Merkblatt zu Mathematischen Formeln

Informatik 1 WiSe 2020/2021
Henning Cui, Julian Linne

11. Februar 2021

Disclaimer

Dieses Dokument soll als eine Übersicht der mathematischen Begriffe und Formeln fungieren, **die in der Informatik 1 verwendet werden**. Es ist möglich, dass einige Angaben vergessen wurden. Für eine genauere Angabe wird auf dem Foliensatz beziehungsweise das Skript verwiesen.

Zahlenräume

In der Informatik 1 verwenden wir folgende Zahlenräume:

- $\mathbb{Z}$: Menge der ganzen Zahlen
- $\mathbb{N} := \{n | n \in \mathbb{Z}, n > 0\}$
- $\mathbb{N}_0 := \{n | n \in \mathbb{Z}, n \geq 0\}$
- $\mathbb{Q} := \left\{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{N}\right\}$
- $\mathbb{R}$: Menge der reellen zahlen

Arithmetische Operationen Wir haben für diese Vorlesung folgende arithmetische Operationen definiert:

Bedeutung	**Operationszeichen**	**Beispiele**
Kleiner	$<$	$1 < 2$
Kleiner gleich	$\leq$	$1 \leq 1, 1 \leq 2$
Größer	$>$	$0 > -1$
Größer gleich	$\geq$	$0 \geq 0, 0 \geq -1$
Gleich	$=$	$0 = 0$
Ungleich	$\neq$	$0 \neq 1$
Addition	$+$	$1 + 2 = 3$
Subtraktion	$-$	$1 - 2 = -1$
Multiplikation	$\cdot$	$1 \cdot 2 = 2$
Reelle Division	$/$	$5/2 = 2.5$
Ganzzahlige Division	$\div$	$5 \div 2 = 2$
Modulo	mod	$5 \bmod 2 = 1$
Abrundung	$\lfloor \cdot \rfloor$	$\lfloor 5.2 \rfloor = 5$
Aufrundung	$\lceil \cdot \rceil$	$\lceil 5.2 \rceil = 6$
Absolutbetrag	$\lvert \cdot \rvert$	$\lvert -6 \rvert = 6$
Positives Vorzeichen	$+$	$+1$
Negatives Vorzeichen	$-$	-1

Mengen und Intervalle

Wir unterscheiden zwischen Mengen und Intervallen.

Intervalle

Ein **Intervall** ist für ein $n, m \in \mathbb{R}$ und $n \leq m$ folgendermaßen definiert:

- $[n, m] := \{x \mid x \in \mathbb{R},\, x \geq n,\, x \leq m\}$
- $[n, m[:= \{x \mid x \in \mathbb{R},\, x \geq n,\, x < m\}$
- $]n, m] := \{x \mid x \in \mathbb{R},\, x > n,\, x \leq m\}$
- $]n, m[:= \{x \mid x \in \mathbb{R},\, x > n,\, x < m\}$
- $[n, \infty[:= \{x \mid x \in \mathbb{R},\, x \geq n\}$
- $]n, \infty[:= \{x \mid x \in \mathbb{R},\, x > n\}$
- $]-\infty, m] := \{x \mid x \in \mathbb{R},\, x \leq m\}$
- $]-\infty, m[:= \{x \mid x \in \mathbb{R},\, x < m\}$

Beachte: Ein Intervall enthält immer alle reellen Zahlen zwischen den angegebenen Intervallgrenzen und lässt sich nicht z.B. auf die ganzen Zahlen im Intervall oder sonstige Teilmengen davon beschränken. Das bedeutet, die Werte innerhalb der Grenzen sind alle reelle Zahlen zwischen n und m. Somit gilt beispielsweise: $[1, 3] = \{1.0, \ldots, 1.1, \ldots, 1.15, \ldots, 2.43, \ldots, 3.0\}$.

Mengen

Eine **Menge** kann Elemente aus einem beliebigen Zahlenraum besitzen. Die Menge A , dessen Elemente durch Eigenschaften $E_1, ..., E_n$ charakterisiert wird, wird folgendermaßen angegeben:

$$A := \{a | E_1, ..., E_n\}$$

Besitzt die Menge A eine Zahlenfolge, kann sie auch folgendermaßen angegeben werden:

$$A := \{x_1, ..., x_n\}$$

wobei $x_1, ..., x_n$ Elemente aus einem beliebigen, oben definierten Zahlenraum sind.

Mengenoperationen Wir besitzen drei Mengenoperationen, die auf beliebige Mengen A, B angewendet werden können:

- Der **Durchschnitt** (die **Schnittmenge**) $A \cap B := \{x \mid x \in A,\, x \in B\}$ von A und B ist eine Zusammenfassung aller Objekte, die Elemente in A und in B sind.
- Die **Vereinigung(smenge)** $A \cup B := \{x \mid x \in A \text{ oder } x \in B \text{ oder } x \in A \cap B\}$ von A und B ist eine Zusammenfassung aller Objekte, die Elemente in A, in B oder in A und in B sind.
- Die **Differenz** $A \setminus B := \{x \mid x \in A,\, x \notin B\}$ von A und B ist eine Zusammenfassung aller Objekte, die Elemente in A, aber nicht in B sind.

Zusätzlich gilt für alle Mengen M (für die Beispiele gilt $M = \{a, b, c\}$)

Teilmenge: $M' = \{a, b\}$ ist eine (echte) Teilmenge von M, formal geschrieben $M' \subseteq M$.

Potenzmenge: Alle Kombinationsmöglichkeiten der Elemente der Menge, inkl. leerer Menge und Menge selbst (da die Potenzmenge *alle* Teilmengen fordert und **keine** *echten* Teilmengen voraussetzt). Somit ist auch stets die ursprüngliche Menge A enthalten. Die Elemente aus M lassen sich wie folgt kombinieren:
$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$

Kartesische Produkt: Sei A eine Menge, so bezeichnet die Menge

$$A^2 := A \times A := \{(a_1, a_2) \mid a_1, a_2 \in A\}$$

das **kartesische Produkt von A mit sich selbst**.

- Ein Element $(a_1, a_2) \in A \times A$ heißt **2-Tupel** oder **geordnetes Paar**
- Es besteht aus den **Komponenten** a_1 und a_2 (a_i ist die **i-te Komponente**)
- Für A endlich gilt: $|A \times A| = |A|^2$

Relationen auf Mengen

Wir besitzen folgende Relationen:

Binäre Relation: Sei A eine Menge. Eine **binäre Relation auf A** ist eine Teilmenge $R \subseteq A^2$. R heißt

- **irreflexiv** $:\Leftrightarrow (a, a) \notin R$ für alle $a \in A$
- **transitiv** $:\Leftrightarrow (a, b), (b, c) \in R \implies (a, c) \in R$ für alle $a, b, c \in A$

Statt $(a, b) \in R$ schreibt man auch aRb (**Infixnotation**).

Logisches Folgern: Sind α, β mathematische Aussagen (die wahr oder falsch sein können), so ist

- $\alpha \Rightarrow \beta$ die mathematische Aussage **Aus α folgt β** (α impliziert β, Wenn α dann β).
  $\Rightarrow$ heißt Implikationspfeil
- $\alpha \Leftrightarrow \beta$ die mathematische Aussage α **genau dann wenn** β (α äquivalent zu β).
  $\Leftrightarrow$ heißt Äquivalenzpfeil

Enthält α einen neuen Begriff, so wird dieser Begriff mit $\alpha :\Leftrightarrow \beta$ durch β definiert.

Ordnungsrelation: Sei A eine Menge. Eine irreflexive, transitive Relation R auf A heißt **(irreflexive) Ordnungsrelation**.

- Ordnungsrelationen haben keine Zyklen, d.h. es gibt kein $n \in \mathbb{N}$ und Elemente $a_1, \dots, a_n \in A$ mit $(a_1, a_2), \dots, (a_{n-1}, a_n), (a_n, a_1) \in R$ (ohne Beweis).
- Für Ordnungsrelationen benutzt man in der Regel nicht das Symbol R, sondern eines der Symbole $<$, $\prec$ oder $\ll$.
- Eine Ordnungsrelation legt eine Reihenfolge zwischen *kleineren* und *größeren* Elementen in A fest.

Geordnete Mengen: Eine **geordnete Menge** besteht aus einer Menge A und einer Ordnungsrelation $<$ auf A. Ist $<$ **total**, d.h. gilt $a < b$ oder $b < a$ für alle Elemente $a, b \in A$, so ist die Menge **total geordnet**.

Abbildungen: Seien A, B Mengen. Eine **Abbildung** oder **Funktion**

$$f : A \to B$$

ordnet jedem Element $a \in A$ ein eindeutiges Element $f(a) \in B$ zu.

- A ist der **Definitionsbereich** von f.
- B ist der **Wertebereich** von f.
- a nennt man **Operand** oder **Argument**.

Alphabete, Wörter und Buchstaben

Grundlagen

Alphabete: Ein **Alphabet** ist eine endliche, total geordnete Menge A.
Deren Elemente nennen wir **Buchstaben**. Die Ordnung bezeichnen wir mit $<$.

Wörter (über einem Alphabet):

- Ein **Wort** (über einem Alphabet A) ist eine endliche Folge $w = a_1a_2 \dots a_k$ von Buchstaben aus A
- Die **Länge** $|w|$ eines Wortes w ist die Anzahl der Buchstaben von w (gleiche Buchstaben werden mehrfach gezählt)
- Das **leere Wort** ε hat die Länge $|\varepsilon| = 0$
  Achtung: ε ist kein Buchstabe!
  Anmerkung: In der Literatur wird auch das Symbol λ verwendet
- Wir bezeichnen mit A^* die **Menge aller Wörter (über** A**)**.
- Wir bezeichnen mit $A^+ := A^* \setminus \{\varepsilon\}$ die Menge aller **nichtleeren** Wörter über A.
- Wir bezeichnen mit $A^k := \{w \mid w \in A^*, |w| = k\}$ die Menge aller Wörter **der Länge** k.
- Eine **formale Sprache (über** A**)** ist eine Teilmenge $L \subseteq A^*$.

Teilwörter:

- Zwei Wörter u und v kann man **hintereinanderschreiben** (**konkatenieren**). Man erhält so das Wort uv.
- Gibt es zu einem Wort x Wörter u, v mit $x = uv$, so heißt u **Anfangsstück** (**Präfix**) von x.
- Gibt es zu einem Wort x Wörter u, v mit $x = uv$, so heißt v **Endstück** (**Suffix**) von x.
- Gibt es zu einem Wort x Wörter u, v, w mit $x = uvw$, so heißt v **Teilwort** von x.

Lexikographische Ordnung: Die **lexikografische Ordnung** $u < v$ **zwischen Wörtern** $u, v \in A^*$(**gebildet aus einem Alphabet A**) ist wie folgt definiert mit vollständiger Induktion nach **der Länge** $n := |u|$:

1. Induktionsanfang $n = |u| = 0$ (also $u = \epsilon$):
   Es gilt $\epsilon < v$ für alle Wörter $v \neq \epsilon$
2. Induktionsschritt $n \to n + 1$:
   Sei $|u| = n + 1$, $u = ax$ und $v = by$ für $a, b \in A$ und $x, y \in A^*$:
   (a) Ist $a < b$, so gilt $u < v$
   (b) Ist $a = b$, so gilt $u < v :\Leftrightarrow x < y$ (Rückführung auf kürzeres Wort x mit Länge n)
   (c) Ist $b < a$, so gilt $v < u$

Codierung

Codierung: Die Codierung ist ein Prinzip, welches jedem Zeichen eines Alphabets ein Wort eines zweiten Alphabets zuordnet.

Seien A, B Alphabete. Eine **Codierung** ist eine Abbildung $c : A \to B^*$ mit $c(a_1) \neq c(a_2)$ für $a_1 \neq a_2$. Der Bildbereich $c(A) := \{c(a) \mid a \in A\}$ heißt **Code**. Jedes Element $b \in c(A)$ heißt **Codewort**.

Decodierung: Die Decodierung kehrt die Codierung wieder um, so dass man wieder die ursprüngliche Eingabe erhält.

Für ein Codewort $b \in B^*$ heißt $a \in A$ **Decodierung von** b, falls $c(a) = b$. Wir schreiben in diesem Fall $c^{-1}(b) := a$.

Wichtige Codierungsklassen

- Allgemeine Codierungsklassen: Seien A, B Alphabete. Eine Codierung
  - $c : A \to B$ heißt **Chiffrierung**
  - $c : A \to B^n$ (mit genau n Zeichen) heißt **Blockcodierung**
- Binär-Codierung: Sei A ein Alphabet. Eine Codierung
  - $c : A \to \mathbb{B}$ heißt **Binärcodierung (von** A**)** (hier wird nur ein Bit verwendet)
  - $c : A \to \mathbb{B}^n$ (n fest) heißt n**-Bit-Codierung (von** A**)** (hier werden n Bits verwendet)

Jedes Wort in $\mathbb{B}^n$ bezeichnen wir als **Bitmuster (der Länge** n**)**. Als solche Bitmuster sind Zahlen und Zeichen im Rechner abgespeichert. Um diese klar unterscheiden zu können, notieren wir diese als $c_{N,n}$: N gibt dabei an, auf welche Codierung wir uns beziehen. n ist die Länge des Bitmusters, es handelt sich also um eine n-Bit-Codierung.