Computer Science I: Set Theory & Logic

Overview

1. motivation: why logic and set theory?

2. mathematical formulae

   formulae as abbreviations:

   logical operators: $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$

   quantifiers: $\forall$, $\exists$

3. set theory: sets & relations

4. Setl2 (set language)

   set based programming

5. propositional logic: logical operators

   conjunctive normalform, *decidablity*

6. predicate logic: quantifiers

   logical calculus: formal proofs

7. Prolog (programming in logic)

8. limits: undecidability of the halting problem

9. Hoare calculus: program verification

Motivation: Why Logic and Set Theory?

Desastrous Software And Hardware Errors

1. Ariane 5: (crash on Juni 9th, 1996)
   (a) sensor measures horizontal inclination
   (b) inclination stored as 64 bit floating point number
   (c) later converted into 16 bit integer
   (d) overflow
   (e) navigations system produces error message (`core dump`)
   (f) control unit interprets core dump as flight data
   (g) control unit tried to correct flight path
   (h) rocket disintegrates because of high acceleration
   (a) expensive fireworks: 4 satellites lost
2. Therac 25: mediacal device for X-ray treatment

   1985: instead of 200 `rad`

   overdose of 25 000 `rad`

   3 people suffered lethal injuries

3. bug in floating point divison unit of Pentium chip

   financial loss for Intel: 400 000 000 Dollar

4. bug in software of *Patriot* anti-missile system

   (a) first golf war: Iraqi *Scud* could not be intercepted

   (b) 28 soldiers: *Game Over*

5. May 3rd, 2000:

   collapse of telephone network in Paris

   no emergency calls possible

6. November 4th, 1990:

   collapse of controlling software of the emergency center in London

   high delay times for patients, resulting in several preventable deaths

7. More errors:

`http://www.csl.sri.com/users/neumann/illustrative.html`

Motivation: Why Logic and Set Theory?

1. software and hardware controll big parts of our life

2. errors in software systems may be life threatening
   (a) collapse of phone system in urban center
   a few hours result in loss of life
   (b) collapse of IT of a major bank for two days
   bankruptcy

3. Development of hard- and software requires
   scientific foundation
   (a) logic
   (b) set theory
   (c) mathematics

Why Use Mathematical Formulae?

natural language description:

> *If wee add two numbers and then square this sum, we will get the same result that we get when we square the numbers separately, add these squares and finally add the product of both numbers twice.*

Question: Which law is described here?

Answer: First binomial theorem!

$$(x+y)^2 = x^2 + y^2 + 2 \cdot x \cdot y$$

Mathematical languages offers three advantages:

1. Easier to understand.
2. Formulae can be manipulated:
   (a) We can <u>compute</u> with formulae.
   (b) Formulae can be processed by software. Automatic theorem proving is possible!
3. Unambiguous meaning

   natural language is ambiguous, example

   "Do not waste any time to accept the application of Mr. X."

   formulae are defined to be unambiguous

Syntax von Formeln

1. *Variablen*: Namen für beliebige Objekte
   Beispiel: x und y in Formel $(x+y)^2 = x^2+y^2+2\cdot x\cdot y$

2. *Konstanten*: Namen für feste Objekte
   (a) π mit $\pi = 3.14159\cdots$
   (b) `Adam`, `Eva`

   Variablen + Konstanten: *atomare Terme*
   atomar: nicht zerlegbar

3. *Funktions-Zeichen*
   (a) $+$: 2-stelliges Funktions-Zeichen
   Infix-Schreibweise: $x+y$
   (b) $\sqrt{\ }$: 1-stelliges Funktions-Zeichen
   Präfix-Schreibweise: $\sqrt{2}$
   (c) Allgemein: sei
      - f n-stelliges Funktions-Zeichen
      - t_1, $\cdots$, t_n Terme

   Dann: $f(t_1,\cdots,t_n)$ neuer *Term*
   Beispiel:
      - `vater`, `mutter`: 1-stellige Funktions-Zeichen
      - `kain`, `abel`: Konstanten

   Dann: `vater(kain)`, `mutter(vater(kain))` Terme

Syntax von Formeln

4. *Prädikats-Zeichen*

   (a) $=$: 2-stelliges Prädikats-Zeichen
   Infix-Schreibweise: $x + y = y + x$

   (b) `teiler`: 2-stelliges Prädikats-Zeichen
   Präfix-Schreibweise: $\texttt{teiler}(x, x^2)$

   (c) Allgemein: sei

   - p n-stelliges Prädikats-Zeichen
   - t_1, $\cdots$, t_n Terme

   Dann $p(t_1, \cdots, t_n)$ *atomare Formel*
   Beispiel:

   `bruder`, **`schwester`**: 2-stellige Prädikats-Zeichen

   Formeln:

   i. $\texttt{bruder}(\texttt{kain}, \texttt{abel})$

   ii. $\texttt{schwester}(\texttt{kain}, \texttt{abel})$

   iii. $\texttt{schwester}(\texttt{mutter}(\texttt{kain}), \texttt{abel})$

Allgemein: aus Termen und Prädikatszeichen werden atomare Formeln gebildet.

Syntax von Formeln

5. *Junktoren* verknüpfen Formeln
   (a) Konjunktion: *und* “$\wedge$”

   $2 < 7$ und $7 < 10$

   $2 < 7 \wedge 7 < 10$

   (b) Disjunktion: *oder* “$\vee$”

   $x \leq y$ oder $y \leq x$.

   $x \leq y \vee y \leq x$.

   (c) Negation: *nicht* “$\neg$”

   x^2 ist nicht 2

   $\neg\, x^2 = 2$.

   (d) Implikation: *wenn, dann* “$\rightarrow$”

   wenn $x < y$, dann $x^2 < y^2$.

   $x < y \rightarrow x^2 < y^2$

6. *Quantoren* klären Verwendung von Variablen
   (a) All-Quantor: “$\forall$”

   Für alle ganzen Zahlen z gilt: $z^2 \geq 0$

   $\forall z \in \mathbb{Z} : z^2 \geq 0$

   (b) Existenz-Quantor: “$\exists$”

   Für alle $u, v \in \mathbb{R}$ gibt es w aus $\mathbb{R}$ mit $u+w = v$.

   $\forall u, v \in \mathbb{Z} : \exists w \in \mathbb{Z} : u + w = v$

Eindeutige Lesbarkeit

1. Ist folgende Formel richtig oder falsch?

   $$1 < 2 \lor 2 = 2 \land 0 = 1$$

   Problem: Wie soll Formel gelesen werden

   (a) $(1 < 2 \lor 2 = 2) \land 0 = 1$: falsch

   (b) $1 < 2 \lor (2 = 2 \land 0 = 1)$: richtig

2. Konsequenz: Formeln klammern!

3. Bindungsregeln zur Vereinfachung

   In **Arithmetik**: Punkt vor Strich

   $x + y \cdot z$ wird gelesen als $x + (y \cdot z)$

   In **Logik**: folgende Konvention

   (a) $\neg$ bindet am stärksten

   (b) $\land$ und $\lor$ binden gleichstark

   (c) $\rightarrow$ bindet schwächer als $\land$, $\lor$

   (d) $\leftrightarrow$ bindet am schwächsten

   Beispiel:

   $$P \land Q \rightarrow R \leftrightarrow \neg R \rightarrow \neg P \lor \neg Q$$

   wird gelesen als

   $$((P \land Q) \rightarrow R) \leftrightarrow ((\neg R) \rightarrow ((\neg P) \lor (\neg Q)))$$

Aufgaben

1. Formalisieren folgende Aussage:

Wenn x der Vater von y ist und y die Mutter von z ist, dann ist x ein Großvater von z.

Lösung:

$$x = \texttt{vater}(y) \wedge y = \texttt{mutter}(z) \rightarrow \texttt{grossvater}(x, z)$$

2. Geben Sie eine vollständige Charakterisierung des Prädikats Großvater.

Lösung:

$$\begin{aligned}
&\texttt{grossvater}(x, z) \quad \leftrightarrow \\
&\quad \Big(\exists y \in \texttt{Person} : x = \texttt{vater}(y) \wedge y = \texttt{mutter}(z)\Big) \quad \vee \\
&\quad \Big(\exists y \in \texttt{Person} : x = \texttt{vater}(y) \wedge y = \texttt{vater}(z)\Big)
\end{aligned}$$

3. Geben Sie eine vollständige Charakterisierung des Prädikats
x ist größter gemeinsamer Teiler von y und z.

Lösung:

1. $\texttt{teiler}(x, y) \leftrightarrow \exists z \in \mathbb{N} : x * z = y$

2. $\texttt{gt}(x, y, z) \leftrightarrow \Big(\texttt{teiler}(x, y) \wedge \texttt{teiler}(x, z)\Big)$

3. $\texttt{ggt}(x, y, z) \leftrightarrow$
$$\texttt{gt}(x, y, z) \quad \wedge \quad \Big(\forall u \in \mathbb{N} : \texttt{gt}(u, y, z) \rightarrow u \leq x\Big)$$

Aufgaben

Aufgabe 1: Definieren Sie das Prädikat

> x *ist das kleinste gemeinsame Vielfache*
> *der Zahlen* y *und* z.

Hinweis: Sie dürfen das Prädikat $\texttt{teiler}(x, y)$ als gegeben voraussetzen.

Lösung:

1. definiere gemeinsames Vielfaches:

   $\forall x, y, z \in \mathbb{N} : \texttt{gv}(x, y, z) \leftrightarrow (\texttt{teiler}(y, x) \wedge \texttt{teiler}(z, x))$

2. definiere kleinstes gemeinsames Vielfaches:

   $$\begin{aligned}&\forall x, y, z \in \mathbb{N} : \texttt{kgv}(x, y, z) \leftrightarrow \\ &\qquad \texttt{gv}(x, y, z) \wedge (\forall u \in \mathbb{N} : \texttt{gv}(u, y, z) \rightarrow x \leq u)\end{aligned}$$

Aufgabe 2: Sei $f : \mathbb{N} \rightarrow \mathbb{N}$. Formalisieren Sie:

1. f is *injektiv*, d.h. für jedes y gibt es höchstens ein x, so daß $f(x) = y$ ist.

2. f is *surjektiv*, d.h. für jedes y gibt es mindestens ein x, so daß $f(x) = y$ ist.

Lösung:

1. $\forall x_1, x_2 \in \mathbb{N} : f(x_1) = f(x_2) \rightarrow x_1 = x_2$.

2. $\forall y \in \mathbb{N} : \exists x \in \mathbb{N} : f(x) = y$.

Naive Mengenlehre

Frage: Was sind Mengen?
Antwort: Ansammlung verschiedener Objekte.

Beispiele:

1. Menge der Zahlen 1, 2 und 5: $\{1, 2, 5\}$.
2. Menge der Buchstaben: $\{a, b, c, \cdots, x, y, z\}$.
3. Menge der natürlichen Zahlen: $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$.

Notation: Statt

"Die Zahl 2 ist eine Element der Menge $\{1, 2, 3\}$"

schreiben wir: $2 \in \{1, 2, 3\}$.

1. Reihenfolge spielt keine Rolle.
   $\{1, 2, 3\} = \{3, 2, 1\}$
2. Eine Menge kann jedes Element höchstens einmal enthalten:
   $\{1, 2, 2, 3\} = \{1, 1, 2, 3, 3\}$.

Extensionalitäts-Prinzip:
Zwei Mengen sind gleich, wenn sie die selben Elemente enthalten:

Formalisiert:

$$M = N \leftrightarrow (\forall x : x \in M \leftrightarrow x \in N)$$

Komprehensions-Axiom

1. Frage: Wie definieren wir Mengen?

2. Erste Antwort (Cantor): Komprehensions-Axiom

   Sei $p(x)$ Formel, in der x auftritt

   $$M = \{x \mid p(x)\}$$

   bezeichnet Menge aller Objekte, für die p gilt.

   Lesart: M ist die Menge aller x, für die $p(x)$ gilt.

   Beispiel:

   (a) Sei $p(x) := (\exists y \in \mathbb{N} : x = y^2)$.

   (b) $Q = \{x \mid p(x)\} = \{x \mid \exists y \in \mathbb{N} : x = y^2\}$
   Menge der Quadrat-Zahlen

   (c) Russell-Menge

   $$R = \{x \mid \neg x \in x\}$$

   führt zu Parodoxie

   (d) Ausweg: R nicht wohldefiniert
   Komprehensions-Axiom nicht zuläßig

3. Heutige Antwort:

   Einschränkung des Komprehensions-Axioms

Teilmenge

Gegeben: Mengen M_1 und M_2

Definition: M_1 *Teilmenge* von M_2 g.d.w.

$$\forall x \in M_1 : x \in M_2$$

Schreibweise: $M_1 \subseteq M_2$

Definition von Mengen

Problem: nicht alle Mengen sind explizit angebbar.
Beispiel: Menge der geraden Zahlen.

$$\{0, 2, 4, 6, \cdots\}$$

"Pünktchen-Schreibweise" nicht eindeutig.

Lösung: Operationen zur Bildung von Mengen

1. Selektion

   Auswahl einer Menge von Elementen aus einer gegebenen Menge

2. Vereinigung von Mengen $\cup$

3. Schnitt von Mengen $\cap$

4. Kartesische Produkte $\times$

5. Potenz-Menge 2^M

6. Abbildungen von Mengen $f(M)$

Selektion

Selektion: Beispiel

$$\{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : x = 2 * y\}$$

beschreibt die Menge der geraden Zahlen.

Allgemein: Sei

1. M gegebene Menge
2. $p(x)$ eine Formel, in der Variable x auftritt.

Dann bezeichnet

$$\{x \in M \mid p(x)\} = \{x \mid x \in M \wedge p(x)\}$$

Menge aller x aus M, für die Eigenschaft p zutrifft.

Schnitt-Menge

Gegeben: Zwei Mengen M_1 und M_2.
Definition:

$$M_1 \cap M_2 = \{x \mid x \in M_1 \wedge x \in M_2\}$$

heißt Schnitt-Menge.

Beispiel: $\{1, 3, 5, 6, 7\} \cap \{4, 5, 6\} = \{5, 6\}$

Vereinigungs-Menge

Gegeben: Zwei Mengen M_1, M_2

Definition:

$$M_1 \cup M_2 = \{x \mid x \in M_1 \vee x \in M_2\}$$

heißt Vereinigungs-Menge.

Beispiel: $\{1, 3, 5, 6, 7\} \cup \{4, 5, 6\} = \{1, 3, 4, 5, 6, 7\}$

Mengen-Komplement

Gegeben: Mengen M_1 und M_2.

Definition: $M_1 \backslash M_2 = \{x \mid x \in M_1 \wedge x \notin M_2\}$

Beispiel: $\{1, 3, 5, 6, 7\} \backslash \{4, 5, 6\} = \{1, 3, 7\}$

Satz: Für beliebige Mengen M und N gilt:

1. $M \cap N \subseteq M$
2. $M \subseteq M \cup N$
3. $M \backslash N \subseteq M$
4. $M \backslash (M \backslash N) = M \cap N$
5. $N \backslash (M \backslash N) = N$

Mengen-Algebra

1. Idempotenz: $M \cup M = M$, $M \cap M = M$

2. Neutrales Element: $M \cup \emptyset = M$, $M \cap \emptyset = \emptyset$

3. Kommutativ-Gesetze

   $M_1 \cup M_2 = M_2 \cup M_1$

   $M_1 \cap M_2 = M_2 \cap M_1$

4. Assoziativ-Gesetze

   $(M_1 \cup M_2) \cup M_3 = M_1 \cup (M_2 \cup M_3)$

   $(M_1 \cap M_2) \cap M_3 = M_1 \cap (M_2 \cap M_3)$

5. Distributiv-Gesetze

   $(M_1 \cup M_2) \cap N = (M_1 \cap N) \cup (M_2 \cap N)$

   $(M_1 \cap M_2) \cup N = (M_1 \cup N) \cap (M_2 \cup N)$

6. DeMorgan-Gesetze

   $N \backslash (M_1 \cup M_2) = (N \backslash M_1) \cap (N \backslash M_2)$

   $N \backslash (M_1 \cap M_2) = (N \backslash M_1) \cup (N \backslash M_2)$

Aufgaben zur Mengen-Bildung

Aufgabe 1: Berechnen Sie

$$M = \{x \in \mathbb{N} \mid (\exists y \in \mathbb{N} : y^2 = x) \wedge x < 10\}.$$

Lösung:

$$M = \{0, 1, 4, 9\}$$

Aufgabe 2: Gegeben seien die folgenden Mengen:

$$M_1 = \{x \in \mathbb{N} \mid x^2 - 5 * x + 6 = 0\}$$

$$M_2 = \{x \in \mathbb{N} \mid x^3 > 8\}$$

Berechnen Sie $M_1 \cap M_2$.

Lösung:

$$M_1 \cap M_2 = \{3\}$$

Aufgabe 3: Geben Sie einen Ausdruck für die Menge P aller Primzahlen an.

Lösung:

$$P = \{x \in \mathbb{N} \mid x \geq 2 \wedge \\ (\forall u, v \in \mathbb{N} : u > 1 \wedge v > 1 \rightarrow u * v \neq x)\}$$

Aufgabe 4: Geben Sie einen Ausdruck für die folgende Menge an:

$$M = \{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20, 22, \cdots\}$$

Lösung:

$$M = \{2, 4, 6, \cdots\} \cup \{5, 15, 20, \cdots\} = \\ \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : x = 2 * y\} \cup \\ \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : x = 5 * y\}$$

Tupel (Endliche Folgen)

Notation: $\langle x_1, x_2, \cdots, x_n \rangle$ heißt n-Tupel.

Sprechweise:

1. n ist die Länge des Tupels.
2. x_i ist die i-te Komponente.

Gleichheit: Es gilt

$$\langle x_1, x_2, \cdots, x_n \rangle = \langle y_1, y_2, \cdots, y_m \rangle$$

g.d.w. folgendes gilt:

1. $n = m$

   Die Länge der Tupel ist gleich.

2. $\forall i \in \mathbb{N} : i \leq n \rightarrow x_i = y_i$

   Die Komponenten stimmen paarweise überein.

Kartesisches Produkt

Gegeben: Mengen M_1 und M_2

Definition: $M_1 \times M_2 = \{\langle x, y \rangle \mid x \in M_1 \wedge y \in M_2\}$

Sprechweise: $M_1 \times M_2$ heißt *kartesisches Produkt* der Mengen M_1 und M_2.

Verallgemeinertes kartesisches Produkt

Wir identifizieren

$$\langle\langle x, y\rangle, z\rangle = \langle x, \langle y, z\rangle\rangle = \langle x, y, z\rangle$$

Daher gilt:

$$\begin{aligned}(M_1 \times M_2) \times M_3 &= M_1 \times (M_2 \times M_3) \\ &= M_1 \times M_2 \times M_3.\end{aligned}$$

Bezeichnung: $M_1 \times M_2 \times \cdots \times M_n$ heißt

$$\boxed{\boxed{\text{verallgemeinertes kartesisches Produkt}}}$$

Binäre Relation

Gilt $R \subseteq M \times M$, so heißt R eine *binäre Relation* auf M.

Beispiele:

1. $\{\langle x, x\rangle \in \mathbb{N} \times \mathbb{N} \mid x \in \mathbb{N}\}$.
2. $\{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid x < y\}$.
3. $\{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid y = x * x\}$.

Schreibweise: $M^2 := M \times M$
Allgemein wird M^n per Induktion nach n definiert:

1. $M^1 := M$
2. $M^{n+1} := M^n \times M$

Ordnungs-Relationen

Infix-Schreibweise: Schreibe xRy statt $\langle x, y\rangle \in R$.

Definition: $R \subseteq M^2$ ist *reflexiv* g.d.w.

$$\forall x \in M : xRx.$$

Definition: $R \subseteq M^2$ ist *symmetrisch* g.d.w.

$$\forall x, y \in M : xRy \to yRx.$$

Definition: $R \subseteq M^2$ ist *anti-symmetrisch* g.d.w.

$$\forall x, y \in M : xRy \wedge yRx \to x = y.$$

Definition: $R \subseteq M^2$ ist *transitiv* g.d.w.

$$\forall x, y, z \in M : xRy \wedge yRz \to xRz.$$

Definition: $R \subseteq M^2$ ist *total* g.d.w.

$$\forall x, y \in M : xRy \vee yRx.$$

Definition:
$R \subseteq M^2$ *partielle Ordnung* im Sinne von $\leq$ g.d.w.

1. R ist reflexiv.
2. R ist anti-symmetrisch.
3. R ist transitiv.

Definition: $R \subseteq M^2$ ist eine *totale Ordnung*
(auch: *lineare Ordnung*) im Sinne von $\leq$ g.d.w.

1. R ist partielle Ordnung.
2. R ist total.

Äquivalenz-Relationen

Definition: $R \subseteq M^2$ ist *Äquivalenz-Relation* g.d.w.

1. R ist reflexiv,
2. R ist symmetrisch und
3. R ist transitiv.

Beispiele

1. $R_1 = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x \leq y\}$
   ist Ordnungs-Relation im Sinne von $\leq$.

2. $R_2 = \{\langle x, y\rangle \in \mathbb{N}^2 \mid \exists z \in \mathbb{N} : x * z = y\}$
   ist Ordnungs-Relation im Sinne von $\leq$.

3. Sei $f : \mathbb{N} \rightarrow \mathbb{N}$ bel. Funktion. Dann gilt:
   $$R_3 = \{\langle x, y\rangle \in \mathbb{N}^2 \mid f(x) = f(y)\}$$
   ist Äquivalenz-Relation.

Definition: Äquivalenz-Klasse

Sei $\sim\, \subseteq M^2$ Äquivalenz-Relation. Für alle $x \in M$ bezeichnet

$$[x]_\sim = \{y \in M \mid x \sim y\}$$

die von x generierte *Äquivalenz-Klasse*.

Satz: Es gilt

1. $\forall x, y \in M : x \sim y \rightarrow [x]_\sim = [y]_\sim$

2. $\forall x, y \in M : \neg x \sim y \rightarrow [x]_\sim \cap [y]_\sim = \emptyset$

Aufgaben

Aufgabe 1: Welche der folgenden Relationen auf $S = \{1, 2, 3\}$ sind Äquivalenz-Relationen?

(a) $R_1 = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 2,3\rangle, \langle 3,2\rangle\}$

(b) $R_1 = \{\langle 2,2\rangle, \langle 3,3\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 2,3\rangle, \langle 1,1\rangle, \langle 1,3\rangle, \langle 3,1\rangle\}$

Aufgabe 2: Wie sieht die kleinste Äquivalenz-Relation auf $S = \{1, 2, 3\}$ aus?

Aufgabe 3: Sei M die Menge aller Menschen.

(a) Ist $R_1 = \{\langle x, y\rangle \in M^2 \mid \texttt{vater}(x) = \texttt{vater}(y)\}$
Äquivalenz-Relation?

(b) Gegeben $x \in M$. Dann bezeichne

$$\texttt{vorfahre}(x) = \{y \in M \mid y \text{ ist vorfahre von } x\}$$

die Menge aller Vorfahren von x. Ist

$$R_2 = \{\langle x, y\rangle \in M^2 \mid y = x \ \lor\ y \in \texttt{vorfahre}(x)\}$$

eine Ordnungs-Relation im Sinne von $\leq$?

Aufgabe 4: Ist

$$R = \{\langle x, y\rangle \in \mathbb{N} \mid x \geq y\}$$

eine Ordnungs-Relation im Sinne von $\leq$?

Aufgaben

Aufgabe 1: Wie sieht die kleinste Ordnungs-Relation im Sinne von $\leq$ auf $S = \{1, 2, 3\}$ aus?

Definition: Sei $R \subseteq M \times M$ eine Ordnungs-Relation im Sinne von $\leq$. Die Ordnung R heißt *total* g.d.w.

$$\forall x, y \in M : xRy \vee yRx.$$

Beispiel: Die Relation $\{\langle x, y\rangle \in \mathbb{N}^2 \mid x \leq y\}$ ist total.

Gegenbeispiel: Die Relation

$$\texttt{Teiler} = \{\langle x, y\rangle \in \mathbb{N}^2 \mid \exists z \in \mathbb{N} : x * z = y\}$$

ist nicht total.

Aufgabe 2: Geben Sie eine totale Ordnungs-Relation im Sinne von $\leq$ auf $S = \{1, 2, 3\}$ an.

Definition: Sei $R_1 \subseteq K \times M$ und $R_2 \subseteq M \times N$

$$R_2 \circ R_1 = \{\langle x, z\rangle \in K \times N \mid \exists y \in M : \langle x, y\rangle \in R_1 \wedge \langle y, z\rangle \in R_2\}$$

Aufgabe 3: Seien $R_1, R_2 \subseteq M \times M$.

Beweisen oder widerlegen Sie:

1. Falls R_1 und R_2 reflexiv sind,
   dann ist auch $R_1 \circ R_2$ reflexiv.
2. Falls R_1 und R_2 symmetrisch sind,
   dann ist auch $R_1 \circ R_2$ symmetrisch.
3. Falls R_1 und R_2 transitiv sind,
   dann ist auch $R_1 \circ R_2$ transitiv.

Schreibweise: Sei $f : M \to N$ Funktion.

$$\{f(x) \mid x \in M\} := \{y \in N \mid \exists x \in M : y = f(x)\}$$
$$f(M) := \{y \in N \mid \exists x \in M : y = f(x)\}$$

Definition: Ist M eine Menge, so bezeichnet

$$2^M = \{N \mid N \subseteq M\}$$

die *Potenz-Menge* von M.

Definition: Ist M endliche Menge, so bezeichnet

$$\mathtt{card}(M)$$

die Anzahl der Elemente von M.

Beispiele:

1. $M = \emptyset$.
$$2^M = \{\emptyset\}, \quad \mathtt{card}(2^M) = 1.$$
2. $M = \{1\}$.
$$2^M = \Big\{\emptyset, \{1\}\Big\}, \quad \mathtt{card}(2^M) = 2.$$
3. $M = \{1, 2\}$
$$2^M = \Big\{\emptyset, \{1\}, \{2\}, \{1, 2\}\Big\},$$
$$\mathtt{card}(2^M) = 4.$$

Satz: Ist M endlich, so gilt

$$\mathtt{card}(2^M) = 2^{\mathtt{card}(M)}$$

Funktionen als Mengen

Definition: Sei $f : M \to N$.

$$\texttt{graph}(f) := \Big\{ \langle x, y \rangle \mid y = f(x) \Big\}$$

Definition: M und N seien Mengen

$$N^M := \Big\{ \texttt{graph}(f) \mid f : M \to N \Big\}$$

Satz: M und N endlich. Dann gilt

$$\texttt{card}(N^M) = \texttt{card}(N)^{\texttt{card}(M)}$$

Satz: M und N endlich. Dann gilt

$$\texttt{card}(M \times N) = \texttt{card}(M) * \texttt{card}(N)$$

Mächtigkeit von Mengen

Definition: M und N *gleichmächtig* g.d.w.

1. es existiert eine <u>injektive</u> Funktion

   $f : M \to N$ und

2. es existiert eine <u>injektive</u> Funktion

   $g : N \to M$

Schreibweise:

$M \approx_{card} N$.

Satz:

1. $M \approx_{card} M$
2. $K \approx_{card} M \wedge M \approx_{card} N \to K \approx_{card} N$

Beispiele:

1. $\{1, 2, 3\} \approx_{card} \{a, b, c\}$
2. $\mathbb{N} \approx_{card} \mathbb{Z}$
3. $\mathbb{N} \approx_{card} \mathbb{N} \times \mathbb{N}$

Mächtigkeit von Mengen

Satz (*Schröder-Bernstein*) Falls $M \approx_{card} N$, dann gibt es eine <u>bijektive</u> Funktion

$$h : M \to N.$$

Definition: N *mächtiger* als M g.d.w.

1. es existiert eine injektive Funktion

   $f : M \to N$ und

2. es existiert <u>keine</u> injektive Funktion

   $g : N \to M$.

Schreibweise: $M \prec_{card} N$

Beispiel: $\{1, 2, 3\} \prec_{card} \{a, b, c, d\}$

Satz: $K \prec_{card} M \land M \prec_{card} N \to K \prec_{card} N$

Definition: Falls $M \approx_{card} \mathbb{N}$, so heißt M *abzählbar unendlich*.

Definition: Falls $\mathbb{N} \prec_{card} M$, so heißt M *überabzählbar*.

Satz: (Cantor)

$$\mathbb{N} \prec_{card} \mathbb{N}^{\mathbb{N}}$$

Beweis: Annahme: $\mathbb{N} \approx_{card} \mathbb{N}^{\mathbb{N}}$

Schröder-Bernstein: existiert $f : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ bijektiv.

Definiere

$$\texttt{diag} : \mathbb{N} \to \mathbb{N}$$

$$\texttt{diag}(n) := \Big(f(n)\Big)(n) + 1.$$

$\texttt{diag} \in \mathbb{N}^{\mathbb{N}}$ also existiert $d \in \mathbb{N}$ mit $f(d) = \texttt{diag}$

Konsequenz:

$$\begin{aligned} \texttt{diag}(d) &= \Big(f(d)\Big)(d) + 1 \\ &= \texttt{diag}(d) + 1 \end{aligned}$$

Widerspruch!

$$\boxed{\boxed{\mathbb{N}^{\mathbb{N}} \text{ ist überabzählbar.}}}$$

Definition:

$$\mathbb{P} \quad := \quad \text{“Menge aller C-Programme”}$$

Satz: $\mathbb{P} \approx_{card} \mathbb{N}$

Beweis: Jedes C-Programme P ist endliche Folge von Bytes B_i:

$$P = B_0 B_1 B_2 \cdots B_n$$

Interpretiere P als Zahl:

$$\sum_{i=0}^{n} B_i * 256^i.$$

Dann gilt $\mathbb{P} \subseteq \mathbb{N}$.

Korollar: Es gibt Funktionen in $\mathbb{N}^{\mathbb{N}}$, die nicht durch ein C-Programm berechenbar sind!

Aufgabe: Zeigen Sie

$$\mathbb{N} \prec_{card} 2^{\mathbb{N}}$$