sigma} I(y))$.

Тема 9. РАЗМЕЧЕННЫЕ ГРАФЫ. ВЕС РЁБЕР И ВЕС МАРШРУТА. ТРЕБОВАНИЯ. ЗАДАЧА ПОИСКА КРАТЧАЙШЕГО МАРШРУТА. АЛГОРИТМ ФЛОЙДА-УОРШАЛЛА.

Вычисление отношения связности позволяет ответить на вопрос, существует ли хотя бы один маршрут из одной вершины в другую, но в процессе вычисления по формуле $\sigma = \hat{\alpha} \cup \Delta_v$ сами маршруты (последовательности вершин) не вычисляются. Большой интерес вызывает вопрос: как именно выглядит маршрут. Более того, если существует несколько маршрутов, то желательно среди них выбрать (или сразу найти) в определённом смысле «лучший», например, самый короткий по длине, или, если у графа есть разметки, оптимизирующей некоторую функцию от значений разметок элементов маршрута (вершин и рёбер).

Обычно рассматривается граф, в котором рёбра размечены численными значениями, называемыми *весами* рёбер и рассматривается задача отыскания *кратчайшего маршрута* – маршрута, обладающего минимальным весом. **Весом маршрута называется сумма весов рёбер, входящих в маршрут.**

Тип численных значений не столь важен. Пусть a и b некоторые такие значения. Тогда $a \leq b$ означает линейную упорядоченность значений (чтобы любые значения можно было сравнивать). $\min(a, b)$ означает минимальное в смысле указанной упорядоченности значение:

$$\min(a, b) = \begin{cases} a & \text{если } a \leq b \\ b & \text{если } b \leq a \end{cases}$$

Для значений определена коммутативная и ассоциативная операция суммирования $a+b$, причём $a \leq a+b$. Это означает, что при суммировании значений сумма не уменьшается.

Это требование важно, если в графе возможны маршруты, многократно проходящие по одному ребру. Если бы требование не выполнялось, вес маршрута можно было бы сделать сколь угодно малым.

Указанному требованию удовлетворяют, например, неотрицательные действительные или целые числа с обычной операцией сложения.

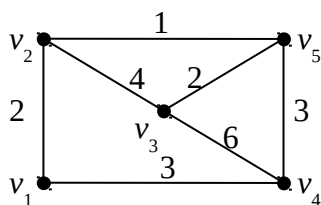
Для поиска кратчайшего пути веса рёбер обычно сводят в матрицу, похожую на матрицу смежности и в определённом смысле заменяющую её – матрица весов рёбер тоже однозначно определяет граф с разметкой рёбер, если в дополнение к значениям-весам ввести дополнительное значение, обозначающее отсутствие ребра. Это значение обычно обозначается символом ∞ и рассматривается как наибольшее возможное значение: $a \leq \infty$ & $a + \infty = \infty$. Также будем считать, что значение, обозначенное символом 0, является наименьшим возможным значением: $0 \leq a$ & $a + 0 = a$.

Матрица весов рёбер \mathbf{W} определяется следующим образом

$$\mathbf{W}_{ij} = \begin{cases} 0 & \text{если } i = j \\ w(\{v_i, v_j\}) & \text{если } \{v_i, v_j\} \in E \\ \infty & \text{если } \{v_i, v_j\} \notin E \end{cases}$$

Здесь $w(\{v_i, v_j\})$ – значение функции разметки рёбер (веса) для ребра $\{v_i, v_j\}$. Множество вершин занумеровано: $V = \{v_1, v_2, \dots, v_n\}$.

Например, показанный на диаграмме граф с разметкой рёбер и нумерацией вершин может быть представлен следующей матрицей весов рёбер. Для сравнения рядом показана матрица смежности этого графа.



$$\mathbf{W} = \begin{bmatrix} 0 & 2 & \infty & 3 & \infty \\ 2 & 0 & 4 & \infty & 1 \\ \infty & 4 & 0 & 6 & 2 \\ 3 & \infty & 6 & 0 & 3 \\ \infty & 1 & 2 & 3 & 0 \end{bmatrix} \quad \mathbf{A} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Аналогично можно представлять и ориентированные графы с разметкой весов дуг. При этом матрица весов может оказаться несимметричной. Для возрастающих в суммировании весов петли всё равно можно опустить, так как прокладывание маршрута через петлю или цикл может только увеличить его вес.

Конечный результат поиска маршрутов минимальных весов представим в виде двух матриц (**L**, **P**):

- Матрица минимальных весов маршрутов **L** организована аналогично матрице весов рёбер: её элементы L_{ij} представляют собой минимальный вес маршрута из вершины v_i в вершину v_j .
- Матрица маршрутов **P**. Вместо того, чтобы представить результат списком маршрутов, используем для них представление, основанное на следующем принципе: если $s_0s_1s_2\dots s_k$ – маршрут минимального веса из k рёбер из вершины $s_0=v_i$ в вершину $s_k=v_j$, то $s_1s_2\dots s_k$ – маршрут минимального веса из $k-1$ рёбер из вершины s_1 в вершину s_k . Это следует из свойств операции суммирования весов. Поэтому, имея в качестве элементов матрицы **P** следующие значения

$$\mathbf{P}_{ij} = \begin{cases} k & \text{если } s_1s_2\dots s_m \text{ - кратчайший маршрут из } v_i \text{ в } v_j \text{ и } s_2 = v_k \\ 0 & \text{если нет маршрута из } v_i \text{ в } v_j \end{cases}$$

можно найти и сами кратчайшие маршруты для любой пары вершин (v_i, v_j) , или установить, что вершины не связаны. Для этого надо отследить маршрут по матрице **P** следующим образом:

$$s_0=v_i, k_1=\mathbf{P}_{ij}, s_1=v_{k_1}, k_2=\mathbf{P}_{k_1j}, s_2=v_{k_2}, k_3=\mathbf{P}_{k_2j}, s_3=v_{k_3} \dots s_m=v_{k_m}=v_j$$

Построение маршрута $s_0s_1\dots s_m$ заканчивается, когда на очередном шаге извлечения маршрута из матрицы **P** в столбце j встречается сам номер j конечной вершины. Если вершины не связаны, уже на первом шаге будет обнаружено $\mathbf{P}_{ij}=0$.

Алгоритм построения матриц **L** и **P** опишем пошагово. Каждый шаг означает исследование в графе маршрутов с длиной, равной номеру шага.

На первом шаге положим $\mathbf{L}^{(0)} = \mathbf{W}$ и $\mathbf{P}_{ij}^{(0)} = \begin{cases} j & \text{если } \mathbf{W}_{ij} \neq \infty \\ 0 & \text{если } \mathbf{W}_{ij} = \infty \end{cases}$.

Это показывает, что при условии, что маршруты имеют длину не более чем 1, веса таких маршрутов есть элементы матрицы весов рёбер. Такие маршруты есть только между связанными вершинами.

Имея $\mathbf{L}^{(0)}$ и $\mathbf{P}^{(0)}$ найдём $\mathbf{L}^{(1)}$ и $\mathbf{P}^{(1)}$ – веса кратчайших маршрутов и сами маршруты, при условии, что длина маршрутов не более чем 2, а промежуточной вершиной является вершина v_1 . Выберем, что лучше: связывающее ребро $\{v_i, v_j\}$ или маршрут $v_i v_1 v_j$. В последнем случае отметим, что первой промежуточной вершиной будет v_1 . Для данного шага можно было бы написать и $\mathbf{P}_{ij}^{(1)} = 1$ при выборе маршрута $v_i v_1 v_j$, но для последующих шагов такая форма записи удобнее. Сравнения и суммирование проводят с учётом специальных значений 0 и ∞ .

$$\mathbf{L}_{ij}^{(1)} = \min(\mathbf{L}_{ij}^{(0)}, \mathbf{L}_{i1}^{(0)} + \mathbf{L}_{1j}^{(0)})$$

$$\mathbf{P}_{ij}^{(1)} = \begin{cases} \mathbf{P}_{ij}^{(0)} & \text{если } \mathbf{L}_{ij}^{(0)} \leq \mathbf{L}_{i1}^{(0)} + \mathbf{L}_{1j}^{(0)} \\ \mathbf{P}_{i1}^{(0)} & \text{если } \mathbf{L}_{ij}^{(0)} > \mathbf{L}_{i1}^{(0)} + \mathbf{L}_{1j}^{(0)} \end{cases}$$

В примере получаем (изменённые элементы отмечены квадратными скобками)

$$\mathbf{L}^{(0)} = \begin{bmatrix} 0 & 2 & \infty & 3 & \infty \\ 2 & 0 & 4 & \infty & 1 \\ \infty & 4 & 0 & 6 & 2 \\ 3 & \infty & 6 & 0 & 3 \\ \infty & 1 & 2 & 3 & 0 \end{bmatrix} \quad \mathbf{P}^{(0)} = \begin{bmatrix} 1 & 2 & 0 & 4 & 0 \\ 1 & 2 & 3 & 0 & 5 \\ 0 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 4 & 5 \\ 0 & 2 & 3 & 4 & 5 \end{bmatrix}$$

$$\mathbf{L}^{(1)} = \begin{bmatrix} 0 & 2 & \infty & 3 & \infty \\ 2 & 0 & 4 & [5] & 1 \\ \infty & 4 & 0 & 6 & 2 \\ 3 & [5] & 6 & 0 & 3 \\ \infty & 1 & 2 & 3 & 0 \end{bmatrix} \quad \mathbf{P}^{(1)} = \begin{bmatrix} 1 & 2 & 0 & 4 & 0 \\ 1 & 2 & 3 & [1] & 5 \\ 0 & 2 & 3 & 4 & 5 \\ 1 & [1] & 3 & 4 & 5 \\ 0 & 2 & 3 & 4 & 5 \end{bmatrix}$$

Это единственные места, где выполнено условие $\mathbf{L}_{ij}^{(0)} > \mathbf{L}_{i1}^{(0)} + \mathbf{L}_{1j}^{(0)}$.

Вообще для последующих шагов получаем рекуррентную формулу

$$\mathbf{L}_{ij}^{(k)} = \min(\mathbf{L}_{ij}^{(k-1)}, \mathbf{L}_{ik}^{(k-1)} + \mathbf{L}_{kj}^{(k-1)})$$

$$\mathbf{P}_{ij}^{(k)} = \begin{cases} \mathbf{P}_{ij}^{(k-1)} & \text{если } \mathbf{L}_{ij}^{(k-1)} \leq \mathbf{L}_{ik}^{(k-1)} + \mathbf{L}_{kj}^{(k-1)} \\ \mathbf{P}_{ik}^{(k-1)} & \text{если } \mathbf{L}_{ij}^{(k-1)} > \mathbf{L}_{ik}^{(k-1)} + \mathbf{L}_{kj}^{(k-1)} \end{cases}$$

Продолжая пример, получим

$$\mathbf{L}^{(2)} = \begin{bmatrix} 0 & 2 & [6] & 3 & [3] \\ 2 & 0 & 4 & 5 & 1 \\ [6] & 4 & 0 & 6 & 2 \\ 3 & 5 & 6 & 0 & 3 \\ [3] & 1 & 2 & 3 & 0 \end{bmatrix} \quad \mathbf{P}^{(2)} = \begin{bmatrix} 1 & 2 & [2] & 4 & [2] \\ 1 & 2 & 3 & 1 & 5 \\ [2] & 2 & 3 & 4 & 5 \\ 1 & 1 & 3 & 4 & 5 \\ [2] & 2 & 3 & 4 & 5 \end{bmatrix}$$

На шагах 3 и 4 изменений в матрицах не будет.

$$\mathbf{L}^{(3)} = \mathbf{L}^{(4)} = \begin{bmatrix} 0 & 2 & 6 & 3 & 3 \\ 2 & 0 & 4 & 5 & 1 \\ 6 & 4 & 0 & 6 & 2 \\ 3 & 5 & 6 & 0 & 3 \\ 3 & 1 & 2 & 3 & 0 \end{bmatrix} \quad \mathbf{P}^{(3)} = \mathbf{P}^{(4)} = \begin{bmatrix} 1 & 2 & 2 & 4 & 2 \\ 1 & 2 & 3 & 1 & 5 \\ 2 & 2 & 3 & 4 & 5 \\ 1 & 1 & 3 & 4 & 5 \\ 2 & 2 & 3 & 4 & 5 \end{bmatrix}$$

Последним будет шаг 5. При этом в матрице будут изменения. Особо заметим $\mathbf{L}_{13}^{(4)} > \mathbf{L}_{15}^{(4)} + \mathbf{L}_{53}^{(4)} \Rightarrow \mathbf{P}_{13}^{(5)} = \mathbf{P}_{15}^{(4)} = 2$.

$$\mathbf{L}^{(5)} = \begin{bmatrix} 0 & 2 & [5] & 3 & 3 \\ 2 & 0 & [3] & [4] & 1 \\ [5] & [3] & 0 & [5] & 2 \\ 3 & [4] & [5] & 0 & 3 \\ 3 & 1 & 2 & 3 & 0 \end{bmatrix} \quad \mathbf{P}^{(5)} = \begin{bmatrix} 1 & 2 & [2] & 4 & 2 \\ 1 & 2 & [5] & [5] & 5 \\ [5] & [5] & 3 & [5] & 5 \\ 1 & [5] & [5] & 4 & 5 \\ 2 & 2 & 3 & 4 & 5 \end{bmatrix}$$

Это был последний шаг, так как число шагов совпадает с числом узлов. Окончательно получаем:

$$\mathbf{L} = \begin{bmatrix} 0 & 2 & 5 & 3 & 3 \\ 2 & 0 & 3 & 5 & 1 \\ 5 & 3 & 0 & 5 & 2 \\ 3 & 5 & 5 & 0 & 3 \\ 3 & 1 & 2 & 3 & 0 \end{bmatrix} \quad \mathbf{P} = \begin{bmatrix} 1 & 2 & 2 & 4 & 2 \\ 1 & 2 & 5 & 5 & 5 \\ 5 & 5 & 3 & 5 & 5 \\ 1 & 5 & 5 & 4 & 5 \\ 2 & 2 & 3 & 4 & 5 \end{bmatrix}$$

Посмотрим, как извлечь из матрицы \mathbf{P} маршрут из v_1 в v_3 . Вес этого маршрута будет $\mathbf{L}_{13}=5$. Сам маршрут строится так:

$$s_0=v_1, k_1=\mathbf{P}_{13}=2, s_1=v_2, k_2=\mathbf{P}_{23}=5, s_2=v_5, k_3=\mathbf{P}_{53}=3, s_3=v_3$$

Получаем маршрут $v_1v_2v_5v_3$.

Данный алгоритм поиска кратчайшего пути известен как *алгоритм Флойда-Уоршалла*. То, что алгоритм действительно решает данную задачу, можно пояснить так. На каждом шаге вычисляется частичный результат, в предположении об определённом максимальном числе промежуточных вершин (но на каждом шаге все вершины рассматриваются как варианты начал и концов маршрутов). При этом и максимальная длина маршрута соответствует числу вершин. На каждом шаге происходит уточнение решения, допуская очередную вершину в качестве промежуточной вершины на маршруте (во все возможные позиции всех маршрутов, ведь в качестве начальных и конечных вершин всегда перебираются все вершины), но и максимальная длина маршрутов увеличивается на 1. Так как кратчайший путь при принятых ограничениях на свойства суммирования весов не может содержать циклов (повторяющихся вершин на маршруте),

задача будет решена правильно – максимальная длина кратчайшего маршрута не более числа вершин графа.

Тема 10. ПЛАНАРНЫЕ ГРАФЫ. ГРАНИ. ФОРМУЛА ЭЙЛЕРА. ПОЛНЫЙ ГРАФ. ДВУДОЛЬНЫЙ ГРАФ. ПОЛНЫЙ ДВУДОЛЬНЫЙ ГРАФ. НЕОБХОДИМЫЕ И ДОСТАТОЧНЫЕ УСЛОВИЯ ПЛАНАРНОСТИ.

Рассмотрим теперь вопрос, связанный с интерпретацией графов как диаграмм на плоскости. С иллюстративной точки зрения неважно, как именно на плоскости рисунка расположены вершины и рёбра – в линию, по окружности, хаотично. Лишь бы они отражали отношение смежности.

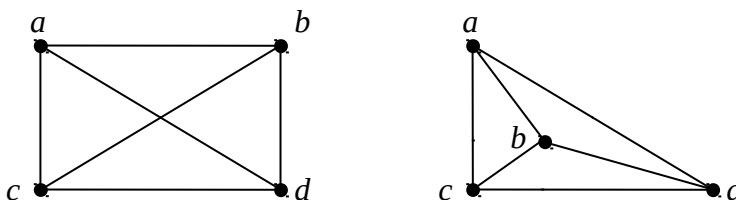
Но есть задачи, где само расположение узлов и рёбер имеет принципиальное значение: электрические схемы, инженерные коммуникации и т.п. Здесь мы кратко рассмотрим только возможность изобразить граф на плоскости без пересечений рёбер.

Граф, который может быть изображен на плоскости без пересечений рёбер, называется планарным графом.

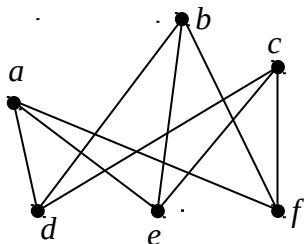
Например, граф

$$G(\{a, b, c, d\}, \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\})$$

можно изобразить и с пересечением и без пересечений рёбер, поэтому этот граф является планарным.

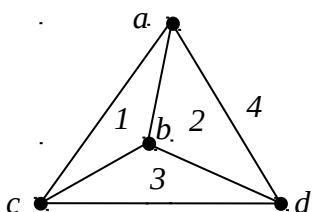


А вот граф, представленный следующей диаграммой, планарным не является.



Для того, чтобы выяснить, при каких условиях граф является планарным, потребуется ввести еще несколько понятий.

Если граф планарный и изображен на плоскости без пересечений рёбер, то диаграмма для графа разделяет плоскость на части, называемые *гранями*. **Грань – максимальный участок плоскости, в котором две точки могут быть соединены линией (любой формы), не пересекающей ребро графа.**



На рисунке три грани изображены треугольниками: $1 - abc$, $2 - abd$, $3 - bcd$. Греть 4 представляет собой внешнюю область плоскости.

Каждая грань соответствует циклическому маршруту в графе.

В примере грани 2 соответствует цикл $abda$.

Если связный граф является планарным и изображен на плоскости без пересечений рёбер, то число граней может быть найдено по известному числу вершин и рёбер. Формула, выражающая число граней через число вершин и рёбер известна как *формула Эйлера*. Она справедлива также и для мультиграфов и для графов с петлями.

Обозначим

число вершин – символом v ,

число рёбер – символом e ,

число граней – символом f (от англ. “face”)

Формула Эйлера: $v - e + f = 2$

Интересно отметить, что эта формула может быть доказана по индукции по числу рёбер графа.

База индукции:

Связный граф без рёбер представляет единственную вершину степени 0. Есть только одна грань – вся плоскость: $v=1, e=0, f=1 \Rightarrow v - e + f = 2$.

Индукционное предположение: $v - e + f = 2$ для некоторого графа с e рёбрами.

Индукционный переход:

Добавим к графу ребро. Есть два способа:

- 1) Добавляемое ребро инцидентно одной вершине исходного графа и новой добавленной вершине. Такое добавление не образует цикла и не меняет числа граней. Соотношение сохраняется. $v'=v+1, e'=e+1, f'=f \Rightarrow v' - e' + f' = 2$.
- 2) Добавляемое ребро инцидентно двум вершинам исходного графа (или, возможно, петля в графе с петлями). Число вершин не меняется: $v'=v, e'=e+1$. При этом обязательно образуется цикл и грань: $f'=f+1 \Rightarrow v' - e' + f' = 2$. (В графе с петлями петля тоже грань).

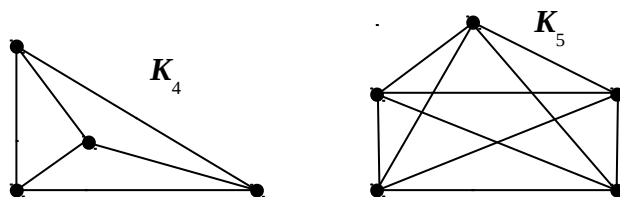
Граф называется *полным*, если все его вершины попарно смежные.

Так как в простом графе все ребра двухэлементные (нет петель) это можно записать так:

$$E = \{ \{x, y\} \mid x \in V \text{ \& } y \in V \} \setminus \{ \{x\} \mid x \in V \}$$

Полный граф с n вершинами (точнее класс графов, изоморфных такому графу) обозначается обычно K_n .

Примеры



Заметьте, что граф K_4 является планарным, а граф K_5 – нет.

Граф называется **двудольным**, если его множество вершин можно представить в виде объединения двух непересекающихся множеств и при этом никакие две вершины одного множества не являются смежными.

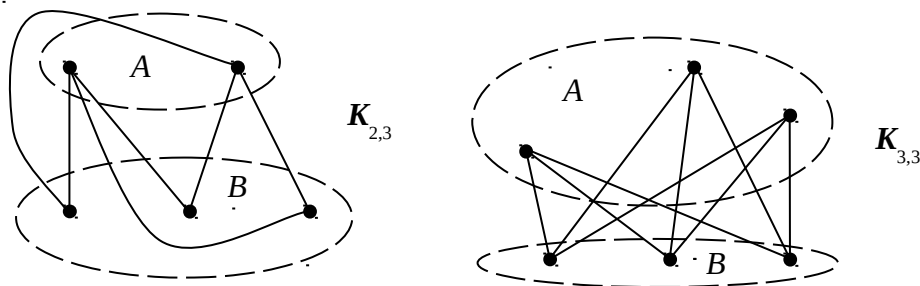
$$V=A \cup B \ \& \ A \cap B = \emptyset \ \& \ (x \in A \ \& \ y \in A \Rightarrow \{x, y\} \notin E) \ \& \ (x \in B \ \& \ y \in B \Rightarrow \{x, y\} \notin E)$$

Двудольный граф называется **полным двудольным**, если любые два элемента разных множеств (*долей*) являются смежными.

$$\forall x \in A \ \forall y \in B \ \{x, y\} \in E$$

Если $|A|=m$ и $|B|=n$ то полный двудольный граф (класс эквивалентности по изоморфизму) обозначается $K_{m,n}$.

Примеры.



Граф $K_{2,3}$ является планарным, а граф $K_{3,3}$ не является.

Теперь рассмотрим следующие утверждения:

В простом планарном графе каждая грань ограничивается, по крайней мере, тремя рёбрами.

Каждое ребро ограничивает не более двух граней.

НЕОБХОДИМОЕ УСЛОВИЕ ПЛАНАРНОСТИ.

Комбинируя их ($3f \leq 2e$) с формулой Эйлера ($v - e + f = 2$), получаем, что **в простом связном планарном графе с более, чем тремя вершинами ($v > 3$) не более $3v - 6$ рёбер.**

$$e \leq 3v - 6$$

Данное условие планарности простого графа связывает только число вершин и рёбер. Используя его можно доказать непланарность графов K_5 и $K_{3,3}$. С его помощью можно доказывать непланарность и других графов.

$$\neg(e \leq 3v - 6) \Rightarrow \text{граф не планарный}$$

Но это условие не является достаточным для планарности.

Необходимое и достаточное условие устанавливается **теоремой Куратовского** (доказательство можно посмотреть в специальной литературе):

Граф является планарным тогда и только тогда, когда он не содержит в качестве подграфов ни K_5 ни $K_{3,3}$.

Тема 11. БИНАРНЫЕ АЛГЕБРЫ С ОДНОЙ ОПЕРАЦИЕЙ: ОТНОШЕНИЕ ИЗОМОРФИЗМА ДЛЯ БИНАРНЫХ АЛГЕБР.

Бинарной алгеброй с одной операцией на множестве A называют упорядоченную пару $\langle A, f \rangle$, где f – функция, ставящая в соответствие упорядоченной паре элементов A значение из этого же множества: $f \in A^{A \times A}$.

Выражения с бинарными операциями удобнее записывать в инфиксной форме. Символ бинарной операции будем обозначать звёздочкой « \star » между операндами:

$$x \star y = f(x, y)$$

Алгебру будем аналогично обозначать таким же символом в упорядоченной паре:

$$\langle A, \star \rangle = \langle A, f \rangle \Leftrightarrow (f \in A^{A \times A} \ \& \ (\forall x \in A \ \forall y \in A \ x \star y = f(x, y)))$$

Если необходимо рассмотреть несколько таких алгебр, будем использовать различные инфиксные символы: \star, \square, \diamond

Алгебры удобно представлять в виде двумерных таблиц, в которых записаны значения результатов операции для всех возможных комбинаций значений левых и правых операндов. Такие таблицы называют *таблицами Кэли*. Мы уже использовали такую форму представления при рассмотрении логических операций и алгебр классов вычетов по модулю некоторого числа. Теперь такие таблицы будем применять к алгебрам с произвольными множествами элементов. Например, для $A = \{a, b, c, d\}$ зададим алгебру $\langle A, \star \rangle$ таблицей

\star	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Такие алгебры с дискретным, но уже возможно не двоичным набором значений являются обобщением двоичных функциональных преобразований, реализуемых логическими элементами в различных технических и информационных системах. Подобно тому, как из логических элементов можно строить схемы (моделью схем являются формулы с логическими операциями), можно представить и недвоичные преобразователи информации. Это может быть более общим подходом, чем сразу переходить к работе с символьной информацией, представленной двоичными или числовыми кодами.

Так же, как для бинарных отношений рассматривается отношение подобия, для алгебр вводят отношение *изоморфизма*. Обозначается символом \sim , как и равномощность множеств, так как для изоморфных алгебр множества действительно равномощны:

$$\langle A, \star \rangle \sim \langle B, \square \rangle \Leftrightarrow (\exists f \in B^A \ (f^{-1} \in A^B) \ \& \ (\forall x \in A \ \forall y \in A \ (f(x \star y) = f(x) \square f(y)))$$

Как и для других подобных отношений, связанных с установлением соответствий между множествами, будем надписывать обозначение устанавливающей соответствие функции над символом \sim : $\langle A, \star \rangle \overset{f}{\sim} \langle B, \square \rangle$.

То, что две алгебры изоморфны, означает, что одна может быть получена из другой при помощи замены обозначений элементов и операций. Структура у изоморфных алгебр одинакова. Рассмотрим это на примере алгебр логических бинарных операций. Возьмём, например, бинарные операции ЛОГИЧЕСКОЕ И (символ $\&$) и ЛОГИЧЕСКОЕ ИЛИ (символ \vee). Обе операции заданы на множестве логических значений $\mathcal{B}=\{0, 1\}$. Обозначим задаваемые этими операциями алгебры как $\langle \mathcal{B}, \& \rangle$ и $\langle \mathcal{B}, \vee \rangle$.

Таблицы для этих алгебр будут иметь вид

$\langle \mathcal{B}, \& \rangle$	$\langle \mathcal{B}, \vee \rangle$
$\&010001$	$\vee0100111$
01	1

Покажем, что структура этих алгебр одинакова. Рассмотрим формулу де Моргана:

$$\forall x \in V \forall y \in V (\neg(x \& y) = \neg x \vee \neg y)$$

Рассматривая унарную логическую операцию НЕ (символ \neg) как биективную функцию $f \in V^V$, видим совпадение структуры этой формулы с определением отношения изоморфизма.

Разберемся, что это именно замена обозначений. Заменим в таблице для алгебры $\langle V, \& \rangle$ все вхождения символа 0 на символ 1 и наоборот, все вхождения символа 1 на символ 0. Заменим обозначение операции $\&$ операцией \vee . Получим таблицу

\vee	1	0
1	1	1
0	1	0

Используя полученную таблицу как исходные данные для вычисления операции \vee , заполним таблицу для этой операции, в которой строки и столбцы озаглавлены в том же порядке, что и в таблицах, изначально использовавшихся для задания операций $\&$ и \vee . Получим таблицу, идентичную исходной для операции \vee .

Общая схема получения изоморфных пар логических операций может быть пояснена следующей парой таблиц, отражающих выражение второй операции через первую $x \sqsupset y = \neg(\neg x * \neg y)$, когда заданы двоичные значения a, b, c, d для всех возможных сочетаний значений операндов операции $*$:

$\langle \mathcal{B}, * \rangle$	$\langle \mathcal{B}, \sqsupset \rangle$
$*010ab1c$	$\sqsupset010\neg d\neg$
d	$c1\neg b\neg a$

Такие операции в алгебре логики называются *двойственными*.

Следующий пример взят из математики действительных чисел. Множество вещественных чисел обозначают символом \mathbb{R} . Обозначим множество действительных положительных чисел символом $P=\{x \mid x \in \mathbb{R} \ \& \ x > 0\}$. Символы $+$ и \cdot обозначают соответственно сложение и умножение действительных чисел. Тогда имеем две алгебры

$\langle \mathbb{R}, + \rangle$ и $\langle P, \cdot \rangle$. Можно записать $\langle \mathbb{R}, + \rangle \overset{\text{Exp}}{\sim} \langle P, \cdot \rangle$, так как экспонента по любому основанию (функция Exp) устанавливает взаимнооднозначное соответствие между множествами \mathbb{R} и P . При этом выполняется соотношение

$$(\forall x \in \mathbb{R} \ \forall y \in \mathbb{R} \ (\text{Exp}(x+y) = \text{Exp}(x) \cdot \text{Exp}(y))$$

Аналогично логарифм (функция Log) по любому основанию устанавливает соотношение $\langle P, \cdot \rangle \overset{\text{Log}}{\sim} \langle \mathbb{R}, + \rangle$: $(\forall x \in P \ \forall y \in P \ (\text{Log}(x \cdot y) = \text{Log}(x) + \text{Log}(y))$. На основе этого изоморфизма основан принцип действия логарифмической линейки: умножение чисел заменяют суммой длинной отрезков, отложенных на неподвижной и перемещаемой части по логарифмической шкале. С этой же шкалы снимают показания в виде результата умножения.

Как и равномощность множеств, **отношение изоморфизма алгебр является отношением эквивалентности:**

$$\text{Рефлексивность: } \langle A, * \rangle \overset{\Delta_A}{\sim} \langle A, * \rangle$$

$$\text{Симметричность: } \langle A, * \rangle \overset{f}{\sim} \langle B, \square \rangle \Rightarrow \langle B, \square \rangle \overset{f^{-1}}{\sim} \langle A, * \rangle$$

$$\text{Транзитивность: } \langle A, * \rangle \overset{f}{\sim} \langle B, \square \rangle \ \& \ \langle B, \square \rangle \overset{g}{\sim} \langle C, \diamond \rangle \Rightarrow \langle A, * \rangle \overset{f \circ g}{\sim} \langle C, \diamond \rangle$$

Класс эквивалентности по отношению изоморфизма некоторой алгебры $[\langle A, * \rangle]_{\sim}$ называют *абстрактной (свободной) алгеброй*.

Например, все бинарные алгебры логических операций

$$M = \{ \langle A, * \rangle \mid \langle A, * \rangle = \langle A, f \rangle \ \& \ (f \in A^{A \times A}) \ \& \ (A = \{0, 1\}) \}$$

(всего их 16) можно разбить на 10 классов свободных алгебр M/\sim . Изоморфными окажутся следующие пары операций: $\&$ и \vee , \oplus и \leftrightarrow , \downarrow и \mid , \rightarrow и \Leftarrow , \leftarrow и \Rightarrow , функция-константа 0 и функция-константа 1. Еще 4 операции в данных обозначениях операндов (0, 1) не имеют изоморфных пар, то есть являются одноэлементными классами. Они не очень интересны с практической точки зрения, так как имеют фиктивные аргументы. Но сам пример интересен тем, что, будучи подвергнуты преобразованию получения двойственной операции, такие алгебры переходят в себя, например, для $x * y = \neg y$ $\langle B, * \rangle = \langle B, \square \rangle$:

$$\begin{array}{ccc} \langle B, * \rangle & & \langle B, \square \rangle & & \langle B, \vee \rangle \\ *0101011 & \Longrightarrow & \square 0101011 & \Longrightarrow & \vee 0101011 \\ 0 & & 1 & & 0 \end{array}$$

Такие логические операции называются *самодвойственными*.

Тема 12. БИНАРНЫЕ АЛГЕБРЫ С ОДНОЙ ОПЕРАЦИЕЙ: СПЕЦИАЛЬНЫЕ СВОЙСТВА ОПЕРАЦИЙ И СПЕЦИАЛЬНЫЕ ЭЛЕМЕНТЫ.

В дальнейшем будем рассматривать не всё многообразие алгебр, а только те, для которых выполнены определённые ограничения на свойства операций и элементов.

В качестве ограничивающих свойств рассмотрим следующие возможные свойства:

1. Бинарная операция $*$ в алгебре $\langle A, * \rangle$ называется *ассоциативной*, если $\forall x \in A \forall y \in A \forall z \in A (x*y)*z = x*(y*z)$
2. Бинарная операция $*$ в алгебре $\langle A, * \rangle$ называется *коммутативной*, если $\forall x \in A \forall y \in A x*y = y*x$

По поведению относительно элементов множества и рассматриваемой операции выделим некоторые специальные элементы.

1. Если для некоторого элемента (обозначим его e_L) в алгебре $\langle A, * \rangle$ выполняется свойство $\forall x \in A e_L * x = x$, то такой элемент называется *левым нейтральным* (или *левым единичным*) *элементом*. Иногда его называют *левой единицей* алгебры.
2. Если для некоторого элемента (обозначим его e_R) в алгебре $\langle A, * \rangle$ выполняется свойство $\forall x \in A x * e_R = x$, то такой элемент называется *правым нейтральным* (или *правым единичным*) *элементом*. Иногда его называют *правой единицей* алгебры.
3. Если для некоторого элемента (обозначим его e) в алгебре $\langle A, * \rangle$ выполняется свойство $\forall x \in A e * x = x * e = x$, то такой элемент называется *двусторонним нейтральным* (или *двусторонним единичным*) *элементом*. Иногда его просто называют *единицей* алгебры.

Для таких элементов выполняются следующие свойства:

1. Если в алгебре $\langle A, * \rangle$ есть и левый e_L и правый e_R нейтральные элементы, то они совпадают (и, таким образом, в такой алгебре есть двусторонний нейтральный элемент).

$$(e_L \in A) \& (e_R \in A) \& (\forall x \in A e_L * x = x) \& (\forall x \in A x * e_R = x) \Rightarrow e_L = e_R$$

$$(e_L \in A) \& (e_R \in A) \& (\forall x \in A e_L * x = x) \& (\forall x \in A x * e_R = x) \Rightarrow (\exists e \in A \forall x \in A e * x = x * e = x)$$

Для доказательства рассмотрим выражение $e_L * e_R$. С одной стороны, $e_L * e_R = e_R$ по определению e_L . С другой стороны $e_L * e_R = e_L$ по определению e_R . По транзитивности равенства $e_L = e_L * e_R = e_R$. Обозначим этот элемент $e = e_L = e_R$. Свойства двустороннего нейтрального элемента для него выполняются.

2. Если в алгебре $\langle A, * \rangle$ есть двусторонний нейтральный элемент e , то он является единственным двусторонним левым нейтральным и единственным правым нейтральным элементом (и единственным двусторонним).

$$(e \in A) \& (\forall x \in A e * x = x * e = x) \Rightarrow (\exists ! e \in A \forall x \in A e * x = x * e = x)$$

Доказывается аналогично. Предположим существование еще одного элемента e' со свойством $\forall x \in A e' * x = x * e' = x$. Тогда $e' * e = e$. Односторонние свойства являются частными случаями двустороннего свойства.

В дальнейшем мы будем чаще иметь дело только с двусторонним нейтральным элементом. Тогда будем его называть просто *нейтральным элементом*.

Аналогично вводятся определения для нулевых элементов (левых, правых и двусторонних). Нейтральные элементы в бинарной операции поглощаются оставшимся операндом. Нулевые сами поглощают оставшийся операнд. Определяющие свойства будут такие:

4. Если для некоторого элемента (обозначим его o_L) в алгебре $\langle A, \star \rangle$ выполняется свойство $\forall x \in A \ o_L \star x = o_L$, то такой элемент называется *левым нулевым элементом* (или *левым нулём*).
5. Если для некоторого элемента (обозначим его o_R) в алгебре $\langle A, \star \rangle$ выполняется свойство $\forall x \in A \ x \star o_R = o_R$, то такой элемент называется *правым нулевым элементом* (или *правым нулём*).
6. Если для некоторого элемента (обозначим его o) в алгебре $\langle A, \star \rangle$ выполняется свойство $\forall x \in A \ o \star x = x \star o = o$, то такой элемент называется *двусторонним нулевым элементом* (или *двусторонним нулём*).

Свойства этих специальных элементов аналогичны: если есть и левый и правый нулевые элементы, то они совпадают и, таким образом, в алгебре будет единственный двусторонний нулевой элемент: $o_L \star o_R = o_L = o_R = o$.

Тема 13. Моноиды. Степени элементов. Обратимость и сократимость. Особенности конечных моноидов.

Используем введённые свойства элементов и операций для введения ограничений в последующем рассмотрении бинарных алгебр: рассмотрим алгебры с ассоциативной операцией и двусторонним нейтральным элементом. Множество таких алгебр можно определить следующей формулой:

$$\mathcal{M} = \{ \langle A, * \rangle \mid (\forall x \in A \ \forall y \in A \ \forall z \in A \ (x*y)*z = x*(y*z)) \ \& \ (\exists e \in A \ \forall x \in A \ e*x = x*e = x) \}$$

Алгебра $\langle A, * \rangle$ с ассоциативной операцией $*$ и двусторонним нейтральным элементом e называется моноидом.

Ассоциативность операции и наличие нейтрального элемента позволяет в определённых ситуациях делать выводы о значениях выражений или отдельных операндов по результатам наблюдений вычисленных по формулам с известной структурой выражений. Это может быть полезно при рассмотрении преобразований символьной информации в задачах кодирования и шифрования.

Рассмотрим некоторые свойства элементов, применимые к анализу выражений в таких алгебрах.

Назовём элемент $a \in A$ алгебры $\langle A, * \rangle \in \mathcal{M}$ *сократимым слева*, если для него имеет место следующее свойство:

$$a*x = a*y \Rightarrow x = y$$

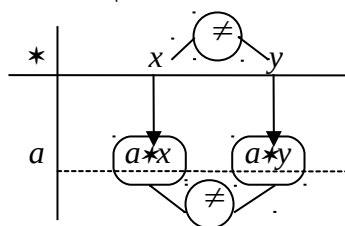
Такое свойство позволяет сокращать одинаковые левые части формул, если все элементы в этих частях формул обладают свойством сократимости. Действительно, если операция ассоциативна, равенства вида $a*b*x = a*b*y$ можно интерпретировать как $a*(b*x) = a*(b*y)$. Сокращая a слева, получаем $b*x = b*y$. Если b тоже сократим слева, далее получаем $x = y$.

Свойство сократимости слева можно проиллюстрировать при помощи таблицы Кэли. Рассмотрим противоположное обратному сократимости слева свойство

$$x \neq y \Rightarrow a*x \neq a*y$$

Для сократимого слева элемента оно тоже выполняется. Выполнимость противоположного обратному некоторого утверждения это известная схема в логике высказываний вида $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.

Такое свойство означает, что все значения, выписанные в строке таблицы, озаглавленной сократимым слева символом a различны, поскольку различны заголовки столбцов таблицы.



В конечной таблице это означает, что строка для сократимого слева элемента представляет собой некоторую *перестановку* элементов множества, на котором задана алгебра, и каждый элемент множества присутствует в такой строке.

Аналогично, свойство $x*a = y*a \Rightarrow x=y$ для элемента a называется *сократимостью справа*. Противоположное обратному для него $x \neq y \Rightarrow x*a \neq y*a$ означает различие элементов в соответствующем столбце таблицы.

Кроме возможности сокращать общую часть выражений, желательно иметь возможность восстановления значения одного из операндов при известном другом операнде по результату, то есть иметь возможность решения уравнений видов $a*x=b$ и $x*a=b$. Для моноидов в этом отношении полезным оказывается свойство обратимости элементов.

Допустим, имеет место равенство $x*y=e$, где e – нейтральный элемент. Тогда элемент x называется *левым обратным* для элемента y , а элемент y – *правым обратным* для элемента x . При этом элемент y называется *обратимым слева*, а элемент x – *обратимым справа*:

$$\begin{aligned} x - \text{обратим слева} &\Leftrightarrow \exists y \, y*x=e \\ x - \text{обратим справа} &\Leftrightarrow \exists y \, x*y=e \end{aligned}$$

Аналогичные двусторонние свойства можно сформулировать так:

$$x - \text{двусторонне обратим} \Leftrightarrow (\exists y \, y*x=e) \ \& \ (\exists y \, x*y=e)$$

То есть, элемент двусторонне обратим, если у него есть левый и правый обратный элемент. Однако не требуется, чтобы они совпадали, хотя в рассматриваемых алгебрах, как далее увидим, это получится автоматически.

$$y - \text{двусторонне-обратный для } x \Leftrightarrow y*x=x*y=e$$

То есть, двусторонне-обратный элемент подходит слева и справа к одному и тому же элементу, давая в результате нейтральный элемент.

Применимость обратимости к решению уравнения $a*x=b$ доказывается следующим образом. Допустим, элемент a обратим слева. Это означает, что $\exists y \, y*a=e$. Применим левый обратный для a к обеим частям уравнения. $y*(a*x)=y*b$. Далее используем ассоциативность операции $*$ для перестановки скобок. Получим $(y*a)*x=y*b$. Так как $y*a=e$ и $e*x=x$, получаем решение $x=y*b$:

$$a*x=b \ \& \ y*a=e \ \& \ a*x=b \Rightarrow y*(a*x)=y*b \Rightarrow \underbrace{(y*a)*x}_{=x} = y*b \Rightarrow x = y*b$$

Аналогично, если $a*y=e$ & $x*a=b \Rightarrow x=b*y$.

Видно, что **из обратимости слева следует сократимость слева**:

$$b*a=e \ \& \ a*x=a*y \Rightarrow b*(a*x)=b*(a*y) \Rightarrow (b*a)*x=(b*a)*y \Rightarrow e*x=e*y \Rightarrow x=y$$

Справедливо и аналогичное свойство в правой форме: $a*b=e$ & $x*a=y*a \Rightarrow x=y$

Вообще левые и правые формы свойств различают только потому, что не выдвигалось требований для операции быть коммутативной. Для коммутативной операции все свойства выполняются в двусторонней форме.

Посмотрим теперь, что для конечного моноида обратимость и сократимость взаимно обуславливается и всегда выполняется в двусторонней форме и сократимый элемент имеет единственный двусторонний обратный.

Для этого введем рекуррентное определение формальной степени элемента $a \in A$ в ассоциативной алгебре $\langle A, \star \rangle \in \mathcal{M}$:

$$\begin{aligned} a^1 &= a \\ a^{k+1} &= a^k \star a \end{aligned}$$

С каждым элементом $a \in A$ в $\langle A, \star \rangle \in \mathcal{M}$ связано множество степеней $B_a \subseteq A$
 $B_a = \{ x \mid \exists k \in \mathbb{N} \ x = a^k \}$

Как для любого ряда степеней в конечном множестве, в ряду степеней элемента a существует цикл, обусловленный конечностью множества B_a (нет инъективных отображений из \mathbb{N} в B_a). Можно записать это так: $\exists i \in \mathbb{N} \ \exists j \in \mathbb{N} \ i < j \ \& \ a^i = a^j$.

Тогда представим показатель степени j как сумму $j = i + k$. При этом $k \in \mathbb{N}$.

По свойству степеней тогда представим $a^j = a^{i+k} = a^i \star a^k$.

С учётом $a^i = a^j$ получаем равенство

$$a^i = a^i \star a^k$$

Если элемент a сократимый слева ($a \star x = a \star y \Rightarrow x = y$), заменим в левой части равенства a^i на $a^i \star e$ и сократим слева элемент a^i раз:

$$a^i = a^i \star a^k \Rightarrow a^i \star e = a^i \star a^k \Rightarrow \underbrace{a \star a \star \dots \star a}_{i \text{ раз}} \star a \star e = \underbrace{a \star a \star \dots \star a}_{i \text{ раз}} \star a \star a^k \Rightarrow e = a^k$$

Для ассоциативной операции скобки в выражениях можно опустить. Получили следующее свойство:

В конечном моноиде $\langle A, \star \rangle \in \mathcal{M}$ нейтральный элемент e представим как степень любого сократимого элемента.

$$\langle A, \star \rangle \in \mathcal{M} \ \& \ |A| = n \ \& \ (a \star x = a \star y \Rightarrow x = y) \Rightarrow \exists k \in \mathbb{N} \ a^k = e$$

Зная, что $\exists k \in \mathbb{N} \ a^k = e$, найдём двусторонний обратный элемент для a .
 Возможно два случая: $k=1$ и $k>1$.

Если $k=1$ то это означает, что $a=e$. Такой элемент сам для себя является двусторонним обратным, так как $e \star e = e$.

Если $k>1$, то $k-1 \in \mathbb{N}$. Тогда $a^{k-1} \star a = a \star a^{k-1} = a^k = e$. Видно, что a^{k-1} является двусторонне-обратным для a .

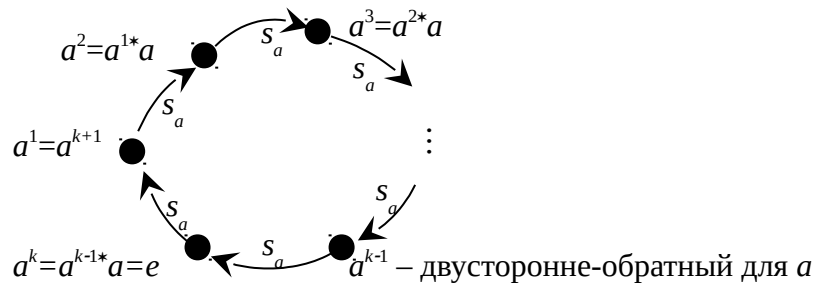
В любом случае $\exists m \in \mathbb{N} \ a^m \star a = a \star a^m = e$.

В конечном моноиде $\langle A, \star \rangle \in \mathcal{M}$ каждый сократимый элемент обратим, и имеет единственный двусторонне-обратный элемент, представимый некоторой своей натуральной степенью.

$$\langle A, \star \rangle \in \mathcal{M} \ \& \ |A| = n \ \& \ (a \star x = a \star y \Rightarrow x = y) \Rightarrow \exists m \in \mathbb{N} \ a^m \star a = a \star a^m = e$$

Единственность такого обратного элемента следует из сократимости (всегда двусторонней): $a \star a^m = e$ & $a \star b = e \Rightarrow b = a^m$.

Получается, что у обратимых и сократимых элементов в конечных моноидах степени образуют циклы (без апериодической части) следующего вида:



Здесь символом s_a обозначена функция следования $s_a \in B_a^{B_a}$, вычисляющая следующую степень по предыдущей: $s_a(x) = x \star a$.

Тема 14. АЛГЕБРАИЧЕСКИЕ ГРУППЫ. ОПРЕДЕЛЕНИЕ И СВОЙСТВА. ПОДГРУППЫ. КОНЕЧНЫЕ ГРУППЫ И ЦИКЛИЧЕСКИЕ ПОДГРУППЫ СТЕПЕНЕЙ ЭЛЕМЕНТОВ.

В качестве следующего, более узкого, класса бинарных алгебр рассмотрим моноиды, в которых все элементы обратимы. Такие алгебры называются группами.

Алгебраическая группа – это алгебра с ассоциативной операцией и нейтральным элементом, в которой у каждого элемента имеется обратный элемент.

Множество таких алгебр можно определить следующей формулой:

$$\mathbf{G} = \{ \langle A, * \rangle \mid (\forall x \in A \ \forall y \in A \ \forall z \in A \ (x*y)*z = x*(y*z)) \ \& \\ (e \in A) \ \& \ (\forall x \in A \ e*x = x*e = x) \ \& \\ (\forall x \in A \ \exists y \in A \ x*y = e) \}$$

Покажем, что **в алгебраической группе у каждого элемента есть единственный двусторонний обратный элемент.**

Заметим, что каждая группа по определению является также моноидом, поэтому для конечных групп это свойство выполняется автоматически (исходя из рассмотренной цикличности множества степеней сократимых элементов – по приведённому определению все элементы обратимы слева, следовательно, также и сократимы слева). Но данное свойство носит общий характер. Даже в бесконечных группах обратимость двусторонняя и единственная.

Вычислим $x*y$, зная, что $x*y=e$:

$$x*y=e \Rightarrow x*y=x*e*y=x*(y*x)*y=(x*y)*(x*y)$$

Обозначим $z=x*y$. Получили уравнение $z*z=z \Rightarrow z*z=z*e$. Сокращая z слева (в группе все элементы сократимы слева) получаем $z*z=z*e \Rightarrow x*y=e$. То есть, **в группе левый обратный некоторого элемента является одновременно и его правым обратным.** Отсюда следует правая сократимость и единственность обратимости.

Поэтому часто в определении для группы $\langle A, * \rangle$ сразу пишут

$$\forall x \in A \ \exists ! y \in A \ x*y=e$$

Это свойство показывает функциональную зависимость обратного элемента от обращаемого. Эту функцию естественно назвать унарной операцией обращения. Обозначим (единственный и двусторонний) обратный для элемента x как x^{-1} :

$$x^{-1}*x=x*x^{-1}=e$$

Кроме единственности обратного элемента, отметим для групп следующие свойства:

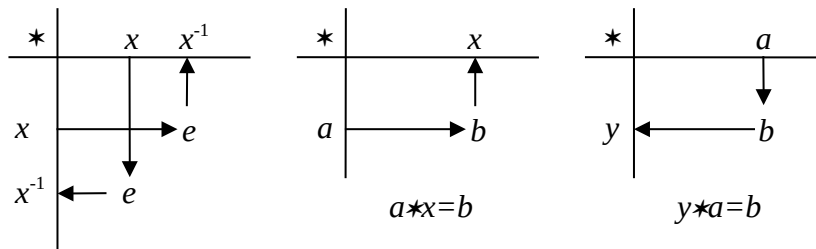
1. **Уравнения $a*x=b$ и $y*a=b$ имеют единственные решения $x=a^{-1}*b$ и $y=b*a^{-1}$ соответственно:**

$$a*x=b \Leftrightarrow x=a^{-1}*b \\ y*a=b \Leftrightarrow y=b*a^{-1}$$

2. **$(a*b)^{-1}=b^{-1}*a^{-1}$**

Замечание. Несмотря на похожие обозначения, рассматривавшаяся ранее операция обращения бинарных отношений $\alpha^{-1}=\{(x, y) \mid (y, x) \in \alpha\}$ в общем случае не может рассматриваться в качестве обратного элемента для отношения по операции композиции. Бинарные отношения относительно композиции образуют моноид, но, в общем случае, не группу. Обозначив $M=\{\alpha \mid \alpha \subseteq A \times A\}$ получаем алгебру композиций отношений $\langle M, \circ \rangle$. Эта алгебра будет моноидом. Действительно, композиция ассоциативна и Δ_A будет играть роль нейтрального элемента: $\Delta_A \circ \alpha = \alpha \circ \Delta_A = \alpha$. Но в такой алгебре есть нулевой элемент – пустое отношение: $\emptyset \circ \alpha = \alpha \circ \emptyset = \emptyset$. При этом $\emptyset^{-1} = \emptyset$ (как обратное отношение), но $\neg \exists \alpha \alpha \circ \emptyset = \Delta_A$ кроме вырожденного случая, когда $A = \emptyset$, $M = \{\emptyset\}$ и $\Delta_A = \emptyset$.

Для конечных групп $\langle A, \star \rangle$ таблицы Кэли представляют собой таблицы, где каждая строка и каждый столбец представляют собой некоторую перестановку элементов множества A . Это следует из двусторонней сократимости всех элементов. В таких таблицах легко проиллюстрировать обратимость и единственность решения уравнений:



В конечных группах все элементы образуют циклы степеней. Множество значений степеней некоторого элемента $B_a = \{x \mid \exists i \in \mathbb{N} x = a^i\}$ обладает свойством замкнутости относительно бинарной операции (по правилу сложения показателей степеней):

$$x \in B_a \ \& \ x \in B_a \Rightarrow \exists i \in \mathbb{N} \ \exists j \in \mathbb{N} \ x = a^i \ \& \ y = a^j \Rightarrow x \star y = a^i \star a^j = a^{i+j} \Rightarrow x \star y \in B_a$$

Число различных значений степеней некоторого элемента – число элементов множества B_a – **называют порядком элемента в группе $\langle A, \star \rangle$** . Порядок элемента обозначают в виде функции от элемента $\text{ord}(a) = |B_a|$. Удобным способом представления элементов $b \in B_a$ является минимальный показатель степени i , в которую надо возвести элемент a , чтобы получить $b = a^i$, так как если $\text{ord}(a) = k$ то выражения a^i и a^{i+k} представляют один и тот же элемент. При этом $a^k = e$, k это минимальный натуральный показатель степени, на котором достигается такое равенство. С учетом такого представления результат операции между двумя степенями $a^i \star a^j = a^{i+j}$ удобно записать в виде

$$a^i \star a^j = a^{R_{\text{ord}(a)}(i+j)}$$

Здесь символом $R_k(m)$ обозначена функция, вычисляющая остаток от деления числа m на число k так, чтобы $m = p \cdot k + R_k(m)$ и $0 \leq R_k(m) < k$. При этом остаток, равный 0 означает, что $a^i \star a^j = a^{i+j} = e$. То есть число $i+j$ делится на $\text{ord}(a)$. Удобно в связи с этим доопределить формальную степень так, чтобы вычислять её не только для натуральных показателей, но и для показателя, равного 0. **По определению**

$$a^0 = e$$

В группах можно ввести и отрицательные степени. По определению, для целого положительного k $a^{-k} = (a^k)^{-1}$. При этом $(a^k)^{-1} = (a^{-1})^k$, так как

$$\underbrace{a^{-1} \star a^{-1} \star \dots \star a^{-1}}_{k \text{ раз}} \star \underbrace{a \star a \star \dots \star a}_{k \text{ раз}} = e$$

Можно назвать операцию сложения показателей $a^i \star a^j = a^{R_{\text{ord}(a)}(i+j)}$ для $\text{ord}(a)=k$ сложением по модулю k и обозначить $R_k(i+j) = i \oplus^k j$. Будем, например, записывать

$$a^i \star a^j = a^{i \oplus^k j}.$$

Кроме замкнутости по бинарной операции, заметим, что для каждого элемента $b \in B_a$ его обратный элемент b^{-1} тоже представим в виде степени элемента (имеет место замкнутость B_a по обратимости):

$$b \in B_a \Rightarrow \exists i \ 0 \leq i < k \ \& \ b = a^i \Rightarrow a^{k-i} \star b = a^{k-i} \star a^i = a^k = e \Rightarrow b^{-1} = a^{k-i} \Rightarrow b^{-1} \in B_a$$

Свойство замкнутости по операции \star позволяет рассматривать на множестве B_a алгебру $\langle B_a, \star \rangle$. Представление элементов B_a показателями степенями элемента a устанавливает взаимнооднозначное соответствие между элементами этого множества и множеством целых чисел $Z_k = \{i \mid 0 \leq i < k\}$. Рассматривая множество Z_k с операцией \oplus^k как алгебру $\langle Z_k, \oplus^k \rangle$, можно заметить её изоморфизм с $\langle B_a, \star \rangle$:

$$\langle Z_k, \oplus^k \rangle \overset{f}{\sim} \langle B_a, \star \rangle$$

При этом в качестве функции $f \in B_a^{Z_k}$ берется функция, определяемая свойством $\forall i \in Z_k \ f(i) = a^i$. Соотношение изоморфизма выглядит следующим образом:

$$\forall i \in Z_k \ \forall j \in Z_k \ f(i \oplus^k j) = f(i) \star f(j) = a^i \star a^j = a^{i \oplus^k j} = f(i \oplus^k j)$$

Точно такую же структуру имеет уже упомянутая алгебра классов вычетов по модулю k с операцией $+$, получается заменой обозначений чисел $i \in Z_k$ на обозначения классов вычетов $[i] \in \mathbb{Z}_k$. Потому $\langle B_a, \star \rangle \sim \langle \mathbb{Z}_k, + \rangle$.

Кроме того, заметим, что $e \in B_a$. Получаем, что внутри множества A группы $\langle A, \star \rangle$ содержится замкнутое подмножество B_a , на котором для операции \star выполнены все определяющие свойства группы.

$$\langle A, \star \rangle \in \mathbf{G} \Rightarrow \forall a \in A \ \langle B_a, \star \rangle \in \mathbf{G}.$$

Если замкнутое в группе $\langle A, \star \rangle$ по бинарной операции \star и по обратимости подмножество $B \subseteq A$ содержит нейтральный элемент, то алгебра $\langle B, \star \rangle$ называется подгруппой группы $\langle A, \star \rangle$.

$$\langle B, \star \rangle - \text{подгруппа } \langle A, \star \rangle \in \mathbf{G} \Leftrightarrow (\forall x \in B \ \forall y \in B \ x \star y \in B) \ \& \ (\forall x \in B \ x^{-1} \in B) \ \& \ (e \in B)$$

В каждой группе, по крайней мере, множество, состоящее только из нейтрального элемента, и вся алгебра целиком являются подгруппами. Эти подгруппы называют

несобственными. Остальные подгруппы, если они существуют, называют *собственными* подгруппами.

Ранее было доказано, что **в конечной группе степени каждого элемента образуют подгруппу.**

Такие подгруппы, как было отмечено, представляют собой циклы степенного ряда образующего элемента. Поэтому их называют *циклическими подгруппами*. Также отметим, что **любая циклическая подгруппа изоморфна алгебре сложения классов вычетов по модулю порядка образующего элемента.**

Тема 15. ЦИКЛИЧЕСКИЕ ГРУППЫ. ИЗОМОРФИЗМ ЦИКЛИЧЕСКИХ ГРУПП И СЛОЖЕНИЯ КЛАССОВ ВЫЧЕТОВ ПО МОДУЛЮ n . СМЕЖНЫЕ КЛАССЫ ЭЛЕМЕНТОВ ПО ПОДМНОЖЕСТВАМ-ПОДГРУППАМ. РАЗБИЕНИЯ МНОЖЕСТВА ЭЛЕМЕНТОВ ГРУППЫ НА СМЕЖНЫЕ КЛАССЫ ПО ПОДГРУППАМ.

Если в группе $\langle A, \star \rangle$ имеется элемент c , своими степенями покрывающий все множество A , то такая группа называется *циклической*. Элемент c называется *порождающим элементом циклической группы*.

$$\langle A, \star \rangle \in \mathbf{G} - \text{циклическая} \Leftrightarrow \exists c \in A \quad \forall x \in A \quad \exists k \in \mathbb{N} \quad x = c^k \Leftrightarrow B_c = A$$

Для циклических групп отметим следующие свойства.

1. **Циклическая группа существует для любого числа элементов.**
Например, $\forall k \in \mathbb{N} \quad \langle \mathbb{Z}_k, + \rangle$ – циклическая группа.
2. **Для заданного числа элементов все циклические группы изоморфны.**
Ранее было показано, что каждая циклическая группа из k элементов изоморфна $\langle \mathbb{Z}_k, + \rangle$. Из транзитивности и симметричности изоморфизма следует взаимный изоморфизм их всех для данного k .
3. **Циклические группы коммутативны.**
Следует из коммутативности сложения показателей степеней образующего элемента.

Так как в конечной группе для каждого элемента его обратный элемент и нейтральный элемент представим как некоторая натуральная степень выбранного элемента, **в конечной группе любое замкнутое подмножество образует подгруппу.**

$$\forall x \in B \quad \forall y \in B \quad x \star y \in B \Rightarrow \forall x \in B \quad \forall k \in \mathbb{N} \quad x^k \in B \Rightarrow \forall x \in B \quad x^{-1} \in B \ \& \ e \in B$$

При рассмотрении таблиц Кэли для групп было отмечено, что их строки и столбцы представляют собой перестановки элементов некоторого множества – каждый элемент присутствует ровно один раз в каждом столбце и в каждой строке. Таблицы с таким свойством называются *латинскими квадратами*. В группах имеется аналог этого свойства для целых подмножеств элементов. Для его рассмотрения дадим следующие определения и обозначения:

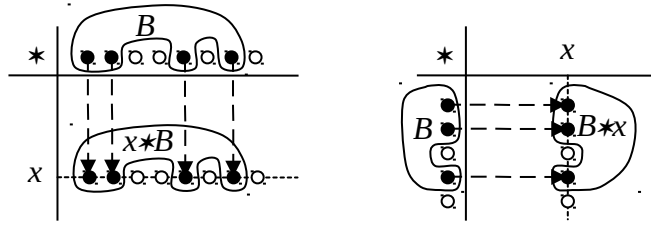
Пусть $\langle A, \star \rangle$ – некоторая алгебра, $B \subseteq A$ и $x \in A$.

Множество $x \star B = \{x \star b \mid b \in B\}$ называется *левым смежным классом*, порождаемым элементом x по подмножеству B .

Множество $B \star x = \{b \star x \mid b \in B\}$ называется *правым смежным классом*, порождаемым элементом x по подмножеству B .

Элемент x называют образующим элементом класса (левого и правого).

Эти множества можно представить как части строк (левые классы) и части столбцов (правые классы), озаглавленных символом x , соответствующие выделенному подмножеству заголовков столбцов или строк (множество B) таблицы Кэли. Следующие рисунки дают иллюстрацию к такому выделению.



Если алгебра является группой, соответствие между выделенными заголовками и элементами на строке (или на столбце) будет взаимнооднозначным. Это следует из свойства сократимости всех элементов.

Это означает, что в группах любое подмножество и оба его смежных класса (левый и правый) при любом образующим элементе будут равномощными множествами.

$$\langle A, * \rangle \in \mathbf{G} \Rightarrow \forall B \subseteq A \quad \forall x \in A \quad (B \overset{f}{\sim} x*B \ \& \ B \overset{g}{\sim} B*x) \Rightarrow \\ \forall B \subseteq A \quad \forall x \in A \quad |B| = |x*B| = |B*x|$$

$$\forall y \in B \quad f(y) = x*y \\ \forall y \in B \quad g(y) = y*x$$

Покажем, что если множество B образует подгруппу в группе $\langle A, * \rangle$, то множество (семейство) смежных классов (неважно, левых или правых) образует разбиение множества A .

Рассмотрим семейство левых смежных классов $\{x*B \mid x \in A\}$ по подгруппе $\langle B, * \rangle$. Семейство правых классов рассматривается аналогично.

Любой смежный класс не является пустым множеством
 $e \in B \Rightarrow x \in x*B \Rightarrow B \neq \emptyset$

Семейство смежных классов покрывает множество A
 $x \in x*B \Rightarrow \bigcup_{x \in A} (x*B) = A$

Если два класса имеют общий элемент, они полностью совпадают.
 Формулировка: $x*B \cap y*B \neq \emptyset \Rightarrow x*B = y*B$

Доказательство. $x*B \cap y*B \neq \emptyset \Rightarrow \exists z \in x*B \ \& \ z \in y*B \Rightarrow \exists z \ \exists u \in B \ \exists v \in B \ z = x*u = y*v$
 Покажем что $x*B \subseteq y*B$. То, что $y*B \subseteq x*B$, показывается аналогично.

$$t \in x*B \Rightarrow$$

$$\exists b \in B \ t = x*b = x*u*b = x*u*u^{-1}*b = y*v*u^{-1}*b = y*w \ \& \ w = v*u^{-1}*b \ \& \ w \in B \Rightarrow$$

$$\exists w \in B \ t = y*w \Rightarrow t \in y*B$$

$$(t \in x*B \Rightarrow t \in y*B) \Rightarrow x*B \subseteq y*B$$

Здесь использовано свойство замкнутости подгруппы по бинарной операции и обращению: $u \in B \ \& \ v \in B \ \& \ b \in B \Rightarrow v*u^{-1}*b \in B$. Объединяя два включения множеств, получаем равенство:

$$x*B \subseteq y*B \ \& \ y*B \subseteq x*B \Rightarrow x*B = y*B$$

Семейство левых смежных классов обозначим
 $A \dot{\setminus} B = \{x*B \mid x \in A\}$

Семейство правых смежных классов обозначим

$$A \text{ }^R B = \{B \star x \mid x \in A\}$$

ТЕОРЕМА О СООТНОШЕНИИ ЧИСЛА ЭЛЕМЕНТОВ ГРУППЫ И ПОДГРУППЫ И ЕЁ СЛЕДСТВИЯ.

Объединяя свойство разбиения множества A и равномощность смежных классов, получаем следующее соотношение между числом элементов множества A , числом элементов в подгруппе $\langle B, \star \rangle$ и числом различных смежных классов по данной подгруппе:

Число элементов в конечной группе $\langle A, \star \rangle$ равно числу элементов в подгруппе $\langle B, \star \rangle$, умноженному на число различных левых смежных классов по данной подгруппе.

Такое же свойство имеет место и для правых смежных классов.

$$\langle A, \star \rangle \in \mathbf{G} \ \& \ |A| \in \mathbb{N} \ \& \ (B \subseteq A) \ \& \ (\forall x \in B \ \forall y \in B \ x \star y \in B) \Rightarrow |A| = |B| \cdot |A \text{ }^L B| = |B| \cdot |A \text{ }^R B|$$

Отсюда видно, что число различных левых смежных классов подгруппы совпадает с числом различных правых смежных классов. Оно равно частному от деления числа элементов в множестве A на число элементов в множестве B .

$$|A \text{ }^L B| = |A \text{ }^R B| = |A| / |B|$$

Это число называют индексом подгруппы $\langle B, \star \rangle$ в группе $\langle A, \star \rangle$.

Так как число элементов A представимо в виде произведения ($|A \text{ }^L B|$ классов по $|B|$ элементов в каждом), **подгруппа по числу элементов должна быть делителем числа элементов в конечной группе.** Это утверждение известно как теорема Лагранжа.

$$\langle A, \star \rangle \in \mathbf{G} \ \& \ |A| \in \mathbb{N} \ \& \ B \subseteq A \ \& \ (\forall x \in B \ \forall y \in B \ x \star y \in B) \Rightarrow |B| \mid |A|$$

Здесь вертикальной чертой \mid показано бинарное отношение делимости чисел, $m \mid n$ читается « m делит n ».

В частности, циклические подгруппы степеней элементов должны подчиняться этому условию: **порядок каждого элемента конечной группы является делителем числа элементов группы.**

$$\langle A, \star \rangle \in \mathbf{G} \ \& \ |A| \in \mathbb{N} \Rightarrow \forall a \in A \ \text{ord}(a) \mid |A|$$

В связи с этим особый случай получается, если число элементов множества A не имеет собственных делителей. В теории чисел такие числа называют *простыми*. Их делителями являются только само число и число 1. В этом случае порядок каждого элемента, как следует из рассмотренного свойства, должен быть делителем простого числа. Это значит, что у каждого элемента в группе с простым числом элементов порядок будет равен либо общему числу элементов в группе, либо 1. Порядок равный 1 может быть только у нейтрального элемента, так как только он может являться решением уравнения $x \star x = x$. Следовательно, все остальные элементы своими степенями обязаны покрывать всё множество A , и группа оказывается циклической. Получили следующее свойство:

Если число элементов группы является простым, группа является циклической и каждый элемент, отличный от нейтрального элемента, является порождающим элементом группы.

$$\langle A, * \rangle \in \mathbf{G} \ \& \ |A|=p \ \& \ (k \nmid p \Leftrightarrow (k=1 \vee k=p)) \Rightarrow \forall c \in A \ (\text{ord}(c)=1 \vee \text{ord}(c)=p) \\ \Rightarrow \forall c \in A \ (c=e \vee (\forall x \in A \ \exists k \in \mathbb{N} \ x=c^k))$$

При простом числе элементов алгебраическая группа единственна с точностью до обозначений элементов и является коммутативной группой (изоморфна алгебре сложения классов вычетов по модулю простого числа).

$$\langle A, * \rangle \in \mathbf{G} \ \& \ |A|=p \ \& \ (k \nmid p \Leftrightarrow (k=1 \vee k=p)) \Rightarrow \langle A, * \rangle \sim \langle \mathbb{Z}_p, + \rangle$$

В группе с простым числом элементов не может быть собственных подгрупп.

$$\langle A, * \rangle \in \mathbf{G} \ \& \ |A|=p \ \& \ (k \nmid p \Leftrightarrow (k=1 \vee k=p)) \ \& \ B \subseteq A \ \& \ (\forall x \in B \ \forall y \in B \ x*y \in B) \\ \Rightarrow (B=A) \vee (B=\{e\})$$

ОТНОШЕНИЕ ЭКВИВАЛЕНТНОСТИ МЕЖДУ ЭЛЕМЕНТАМИ ГРУПП. КРИТЕРИЙ ЭКВИВАЛЕНТНОСТИ ЭЛЕМЕНТОВ. НОРМАЛЬНЫЕ ПОДГРУППЫ. ФАКТОРГРУППЫ.

Как и для всяких разбиений, с разбиением на смежные классы по подгруппе связано отношение эквивалентности. Два элемента эквивалентны тогда и только когда, когда они принадлежат одному и тому же смежному классу. В некоммутативном случае можно различать два таких отношения эквивалентности: $\overset{L}{\cong}_B$ для левых и $\overset{R}{\cong}_B$ для правых разбиений по подмножеству B :

$$x \overset{L}{\cong}_B y \Leftrightarrow (\exists z \ x \in z*B \ \& \ y \in z*B)$$

$$x \overset{R}{\cong}_B y \Leftrightarrow (\exists z \ x \in B*z \ \& \ y \in B*z)$$

Каждый смежный класс представляет собой в точности множество всех своих образующих элементов. Поэтому без потери общности можно записать

$$x \overset{L}{\cong}_B y \Leftrightarrow x \in y*B \Leftrightarrow y \in x*B$$

$$x \overset{R}{\cong}_B y \Leftrightarrow x \in B*y \Leftrightarrow y \in B*x$$

Докажем, например, утверждение $x \overset{L}{\cong}_B y \Rightarrow x \in y*B$:

$$x \overset{L}{\cong}_B y \Rightarrow (\exists z \ x \in z*B \ \& \ y \in z*B) \Rightarrow u \in B \ \& \ v \in B \ \& \ x=z*u \ \& \ y=z*v \Rightarrow$$

$$u \in B \ \& \ v \in B \ \& \ x=z*v*v^{-1}*u \ \& \ y=z*v \Rightarrow u \in B \ \& \ v \in B \ \& \ x=y*v^{-1}*u \Rightarrow x \in y*B$$

Такие отношения эквивалентности интересны тем, что для проверки условия $x \overset{L}{\cong}_B y$ (или $x \overset{R}{\cong}_B y$) нет необходимости просматривать всё множество классов разбиения ($A \overset{L}{\nearrow} B$ либо $A \overset{R}{\nearrow} B$). Достаточно уметь выполнять операцию $*$ и обращение, а также определять условие принадлежности элемента подгруппе:

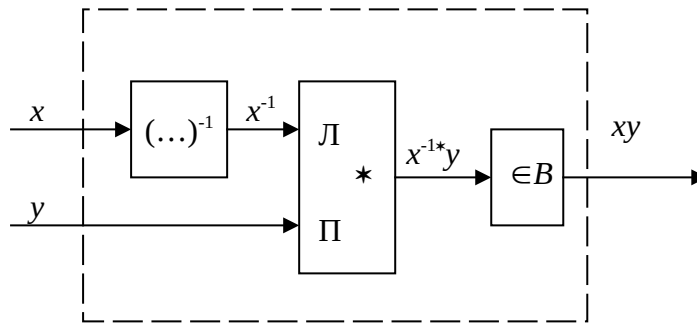
$$x \overset{L}{\underset{B}{\cong}} y \Leftrightarrow y^{-1} * x \in B \Leftrightarrow x^{-1} * y \in B$$

$$x \overset{R}{\underset{B}{\cong}} y \Leftrightarrow x * y^{-1} \in B \Leftrightarrow y * x^{-1} \in B$$

Докажем, например, что $x \overset{L}{\underset{B}{\cong}} y \Rightarrow y^{-1} * x \in B$:

$$x \overset{L}{\underset{B}{\cong}} y \Rightarrow x = y * b \text{ \& } b \in B \Rightarrow y^{-1} * x = y^{-1} * y * b \text{ \& } b \in B \Rightarrow y^{-1} * x = b \text{ \& } b \in B \Rightarrow y^{-1} * x \in B$$

Структурная схема для проверки условия $x \overset{L}{\underset{B}{\cong}} y$ может выглядеть следующим образом:



Здесь представлены три блока: блок обращения, блок вычисления бинарной операции и блок опознавания принадлежности подмножеству. Все сигналы, кроме выхода блока опознавания реализуют представление элементов группы. Выход блока опознавания логический. У блока вычисления бинарной операции отмечены левый (Л) и правый (П) входы. Если все указанные процедуры легко реализуемые, для проверки попадания элемента в некоторый класс достаточно подать на другой вход схемы код любого представителя класса.

Процедура ещё проще, если левые и правые семейства разбиений совпадают. Подгруппу со свойством $A \overset{L}{\underset{B}{\cong}} B = A \overset{R}{\underset{B}{\cong}} B$ называют *нормальной подгруппой*. В коммутативной группе все подгруппы нормальные.

В случае если подгруппа нормальная, нет необходимости различать левые и правые формы разбиений на смежные классы. В этом случае просто пишут

$$A \overset{L}{\underset{B}{\cong}} B = A \overset{R}{\underset{B}{\cong}} B \Rightarrow A/B = A \overset{L}{\underset{B}{\cong}} B = A \overset{R}{\underset{B}{\cong}} B \text{ и } x \overset{L}{\underset{B}{\cong}} y \Leftrightarrow x \overset{R}{\underset{B}{\cong}} y \Leftrightarrow x \overset{R}{\underset{B}{\cong}} y$$

Отношение «быть нормальной подгруппой» обычно обозначают $\langle B, * \rangle \trianglelefteq \langle A, * \rangle$.

Отношение $\overset{\cong}{\underset{B}{}}$ для разбиения по нормальной подгруппе обладает свойством конгруэнции относительно бинарной операции. Это позволяет ввести алгебру смежных классов на множестве A/B :

$$\langle B, * \rangle \trianglelefteq \langle A, * \rangle \Rightarrow (x * B) * (y * B) = (x * y) * B$$

Левые и правые классы в этом случае не различаются.

Алгебра классов нормальной подгруппы является группой: $\langle B, * \rangle \trianglelefteq \langle A, * \rangle \Rightarrow \langle A/B, * \rangle$ – группа. Нейтральным элементом при этом будет класс, образованный нейтральным элементом $\langle A, * \rangle$: $e * B = B * e = B$. Обратным каждому классу будет класс, образованный обратным любого элемента обращаемого класса: $(x * B)^{-1} = (x^{-1} * B)$.

Алгебру классов $\langle A/B, \star \rangle$ называют *факторгруппой*.

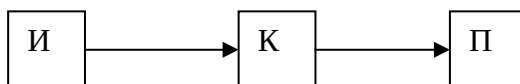
Примером может служить алгебра сложения классов вычетов по некоторому модулю n . Рассматривая обычную алгебру сложения целых чисел $\langle \mathbb{Z}, + \rangle$ как группу с нейтральным элементом 0 и обращением элементов как сменой знака целого числа $-x$, рассмотрим множество чисел, кратных n : $M_n = \{x \cdot n \mid x \in \mathbb{Z}\}$.

Видно, что $\langle M_n, + \rangle \trianglelefteq \langle \mathbb{Z}, + \rangle$. Тогда $\langle \mathbb{Z}/M_n, + \rangle = \langle \mathbb{Z}_n, + \rangle$.

Тема 16. ДВОИЧНЫЕ ГРУППОВЫЕ КОДЫ: ПОСТАНОВКА ЗАДАЧИ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ПРИ ПЕРЕДАЧЕ ДИСКРЕТНОЙ ИНФОРМАЦИИ ПО НЕНАДЁЖНОМУ КАНАЛУ. БЛОКОВОЕ КОДИРОВАНИЕ.

В качестве примера практического использования алгебраических свойств групп рассмотрим задачу повышения достоверности при передаче дискретной информации по ненадёжному каналу.

В отсутствие средств повышения достоверности передачи двоичной информации от источника к получателю выглядела бы следующим образом:



И - Источник, К - Канал, П - Получатель

Считая, что в канале нет ошибок вида пропадания или вставки символов (идеальная синхронизация) единственным видом ошибок является замена одного символа другим. В двоичном канале наличие ошибки означает замену символа противоположным (0 на 1 или 1 на 0). Замена символа на противоположный может быть выражена как результат операции “исключающее или” искаженного символа с константой 1, а отсутствие ошибки может быть выражено как операция “исключающее или” с константой 0. Поэтому такой идеализированный двоичный канал можно представить как устройство, где входная последовательность y поэлементно “складывается” (поэлементно выполняется операция “исключающее или”) с последовательностью ошибок e (рис. 2). В результате получается последовательность на выходе канала $\tilde{y}=y+e$. Здесь символ $+$ означает поэлементную операцию над двоичными последовательностями $\tilde{y}_i=y_i\oplus e_i$.

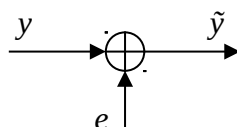


Рис. 2.

Для борьбы с ошибками на передающей стороне вводится некоторая избыточность в передаваемой информации, а на приемной стороне на основании принятой последовательности и статистических свойств источника информации и канала выбирается наиболее правдоподобная комбинация возможной передаваемой последовательности \hat{x} и последовательности ошибок \hat{e} . Такая схема иллюстрируется рис. 3.

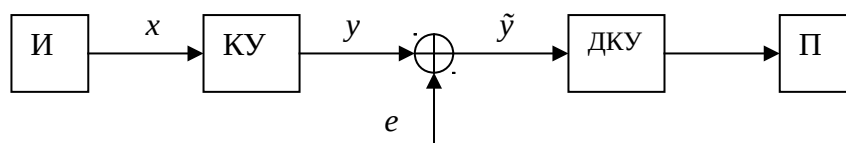


Рис. 3.

И - источник, КУ - кодирующее устройство (кодер), ДКУ - декодирующее устройство (декодер), П - получатель

Чтобы такая схема работала, необходимо, чтобы зависимость $y=f(x)$ была обратимой. Тогда $\mathcal{Y} = \tilde{y} + \hat{e}$, а $\hat{x} = f^{-1}(\mathcal{Y})$. Можно также написать $\hat{e} = \tilde{y} + f(\hat{x})$.

Декодирующее устройство должно выбрать такую оценку передаваемого сообщения, которое максимизирует значение следующего выражения

$$P_s(\hat{x}) \cdot P_e(\tilde{y} + f(\hat{x}) | f(\hat{x})),$$

где $P_s(X)$ - вероятность появления последовательности X на выходе источника, $P_e(E|Y)$ - вероятность появления последовательности ошибок E в канале при условии подачи последовательности Y на вход канала.

Если все возможные последовательности на выходе источника равновероятны, а последовательность ошибок не зависит от передаваемой последовательности, декодер должен максимизировать только $P_e(\tilde{y} + f(X))$ - безусловную вероятность последовательности ошибок. Таким образом, при данных допущениях оценка передаваемого сообщения принимает вид

$$\hat{x} : P_e(\tilde{y} + f(\hat{x})) \geq P_e(\tilde{y} + f(X)), \quad X, \hat{x} \in D,$$

где D - множество допустимых последовательностей на выходе источника.

Если сразу несколько последовательностей удовлетворяют такому условию, декодирующее устройство не может однозначно выбрать оценку передаваемой последовательности. В этом случае ошибка в передаче обнаруживается, но не может быть исправлена. При этом получателю может быть выдан некоторый сигнал. Схематически структура такого декодера показана на рис. 4.



Рис. 4.

Если только одна последовательность удовлетворяет приведенному условию, именно она и выдается получателю. При этом получатель может быть информирован об условиях принятия решения: он получит либо сигнал “в канале ошибки не обнаружены” если $\tilde{y} \in f(D)$ или сигнал “при передаче ошибки были, но были исправлены” в противном случае. Во втором случае декодер может даже сопроводить оценку сообщения некоторой количественной характеристикой, отражающей качество канала, например, расстоянием Хэмминга между последовательностями \tilde{y} и $f(\hat{x})$ - числом позиций, в которых эти последовательности отличаются. Такая характеристика будет количественной мерой достоверности принятого сообщения.

Нужно обратить внимание на то, что \hat{x} является только оценкой и может всегда с ненулевой вероятностью отличаться от переданной последовательности даже в тех случаях, когда декодер сообщает об отсутствии ошибок или об обнаруженных, но исправленных ошибках. В этом случае получатель получит искаженное сообщение.

Приведем классификацию событий, которые могут иметь место в рассматриваемой системе связи:

- 1) Ошибок нет ($\tilde{y}=y$), у получателя неискаженное сообщение ($\hat{x}=x$).
- 2) Ошибки есть ($\tilde{y} \neq y$), декодер нашел единственную последовательность \hat{x} , удовлетворяющую правилу приема и $\hat{x}=x$, у получателя неискаженное сообщение.
- 3) Ошибки есть и существует несколько последовательностей, удовлетворяющих правилу приема - у получателя признак обнаружимой, но не исправимой ошибки.
- 4) Ошибки есть и обнаружены декодером так как $\tilde{y} \notin f(D)$, декодер нашел единственную последовательность \hat{x} , удовлетворяющую правилу приема, но $\hat{x} \neq x$ - у получателя искаженное сообщение, но сопровождаемое сигналом недостоверности (если такая возможность реализована в системе).

5) Ошибки есть, но принятая из канала последовательность является допустимой - у получателя искаженное сообщение без признаков недостоверности: $\hat{y} \neq y, \hat{y} \in f(D)$.

Обычно выделяют два типа систем защиты от ошибок: с исправлением или только с обнаружением ошибок.

Если используется исправление ошибок, то:

- Правильному приему соответствуют события 1 и 2.
- Отказу от приема соответствует событие 3
- Неправильному приему соответствуют события 4 и 5.

Если используется только обнаружение ошибок, то

- Правильному приему соответствуют события 1.
- Отказу от приема соответствуют события 2, 3 и 4.
- Неправильному приему соответствует событие 5.

Наиболее часто считают, что чем меньше ошибок в канале (число символов 1 в последовательности e) тем такая ситуация является более вероятной. К такому заключению приводит, например, предположение о том, что в канале с вероятностью p символ 0 трансформируется в символ 1 или символ 1 трансформируется в символ 0 независимо от положения символа в последовательности и значений остальных символов (двоичный симметричный канал). Тогда вероятность появления последовательности ошибок e длиной L определяется только числом символов 1 в ней:

$$P_e(e) = (1-p)^{L-w(e)} \cdot p^{w(e)}.$$

где $w(X) = \sum_{i: X_i=1} 1$ - вес последовательности. В таком случае правило для декодирующего устройства будет иметь следующий вид:

$$\hat{x}: w(\tilde{y} + f(\hat{x})) \leq w(\tilde{y} + f(X)), \quad X, \hat{x} \in D$$

или

$$\hat{x} = f^{-1}(\mathcal{Y}): w(\tilde{y} + \mathcal{Y}) \leq w(\tilde{y} + Y), \quad Y, \mathcal{Y} \in f(D)$$

Таким образом, декодер минимизирует вес оценки последовательности ошибок $\hat{e} = \tilde{y} + \mathcal{Y}$. Можно также сказать, что в качестве оценки \mathcal{Y} передаваемой по каналу последовательности выбирается ближайшая по расстоянию Хэмминга от полученной из канала последовательности \tilde{y} допустимая (принадлежащая $f(D)$) последовательность:

$$\hat{y}: d(\tilde{y}, \hat{y}) \leq d(\tilde{y}, Y), \quad Y, \hat{y} \in f(D)$$

$$d(X, Y) = \sum_{i: X_i \neq Y_i} 1$$

В нашем курсе мы не будем рассматривать модели каналов, которые приводят к другим оптимальным правилам приема дискретных сообщений.

Рассмотрим теперь процедуру кодирования - реализации функции f в кодере. Обычно это устройство обрабатывает входную последовательность порциями (блоками) символов и порциями символов (блоками) выдает выходную последовательность. Если результат обработки каждого блока зависит только от символов, входящих в этот блок, и не зависит от обработанных ранее блоков, код называется блоковым. Наоборот, если такая зависимость есть, код называется непрерывным.

Характеристиками двоичного блокового кода являются размеры входных k и выходных n блоков. Такой код называется двоичным (k, n) кодом. Входом является двоичные вектора размерности k (элементы V^k), а выходом - двоичные вектора размерности n (элементы V^n). $V = \{0, 1\}$. Обычно допустимыми сообщениями являются все возможные вектора ($D = V^k$).

Обратите внимание, что на каждое из множеств V^k и V^n с операциями поэлементного исключения или образует алгебраические группы $\langle V^k, + \rangle$ и $\langle V^n, + \rangle$, являющиеся степенными расширениями двухэлементной группы $\langle V, \oplus \rangle$, а $f \in (V^n)^{V^k}$. Обозначим $A = V^n$. Множество $B = f(V^k) \subset A$ называется множеством допустимых кодовых

комбинаций. Код называется групповым, если $\langle B, + \rangle$ - подгруппа $\langle A, + \rangle$. “Сумма” любых допустимых кодовых слов также является допустимым кодовым словом в групповом коде.

Условие обратимости функции f проще всего выполнить, если все k символов из входного блока копируются в выходной, а остальные $n-k$ символов выходного блока вычисляются по входным k символам. Такой код называется систематическим. Структура такого кодера показана на рис. 5.

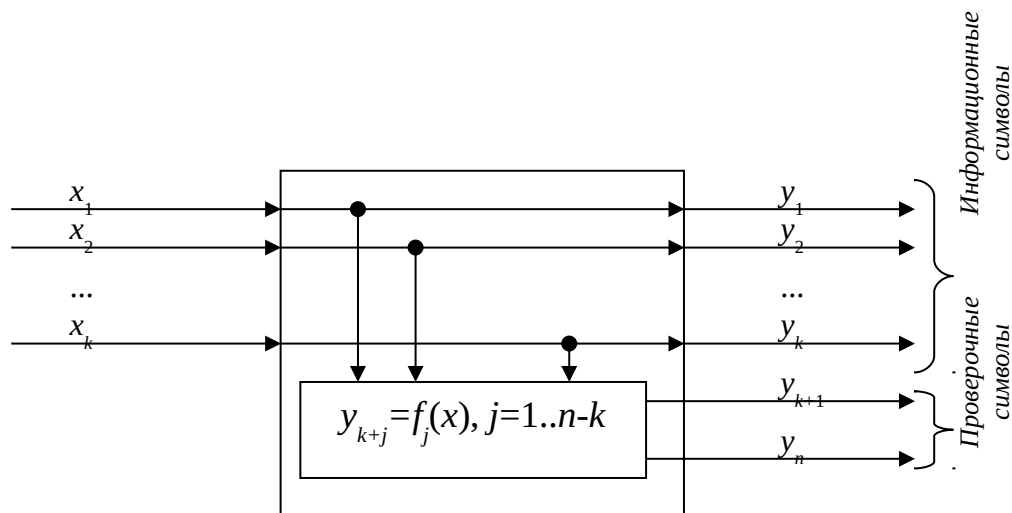


Рис. 5.

Такой код однозначно задается набором $n-k$ функций k двоичных аргументов. Вычисляемые символы называются проверочными символами блока.

Тема 17. ДВОИЧНЫЕ ГРУППОВЫЕ КОДЫ: МАТРИЧНОЕ КОДИРОВАНИЕ, ГРУППОВЫЕ СВОЙСТВА И ТАБЛИЦА СТАНДАРТНОЙ РАССТАНОВКИ. ИСПРАВЛЕНИЕ ОШИБОК.

Рассмотрим способ задания кода, обеспечивающий свойства группы для $\langle B, + \rangle$. Для этого введем операцию “умножения” двоичного вектора на двоичную матрицу, аналогичную операции умножения числового вектора на числовую матрицу. Определение получится заменой умножения на операцию $\&$ - “логическое и” и сложения на операцию \oplus - “исключающее или”. Порядок перебора индексов и требования к размерностям не изменяются. В результате получаем определение для операции \cdot :

$$y = x \cdot M, \quad y_j = \bigoplus_{i=1}^k x_i \& M_{ij} \quad j=1..n$$

Можно проверить (аналогично числовым матрицам), что для операции \cdot выполняется дистрибутивность относительно поэлементного “исключающего или”: $(x+y) \cdot M = x \cdot M + y \cdot M$. Кроме того, если матрица невырожденная $x \cdot M = 0 \Leftrightarrow x = 0$ (0 - вектор, все компоненты которого равны 0). Эти свойства обеспечивают задание двоичного группового кода любой невырожденной двоичной матрицей, если задать $y = f(x) = x \cdot M$ (здесь используется представление входных и выходных последовательностей в виде векторов-строк). Такое задание называется матричным кодированием. Проверим выполнение свойств подгруппы для множества B при матричном кодировании.

1. Замкнутость:

$$y \in B, z \in B \Rightarrow \exists x, t \in V^k: y = x \cdot M, z = t \cdot M \Rightarrow y + z = x \cdot M + t \cdot M = (x + t) \cdot M \in B$$

2. 0 - нейтральный элемент в A ,

$$0 = 0 \cdot M \in B$$

3. Обратимость:

$$\forall y \in B \quad y + y = 0.$$

Систематическому коду соответствует матрица (очевидно, невырожденная) с единичной подматрицей вида:

$$\left[\begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & M_{1,k+1} & \dots & M_{1,n} \\ 0 & 1 & \dots & 0 & M_{2,k+1} & \dots & M_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & M_{k,k+1} & \dots & M_{k,n} \end{array} \right]$$

Рассмотрим структуру вычисления отдельных проверочных символов. Она задается соответствующим столбцом матрицы. Единичные элементы показывают, какие входные символы кодера участвуют в вычислении данного проверочного символа. А вычисление заключается в сложении по модулю 2. Поэтому такой код называется также кодом с проверками на четность.

Пример задания кода - двоичный групповой систематический (3,6) код:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Схема кодирующего устройства приведена на рис. 6.

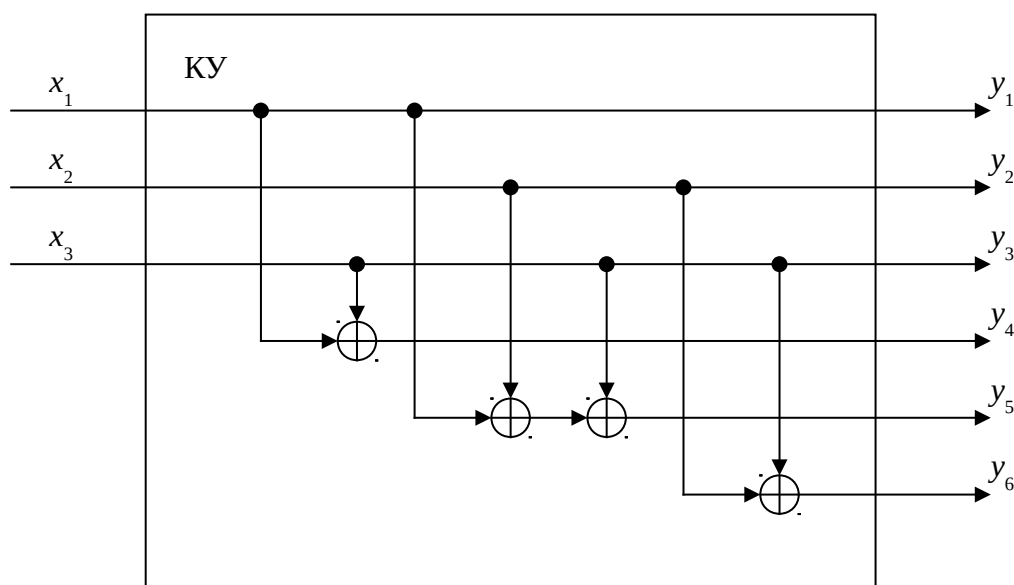


Рис. 6.

Чтобы сделать связь структуры кодера с порождающей матрицей нагляднее, схема умышленно оставлена неоптимальной по сложности (числу операций \oplus).

Рассмотрим теперь построение декодера и оценим его сложность. Всего из канала может быть получено 2^n различных блоков. Если сопоставить каждому возможному входу выход декодера из k разрядов оценки \hat{x} и еще один разряд - признак неисправимой ошибки, потребуется память из $2^n (k+1)$ -разрядных ячеек. Декодирование осуществляется за одну операцию выборки из памяти. Такой подход пригоден только для очень малых размеров блоков.

Для упрощения декодирования рассмотрим разбиение множества A на смежные классы по подгруппе B : $A/B = \{y+B | y \in A\}$. Смежный класс, порожденный нейтральным элементом - вектором 0 - запишем в виде первой строки таблицы, а остальные классы - следующими строками. Первая строка совпадает с самой подгруппой допустимых кодовых комбинаций $0+B=B$. Всего в таблице будет 2^{n-k} строк по 2^k элементов в каждой строке.

Рассмотрим условие возникновения необнаруженной ошибки. Для этого необходимо, чтобы $\tilde{y} \in B$ или $y+e=z$, $z \in B$. Тогда, так как в рассматриваемой группе каждый элемент обратный самому себе, $e=y+z$ и, так как $y \in B$, по замкнутости подгруппы относительно бинарной операции $+$ $e \in B$. Таким образом, не обнаруживаются те и только те комбинации ошибок, векторные представления которых сами являются допустимыми кодовыми комбинациями. Всего таких комбинаций будет $2^k - 1$, так как элемент $0 \in B$ - не ошибка. Запишем первую строку таблицы так, чтобы первым элементом был вектор 0 .

Остальные строки таблицы могут быть двух видов:

1) В строке (классе разбиения $p+B$) существует единственный элемент с наименьшим весом: $\exists z \in p+B: \forall t \in p+B w(z) \leq w(t)$. Тогда такой вектор z назовем *лидером* класса $p+B$, выберем его порождающим элементом (любой элемент класса может быть порождающим) и запишем первым в данной строке.

2) В строке такого элемента нет - порождающим элементом выберем произвольный элемент класса и запишем первым в данной строке.

Порядок расположения остальных элементов в строках зададим такой, чтобы элемент являлся "суммой" (результатом бинарной операции $+$) между заголовком строки (лидером z для строк первого типа или произвольным порождающим элементом для строк второго типа) и заголовком столбца (элементом подгруппы допустимых кодовых комбинаций). Схема построения такой таблицы показана на рис. 7.

0 - нейтр. эл-т	b_1	b_2	...	b_{2^k}
z_1	z_1+b_1	z_1+b_2	...	$z_1+b_{2^k}$
z_2	z_2+b_1	z_2+b_2	...	$z_2+b_{2^k}$
...
z_m	z_m+b_1	z_m+b_2	...	$z_m+b_{2^k}$
p_1	p_1+b_1	p_1+b_1	...	$p_1+b_{2^k}$
...
$p_{2^{n-k}-m-1}$	$p_{2^{n-k}-m-1}+b_1$	$p_{2^{n-k}-m-1}+b_2$...	$p_{2^{n-k}-m-1}+b_{2^k}$

Рис. 7

На этом рисунке m строк первого типа и $2^{n-k}-m$ строк второго типа. Всеми своими элементами таблица полностью покрывает множество векторов, которые могут быть получены из канала. Поэтому правило оптимального приема с исправлением ошибок будет заключаться в следующем:

1) Если принятый вектор попал в первую строку, то наиболее вероятно, что ошибок нет и $\hat{x} = f^1(\tilde{y})$ - то есть для систематического кода просто берутся информационные символы.

2) Если принятый вектор попал в одну из строк первого типа, то наиболее вероятно, что ошибка имеет конфигурацию лидера этой строки, а передаваемая информация - заголовок столбца, содержащего принятый вектор.

3) Если принятый вектор попал в одну из строк второго типа, то фиксируется обнаруженная, но не исправляемая ошибка.

Таким образом, двоичный групповой код исправляет те и только те конфигурации ошибок, которые являются лидерами в строках первого типа. На рисунке 7 всего m таких конфигураций.

Можно представить декодер как устройство, в котором запомнены все исправляемые конфигурации ошибок $z_1...z_m$, которое, если принятый вектор не является допустимым, осуществляет подбор (не более чем за m шагов) образца наиболее вероятной ошибки по условию $z_i + \tilde{y} \in B$, или, если это условие не выполняется, фиксирует неисправляемую ошибку. Это намного проще, чем табличное сопоставление вход и выхода декодера из первого подхода, но все-таки требует определенного числа операций и, возможно, памяти для элементов множества B .

ПРОВЕРОЧНАЯ МАТРИЦА И СИНДРОМНОЕ ДЕКОДИРОВАНИЕ.

Так как код является систематическим, проверку принадлежности можно заменить на повторное вычисление проверочных символов по информационным и сравнение с имеющимися проверочными символами. Сравнение будет заключаться в вычислении результата операции \oplus между вычисленным и принятым из канала проверочными символами (всего $n-k$ результатов). Если вектор $\in B$, то все результаты равны 0. Можно представить эту процедуру в виде умножения принятого вектора на проверочную матрицу:

$$s = \tilde{y} \cdot H$$

где H - матрица размером $n \times (n-k)$, s - вектор-строка размерности $n-k$, называемый вектором синдрома.

Можно проверить, что $s = \mathbf{0} \Leftrightarrow \tilde{y} \in B$ и, что два вектора \tilde{y} и \tilde{y}' тогда и только тогда принадлежат одному и тому же смежному классу, когда их синдромы совпадают. Поэтому декодер можно еще упростить, сопоставив каждому из возможных 2^{n-k} синдромов оценку ошибки и сигнал о необнаруженной ошибке (в пределах каждой строки таблицы синдромы одинаковые, а у разных строк они различны). Так как исправлять необходимо только ошибки в информационных символах, можно представить следующую схему декодера:

1) По принятому вектору из n разрядов вычисляется $n-k$ разрядов вектора синдрома (схема аналогична кодеру).

2) $n-k$ разрядов синдрома используются как адрес в памяти части образцов ошибок для информационной части из k разрядов. Еще один разряд нужен для признака неисправимой ошибки (всего 2^{n-k} ячеек по $k+1$ разрядов).

3) k разрядов из памяти поступают на схему исправления ошибок (k операций \oplus , выполняемых параллельно), а признак неисправимой ошибки передается получателю.

При этом, несмотря на значительное упрощение (2^{n-k} ячеек по $k+1$ разрядов против 2^n ячеек по $k+1$ разрядов), декодер остается эквивалентным декодеру максимального правдоподобия, рассмотренному в начале лекции.

Таким образом, если используется только обнаружение ошибок, код будет или обнаруживать $2^n - 2^k$ конфигураций ошибок, а не обнаруживать $2^k - 1$ конфигураций ошибок. Если используется исправление ошибок, то код будет исправлять t конфигураций ошибок, обнаруживать, но не исправлять $2^k(2^{n-k} - t - 1)$ конфигураций ошибок, не обнаруживать $2^k - 1$ конфигураций ошибок, и, наконец, обнаруживать, но не правильно исправлять $t(2^k - 1)$ конфигураций ошибок.

Тема 18. АЛГЕБРЫ С ДВУМЯ БИНАРНЫМИ ОПЕРАЦИЯМИ: КЛАССИФИКАЦИЯ, КОЛЬЦА, ОБЛАСТИ ЦЕЛОСТНОСТИ И ПОЛЯ, СВОЙСТВА ЭЛЕМЕНТОВ.

Алгебры с двумя бинарными операциями

Обозначения

$\langle A, +, \cdot \rangle$ - Алгебра с двумя бинарными операциями $+$ и \cdot на множестве A .

0 - нейтральный элемент для операции $+$, если он есть.

1 - нейтральный элемент для операции \cdot , если он есть.

$-x$ - унарная операция вычисления обратного элемента к x в алгебре $\langle A, + \rangle$, если ее элементы обратимые.

x^{-1} - унарная операция вычисления обратного элемента к x в алгебре $\langle A \setminus \{0\}, \cdot \rangle$, если $A \setminus \{0\}$ замкнуто относительно операции \cdot и все элементы этой алгебры обратимые.

$x-y$ - обозначение для $x+(-y)$.

${}^i x$ - степень элемента x в алгебре $\langle A, + \rangle$ ($\underbrace{x+x+\dots+x}_{i \text{ раз}}$).

x^i - степень элемента x в алгебре $\langle A, \cdot \rangle$ ($\underbrace{x \cdot x \cdot \dots \cdot x}_{i \text{ раз}}$).

$\frac{x}{y}$ - обозначение для $x \cdot y^{-1}$.

Типы алгебр с двумя операциями.

1. Кольца

Среди всех возможных типов рассмотрим только случай, когда:

- 1) $\langle A, + \rangle$ - коммутативная группа;
- 2) $\langle A, \cdot \rangle$ - полугруппа (\cdot - ассоциативная операция);
- 3) Выполняются два закона дистрибутивности:

$$\begin{aligned}x \cdot (y+z) &= (x \cdot y) + (x \cdot z) \\(x+y) \cdot z &= (x \cdot z) + (y \cdot z).\end{aligned}$$

Такая алгебра называется кольцом. В дальнейшем в записи выражений считается, что операция \cdot имеет более высокий приоритет, чем операция $+$ и скобки в правых частях выражений можно опустить.

По свойствам операции \cdot кольца можно разделить на следующие типы:

1. По существованию нейтрального элемента 1 в алгебре $\langle A, \cdot \rangle$ можно выделить кольца с единицей ($\exists 1 \in A: \forall x \in A \ 1 \cdot x = x \cdot 1 = x$) и без единицы.
2. По коммутативности операции \cdot кольца разделяются на коммутативные ($\forall x, y \in A \ x \cdot y = y \cdot x$) и некоммутативные. Эти свойства независимы, поэтому определяют четыре типа колец.
3. Если для некоторых $x, y \in A \setminus \{0\}: x \cdot y = 0$, то оба элемента x и y называются делителями нуля. По наличию или отсутствию таких элементов кольца разделяются на кольца с делителями нуля и кольца без делителей нуля. Среди всех возможных комбинаций рассмотренных свойств отдельно рассмотрим следующий случай:

2. Области целостности.

Область целостности это коммутативное кольцо с единицей без делителей нуля. Через свойства элементов это можно записать следующим образом:

$\langle A, +, \cdot \rangle$ - область целостности \Leftrightarrow

$$\forall x, y, z \in A \begin{cases} (x + y) + z = y + (x + z) \\ (x \cdot y) \cdot z = y \cdot (x \cdot z) \end{cases};$$

$$\exists 0 \in A: \forall x \in A \ 0 + x = x + 0 = x;$$

$$\exists 1 \in A: \forall x \in A \ 1 \cdot x = x \cdot 1 = x$$

$$\forall x \in A \ \exists !(-x) \in A: x + (-x) = (-x) + x = 0;$$

$$\forall x, y \in A \begin{cases} x + y = y + x \\ x \cdot y = y \cdot x \end{cases};$$

$$\forall x, y \in A \setminus \{0\} \ x \cdot y \neq 0$$

3. Поля.

Поле - алгебра с двумя операциями, в которой выполняются следующие свойства:

1. Множество с первой операцией образует коммутативную группу;
2. Множество, исключая нейтральный элемент, со второй операцией образует коммутативную группу;
3. Вторая операция дистрибутивна относительно первой.

Через свойства элементов это можно записать следующим образом:

$\langle A, +, \cdot \rangle$ - поле $\Leftrightarrow \begin{cases} \langle A, + \rangle - \text{коммутативная группа} \\ \langle A \setminus \{0\}, \cdot \rangle - \text{коммутативная группа} \end{cases} \Leftrightarrow$

$$\forall x, y, z \in A \begin{cases} (x + y) + z = y + (x + z) \\ (x \cdot y) \cdot z = y \cdot (x \cdot z) \end{cases};$$

$$\exists 0 \in A: \forall x \in A \ 0 + x = x + 0 = x;$$

$$\exists 1 \in A \setminus \{0\}: \forall x \in A \setminus \{0\} \ 1 \cdot x = x \cdot 1 = x$$

$$\forall x \in A \ \exists !(-x) \in A: x + (-x) = (-x) + x = 0;$$

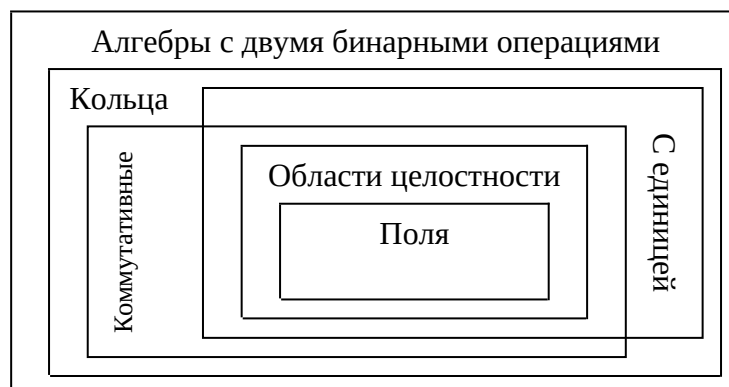
$$\forall x \in A \setminus \{0\} \ \exists !x^{-1} \in A: x \cdot x^{-1} = x^{-1} \cdot x = 1;$$

$$\forall x, y \in A \begin{cases} x + y = y + x \\ x \cdot y = y \cdot x \end{cases};$$

$$\forall x, y \in A \setminus \{0\} \ x \cdot y \in A \setminus \{0\}.$$

Видно, что это частный случай области целостности.

Таким образом, классификация имеет следующую структуру:



Свойства элементов колец

1. $0 \cdot x = x \cdot 0 = 0$

Доказательство:

$$x = x + 0 \Rightarrow \begin{cases} x \cdot x = x \cdot (x + 0) = x \cdot x + x \cdot 0 \\ x \cdot x = x \cdot x + 0 \end{cases} \Rightarrow x \cdot x + x \cdot 0 = x \cdot x + 0 \Rightarrow x \cdot 0 = 0. \text{ Используется правило}$$

сокращения слева для элемента $x \cdot x$ в алгебре $\langle A, + \rangle$. Аналогично доказывается $0 \cdot x = 0$.

2. $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$

Доказательство: Проверяется, что $(-x) \cdot y$ обратный для $x \cdot y$:

$$x \cdot y + (-x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0. \text{ Используется доказанное свойство 1.}$$

Аналогично проверяется, что $x \cdot (-y)$ обратный для $x \cdot y$. Из единственности обратных следует их совпадение.

3. В кольце с единицей $-x = (-1) \cdot x = x \cdot (-1)$. Свойство следует из 2.

Конечные области целостности

Свойство: Конечная область целостности является полем.

Доказательство: По определению через свойства элементов, для того, чтобы область целостности была полем, необходима обратимость элементов в $A \setminus \{0\}$.

$$(a \cdot x = a \cdot y, a \in A \setminus \{0\} \Rightarrow a \cdot x - a \cdot y = 0 \Rightarrow a \cdot (x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y) \Rightarrow a - \text{сократимый слева.}$$

В конечных моноидах из сократимости следует обратимость. \Rightarrow

$$\forall x \in A \setminus \{0\} \exists ! x^{-1} \in A: x \cdot x^{-1} = x^{-1} \cdot x = 1$$

Остальные свойства элементов в определениях поля и области целостности совпадают.

Идеалы и факторкольца.

Идеалы

$\langle A, +, \cdot \rangle$ - кольцо с единицей. Множество $I \subset A$ называется идеалом кольца с единицей, если выполнены условия:

1. $\forall x, y \in I \quad x + y \in I$
2. $\forall x \in I \quad \forall y \in A \quad x \cdot y \in I, y \cdot x \in I$

Отношение сравнимости

Элементы a, b кольца $\langle A, +, \cdot \rangle$ называются сравнимыми по модулю идеала I , если $a - b \in I$.

Это есть бинарное отношение на множестве A . Обозначение в инфиксной форме $a \equiv_I b$:
 $a \equiv_I b \Leftrightarrow a - b \in I$

Это отношение будет отношением эквивалентности.

Доказательство:

- 1) Рефлексивность: $\forall x \in I \quad 0 \cdot x \in I \Rightarrow 0 \in I \Rightarrow \forall a \in A \quad a - a = 0 \in I \Rightarrow \forall a \in A \quad a \equiv_I a$.
- 2) Симметричность: $a \equiv_I b \Rightarrow a - b \in I \Rightarrow (-1) \cdot (a - b) \in I \Rightarrow b - a \in I \Rightarrow b \equiv_I a$.
- 3) Транзитивность: $\begin{cases} a \equiv_I b \\ b \equiv_I c \end{cases} \Rightarrow a - b \in I, b - c \in I \Rightarrow (a - b) + (b - c) = a - c \in I. \Rightarrow a \equiv_I c$.

Классы вычетов

По отношению сравнимости для произвольно взятого элемента можно построить класс эквивалентности (множество элементов, находящихся в отношении сравнимости с выбранным), называемый классом вычетов элемента x по модулю идеала I :

$$[x]_{\equiv_I} = [y]_{\equiv_I} \Leftrightarrow x \equiv_I y$$

Когда множество ясно из контекста, нижние индексы в записи обычно опускают: $[x] = \{y \mid x \equiv y\}$.

Операции над классами вычетов

Определение и обозначение:

$$[x] + [y] = [x + y]$$

$$[x] \cdot [y] = [x \cdot y]$$

Необходимо проверить, что эти выражения действительно определяют бинарные операции на $A/\equiv = \{[x] \mid x \in A\}$ - фактормножестве (множестве всех различных классов эквивалентности). Именно, что введенные обозначения не зависят от выбора порождающих элементов:

$$[x] = [x'], [y] = [y'] \Rightarrow$$

$$\Rightarrow x \equiv x', y \equiv y' \Rightarrow x - x' \in I, y - y' \in I \Rightarrow$$

$$1) (x+y) - (x'+y') = (x-x') + (y-y') \in I \Rightarrow x+y \equiv x'+y' \Rightarrow [x+y] = [x'+y']$$

$$2) x \cdot y - x' \cdot y' = x \cdot y - x' \cdot y + x' \cdot y - x' \cdot y' = (x-x') \cdot y + x' \cdot (y-y') \in I \Rightarrow x \cdot y \equiv x' \cdot y' \Rightarrow [x \cdot y] = [x' \cdot y']$$

Факторкольца (кольца классов вычетов)

Фактормножество $A/\equiv = \{[x] \mid x \in A\}$ вместе с введенными операциями $+$ и \cdot на нем называется факторкольцом или кольцом классов вычетов $\langle A/\equiv, +, \cdot \rangle$.

Элемент $[0]$ играет роль нейтрального элемента первой операции, а элемент $[1]$ - второй. Элемент $[-x]$ является обратным для $[x]$. Алгебра $\langle A/\equiv, +, \cdot \rangle$ обладает всеми свойствами кольца.

Если взять в качестве алгебры $\langle A, +, \cdot \rangle$ кольцо целых чисел с операциями сложения и умножения $\langle \mathbb{Z}, +, \cdot \rangle$, а в качестве идеала I множество чисел, кратных некоторому числу p ($I = \{n \cdot p \mid n \in \mathbb{Z}\}$), то получится кольцо классов вычетов по модулю числа p , в котором каждый класс может быть представлен числом от 0 до $p-1$. Для него предусмотрено обозначение \mathbb{Z}/p .

$$\mathbb{Z}/p = \langle \mathbb{Z}/\equiv_{\{n \cdot p \mid n \in \mathbb{Z}\}}, +, \cdot \rangle$$

Вычисления в этой алгебре заключаются в сложении или умножении порождающих элементов и вычислении остатков от деления на p .

Тема 19. КОНЕЧНЫЕ ОБЛАСТИ ЦЕЛОСТНОСТИ И ПОЛЯ. ПОЛЯ ПРОСТОГО ПОРЯДКА. ЭЛЕМЕНТЫ, КРАТНЫЕ ЕДИНИЦЕ. ХАРАКТЕРИСТИКА ПОЛЯ. ВЕКТОРНОЕ ПРЕДСТАВЛЕНИЕ ЭЛЕМЕНТОВ ПОЛЯ. ХАРАКТЕРИСТИКА И РАЗМЕРНОСТЬ.

Поля простого порядка

Если p - простое число, то кольцо классов вычетов по модулю числа p будет областью целостности, так как $0 < a, b < p \Rightarrow a \cdot b \neq n \cdot p$.

Так как число классов вычетов конечно, то эта алгебра будет также и полем:

$p \in P \Rightarrow \mathbb{Z}/p$ - поле.

Конечные поля.

Характеристика поля

Число $p = \min m: m \cdot 1 = 0$ называется характеристикой поля (порядок элемента 1 по операции +).

Характеристика поля - простое число.

Доказательство:

Если характеристика поля p - составное, то $p = p_1 p_2$, $p_1, p_2 < p \Rightarrow p \cdot 1 = p_1 p_2 \cdot 1 = p_1 \cdot p_2 \cdot 1 = 0 \Rightarrow$

$\begin{cases} p_1 \cdot 1 = 0 \\ p_2 \cdot 1 = 0 \end{cases}$, что противоречит определению характеристики. Поэтому p - простое число.

Такой же порядок по операции + имеют все элементы из $A \setminus \{0\}$

Подполе простого порядка

В каждом конечном поле содержится подполе простого порядка.

Множество элементов $\{k \cdot 1 | k \in \mathbb{N}\}$ образует подполе (замкнутость по + и \cdot , наличие элементов $0 = p \cdot 1$ и $1 = 1 \cdot 1$). Оно изоморфно \mathbb{Z}/p :

Взаимно однозначное соответствие для $k \in 1..p-1$

$f(k) = k \cdot 1$.

Сохранение операций:

$f(x+y \bmod p) = f(x) + f(y) = x \cdot 1 + y \cdot 1 = (x+y) \cdot 1 = (x+y \bmod p) \cdot 1$

$f(xy \bmod p) = f(x) \cdot f(y) = x \cdot 1 \cdot y \cdot 1 = xy \cdot 1 = (xy \bmod p) \cdot 1$

Векторное представление элементов

Процедура получения представления элементов как линейной комбинации "базисных" элементов с "коэффициентами" - элементами подполя.

$\langle A, +, \cdot \rangle$ - конечное поле, $\langle B, +, \cdot \rangle$ - некоторое подполе (обычно $\langle \{k \cdot 1 | k \in \mathbb{N}\}, +, \cdot \rangle$, так как эта алгебра всегда будет подполем).

Шаг 1. Взять любой элемент x_1 из $A \setminus \{0\}$. Построить множество $A_1 = \{a_1 \cdot x_1 | a_1 \in B\}$.

Если $A_1 = A$ (и $= B$) то построение закончено - поле имело простой порядок - x_1 будет базисным элементом. Иначе перейти к шагу 2.

Шаг 2. Взять любой элемент x_2 из $A \setminus A_1$. Построить множество $A_2 = \{a_1 \cdot x_1 + a_2 \cdot x_2 | a_1, a_2 \in B\}$.

$A_1 \subseteq A_2$, $x_2 \notin A_1$, $x_2 \in A_2$, так что число элементов может только увеличиться. Если $A_2 = A$, то построение закончится на этом шаге, x_1, x_2 -базисные вектора. Иначе аналогично поступают с $A \setminus A_2$.

В результате на некотором шаге m из-за исчерпания элементов в конечном множестве A будет получено следующее представление:

$$A=A_m=\{a_1 \cdot x_1+a_2 \cdot x_2+\dots+a_m \cdot x_m|a_i \in B\}$$

Такое представление элементов обладает свойством

Каждый элемент представим в виде $a_1 \cdot x_1+a_2 \cdot x_2+\dots+a_m \cdot x_m$ единственным образом (при фиксированных выбранных по описанной процедуре базисных элементах x_1, x_2, \dots, x_m).

Тема 20. Кольцо многочленов с коэффициентами из поля. Операции над многочленами. Конечные поля: построение путём разложения на классы вычетов по модулю неприводимого многочлена.

Рассмотрим теперь удобное представление для элементов конечного поля, позволяющее эффективно выполнять обе операции без необходимости хранения двух таблиц Кэли.

Введём для этого вспомогательную алгебру на множестве полубесконечных последовательностей с элементами из множества A , на котором построена алгебра, являющаяся полем $\langle A, +, \cdot \rangle$.

Удобнее будет нумеровать элементы таких последовательностей, начиная с позиции 0, а не с 1 в связи с особенностями используемой далее системой обозначений:

$$(a_0, a_1, a_2, a_3, \dots)$$

Будем обозначать такие последовательности формальным степенным рядом $\sum_i a_i X^i$ - многочленом от формального символа X . Будем записывать только те элементы ряда, в которых коэффициенты a_i не равны 0. Последовательности полубесконечные, но, если начиная с некоторого номера позиции они содержат только значения 0, их можно представить конечной формулой в виде степенного ряда. Например, последовательность

$$(1, 1, 1, 0, 1, 0, 1, 0, 0, \dots)$$

с двоичными элементами представляется как

$$1X^0 + 1X^1 + 1X^2 + 1X^4 + 1X^6.$$

Будет удобнее, если опускать X^0 и 1 перед X и в показателе. Запишем эту последовательность тогда как

$$1 + X + X^2 + X^4 + X^6$$

Многочлен, соответствующий последовательности из одних символов 0 обозначим 0.

Кроме возможности компактно представить полубесконечную последовательность конечной формулой, заметим, что порядок записи термов многочлена не играет роли.

Два многочлена называют равными, если коэффициенты при одинаковых степенях формального символа X совпадают.

Множество всех возможных многочленов над $\langle A, +, \cdot \rangle$ обозначают $F[X]$.

Самый большой номер (считая от 0) ненулевого элемента последовательности называют степенью многочлена. Обозначается символом \deg . Степень многочлена 0 обычно считают неопределённой. Можно ввести специальный нечисловой символ на этот случай, например, λ .

Пример

$$\deg(1 + X + X^2 + X^4 + X^6) = 6$$

$$\deg(1 + X^2) = 2$$

$$\begin{aligned}\deg(1+X) &= 1 \\ \deg(1) &= 0 \\ \deg(0) &= \lambda\end{aligned}$$

Введём на множестве $F[X]$ две операции – сложение и умножение многочленов – соответствующие тому, как это делается для обычных алгебраических многочленов.

$$\begin{aligned}(\sum_i a_i X^i) + (\sum_i b_i X^i) &= \sum_i (a_i + b_i) X^i \\ (\sum_i a_i X^i) \cdot (\sum_i b_i X^i) &= \sum_k (\sum_{i+j=k} (a_i \cdot b_j)) X^k\end{aligned}$$

Получаем алгебру многочленов $\langle F[X], +, \cdot \rangle$. Такая алгебра будет кольцом, и даже областью целостности, но не полем, так как она бесконечна.

Действительно, для операции $+$ мы получили коммутативную группу $\langle F[X], + \rangle$. В ней многочлен 0 – нейтральный элемент и $-(\sum_i a_i X^i) = \sum_i (-a_i) X^i$.

Многочлен 1 (то есть $1X^0$) – нейтральный элемент для коммутативной операции \cdot .

$$(1) \cdot (\sum_i a_i X^i) = \sum_i a_i X^i.$$

Но обратимыми являются только многочлены степени 0: $(a X^0) \cdot (a^{-1} X^0) = 1X^0$.

Алгебра $\langle F[X], +, \cdot \rangle$ называется кольцом многочленов с коэффициентами из поля $\langle A, +, \cdot \rangle$.

Для операции \cdot можно ввести операцию деления с остатком.

$$g \in F[X] \text{ \& } h \in F[X] \text{ \& } g \neq 0 \Rightarrow \exists! q \in F[X] \exists! r \in F[X] \deg(r) < \deg(g) \text{ \& } h = q \cdot g + r$$

Здесь многочлен q – частное от деления, r – остаток.

Справедливость этого утверждения следует из алгоритма деления с остатком для алгебраических многочленов.

Если $\deg(h) = m$ и $\deg(g) = n$ и $m > n$ то $h = aX^m + \dots$ и $g = bX^n + \dots$. Тогда $q = (a \cdot b^{-1})X^{m-n} + \dots$.

Вычислен один член частного (при его самой старшей степени). Вычисляем частичный остаток $p = h - ((g) \cdot ((a \cdot b^{-1})X^{m-n}))$ и продолжаем процедуру деления теперь для p вместо h . Процедура заканчивается, когда выполнится $\deg(p) < \deg(g)$.

При построении простого поля как кольца классов вычетов, необходимо было рассматривать остатки от деления на простое число (не имеющее собственных делителей). Для многочленов аналогично вводится понятия *неприводимого* многочлена (в поле $\langle A, +, \cdot \rangle$). Рассмотрим, например, двоичное поле и множество многочленов над ним.

В порядке возрастания степеней это будут

$$\begin{array}{ll}\deg=\lambda & 0 \\ \deg=0 & 1 \\ \deg=1 & X, \quad X+1 \\ \deg=2 & X^2, \quad X^2+1, \quad X^2+X, \quad X^2+X+1 \\ \dots & \\ \text{Но} & (X) \cdot (X) = X^2, \quad (X) \cdot (X+1) = X^2+X, \quad (X+1) \cdot (X+1) = X^2+1.\end{array}$$

Видно, что X^2+X+1 не представим в виде произведения многочленов меньшей степени. Можно рассмотреть таблицу операции умножения многочленов степени менее 2 с последующим вычислением остатка от деления на этот многочлен. Такой остаток для ненулевых операндов никогда не будет равен 0. Поэтому такая алгебра будет являться конечной областью целостности и, следовательно, полем.

Пример такой таблицы показан ниже.

·	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

Здесь в каждую ячейку вписан остаток от деления на X^2+X+1 для произведения операндов. Добавляя к такой таблице поэлементное сложение многочленов, получаем поле из 4 элементов.

Продолжая этот пример, заметим, что с ростом степени многочлена возможно иметь несколько неприводимых многочленов одной степени. Например, среди 8 многочленов степени 3 есть 2 неприводимых многочлена (над двоичным полем): X^3+X^2+1 и X^3+X+1 : аналогично тому, как простые числа некоторого диапазона не покрывают своими произведениями множества всех чисел, многочлены степени не более заданной не покрывают своими произведениями даже следующей по порядку степени. Можно доказать, что над любым полем для любой степени существует по крайней мере один неприводимый многочлен.

Таким образом особенно удобно реализовывать вычисления в полях характеристики 2. В них операция $+$ соответствует поэлементному исключающему или, а операция \cdot соответствует серии поэлементных исключающих или и сдвигов (реализующих рассмотренный алгоритм деления многочленов).

Литература

- Новиков, Ф.А. Дискретная математика для программистов : учеб. пособие для вузов по направлению 2003, 2003, 2004 / Ф.А. Новиков — М. [и др.] : Питер, 2004
- Дискретная математика и комбинаторика. / Андерсон Дж. А. — М., СПб., Киев Издательский дом «Вильямс», 2004
- Лекции по дискретной математике. / Дехтярь. М.И. — М. БИНОМ, 2007
- Дискретная математика. / Соболева Т.С. Чечкин А.В. — М. Академия, 2006
- Дискретная математика : курс лекций и практ. занятий : учеб. пособие для вузов по спец. 220200 \ / Шапорев С. Д. — СПб. : БХВ-Петербург, 2006