## CHAPTER 1 INTRODUCTION


#### Abstract

This introductory chapter provides basic concepts, devices, and notations that facilitate the developments of the present study on threshold transformations and dynamical systems of neural networks.


### 1.1 Basic notations

In this chapter we describe basic concepts, devices, and notations that facilitate the developments of the present study. Most of the basic concepts in this chapter are found in introductory chapters of traditional textbooks on "abstract" algebra or in good introductory textbooks on discrete mathematics or combinatorics such as Williamson (1985), Krishnamurthy (1986), and Biggs (1989). We usually deal with finite sets in this book. The number of elements of a finite set $X$ will be denoted by $|X|$. For set operations, the prefix ${ }^{c}$ denotes the complement of a subset, $\backslash$ denotes the difference of sets:

$$
A \backslash B=A \cap B^{c}=\{x \mid x \in X, x \notin Y\}
$$

and $\dot{+}$ denotes the symmetric difference of sets:

$$
A \dot{+} B=(A \backslash B) \cup(B \backslash A)
$$

Then

$$
(A \dot{+} B) \dot{+} C=A \dot{+}(B \dot{+} C) .
$$

If $q \in X$, then $A \backslash\{q\}$ and $A \cup\{q\}$ are respectively written as $A \backslash q$ and $A \cup q$. A partition of a set $S$ is a family of disjoint subsets $A 1, . .$, An such that

$$
S=\bigcup_{i=1}^{n} A_{i}
$$

If $F$ is a function from $X$ to $Y$, denoted by $F: X \rightarrow Y$, and if $A \subseteq X$, then the image of $A$ under $F$ is

$$
F A=\{y \mid y=F x \text { for some } x \in A\}
$$

and the inverse image of A is

$$
F^{-1} A=\{x \mid F x \in A, x \in X\}
$$

The inverse image of $a \in Y$ is

$$
F^{-1} a=\{x \mid F x=y, x \in X\}
$$

If $B=F A$, then the expression $A \rightarrow_{F} B$ is also used.
A function $F: X \rightarrow Y$ is called an onto function or a surjection if $F X=Y . F$ is called a one-to-one function or an injection if $F x=F x \prime$ for $x, x \prime \in X$ implies $x=x \prime . F$ is called a bijection if $F$ is both a surjection and an injection. If $D$ and $X$ are any sets, then $X^{D}$ denotes the set of all functions from $D$ to $X$. If $F$ is a function from a set $X$ to a set $Y$, and if $G$ is a function from the set $Y$ to a set $Z$, then the composition $G \circ F$, often simply written as $G F$, is the function from $X$ to
$Z$ defined as $(G F) x=G(F x)$ for every $x \in X$. $G F$ is also called the product of $G$ and $F$. If $C \subseteq X$, the restriction of a function $F: X \rightarrow Y$ to $C$ is denoted by $F \mid C$.

The set of all integers will be denoted by $\mathbf{Z}$, the set of non-negative integers will be denoted by $\mathbf{Z}_{+}$, and the set of positive integers will be denoted by $\mathbf{Z}^{+}$. A sequence $V=\left(v_{0}, v_{1}, \ldots\right)$ in $X$ is a function $V: \mathbf{Z}_{+} \rightarrow X$. The image of $V$, that is, the set $\left\{x \mid x=v_{i}\right.$ for some $\left.i\right\}$, is denoted by $\mathbf{V}$.

A graph $G$ consists of a finite set $V$, whose members are called vertices, and a set $E$ of 2-element subsets of $V$, whose members are called edges. $V$ is called a vertex set, $E$ is called an edge set, and $G$ is expressed as $G=(V, E)$. A directed graph, or digraph consists of a finite set, whose members are called vertices, and a set $A$ of ordered pairs of elements of $V$, whose members are called arcs. $V$ is called a vertex set, $A$ is called an arc set, and $G$ is expressed as $G=(V, A)$. An arc $(x, y)$ will be expressed by $x \rightarrow y$. An arc $(x, x)$ is called a loop, and will be expressed by $x \partial$. Let $G=(V, A)$ and $H=(W, B)$ be digraphs. Let $F$ be a bijection from $V$ to $W$. Assume that $(x, y) \in A$ if and only if $(F x, F y) \in B$. Then a function $F \prime$ from $A$ to $B$ can be defined as $F \prime(x, y)=(F x, F y)$ for each $(x, y) \in A$. In this case, $G$ and $H$ are called isomorphic under the isomorphism $\left(F, F^{\prime}\right)$ induced by $F$.

A walk in a graph $G$ is a fnite sequence of vertices $V=\left(v_{1}, v_{2}, . ., v_{k}\right)$ such that $\left\{v_{i}, v_{i+1}\right\}$ is an edge of $G$ for every $1 \leq i \leq k-1$. Similarly, a walk in a digraph $G$ is a sequence of vertices $V=\left(v_{1}, v_{2}, . ., v_{k}\right)$ such that $\left(v_{i}, v_{i+1}\right)$ is an arc of $G$ for every $1 \leq i \leq k-1$. In this case, the walk $V$ is expressed as $v_{1} \rightarrow v_{2} \rightarrow \ldots \rightarrow v_{k+1}$. If all its vertices are distinct, a walk is called a path. A walk $v_{1} \rightarrow v_{2} \rightarrow \ldots \rightarrow v_{k+1}$ whose vertices are all distinct except that $v_{1}=v_{k+1}$ is called a $k$ - cycle or a cycle of length $k$. A cycle of a graph $G$ is called Hamiltonian, if it contains all vertices of $G$.

By a transformation of $F$ of a set $X$ we mean a function from the set to itself. In particular, if $F$ is a bijection, it is called a one-to-one transformation. If $F$ is a transformation of a set $X$, then $F$ defines its digraph,

$$
\operatorname{GRAPH}(F)=(X, A)
$$

consisting of the vertex set $X$ and the arc set $A$ defined by

$$
A=\{(x, y) \mid x \in X, F x=y\}
$$

If $v_{1} \rightarrow v_{2} \rightarrow \ldots \rightarrow v_{k} \rightarrow v_{1}$ is a cycle of a digraph, then $v_{i} \rightarrow v_{i+1} \rightarrow \ldots \rightarrow$ $v_{k} \rightarrow v_{1} \rightarrow \ldots \rightarrow v_{i}$ is also a cycle. Therefore, in $\operatorname{GRAPH}(F)$, these two cycles are regarded as the same. With this identification in mind, the set of all cycles in $\operatorname{GRAPH}(F)$ is denoted by $\operatorname{CY}(F)$ (a loop is a 1-cycle).

If $F$ and $G$ are transformations of $X$ and $G F=F G$, then $F$ is called commutative with $G$. A particular case where $F$ and $G$ are commutative is described in the following. If $F x=x$, that is, $(x)$ is a loop of $\operatorname{GRAPH}(F)$, then $x$ is called a fixed point of $F$; if $F x \neq x$, then $x$ is called a non-fixed point of $F$. If $F A \subseteq A$ for a subset $A$ of $X$, then the restriction $F \mid A$ is the transformation of $A$. We call the set of all non-fixed points of $F$ the carrier of $F$ and write $\operatorname{Car} F$. If $\operatorname{Car} F$ and $\operatorname{Car} G$ are disjoint, then a transformation $H$ can be defined by $H x=F x$ if $x \in \operatorname{Car} F$, $H x=G x$ if $x \in \operatorname{Car} G$, and $H x=x$ if $x \in(\operatorname{Car} F \cup \operatorname{Car} G)^{c} . H$ is called the sum of $F$ and $G$ and denoted by $F+G$. If $H=F+G$, and if the images $F(\operatorname{Car} F)$ and $G(\operatorname{Car} G)$ are disjoint, then $F$ is commutative with $G$, and $H=G F=F G$. In this case, $H$ is called the direct sum or more conventionally disjoint composition of $F$ and $G$ and denoted by $H=F \odot G$.

If $X$ and $Y$ are sets, then the Cartesian product $X \times Y$ is the set of ordered pairs $(x, y), x \in X$ and $y \in Y$. If $F$ is a transformation of $X$ and $G$ is a transformation of $Y$, then the direct product $F \times G$ is the transformation of $X \times Y$ defined by $(F \times G)(x, y)=(F x, G y)$ for every $(x, y) \in X \times Y$. The Cartesian products of $n$ sets and the direct product of $n$ transformations are similarly defined.

Let $X$ be a set and $d$ be a function from $X \times X$ to the set of non-negative real numbers satisfy the following conditions:

$$
\begin{aligned}
d(a, b) & =0 \text { if and only if } a=b \\
d(a, b) & =d(b, a) \text { for every } a, b \\
d(a, b) & \leq d(a, c)+d(c, b) \text { for every } a, b, c
\end{aligned}
$$

Then, $d$ is called a distance and $X$ is called a metric space. If $X$ is a finite set, then $X$ is called a finite metric space. The distance between a point $x$ and a non-empty subset $A$ of $X$ is defined by

$$
d(x, A)=\min \{d(x, y) \mid y \in A\}
$$

where min denotes the minimum element. The distance between non- empty subsets $A$ and $B$ is defined by

$$
d(A, B)=\min \{d(x, B) \mid x \in A\}
$$

### 1.2 Permutations

Let $m$ be a positive integer. Integers $a$ and $b$ are called congruent modulo $m$, and written as $a \equiv b \bmod m$, if $a-b$ is divisible by $m$. Further, if $0 \leq b<m$ here, $b$ is the remainder obtained by dividing $a$ by $m$ and denoted by $a \% m$. The relation $\equiv \bmod m$ is an equivalence relation on $\mathbf{Z}$. The set of all equivalence classes with respect to this equivalence relation is called the residue class ring with $m$ elements. We use the two expressions $\mathbf{Z}_{m}=\{0,1,2, . ., m-1\}$ and $\mathbf{N}_{m}=\{1,2, . ., m\}$ for the residue class ring, where each equivalence class containing a representative integer a is expressed by the same integer $a$. Since we mostly use the second expression $\mathbf{N}_{m}$, its algebraic structure is described in the following. If $a$ and $b$ are elements of $\mathbf{N}_{m}$, then $a+b$ is the element $c$ of $\mathbf{N}_{m}$ such that $c \equiv a+b \bmod m$, and $a \cdot b$ is the element $c$ of $\mathbf{N}_{m}$ such that $c \equiv a \cdot b \bmod m$. Then $\mathbf{N}_{m}$ is a ring with $m$ as the zero element. For example, $-a=n-a$ for any $a=1,2, . ., m-1$, and $-m=m$. Further, we assume the order relation $1<2<\ldots<m-1<m$ in $\mathbf{N}_{m}$. Hereafter, we denote $\mathbf{N}_{n}$ simply by $\mathbf{N}$.

Lemma 1.2.1 The equation

$$
\begin{equation*}
s \cdot x=1 \tag{1.2.1}
\end{equation*}
$$

in $\mathbf{N}$ has a unique solution $x$, if and only if $s$ and $n$ are relatively prime.
Proof. For example, see Theorem 10.2 of Ore (1988, p. 238).
The unique solution $x$ of (1.2.1) is called the inverse of $s$ and denoted by $s^{-1}$ or $1 / s$. Let $\mathbf{U}_{\mathbf{n}}$ denote the set of all elements $x$ of $\mathbf{N}$ such that $x$ and $n$ are relatively prime. As shown by Lemma 1.2.1, $\mathbf{U}_{\mathbf{n}}$ is the set of all invertible elements of $\mathbf{N}$, that is, elements having multiplicative inverses, and forms a multiplicative abelian group.

If $\mathbf{G}$ is a group, then $|\mathbf{G}|$ is called the order of $\mathbf{G}$. For the order $\varphi(n)$ of $\mathbf{U}_{\mathbf{n}}, \varphi$ is known as Euler's function. If $\mathbf{H}$ is a subgroup of $\mathbf{G}$ generated by elements $\tau, \ldots, \omega$
of $\mathbf{G}$, then $\mathbf{H}$ is denoted by $\langle\tau, . ., \omega\rangle$. If $\sigma$ and $\tau$ are elements of a group $\mathbf{G}$ and if there exists an element $\gamma$ of $\mathbf{G}$ such that $\tau=\gamma^{-1} \sigma \gamma$, then $\tau$ is called a conjugate of $\sigma$, and $\sigma$ and $\tau$ are said to be conjugate.

If $h$ is a function from a group $\mathbf{G}$ to a group $\mathbf{H}$ such that $h(\sigma \tau)=(h \sigma)(h \tau)$ for all elements $\sigma$ and $\tau$ of $\mathbf{G}$, then $h$ is called a homomorphism from $\mathbf{G}$ to $\mathbf{H}$. The direct product of $n$ groups $\mathbf{G}_{\mathbf{1}}, . ., \mathbf{G}_{\mathbf{n}}$ is the Cartesian product $\mathbf{G}_{\boldsymbol{1}} \times \ldots \times \mathbf{G}_{\mathbf{n}}$ with the multiplication defined by $\left(g_{1}, \ldots, g_{n}\right)\left(g \prime_{1}, \ldots, g \prime_{n}\right)=\left(g_{1} g_{1}, \ldots, g_{n} g \prime_{n}\right)$. If $X$ is a finite set, then the set of all one-to-one transformations, which are called permutations of $X$, is a group with the composition of transformations as its binary operation. This group is called the symmetric group on $X$ and denoted by $\operatorname{SYM}(X)$. The order of $\operatorname{SYM}(X)$ is $|X|$ !. The identity element of $\operatorname{SYM}(X)$ is the identity permutation $\iota$ of $X$. A one-to-one transformation $\tau$ of length $m$ of a finite set $X$ is called a cyclic permutation, if $\operatorname{GRAPH}(\tau)$ consists of one $m$-cycle and loops. In particular, a cyclic permutation $\sigma$ of length $m$ of $X$ can be expressed by

$$
\sigma=\left(s_{1}, s_{2}, . ., s_{m}\right)
$$

if $\sigma s_{i}=s_{i+1}$ for every $1 \leq i \leq m-1, \sigma s_{m}=s_{1}$, and $\sigma j=j$ for every $j \in X$ not belonging to $\left\{s_{1}, s_{2}, . ., s_{m}\right\}$. In particular, the cyclic permutation

$$
\rho=(1,2, . ., n)
$$

is defined by $\rho i=i+1$ for every $i \in \mathbf{N}$. Then we have the following elementary theorem on permutations.

Proposition 1.2.2 If $\tau$ is not the identity permutation, then $\tau$ is a disjoint composition of cyclic permutations, each of length at least 2 .

Consider a linear function $\tau$ :

$$
\begin{equation*}
\tau i=a \cdot i+b \tag{1.2.2}
\end{equation*}
$$

on $\mathbf{N}$. For $\tau$ to be a permutation, it is necessary and sufficient that $a$ is invertible. We call $(a, b)$ the coefficients, $a$ the slope, and $b$ the segment of the linear permutation $\tau$. In this case, it is verified that

$$
\begin{gather*}
\tau \rho=\rho^{a} \tau,  \tag{1.2.3}\\
\rho \tau=\tau \rho^{a^{-1}} \tag{1.2.4}
\end{gather*}
$$

for the cyclic permutation $\rho=(1,2, . ., n)$.
The cyclic permutation $\rho$ itself is a linear permutation of coefficients $(1,1)$. If $\tau$ is a linear permutation of coefficients $(a, b)$ then $\tau^{-1}$ is a linear permutation of coefficients $\left(a^{-1},-a^{-1} b\right)$. For example, let $\tau \in \operatorname{SYM}(\mathbf{N})$ be a linear permutation of slope $-1=n-1$. If the coefficients of $\tau$ are $(-1, t)$, then $\tau^{-1}$ is a linear permutation of coefficients $(1 /-1,-t /-1)=(-1, t)$. Therefore, $\tau^{-1}=\tau$. In particular, if the coefficients of $\tau$ are $(-1,1)$, then $\tau$ is

$$
\lambda=(1, n)(2, n-1) \cdots([n / 2], n-[n / 2]+1)
$$

where $[x]$ denotes the greatest integer equal to or less than $x$. If $\sigma$ and $\tau$ are linear permutations of respective coefficients $(a, b)$ and $(c, d)$, then $\sigma \tau$ is a linear permutation of coefficients $(a c, a d+b)$. If $\tau$ is a linear permutation of slope $a$, then $\tau \rho$ and $\rho \tau$ are also linear permutations of slope $a$. Since the coefficients of $\rho$ are $(1,1)$, the coefficients of $\tau \rho$ and $\rho \tau$ are respectively $(a, a+b)$ and $(a, b+1)$, if the coefficients
of $\tau$ are $(a, b)$. In summary, we have
Proposition 1.2.3 Let $\operatorname{LIN}(\mathbf{N})$ denote the set of all linear permutations of $\mathbf{N}$. Then $\operatorname{LIN}(\mathbf{N})$ is a subgroup of the symmetric group $\operatorname{SYM}(\mathbf{N})$, and the function $h$ from $\operatorname{LIN}(\mathbf{N})$ to $\mathbf{U}_{\mathbf{n}}$ that associates each $\tau$ of $\operatorname{LIN}(\mathbf{N})$ with its slope is a homomorphism.

### 1.3 PÓLYA ACTIONS

Let $\mathbf{G}$ be a group and $X$ be a set. Then it is said that $\mathbf{G}$ acts on $X$, or $\mathbf{G}$ is a transformation group for $X$, if there is a homomorphism $H$ from $\mathbf{G}$ to $\operatorname{SYM}(X)$. In this case, $H$ is called an action of $\mathbf{G}$ on $X$ or a representation of $\mathbf{G}$ on $X$. The action $H$ is omitted from expressions in the following, when it is clear, so that $(H \tau) x$ is simply written as $\tau x$ for an element $\tau$ of $\mathbf{G}$ and an element $x$ of $X$. If $\mathbf{G}$ acts on $X$ and $x$ is an element of $X$, then the subgroup $\mathbf{G}_{x}$ defined by

$$
\mathbf{G}_{x}=\{g \in \mathbf{G} \mid g x=x\}
$$

is called the stabilizer of $x$.

Example 1.3.1 If $F$ is a one-to-one transformation of a set $X$, then the set $\mathbf{G}=\left\{F^{i} \mid i \in \mathbf{Z}\right\}$ is a subgroup of $\operatorname{SYM}(X)$ generated by $F . \mathbf{G}$ is a transformation group for $X$ since $H: \mathbf{G} \rightarrow \operatorname{SYM}(X)$ defined by $H\left(F^{i}\right)=F^{i}$ is clearly a homomorphism. The order of $\mathbf{G}$ is called the order of $F$.

If a group $\mathbf{G}$ acts on a set $D$, and $X$ is a set, then the Pólya action $H$ of $\mathbf{G}$ on $X^{D}$ is defined by

$$
((H \tau) f) d=f\left(\tau^{-1} d\right)
$$

for every element $\tau$ of $\mathbf{G}$, every element $f$ of $X^{D}$, and every element $d$ of $D$. If $\sigma$ and $\tau$ are elements of $\mathbf{G}$, then

$$
\begin{aligned}
((H(\sigma \tau)) f) d & =f\left((\sigma \tau)^{-1} d\right)=f\left(\left(\tau^{-1} \sigma^{-1}\right) d\right) \\
& =f\left(\tau^{-1}\left(\sigma^{-1} d\right)\right)=((H \tau) f)\left(\sigma^{-1} d\right)=((H \sigma)((H \tau) f)) d \\
& =(((H \sigma)(H \tau)) f) d
\end{aligned}
$$

That is,

$$
H(\sigma \tau)=(H \sigma)(H \tau)
$$

Therefore, the Pólya action is an homomorphism and hence in fact an action.
Let $\mathbf{Q}=\{0,1\}$. Then $\mathbf{Q}^{\mathbf{N}}$ is the set of all binary strings of length $n$. Let $x=\left(x_{1}, x_{2}, . ., x_{n}\right) \in \mathbf{Q}^{m}$ athbf $N$. The period of $x$ is the minimum element $k$ of $\mathbf{N}$ such that $x_{i+k}=x_{i}$ for every $i \in \mathbf{N}$. The density of $x$ denoted by $d(x)$ is the number of 1 s in $x$, i.e.

$$
d(x)=\left|\left\{i \mid x_{i}=1\right\}\right| .
$$

The Pólya action $H$ of $\operatorname{SYM}(\mathbf{N})$ on $\mathbf{Q}^{\mathbf{N}}$ associates a permutation $\tau$ of $\mathbf{N}$ with a permutation of coordinates of $\mathbf{Q}^{\mathbf{N}}$ by

$$
(H \tau)\left(x_{1}, x_{2}, . ., x_{n}\right)=\left(x_{\tau^{-1} 1}, x_{\tau^{-1} 2}, . ., x_{\tau^{-1} n}\right)
$$

$\mathbf{Q}^{\mathbf{N}}$ is simply denoted by $\mathbf{Q}^{n}$ hereafter. For example, let $\rho$ be the cyclic permutation $(1,2, . ., n)$. The transformation $\rho$ defined by the Pólya action on $\mathbf{Q}^{n}$ is the right rotation of coordinates of $\mathbf{Q}^{n}$, that is,

$$
\rho\left(x_{1}, x_{2}, . ., x_{n}\right)=\left(x_{n}, x_{1}, . ., x_{n-1}\right)
$$

for every $x=\left(x_{1}, x_{2}, . ., x_{n}\right) \in \mathbf{Q}^{n}$.
If a group $\mathbf{G}$ acts on a set $X$, then an equivalence relation $\sim_{\mathbf{G}}$ on $X$ can be defined by $x \sim_{\mathbf{G}} y$ if there is an element $\tau \in \mathbf{G}$ such that $\tau x=y$. Each equivalence class with respect to the equivalence relation $\sim_{\mathbf{G}}$ is called an orbit of $\mathbf{G}$ acting on $X$. The orbit containing an element $x$ of $X$ is denoted by $\operatorname{Orb}_{\mathbf{G}} x$. The union $\bigcup_{x \in S} \operatorname{Orb}_{\mathbf{G}} x$ of the orbits for a subset $S \subseteq X$ is denoted by $\operatorname{Orb}_{\mathbf{G}} S$. Then, the equivalence relation $\sim_{\mathbf{G}}$ is extended to the set of all non-empty subsets of $X$, that is, $A \sim_{\mathbf{G}} B$ if $\operatorname{Orb}_{\mathbf{G}} A=\operatorname{Orb}_{\mathbf{G}} B$.

### 1.4 Boolean functions

From now on, $\mathbf{Q}=\{0,1\}$ is not simply a two-point set, but regarded as the minimal Boolean algebra with the unary operation $\neg$ called complementation or negation and the binary operations $\vee$ called disjunction or $O R$ and called conjunction or AND such that

$$
\begin{aligned}
\neg 0 & =1, \quad \neg 1=0 \\
0 \vee 0 & =0, \quad 0 \vee 1=1 \vee 0=1, \quad 1 \vee 1=1 \\
0 \cdot 0 & =0 \cdot 1=1 \cdot 0=0, \quad 1 \cdot 1=1
\end{aligned}
$$

Further, the binary relation (=) can be introduced by defining

$$
x(=) y=x \cdot y \vee \neg x \cdot \neg y
$$

Let $L, M \subseteq \mathbf{N}$. If $x \in \mathbf{Q}^{M}$, then the value of $x$ at $i \in M$ is denoted by $x_{i}$. A function from $\mathbf{Q}^{M}$ to $\mathbf{Q}^{L}$ is called a Boolean function. A function from $\mathbf{Q}^{M}$ to itself is called a Boolean transformation. If $A \subseteq \mathbf{Q}^{M}$, then $1_{A}$ denotes the characteristic function for $A$, i.e. $1_{A} x=1$ if and only if $x \in A$. Let $L \subseteq M \subseteq \mathbf{N}$. Then the projection function $P_{L}: \mathbf{Q}^{M} \rightarrow \mathbf{Q}^{L}$ is defined by

$$
\left(P_{L} x\right)_{i}=x_{i} \text { for every } i \in L \text { for every } x \in \mathbf{Q}^{M}
$$

If $j \in M$, then the projection function $p_{j}: \mathbf{Q}^{M} \rightarrow \mathbf{Q}$ is defined by

$$
p_{j} x=x_{j} \text { for every } x \in \mathbf{Q}^{M} .
$$

Let $L$ and $M$ be disjoint subsets of $\mathbf{N}$. Then $\mathbf{Q}^{L \cup M}$ can be identified with the Cartesian product $\mathbf{Q}^{L} \times \mathbf{Q}^{M}$ by identifying $x \in \mathbf{Q}^{L \cup M}$ with $\left(P_{L} x, P_{M} x\right) \in$ $\mathbf{Q}^{L} \times \mathbf{Q}^{M}$, where $P_{L}: \mathbf{Q}^{L \cup M} \rightarrow \mathbf{Q}^{L}$ and $P_{M}: \mathbf{Q}^{L \cup M} \rightarrow \mathbf{Q}^{M}$ are the projection functions defined above.

Hereafter, $\mathbf{Q}^{\mathbf{N}}$ is simply denoted by $\mathbf{Q}^{n}$. Let $f$ and $g$ be Boolean functions from $\mathbf{Q}^{n}$ to $\mathbf{Q}$. Then the conjunction of $f$ and $g$ denoted by $f \cdot g$ is the function: $\mathbf{Q}^{n} \rightarrow \mathbf{Q}$ defined by

$$
(f \cdot g) x=(f x) \cdot(g x)
$$

for every $x \in \mathbf{Q}^{n}$. The disjunction of $f$ and $g$ denoted by $f \vee g$ is the function: $\mathbf{Q}^{n} \rightarrow \mathbf{Q}$ defined by

$$
(f \vee g) x=(f x) \vee(g x)
$$

for every $x \in \mathbf{Q}^{n}$. Also a unary operation $\neg$ called complementation is defined by

$$
(\neg f) x=\neg(f x)
$$

for every $x \in \mathbf{Q}^{n}$. Further, $f(=) g$ is defined by

$$
f(=) g=f \cdot g \vee \neg f \cdot \neg g
$$

In this book, we refer to the set $f$ for a Boolean function $f: \mathbf{Q}^{n} \rightarrow \mathbf{Q}$ meaning the set $f^{-1} 1$, i.e. the inverse image of 1 . Therefore, $x \in f$ means $f x=1$. Also, the set $\neg f$ is the set $f^{-1} 0$. The formula $f \subseteq g$ for Boolean functions $f$ and $g$ is clear by this identification of a Boolean function with a set. Also, $|f|$ is the number of elements of $f^{-1} 1$. Further,

$$
\begin{aligned}
f \cdot g & =f \cap g \\
f \vee g & =f \cup g \\
\neg f & =f^{c}
\end{aligned}
$$

Therefore, the corresponding laws such as the associative and commutative laws for set operations $\cap, \cup$, and ${ }^{c}$ hold for $\cdot, \vee$, and $\neg$ respectively. In particular, we will frequently use the distributive laws:

$$
\begin{aligned}
f \cdot(g \vee h) & =f \cdot g \vee f \cdot h \\
f \vee(g \cdot h) & =(f \vee g) \cdot(f \vee h)
\end{aligned}
$$

and De Morgan's law:

$$
\begin{aligned}
\neg(f \vee g) & =(\neg f) \cdot(\neg g), \\
\neg(f \cdot g) & =\neg f \vee \neg g .
\end{aligned}
$$

A conjunction $g=f_{1} \cdot f_{2} \cdots f_{m}$ of Boolean functions $f_{i}: \mathbf{Q}^{n} \rightarrow \mathbf{Q}$ is called a term of degree $m$, if there exists an injection $\varphi: \mathbf{N}_{m} \rightarrow \mathbf{N}$ such that $f_{i}=p_{\varphi i}$ or $\neg p_{\varphi i}$ for each $i$. A term $g$ is called an implicant of a Boolean function $f$ if $g \subseteq f$. An implicant $g$ of $f$ is called a prime implicant if $h=g$ for any implicant $h$ of $f$ such that $g \subseteq h$. The disjunction of terms are called a disjunctive form. A Boolean function $f$ can be represented by the disjunctive form that is the disjunction of all its prime implicants. An irredundant disjunctive form of a Boolean function $f$ is a disjunctive form that represents $f$ such that the removal of any one of its terms does not represents $f$. In this book, Boolean functions are usually expressed by an irredundant disjunctive form.

Let $L$ and $M$ be disjoint subsets of $\mathbf{N}$, and $f$ and $g$ be respectively Boolean functions from $\mathbf{Q}^{L}$ to $\mathbf{Q}$ and $\mathbf{Q}^{M}$ to $\mathbf{Q}$. Then the product $f \cdot g$ is the function from $\mathbf{Q}^{L \cup M}$ to $\mathbf{Q}$ defined by

$$
f \cdot g=\left(f \circ P_{L}\right) \cdot\left(g \circ P_{M}\right)
$$

Let $a$ an element of $\mathbf{Q}^{M}$, where $M$ is a proper subset of $\mathbf{N}$, and $f: \mathbf{Q}^{\mathbf{N}} \rightarrow \mathbf{Q}$. Then $f \mid a$ is the function from $\mathbf{Q}^{\mathbf{N} \backslash \mathbf{M}}$ to $\mathbf{Q}$ defined by

$$
(f \mid a) x=f(x, a)
$$

where $(a, x)$ is an element of $\mathbf{Q}^{\mathbf{N}}$ defined by

$$
P_{M}(a, x)=a \quad \text { and } \quad P_{N \backslash M}(a, x)=x
$$

Clearly $\neg f \mid a=\neg(f \mid a) . f$ can be expressed as

$$
f=p_{i} \cdot(f \mid 1) \vee \neg p_{i} \cdot(f \mid 0),
$$

where $1,0 \in \mathbf{Q}^{\{i\}}$. Conversely, if $f=p_{i} \cdot g \vee \neg p_{i} \cdot h$ for $g, h: \mathbf{Q}^{\mathbf{N} \backslash i} \rightarrow \mathbf{Q}$, then $g=f \mid 1$ and $h=f \mid 0$.

