Ivan Treshchev

Discrete Math

for students of technical specialties

Ivan Treshchev

Discrete Math. For students of technical specialties

http://www.litres.ru/pages/biblio_book/?art=54975664
ISBN 9785449876010

Аннотация

The manual is intended for students of the specialty information security of automated systems when studying the course “Discrete mathematics”, and can also be used by students of other specialties studying similar courses.The author would like to express gratitude to his supervisor A. Khusainov and Mikhailova N.N.

Содержание

Discrete Math
For students
of technical specialties

Ivan Treshchev

Assistnt Anastasiya Sergeevna Vatolina

ISBN 978-5-4498-7601-0
Created with Ridero smart publishing system

Introduction

The tutorial is devoted to the consideration of theoretical issues in the framework of the course «Discrete Mathematics». The basic theoretical information on finite mathematics for students in the study of relevant courses, the principles of constructing mathematical models and methods for their analysis are presented. The manual can be useful not only to students of technical specialties and specialties associated with the design of information systems and the development of software modules, but also to students of humanitarian specialties. The sections discussed in the manual fully reflect the necessary material.

The main focus of the manual is on the set-theoretic approach. The basic information on combinatorics, coding theory and mathematical modeling, graph theory is presented. Many theses are illustrated clearly.

1. PLURALITY

1.1. Definitions and examples

The concept of set is one of the fundamental concepts of mathematics. The set is known, at least, that it consists of elements.

By the set S we mean any collection of defined and distinguishable objects, conceivable as a whole. These objects are called elements of the set S. As examples of the sets, one can cite: the set of students present at the lecture, the set of even numbers, etc. Usually, sets are indicated in capital letters of the Latin alphabet: $A, B, C, \ldots$; and the elements of sets are in lower case: $a, b, c, \ldots$

If the object x is an element of the set M, then they say that x belongs to M: $x \in M$. Otherwise, they say that x does not belong to M: $x \notin M$.

A set A is called a subset of B if every element of A is an element of B. If A is a subset of B and B is not a subset of A, then they say that A is a strict (proper) subset of B. In the first case, denote: $A \# B$, in the second: $A \subset B$.

Note that the symbol $\in$ defines the relationship between some element and the set, and the symbol # defines the relationship between the sets, one of which is a subset of the other. So, it is

not true that $1 \in \{\{1\}, \{2\}\}$, or that $\{1\} \# \{\{1\}, \{2\}\}$; it is true that $\{1\} \in \{\{1\}, \{2\}\}$ and $\{\{1\}\} \# \{\{1\}, \{2\}\}$. This example illustrates the difference between membership and inclusion.

For arbitrary sets X, Y, Z the following relations are true:

– $X \# X$;

– if $X \# Y$, $Y \# Z$, then $X \# Z$;

– if $X \# Y$, $Y \# X$, then $X = Y$.

A set containing no elements is called empty, denoted as: $\varnothing$. It is a subset of any set. The set U is called universal, that is, all the sets under consideration are its subset.

We consider two definitions of equality of sets.

– The sets A and B are considered equal if they consist of the same elements, then they write: $A = B$ and $A \neq B$ – otherwise.

– The sets A and B are considered equal if: $A \subset B$, $B \subset A$.

The power of a finite set A is the number of its elements. The power sets are denoted by $| A |$. Note that $| \varnothing | = 0$, $| \{\varnothing\} | = 1$. Sets are called equipotent if their powers coincide.

The degree-set (boolean) of A is the set 2^A (the alternative notation is $P(A)$) of all its subsets.

Theorem. If the set A contains n elements, then the set $P(A)$ contains 2^n elements. In this regard, the notation of the set-degree of the set A in the form 2^A is also used.

Proof 1: by induction. Base: if $| M | = 0$, then $M = \varnothing$ and $2^{\varnothing} = \{\varnothing\}$. Therefore: $| 2^{\varnothing} | = | \{\varnothing\} | = 1 = 2^0 = 2^{| \varnothing |}$. Induction transition: let $\forall M \, | M | < k \Rightarrow | 2^M | = 2^{| M |}$

Consider: $M = \{a_1, \ldots, a_k\}$, $| M | = k$. Put: $M_1 = \{X \subset 2^M \# | a_k \in X\}$ and $M_2 = \{X \subset 2^M \dashv | a_k \notin X\}$.

We have: $2^M = M_1 \cup M_2$ and $M_1 \cap M_2 = \varnothing$.

By the induction hypothesis: $| M_1 | = 2^{k-1}$, $| M_2 | = 2^{k-1}$.

Therefore: $| 2^M | = | M_1 | + | M_2 | = 2^{k-1} + 2^{k-1} = 2 * 2^{k-1} = 2^k = 2^{|M|}$

THEOREM IS PROVEN

Proof 2: Suppose there is some set $\{a_1, a_2 \ldots a_n\}$. To each subset of this set we associate a sequence consisting of zeros and ones, where *0* – means that the *n*-th element is not, and *1* – means that it is.

We get:

00 … 00

00 … 01

00 … 11

…

11 … 11

Obviously, there are only 2^n such sequences.

THEOREM IS PROVEN

For example, there is some set A = {1, 2, 3}. Consider the set of all its subsets. Obviously, there are only 2^n such representations, in this case n = 3.

1.2. Ways to Define Sets

The sets are set:

by listing the elements: $M = \{a_1, a_2, \ldots, a_k\}$, i.e., a list of its elements;

characteristic predicate: $M = \{x|P(x)\}$ – a description of the characteristic properties that its elements must possess;

generative procedure: $M = \{x|x=f\}$, which describes a method for obtaining elements of a set from already obtained elements or other objects. In this case, the elements of the set are all objects that can be constructed using such a procedure. For example, the set of all integers that are powers of two.

When defining sets by enumeration, the notation of elements is usually enclosed in curly brackets and separated by commas. By enumeration, only finite sets can be specified (the number of elements in the set is finite, otherwise the set is called infinite). A characteristic predicate is a condition expressed in the form of a logical statement or procedure that returns a logical value. If the condition is satisfied for a given element, then it belongs to the set being defined, otherwise it does not. A generating procedure is a procedure that, when launched, generates some objects that are elements of a defined set. Infinite sets are given by a characteristic predicate or generating procedure.

Examples:

$M = \{1, 2, 3, 4\}$. – enumeration of elements of the set.

M = {m| m ∈ N and ≤ 10} – is a characteristic predicate.

Tribonacci numbers are specified by the conditions (generative procedure): $a_0=0, a_1=1, a_2=2, a_n=a_{n-1}+ a_{n-2}+ a_{n-3}$, for n> 3

1.3. Set Operations

Operations on sets are considered to obtain new sets from existing ones.

The union of the sets A and B is the set consisting of all those elements that belong to at least one of the sets A, B (Fig. 1.1): $A \cup B = \{x \mid x \in A \vee x \in B\}$.

The intersection of sets A and B is the set consisting of all those and only those elements that belong simultaneously to both the set A and the set B (Fig. & 1.2): $A \cap B = \{x \mid x \in A \wedge x \in B\}$.

The difference between the sets A and B is the set of all those and only those elements A that are not contained in B (Fig. 1.3): $A \backslash B = \{x \mid x \in A \text{ and } x \notin B\}$,

The symmetric difference of sets A and B is the set of elements of these sets that belong either to the set A or to the set B, but do not belong to their intersection (Fig. & 1. 4): $A+B= \{x \mid x \in A, \text{ or } x \in B, x \notin A \cap B\}$,

Absolute complement (negation) of the set A is the set of all those elements that do not belong to the set A (Fig. & 1. 5): $\bar{A}=U \backslash A$,

1.4. Set Operations Properties

For arbitrary sets *A*, *B*, and *C*, the following relations are true.

Commutativity of the union: $A \cup B = B \cup A$,

Commutativity of the intersection: $A \cap B = B \cap A$,

Associativity of the union: $A \cup (B \cup C) = (A \cup B) \cup C$,

Associativity of the intersection: $A \cap (B \cap C) = (A \cap B) \cap C$,

Distribution of the union with respect to the intersection: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

Distribution of intersection with respect to the union: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

Laws of action with empty and universal sets: $A \cup \varnothing = A$, $A \cup A = U$, $A \cup U = U$, $A \cap U = A$, $A \cap A = \varnothing$, $A \cap \varnothing = \varnothing$

The law of idempotency of the union: $A \cup A = A$,

The law of idempotency of the intersection: $A \cap A = A$,

De Morgan's laws: $A \cup B = A \cap B$, $A \# B = A \cup B$,

Laws of absorption: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$,

Gluing laws: $(A \cap B) \cup (A \cap B) = A$, $(A \cup B) \cap (A \cup B) = A$,

Poretsky Laws: $A \cup (A \cap B) = A \cup B$, $A \cap (A \cup B) = A \cap B$,

Double Supplement Law $\not{A}=A$,

1.5. Euler-Venn Diagrams

The illustrations below are called Euler-Venn diagrams, they can be used to illustrate the equalities sets expressed through given sets, as well as receive new equalities.

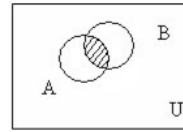


Fig. 1.1 – Intersection of sets

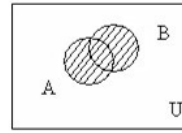


Fig. 1.2 – Combining sets

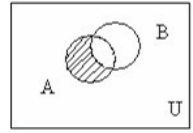


Fig. 1.3 – The difference of the sets

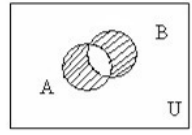


Fig. 1.4 – The symmetric difference of sets

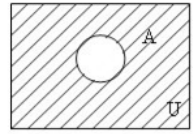


Fig. 1.5 – Absolute complement (negation) of the set

1.6. Characteristic functions
1.6.1. Main relations

To prove complex set-theoretic identities, it is more efficient to use characteristic functions.

A characteristic function X_A of the set $A \subseteq U$ is a function defined on the set *U* with values on the set *{0,1}*: $X_A(x) = \{1$ *if* $x \in A$ 0 *if* $x \notin A\}$,

Obviously, the identity *L* = *R* will be valid if the characteristic functions of the sets *L*, *R*are equal, i.e.. $X_L(x) = X_R(x)$.

We give the characteristic functions of intersection, union, difference, absolute complement and symmetric difference, as well as an important property of the characteristic functions:

– $X_{A \cap B}(x) = X_A(x) * X_B(x)$

– $X_{A \cup B}(x) = X_A(x) + X_B(x) - X_A(x) * X_B(x)$

– $X_{A \setminus B}(x) = X_A(x) - X_A(x) * X_B(x)$

– $X_{\bar{A}}(x) = 1 - X_A(x)$

– $X_{A+B}(x) = X_A(x) + X_B(x) - 2X_A(x)\, X_B(x)$

– $X_A(x) = X^2{}_A(x)$

1.6.2. The process of evidence by the characteristic function

To prove the validity of the set-theoretic identities should express the characteristic features of its left and right sides of the

characteristic features contained in them sets.

As an example, we prove the validity of one of the laws of action with an empty set: $A \cap A = \varnothing$.

Using the characteristic functions: $X_{A \cap B}(x) = X_A(x) * X_B(x)$, $X_A(x) = 1 - X_A(x)$, we obtain: $X_{A \cap A}(x) = X_A(x) * X_A(x) = X_A(x) * (1 - X_A(x)) = X_A(x) - X^2_A(x) = 0$

WHAT AND NEEDED TO BE PROVEN.

1.7. Relationships

Relationship is a mathematical structure that formally defines the properties of various objects and their relationships. Relations are usually classified by the number of objects to be linked and their own properties.

An ordered pair (x,y) is intuitively defined as a collection consisting of two elements *x* and *y*arranged in a specific order. Two pairs (x,y), (u,v) are considered equal if x=u, y=v and only if. The ordered *n*-th elements $x_1,\ldots,x_n$ are denoted by $(x_1,\ldots,x_n)$.

The Cartesian product of the sets *X* and *Y* is the set $X \times Y$ of all ordered pairs (x, y) such that $x \in X$, $y \in Y$.

A binary (or two-place) relation *R* is the set of ordered pairs, a binary relation is a subset of the Cartesian product.

If *R* is a relation and the pair (x, y) belongs to this relation, then along with the record (x, y) R, the notationis also used *xRy*. Elements *x* and *y* are called the coordinates (or components) of the ratio R.

The domain of a binary relation *R* is the set $D_R = \{x \vee \exists\, y, xRy\}$. The range of binary relations *R* is the set $E_R = \{y \vee \exists\, x, xRy\}$.

Let R XY be defined in accordance with the image in Figure 1.6

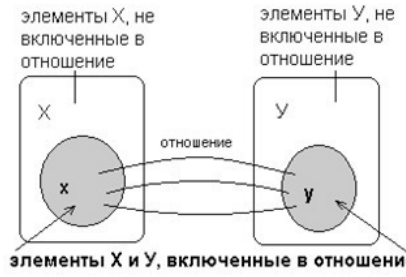


Fig. 1.6 – Definition of the relation R

The domain of definition of D_R and the range of values of E_R *are* defined respectively: $D_R = \{x: (x, y) \in R\}$, $E_R = \{y: (x, y) \in R\}$. The binary relation can be set in any of the ways job sets. In addition, relations defined on finite sets are usually specified: by a

– list (enumeration) of pairs for which this relation is satisfied;

– matrix – the binary relation corresponds to a square matrix of order n, in which the element r_{ij}, standing at the intersection of the i-th row and the j-th column, is 1 if a_i and a_j is the relation, or 0 if it is absent: $R = r_{ij}$, $r_{ij} = [0, (a_i, a_j) \notin R\ 1, (a_i, a_j) \in R]$

1.7.1. Properties of binary relations

– relationship R on the set X is reflexive if for any element $xX\ hRh$ performed.

– The ratio R for the set X is called anti-reflective (irreflexive)

if for any element xX performed ¬ (xRx).

– The ratio R for the set X is symmetric if for all x,x from hRu should be uRh.

– The ratio R for the set X is antisymmetric if for all x, yX of hRu and that $x=y$.

– A relation R on a set X is called transitive if, for any x, y, z X from xRy, and xRz follows yRz.

A partial order relation R is called linear order if the condition $\forall x, y \in X: xRy \vee yRx$ *is satisfied*.

A relation R is called a strict order relation on a set Xif it is antireflexive, antisymmetric, and transitive.

Reflective, symmetric, transitive relation on a set X is an equivalence relation on the set X.

Reflexive transitive and antisymmetric ratio is called a partial order relation, or the ratio of the non-strict order on the set X.

If theon the set X relation of partial orderis given ≤, then the set X is called partially ordered. If theon the set X relation of linear orderis given ≤, then the set X is called linearly ordered. If aon a set X relation of full orderis given ≤, then the set X is said to be completely ordered.

Let R – equivalence relation on the set X.

An equivalence class generated by an element $x \in X$ is a subset of the set Xconsisting of those elements y X for which xRy. It is designated as: $[x] = \{y \in X \mid xRy\}$.

A partition of a set X is a collection of pairwise disjoint subsets of Xsuch that each element of the set X belongs to one and only

one of these subsets.

Examples:

1. X= {1,2,3,4,5} Partition: {{1,2}, {3,5}, {4}}.

2. The partition of many students of the institute can be a set of groups.

In other words, a partition of a set *X* is a family: $X = \cup_{i \in I} X_i \forall i, j\ X_i \cap X_{j\ j} = 0$, $X_i \subseteq X$ is an element of the partition.

The set of equivalence classes of elements of any set of X by the equivalence relation R setis the quotient of the set X with respect R denotedand X/R.For example, a plurality of student groups of a given university is a factor in a plurality of a plurality of university students in relation to belonging to one group.

Examples:

– $(x, \leq)\ x \leq y\ (x,y) \in \leq$ – are comparable;

– $(x,y) \notin \leq$ – are not comparable.

If $(x, \leq), \forall x \in X\ \exists a \in X \vee a \leq x$ then *a* is the smallest element. If $\exists a \in X \vee \forall x \in X\ x \leq a$, then a is the largest element.

Statement: the largest or smallest element is single.

Proof: let *a* and *b* be the largest elements in $(x, \leq)$, then $\forall x \in X\ a \geq x$, in particular $a \geq b$. Similar to $b \geq a$, therefore a=b.

In a similar way, the statement for the smallest elements is proved.

APPROVED PROVEN

1.7.2. Operations on binary relations

Since relations on *X* are defined by subsets $R \subseteq X \times Y$, the same operations are defined for them as on sets.

– The union $R_1 \cup R_2$: $R_1 \cup R_2 = \{(x,y) \mid (x,y) \in R_1 \text{ or } (x,y) \in R_2\}$

– Intersection $R_1 \cap R_2$: $R_1 \cap R_2 = \{(x,y) \mid (x,y) \in R_1 \text{ and } (x,y) \notin R_2\}$

– Difference R_1/R_2: $R_1/R_2 = \{(x,y) \mid (x,y) \in R_1 \textit{ and } (x,y) \notin R_2\}$

– Addition *R: R=U/R, where* $U=M_1 \times M_2$ *(or* $U=M^2$*)*

The inverse ratio R^{-1}:x R^{-1}y if and only if yRx, $R^{-1} = \{(x,y) \vee (y,x) \in R\}$.

Compound ratio (composition) R1 ∝ R2. Let the sets M_1, M_2 and M_3 and the relationship $R_1M_1M_2$ and $R_2M_2M_3$. The composite relation acts from M_1 to M_2 by means of R_1, and then from M_2 to M_3 by R_2, i.e. (a,b) R1 ∝ R2, if there is such *an* M_2 that *(a,c)* R_1 and (a,c) R_2.

The transitive closure of R.A transitive closure consists of such and only such pairs of elements *a* and *b* from *M*, that is, (a, b) R, for which in *M* there exists a chain of (*k* +2) elements *M*, k 0 such that $a, c_1, c_2, \ldots c_k, b$, between whose adjacent elementsis fulfilled *R*. In other words, $ARC_1, with_1RC_2, \ldots, with_kRb$.

Two partially ordered sets are called isomorphic if there is a one-to-one correspondence between them that preserves order.

Example: $(x, \leq_1)$, $(y, \leq_2)$ *x*, *y* are isomorphic if, where $\exists\varphi$:X → Y is a bijective function that preserves order (the definition of a function and a bijective function is given below).

A binary relation is called tolerance if it is reflective and

symmetrical. A binary relation is called a quasiorder if it is irreflexive, antisymmetric, and transitive (preorder).

1.8. Functions

A binary relation f is called a function if from *(x. y) f* and *(x. z) f* it follows that *y=z*. Since functions are binary relations, the two functions f and g are equal if they consist of the same elements. The domain of the function is denoted by Df, and the domain is Rf. They are defined in the same way as for binary relations.

If f is a function, then instead of *(x. y) f* they write *y=f (x)* and say that y is the value corresponding to the argument x, or y is the image of the element x under the mapping f. Moreover, x is called the inverse image of the element y.

The concept of «display» is also often used. Display is some function that reflects the interconnection of elements between sets. In other words, the concepts of «function» and «display» are equivalent.

Let *f: XY*. A function f is called injective (injection) if: $\forall x_1,x_2,y: \{x_1 f y x_2 f y \Rightarrow x_1=x_2\}$,

That is, each value of the function corresponds to a single value of the argument. A function *f* is called surjective (surjection) if $\forall\ y\ \exists\ x \mid xfy$. A function *f* is called bijective (bijection) if *f is* both surjective and injective.

Figure 1.7 illustrates the concepts of relationship, function, injection, surjection, and bijection.

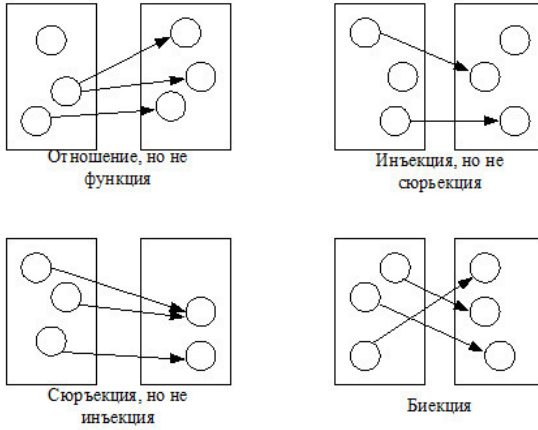


Fig. 1.7 – Relations and functions

1.9. Algebraic operations

An algebraic operation on a set M is a function $\varphi: {}^{Mn} \rightarrow M$, for n = 1 – unary operation, n = 2 – binary, n = 3 – triary (ternary).

It is said thaton M a binary algebraic operation is definedif, by anyany ordered pair of elements of the set M. law, a well-defined element of the same set is associated withFor functions, multiplicative and additive terminology is used.

Multiplicative	Additive
Elements arranged in pairs, any binary algebraic operations are called factors.	Elements arranged in pairs are terms.
The result is a work.	The result is the sum.
The operation is multiplication.	Operation is addition.

Comparison of operations Table 1.1

Properties:

– commutativity: a+b=b+a, a*b=b*a,

– () Associativity: a+b+c=a (a*b) *c=a* (b*c),

– distributivity: (a+b) *c=a*c+b*c,

A neutral element *e of the* set *M* for a binary algebraic operation $\varphi: M^2 \rightarrow M$ is an element: $e \in M \vee \forall x \in M \ \varphi(x, e) = \varphi(e, x) = x$,

Theorem: the neutral element is the only one.

Proof: suppose that in the set *M* there are two neutral elements

e and *e»*. Then $\forall x \in M$ the equalities hold: $\varphi(x, e) = x$ and $\varphi(e', x) = x$. Therefore, these equalities hold for x=e' and x=e: $\varphi(e', e) = e'$ and $\varphi(e', e) = e$, and it follows that e=e'.

THEOREM IS PROVEN.

1.10. Hasse diagrams

If x ≤ (precedes) y and x ≠ y, then write: x <(strictly precedes) y.

It is said that an element y covers an element xif x <y, and there is no element usuch that x <u <y. In the general case, if x <y, then either y covers x, or there exist elements x1, x2, …, xi, xi +1, …, xnsuch that x = x1 <x2 <… <xi <xi +1 <… <xn = y, where xi +1 covers xi for all i.

To illustrate the partial order on the set X, schemes are used that are called Hasse diagrams. In these diagrams, the elements of the set are represented as points on the plane. At the very bottom, the smallest element is depicted, if it exists and belongs to the set, or minimal elements, the elements covering the elements of the previous row, etc. are located higher, and if y covers x, then the points corresponding to them are connected by segments. Figure 1.8 shows the Hasse diagrams of two sets, and Figure 1.9b corresponds to a linearly ordered set.

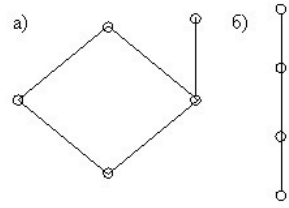


Fig. 1.8 – Examples of Hasse diagrams

Let $A = \{1,2,3\}$. On the set $2^A = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$, we define the partial order relation «to be a subset», that is, $x \le y$ if and only if when $x \subseteq y$. The Hasse diagram for this set is shown in Figure 1.9a.

Let $X = \{1,2,3,5,6,10,15,30\}$. On this set (divisors of 30), we define a partial order relation: $x \mid y$ if and only if x divides y. The Hasse diagram for this set is shown in Figure 1.10.2b.

On a numerical set $Y = \{1,2,3,4,5,6,7,8\}$ consider the relation $\le$ (less than or equal to). The Hasse diagram for this set is shown in Figure 1.9c.

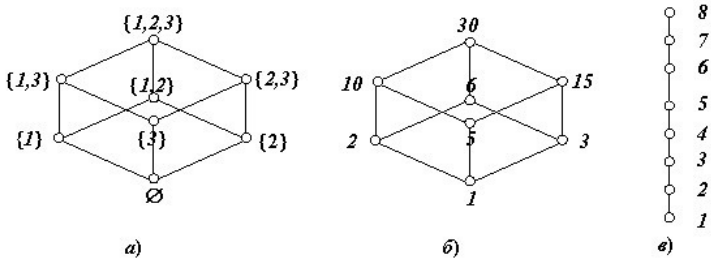
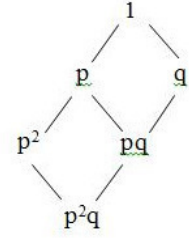


Fig. 1.9 – Hasse diagrams of ordered sets 2^A, X, Y

A Hasse diagram is a directed graph of the form: o→o→… →o→o

Consider the set of divisors of *n*ordered by the divisibility relation. a/b ⇔ a divisor b $(D_n,1)$,n ≥ 1,

Let p and q be prime integers greater than 1. We construct a Hasse diagram for which $n=p^2q$.



In the most general case, the Hasse diagram of a partially ordered set (D_n, 1) consists of edges of an n-dimensional parallelepiped, where n is the number of different prime divisors of n.

Theorem: $n > 0$, $n = p_{1a1p2a2\ldots pm}^{am}$ is the decomposition of the number n into the product of pairwise unequal simple factors. $\forall\ i,j\ (i \neq j) \Rightarrow p_i \neq p_j$. The partially ordered set (D_n, 1) will be isomorphic to the Cartesian product of $[a_1] \times [a_2] \times \ldots \times [a_m]$ linearly ordered sets.

Proof: we define an isomorphism as follows (by mapping into an m-dimensional cube): $p_1^{\beta 1} * p_2^{\beta 2} * \ldots * p_m^{\beta m} \rightarrow (\beta_1, \beta_2, \beta_3, \ldots, \beta_m)$,

THEOREM IS PROVED.

1.11. Theorem

Two partially ordered sets X and Y Isomorphismare called isomorphic if there exists a bijection $\varphi: X \to Y$ that preserves a partial order relation. Otherwise: $x_1 \leq_x x_2$ if and only if $\varphi(x_1) \leq_y \varphi(x_2)$, where $\leq_x$ is the partial order relation on the set X, and $\leq_y$ is the partial order relation on the set Y.

Statement: every partially ordered set X is isomorphic to some system of subsets of the set X partially ordered by the inclusion relation.

1.12. Algebraic structure

Everywhere defined (total function) φ: $M^nM\rightarrow$ called n-ary (n-place) operation on M.The set M together with the set of operations $\sum=(\varphi_1, \varphi_2,\ldots\varphi_m)$, φ_i: $^{Mn}\rightarrow M$, where ni is the arity of the operation φi, is called an algebraic structure, a universal algebra, or simply an algebra.

The set M is called the support or basis of algebra. The arity vector of operations $(n_1,n_2,\ldots,n_m)$ is called the type of algebra. The set $\sum$ is called a signature.

A subset X of the set M ($X \subset M$) is said to be closed under the operation φif: $\forall x_1,x_2,\ldots,x_n \in X\ \varphi\ (x_1,x_2,\ldots,x_n) \in X$, (1.12.1)

If the set X is closed $\forall\ \varphi \in \sum$, then X is called the support of another algebra: $(X, \sum_x)$ – and the set X together with the set of operations is called a subalgebra.

Theorem 1 (formulation 1): a nonempty intersection of subalgebras is also a subalgebra.

Proof: let $(X_i, \sum X_i)$ be the subalgebra $(M; \sum)$. Then: $\forall$ i,j φ_i^{Xi} $(x_1,\ldots,x_n) \in X_i \Rightarrow \forall$ j $\varphi_j^{Xi}(x_1,\ldots,x_n) \in \bigcap X_i$, (1.12.2)

THEOREM IS PROVED.

Theorem 1 (formulation 2): the intersection of any system of subalgebras of the algebra *G*, if it is not empty, will be a subalgebra of this algebra.

Proof: indeed, if G takes a system of subalgebras A_i, $i \in I$, with non-empty intersection D and if $\omega \in \Omega_n$, $n \geq 1$ and $d_1, d_2, \ldots, d_n$ are any elements from D, then the element $d_1, d_2, \ldots, d_n\omega$ contained in each of the subalgebras a_i, and therefore is contained in D. On the other hand, in each of the subalgebras A_i, and therefore also in D, there are elements marked in G *by* all nullary operations from Ω. It follows that if M is a nonempty subset of the algebra G, then in G there exists a minimal among the subalgebras containing the whole set M, namely, the intersection of all such subalgebras. One of them is the algebraitself G.

THEOREM IS PROVEN.

The closure of the set $X \subset M$ with respect to the signature $\sum$ (denoted by $|X|_{\sum}$) is the set of all elements (including the elementsthemselves X) that can be obtained from Xusing the operations from $\sum$. If the signature is implied, it can be omitted.

1.13. Theory

CategoryCategory *C*is a pair (Ob_c, Hom_c (A,B)):

– set objects Ob_c;

– for each pair of objects *A, B* from the set of objects, a lot of morphisms (or arrows) are given Hom_c (A,B), and each morphism corresponds to unique *A* and *B*;

– for a pair of morphisms $f \in Hom\ (A,B),\ g \in Hom\ (B,C)$ a composition is defined $f \circ g \in$ Hom (A,C);

– for each object *A,* an identical morphism is given $id_A \in Hom\ (A,A)$;

moreover, two axioms are fulfilled: the

– composition operation is associative;

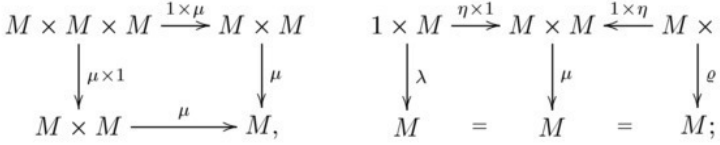
– identity morphism acts $f \circ id_A = id_B \circ f = f$ trivially.

If $\varphi \circ f = f \circ \varphi$ – then the morphism is called a homomorphism. A homomorphism, which is an injection, is called a monomorphism. A homomorphism that is surjection is called an epimorphism. A homomorphism, which is a bijection, is called an isomorphism.

If the supports of the algebra coincide, then the homomorphism is called an endomorphism, and the isomorphism is called an automorphism.

The most important role in category theory is played by the concept of a monoid (semigroup with unity). The monoid *M*

can be described as a set M with two functions: $\mu M \times M \to M\eta,:1 \to M$, such that the following diagrams are commutative:



here 1 in the expression $1 \times \mu$ is the identical function $M \times M$, and 1 in the expression $1 \times M$ is a one-point set $1 = \{0\}$, while $\lambda \wedge \rho$ are bijections. The commutativity of the diagrams means that the following products coincide: $\mu\ ^{o}\ (1 \times \mu) = \mu\ ^{o}\ (\mu \times 1)$, $\mu\ ^{o}\ (\eta \times 1) = \lambda$, $\mu\ ^{o}\ (1 \times \eta) = \varrho$, (1.13.1)

Theorem: let two algebras be given: $A= (A,\sum_A)$ and $B= (B,\sum_B)$, then if $f: A \to B$ is an isomorphism, then $f^{-1}: B \to A$ is also an isomorphism.

Proof: consider an arbitrary operation φ from signature A and the corresponding operation ψ from signature B.

We have: $f\ (\varphi\ (a_1,\ldots,a_n)) = \psi\ (f\ (a_1),\ldots,f\ (a_n))$, in addition, f is a bijection.

denote $B_1:= f\ (a_1)\ \ldots,bn:= f$ (a wherein $a_1 = f^{-1}\ (b_1)\ ^{\ldots,an=f\text{-}1\ ()}$

Then: $f^{-1}\ (\psi\ (b_1,\ldots,b_n)) = f^{-1}\ (\psi\ (f\ (a_1),\ldots,f\ (a_n))) = f^{-1}\ (f\ (\varphi\ (a_1,\ldots,a_n))) = \varphi\ (a_1,\ldots,a_n) = \varphi\ (f^{-1}\ (b_1),\ldots,f^{-1}\ (b_n))$

THEOREM IS PROVED.

If f: A → B is an isomorphism, then the algebras A and B are called isomorphic and are denoted as follows $A \sim^{f} B$:

The isomorphism relation on the set of algebras of the same type is equivalent:

– reflexivity: $A \sim^{f} A$, f:=I;

– symmetry: $A \sim^{f} B \Rightarrow B \sim^{f^{-1}} A$;

– transitivity: $A \sim^{f} B \ \& \ B \sim^{g} G \Rightarrow A \sim^{f \circ g} G$

1.14. Algebras with one operation (semigroups)

Semigroup – algebra with one associative operation: $M=(M,^o)$, $(a^o b)^o c=a^o (b^o c)$,

Monoid is a semigroup with unit: $\exists e \in M | \forall x: e^o x=x^o e=x$.

Theorem: the unit is the only one.

Proof: let: $\exists e_1,e_2 \forall a: a^o e_1=e_1^o a= a$ & $a^o e_2=e_2^o a= a$. Then: $e_1^o e_2=e_1$ & $e_1^o e_2 =e_2 \Rightarrow e_1=e_2$

THEOREM IS PROVEN.

A group is a monoid in which: $\forall a \in M \exists a^{-1} \in M | a^o a^{-1} = a^{-1} o a=e$. The element a^{-1} is called the inverse. It is sometimes referred to as *a»*.

Theorem: if thein the monoid for the element *x* opposite exists, then it is unique, that is, if x'*x=x*x'=e=x'«*x=x*x», then x'=x».

Proof: indeed, from the relations x*x»=e and x'*x=e it follows that: x'=x'*e=x'* (x*x») = (x'*x) *x»=e*x»=x».

THEOREM IS PROVEN.

Theorem: in the group the equationuniquely resolved $a^o x=b$ is.

Proof: let: $a^o x=b \Rightarrow a^{-1} o (a^o x) = a^{-1} o b \Rightarrow (a^{-1} o a)^o x = a^{-1} o b$

$\Rightarrow e \circ x = a^{-1} \circ b \Rightarrow x = a^{-1} \circ b$.

THEOREM IS PROVEN.

A commutative group, that is, a group in which $a \circ b = b \circ a$ is called Abelian. The following notation is used in abelian groups: a group operation is denoted by + or $\oplus$ the inverse of *a*: *-a*, the unit of the group denotes 0 and is called zero.

1.15. Algebra with two operations two operations

Let be given on a set: $\otimes:M^2\to M$ *is the* multiplication and $\oplus:M^2\to M$ is the addition. A ring is a set *M* with two binary operations $\oplus$ and $\otimes$, in which:

– addition is associative: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

– there is an addition unit: $\exists 0 \in M \forall a a \oplus 0 = 0 \oplus a = a$

– there is an inverse addition element: $\forall a \exists -a, a \oplus -a = 0$

– addition is commutative, that is, a ring is an Abelian addition group: $a \oplus b = b \oplus a$

– multiplication is associative, that is, a ring is a semigroup of multiplication: $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ the

– multiplication is distributive left and right: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$, $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ The ring is called commutative, if the multiplication is commutative: $a \otimes b = b \otimes a$. A commutative ring is called a unit ring if there is a unit of multiplication: $\exists 1 \in M a \otimes 1 = 1 \otimes a = a$; that is, a ring with a unit is a monoid of multiplication.

1.16. Vector spaces

A field is a set *M* with two binary operations ⊕⊗ andsuch that:

– (a ⊕ b) ⊕ c= a ⊕ (b ⊕ c) – addition is associative;

– ∃0∈Ma⊕0=0⊕a=a – there is zero;

– ∀a∃-a | a⊕ (-a) =0 – there is an inverse element in addition;

– a ⊕ b = b ⊕ a – addition is commutative (field is an Abelian group by addition);

– a ⊗ (b ⊗ c) = (a ⊗ b) ⊗ c – multiplication is associative;

– ∃1∈M|a⊗1=1⊗a=a – there is a unit;

– $\forall a \neq 0 \exists a^{-1} \mid a^{-1} \otimes a=1$ – there is an inverse element for multiplication;

– a ⊗ b = b ⊗ a – multiplication is commutative (field is an Abelian group by multiplication);

– a ⊗ (b ⊕ c) = (a ⊗ b) ⊕ (a ⊗ c) – Multiplication is distributive with respect to addition.

Let F= <F;+,.> be a field with the addition operation +, the operation of multiplication., the additive unit 0 and the multiplicative unit 1. Let V= <V;+,.> be some Abelian group with the operation + and the unit 0. If there exists an operation F × V → V (the sign of this operation is omitted) such that for any a,b ∈ F and for any x,y ∈ V the following relations hold: (a+b) →x=a→x⊕b→x;a (→x+→y) =a→x⊕a→y; (a*b) →x=a (b→x);1→x+x, then V is called the vector space over the field F, the elements of *F* are called scalar, the elements

of *V* are called vectors, and the undefined operation $F \times V \to V$ is called the multiplication of the vector by the scalar.

The unit of the group V is called $\to 0$ (zero-vector).

Theorem: $\forall x \in V: 0 * \to x = \to 0$, $\forall a \in F: a * \to 0 = \to 0$

Proof: $(1 — 1) \to x = 1 * \to x - 1 * \to x = \to x - \to x = \to 0$

$a (\to 0 - \to 0) = a * \to 0 - a * \to 0 = \to 0 - \to 0 = \to 0$

THEOREM IS PROVED.

1.17. Modular arithmetic

It is said that the number *a is* comparable modulo *n* with the number *b* (a=b (mod n)) if *a* and *b* divided by *n* give the same remainder: a=b (mod n) ⇔ a mod n=b mod n.

The comparability relation is reflexive, symmetric and transitive and is an equivalence relation. Equivalence classes with respect to comparability are called residues modulo *n*. The set of residues modulo *n is* denoted by z_n. Over the residue modulo *n*, the operationsdefined $+_n$, $*_n$ are: $a+_nb = (a+b) \bmod n$, $a*_nb = (a*b) \bmod n$,

It is easy to see that $(z_n, +_n)$ is an Abelian group, and $(z_n, +_n, *_n)$ is a commutative semiring.

Numbers *a* and *b* are called coprime if their greatest common divisor is 1.

Let *n* – a positive integer, n ∈ N. φ (n) is the number of natural numbers 0 <a ≤ n coprime to *n*. n=10,d= {1,3,7,9}, φ (10) =4,

Function φ (n) is named after Euler. Assuming $z_n^* \subset z_n$ is the set of numbers coprime to *n*, we obtain that the Euler function $\varphi(n) = |z_n^*|$.

Let a natural number *n*be presented, represented as its canonical decomposition into simple factors p_i: $n=^k \prod_{i=1}= p_i^{ai}$

Then the Euler function can be calculated by the formula: φ

$(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i-1)$

It is assumed that $\varphi(1) = 1$.

The Euler function can also be represented as the so-called Euler product: $\varphi(n) = n\prod_{p|n}(1-(1/p))$

where *p* is a prime number and runs through all the values involved in the expansion of *n* into prime factors.

Euler's theorem (**a**generalization of Fermat's small theorem)**:** $\forall a \in z_n^*, a^{\varphi(n)} = 1 \pmod n$

1.18. Commutative semiring

A nonempty set S with the binary operationsdefined on it + and certain is called a commutative semiring if the following axioms hold.

– (S, +) is a commutative semigroup with neutral element 0, i.e.: $\forall a,b \in S: a+b=b+a$; $\forall a,b,c \in S: (a+b)+c=a+(b+c)$; $\exists 0 \in S$, $\forall a \in S, 0+a=a+0=a$

– (S, *) is a commutative semigroup with neutral element 1, i.e.: $\forall a,b \in S: ab=ba$; $\forall a,b,c \in S: (ab)c=a(bc)$; $\exists 1 \in S$, $\forall a \in S, 1a=a1=a$

– Multiplication is distributive with respect to addition: $\forall a,b,c \in S: a(b+c)=ab+ac$, $(a+b)c=ac+bc$

– $\forall a \in S: 0a=a0=0$

To construct the classical semiring of quotients, one can use the following method.

Consider a pair of non-negative integers $(a,b), b \neq 0$.

We assume that the pairs (a, b) and (c, d) are equivalent, if $ad = bc$, we obtain a partition of the set of pairs into equivalence classes. Then we introduce operations on classes that turn the set of classes of equivalent pairs into a half-field that contains a semiring of non-negative numbers.

Weelement $n \in S$ call anmultiplicatively reducible if $\forall a,b \in S$ from the equality $an = bn$ that $a = b$. Denote by *R the* set of all multiplicatively reducible elements.

Statement: a multiplicatively reducible element is not a zero divisor.

Proof: Let s be a zero divisor, i.e. $as = 0$ for some $a \neq 0$. Then $as = 0s$, but $a \neq 0 \Rightarrow$ is reducible not multiplicatively.

APPROVED PROVEN.

Let S – commutative semiring contractibly by elements of $(s,r) \in S \times R$. Consider the set of ordered pairs of We introduce the relation ~ on $S \times R$: $(a,b) \sim (c,d) \Leftrightarrow ad=bc$ for all $a,c \in S$ and $b,d \in R$.

Adoption: attitude ~ is an equivalence relation on S.

We show that ~ is an equivalence relation. To do this, it is necessary to show reflectivity, symmetry and transitivity.

Reflectivity: due to the commutativity of the semiring S: $ab=ba \Rightarrow (a,b) \sim (a,b)$;

Symmetry: $(a,b) \sim (c,d) \Leftrightarrow ad=bc \Leftrightarrow cb=da \Leftrightarrow (c,d) \sim (a,b)$;

Transitivity: $(a,b) \sim (c,d) \Leftrightarrow ad=bc \mid \times f \Rightarrow adf=bcf \Rightarrow afd=bcf$

$(c,d) \sim (e,f) \Leftrightarrow cf=de \mid \times b \Rightarrow cfb=deb \Rightarrow bcf=bed$

Consequently: $afd=bed \Rightarrow af=be \Leftrightarrow (a,b) \sim (e,f)$

Thus, the ratio ~ is an equivalence relation on S.

APPROVED PROVEN

The semiring S *is* divided into equivalence classes; in each class are those elements that are in relation ~.

Denote by $[a, b]$ the equivalence class of the pair (a, b). We introduce operations on the set $Q_{cl}(S)$ of all equivalence classes:

$[a,b] + [c,d] = [ad+bc, bd]$

$[a,b] * [c,d] = [ac, bd]$

bd ∈ R since for n ∈ R,m ∈ R,a,b ∈ S, nma=nmb from here, since n ∈ R We obtain *ma = mb,* and since m ∈ R, then *a = b,* hence mn∈ R.

We show the correctness of the operations introduced.

Let: (a,b) ~ (a',b'), (c,d) ~ (c',d')

Then (ad+bc) b'd'=adb'd'+bcb'd'=ab'dd'+cd'bb'=ab'dd'+c'dbb'=a'd'bd +c'd'bd= (a'd'+b'c') bd ⇒ (ad+bc, bd) ~ (a'd'+b'c',b'd'), (1.18.5)

acb'd'=ab'cd'=ba'dc'=bda'c'=a'c'bd ⇒ (ac, bd) ~ (a'c', b'd'), (1.13.1)

Theorem: (Q_{cl} (S),+,*) is a commutative semiring with 1,S ⊆ Q_{cl} (S).

Evidence: to prove that the set *Q_{cl} (S) of* all equivalence classes is a commutative semiring with 1, we need to show the closedness of operations on it.

– Addition. ∀ a,c,e ∈ S and ∀ b,d,f ∈ R: [a,b] + [c,d] = [ad+bc, bd] = [cb+da, db] = [c,d] + [a,b]; ([a,b] + [c,d]) + [e,f] = [ad+bc, bd] + [e,f] = [(ad+bc) f+bde, bdf] = [adf+bcf+bde, bdf]; [a,b] + ([c,d] + [e,f]) = [ab] + [cf+ de, df] = [adf+b (cf+de), bdf] = [adf+bdf+bde, bdf].

Since the right-hand sides are equal, the left-hand sides are also equal: ([a,b] + [c,d]) + [e,f] = [a,b] + ([c,d] + [e,f])

We show that ∀ n,n' ∈ R: [0,n] = [0,n']. Since 0n' = n0 ⇔ (0,n) ~ (0,n') ⇒ [0,n] = [0,n']. The class [0, *n*] is neutral in +: [a,b] + [0,n] = [an, bn]

From the equality anb=bna ⇒ (an, bn) ~ (a,b) then [an, bn] =

[a,b].

∀ n ∈ R [0,n] is a separate class playing thein Q_{cl} *(S)* role of zero.

– Multiplication. ∀ a,c,e ∈ S and ∀ b,d,f ∈ R: [a,b] * [c,d] = [ac, bd] = [ca, db] = [c,d] * [a,b]; ([a,b] * [c,d]) * [e,f] = [ac, bd] * [e,f] = [ace, bdf]; [a,b] * ([c,d] * [e,f]) = [a,b] * [ce, df] = [ace, bdf].

From the equality of the right-hand sides it follows that: ([a,b] * [c,d]) * [e,f] = [a,b] * ([c,d] * [e,f])

Let us show that for ∀ n,n' ∈ R [n,n] = [n',n']. Let nn'=nn' ⇔ (n,n) ~ (n',n') ⇒ [n,n] = [n',n'].

The class [*n*, *n*] is neutral in multiplication (a unit of a half ring), because [a,b] * [n.n] = [an, bn] = [a,b], since from the equality anb=bna ⇒ (an, bn) ~ (a,b); then [an, bn] = [a,b].

Multiplication is distributive with respect to addition: ([a,b] + [c,d]) * [e,f] = [ad+bc, bd] * [e,f] = (ade+bce, bdf]; [a,b] * [e,f] + [c,d] * [e,f] = [ae, bf] + [ce, df] = [aedf + bfce, bfdf] = [(ade + bce) f, (bfd) f] = [ade + bce, bfd] * [f,f] = [ade + bce, bfd]

Consequently, the right-hand distribution law holds:-hand distribution law is ([a,b] + [c,d]) * [e,f] = [a,b] * [e,f] + [c,d] * [e,f]

The leftproved in the same way.

THEOREM IS PROVEN

1.19. Group

Substitution on the set is the map of $Z_n = \{1,2,\ldots,n\}$ into itself. Substitution: $\pi = (1,2,\ldots,n; i_1,i_2,\ldots,i_n)$

we will set the line $(i_1,i_2,\ldots,i_n)$.

A permutation is called cyclic (or a cycle) if some number $j_{1\ is}$ translated by it into j_2, j_2 – by j_3, etc., $j_{k-1\ is}$ translated into j_k, j_k – by j_1, and all the others the numbers remain in place. Such a cycle is denoted by $(j_1,j_2,\ldots,j_k)$. The number k is called the cycle length. Arbitrary substitution can be represented as a product of cycles. For example: (1,2,3,4,5;2,1,4,5,3) = (1,2) (3,4,5)

A cycle of length 2 is called transposition.

Theorem: any substitution is representable as a product (i.e., sequential execution) of transpositions.

A substitution that can be represented as the product of an even (odd) number of transpositions is called even (respectively, odd).

Theorem: permutations on the set Z_n form a group with respect to the product operation.

Proof: the operation of the product of permutations π_1 and π_2 consists in their sequential application. For example, if: π_1= (1,2,3,4;2,4,3,1) π_2= (1,2,3,4;1,4,3,2)

then: $\pi_1\pi_2$= (1,2,3,4;4,2,3,1)

The product operation has, as is easily verified, the associativity property: $\pi(\sigma\tau) = (\pi\sigma)\tau$ The identity element of the group is the identity substitution: The $(1,2,\ldots,n;1,2,\ldots,n)$

substitution inverse to: $(1,2,\ldots,n;i_1,i_2,\ldots,i_n)$

is the substitution: $(i_1,i_2,\ldots,i_n;1,2,\ldots,n)$

THEOREM IS PROVED.

Group permutations on the set Z_n called symmetric group *n*th power, denoted by S_n. The number of elements of the symmetric group *n*th power is equal to n!.

If the substitution on the set N^n is represented as the product of b_1 cycles of length 1, b_2 cycles of length 2, etc., b_n cycles of length *n*, then they say that the substitution is of the type: $b_1,b_2,\ldots,b_n$ For example, wildcard: $\pi_1 = (1,2,3,4;2,4,3,1)$

has a type (1,0,1,0).

Let *M* and *N* be finite sets, and *G* and *H* be permutation groups onrespectively *M* and *N*,. Degreesgroup H^G consists of all possible pairs of $(\pi; \sigma)$, where the $\pi \in G$, $\sigma \in H$ and acts on a plurality N^M of all functions $f:M \to N$.

Moreover, by definition $(\pi;\sigma)\, f(x) = \sigma f(\pi(x))$ for all $x \in M$ and $f \in N\, M$.

Functions f_1 and f_2 from N^M are called equivalent ($f_1 \sim f_2$) if: $\exists\pi \mid f_1(\pi x) = f_2(x)$ for all $x \in M$

1.20. Boolean functions

A Boolean function (either a logical function or a function of a logic algebra or a switching function) of n variables is a mapping: $f:E_2^n \to E_2$

where $E_2^n = \{0,1\}$ Is a Boolean set.

Elements of the Boolean sets 1 and 0 are usually interpreted as logical values of «true» and «false», although in the general case they are considered as formal symbols that do not carry a certain meaning. A non-negative integer n is called the arity or locality of the function; in the case $n = 0$, the Boolean function turns into a Boolean constant. Elements of the Cartesian product are called Boolean vectors.

The set of all possible Boolean functions: $P_n = \{f|f:E_2^n \to E_2\}$

Each Boolean function of arity n *is* completely determined by setting its values on its domain of definition, that is, on all Boolean vectors of length n. It is easy to calculate the number of all Boolean functions of n variables.

Theorem:$|P_n|=2^{2n}$

Proof: Indeed, the number of functions from a k-element set A to an m-element set B is equal to m^k (this fact is proved in the section on combinatorics). In our case, $B = \{0, 1\}$, and $A = B^n$. Then $m = 2$ and $k = |B^n| = 2^n$. This implies the statement of the

theorem.

THEOREM IS PROVEN

Any Boolean function can be set by the truth table.

x_1	x_2	...	x_n	$f(x_1, x_2, ..., x_n)$
0	0	0	1	
0	0	1	0	

The truth table of Boolean functions Table 1.2

x_1	x_2	f_1	f_2
0	0	0	1
0	1	0	1
1	0	1	0
1	1	1	0

An example of the truth of Boolean functions Table 1.3

For these functions, $x_{1\ is}$ essential and x_2 Is an inconsequential variable. The variablevalue of functions x_2 does not affect the, i.e. the value of the function does not significantly depend on the variable x_2. $f_1=x_1, f_2= \neg x_1$

Boolean functions are equal if one of the other is obtained by introducing or deleting non-essential variables.

1.20.1. Boolean functions of one variable

NAME	SYMBOL
identically zero (false)	0
is the identity function	x
negation	$\neg x$
unitidentical (true)	1

Boolean functions of one variable Table 1.4

1.20.2. Boolean functions of two variables of

NAME	SYMBOL	NOTE
identically zero (false)	0	
identity function	x	
identity unit (truth)	1	
conjunction	$;\wedge\,\mathbf{\Lambda}$	&& - *and*
addition modulo 2	$\oplus + \wedge$	$(a + b)\%\ 2$ *xor*
disjunction	$\vee$	|| - *or*
arrow pierce	$\downarrow$	
implication	$\rightarrow, \Rightarrow$	
Schaeffer stroke	|	

Boolean functions of two variables Table 1.5

$F= (f_1,f_2,\ldots,f_n)$, $\forall$ i: $f_i \in P_n$

Formula over F: Φ [F] = f_i ($t_1,t_2,\ldots,t_m$), $f_i \in F$, t_i – variable or formula. The set *F* is called a basis. The function f_i is called an external (main) operation; t_i is the subformula.

1.21. Equivalent formulas

Formulas are called equivalent if they implement the same function. In other words, two logical formulas are called equivalent if, for any values of their logical variables that are the same for both functions, these formulas take the same values. $F_1=F_2$:=func (F_1) =f&func (F_2) =f

Equivalent formulas serve to express some logical operations through others, simplify formulas or, more precisely, replace some logical formulas with others that are equivalent, but simpler. In reasoning one can replace complex statements with simpler ones equivalent to them.

A formula is called identically true or a tautology if it implements an identity unit.

A formula is called identically false if it implements an identity zero.

Statement: the equivalence relation of formulas is equivalence.

$x \vee (y \vee z) \equiv (x \vee y) \vee z$	associativity of disjunction
$x \vee y \equiv y \vee x$	is commutative disjunction
$x \wedge (y \wedge z) \equiv (x \wedge y) \wedge z$	associativity of conjunction
$x \wedge y \equiv y \wedge x$	is commutative conjunction of
$x \wedge (y \vee z) \equiv x \wedge y \vee x \wedge z$	distributive conjunctions with respect to disjunction
$x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z)$	distributivity of disjunction with respect to the conjunction
$\left.\begin{array}{l} x \vee x \equiv x \\ x \wedge x \equiv x \end{array}\right\}$	idempotency or "absorption laws,"
$\neg\neg X \equiv X$	"denial law,"
$\left.\begin{array}{l} \neg(x \vee y) \equiv \neg x \wedge \neg y \\ \neg(x \wedge y) \equiv \neg x \vee \neg y \end{array}\right\}$	"the law of de Morgan's"
$x \rightarrow y \equiv \bar{x} \vee y$	implication
$x \rightarrow y \equiv \bar{y} \rightarrow \bar{x}$	"contraposition"
$x \wedge 1 \equiv x$	
$x \wedge 0 \equiv 0$	
$x \vee 1 \equiv 1$	
$x \vee 0 \equiv x$	
$\bar{0} \equiv 1$	denial of 0
$\bar{1} \equiv 0$	negation 1
$x \wedge \bar{x} \equiv 0$	" the law of contradiction,
$x \vee \bar{x} \equiv 1$	""the law of the excluded middle

Key equivalence Table 1.6

«Allequivalence can be checked by the relevant construction of the truth table STI.

The set (E_2, ¬, ∨, ∧) is called a binary Boolean algebra. In other words, 2 constants are defined on it: 1 and 0, and the operations of negation, conjunction and disjunction.

Substitution rule: if in the equivalent formulas instead of the same variable *x we* substitute the same formula, then we get equivalent formulas. $\forall\Gamma\ (\Phi_1\ (\ldots x\ldots) = \Phi_2\ (\ldots x\ldots))\ \Phi_1\ (\ldots x\ldots)\ \{\Gamma \backslash\backslash x\} = \Phi_2\ (\ldots x\ldots)\ \{\Gamma \backslash\backslash x\}$

In this case, the sign \\ we have designated the replacement of all occurrences of a variable with a formula. The condition for replacing all occurrences is essential.

Replacement rule: if in some formula we replace some subformula (we use the \ sign to replace) with an equivalent one, we get an equivalent formula. $\Phi\ (\ldots\Gamma\ldots) \vee \Gamma_1 = \Gamma_2 \Rightarrow \Phi\ (\ldots\Gamma\ldots)\ \{\Gamma_1 \backslash \Gamma\} = \Phi\ (\ldots\Gamma\ldots)\ \{\Gamma_2 \backslash \Gamma\}$

1.22. Algebra of Boolean functions

Define the conjunction, disjunction and negation functions: $\wedge$, $\vee$: $P_n^2 \to P_n$; $\neg$: $P_n \to P_n$

They are operations on the set of Boolean functions. The algebraic structure $(P_n, \vee, \wedge, \neg)$ is called the algebra of Boolean functions. The algebra of Boolean functions is a Boolean algebra. All axioms of Boolean algebra are satisfied in the algebra of Boolean functions.

Φ is the set of formulas equivalent to given ones; we denote $K = \{\Phi\}_\Phi$ is the equivalence class with respect to equivalence.

An algebra of the class of formulas $(K, \neg, \vee, \wedge)$ is called the Lindenbaum-Tarski algebra. This algebra is isomorphic to the algebra of Boolean functions and is a Boolean algebra.

1.23. The principle of duality

In Boolean algebras, there are dual statements; they are either true or false at the same time. Namely, if in a formula that is true in some Boolean algebra, change all conjunctions to disjunctions, 0 to 1, ≤ to ≥ and vice versa, then we get a formula that is also true in this Boolean algebra. $f(x_1,x_2,\ldots,x_n) \in P_n$

$f(x_1,x_2,\ldots,x_n) = f(x_1,x_2,\ldots,x_n)$ is the dual function f.

Theorem: duality is foreign-valued: $(f^*)^* = f$

Proof: $f^* = f(x_1,x_2,\ldots,x_n)$

$(f^*)^* = f(x_1,x_2,\ldots,x_n) \stackrel{def}{=} f(x_1,x_2,\ldots,x_n)$

THEOREM IS PROVED.

A function is called self-dual if $f^*=f$.

Theorem: let $\varphi(x_1,x_2,\ldots,x_n)$ be realized by the formula:

$f(f_1(x_1,x_2,\ldots,x_n),\ldots,f_n(x_1,x_2,\ldots,x_n))$

then the formula :

$f^*(f_1^*(x_1,x_2,\ldots,x_n),\ldots,f_n^*(x_1,x_2,\ldots,x_n))$

implements the function:

$\varphi(x_1,x_2,\ldots,x_n)$

Proof: $\varphi^*(x_1,\ldots,x_n) = \varphi(x_1,\ldots,x_n) = \varphi(x_1,\ldots,x_n) = f(f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n)) = f(f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n)) = f(f_1^*(x_1,\ldots,x_n),\ldots,f_n^*(x_1,\ldots,x_n)) = f^*(f_1^*(x_1,\ldots,x_n),\ldots,f_n^*(x_1,$

$\ldots,x_n))$

THEOREM IS PROVEN.

Corollary: $\Phi_1=\Phi_2 \Rightarrow \Phi_1^*=\Phi_2^*$.

Further, proving a theorem, by the principle of duality we immediately get a dual theorem: $x_1 \vee x_2 = x_1 \wedge x_2$

$x_1 \wedge x_2 = x_1 \vee x_2$

By normal form we mean a syntactically unique way of writing a formula. We introduce a special kind of entry: $x^y=x \equiv y$, if $x = y$, $x^y=1$, if $x \neq y$, $x^y=0$

The decomposition theorem of a Boolean function can be represented as a disjunctive conjunction of conjunction: $f(x_1,x_2, \ldots,x_m, x_{m+1},\ldots,x_n) = \| = {}_{\delta 1, \delta 2,\ldots,\delta m} x_1^{\delta} \wedge x_2^{\delta} \wedge \ldots \wedge x_m^{\delta m} \wedge f(\delta_1, \delta_2,\ldots,\delta_m, x_{m+1},\ldots,x_m)$

where disjunctions are taken over all possible δ.

Proof: in order to prove that a given formula implements a function, it is enough to take an arbitrary set of argument values, calculate the values of formulas on this set and, if it turns out to be equal to the value of the function, then the formula really implements the function:

$({}_{\delta 1, \delta 2,\ldots,\delta m} x_1^{\delta} \wedge \ldots \wedge x_m^{\delta m} \wedge f(\delta_1,\ldots,\delta_m, x_{m+1},\ldots,x_n))(a_1,a_2, \ldots,a_n) = {}_{\delta 1, \delta 2,\ldots,\delta m} a_1^{\delta 1} \wedge \ldots \wedge a_m^{\delta m} \wedge f(\delta_1,\ldots,\delta_m, a_{m+1},\ldots,a_n) = a^{a1} \wedge a_2^{a2} \wedge \ldots \wedge a_m^{am} \wedge f(a_1,a_2,\ldots,a_n) = f(a_1,a_2,\ldots,a_n)$

THEOREM IS PROVED.

1.24. Perfect normal forms

All algebraic terms of a formula include all variables. It is said that a certain class of formulas *K* has a normal form if there is another class of formulas *K»*, which are called normal forms, such that any formula of the class *K* has a unique equivalent formula from the class *K»*: $\exists K!\ \forall \Phi \in K \exists ! \Gamma \in K» \vee \Phi = \Gamma$

1.24.1. Perfect Disjunctive Normal Form

Representation of a Boolean function in the form (a disjunction is a union sign):

$f(x_1,x_2,\ldots,x_n) = \underset{\delta 1,\ \delta 2,\ldots,\delta m}{} x_1^{\delta 1} \wedge x_2^{\delta 2} \wedge \ldots \wedge x_n^{\delta n}$

is called a perfect disjunctive normal form (SDNF).

Theorem: $\forall f \in P_n \vee \{0\}\ \exists$ the only representation in the form of SDNF.

Proof: we use the decomposition theorem for a Boolean function:

$f(x_1,x_2,\ldots,x_n) = \underset{\delta 1,\ \delta 2,\ldots,\delta n}{} x_1^{\delta 1} \wedge \ldots \wedge x_n^{\delta n} \wedge f(\delta_1,\ldots,\delta_n)) = \underset{f\ (\delta 1,\ \delta 2,\ldots,\delta n)\ =1}{} x_1^{\delta} \wedge \ldots \wedge x_n^{\delta n} \wedge f(\delta_1,\ldots,\delta_n)) = \underset{f\ (\delta 1,\ \delta 2,\ldots,\delta n)\ =1}{} x_1^{\delta} \wedge \ldots \wedge x_n^{\delta n}$

THEOREM IS PROVED.

Theorem: every Boolean function can be expressed in terms of disjunction, conjunction and negation: $\forall f \in P_n \exists \Phi\ \{\neg, \vee, \wedge\}$ |

funcΦ=f

Proof:0=x ∧ $\bar{x}$. In other cases, see the theorem above.

THEOREM IS PROVEN.

1.24.2. Perfect conjunctive normal forms

Theorem: every Boolean function can be represented in the form:

$f(x_1,\ldots,x_n) = {}_{f(\delta 1,\ldots,\delta 2)=1} x_1^{\delta} \vee \ldots \vee x_n^{\delta n}$

Proof: by the duality principle from the SDNF theorem, it can be argued that every Boolean function has an SKNF.

Q.E.D.

1.25. Closed classes of Boolean functions

Let F be the set of Boolean functions: $F= \{f_1,f_2, \ldots,f_n\}, \forall if_i \in P_n$

The closure of the set F is the set of Boolean functions realized by formulas over F: $[F] = \{f \in P_n \mid f=func\ \Phi\ [F]\}$

We introduce a special type of classes of Boolean functions.

– $T_0= \{f|f\ (0,0,\ldots,0) =0\}$ – a class of functions that preserves 0;

– $T_1= \{f|f\ (1,1,\ldots,1) =1\}$ – a class of functions that preserves 1;

– $T_* = \{f|f =f^*\}$ is the class of self-dual functions;

– $T_{\leq}= \{f|\alpha \leq \beta \Rightarrow f\ (\alpha) \leq f\ (\beta), \alpha= (\alpha_1,\alpha_2,\ldots,\alpha_n), \beta= (\beta_1,\beta_2, \ldots,\beta_n)\ \forall ia_i,\ _{bi} \in E_2, \alpha \leq \beta \Leftrightarrow \forall ia_i \leq b_i$ is the class of monotonic functions;

– $T_L= \{f|f=x_0+C_1x_1+C_2x_2+\ldots+C_nx_n\}$ is the class of linear functions.

Theorem: classes: $T_0,T_1,T_*,T_{\leq},T_L$ – closed.

Proof: in order to prove that some class is closed, it is enough to prove that if a function is implemented as a formula over this class, then it belongs to this class. The proof of the isolation of classes 4 and 5 is provided to readers as an exercise.

It can be proved that an arbitrary formula has this property by induction on the structure of formulas. The basis of each

such induction is obvious. Functions from F are realized as trivial formulas over F. Thus, only inductive transitions need to be proved.

$f_0,f_1,\ldots,f_n \in T_0$, $\Phi = f_0\,(f_1\,(x_1,\ldots,x_n),\ldots,\, f_n\,(x_1,\ldots,x_n)) = f_0\,(0,\ldots,0) = 0 \Rightarrow \Phi \in T_0$

$f_0,f_1,\ldots,f_n \in T_1$,, $\Phi = f_0\,(f_1\,(x_1,\ldots,x_n),\ldots,f_n\,(x_1,\ldots,x_n)) = f_0\,(1,\ldots,1) = 1 \Rightarrow \Phi \in T_1$

$f_0,f_1,\ldots,f_n \in T_*$,, $\Phi^* = f_0^*\,(f_1^*\,(x_1,\ldots,x_n),\ldots,\, f_n^*\,(x_1,\ldots,x_n)) = f_0\,(f_1\,(x_1,\ldots,x_n),\ldots,\, f_n\,(x_1,\ldots,x_n)) \Rightarrow \Phi^* \in T_*$,,

Q.E.D.

1.26. Completeness of a system of Boolean functions

As already mentioned, a Booleanis an arbitrary *n*-function place function f $(x_1,x_2,\ldots,x_n)$, where $x_i \in \{0,1\}$. The complete system of Boolean functions is denoted by *E* and has the following form: f_1 $(x_1,x_2,\ldots,x_{k1})$ f_2 $(x_1,x_2,\ldots,x_{k2})$ … f_e $(x_1,x_2,\ldots,x_{ke})$

A system of functions *E*is called complete if any of its Boolean functions can be expressed using f_1, f_2, … f_e through superposition.

A superposition is a function f^*, which is obtained from a function *f* using the following transformations:

– change of variable: f $(x_1,x_2, x_j, \ldots,x_n)$ f^* = f $(x_1,x_2, x_{j-1},y, x_{j+1}, \ldots,x_n)$;

– substitution instead of $x_{j\ of}$ some function from the system.

$f^* = f_i (x_1,x_2, x_{j-1}, f_e (x_1,x_2,\ldots,x_{ke}),x_{j+1}, \ldots,x_{ki})$

Example: system of functions $\{\neg, \cup, \cap\}$ $=E_1$ *is* always complete, because each function of this system can be represented as SDNF, therefore, SDNF is a superposition through which any of the functions of the system can be expressed.

Example: the system of functions $\{\neg, \cup\}$ $=E_2$ *is* also complete,

since the missing function ∩ can be expressed in terms of the other two by the de Morgan rule and double negation:

$x_1 \cap x_2 = \neg (\neg x_1 \cup \neg x_2)$

Example: prove the completeness of the system: $X \rightarrow Y,0$.

For clarity, this system can be written as follows: $\{\rightarrow,0\}$. That is, we are given a system consisting of a Boolean function (implication) and a constant 0. With their help we can express the negation operation, for this we substitute the constant 0 instead of one of the variables:

$X \rightarrow 0 = \neg X \cup 0 = \neg X$

Therefore, this system is complete.

Consider alternative definitions.

The set of Boolean functions of $B = \{f\ 1, f_2, f_m, \ldots, \ldots\}$ is called a full system if any Boolean function can be implemented by the formula above B.

Theorem (on completeness): let two systems of functions frombe given P_2: $B_1 = \{f_1, f_2, \ldots\}$ and $B_2 = \{g_1, g_2, \ldots\}$. Then, if the system B_1 is complete and each of its functions can be realized by a formula over B_2, then the system $B_{2\ is}$ also complete.

Proof: let h be an arbitrary function from P_2. We show that it can be realized by the formula over B_2.

Due to the completeness of B_1 h is realized by the formula over B_1, i.e. $h = [ff_1, f_2, \ldots]$. In addition, by condition $f_1, f_2, \ldots$ are realized by formulas over B_2, i.e. $f_i = \Phi_i\ [g_1, g_2, \ldots]$. Therefore, in the formula Φ we can exclude the occurrence of symbols

of functions $f_1,f_2,\ldots$, replacing them with the corresponding formulas: $\Phi\,[\Phi_1\,[g_1,g_2,\ldots],\,\Phi_2\,[g_1,g_2,\ldots],\ldots]$, (1.26.5)

The resulting expression defines a formula over B_2that implements h.

THEOREM IS PROVEN

Example: the system $\{x,x \wedge y\}$ is complete. Indeed, consider the systems $B_1= \{x,x \wedge y, x \vee y\}$ and $B_2= \{x,x \wedge y\}$. The system B_1 is complete and, since $x \vee y= x \wedge y$, then each function of this system is expressed by a formula over B_2. Thus, the conditions of the completeness theorem are satisfied and, therefore, the system $B_2= \{x,x \wedge y\}$ is a complete system.

Example: the system $\{x|y\}$ is complete. Indeed, consider the systems $B_1= \{x,x \wedge y\}$ and $B_2= \{x|y\}$. We have: $x|y= x \vee y =xy$. Therefore:

$x|x=xx=x$ and $xy=x|y= (y) \mid (x|y)$, (1.26.6)

Thus, each function of the system B_1 is realized by a formula over B_2. In addition, system B_1 is complete. Therefore, the conditions of the completeness theorem are fulfilled and, therefore, $B_2= \{x|y\}$ is a complete system.

2. COMBINATORY

2.1. The basic principles of combinatorics

Theorem (principle of multiplication): if some action can be performed in k stages, and the number of possible ways of *i-th*stage is equal to n_i (i=1,2,…,k),then the total number N_k of all possible ways of performing said action is calculated according to the formula:

$N_k=n_1*n_2*\ldots*n_k=\prod_{i=1}^{k} n_i$, (2.1.1)

Proof: we use induction on the number of stages. If $k = 1$ then, obviously, $N_1 = n_1$ and, therefore, formula (2.1.1) is valid for $k = 1$.

Further, let $k = 2$. Then, since each of the n_1 methods for implementing the first stage can take place with each of the n_2 methods for implementing the second stage, then $N_2=n_1*n_2$, i.e. formula (2.1.1) is also valid for $k = 2$.

Now suppose that formula (2.1.1) is valid for $k = m - 1$, i.e. the formula holds:

$N_{m-1}=\prod_{i=1}^{m-1} n_i$, (2.1.2)

Then, if $k = m$ then, considering the first $m - 1$ stages as the first stage with the total number of implementation methods

defined by the formula (2.1.2), and applying a result similar to the second step of induction, we obtain:

$N_m=N_{m-1}*n_m=\prod_{i=1}^{m} n_i$,

i.e. formula (2.1.1) is also valid for $k = m$.

THEOREM IS PROVEN.

Theorem: the number of elements of the Cartesian product is equal to the product of the numbers of the elements of the set participating in this Cartesian product:

$|X\times Y|=|X|*|Y|$

Proof: Consider an action consisting of 2 stages. The first stage is the choice of the 1st element of an ordered pair. The second stage – the choice of the 2nd element of an ordered pair.

Then the 1st stage can be completed in |X| steps, the 2nd stage in |Y| steps. By the principle of multiplication,

THEOREM IS PROVED.

Theorem: the number of all possible functions from *M* to *N*, where the number of elements |M|=n, the number of elements |N|=m, is m^n.

Proof: the first element from the set *M* can be mapped to *m* elements, the second element from the set *M* can be mapped to *m* elements, the third *n* etc. We get: $m*m*\ldots*m=\prod_{i=1}^{n} m_i=m^n$, where $\forall i\ m_i = m$.

THEOREM IS PROVEN.

Theorem (addition principle): if object *a* can be obtained in *n* ways, object *b* – in *m* ways, then object «*a or b*» can be obtained

in $n + m - k$ ways, where k is the number of repeated methods. Set theoretic wording. If A ⋂ B ≠ ∅,then| ∪ || || AB=A+B-A ⋂ |

Lemma: If A ⋂ B=∅,then |A ⋂ B|= 0,then |A ∪ |=|A|+|B|B.

Proof of the lemma: let A and B be finite sets such that A ⋂ B=∅, |A|=m, |B|=n. If the element a ∈ A can be selected in m ways, and the element b ∈ B – n ways, then the elementselected in x ∈ A ∪ B can be $m + n$ ways. Let $X_1,X_2,\ldots,X_k$ be pairwise disjoint sets, $X_i \cap X_j = \varnothing$, where i ≠ j. Then, obviously, the equality holds:

$| \cup_{i=1}^{k} X_i| = \sum_{i=1}^{k} |X_i|$

The lemma is proved.

Proof of the principle: if we consider the union of two sets A and B, then we will not change anything if we consider a union of this kind:

A ∪ B=A ∪ (B\A)

It can be opened:

A ∪ B=A ∪ (B ⋂ A)

Now the number of union elements is:

|A ∪ B|=|A ∪ (B\A) |

Next we consider A ⋂ (B\A), which is equal to ∅. Accordingly, you can open the difference of the sets:

A ⋂ B ⋂ A= ∅ ⋂ B= ∅

We have the intersection of two sets, it is empty and there are the number of elements combining these sets. We use the lemma. We get:

|A ∪ B|=|A| + |B\A|

Further we consider the set *B*, it is:

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

Moreover, if we take the intersection of these sets, we get:

$(A \cap B) \cap (B\backslash A) = \varnothing$

Once again we return to the lemma and get: $|B|= |A \cap B| \cup |B\backslash A|$. Let us express from here: $|B\backslash A|$, $|B\backslash A|= |B| – |A \cap B|$

Substitute it in: $|A \cup B| =|A \cup (B\backslash A)|$ and get: $|A \cup B| =|A| + |B| – |A \cap B|$

PRINCIPLE PROVED.

2.2. Placements

A placement with repetitions is the function f: $\{x_1,x_2,\ldots,x_m\} \rightarrow \{y_1,y_2,\ldots,y_n\}$. Elements x_i are called objects, and y_j – drawers.

Placements with repetitions – combinatorial compounds made up of n elements of *m*. Moreover, each of the *n* elements may be contained as many times as desired or absent altogether.

Theorem: the number of all arrangements with repetitions is equal to the number of sequences $\{a_1,a_2,\ldots,a_m\}$ of numbers $1 \leq a_i \leq n$ and, therefore, it is equal to n^m.

Non-repetitive placements are combinatorial compounds made up of *n* elements of *m each*. In this case, two compounds are considered different if they either differ from each other by at least one element, or consist of the same elements, but located in different order.

Theorem: the number of placements without repetition is:

$A_n^m = ((n!) / (nm)!)$

Proof: the first item can be placed in *n* ways, the second – $(n - 1)$, ···, *mth*– $(n - m + 1)$. We get: $A_n^m = n\ (n-1)\ \ldots\ (n-m+1) = ((n!) / (nm)!)$

THEOREM IS PROVEN.

2.3. Combinations

Of a combination of elements of the set X is a subset of a finite set $A \subseteq X$. If $|A|=k, |X|=n$, then the subset A is called a combination of n in k, denoted by: ${}_{C}{}^{nk}$. For example, combinations of the three colors of a seven-color rainbow will be described by subsets of three elements.

The combination can be interpreted as the placement of indistinguishable objects. Combinations are a k-element subset of a given set.

Theorem: the number of combinations of n over k is equal to:

$C_n^k = ((n!) / (k! (nk)!))$

Proof 1: from the formulas: $A_k^n = C_k^n * k!$ and $A_n^k = ((n!) / ((nk)!)$ – we get the necessary formula.

THEOREM IS PROVEN.

Proof 2: we consider an action consisting of two stages.

Stage I: $n_1 = C_n^{k-1}$

Stage II: $n_2 = (n-k+1) / (k)$, $C_n^k = C_n^{k-1} * ((n-k+1) / (k))$

Using this formula, we get: $C_n^k = ((n!) / (k! (nk)!))$

THEOREM IS PROVEN.

Property 1: $C_n^k = C_{n-1}^{k-1} + C_{n-2}^{k-1} + \ldots + C_{k-1}^{k-1}$

Proof (by induction): for $n = 1$, the induction basis holds.

For $n = n + 1$: $C_{n+1}^{k}=C_{n}^{k-1}+C_{n}^{k}$

$C_{n+1}^{k}=C_{n}^{k-1}+C_{n-1}^{k-1}+C_{n-2}^{k-1}+\ldots+C_{k-1}^{k-1}$

((n+1)!) / (k! (n+1-k)!) = (n!) / ((k-1)! ((n-k+1)!)) + (n!) / (k! (n-k)!)

(n!* (n+1)!) / ((k-1)!*k (n-k)!* (n-k+1)) = (n!) / ((k-1)! (n-k)!* (n-k+1)) + (n!) / ((k-1)!*k (n-k)!)

(n+1) / (k (n-k+1)) = (1) / (n-k+1) + (1) / (k)

(n+1) / (k (n-k+1)) = (k+n-k+1) / (k* (n-k+1))

1 = 1 (true). Thus, the statement is true for any n.

PROPERTY PROVED

Proof (combinatorial):

$C_{n}^{k}=C_{n-1}^{k-1}+C_{n-2}^{k-1}+\ldots+C_{k}^{k-1}+C_{K-1}^{k-1}$

$C_{n+1}^{k}=C_{n}^{k-1}+C_{n}^{k}$

$C_{n-1}^{k}=C_{n-1}^{k-1}+C_{n-1}^{k}$

$C_{n-1}^{k}=C_{n-2}^{k-1}+C_{n-2}^{k}$

$C_{n-2}^{k}=C_{n-3}^{k-1}+C_{n-3}^{k}$

…

$C_{k+1}^{k}=C_{k}^{k-1}+C_{k}^{k}$

PROPERTY PROVED.

Property 2: $C_{n}^{k}=C_{n-1}^{k}+C_{n-1}^{k-1}$

Proof:

((n-1)!) / (k! (n-1-k)!) + ((n-1)!) / ((k-1)! ((n-1-k+1)!)) = ((n-1)!) / (k! (n-1-k)!) + ((n-1)!) / ((n-1)! (n-k)!)) = ((n-1)! (n-

k)) / (k! (n-k)!) + ((n-1)!k) / (k! (n-k)!) = ((n-1)! (n-k+k)) / (k! (n-k)!) + (n!) / (k! (n-k)!)

PROPERTY IS PROVED.

Property 3: Blaise Pascal suggested to consider and illustrate the properties associated with binomial coefficients, consider the Pascal triangle.

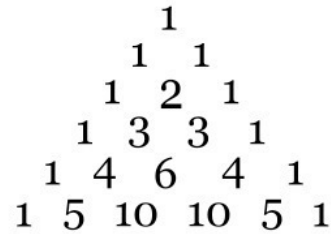


Fig. 2.1 – Pascal Triangle

Theorem: $\sum_{k=0}^{n} C_n^k = 2^n$

Proof (combinatorial): on the left side of the equality is the number of all possible subsets of the set – by the Boolean theorem this number is 2^n.

THEOREM IS PROVEN

Proof (by induction):

– For k = 0: $\sum_{k=0}^{0} C_0^k = C_0^0 = 1 = 2^0$ the $\Rightarrow$ equality is true.

– Assume that the equality holds for k = n, we prove

the equality for k = n +1, i.e. we prove the equality: $\sum_{k=0}^{n+1} C_{n+1}^{k}=2^{n+1}=2*\sum_{k=0}^{n}C_n^k$, or: $C_{n+1}^{0}+C_{n+1}^{1}+C_{n+1}^{2}+C_{n+1}^{3}+\ldots+C_{n+1}^{n-1}+C_{n+1}^{n}+C_{n+1}^{n+1}=2\ (C_n^0+C_n^1+C_n^2+C_n^{n-2}+C_n^{n-1}+C_n^n)$, (2.3.1)

To prove equality (2.3.1), we use: $C_{n+1}^{k}=C_n^{k-1}+C_n^k$, (2.3.2)

Let us prove this equality: (n! (N+1)) / (k! (nk)! (n-k+1)) = (n!k) / (k! (nk)! (n-k+1)) + (n!) / (k! (nk)!)

(n+1) / (n-k+1) = (k) / (n-k+1) +1 $\Leftrightarrow$ (n+1) / (n-k+1) = (n+1) / (n-k+1) the $\Rightarrow$ equality (2.3.2) is proved. We return to the proof of (2.3.1): using equality (2.3.2) we obtain that: $C_{n+1}^{1}=C_n^0+C_n^1;C_{n+1}^{2}=C_n^1+C_n^2$

…

$C_{n+1}^{n-1}=C_n^{n-2}+C_n^{n-1};C_{n+1}^{n}=C_n^{n-1}+C_n^n$

i.e. equality (2.3.1) takes the form: $C_{n+1}^{0}+C_{n+1}^{n+1}=C_n^0+C_n^n;1+1=1+1\Rightarrow$

THEOREM IS PROVED.

Property 4: $C_m^n=C_m^{mn}$ is the symmetry of the Pascal triangle.

Proof: (m!) / (n! (m-n)!) = (m!) / ((m-n)! (m-m+n)!)

PROPERTY PROVED.

Property 5: $C_n^iC_i^m=C_n^mC_{nm}^{im}$

Proof: (n!) / (i! (n-i)!) * (i!) / (m! (i-m)!) = (n!) / (m! (n-m)!) * ((n-m)!) / ((i-m)! (n-m-i+m)!)

PROPERTY PROVED.

Suppose there are objects of n different kinds, and from them are made up sets containing k elements. Such samples are called repeat combinations. Their number is denoted by C_n^k.

Theorem: The number of combinations with repetitions can be calculated by the formula: $C_m^n = C_{n+m-1}^n = ((n+m-1)!) / (n! (m-1)!)$, (2.3.3)

Example (cake problem): let it be required in the store to buy 7 cakes. The store has cakes of one of the types: eclairs, sand, puff, Napoleon. How many choices?

With each purchase we put in correspondence a sequence consisting of seven units and three delimiters 0. A total of 4 types of cakes, then zeros – 3.

2	2	2	1
110	110	110	1

Option table Table 2.1

Summarize the previous problem. The number of purchase options is equal to the number of permutations of n type I elements (units (cakes)) and m type II objects (zeros (delimiters)). Thus, rearranging by all means n units and $(m – 1)$ zeros, we get the desired number:

$P(n,m-1) = ((n+m-1)!) / (n! (m-1)!) = C_m^n$

The solution to the generalized purchase problem is a proof

of (2.3.3).

2.4. Number of permutations

Letbe given n_1 elements of the first type, n_2 – the second type, …, n_k – the$k$-th type, total n elements. Ways to place them in n different places are called repetitive permutations. Their number is denoted by:

$P_n(n_1,n_2,\ldots,n_k)$

Theorem: the number of permutations without repetition is:

$P_n(k_1,k_2,\ldots,k_m) = (n!) / (k_1!k_2!\ldots,k_m!)$

Proof: a subset of A_1 can be chosen C_n^{k1} in ways. A subset of A_2 is selected from the remaining $(n - k_1)$ elements, it can be selected in C_{n-k1}^{k2} ways. A subset of A_3 – $C_{n-k1-k2}^{k3}$ ways, etc. Select a subset A_m defined by previous subsets. From here we get:

$P(k_{1,k2,\ldots,km)=Cnk1Cn-k1k2\ldots Cn-k1-\ldots -km-2}^{km-1} = (n!) / (k_1!\,(n-k_1)!) * ((n-k_1)!) / (k_2!\,(n-k_1-k_2)!) \ldots ((n-k_1-\ldots -k_{m-2})!) / (k_{m-1}!\,(n-k_1-\ldots -k_{m-2}-k_{m-1})!)$

Since $n-k_1-\ldots -k_{m-1}= k_m$, then after reducing the fraction we get the desired equality.

THEOREM IS PROVEN.

The number of one-to-one functions, or the number of permutations of n objects, is denoted by $P(n)$.

Theorem: the number of permutations of elements is $n!$ or n elements can be rearranged $n!$ way, i.e. $P(n) = n!$

Proof: we can put the first item in one of n positions, the second in $(n-1)$, etc., the last item can only be put in one place, and this is the definition of $n!$:

$$P(n) = A_n^n = n*(n-1)*\ldots*(n-n+1) = n*(n-1)*\ldots*1 = n!, \quad (2.4.4)$$

THEOREM IS PROVED.

Comment. Fair recurrence formula: $P(n) = n*P_{n-1}$

2.5. Inclusion and exclusion formula (main theorem)

The formulas and algorithms given in the previous sections give methods for calculating combinatorial numbers for some common combinatorial configurations. Practical tasks are not always directly reduced to known combinatorial configurations. In this case, various methods are used to reduce some combinatorial configurations to others.

Consider the principle of inclusion and exclusion.

The rule (principle) of inclusion / exclusion allows you to calculate the power of the union of sets if their powers and powers of all intersections are known.

Theorem: $|_{i=1}{}^{n}A_i|=\sum_{i=1}{}^{n}|A_i|-\sum_{I\le i1\le i2\le n}|A_{i1} \cap A_{i2}|+\ldots+ (-1)^{k+1}\sum_{I\le i1\le \ldots \le i2\le n}|A_{i1} \cap A_{i2} \cap \ldots \cap A_{ik}|+ \ldots+ (-1)^{n+1}|A_{i1} \cap A_{i2} \cap \ldots \cap A_{in}|$

Proof: by induction, for $n = 1$, *the* statement is obvious.

For $n = 2$, *we* obtain the addition theorem, i.e. if $A \cap B=\varnothing$, then $|\cup| \; || \; ||AB=A+B-A\cap|$

Let it be true for $n - 1$, we prove for n. Note that the relation holds: $(_{i=1}{}^{n-1}A_i) \cap A_n= {}_{i=1}{}^{n-1} (A_i \cap A_n)$

and for $(n - 1)$ it holds.

Let us prove for n: $|_{i=1}{}^{n}A_i|=| (_{i=1}{}^{n-1}A_i) \cup A_n|=|_{i=1}{}^{n-1}A_i|+|A_n|-|$

$(\bigcup_{i=1}^{n-1} A_i) \cap A_n| = \sum_{i=1}^{n-1}|A_i| - \sum_{I \le i < j \le n-1}|A_i \cap A_j| + \ldots + (-1)^n|A_1 \cap A_2 \cap \ldots \cap A_{n-1}| + |A_n| - \sum_{I \le i \le n-1}|A_i \cap A_n| + \sum_{I \le i < j \le n-1}|A_i \cap A_j \cap A_n| + \ldots = \sum_{i=1}^{n-1}|A_i| - \sum_{I \le i < j \le n-1}|A_i \cap A_j| + \ldots + (-1)^{n+1}|A_1 \cap A_2 \cap \ldots \cap A_n|$

Therefore, the statement is true for *n* sets.

Q.E.D.

Formulation using Euler-Venn diagrams: 3 setsare marked on the diagram *A*, *B*, *C*:

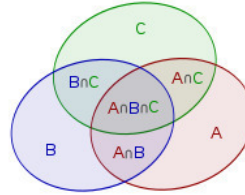


Fig. 2.2 – Illustration to the inclusion-exclusion formula

Then the area of the union $A \cup B \cup C$ is equal to the sum of the areas *A*, *B*, *C* minus the twice-covered areas $A \cap B$,$A \cap C$,$B \cap C$, but with the addition of the three-times covered area $A \cap B \cap C$: $S(A \cup B \cup C) = S(A) + S(B) + S(C) - S(A \cap B) - S(A \cap C) - S(B \cap C) + S(A \cap B \cap C)$

In a similar way, it is generalized to the union of *n* sets.

2.5.1. A special case of the theorem on inclusions and exceptions

In some cases, the number of objects that have a certain set of properties depends only on the number of these properties. Then the formula for counting the number of objects that do not have any of the selected properties is simplified.

For arbitrary n we have: $N(n) = n! - C_n^1 * N(1) + C_n^2 * N(2) - \ldots + (-1)^n N(n)$

In the general case, when rearranging n objects, the number of arrangements in which no object is located on in its place: $N(n) = n! - C_n^1 * (n-1)! + C_n^2 * (n-2)! - \ldots + (-1)^n 0! = D_n$

The resulting value of D_n *is* sometimes called a complete disorder formula or sub-factor. The subfactorial D_n can also be represented as follows: $D_n = n! [1 - (1) / (1!) + (1) / (2!) - (1) / (3!) + \ldots + (-1)^n / (n!)]$

where the expression in […] tends to e^{-1} with an unlimited increase in n.

A subfactorial has properties similar to those of a regular factorial. For example:

– $n! = (N-1) [(n-1)! + (N-2)!]$ – for a regular factorial;

– $D_n = (n-1) [D_{n-1} + D_{n-2}]$ – for the sub-factorial.

Subfactorials are calculated by the formula: $D_n = nD_{n-1} + (-1)^n$

2.5.2. Caravan

Problem Let us consider a problem in which a solution can be

obtained using the main combinatorics theorem.

Task: 9 camels go in a bargain. How many combinations of camel rearrangements exist, in which no camel follows the one he followed earlier?

We distinguish the forbidden pairs: (1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (6, 7),

(7, 8), (8, 9) To solve, we apply the main theorem of combinatorics.

To do this, we define what an object is and what properties are. By objects we mean various arrangements of camels. In total there will be $N = 9!$. By properties we mean the presence of a certain pair

in the permutation. Thus, the number of properties is 8. Then the number of permutations that do not have any of the 8 properties: $N(8) = 9! - C_8^1*8! + C_8^2*7! - C_8^3*6! + C_8^4*5! - C_8^5*4! + C_8^6*3! - C_8^7*2! + C_8^8*1! = 142729 = D_9 = D_8$

In the general case, for n camels, we have: $D_n + D_{n-1}$

2.5.3. Problem about disturbances

Set we denote all permutations by S, and the list of properties will consist of properties p_i: property p_i is the property of this or that substitution to leave elementin place i. It is clear that disorder is just such a permutation that does not have any properties from $P = \{p_1, \ldots, p_n\}$. Following the inclusion-exclusion formula, we get: $N = M - \sum_{i=1}^{n} S(p_i) + \sum_{i,j} S(p_i p_j) - \ldots + (-1)^k \sum S(p_{i1}, p_{i2}, \ldots p_{ik}) + \ldots + (-1)^n S(p_1, p_2, \ldots p_n) = n! - C_n^1 (n-1)!$

$+C_n^2\ (n-2)!\ -\ldots+\ (-1)^k C_n^k\ (n-k)!+\ldots+\ (-1)^n=n!\ (1—1+\ (1)\ /\ (2!)-(1)\ /\ (3!)+\ldots+\ (-1)^k/\ (k!)+\ldots+\ (-1)^n/\ (n!))\approx (n!)\ /\ (e).$

2.6. The concept of a lattice, a distributive lattice

A lattice is a partially ordered set in which each two-element subset has both an exact upper (*sup*) and an exact lower (*inf*) face. This implies the existence of these faces for any nonempty finite subsets.

Any two elements in such a partially ordered set must be comparable: ∀a,b must be either a ≤ b ∨ b ≤ a.

Precision (smallest) of the upper edge (boundary) or supremum subset *X* ordered set (or class) *M,* is the smallest element *M,* which is equal to or more than all of the elements of *X*.In other words, the supremum is the smallest of all the upper faces.

More ∈ formally: SX= {yM | ∈ ≤

the set of upper bounds of *X,* that is, elements of *M,* equal to or greater than any element X.

s=sup sup X ⇔ ∈ s S_x ∧ ∀y ∈ S_x: s ≤ y)

H=sup sup (a,b) = ∧ – *the* exact upper face of the two elements.

Precision (maximum) of the bottom face (boundary) orinfimum subset *X* of an ordered set (or class) *M,* is called the largest element *M,* which is equal to or less than all of the elements of *X*.In other words, the infimum is the largest of all

the lower faces.

L=inf inf (a,b) = ∨ – *the* exact lower bound of the two elements.

Theorem: if the lower (upper) face exists, then it is unique.

Proof: x=inf inf (a,b) ∧ y =inf inf (a,b) ⇒ y≤x ∧ x≤y ⇒ x=y

THEOREM IS PROVED.

A lattice is called distributive if *sup* and *inf are* distributive:

a∪ (b⋂c) = (a∪b) ⋂ (a∪c),a⋂ (b∪c) = (a⋂b) ∪ (a⋂c), (2.6.4)

Lemma: the set of natural numbers N^+ is a lattice with respect to operations ≤,max, min.

Proof: by definition, a lattice is a partially ordered set. Let us show that the set of natural numbers is a partially ordered set. Moreover, a linearly ordered set.

Consider the relation ≤. This is a relation of order because it is:

– Reflective:∀a ∈ N,a ≤ a

– Transitive: ∀a,b,c ∈ N,a ≤ b ⋂ b ≤ c ⇒ a ≤ c

– Antisymmetric: ∀a,b ∈ N,a ≤ b ⋂ b ≤ a ⇒ a = b

In addition, there are many natural numbers linearly ordered, because: ∀a,b ∈ N,a ≤ b ⋂ b ≤ a)

To prove that the set *N* is a lattice, it remains to show that for any two-element subset X ⊂ N there are exact upper and lower faces. This follows from linear ordering. X= {a,b}

Supposeb a ≤ b. Then: in fX=a, supX=b

Similarly, we can reason for another case.

APPROVED PROVEN

2.7. The principle of mathematical induction

Formulation: suppose that it is required to establish the validity of an infinite sequence of statements numbered by natural numbers: P (1),P (2),…,P (n),P (n+1).

Assume that:

– It is established that$P\,(1)$ is true (this statement is called the base of induction).

– For any$n,$ it is proved that if$P\,(n)$ is true, thenis true$P\,(n+1)$ (this statement is called the induction transition).

Then all the statements of our sequence are true.

Proof:

– induction basis. Let $P\,(1)$ be true, i.e.holds $P\,(k)$ for some $k \in N^+$.

– inductive step. If $(P + k)$ – true, then $\forall n \in N^+ P\,(n)$ – true.

We prove that the method of mathematical induction can be applied using the method of proof by contradiction. Suppose that for some numbers in the natural series the method of mathematical induction is incorrect.

Let them form the set $N» \subseteq N^+$. N^+ is a lattice with respect to the operations ≤,max, min (by the lemma proved in Section 2.6); therefore, $N»$, as its subset, is also a lattice $\Rightarrow \exists m \mid \forall k \in N»(m,k) = m$.

– If $m = 1$, then a contradiction with (a) the condition.

– If $m \neq 1$, then $(m - 1)$ is not natural.

$P\,(m - 1 + 1)$ is true (by condition (b)); therefore, $P\,(m)$ is true (a contradiction to condition (b)).

PRINCIPLE PROVED

2.8. The Cantor diagonal method

If each element of the set X corresponds to a single element from the set Y, then it is said that a one-to-one correspondence is established between these sets.

Consider 2 infinite sets: the

– set of natural numbers 1, 2, 3, 4, 5, …, n, …;

– the set of even positive integers 2, 4, 6, …, $2n$, … (this is a subset of the first set).

Since a series of even numbers can be numbered using natural numbers, a one-to-one correspondence can be established between these two sets. If a one-to-one correspondence cannot be established between a set and its certain subset, then the set is finite.

A set equivalent to a set of natural numbers is called countable. In other words, a countable set can be established one-to-one correspondence with a set of natural numbers.

Theorem: the set of real numbers of the interval [0, 1] is uncountable.

Proof (by diagonalization method): each number is represented as an infinite decimal fraction: 0. $a_1\ a_2\ a_3\ldots$ consisting of digits and not having a period of 9. Suppose that some countable set (of all or only some) of real numbers*a*lying on the interval [0, 1]. Then they can be arranged as a list of lines:

0. $a_{11}\ a_{12}\ a_{13}\ a_{14}\ldots$

0. $a_{21}\ a_{22}\ a_{23}\ a_{24}\ldots$

0. $a_{31}\ a_{32}\ a_{33}\ a_{34}\ldots$

…

Consider the sequence of numbers: $b_1 \neq a_{11}, b_2 \neq a_{22}, b_3 \neq a_{33}$, …,not equal to 9. Then the number 0. $b_1\ b_2\ b_{3is}\ldots$ not in the list, although it is in the interval on the segment [0, 1]. This means that all real numbers from this segment cannot be enumerated using natural numbers. Thus, no countable set of real numbers lying on the segment [0, 1] does not exhaust this segment.

THEOREM IS PROVEN.

2.9. The principle of transfinite induction

Transfinite induction is a method of proof that generalizes mathematical induction to the case of an uncountable number of parameter values.

Transfinite induction is based on the following statement.

Statement: let a completely ordered setbe given A. P (x),x $\in$ A is a statement. Suppose that for each element of the set A, since P (y) is true for all $y < x$, it follows that p (x) is true. Then the statement P (x) is true for any x.

Mathematical induction is a special case of transfinite induction. Indeed, let M be the set of natural numbers. Then the statement of transfinite induction turns into the following: if for any positive integer n *the* truth of statements P (1), P (2), …, P (n – 1) implies the truth of statement P (n), then all statements P (n) Moreover, the induction base, that is, P (1), turns out to be a trivial special case for n = 1.

2.10. Newton's binomial
2.10.1. Case of two variables

Formula (Newton's binomial). A formula for decomposing into separate terms a non-negative integer power of the sum of two variables, having the form: $(a+b)^n=\sum_{k=0}^{n} C_n^k a^{nk} b^k$

Proof (by induction). We have the formula: $(a+b)^n=\sum_{k=0}^{n} C_n^i a^{ni} b^i = C_n^0 a^n + C_n^1 a^{n-1} b^1 + \ldots + C_n^n a^0 b^n$

Induction base: for $n = 2$, the statement is obvious: $(a+b)^2=C_2^0 a^2 b^0 + C_2^1 a^1 b^1 + C_2^2 a^0 b^2 = a^2+2ab+b^2$

Induction step: suppose that the statement is true for $n - 1$ and show that it will be true for n. $(a+b)^{n-1}=\sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} b^i$

$(a+b)^n = (a+b)^{n-1} * (a+b) = \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} b^i * (a+b)$

Which is equivalent: $(C_{n-1}^0 a^{n-1} b^0 + C_{n-1}^1 a^{n-2} b^1 + \ldots + C_{n-1}^{n-1} a^0 b^{n-1}) * (a+b)$

And: $C_{n-1}^0 a^n b^0 + C_{n-1}^1 a^{n-1} b^1 + \ldots + C_{n-1}^{n-1} a^1 b^{n-1} + C_{n-1}^0 a^{n-1} b^1 + C_{n-1}^1 a^{n-2} b^2 + \ldots + C_{n-1}^{n-1} a^0 b^n$

Group the terms: $C_{n-1}^0 a^n + (C_{n-1}^0 + C_{n-1}^1) a^{n-1} b^1 + \ldots + C_{n-1}^{n-1} b^n$

Using the proven earlier identity $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$ we get:

$C_n^0 a^n + C_n^1 a^{n-1} b^1 + C_n^2 a^{n-2} b^2 + \ldots + C_n^n b^n$

WHAT YOU NEED TO PROVE.

2.10.2. Ordered partitions and the generalized

Newton bin recall that a partition of a set A is the family $\{A_i\}$ of its pairwise disjoint subsets such that: $\cup_i A_i=A$. Thesubsets A_i are called partition blocks. If the family takes into account the order of the subsets, then it is called an ordered partition. We say that the ordered partition $(A_1,A_2,\ldots,A_{m \text{ of the}})$ set $E= \{e_1,e_2, \ldots,e_n\}$ is of type $(k_1,k_2,\ldots,k_m)$ if $|A_1|=k_1,|A_2|=k_2,\ldots,|A_m|=k_m$. The number of such partitions is denoted by $P(k_1,k_2,\ldots,k_m)$ or $P_n(k_1,k_2,\ldots,k_m)$, where $n=k_1+k_2+\ldots+k_m$.

$P_n(k_1,k_2,\ldots,k_m) = (n!) / (k_1!k_2!\ldots k_m!)$

This is the number of permutations with repetitions. For the proof of this formula, see §2.4.

Theorem: $(x_1+x_2+\ldots+x_m)^n=n!\sum_{k1+k2+\ldots+km=n} ((1) / (k_1!k_2! \ldots k_m!))\, x_1^{k1}x_2^{k2}\ldots x_m^{km}$

Proof: we consider how the boxes are factors of the product: $(x_1+x_2+\ldots+x_m)\,(x_1+x_2+\ldots+x_m)\,\ldots\,(x_1$

Конец ознакомительного фрагмента.