Дискретни структури, лекция 2: множества

Минко Марков

minkom@fmi.uni-sofia.bg

Факултет по Математика и Информатика
Софийски Университет "Свети Климент Охридски"

31 март 2021 г.

Опит за определение на "множество"

Да се опитаме да дефинираме "множество", използвайки интуитивната си представа за понятието.

Определение 1

Множество е неподредена колекция от различни обекти.

Но какво означава "колекция"?

Определение 2

Колекция е неподреден агрегат от различни обекти.

Но какво означава "агрегат"? И така нататък.

Нито едно от тези така наречени "определения" всъщност **не е определение**, защото или ползва неопределено понятие, или води до зацикляне.

“Множество” е първично понятие

Очевидно трябва да има поне едно понятие, което не се дефинира.

Конвенция 1

“Множество” (на английски е set) е първично понятие.

Първично е понятие, което не се дефинира.

Защо множествата са важни

При изграждане на фундамента на математиката хората са установили, че всички дялове могат да се формализират чрез множества.

> Underlying the mathematics we study in algebra, geometry, combinatorics, probability, and almost every other area study of contemporary mathematics is the notion of a set. Very often this concept provides an underlying structure for a concise formulation of the mathematical topic being investigated.
>
> Ralph Grimaldi, Discrete and Combinatorial Mathematics, 5th edition, Pearson Education, pp. 123

Как означаваме множествата (1)

Обикновено, но не винаги, имената на множествата са главни латински букви: A, B и така нататък. При изреждане на елементите се ползват фигурните скоби "{" и "}", а имената на елементите са разделени със запетаи, например

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

Принадлежността към множество се означава с "$\in$", а непринадлежността с "$\notin$", например

$$a \in \{a, b, c\}, \qquad d \notin \{a, b, c\}$$

Редът на изброяване на елементите е без значение:

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

Многократни появи на име на елемент нямат значение:

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

Как означаваме множествата (2)

Следните две множества са **различни**:

$$A = \{a, b\} \qquad \text{и} \qquad B = \{\{a, b\}\}$$

A има точно два елемента: a и b. B има точно един елемент: множеството A.

Мнножества може да са елементи на други множества!

Следният запис не означава множество, понеже е е **синтактично неправилен**:

$$\{\{a, b\}$$

Фигурните скоби имат значение!

Нека $A = \{a, \{a, b\}, b\}$. Вярно е, че

$$a \in A$$
$$b \in A$$
$$\{a, b\} \in A$$

Но не е вярно, че

$$\{a\} \in A$$

тъй като нито един от елементите на A не е $\{a\}$. Наистина, A има елемент a, но вече знаем, че a и $\{a\}$ са съвършено различни обекти.

Историческа справка

През 19 век Gottlob Frege (The Foundations of Arithmetic, 1884) създава чисто логическа теория–основа на естествените числа, твърдейки, че аритметиката и дори цялата математика може да се разглежда като дял на логиката. Този възглед се казва *logicism*.

Frege дефинира естествените числа чисто логически.
Например, 3 е свойство на следните множества:

- $\{а, б, в\}$,
- множеството от моето собствено, бащино и фамилно име,
- множеството от образователните степени бакалавър, магистър и доктор,
- и други.

Безразборното ползване на "множество" води до парадокси (1)

През 1902 г. Bertrand Russell показва, че целият труд на Frege е неконсистентен, защото ползва "множество от множества" без ограничения.

Определение 3

Множество, което не съдържа себе си, е обикновено.
Множество, което съдържа себе си, е необикновено.

Примерът на Russell за необикновено множество:

> *The set of all those things that can be defined in less than 19 English words*

Тук ползваме само 16 думи, така че това множество е елемент на себе си.

Безразборното ползване на "множество" води до парадокси (2)

Определение 4

$\mathcal{O}$ *е множеството от всички обикновени множества.*

Дали $\mathcal{O}$ е обикновено, или е необикновено?

- Да допуснем, че $\mathcal{O}$ е обикновено. Съгласно Определение 4 то е множеството от **обикновените** множества, следователно $\mathcal{O}$ е елемент на себе си. Но това го прави необикновено съгласно Определение 3. ↯
- Да допуснем, че $\mathcal{O}$ е необикновено. Съгласно Определение 4 то е множеството от **обикновените** множества, следователно $\mathcal{O}$ не е елемент на себе си. Но това го прави обикновено съгласно Определение 3. ↯

Това е *парадоксът на Russell*.

Аксиома за обема

За да няма парадокси са въведени *аксиоми* за множествата. Стандартната аксиоматизация е на Zermelo-Fraenkel (ZF). В този курс разглеждаме само част от ZF.

Аксиома 1 (Аксиома за обема (extensionality))

Две множества са равни тстк съдържат едни и същи елементи.

$$\forall X\ \forall Y\ (\forall z(z \in X \leftrightarrow z \in Y) \rightarrow X = Y)$$

Веднага следва, че редът, в който са записани елементите на дадено множество, както и наличието на повторения на елементи, е без значение.

Аксиома за отделянето (separation) (1)

С предикат може да отделим подмножество от множество.

Аксиома 2 (Аксиома за отделянето (separation))

Ако X е множество и π е предикат с домейн X, то съвкупността Y от елементите на X, които имат свойството π, е множество.

$$\forall X \, \exists Y \, \forall z \, (z \in Y \leftrightarrow \pi(z))$$

Конструкторска нотация (*set constructor notation* или *set builder notation*) за записване на "отделени множества":

$$Y = \{a \in X \mid \pi(a)\} \text{ е множество}$$

Изразът в скобите се чете "всички a от X, за които $\pi(a)$".
Алтернативен запис е

$$Y = \{a \in X \, : \, \pi(a)\} \text{ е множество}$$

Аксиома за отделянето (separation) (2)

Нека A е множество, π е предикат над него и $B = \{a \in A : \pi(a)\}$. Казваме, че B е *подмножество* на A и пишем

$$B \subseteq A$$

Понякога пишем $A \supseteq B$ и казваме, че A е *надмножество* на B.

От особен интерес са следните два екстремни случая:

- $\forall a \in A : \pi(a)$. В този случай $B = A$. Виждаме, че всяко множество е подмножество на себе си. Неслучайно символът "$\subseteq$" прилича на "$\leqslant$".
- $\neg\exists a \in A : \pi(a)$. В този случай B няма елементи. Казваме, че B е *празното множество* и пишем $B = \varnothing$ или $B = \{\}$. Празното множество е подмножество на всяко множество, включително и на себе си.

Аксиома за отделянето (separation) (3)

Забележете разликата между $\varnothing$ и $\{\varnothing\}$! Второто не е празното множество, а множеството, чийто единствен елемент е празното множество. В сила са

$$\varnothing \subseteq \{\varnothing\} \tag{1}$$
$$\varnothing \in \{\varnothing\} \tag{2}$$

но по различни причини. $\varnothing$ е подмножество на всяко множество, така че (1) е вярно независимо от множеството вдясно, докато (2) е вярно само защото множеството вдясно има елемент $\varnothing$.

Интересен е и случаят, в който $B \subseteq A$, но $B \neq A$. Тогава казваме, че B е *същинско* подмножество на A и пишем $B \subset A$, като "$\subset$" прилича на "$<$". За да е изпълнено $B \subset A$, то трябва да съществува $a \in A$, такъв че $a \notin B$. Понякога казваме, че A е същинско надмножество на B и пишем $A \supset B$.

Аксиома за степенното множество (powerset)

Аксиома 3 (Аксиома за степенното множество)

За всяко множество X съществува множеството от всички негови подмножества, което наричаме степенното множество на X

$$\forall X\, \exists Y\, \forall z\, (z \in Y \leftrightarrow z \subseteq X)$$

На английски казваме *the power set*. Степенното множество на X бележим с 2^X или $\mathcal{P}(X)$ или $\mathrm{pow}(X)$.

Примери:

- Нека $X = \varnothing$. Тогава $2^X = \{\varnothing, \varnothing\} = \{\varnothing\}$.
- Нека $X = \{a, b, c\}$. Тогава

$$2^X = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Максималност по включване (1)

Нека е дадено множество A и предикат σ върху 2^A (предикатът е върху подмножествата на A, а не върху елементите на A!).

Определение 5

За всяко $B \subseteq A$, казваме, че B е максимално по включване по отношение на σ, ако

1. $\sigma(B)$ *и*
2. $\forall C(B \subset C \subseteq A \rightarrow \neg\sigma(C))$

На чист български, максимално по включване подмножество е такова, за което свойството (предикатът) е в сила, но то не е в сила за никое същинско негово надмножество.

За да говорим за максималност по включване, трябва да имаме предвид свойство (предикат). Без свойство, това понятие няма смисъл.

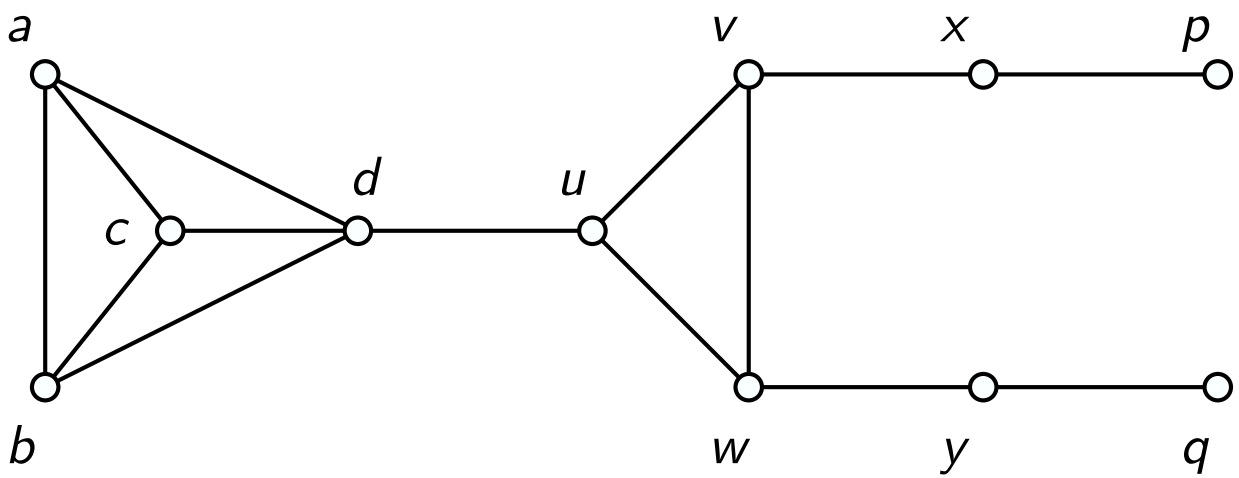
Максималност по включване (2)

На английски има елегантно терминологично разграничение между “максимално по включване” и “глобално максимално”:

1. “максимално по включване” е *maximal*,
2. а “глобално максимално” е *maximum*.

На български няма аналогична терминологична разлика, базирана на различни суфикси.

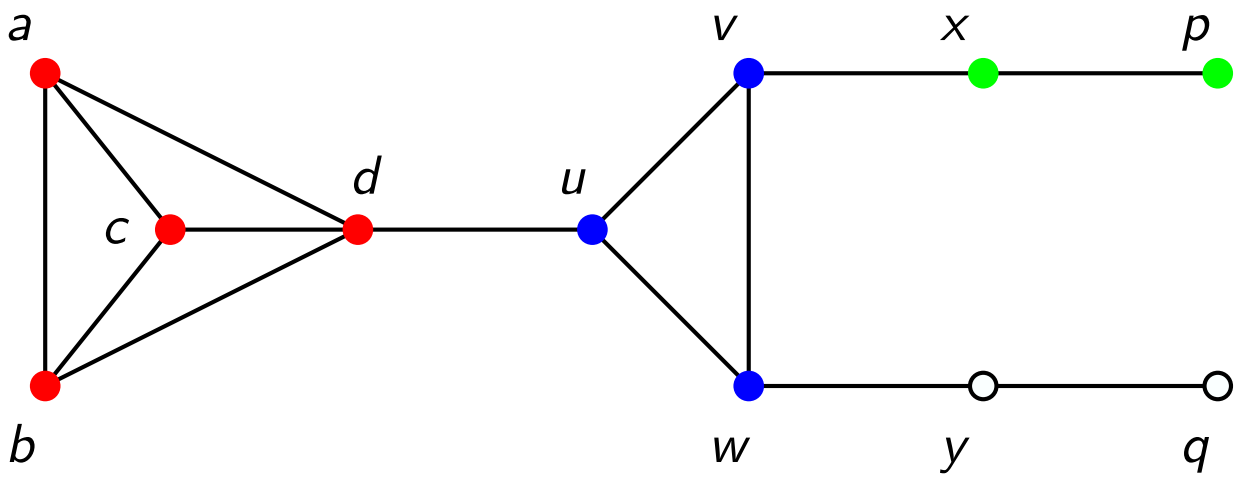
Граф е обект, който се състои от *върхове* и *ребра*. Ето примерна рисунка на граф, като върховете са точките, а ребрата са отсечките:



Максималност по включване: пример с клика в графи

Какво е клика (1)

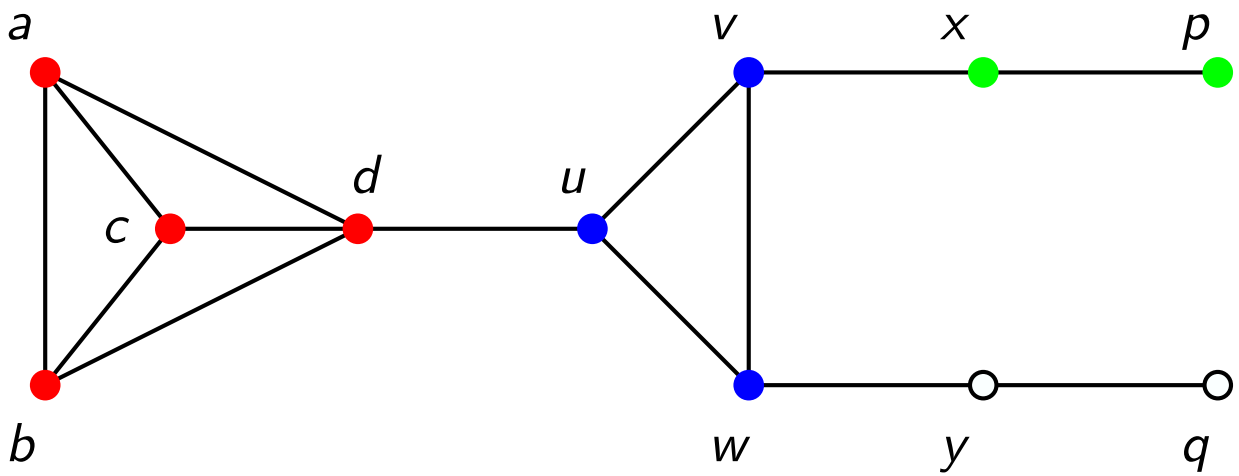
Клика е множество от върхове, всеки два от които са свързани с ребро. Всеки връх е (тривиална) клика. Краищата на всяко ребро представляват клика; примерно, $\{x, p\}$ и $\{v, x\}$ са клики. Освен това, в примера $\{u, v, w\}$ е клика и $\{a, b, c, d\}$ е клика.



Максималност по включване: пример с клика в графи

Какво е клика (2)

$\{a, b, c, d\}$ е най-голямата клика – друга клика с четири върха няма. Ясно е защо $\{a, b, c, d\}$ е максимална клика.
Дали $\{u, v, w\}$ е максимална клика в **някакъв смисъл**?



Да: към $\{u, v, w\}$ не може да добавим връх, запазвайки свойството множеството да е клика.
$\{a, b, c, d\}$ е **maximum**, докато $\{u, v, w\}$ е **maximal**.

Нека е дадено множество A и предикат σ върху 2^A.

Определение 6

За всяко $B \subseteq A$, казваме, че B е минимално по включване по отношение на σ, ако

1. $\sigma(B)$ *и*
2. $\forall C(C \subset B \to \neg\sigma(C))$

На чист български, минимално по включване подмножество е такова, за което свойството (предикатът) е в сила, но то не е в сила за никое същинско негово подмножество.

За да говорим за миниималност по включване, трябва да имаме предвид свойство (предикат). Без свойство, това понятие няма смисъл.

Операции върху множества

Дефинираме няколко основни операции (действия) върху множества: обединение, сечение, разлика, симетрична разлика, допълнение.

Нека A и B са множества.

Определение 7

Обединението на A и B е множеството:

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

Обединението е аналог на логическия съюз дизюнкция.

Пример:

$$\{a, b, c, d\} \cup \{a, b, x, y\} = \{a, b, c, d, x, y\}$$

Определение 8

Сечението на A и B е множеството:

$$A \cap B = \{a \,|\, a \in A \wedge a \in B\}$$

Сечението е аналог на логическия съюз конюнкция. Сечението е комутативно.

Пример:

$$\{a, b, c, d\} \cap \{a, b, x, y\} = \{a, b\}$$

Определение 9

Разликата A без B е множеството:

$$A \backslash B = \{a \mid a \in A \wedge a \notin B\}$$

Разликата е аналог на логическия съюз импликация; по-точно, отрицание на импликация. Разликата не е комутативна.

Пример:

$$\{a, b, c, d\} \backslash \{a, b, x, y\} = \{c, d\}$$

Определение 10

Симетричната разлика на A и B е множеството:

$$A \triangle B = \{a \mid a \in A \oplus a \in B\}$$

Симетричната разлика е аналог на логическия съюз изключващо-или. Тя е комутативна.

Пример:

$$\{a, b, c, d\} \triangle \{a, b, x, y\} = \{c, d, x, y\}$$

Определение 11

Нака е дадено универсално множество, или универсум, U. Допълнението на A до U е множеството:

$$\overline{A^U} = \{a \mid a \in U \wedge a \notin A\}$$

Ако U се подразбира, пишем просто "$\overline{A}$".

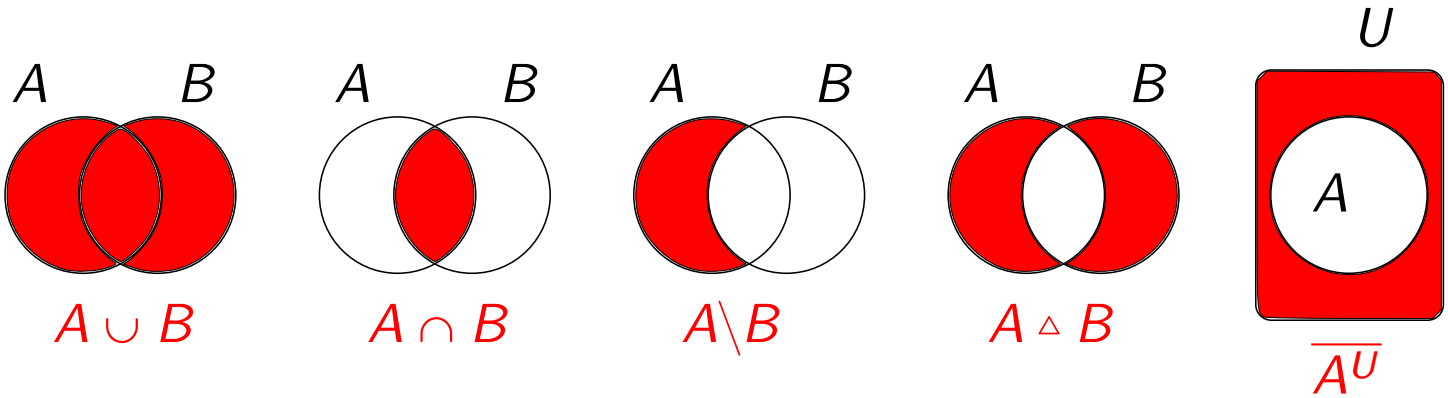
Разликата е аналог на логическия съюз отрицание.

Пример: ако $U = \{a, b, c, d, e, f, g, h\}$, то

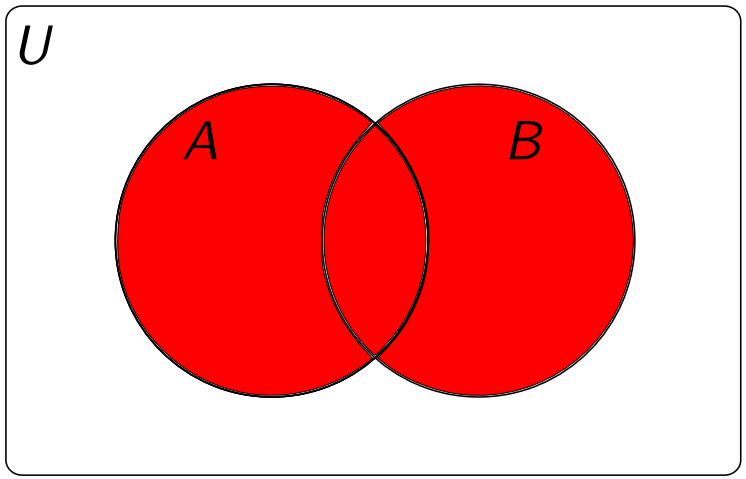
$$\overline{\{a, b, c, d\}} = \{e, f, g, h\}$$

ВАЖНО: най-голям универсум **няма**.

При две множества: две окръжности в общо положение.

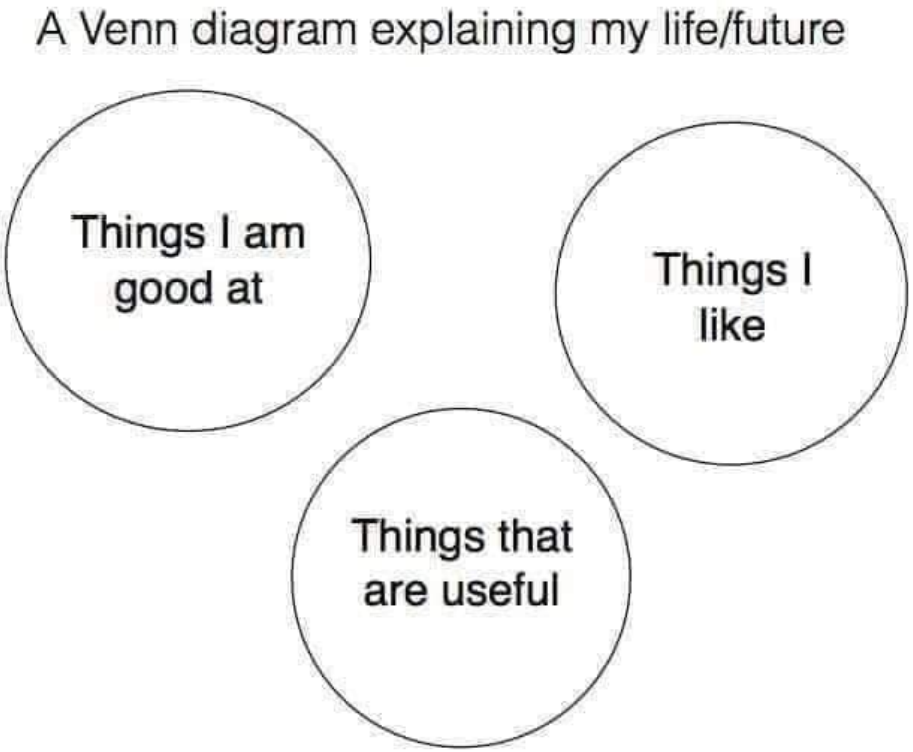


Ако е нарисуван и универсумът, районите са точно 2^n при n множества. Ето илюстрация на обединението: три от четирите района са включени в $A \cup B$, съответно един район (външният) не е включен.



Диаграми на Venn в частни случаи

Ако окръжностите не са в общо положение, то диаграмата на Venn моделира ситуация, за която се знае предварително, че има особености (а не е най-общата възможна).



Свойства на операциите върху множества (1)

Напълно аналогични на съответните свойства на логическите съюзи. Примерно, обединението и сечението са идемпотентни, комутативни и асоциативни, понеже съответно дизюнкцията и конюнкцията са такива:

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

Обединетието и сечението дистрибутират едно спрямо друго:

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

Свойства на операциите върху множества (2)

Свойствата на константите се пренасят директно върху операции с множества, ако празното множество съответства на $\mathtt{F}$, а универсумът съответства на $\mathtt{T}$:

$$A \cup \varnothing = A, \quad A \cap \varnothing = \varnothing, \quad A \cup U = U, \quad A \cap U = A$$

Законът за двойното отрицание от логиката има следният аналог:

$$\overline{\overline{A}} = A$$

Свойства на операциите върху множества (3)

Аналозите на законите на De Morgan са

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Свойства на операциите върху множества (4)

Асоциативните операции като обединение и сечение може да се обобщават недвусмислено така за $k > 2$:

$$A_1 \cup A_2 \cup \cdots \cup A_k$$
$$A_1 \cap A_2 \cap \cdots \cap A_k$$

Ползваме следната нотация:

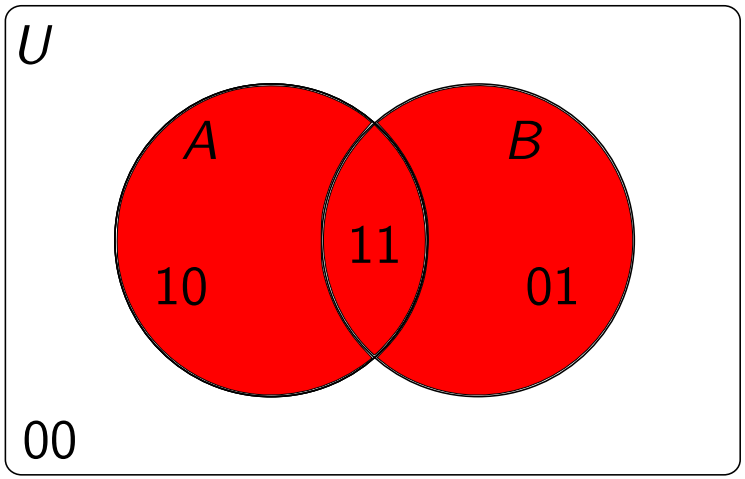
$$\bigcup_{i=1}^{k} A_i = A_1 \cup A_2 \cup \cdots \cup A_k$$
$$\bigcap_{i=1}^{k} A_i = A_1 \cap A_2 \cap \cdots \cap A_k$$

Основните операции, представени с таблица:

A	B	$A \cup B$	$A \cap B$	$A \setminus B$	$A \triangle B$	$\overline{A}$
0	0	0	0	0	0	1
0	1	1	0	0	1	1
1	0	1	0	1	1	0
1	1	1	1	0	0	0

Има директно съответствие на таблиците на логическите съюзи.

Интерпретация на таблицата – например за дизюнкцията. Има четири района 00, 01, 10, 11. Например, 01 означава подмножеството от елементите, непринадлежащи на A и принадлежащи на B (допускаме наредба, при която A е вляво от B).



A	B	$A \cup B$
0	0	0
0	1	1
1	0	1
1	1	1

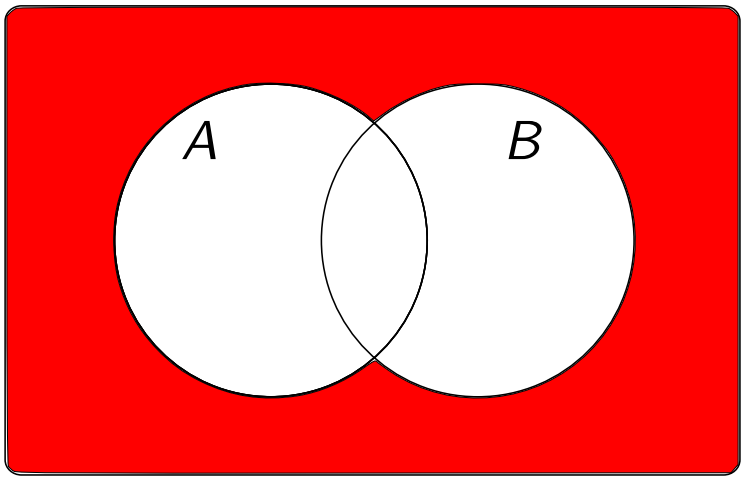
Доказателства на равенства на множества

Един от законите на De Morgan, таблично

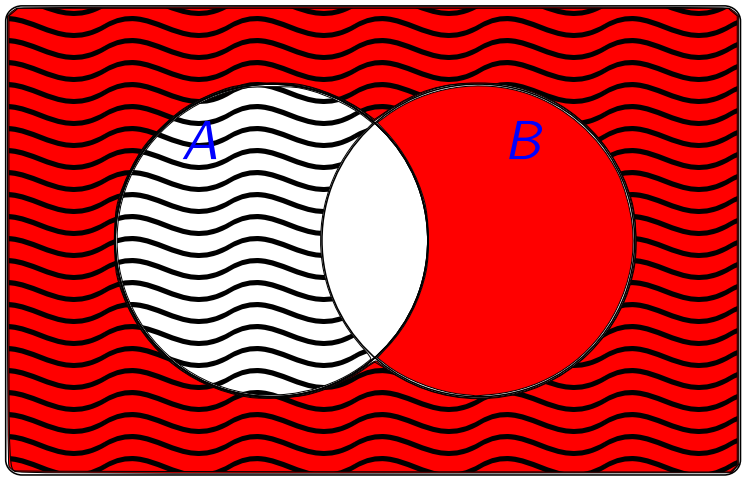
A	B	$A \cup B$	$\overline{A \cup B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cap \overline{B}$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

От равенството на четвъртата и седмата колона отляво надясно следва, че $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

$\overline{A \cup B}$



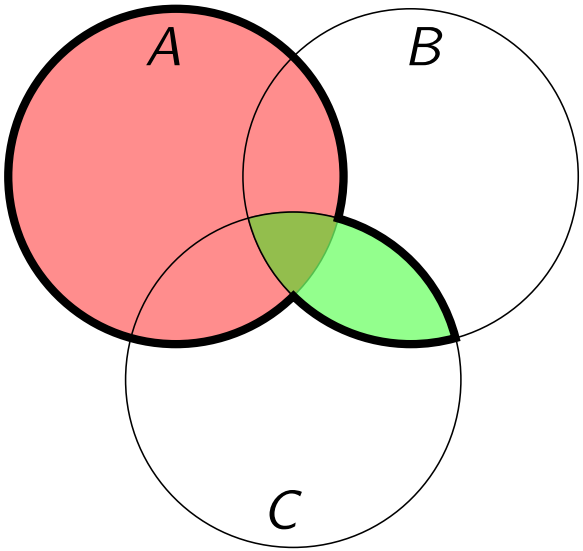
$\overline{A} \cap \overline{B}$



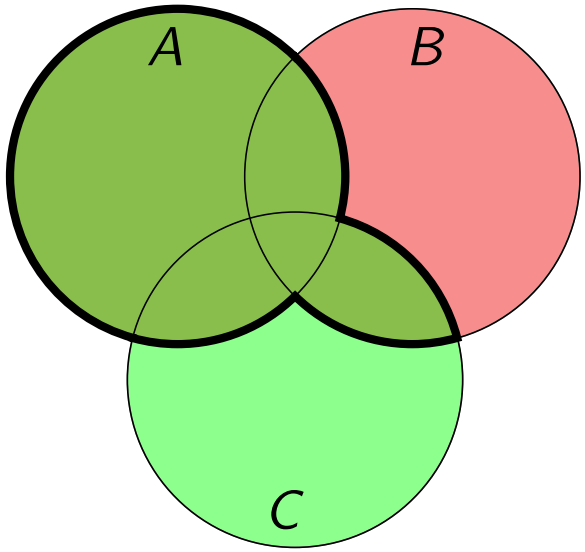
И двата израза определят едно и също множество от райони, а именно "външният" район с адрес 00.

Диаграми на Venn за три множества
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cup (B \cap C)$



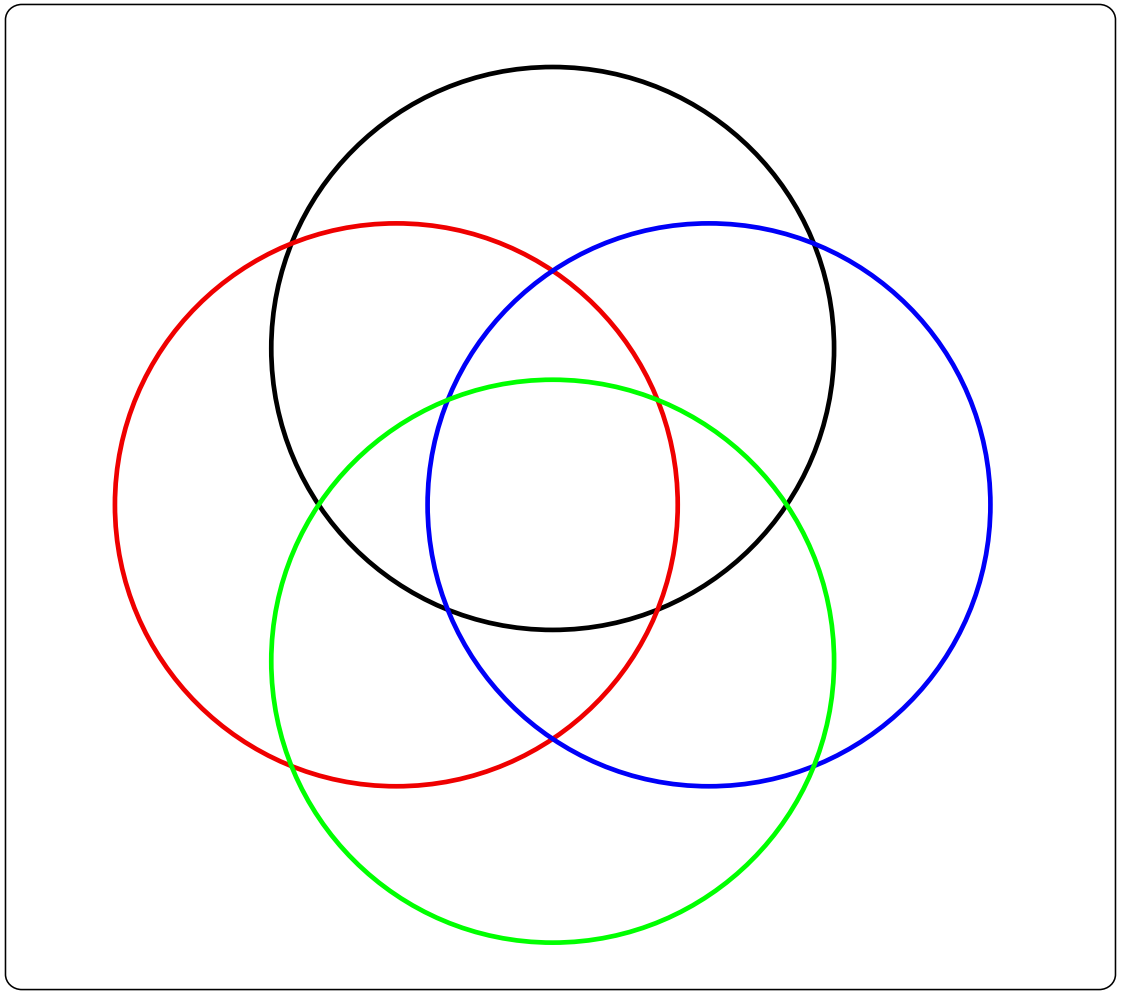
$(A \cup B) \cap (A \cup C)$



Диаграми на Venn за четири множества (1)

С окръжности не може

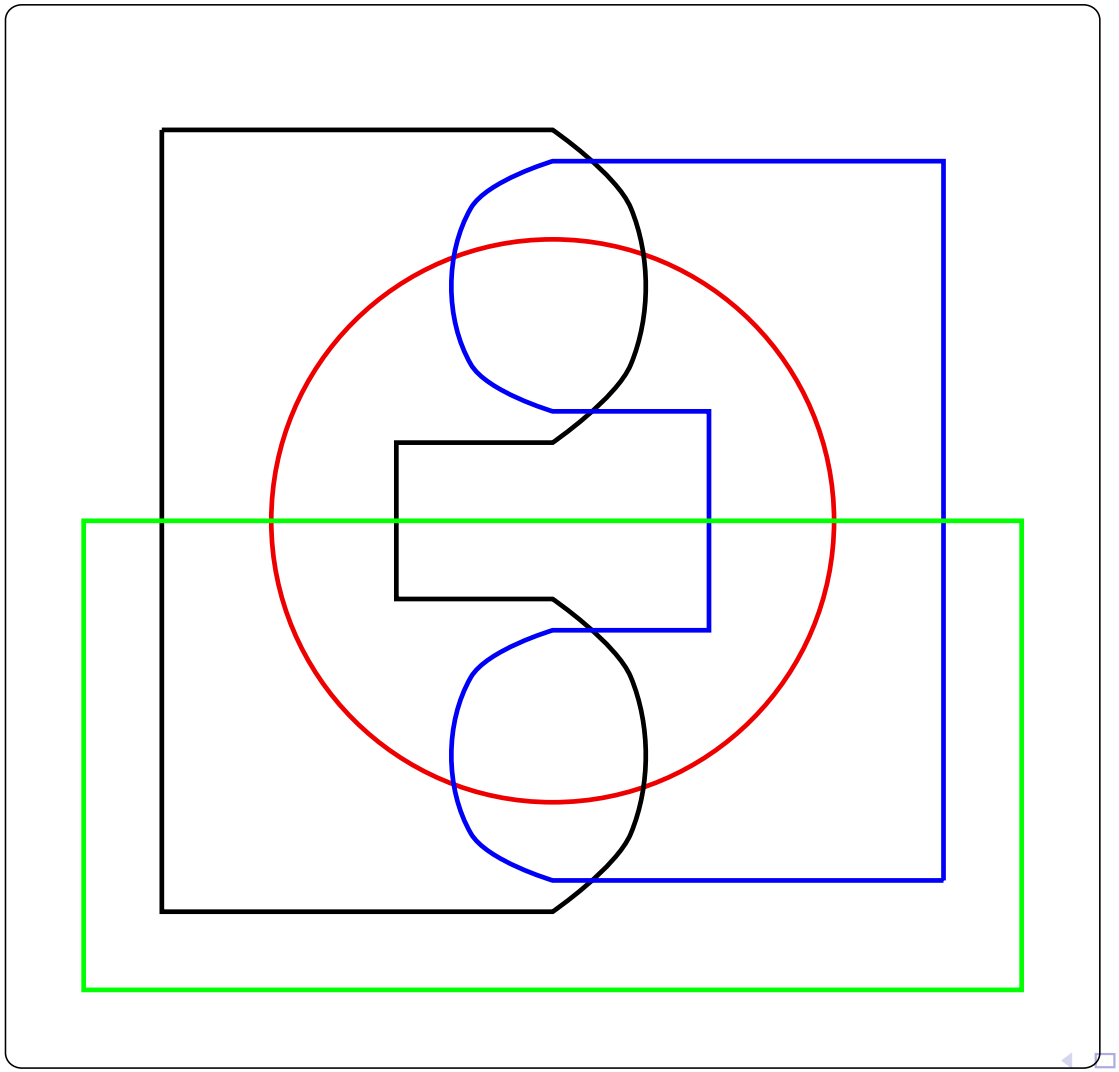
Не може да е диаграма на Venn за общия случай: има само 14 района. Липсват само-синьо-червен и само-черно-зелен.



Диаграми на Venn за четири множества (1)

С фигури, които не са непременно изпъкнали, може

Всички 16 района са налице.



Диаграмите на Venn не са формални доказателства

Диаграмите на Venn са чудесно средство за онагледяване и получаване на интуиция. Те обаче **не са** формални символни доказателства, каквото са таблиците или еквивалентните преобразувания.

Искаме да въведем наредба – това е полезно и смислено. Примерно, има два елемента a и b и искаме да кажем, че a е вляво от, или преди, b.

Как да го направим? "Ляво" и "дясно" са неформални поянтия. Лесно можем да въведем нотацията за наредба (a, b), но как да кажем формално какво означава това?

Не искаме да въвеждаме ново първично понятие и нова първична нотация. "(a, b)" би трябвало да може да се изрази в езика на теорията на множествата.

Наредена двойка (ordered pair)

Дефиниция на Kuratowski

Определение 12

Всяко множество $\{\{a\}, \{a, b\}\}$ наричаме наредена двойка с първи елемент a и втори елемент b. Краткият запис е "(a, b)".

Тъй като дефиницията ползва множество, със същия успех можехме да напишем $\{\{a, b\}, \{a\}\}$ и така нататък.

Основното свойство на наредените двойки

Следният важен резултат приемаме без доказателство.

Теорема 1

$(a, b) = (c, d)$ *тстк* $a = c$ *и* $b = d$.

Наредена тройка, четворка, . . . , k-торка

Без формални обяснения приемаме, че понятията "наредена тройка" и така нататък имат очевиден смисъл. Нотациите са:

- (a, b, c) за наредена тройка (triple).
- (a, b, c, d) за наредена четворка (quadruple).
- $(a_1, a_2, \ldots, a_k)$ за наредена k-орка (k-tuple).

Декартово произведение

Нека A и B са множества. *Декартовото произведение на A и B* (Cartesian product) е множеството

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Пример: нека $A = \{1, 2\}$ и $B = \{a, b, c\}$. Тогава

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$
$$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

В общия случай $A \times B \neq B \times A$. Тоест, операцията не е комутативна. Тя не е и асоциативна – защо?

Обобщено Декартово произведение

Чрез неформално въведените понятия наредена тройка, наредена четворка и наредена k-торка можем да направим следните дефиниции. Нека A, B, C, D, A_1, A_2, $\ldots$, A_k са множества.

$$A \times B \times C = \{(a, b, c) \mid a \in A \wedge b \in B \wedge c \in C\}$$
$$A \times B \times C \times D = \{(a, b, c, d) \mid a \in A \wedge b \in B \wedge c \in C \wedge d \in D\}$$
$$A_1 \times A_2 \times \cdots \times A_k = \{(a_1, a_2, \ldots, a_k) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_k \in A_k\}$$

Може да пишем "$\bigtimes_{i=1}^{k} A_i$" вместо "$A_1 \times A_2 \times \cdots \times A_k$".

Фамилия

В аксиоматиката ZF всичко е множество. Ние приемаме различен възглед: има протоелементи, които обикновено бележим с малки букви като a, b и така нататък; протоелементите **не са множества**, а множествата изграждаме от протоелементи и/или други множества, примерно $\{a, \{b\}\}$.

Множество от множества ще наричаме *фамилия* (family). Множеството от протоелементите, които може да се появяват, се нарича *опорното множество* (ground set). Като пример, нека опорното множество е $A = \{a, b, c, d\}$. Фамилии над A са, примерно,

$$X = \{\{a, b\}, \{a, c, d\}, \{b, d\}, \{d\}\}$$
$$Y = \{\{a, d\}\}$$
$$W = \{\emptyset\}$$
$$Z = \{\} = \emptyset$$

Разбиване и покриване на множество

Нека A е непразно опорно множество. *Покриване на* A (set cover) е всяка фамилия $X = \{X_1, X_2, \ldots, X_k\}$, такава че $k \geqslant 1$ и:

1. $\forall i \in \{1, 2, \ldots, k\} : X_i \subseteq A$,
2. $\forall i \in \{1, 2, \ldots, k\} : X_i \neq \varnothing$,
3. $\bigcup_{i=1}^{k} X_i = A$.

Ако освен това е вярно, че

4. $\forall i \forall j (1 \leqslant i < j \leqslant k \rightarrow X_i \cap X_j = \varnothing)$

казваме, че X е *разбиване* (set partition) на A.

Пример за разбиване и покриване на множество

Нека $A = \{a, b, c, d\}$. Покриване на A е, примерно,

$$\{\{a, b, d\}, \{b, c\}, \{a, b, c, d\}\}$$

Разбиване на A е, примерно,

$$\{\{a, c\}, \{b\}, \{d\}\}$$

Нотации върху фамилии

Нека X е фамилия над A. Тогава "$\bigcup X$" означава обединението на множествата-елементи на X:

$$\bigcup X = \{a \mid \exists S \in X : a \in S\}$$

Забележете, че тази нотация не може да се използва, ако X не е фамилия, тоест, ако X има елементи, които не са множества (а са протоелементи).

Дуалната нотация е "$\bigcap X$":

$$\bigcap X = \{a \mid \forall S \in X : a \in S\}$$

Аксиома за индукцията

Тази аксиома не е част от ZF. Удачно е да мислим за нея като за конструкция, или безкрайна процедура, която генерира множество, стартирайки от някаква база и прилагайки итеративно някакви операции.

Аксиома 4 (Аксиома за индукцията)

Нека е дадено непразно множество M_0, което наричаме базово множество, и непразно множество от операции $\mathcal{F}$, приложими в тази конструкция.

- *Включваме елементите на M_0 в M, тоест, $M \leftarrow M_0$.*
- *Прилагаме неограничено следното:*
  - *Нека M' е множеството от елементите, които се получават при всевъзможните прилагания на операциите от $\mathcal{F}$ върху текущото M;*
  - *Добавяме M' към M, тоест, $M \leftarrow M \cup M'$.*

Така полученото M е множество. Пишем $M = (M_0, \mathcal{F})$.

Индуктивно генерирани множества. Пример с $\mathbb{N}$. (1)

Множества, дефинирани чрез безкрайната процедура от аксиомата за индукцията, са *индуктивно генерирани множества*.

Най-простият пример за индуктивно генерирано множество е множеството $\mathbb{N}$ от естествените числа. При него $M_0 = \{0\}$, а $\mathcal{F}$ съдържа една единствена операция: добавяне на единица. На английски наричат тази операция *successor operation*, поради което е удачно да я бележим със "succ"; примерно, $\text{succ}(0) = 1$, $\text{succ}(1) = 2$, $\text{succ}(99) = 100$ и така нататък.

Индуктивно генерирани множества. Пример с $\mathbb{N}$. (2)

Съгласно казаното дотук, нулата е естествено число, защото конструкцията на $\mathbb{N}$ започва с $\{0\}$.

- Прилагайки операцията succ по всевъзможните начини към $\{0\}$, получаваме 1. Добавяме 1 към $\mathbb{N}$ и то вече съдържа 0 и 1.
- Прилагайки операцията succ по всевъзможните начини към $\{0, 1\}$, получаваме 1 и 2. Добавяме 1 и 2 към $\mathbb{N}$ и то вече съдържа 0, 1 и 2.
- Прилагайки операцията succ по всевъзможните начини към $\{0, 1, 2\}$, получаваме 1, 2 и 3. Добавяме 1, 2 и 3 към $\mathbb{N}$ и то вече съдържа 0, 1, 2 и 3.
- И така нататък.

Пишем $\mathbb{N} = \{0, 1, 2, \ldots, \}$, като "..." в десния край казва, че тази последователност е безкрайна.

Доказателствата по индукция са мощно средство. Те имат ключова роля в дискретната математика.

Типичната ситуация е такава. Даден е предикат $P(n)$ и трябва да докажем $\forall n \in \mathbb{N} : P(n)$. Схемата на доказателствата по индукция върху естествените числа е следната.

- Доказваме $P(0)$, като просто проверяваме истинността на предиката за $n = 0$.
- Допускаме $P(n)$ за **произволно** $n \in \mathbb{N}$ и въз основа на това допускане доказваме $P(n + 1)$.

Даден е предикат $P(n)$ и трябва да докажем $\forall n \in \mathbb{N} : P(n)$. Схемата на доказателствата със силна индукция върху естествените числа е следната.

- Доказваме $P(0)$, като просто проверяваме истинността на предиката за $n = 0$.
- Допускаме, че за **произволно** $n \in \mathbb{N}$ е изпълненено:
  - $P(0)$,
  - $P(1)$,
  - $\ldots$,
  - $P(n)$.

  Въз основа на всички тези допускания доказваме $P(n+1)$.

Пример за доказателство със силна индукция.

Теорема 2

Всяко естествено число, по-голямо или равно на 2, е произведение на едно или повече прости числа.

Даказателство: Ще докажем теоремата със силна индукция. Базата е $n = 2$ (а **не** $n = 0$). Твърдението за стойност на аргумента 2 е тривиално вярно: 2 е произведение на едно просто число, а именно 2. С това доказахме базовия случай.

Индуктивното предположение е, че за произволно $n \geqslant 2$ е вярно, че за всяко $k \in \{2, 3, \ldots, n\}$ е вярно, че k е произведение от едно или повече прости числа.

В индуктивната стъпка разлеждаме твърдението за стойност на аргумента $n+1$. Следните подслучаи са изчерпателни:

- $n+1$ е просто. Тогава $n+1$ се явява произведение на едно просто число.
- $n+1$ е съставно. Тогава по дефиниция $n+1 = p \cdot q$, където $p, q \in \{2, 3, \ldots, n\}$. Съгласно индуктивното предположение, и p, и q са произведения от едно или повече прости числа. Тогава $n+1$ е произведение от едно или повече прости числа. **QED**

Силната индукция е еквивалентна на обикновената (и се казва "силна" по дидактични причини). Ако дефинираме предиката $Q(n)$ така:

$$P(k) \text{ е в сила за } k \in \{0, 1, \ldots, n\}$$

то да докажем $P(n)$ със силна индукция е същото като да докажем $Q(n)$ с обикновена индукция.

В по-общия случай доказваме предикат $P(x)$, където домейнът е някакво индуктивно дефинирано множество $M = (M_0, \mathcal{F})$. Схемата е следната:

- За всеки елемент x от M_0 проверяваме истинността на $P(x)$.
- Допускаме $P(x)$ за **произволно** $x \in M$ и въз основа на това допускане доказваме, че за всеки y, който се получава при прилагането на операциите от $\mathcal{F}$ върху текущото M, $P(y)$ е вярно.

Тази индукция се казва *структурна индукция*, на английски е *structural induction*, и се прилага широко в области като теорията на графите.

Мултимножества (1)

Неформално: *мултимножество* (*multiset*) е нещо като множество, но многократните появи на даден елемент са от значение. Примерно, мултимножеството от три единици и една двойка е различно от мултимножеството от две единици и една двойка.

При мултимножествата няма наредба, също като в обикновените множества няма наредба.

Няма утвърдена нотация за мултимножествата. Авторът ползва нотация с фигурни скоби, но с един субскрипт "M":

$$\{1, 1, 1, 2\}_M$$

И така, $\{1, 1, 1, 2\}_M = \{1, 2, 1, 1\}_M$, но $\{1, 1, 1, 2\}_M \neq \{1, 2, 1\}_M$.

Мултимножества (2)

Можем спокойно да минем без понятието “мултимножество”. То изглежда обобщение на “множество”, но можем да ползваме “множество” и “кратност”, за да изразим това, което изразяваме чрез “мултимножество”.

От друга страна, “мултимножество” е много удобно и ще се ползва в изложението за комбинаторни конфигурации (структури) и рекуренти уравнения. Единствената операция, която въвеждаме за мултимножества, е обединение. То е подобно на обединението на обикновени множества, но кратностите се сумират. Примерно,

$$\{a, a, b, c, c, d\}_M \cup \{a, b, b, f\}_M = \{a, a, a, b, b, b, c, c, d, f\}_M$$

Мултимножества и фамилии

Някои автори дефинират "фамилия над дадено опорно множество A" като **мултимножество**, чиито елементи-множества са подмножества на A. Това означава, че фамилия може да има повтарящи се елементи, което на свой ред влече, че ако A е *крайно* множество (понятие, което все още не сме дефинирали формално!) с n елемента, не може да дадем горна граница за броя на фамилиите над A.

За целите на тези лекции, фамилиите са множества (което означава, че нямат повтарящи се елементи) и, ако A има n елемента, то има най-много 2^{2^n} фамилии над A и тази граница е точна. Защо това е така, ще видим в следваща лекция.

КРАЙ