PARIS LODRON UNIVERSITÄT SALZBURG
Fachbereich Informatik

VO Formale Systeme

Formulary

Universität:	PLUS Salzburg
Fachbereich:	Informatik
Lehrveranstaltung:	Formale Systeme VO
LV-Leiter:	Assoz. Prof. Priv.-Doz. Dr. Ana Sokolova
Verfasser ©:	Günther Pritz
Matrikelnummer:	09620251
Abgabedatum:	30.01.2023
Dokumentenversion:	V_07

Part I
Calculations

1 Equivalences for connectives

1.1 Commutativity

$$P \wedge Q \overset{val}{=\!=} Q \wedge P$$
$$P \vee Q \overset{val}{=\!=} Q \vee P$$
$$P \Leftrightarrow Q \overset{val}{=\!=} Q \Leftrightarrow P$$

1.2 Associativity

$$P \wedge Q \overset{val}{=\!=} Q \wedge P$$
$$P \vee Q \overset{val}{=\!=} Q \vee P$$
$$(P \Leftrightarrow Q) \Leftrightarrow R \overset{val}{=\!=} P \Leftrightarrow (Q \Leftrightarrow R)$$

1.3 Idempodence

$$P \wedge P \overset{val}{=\!=} P$$
$$P \vee P \overset{val}{=\!=} P$$

1.4 Double Negation

$$\neg\neg P \overset{val}{=\!=} P$$

1.5 Inversion

$$\neg True \overset{val}{=\!=} False$$
$$\neg False \overset{val}{=\!=} True$$

1.6 True/False elemination

$$P \wedge True \overset{val}{=\!=} P$$
$$P \wedge False \overset{val}{=\!=} False$$
$$P \vee True \overset{val}{=\!=} True$$
$$P \vee False \overset{val}{=\!=} P$$

1.7 Negation

$$\neg P \overset{val}{=\!=} (P \Rightarrow False)$$

1.8 Contradiction / Excl. middle

$$P \wedge \neg P \overset{val}{=\!=} False$$
$$P \vee \neg P \overset{val}{=\!=} True$$

1.9 Distributivity

$$P \wedge (Q \vee R) \stackrel{val}{=\!=} (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) \stackrel{val}{=\!=} (P \vee Q) \wedge (P \vee R)$$

1.10 De Morgan

$$\neg(P \wedge Q) \stackrel{val}{=\!=} \neg P \vee \neg Q$$
$$\neg(P \vee Q) \stackrel{val}{=\!=} \neg P \wedge \neg Q$$

1.11 Implication

$$P \Rightarrow Q \stackrel{val}{=\!=} \neg P \vee Q$$

1.12 Contraposition

$$P \Rightarrow Q \stackrel{val}{=\!=} \neg Q \Rightarrow \neg P$$

1.13 Bi-implication

$$P \Rightarrow Q \stackrel{val}{=\!=} \neg P \vee Q$$

1.14 Self-equivalence

$$P \Rightarrow Q \stackrel{val}{=\!=} \neg Q \Rightarrow \neg P$$

1.15 Absorption

$$P \wedge (P \vee Q) \stackrel{val}{=\!=} P$$
$$P \vee (P \wedge Q) \stackrel{val}{=\!=} P$$

Notes

2 Weakening rules

2.1 $\wedge\vee$ - weakening

$$P \wedge Q \stackrel{val}{\models} P$$
$$P \stackrel{val}{\models} P \vee Q$$

2.2 Extremes

$$False \stackrel{val}{\models} P$$
$$P \stackrel{val}{\models} P$$

2.3 Monotonicity

If $P \stackrel{val}{\models} Q$, then $P \wedge R \stackrel{val}{\models} Q \wedge R$
If $P \stackrel{val}{\models} Q$, then $P \vee R \stackrel{val}{\models} Q \vee R$

3 Properties for proposional logic

3.1 Lemma E1

$P \stackrel{val}{=\!=} Q$ **iff** $P \Leftrightarrow Q$ is a tautology

3.2 Lemma EW1

$P \stackrel{val}{=\!=} Q$ **iff** $P \stackrel{val}{\models} Q$ and $Q \stackrel{val}{\models} P$

3.3 Lemma W2

$P \overset{val}{\models} P$

3.4 Lemma W3

$P \overset{val}{\models} Q$ and $Q \overset{val}{\models} R$ **then** $P \overset{val}{\models} R$

3.5 Lemma W4

$P \overset{val}{\models} Q$ **iff** $P \Rightarrow Q$ is a tautology

4 Equivalences for quantifiers

4.1 Bound variable

$$\forall_x [P : Q] \overset{val}{=\!=} \forall_y [P[y \text{ for } x] : Q[y \text{ for } x]]$$
$$\exists_x [P : Q] \overset{val}{=\!=} \exists_y [P[y \text{ for } x] : Q[y \text{ for } x]]$$

4.2 Domain splitting

$$\forall_x [P \vee Q : R] \overset{val}{=\!=} \forall_x [P : Q] \wedge \forall_x [P : R]$$
$$\exists_x [P \vee Q : R] \overset{val}{=\!=} \exists_x [P : Q] \vee \exists_x [P : R]$$

4.3 One element

$$\forall_x [x = n : Q] \overset{val}{=\!=} Q[n \text{ for } x]$$
$$\exists_x [x = n : Q] \overset{val}{=\!=} Q[n \text{ for } x]$$

4.4 Empty domain

$$\forall_x [False : Q] \overset{val}{=\!=} True$$
$$\exists_x [False : Q] \overset{val}{=\!=} False$$

4.5 Domain weakening

$$\forall_x [P \wedge Q : R] \overset{val}{=\!=} \forall_x [P : Q \Rightarrow R]$$
$$\exists_x [P \wedge Q : R] \overset{val}{=\!=} \exists_x [P : Q \wedge R]$$

4.6 De Morgan

$$\neg\forall_x [P : Q] \overset{val}{=\!=} \exists_x [P : \neg Q]$$
$$\neg\exists_x [P : Q] \overset{val}{=\!=} \forall_x [P : \neg Q]$$

4.7 Exchange trick

$$\forall_x [P : Q] \overset{val}{=\!=} \forall_x [\neg Q : \neg P]$$
$$\exists_x [P : Q] \overset{val}{=\!=} \exists_x [Q : P]$$

4.8 Term splitting

$$\forall_x [P : Q \wedge R] \stackrel{val}{=\!=} \forall_x [P : Q] \wedge \forall_x [P : R]$$
$$\exists_x [P : Q \vee R] \stackrel{val}{=\!=} \exists_x [P : Q] \vee \exists_x [P : R]$$

4.9 Monotonicity of quantifiers

$$\forall_x [P : Q \Rightarrow R] \Rightarrow (\forall_x [P : Q] \Rightarrow \forall_x [P : R]) \stackrel{val}{=\!=} True$$
$$\forall_x [P : Q \Rightarrow R] \Rightarrow (\exists_x [P : Q] \Rightarrow \exists_x [P : R]) \stackrel{val}{=\!=} True$$

5 Properties for predicate logic

5.1 Lemma E1

$P \stackrel{val}{=\!=} Q$ **iff** $P \Leftrightarrow Q$ is a tautology

5.2 Lemma EW1

$P \stackrel{val}{=\!=} Q$ **iff** $P \stackrel{val}{\models} Q$ and $Q \stackrel{val}{\models} P$

5.3 Lemma W2

$P \stackrel{val}{\models} P$

5.4 Lemma W3

$P \stackrel{val}{\models} Q$ and $Q \stackrel{val}{\models} R$ **then** $P \stackrel{val}{\models} R$

5.5 Lemma W4

$P \stackrel{val}{\models} Q$ **iff** $P \Rightarrow Q$ is a tautology

5.6 Lemma W5

$Q \stackrel{val}{\models} R$ **then** $\forall_x [P : Q] \stackrel{val}{\models} \forall_x [P : R]$

Part II
Derivations

6 Flag derivation rules for connectives

6.1 $\wedge$ - elimination

	$\ldots$
(k)	$P \wedge Q$
	$\ldots$
	$\{ \wedge$ - **elim** on (k) $\}$
(l)	P
	$\ldots$
	$\{ \wedge$ - **elim** on (k) $\}$
(m)	Q

$(k < l) \wedge (k < m)$

6.2 $\wedge$ - introduction

	$\ldots$
(k)	P
	$\ldots$
(l)	Q
	$\ldots$
	$\{ \wedge$ - **intro** on (k) and (l) $\}$
(m)	$P \wedge Q$

$(k < m) \wedge (l < m)$

6.3 $\Rightarrow$ - elimination

	$\ldots$
(k)	$P \Rightarrow Q$
	$\ldots$
(l)	P
	$\ldots$
	$\{ \Rightarrow$ - **elim** on (k) and (l) $\}$
(m)	Q

$(k < m) \wedge (l < m)$

6.4 $\Rightarrow$ - introduction

	$\ldots$
	$\{$ Assume $\}$
(k)	$\boxed{P}$
	$\quad \ldots$
$(l-1)$	$\quad Q$
	$\{ \Rightarrow$ - **intro** on (k) and (l) $\}$
(l)	$P \Rightarrow Q$

6.5 $\neg$ - elimination

$$
\begin{array}{ll}
 & \dots \\
(k) & P \\
 & \dots \\
(l) & \neg P \\
 & \dots \\
 & \{\ \neg\text{ - }\textbf{elim}\text{ on } (k) \text{ and } (l)\ \} \\
(m) & F
\end{array}
$$

$(k < m) \wedge (l < m)$

6.6 $\neg$ - introduction

$$
\begin{array}{ll}
 & \dots \\
 & \{\ \text{Assume}\ \} \\
(k) & \boxed{P} \\
 & \quad \dots \\
(l-1) & \quad F \\
 & \{\ \neg\text{ - }\textbf{intro}\text{ on } (k) \text{ and } (l-1)\ \} \\
(l) & \neg P
\end{array}
$$

6.7 F - elimination

$$
\begin{array}{ll}
 & \dots \\
(k) & F \\
 & \dots \\
 & \{\ F\ \textbf{elim}\text{ on } (k)\ \} \\
(l) & P
\end{array}
$$

$(k < l)$

6.8 F - introduction

$$
\begin{array}{ll}
 & \dots \\
(k) & P \\
 & \dots \\
(l) & \neg P \\
 & \dots \\
 & \{\ F\text{ - }\textbf{intro}\text{ on } (k) \text{ and } (l)\ \} \\
(m) & F
\end{array}
$$

$(k < m) \wedge (l < m)$

6.9 $\neg\neg$ - elimination

$$
\begin{array}{ll}
 & \dots \\
(k) & \neg\neg P \\
 & \dots \\
 & \{\ \neg\neg\text{ - }\textbf{elim}\text{ on } (k)\ \} \\
(l) & P
\end{array}
$$

$(k < l)$

6.10 $\neg\neg$ - introduction

$$
\begin{array}{ll}
 & \dots \\
(k) & P \\
 & \dots \\
 & \{\ \neg\neg\text{ - }\textbf{intro}\text{ on } (k)\ \} \\
(l) & \neg\neg P
\end{array}
$$

$(k < l)$

6.11 $\vee$ - elimination

$$
\begin{array}{ll}
 & \dots \\
(k) & P \vee Q \\
 & \dots \\
 & \{\ \vee\text{ - }\textbf{elim}\text{ on } (k)\ \} \\
(l) & \neg P \Rightarrow Q \\
 & \dots \\
 & \{\ \vee\text{ - }\textbf{elim}\text{ on } (k)\ \} \\
(m) & \neg Q \Rightarrow P
\end{array}
$$

$(k < m) \wedge (l < m)$

6.12 $\vee$ - introduction

$$
\begin{array}{ll}
 & \dots \\
 & \{\ \text{Assume}\ \} \\
(k) & \boxed{\neg P} \\
 & \quad \dots \\
(l-1) & \quad Q \\
 & \{\ \vee\text{ - }\textbf{intro}\text{ on } (k) \text{ and } (l-1)\ \} \\
(l) & P \vee Q
\end{array}
$$

6.13 ⇔ - elimination

	$\ldots$
(k)	$P \Leftrightarrow Q$
	$\ldots$
	$\{ \Leftrightarrow$ - **elim** on (k) $\}$
(l)	$P \Rightarrow Q$
	$\ldots$
	$\{ \vee$ - **elim** on (k) $\}$
(m)	$Q \Rightarrow P$

$(k < m) \wedge (l < m)$

6.14 ⇔ - introduction

	$\ldots$
(k)	$P \Rightarrow Q$
	$\ldots$
(l)	$Q \Rightarrow P$
	$\ldots$
	$\{ \Leftrightarrow$ - **intro** on (k) and (l) $\}$
(m)	$P \Leftrightarrow Q$

$(k < m) \wedge (l < m)$

6.15 Proof by contradiction

	$\ldots$
k	$\boxed{\neg P}$
	$\ldots$
$(l-1)$	F
	$\{ \neg$ - **intro** on (k) and $(l-1)$ $\}$
(l)	$\neg\neg P$
	$\{ \neg\neg$ - **elim** on (l) $\}$
$(l+1)$	P

$(k < l)$

6.16 Proof by case distinction

	$\ldots$
(k)	$P \vee Q$
	$\ldots$
(l)	$P \Rightarrow R$
	$\ldots$
(m)	$Q \Rightarrow R$
	$\ldots$
	$\{$ **case-dist** on (k),(l),(m) $\}$
(n)	R

$(k < n) \wedge (l < n) \wedge (m < n)$

7 Flag derivation rules for quantifiers

7.1 $\forall$ - elimination

$$\begin{array}{ll}
 & \ldots \\
(k) & \forall_x\,[P(x) : Q(x)] \\
 & \ldots \\
(l) & P(a) \\
 & \ldots \\
 & \{\ \forall\text{ - }\textbf{elim}\text{ on } (k) \text{ and } (l)\ \} \\
(m) & Q(a)
\end{array}$$

$(k < m) \wedge (l < m)$

7.2 $\forall$ - introduction

$$\begin{array}{ll}
 & \ldots \\
 & \{\ \text{Assume}\ \} \\
(k) & \boxed{\textbf{var } x; P(x)} \\
 & \quad \ldots \\
(l-1) & \quad Q(x) \\
 & \{\ \forall\text{ - }\textbf{intro}\text{ on } (k) \text{ and } (l)\ \} \\
(l) & \forall_x\,[P(x) : Q(x)]
\end{array}$$

7.3 $\exists$ - elimination

$$\begin{array}{ll}
 & \ldots \\
(k) & \exists_x\,[P(x) : Q(x)] \\
 & \ldots \\
(l) & \forall_x\,[P(x) : \neg Q(x)] \\
 & \ldots \\
 & \{\ \exists\text{ - }\textbf{elim}\text{ on } (k) \text{ and } (l)\ \} \\
(m) & False
\end{array}$$

$(k < m) \wedge (l < m)$

7.4 $\exists$ - introduction

$$\begin{array}{ll}
 & \ldots \\
 & \{\ \text{Assume}\ \} \\
(k) & \boxed{\forall_x\,[P(x) : \neg Q(x)]} \\
 & \quad \ldots \\
(l-1) & \quad F \\
 & \{\ \exists\text{ - }\textbf{intro}\text{ on } (k) \text{ and } (l-1)\ \} \\
(l) & \exists_x\,[P(x) : Q(x)]
\end{array}$$

7.5 $\exists*$ - elimination

$$\begin{array}{ll}
 & \ldots \\
(k) & \exists_x\,[P(x) : Q(x)] \\
 & \ldots \\
 & \{\ \exists*\text{ - }\textbf{elim}\text{ on } (k)\ \} \\
(l) & \textbf{Pick } a \text{ with } P(a) \text{ and } Q(a)
\end{array}$$

$(k < l)$

7.6 $\exists*$ - introduction

$$\begin{array}{ll}
 & \ldots \\
(k) & P(a) \\
 & \ldots \\
(l) & Q(a) \\
 & \ldots \\
 & \{\ \exists*\text{ - }\textbf{intro}\text{ on } (k) \text{ and } (l)\ \} \\
(m) & \exists_x\,[P(x) : Q(x)]
\end{array}$$

$(k < m) \wedge (l < m)$

Part III
Sets

8 Sets definitions

8.1 Subset $\subseteq$

Let X and Y be sets. X is subset of Y iff every element of X is element of Y.

$$X \subseteq Y :\Leftrightarrow \forall_x \left[x \in X \Rightarrow x \in Y\right]$$

8.2 Set equality $=$

Two sets X and Y are equal iff both $X \subseteq Y$ and $Y \subseteq X$ hold.

$$X = Y :\Leftrightarrow X \subseteq Y \wedge Y \subseteq X$$

or

$$X = Y :\Leftrightarrow \forall_x [x \in X \Leftrightarrow x \in Y]$$

8.3 Proper subset $\subset$

Let X and Y be sets. X is proper subset of Y iff every element of X is element of Y and $X \neq Y$.

$$X \subset Y :\Leftrightarrow X \subseteq Y \wedge X \neq Y$$

8.4 Union $\cup$

Let X and Y be sets. The union of X and Y is the set

$$X \cup Y = \{x \mid x \in X \vee x \in Y\}$$

8.5 Intersection $\cap$

Let X and Y be sets. The intersection of X and Y is the set

$$X \cap Y = \{x \mid x \in X \wedge x \in Y\}$$

8.6 Set difference $\setminus$

Let X and Y be sets. The set difference of X and Y is the set

$$X \setminus Y = \{x \mid x \in X \land x \notin Y\}$$

8.7 Disjoint sets

Let X and Y be sets. X and Y are disjoint if $X \cap Y = \emptyset$

8.8 Complement ^{c}

Let X be a set. The complement of X in a universial set $\mathbb{U}$ is the set

$$X^c = \{x \mid x \in \mathbb{U} \land x \notin X\}$$

8.9 Direct product $\times$

The direct product, or just product, of X and Y is the set

$$X \times Y = \{(x, y) \mid x \in X \land y \in Y\}$$

8.10 Powerset $\mathcal{P}$

The powerset of X is the set of all subsets of X

$$\mathcal{P}(X) = 2^X = \{S \mid S \subseteq X\}$$

$|\mathcal{P}(X)| = 2^{|X|}$

Part IV
Relations

9 Relations definitions

9.1 Definition 1: (Binary) Relation

Let A and B be sets. A (binary) relation between A and B is a subset of $A \times B$. Hence, $R \subseteq A \times B$.

9.2 Definition 2: Relation on a set

R is a relation on A if $R \subseteq A \times A$.

10 Relation properties for $R \subseteq A \times A$

10.1 Definition: reflexive

$reflexive :\Leftrightarrow \forall a\, [a \in A \mid (a, a) \in R]$

10.2 Definition: irreflexive

$irreflexive :\Leftrightarrow \forall a\, [a \in A : (a, a) \notin R]$

10.3 Definition: symmetric

$symmetric :\Leftrightarrow \forall a, b\, [a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R]$

10.4 Definition: asymmetric

$asymmetric :\Leftrightarrow \forall a, b\, [a, b \in A : (a, b) \in R \Rightarrow (b, a) \notin R]$

10.5 Definition: antisymmetric

$antisymmetric :\Leftrightarrow \forall a, b\, [a, b \in A : (a, b) \in R \wedge (b, a) \in R \Rightarrow a = b]$

10.6 Definition: transitive

$transitive :\Leftrightarrow \forall a, b, c\,[a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R]$

10.7 Definition: total

$total :\Leftrightarrow \forall a, b\,[a, b \in A : (a, b) \in R \vee (b, a) \in R]$

11 Special relations

11.1 Definition 3: Equivalence

A relation for $R \subseteq A \times A$ is an equivalence iff R is

- reflexive
- symmetric
- transitive

11.2 Definition 4: (Partial) order

A relation for $R \subseteq A \times A$ is a partial order iff R is

- reflexive
- antisymmetric
- transitive

11.3 Definition 5: Strict order

A relation for $R \subseteq A \times A$ is a strict order iff R is

- irreflexive
- transitive

11.4 Definition 6: Preorder

A relation for $R \subseteq A \times A$ is a preorder iff R is

- reflexive
- transitive

11.5 Definition 7: Total order

A relation for $R \subseteq A \times A$ is a total order or (linear order, chain) iff R is a total partial order. So R is

- reflexive
- antisymmetric
- transitive
- total

11.6 Obvious properties

- Every partial order is a preorder.
- Every total order is a partial order.
- Every total order is a preorder
- If $R \subseteq A \times A$ is relation that contains a cycle, i.e.,
  $\exists a, b \in A.\ a \neq b \wedge aRb \wedge bRa$
  then R is **not a partial order, not a strict order, not a total order**.

12 Operations on relations

12.1 Definition 8: Relation composition $\circ$

Given $R \subseteq A \times B$ and $S \subseteq B \times C$, the relation composition $R \circ S \subseteq A \times C$ is given by

$$R \circ S := \{(a,c) \in A \times C \mid \exists b \in B.(a,b) \in R \wedge (b,c) \in S\}$$

Composition relation is associative

$$R \circ (S \circ T) = (R \circ S) \circ T$$

We write R^n for the composition of R with itself n times, if $R \subseteq A \times A$

12.2 Definition 9: Inverse relation R^{-1}

Given a relation $R \subseteq A \times B$, the inverse relation of R, is defined as

$$R^{-1} := \{(b,a) \mid (a,b) \in R\}$$

For $R \subseteq A \times B$ we have $R^{-1} \subseteq B \times A$.

12.3 Lemma 1

Let $R \subseteq A \times A$ then

- R is reflexive iff $\Delta_A \subseteq R$
- R is symetric iff $R \subseteq R^{-1}$
- R is transitive iff $R^2 \subseteq R$

13 Important relations

13.1 Definition: Diagonal on X Δ_X

Let X be an arbitrary set, then the Diagonal on X, Δ_X, is defined as

$$\Delta_X = 1_X = Id_X := \{(x,y) \in X \times X \mid x = y\} = \{(x,x) \mid x \in X\}$$

13.2 Definition: Divisibility relation $\mid$

Let $n \in \mathbb{N}$ and $z \in \mathbb{Z}$ then

$$n \mid z :\Leftrightarrow \exists k \in \mathbb{Z}.\ z = k \cdot n$$

13.3 Definition 10: Equivalence modulo n $\equiv_n$

Let $n \in \mathbb{N}$. The relation $\equiv_n$ on $\mathbb{Z}$ is defined as

$$i \equiv_n j :\Leftrightarrow n \mid (i - j)$$

or

$$i \equiv_n j :\Leftrightarrow \exists k \in \mathbb{Z}.\ i - j = k \cdot n$$

13.4 Lemma 2

The relation $\equiv_n$ is an equivalence for every $n \in \mathbb{N}$.

Part V
Equivalences

14 Equivalences

14.1 Definition 1: Equivalence Class

Let $R \subseteq A \times A$ an equivalence relation on A, and let $a \in A$. Then the equivalence class of a under R, notation $[a]_R$ is the set

$$[a]_R := \{b \in A \mid (a, b) \in R\}$$

14.2 Definition 2: Quotient

Let $R \subseteq A \times A$ an equivalence relation on A, then the quotient (D. Faktormenge od. Quotionentenmenge) of A under R is the set of all R-equivalence classes, i.e.

$$A/R := \{[a]_R \mid a \in A\}$$

14.3 Lemma 1:

Let R be an equivalence on A. Then

$$\forall a, b \in A.\ [a]_R = [b]_R \ \vee \ [a]_R \cap [b]_R = \emptyset$$

14.4 Lemma 2:

Let R be an equivalence on A. Then

$$A = \bigcup_{a \in A} [a]_R$$

15 Partitions

15.1 Definition 3: Partition

Let A be a set. A subset P of the powerset of A ($P \subseteq \mathcal{P}(A)$) is a partition of A if it satisfies the following properties:

P1.)
$$\forall U \in P.\ U \neq \emptyset$$

P2.)
$$\forall U, V \in P.\ U \neq V \Rightarrow U \cap V = \emptyset$$

P3.)
$$\bigcup_{U \in P} = A$$

The elements of a partition are called **classes**.

15.2 Theorem 1: Equivalence and Partitions

Let A be a set.

1.) If R is an equivalence on A, then the set
$$P(R) := A/R = \{[a]_R \mid a \in A\}$$
is a **partition**.

2.) If P is a partition of A, then the relation
$$R(P) := \{(x, y) \in A \times A \mid \exists U \in P.\ x \in U \wedge y \in U\}$$
is an **equivalence**.

The assignments $R \mapsto P(R)$ and $P \mapsto R(P)$ are inverse to each other, i.e.,
$$R(P(R)) = R \quad \text{and} \quad P(R(P)) = P$$

16 Transitive closure

16.1 Definition 4: Transitive closure

Let $R \subseteq A \times A$ be a relation on A. The transitive closure of R, notation R^+, is the relation (inner-characterisation)
$$R^+ := \bigcup_{\substack{n \in \mathbb{N} \\ n \neq 0}} R^n = R \cup R^2 \cup R^3 \cup \dots$$

Alternative definition (outer-characterisation):
$$R^+ := \bigcap_{\substack{T \subseteq A \times A \\ T^2 \subseteq T \\ R \subseteq T}} T$$

16.2 Definition 5: Transitive and reflexive closure

Let $R \subseteq A \times A$ be a relation on A. The transitive closure of R, notation R^*, is the relation

$$R^* := \Delta_A \cup R^+$$

hence $R^0 = \Delta_A$

$$R^* := \bigcup_{n \in \mathbb{N}} R^n = \Delta_A \cup R \cup R^2 \cup R^3 \cup \dots$$

16.3 Definition 6: Equivalence closure

Let $R \subseteq A \times A$ be a relation on A. The equicalence closure of R, notation $E(R)$, is the relation

$$E(R) := (R \cup R^{-1})^*$$

16.4 Proposition 1: Transitive closure

Let R be a relation on A.
The transitive closure R^+ is the smallest transitive relation that contains R.

16.5 Proposition 2: Transitive and reflexive closure

Let R be a relation on A.
The transitive and reflexive closure R^* is the smallest transitive and reflexive relation that contains R.

16.6 Proposition 3: Equivalence closure

Let R be a relation on A.
The equivalence closure $E(R)$ is the smallest equivalence relation that contains R.

Part VI
Functions

17 Functions

17.1 Definition 1: Function, Map, Mappings

Let A and B be sets. A function f from A (domain) to B (codomain), notation $f : A \to B$ is an assignment of elements of B to elements of A that satisfies:

$$\forall a \in A.\ \exists! b \in B.\ b = f(a)$$

This can be split into the following two predicate logic formulas:

$$\forall a \in A.\ \exists b \in B.\ b = f(a)$$
$$\forall a_1, a_2 \in A.\ a_1 = a_2 \Rightarrow f(a_1) = f(a_2)$$

17.2 Definition 2: Equality of functions

Two functions $f : A \to B$ to $g : C \to D$ are equal iff

1.) $A = C$, dom f = dom g, domains are equal

2.) $B = D$, cod f = cod g, codomains are equal

3.) $\forall a \in A.\ f(a) = g(a)$, images are equal

17.3 Definition 3: Graph

If $f : A \to B$ is a function, then the graph of f, notation graph(f), is a relation defined by:

$$\text{graph}(f) := \{(x, y) \in A \times B \mid y = f(x)\}$$

17.4 Definition 4: Image

Let $f : A \to B$ and $A' \subseteq A$. The Image of A' is the set:

$$f(A') := \{f(a) \mid a \in A'\}$$

Alternative definition:

$$f(A') := \{b \in B \mid \exists a \in A'.\ b = f(a)\}$$

From this definition we see:
$$f(A') \subseteq B$$
$$a \in A' \Rightarrow f(a) \in f(A')$$

17.5 Definition 5: Inverse image

Let $f : A \to B$ and $B' \subseteq B$. The inverse image of B' is the set:

$$f^{-1}(B') := \{a \mid f(a) \in B'\}$$

From this definition we see:
$$f^{-1}(B') \subseteq A$$
$$a \in f^{-1}(B') \Leftrightarrow f(a) \in B'$$

The inverse image induces a function

$$f^{-1} : \mathcal{P}(B) \to \mathcal{P}(A)$$

17.6 Lemma 1:

Let $f : A \to B$, $A' \subseteq A$, $B' \subseteq B$. then

$$A' \subseteq f^{-1}(f(A')) \quad \text{and} \quad f(f^{-1}(B')) \subseteq B'$$

18 Special Functions

18.1 Definition 6: Injection

A function $f : A \to B$ is injective, or an injection, iff

$$\forall a, b \in A.\ f(a) = f(b) \Rightarrow a = b$$

18.2 Definition 7: Surjection

A function $f : A \to B$ is surjective, or a Surjection, iff

$$\forall b \in B.\ \exists a \in A.\ b = f(a)$$

18.3 Definition 8: Bijection

A function $f : A \to B$ is bijective, or a Bijection, iff f is both, injective and surjective.

18.4 Lemma 2:

A function $f : A \to B$ is injective iff

$$\forall b \in B.\ |f^{-1}(\{b\})| \leq 1$$

18.5 Lemma 3:

A function $f : A \to B$ is surjective iff

1.) $\forall b \in B.\ |f^{-1}(\{b\})| \geq 1$

2.) $f(A) = B$

18.6 Lemma 4:

A function $f : A \to B$ is bijective iff

$$\forall b \in B.\ |f^{-1}(\{b\})| = 1$$

18.7 Proposition 1:

Let function $f : A \to B$ be injective and let $A' \subseteq A$. Then

$$f^{-1}(f(A')) = A'$$

Special case of *Lemma 1*

18.8 Lemma 5:

Let function $f : A \to B$ be injective and let $A' \subseteq A$. Then

$$a \in A' \Leftrightarrow f(a) \in f(A')$$

18.9 Proposition 2:

Let function $f : A \to B$ be surjective and let $B' \subseteq B$. Then

$$f(f^{-1}(B')) = B'$$

Special case of *Lemma 1*

19 Function Composition and Inverse Fucntion

19.1 Definition 9: Composition

For $f : A \to B$ and $g : B \to C$ the composition $g \circ f$, read as g after f, is the function

$$g \circ f : A \to C$$

defined by

$$\forall a \in A.\ g \circ f(a) := g(f(a))$$

19.2 Lemma 6:

For $f : A \to B$ and $g : B \to C$ be injective. Then $g \circ f$ is injective.

19.3 Lemma 7:

For $f : A \to B$ and $g : B \to C$ be surjective. Then $g \circ f$ is surjective.

19.4 Corollary 1:

For $f : A \to B$ and $g : B \to C$ be bijective. Then $g \circ f$ is bijective.

19.5 Definition 10: Inverse Function

Let $f : A \to B$ be bijective. Then there exists a function $f^{-1} : B \to A$, read "f inverse", defined by

$$f^{-1}(b) = a \Leftrightarrow f(a) = b$$

19.6 Lemma 8:

Let $f : A \to B$ be bijective. Then

$$f^{-1} \circ f = id_A$$

$$f \circ f^{-1} = id_B$$

where $id_X : X \to X$ is the (bijective) function defined by

$$id_X(x) = x$$

19.7 Theorem 1:

A function $f : A \to B$ is bijective iff there exists a function $g : B \to A$ with

$$g \circ f = id_A \quad \text{and} \quad f \circ g = id_B$$

Part VII
Cardinals

20 Cardinals

20.1 Definition 1: Equivalent sets, equal cardinality $|A| = |B|$

Let A and B be sets. We say, that A and B have the same cardinality, or are equivalent, and write $A \sim B$ or $|A| = |B|$ iff there exists a bijection $f : A \to B$.

20.2 Definition 2: Cardinality $|A|$

Given a set A, we write $|A|$ for the $\sim$-equivalence class

$$\begin{aligned}[A]_\sim &= \{X \mid X \text{ is a set and } A \sim X\} \\ &= \{X \mid \text{ there exists bijection} f : A \to X\}\end{aligned}$$

and call it the cardinality of A.

20.3 Proposition 1: Equivalent sets, equal cardinality

The relation $\sim$ is a equivalence relation on sets.

21 Relations on cardinals

21.1 Definition 3: $\leq$

The relation $\leq$ is defined on cardinals by

$$A \leq B :\Leftrightarrow \text{ there exists an injection } f : A \to B$$

21.2 Definition 4: $\geq$

The relation $\geq$ is defined on cardinals by

$$A \geq B :\Leftrightarrow B = \emptyset \text{ or there exists a surjection } f : A \to B$$

21.3 Definition 5: $<$

The relation $<$ is defined on cardinals by

$$A < B :\Leftrightarrow \text{ there exists an injection } f : A \to B \text{ but no surjection } f : A \to B$$

21.4 Lemma 1:

The relation $\leq$ on cardinals is well-defined, i.e., if A, B, C, D are sets such that $|A| = |C|$ and $|B| = |D|$ and $|A| \leq |B|$, then $|C| \leq |D|$.

21.5 Lemma 2:

Let A, B be sets. Then
$$|A| \geq |B| \Leftrightarrow |B| \leq |A|$$

21.6 Lemma 3:

The relation $\leq$ on cardinals is reflexive.

21.7 Lemma 4:

The relation $\leq$ on cardinals is transitive.

21.8 Theorem 5: Cantor-Schröder-Bernstein

If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$

22 Operations on relations

22.1 Definition 6: $+$

Let $|A|$ and $|B|$ be two cardinals with $A \cap B = \emptyset$. Then
$$|A| + |B| := |A \cup B|$$

22.2 Definition 7: $\circ$

Let $|A|$ and $|B|$ be two cardinals. Then
$$|A| \circ |B| := |A \times B|$$

22.3 Definition 8: $|A|^{|B|}$

Let $|A|$ and $|B|$ be two cardinals. Then
$$|A|^{|B|} := |A^B|$$
where
$$A^B := \{f \mid f : B \to A\}$$

22.4 Proposition 2:

Let A be a set. Then

$$|\mathcal{P}| = 2^{|A|}$$

with

$$2 = |\{0, 1\}|$$

23 Finite Sets, Finite Cardinals

23.1 Definition 9: Finite set

A set A is finite iff $|A| = k$ for some $k \in \mathbb{N}$

24 Infinite, Countable and Uncountable Sets

24.1 Lemma 5:

$$\aleph_0 + 1 = \aleph_0$$

24.2 Lemma 6:

$$\aleph_0 + \aleph_0 = \aleph_0$$

24.3 Definition 10: Countable set

A set A is countable iff $|A| = \aleph_0$

24.4 Definition 11: Ininite set

A set A is infinite iff $|A| \geq \aleph_0$

24.5 Definition 12: Uncountable set

A set A is uncountable iff $|A| > \aleph_0$

24.6 Proposition 3:

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable sets.

24.7 Proposition 4:

$\mathbb{R}$ is uncountable.

24.8 Definition 13: c

We write c for the cardinality of $\mathbb{R}$, i.e. $c := |\mathbb{R}|$. Here c stands for *continuum.*

24.9 Theorem 2: small Cantor theorem

Let A be any set. Then $|A| < |\mathcal{P}(A)|$, i.e., $|A| < 2^{|A|}$.

24.10 Corollary 1:

Cardinals are unbounded, i.e., for any cardinal $|A|$ we can construct an infinite ascending chain of cardinals:

$$|A| < \mathcal{P}(A) < \mathcal{P}(\mathcal{P}(A)) < \mathcal{P}(\mathcal{P}(\mathcal{P}(A))) < \dots$$

24.11 Corollary 2:

$$\aleph_0 < c$$

Part VIII
Naturals

25 Naturals

First let us define a function $s : \mathbb{N} \to \mathbb{N}$, with $s(n) = n + 1$ (successor function).
Now we construct $\mathbb{N}$ as the unique set with structure $(\mathbb{N}, 0, s : \mathbb{N} \to \mathbb{N})$ that satisfies the following Peano axioms:

25.1 Peano axiom 1:

Different natural numbers have different successors, i.e.,

$$\forall m, n \in \mathbb{N}.\ \ m \neq n \Rightarrow s(m) \neq s(n)$$

Or alternatively

$$\forall m, n \in \mathbb{N}.\ \ s(m) \neq s(n) \Rightarrow m \neq n$$

Clearly, this shows that s is an injective function.

25.2 Peano axiom 2:

0 is not a successor, i.e.,

$$\forall n \in \mathbb{N}.\ \ \neg(s(n) = 0)$$

25.3 Peano axiom 3:

All natural numbers except 0 are successors, i.e.,

$$\forall n \in \mathbb{N}.\ \exists m \in \mathbb{N}.\ \ n = s(m)$$

25.4 Peano axiom 4:

For every (unary) predicate P on $\mathbb{N}$, the following formula is true:

$$P(0) \wedge \forall i \in \mathbb{N}.\ \ P(i) \Rightarrow P(i+1) \quad \Rightarrow \quad \forall n \in \mathbb{N}.\ \ P(n)$$

25.5 Peano axiom 4’:

Let $K \subseteq \mathbb{N}$ have the property that

1.) $0 \in K$

2.) $\forall n \in \mathbb{N}.\ n \in K \Rightarrow (n+1) \in K$

Then $K = \mathbb{N}$.

25.6 Lemma 1:

The axioms 4 and 4’ are equivalent.

Contents