1
Combinatorial configurations

The first section of this chapter is of an introductory nature and presents a summary of the main notions and results from the set theory and algebra which will be used in the book. In the sections that follow we consider various combinatorial configurations which may be introduced on the basis of the general notion of a configuration given in terms of mappings of sets. As examples of combinatorial configurations we consider Latin squares, orthogonal Latin squares, block designs and finite projective planes.

1.1 Notions of set theory and algebra

1.1.1 Boolean operations on sets

A set is a collection of elements of abstract nature, objects or notions, united by some common property. Along with the word "set" we sometimes use equivalent words such as "collection", "family", etc. A set consists of elements, and the formula $x \in X$ means that the element x belongs to the set X; otherwise we write $x \notin X$. If for each $x \in X$ the inclusion $x \in Y$ holds, then we say that X is a subset of Y and write $X \subseteq Y$. Sets X and Y are equal if $X \subseteq Y$ and $Y \subseteq X$. We say that a set X is a proper subset of Y and write $X \subset Y$ if $X \subseteq Y$ and $X \neq Y$. Any set contains, as a subset, the empty set denoted by $\varnothing$.

A set can be determined either by enumeration of its elements or by pointing out the common properties that characterize the elements. Using this second approach to the description of a set, let us define the so-called Boolean operations.

Union The union of sets X and Y is the set

$$X \cup Y = \{x : x \in X \text{ or } x \in Y\},$$

that is, $X \cup Y$ is the set of elements which belong to at least one of the sets X and Y.

Intersection The intersection or product of sets X and Y is the set

$$X \cap Y = \{x : x \in X \text{ and } x \in Y\}.$$

Difference The difference of sets X and Y is the set

$$X \setminus Y = \{x : x \in X \text{ and } x \notin Y\}.$$

Complement The complement of a set X to a set Y such that $X \subset Y$ is the set

$$\bar{X} = Y \setminus X.$$

The collection of all subsets of a set X is called the power set of X and is denoted by 2^X. Elements $X_1, \ldots, X_r$ from the power set of X constitute a partition of the set X if $X_i \neq \varnothing$, $i = 1, \ldots, r$, and

$$X = X_1 \cup \cdots \cup X_r, \quad X_i \cap X_j = \varnothing, \quad i \neq j. \tag{1.1.1}$$

The sets $X_1, \ldots, X_r$ are called the blocks of the partition.

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

$$X \times Y = \{(x, y) : x \in X,\ y \in Y\}.$$

The Cartesian product of several sets is defined similarly:

$$X_1 \times \cdots \times X_r = \{(x_1, \ldots, x_r) : x_1 \in X_1, \ldots, x_r \in X_r\},$$

if $X_1 = \cdots = X_r = X$, then the Cartesian power is

$$X^{(r)} = X \times \cdots \times X.$$

Let X be a finite set and let $|X|$ denote the number of its elements. We give an obvious rule which is the basis of many combinatorial calculations and estimates.

The summation rule If X is a finite set and $X = X_1 \cup \cdots \cup X_r$, $X_i \in 2^X$, $i = 1, \ldots, r$, then

$$|X| \leqslant |X_1| + \cdots + |X_r|, \tag{1.1.2}$$

where the equality is attained only if $X_1, \ldots, X_r$ is a partition of the set X.

Let us now give a second simple rule which is also used in combinatorial analysis.

The multiplication rule If sets $X_1,\dots,X_r$ are finite, then

$$|X_1 \times \cdots \times X_r| = |X_1| \cdots |X_r|. \tag{1.1.3}$$

1.1.2 Binary correspondences and binary relations

Any set R of pairs from $X \times Y$ is called a binary correspondence on the sets X and Y. If $(x,y) \in R$, then we call x and y the projections of (x,y) on X and Y, respectively, and write

$$x = \pi_1(x,y), \qquad y = \pi_2(x,y).$$

For a binary correspondence $R \subseteq X \times Y$, its projections on X and Y can be defined as

$$\pi_1(R) = \{x : x = \pi_1(x,y),\ (x,y) \in R\},$$
$$\pi_2(R) = \{y : y = \pi_2(x,y),\ (x,y) \in R\}.$$

The projections $\pi_1(R)$ and $\pi_2(R)$ are sometimes called the *domain of definition* and *range of values* of R respectively. The *image* of an element $x \in R$ in the correspondence R is the set

$$\delta_1(x;R) = \{y : y \in Y,\ (x,y) \in R\}.$$

Similarly, the set

$$\delta_2(y;R) = \{x : x \in X,\ (x,y) \in R\}$$

is the *preimage* of an element $y \in Y$ in the correspondence R.

A binary correspondence $\varphi \subseteq X \times Y$ is called a *functional* correspondence if the image of any element $x \in X$ consists of only one element. If $X = \{x_1,\dots,x_n\}$ and $Y = \{y_1,\dots,y_m\}$, then a binary correspondence $R \subseteq X \times Y$ can be associated with the matrix $A = \|a_{ij}\|$, $i = 1,\dots,n$, $j = 1,\dots,m$, where

$$a_{ij} = \begin{cases} 1, & (x_i,y_j) \in R, \\ 0, & (x_i,y_j) \notin R. \end{cases}$$

Matrices whose elements take values 0 and 1 are called $(0,1)$-matrices. The $(0,1)$-matrix A associated with a binary correspondence R is called the *incidence* matrix of R.

For $X = Y$ a binary correspondence $R \subseteq X \times Y$ is called a *binary relation* on the set X. The equality relation $\Delta_X = \{(x,x) : x \in X\}$, which is called the *diagonal*, is an example of a binary relation on X. Another

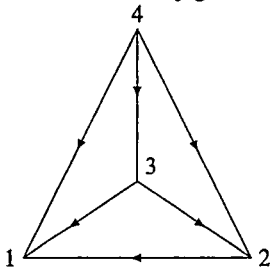

Fig. 1.1.1. The diagram $\Gamma(X, R)$

example is given by the relation of natural order R on a set X of real numbers, where $(x_1, x_2) \in R$ for $x_1, x_2 \in X$ if and only if $x_1 < x_2$.

A binary relation R on a finite set X is associated with a geometric object which is called a *directed graph* or *diagram*. Each element $x \in X$ corresponds to a point on the plane called a vertex. If $(x, x') \in R$, then the points labeled x and x' are connected by an arrow from x to x', called an *edge*. The collection of the vertices and edges formed in such a way is the diagram $\Gamma(X, R)$ of the relation R. The diagram $\Gamma(X, R)$ for $X = \{1, 2, 3, 4\}$ and the natural order R is presented in Figure 1.1.1.

For a binary relation R on a set X we write xRx' if $(x, x') \in R$. Using this notation, we list some properties which can be satisfied by binary relations.

Reflexivity: xRx for all $x \in X$.
Antireflexivity: $R \cap \Delta_X = \varnothing$.
Symmetry: xRx' implies $x'Rx$.
Antisymmetry: xRx' and $x'Rx$ imply $x = x'$.
Transitivity: xRx' and $x'Rx''$ imply xRx''.
Dichotomy: if $x, x' \in X$, then either xRx' or $x'Rx$ holds.

A binary relation R is called an *equivalence relation* if it is reflexive, symmetric and transitive. If R is an equivalence relation and xRx', then we usually write $x \sim x'$. The set $K(x) = \{x' : x' \sim x\}$ is called the *equivalence class* of the element x, $x \in X$. The equivalence classes form a partition of the set X. Conversely, any partition of X determines an equivalence relation whose classes coincide with the blocks of the partition. The set of all equivalence classes is called the *factor set* with respect to the given equivalence relation.

A binary relation R on a set X is called a *partial order*, if R is reflexive,

antisymmetric and transitive. In this case the set X is called a partially ordered set. If R is a partial order relation and xRx', then we usually write $x \preccurlyeq x'$.

A partial order relation R with the dichotomy property is called a *linear* order or, simply, order. The expression $x \leqslant x'$ means that x and x' satisfy a linear order relation R, that is, xRx'.

We can define a strict partial (linear) order relation $\prec$ ($<$) on X, setting $x \prec x'$ ($x < x'$) if $x \preccurlyeq x'$ ($x \leqslant x'$) and $x \neq x'$.

It is clear that we can always define a strict order relation on any finite set X. Each such relation is equivalent to a permutation of the elements of X and, consequently, the number of such relations is equal to $|X|!$.

We can define a partial order relation on the power set 2^X of a finite set X, setting $A \preccurlyeq A'$, $A, A' \in 2^X$, if and only if $A \subseteq A'$. In turn we can define a linear order relation on the Cartesian power $X^{(r)}$ of a set X with a strict linear order relation setting

$$(x_1, \ldots, x_r) < (x'_1, \ldots, x'_r)$$

for $(x_1, \ldots, x_r)$, $(x'_1, \ldots, x'_r) \in X^{(r)}$ if for the smallest index i such that $x_i \neq x'_i$ the relation $x < x'$ holds. This ordering is used to order entries in dictionaries and is referred to as the *lexicographical ordering*.

1.2 Mappings and composition laws

1.2.1 Mappings

A rule φ which assigns a single element $\varphi(x) \in Y$ to each $x \in X$ is called a *single-valued mapping* of the set X into the set Y or a function defined on X and taking values from Y. In such a case we write $\varphi : X \to Y$. It is clear that a single-valued mapping $\varphi : X \to Y$ is a functional binary correspondence $\varphi \subseteq X \times Y$. We define a *many-valued mapping* ψ of a set X into a set Y as a rule which assigns a set $\psi(x) \subseteq Y$ to each element $x \in X$, where the case $\psi(x) = \varnothing$ is not ruled out. It is clear that a many-valued mapping ψ is a binary correspondence $\psi \subset X \times Y$. In what follows we use single-valued mappings, unless otherwise specified. Therefore, let us consider some properties of single-valued mappings without explicitly mentioning their single-valuedness.

The most commonly used representations of a mapping are a functional form and a two-row matrix form. The *functional representation* $y = \varphi(x)$ means that under the mapping $\varphi : X \to Y$ any element $x \in X$ transfers to the element $y = \varphi(x) \in Y$. The two-row matrix representation

is convenient for finite sets X and Y. Let $X = \{x_1,\dots,x_n\}$ and $Y = \{y_1,\dots,y_m\}$, then the two-row representation corresponding to $\varphi : X \to Y$ is of the form

$$\varphi = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \varphi(x_1) & \varphi(x_2) & \dots & \varphi(x_n) \end{pmatrix}.$$

Let us consider the matrix $A = \|a_{ij}\|$, $i = 1,\dots,n$, $j = 1,\dots,m$, where

$$a_{ij} = \begin{cases} 1, & y_j = \varphi(x_i), \\ 0, & y_j \neq \varphi(x_i). \end{cases}$$

The matrix A is called the *incidence matrix* of the mapping φ of the set $X = \{x_1,\dots,x_n\}$ into the set $Y = \{y_1,\dots,y_m\}$. By virtue of the single-valuedness of the mapping φ there is exactly one unit in each row of the matrix A. Such matrices are usually called *elementary matrices*.

Two mappings $\varphi_1 : X_1 \to Y_1$ and $\varphi_2 : X_2 \to Y_2$ are considered equal if $X_1 = X_2$, $Y_1 = Y_2$ and $\varphi_1(x) = \varphi_2(x)$ for all $x \in X$. A mapping $\varphi' : X' \to Y$ is a *restriction* or *truncation* on X' of a mapping $\varphi : X \to Y$ if $X' \subseteq X$ and $\varphi'(x) = \varphi(x)$ for all $x \in X'$.

The set $\varphi^{-1}(y) = \{x : \varphi(x) = y,\ x \in X\}$ is called the *preimage* of an element y under a mapping $\varphi : X \to Y$. The preimage of an element y coincides with the preimage of this element under the functional binary correspondence $R \subseteq X \times Y$ related to the mapping φ. A mapping $\varphi : X \to Y$ is *surjective* if for any $y \in Y$ there exists $x \in Y$ such that $y = \varphi(x)$. In this case we say that φ is a mapping of X onto Y. It is clear that under a surjective mapping the preimage of any $y \in Y$ is not empty. A mapping $\varphi : X \to Y$ is *injective* if $\varphi(x) \neq \varphi(x')$ for any $x, x' \in X$ such that $x \neq x'$. The preimage of any $y \in Y$ contains no more than one element under an injective mapping. A mapping $\varphi : X \to Y$ is *bijective* if it is both surjective and injective. Such mappings are usually referred to as *one-to-one* mappings.

If $X = Y$, then a bijective mapping $\varphi : X \to X$ is called a *substitution*. A substitution of a finite set X can be associated with a square incidence matrix of size $|X|$ each row and each column of which contain exactly one unit. Such matrices are called permutation matrices.

1.2.2 Composition laws

A *composition* law or an operation (binary) on a set X is a mapping $f : X \times X \to X$. If $f(x, y) = z$, where $x, y, z \in X$, then we write $x \top y = z$.

A composition law $\top$ is *associative* if for any $x, y, z \in X$

$$(x \top y) \top z = x \top (y \top z).$$

A composition law $\top$ which satisfies the condition

$$x \top y = y \top x$$

is called *commutative.*

A composition law $\top$ is *distributive* with respect to a composition law $\perp$ if for any $x, y, z \in X$

$$x \top (y \perp z) = (x \top y) \perp (x \top z),$$
$$(y \perp z) \top x = (y \top x) \perp (z \top x).$$

We now introduce the *inverse* element for a given element, and the unit element. An element $e \in X$ is called the unit element or the *neutral* element with respect to a composition law $\top$ if for any $x \in X$

$$x \top e = e \top x = x.$$

If such an element exists then it is unique. Let a composition law $\top$ have the unit element. Then an element x^{-1} is the *inverse* or *symmetric* element for an element $x \in X$ with respect to the composition law if

$$x \top x^{-1} = x^{-1} \top x = e.$$

A set X where a composition law is defined is called a *groupoid.* A groupoid X where each of the equations $a \top x = b$ and $y \top a = b$ has a unique solution with respect to unknowns x and y for any $a, b \in X$ is called a *quasigroup.* Obviously, a quasigroup can also be defined as a set X such that each two elements from the relation $a \top b = c$, where $a, b, c \in X$, uniquely determine the third. If the composition law $\top$ is associative, then the groupoid is called a *semigroup* or *monoid.* If the operation is commutative, then the semigroup is called *Abelian.* A semigroup with unit element such that the inverse element exists for any of its elements is called a *group.* A group is *monogenic* if each of its elements can be obtained from an element other than the unit by sequential application of the composition law. A monogenic group is necessarily Abelian. A finite monogenic group is called cyclic.

For a finite group X the value $|X|$ is called the *order* of the group. Let X and Y be finite groups of arbitrary orders with operations $\top$ and $\perp$, respectively, and let $\varphi : X \to Y$ be a mapping such that for any $x, x' \in X$

$$\varphi(x \top x') = \varphi(x) \perp \varphi(x').$$

Such a mapping is called a *homomorphism* of the group X into the group Y. If the mapping φ is bijective, then the homomorphism is called an *isomorphism.*

A non-empty subset Y of a group X with a composition law $\top$ is called a *subgroup* if the following conditions are fulfilled:

(1) the inclusion $y \in Y$ implies $y^{-1} \in Y$;
(2) the inclusions $y \in Y$, $y' \in Y$ imply $y \top y' \in Y$.

If the composition of any two elements from $Y \subset X$ belongs to Y, then we say that Y is *closed* with respect to this composition law. A subgroup Y of a group X is a set closed with respect to the composition law and containing the inverse elements of all its elements.

A subgroup Y of a group X determines an equivalence relation on the group. For any $x, x' \in X$ let $x \sim x'$ if $x' \top x^{-1} \in Y$. The corresponding equivalence classes are called the *right residue classes* of X with respect to the subgroup Y. Similarly, we can put $x \sim x'$ if $x^{-1} \top x' \in Y$. The corresponding equivalence classes are called the *left residue classes* of X with respect to the subgroup Y. If x belongs to some right (left) residue class with respect to the subgroup Y, then the whole class consists of elements of the form $y \top x$ ($x \top y$), where $y \in Y$, and is denoted by Yx (xY). The corresponding partition of X is called the *decomposition* of X into the right (left) residue classes with respect to the subgroup Y.

If X is a finite group and $x_1, \ldots, x_{k-1}$ are representatives of all residue classes, except Y itself, then the decomposition can be written as

$$X = Y \cup Yx_1 \cup \cdots \cup Yx_{k-1}.$$

For the left residue classes the decomposition has the form

$$X = Y \cup x_1 Y \cup \cdots \cup x_{k-1} Y,$$

where xY is the left residue class containing the element x. The number k is called the *index* of the subgroup Y in the group X.

A subgroup Y is an invariant subgroup in a group X if $xY = Yx$ for any $x \in X$. It is clear that the decompositions of X into the right and left residue classes with respect to an invariant subgroup coincide. For the sake of definiteness the residue classes of a group X with respect to an invariant subgroup Y are considered as the right residue classes. Let us define the composition law $*$ putting $(Yx) * (Yx') = Y(x \top x')$, where $\top$ is the composition law of the group X. The inverse element with respect to the operation $*$ is defined by the equality $(Yx)^{-1} = Yx^{-1}$; the role of

the neutral element is played by Y. As a result the set of residue classes becomes a group which is called the *factor group* and is denoted by X/Y.

A set X with two operations $\perp$ and $\top$ is called a *ring* if it is an Abelian group with respect to the operation $\perp$, a semigroup with respect to the operation $\top$ and the composition law $\top$ is distributive with respect to the composition law $\perp$.

If in a power set 2^X we take the operation $\cup$ as the composition law $\perp$ and the operation $\cap$ as the composition law $\top$ and add the operation of taking complements of sets to these two operations, then we obtain the Boolean algebra.

The set of integers $\mathbf{Z}$ with ordinary addition and multiplication as the composition laws forms a ring. We say that numbers $a, b \in \mathbf{Z}$ are congruent modulo m if the difference $a - b$ is divisible by m. In this case we write $a \equiv b \pmod{m}$. The congruence is an equivalence relation and the corresponding equivalence classes are called the residue classes modulo m. Each of the classes contains exactly one of the numbers $0, 1, \ldots, m-1$ which are representatives of the classes and form the full system of the least non-negative residues modulo m. Denote by K_i the class whose representative is the number i, $0 \leqslant i \leqslant m-1$. On the set of classes $K_0, \ldots, K_{m-1}$ we can introduce operations of addition and multiplication, which for simplicity we also denote by the symbols $+$ and $\cdot$. We define these operations on the classes as follows: $K_i + K_j = K_l$ if $i + j \equiv l \pmod{m}$, $K_i \cdot K_j = K_l$ if $i \cdot j \equiv l \pmod{m}$. As a result we obtain the ring of residue classes modulo m which will be denoted by $\mathbf{Z}_m$.

In a ring the neutral elements with respect to the operations $\perp$ and $\top$ are called the *zero* and *identity* respectively.

If the set of non-zero elements with respect to the composition law $\top$ is an Abelian group, then the ring is a field. A field with a finite number of elements is called *finite*. If p is a prime number, then the set of residue classes modulo p forms a finite field with p elements.

A finite field with n elements exists if and only if $n = p^\alpha$, where p is prime and α is natural. Such a field is unique up to isomorphisms preserving both the composition laws. This field is called the *Galois field* and is denoted by $\mathrm{GF}(p^\alpha)$. If $\alpha = 1$, then $\mathrm{GF}(p)$ is isomorphic to the field of residue classes modulo p.

Let $\mathscr{P}$ be a field with operations $+$ and $\cdot$, and let X be an Abelian group with a composition law $\perp$. A mapping $\varphi : \mathscr{P} \times X \to X$ determines the

so-called outer composition law $\top$, which has the following properties:

$$a \top (x \perp y) = a \top x \perp a \top y,$$
$$(a + b) \top x = a \top x \perp b \top x,$$
$$a \top (b \top x) = (a \cdot b) \top x,$$
$$e \top x = x,$$

where $a, b \in \mathscr{P}$, $x, y \in X$ and e is the identity of the field $\mathscr{P}$. An Abelian group with such operations $\perp$ and $\top$ is a *vector space* over $\mathscr{P}$, and its elements are called *vectors*. Vectors $x_1, \ldots, x_n$ are linearly independent if the equality

$$a_1 \top x_1 \perp \cdots \perp a_n \top x_n = \bar{0},$$

where $a_1, \ldots, a_n \in \mathscr{P}$ and $\bar{0}$ is the neutral element of the Abelian group X, implies that $a_1 = \cdots = a_n = 0$, where 0 is the zero of $\mathscr{P}$. A maximal set of linearly independent vectors $x_1, \ldots, x_n$ is called a basis of the space. A vector space which has at least one basis with finite number n of elements is called finite-dimensional, and the number n is its *dimension*. A vector space of dimension n is isomorphic to the vector space V_n of row-vectors of the form $v = (a_1, \ldots, a_n)$ with coordinates from the field $\mathscr{P}$, where the operation $\perp$ is the ordinary coordinate-wise addition and $\top$ is the multiplication of the coordinates by an element of $\mathscr{P}$. If $e_1, \ldots, e_n$ is a basis of the space V_n, then any vector $v \in V_n$ can be uniquely represented as a linear combination of the basis vectors in the form

$$v = \alpha_1 e_1 + \cdots + \alpha_n e_n, \quad \alpha_j \in \mathscr{P}, \quad 1 \leqslant j \leqslant n.$$

A ring X is an algebra over $\mathscr{P}$ with composition laws $+$ and $\cdot$, if the group X with respect to the first composition law is a vector space over the field $\mathscr{P}$, and the second composition law $\top$ and multiplication $\cdot$ by elements of $\mathscr{P}$ are related by the formula

$$a \cdot (x \top y) = (a \cdot x) \top y = x \top (a \cdot y).$$

The dimension of the vector space is called the *rank* of the algebra. For example, the set of all $n \times n$ matrices with complex elements with the ordinary operations of addition and multiplication and with the operation of multiplication of a matrix by a complex number, is an algebra of rank n^2 over the field of complex numbers.