Einführung in die Computerorientierte Mathematik

Wintersemester 2017/18

Thomas Gerstner

Institut für Mathematik
Goethe-Universität Frankfurt

Inhaltsverzeichnis

Kapitel 1

Zahlen

1.1 Zahlenmengen

Zahlen sind die Grundbausteine der Arithmetik. Die wichtigsten *Zahlenmengen* sind:

- *Natürliche Zahlen*: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ $(= \mathbb{N}^+)$
  $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$
- *Ganze Zahlen*: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
  $= \{0, +1, -1, +2, -2, +3, -3, \ldots\}$
- *Rationale Zahlen*: $\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}\}$
  $= \{0, \pm\frac{1}{1}, \pm\frac{2}{1}, \pm\frac{1}{2}, \pm\frac{3}{1}, \pm\frac{2}{2}, \pm\frac{1}{3}, \ldots\}$ (1. Cantorsches Diagonalverfahren)
- *Reelle Zahlen*: $\mathbb{R} =$ die gesamte Zahlengerade (wird später genauer definiert)
- *Komplexe Zahlen*: $\mathbb{C} = \{z + iw \mid z, w \in \mathbb{R}\}$ (i ist die imaginäre Einheit: $i^2 = -1$)

Jede dieser Zahlenmengen entsteht aus einer Erweiterung des vorangegangenen Zahlenbereichs, um bestimmte mathematische Probleme lösen zu können:

- Ganze Zahlen: löse (beispielsweise) $2 + x = 1$
- Rationale Zahlen: löse (beispielsweise) $2 \cdot x = 1$
- Reelle Zahlen: löse (beispielsweise) $x^2 = 2$
- Komplexe Zahlen: löse (beispielsweise) $x^2 = -1$

1.2 Stellenwertsystem

Zahlen können auf verschiedene Weisen angegeben werden. Das *Stellenwertsystem* (b-adische Darstellung) ist eine häufig verwendete Möglichkeit. Hierzu wird eine *Basis* $b \in \mathbb{N}$ mit $b > 1$ gewählt und als *Ziffernmenge* $Z = \{0, 1, \ldots, b - 1\}$ verwendet. Ein bekanntes Beispiel ist das Dezimalsystem, das der Wahl von $b = 10$ und $Z = \{0, 1, \ldots, 9\}$ entspricht.

Die Zahlen der verschiedenen Zahlenmengen haben dann folgende Darstellungen:

- $z \in \mathbb{N}_0 : z_n z_{n-1} \ldots z_0 = z_n \cdot b^n + z_{n-1} \cdot b^{n-1} + \ldots + z_1 \cdot b^1 + z_0 \cdot b^0 = \sum_{i=0}^{n} z_i \cdot b^i$

  mit $n \in \mathbb{N}_0$ und $z_i \in Z$ für $i = 0, \ldots, n$
  Beispiel: $b = 10, z = 235 = 2 \cdot 10^2 + 3 \cdot 10^1 + 5 \cdot 10^0 = 200 + 30 + 5$

- $z \in \mathbb{Z} : \pm z_n z_{n-1} \ldots z_0$

- $z \in \mathbb{Q} : (\pm p_n p_{n-1} \ldots p_0, q_m q_{m-1} \ldots q_0)$ als Zahlenpaar aus Zähler und Nenner

- $z \in \mathbb{R} : \pm z_n z_{n-1} \ldots z_0, z_{-1} z_{-2} z_{-3} \ldots =$

  $\pm z_n \cdot b^n + \ldots + z_1 \cdot b^1 + z_0 \cdot b^0 + z_{-1} \cdot b^{-1} + z_{-2} \cdot b^{-2} + \ldots = \pm \sum_{i=-\infty}^{n} z_i \cdot b^i$
  Beispiel: $\sqrt{2} = 1,41421\ldots = 1 \cdot 10^0 + 4 \cdot 10^{-1} + 1 \cdot 10^{-2} + 4 \cdot 10^{-3} + \ldots$

- $z \in \mathbb{C} : (\pm z_n \ldots z_0, z_{-1} \ldots, \pm w_n \ldots w_0, w_{-1} \ldots)$ als Paar reller Zahlen

Eine Zahl hat bezüglich verschiedener Basen b_1, b_2 unterschiedliche Darstellungen, zum Beispiel bei einer natürlichen Zahl: $(z_n \ldots z_0)_{b_1} = (w_n \ldots w_0)_{b_2}$. Beispielsweise ist $21_{10} = 2 \cdot 10 + 1 \cdot 1 = 30_7 = 3 \cdot 7 + 0 \cdot 1$.

Die Ziffernfolge einer Zahl kann mittels *Division mit Rest* wie folgt berechnet werden.

$$\begin{aligned}
\text{Zahl der Ziffern: } n &= \lfloor \log_b z \rfloor \\
\text{Einzelne Ziffern: } z_i &= \left\lfloor \frac{z}{b^i} \right\rfloor - b \left\lfloor \frac{z}{b^{i+1}} \right\rfloor
\end{aligned}$$

Hierbei ist $\log_b$ der *Logarithmus zur Basis* b, das heißt $\log_b z$ ist die Lösung der Gleichung $b^x = z$. Zum Beispiel ist $\log_{10} 10 = 1, \log_{10} 100 = 2, \log_{10} 1000 = 3, \ldots$.

Die *Gauß-Klammer* $\lfloor z \rfloor$ entspricht der größten ganze Zahl kleiner gleich z. Umgekehrt ist $\lceil z \rceil$ die kleinste ganze Zahl größer gleich z:

$$\begin{aligned}
\lfloor z \rfloor &= \max\{y \in \mathbb{Z} \mid y \leq z\} \\
\lceil z \rceil &= \min\{y \in \mathbb{Z} \mid y \geq z\}
\end{aligned}$$

Beispielsweise ist $\lfloor 5,5 \rfloor = 5$ und $\lceil 5,5 \rceil = 6$.

Beispiel für eine Umwandlung: Gesucht ist die Darstellung der Dezimalzahl 86 zur Basis 7: $86_{10} =?_7$

$$\begin{aligned}
n &= \lfloor \log_7 86 \rfloor = 2 \\
z_2 &= \left\lfloor \frac{86}{7^2} \right\rfloor - 7 \cdot \left\lfloor \frac{86}{7^3} \right\rfloor = 1 - 7 \cdot 0 = 1 - 0 = 1 \\
z_1 &= \left\lfloor \frac{86}{7^1} \right\rfloor - 7 \cdot \left\lfloor \frac{86}{7^2} \right\rfloor = 12 - 7 \cdot 1 = 12 - 7 = 5 \\
z_0 &= \left\lfloor \frac{86}{7^0} \right\rfloor - 7 \cdot \left\lfloor \frac{86}{7^1} \right\rfloor = 86 - 7 \cdot 12 = 86 - 84 = 2 \\
&\Rightarrow 86_{10} = 152_7 = 1 \cdot 49 + 5 \cdot 7 + 2 \cdot 1
\end{aligned}$$

Weiteres Beispiel: Stelle die Zahl π zur Basis 2 dar: $\pi = 3,141\ldots_{10} =?_2$

$$\begin{aligned}
n &= \lfloor \log_2 \pi \rfloor = 1 \\
z_1 &= \left\lfloor \frac{\pi}{2^1} \right\rfloor - 2 \cdot \left\lfloor \frac{\pi}{2^2} \right\rfloor = 1 - 0 = 1 \\
z_0 &= \left\lfloor \frac{\pi}{2^0} \right\rfloor - 2 \cdot \left\lfloor \frac{\pi}{2^1} \right\rfloor = 3 - 2 = 1 \\
z_{-1} &= \left\lfloor \frac{\pi}{2^{-1}} \right\rfloor - 2 \cdot \left\lfloor \frac{\pi}{2^0} \right\rfloor = 6 - 6 = 0 \\
z_{-2} &= \left\lfloor \frac{\pi}{2^{-2}} \right\rfloor - 2 \cdot \left\lfloor \frac{\pi}{2^{-1}} \right\rfloor = 12 - 12 = 0 \\
z_{-3} &= \left\lfloor \frac{\pi}{2^{-3}} \right\rfloor - 2 \cdot \left\lfloor \frac{\pi}{2^{-2}} \right\rfloor = 25 - 24 = 1 \\
& \Rightarrow \pi = 11,001\ldots_2 = 1 \cdot 2 + 1 \cdot 1 + 0 \cdot \frac{1}{2} + 0 \cdot \frac{1}{4} + 1 \cdot \frac{1}{8} + \ldots
\end{aligned}$$

Häufig verwendete *Zahlensysteme*:

- $b = 2$: Binärsystem / Dualsystem
- $b = 8$: Oktalsystem
- $b = 10$: Dezimalsystem
- $b = 12$: Duodezimalsystem
- $b = 16$: Hexadezimalsystem ($Z = \{0, \ldots, 9, A, B, C, D, E, F\}$)
- $b = 20$: Vingesimalsystem
- $b = 60$: Sexagesimalsystem

1.3 Computerzahlen

Ein (digitaler) Computer ist *endlich*:

- endlicher (Haupt-)Speicher, z.B. 2 GByte
- endlicher Sekundär-Speicher, z.B. Festplatte 1 TByte
- endlicher interne Rechengenauigkeit, z.B 32 Bit, 64 Bit

Zahlen werden durch endliche Folgen von 0 und 1 dargestellt.

Darstellung ganzer Zahlen

Natürliche Zahlen werden unter Verwendung von N Bits als *Dualzahl* dargestellt

$$\boxed{d_{N-1} d_{N-2} \ldots d_0} \mathrel{\widehat{=}} \sum_{i=0}^{N-1} d_i 2^i, \;\; d_i \in \{0, 1\}$$

Für festes N umfasst der *darstellbare Bereich* alle natürlichen Zahlen z mit

$$z_{min} = 0 \leq z \leq 2^N - 1 = z_{max}$$

Beispiel ($N = 4$): $0000 \mathrel{\widehat{=}} 0$
$0001 \mathrel{\widehat{=}} 1$
$0010 \mathrel{\widehat{=}} 2$
$\vdots$
$1111 \mathrel{\widehat{=}} 15 = 2^4 - 1$

Negative Zahlen könnte man im sogenannten *Einerkomplement* durch Invertieren aller Bits darstellen als

$$\boxed{1 \mid d_{N-2}d_{N-3}\dots d_0} \;\widehat{=}\; -\sum_{i=0}^{N-2}(1-d_i)2^i$$

die führende Eins zeigt dabei an, dass es sich um eine negative Zahl handelt.

Beispiel ($N = 4$): $5 = 0101, -5 = 1010$

Der darstellbare Bereich ist

$$z_{min} = -(2^{N-1} - 1) \leq z \leq 2^{N-1} - 1 = z_{max}$$

Ein Nachteil ist hierbei, dass die Darstellung der 0 nicht eindeutig ist ($0\ 0\ \dots\ 0, 1\ 0\ \dots\ 0$). Deswegen werden negative ganze Zahlen in der Regel im *Zweierkomplement* dargestellt

$$\boxed{1 \mid d_{N-2}d_{N-3}\dots d_0} \;\widehat{=}\; -\left(1 + \sum_{i=0}^{N-2}(1-d_i)2^i\right)$$

Das Vorgehen ist dabei ausgehend von der Dualdarstellung von $-z$ alle Bits umzuklappen und 1 zu addieren, z.B.

-3	$\widehat{=}\ -0011$	$= 1100 + 1$	$= 1101$
Dezimalzahl	$-$Dualzahl	Umklappen + 1	Bitmuster von z

Beispiel ($N = 4$):

$$\begin{aligned}
1111 &\;\widehat{=}\; -(1 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0) = -1\\
1110 &\;\widehat{=}\; -(1 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) = -2\\
&\vdots\\
1000 &\;\widehat{=}\; -(1 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0) = -8
\end{aligned}$$

Der darstellbare Bereich von Zahlen im Zweierkomplement ist

$$z_{min} = -2^{N-1} \leq z \leq 2^{N-1} - 1 = z_{max}$$

Alle ganzen Zahlen im darstellbaren Bereich können im Einer- bzw. Zweierkomplement exakt dargestellt werden. Der Versuch ganze Zahlen mit $z < z_{min}$ oder $z > z_{max}$ (z.B. als Ergebnis einer Rechnung) darzustellen, führt zu *Überlauf*. Mögliche Reaktionen sind:

- Abbrechen mit Fehlermeldung
- Weiterrechnen mit $\tilde{z} = z \bmod z_{max}$ bzw. z_{min}
- Weiterrechnen mit $\tilde{z} = z_{max}$ bzw. z_{min}
- Weiterrechnen mit $\tilde{z} = +\infty$ bzw. $-\infty$ als spezielle Zahl

In modernen Programmierumgebungen wird hier eine Ausnahme (Exception) geworfen und der Benutzer kann selbst entscheiden, ob er mit dem Ergebnis weiterrechnen will.

Darstellung reeller Zahlen

Reelle Zahlen sind bekanntermassen überabzählbar, lückenlos und unbegrenzt, d.h.

- zu jeder reellen Zahl gibt es noch größere und kleinere reelle Zahlen
- zu jedem Paar reeller Zahlen gibt es unendlich viele weitere dazwischen liegende

Die Zahldarstellung eines Computers ist immer endlich, diskret und beschränkt. Demnach kann die Darstellung reeller Zahlen nur *näherungsweise* erfolgen. Ziele sind daher:

1. mache einen möglichst geringen Fehler bei der Darstellung
2. decke einen möglichst großen Zahlenbereich ab

Jeder Zahl $x \in \mathbb{R}$ im darstellbaren Bereich wird dabei eine Maschinenzahl $rd(x)$ so zugeordnet, dass entweder

$$|x - rd(x)| \leq \varepsilon \quad (\textit{absoluter Fehler})$$

oder

$$\frac{|x - rd(x)|}{|x|} \leq \varepsilon \quad (\textit{relativer Fehler})$$

für eine vorgegebene Fehlerschranke ε gilt.

Im *Festkommaformat* wird versucht, den absoluten Fehler bei vorgegebenen Zahlenbereich zu minimieren. Eine Maschinenzahl im Festkommaformat mit N Bits und K Nachkommastellen ist definiert als

$$\boxed{s \mid d_{N-2}d_{N-3}\dots d_K \mid d_{K-1}d_{K-2}\dots d_0} \mathrel{\widehat{=}} (-1)^s \sum_{i=0}^{N-2} d_i 2^{i-K}$$

Beispiel ($N = 6, K = 2$):

$$7.25 = 0 \mid 111 \mid 01 = 1 \cdot 4 + 1 \cdot 2 + 1 \cdot 1 + 0 \cdot \frac{1}{2} + 1 \cdot \frac{1}{4}$$

Der darstellbare Bereich ist

$$x_{min} = -(2^{N-1} - 1)2^{-K} \leq x \leq (2^{N-1} - 1)2^{-K} = x_{max}$$

Die betragsmässig kleinste darstellbare Zahl ungleich Null ist

$$x_{|min|} = 2^{-K}$$

Der maximale absolute Fehler bei der Darstellung einer reellen Zahl x im darstellbaren Bereich ist im Festkommaformat

$$|x - rd(x)| < 2^{-K}$$

Beispiel ($N = 6, K = 2$):

Abbildung 1.1: Alle Festkommazahlen für $N = 7, K = 2$.

Nachteile:

- der darstellbare Bereich ist eng, betragsmäßig kleine und große Zahlen können nicht gut dargestellt werden

- es wird Speicherplatz verschwendet (siehe unten)
- der relative Fehler ist im allgemeinen das sinnvollere Fehlermass

Im *Gleitkommaformat* wird versucht, den relativen Fehler bei vorgegebenem Zahlenbereich zu minimieren. Eine Maschinenzahl im *(normalisierten) Gleitkommaformat* mit Mantissenlänge M, Exponentlänge E und Bias B ist definiert als

$$\boxed{s \mid e_{E-1}e_{E-2}\dots e_0 \mid d_{M-1}d_{M-2}\dots d_0} \mathrel{\widehat{=}} (-1)^s d \cdot 2^e \text{ mit } d = 1 + \sum_{i=0}^{M-1} d_i 2^{i-M} \text{ und } e = \left(\sum_{j=0}^{E-1} e_j 2^j\right) - B$$

Beispiel $(M = 3, E = 3, B = 3)$:

$$0 \mid 011 \mid 010 = (1 + 2 \cdot 2^{-3}) \cdot (2^{3-3}) = 1.25$$

Dabei muss die führende Eins in der Mantisse nicht abgespeichert werden.

Der Wertebereich für den Exponenten ist

$$e_{min} = -B \le e \le (2^E - 1) - B = e_{max}$$

Der darstellbare Bereich für normalisierte Gleitkommazahlen ist damit

$$x_{min} = -(2 - 2^{-M})2^{e_{max}} \le x \le (2 - 2^{-M})2^{e_{max}} = x_{max}$$

und die betragsmäßig kleinste darstellbare Zahl ist

$$x_{|min|} = 2^{e_{min}}$$

Beispiel $(M = 3, E = 3, B = 3)$:

$$e_{min} = -3, e_{max} = (2^3 - 1) - 3 = 4, x_{max} = (2 - 2^{-3})2^4 = 30, x_{|min|} = 2^{-3} = \frac{1}{8}$$

Abbildung 1.2: Alle (positiven) Gleitkommazahlen für $M = 3, E = 3, B = 3$.

Für den relativen Abstand zweier aufeinander folgender Gleitkommazahlen x_1, x_2 gilt

$$2^{-M-1} \le \frac{|x_1 - x_2|}{|x_1|} \le 2^{-M}$$

Die untere Schranke wird für Mantissen $0\dots00$ und $1\dots11$, die obere Schranke für Mantissen $0\dots00$ und $0\dots01$ angenomen.
Beispiel $(M = 3, E = 3, B = 3)$:

$$0 \mid 110 \mid 111 = 15; 0 \mid 111 \mid 000 = 16; 0 \mid 111 \mid 001 = 18$$
$$(16 - 15)/16 = 2^{-4}, (18 - 16)/16 = 2^{-3}$$

Der maximale relative Fehler bei der Darstellung reeller Zahlen im darstellbaren Bereich ist für normalisierte Gleitkommazahlen bei korrekter Rundung

$$\varepsilon = \frac{1}{2} 2^{-(M+1)+1} = 2^{-(M+1)} = eps$$

Die Zahl *eps* wird *Maschinengenauigkeit* genannt.

IEEE 754 Standard für Gleitkommazahlen

IEEE (sprich „I-Triple-E“) = Institute of Electrical and Electronics Engineers
Im IEEE 754 Standard (1985) werden (u.a.) definiert:

Zahl der Bits	Genauigkeit	Typ	Vorzeichen	Mantisse	Exponent	Bias
32 Bit	einfach	float	1 Bit	23 Bits	8 Bits	127
64 Bit	doppelt	double	1 Bit	52 Bits	11 Bits	1023

Im IEEE 754 Standard ist der Bias immer $B = 2^{E-1} - 1$. Der maximale ($e = 1\ldots1$) und minimale ($e = 0\ldots0$) Exponent sind reserviert, sodass für den Wertebereich des Exponenten gilt

$$e_{min} = -2^{E-1} + 2 \leq e \leq 2^{E-1} - 1 = e_{max}$$

Um Zahlen, die betragsmässig kleiner als $x_{|min|}$ darzustellen, werden, wenn der Exponent Null, die Mantisse aber ungleich Null ist, *denormalisierte Gleitkommazahlen* (d.h. ohne die führende Eins) verwendet. Auf diese Weise wird die Lücke zur Null weiter geschlossen, was jedoch auf Kosten der Genauigkeit geschieht. Der Versuch, noch kleinere Zahlen darzustellen, führt zu *Unterlauf.*

Damit gilt:

Typ	x_{max}	$x_{\|min\|}$	eps
float	$(2-2^{-23}) \cdot 2^{127} \approx 3.4 \cdot 10^{38}$	$2^{-23} \cdot 2^{-126} \approx 1.4 \cdot 10^{-45}$	$2^{-23+1} \approx 6.0 \cdot 10^{-8}$
double	$(2-2^{-52}) \cdot 2^{1023} \approx 1.8 \cdot 10^{308}$	$2^{-52} \cdot 2^{-1022} \approx 4.9 \cdot 10^{-324}$	$2^{-52+1} \approx 1.1 \cdot 10^{-16}$

Kapitel 2

Mengen und Aussagen

2.1 Mengen

Eine *Menge* ist eine Zusammenfassung bestimmter, wohlunterscheidbarer mathematischer Objekte, die Elemente der Menge genannt werden, zu einem Ganzen.

Bezeichnungen sind: Menge M, Element der Menge $m \in M$ und kein Element der Menge $m \notin M$.

Die Zahl der Elemente einer Menge (die *Mächtigkeit* der Menge) wird durch $|M|$ oder $\#M$ notiert. Die leere Menge ist dadurch charakterisiert, dass sie kein Element enthält, und wird durch $\{\}$ oder $\emptyset$ bezeichnet. Die Mächtigkeit der bereits bekannten Zahlmengen ist nicht endlich, sondern abzählbar unendlich ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}$) bzw. überabzählbar unendlich ($\mathbb{R}, \mathbb{C}$).

Es gibt verschiedene Möglichkeiten, Mengen zu definieren. Eine *Umfangsdefinition* besteht in der direkten Angabe aller Elemente der Menge, zum Beispiel:

$$\begin{aligned} M &= \{1,2,3\} = \{2,3,1\} = \{3,3,1,2,2\} \\ M &= \{1,2,3,4,5,6,7,8\} = \{1,2,\ldots,8\} = \{1,\ldots,8\} \end{aligned}$$

Eine *Inhaltsdefinition* besteht in der Angabe der Eigenschaften der Elemente der Menge, zum Beispiel die Menge der geraden Zahlen:

$$\begin{aligned} M &= \{z \in \mathbb{Z} \mid z \text{ ist gerade}\} \\ M &= \{z \in \mathbb{Z} \mid z \text{ ist durch 2 teilbar}\} \\ M &= \{z \in \mathbb{Z} \mid 2\lfloor \tfrac{z}{2} \rfloor = z\} \end{aligned}$$

Teilmengen und Gleichheit:

- *Teilmenge*: $A \subseteq B$: für alle $x \in A$ ist auch $x \in B$
- *Gleichheit*: $A = B$: $A \subseteq B$ und $B \subseteq A$
- *Ungleichheit*: $A \neq B$: es existiert ein $a \in A$, sodass $a \notin B$ oder ein $b \in B$, sodass $b \notin A$
- *Echte Teilmenge*: $A \subsetneq B$: $A \subseteq B$ und $A \neq B$

Mengenoperationen:

- *Durchschnitt*: $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$
- *Vereinigung*: $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$
- *Differenz (relatives Komplement)*: $A \setminus B = \{x \mid x \in A \text{ und } x \notin B\}$
- *Absolutes Komplement*: $B^{\mathrm{C}} = \{x \mid x \notin B\} = G \setminus B$, G ist die Grundmenge
- *Symmetrische Differenz*: $A \Delta B = (A \setminus B) \cup (B \setminus A)$

Rechenregeln:

- *Transitivität*: $A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$
- *Assoziativität*: $A \cup (B \cup C) = (A \cup B) \cup C$
  $A \cap (B \cap C) = (A \cap B) \cap C$
- *Kommutativität*: $A \cup B = B \cup A$
  $A \cap B = B \cap A$
- *Distributivität*: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Die *Potenzmenge* $\mathcal{P}(A)$ einer Menge A ist die Menge aller Teilmengen von A:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Beispiel: $A = \{1, 2, 3\}, \mathcal{P}(A) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Die Potenzmenge einer Menge mit $|A| = n$ Elementen besteht aus $|\mathcal{P}(A)| = 2^n$ Elementen.

2.2 Tupel

Ein *(geordnetes) Paar* ist eine Zusammenfassung zweier, nicht notwendigerweise verschiedener mathematischer Objekte. Man schreibt $P = (a, b)$. Hierbei spielt die Reihenfolge eine Rolle, im Allgemeinen ist $(a, b) \neq (b, a)$.

Beispiele: Paar aus Zahlen: $(1, 2)$, Paar aus Mengen: $(\{1, 2, 3\}, \{4, 5, 6\})$, Paar aus Zahl und Menge: $(1, \{\})$.

Zwei Paare (a, b) und (c, d) sind genau dann gleich, wenn $a = c$ und $b = d$ gilt.

Ein *Tupel* ist eine Zusammenfassung mehrerer, nicht notwendigerweise verschiedener mathematischer Objekte. Man schreibt ein n-Tupel als $T = (a_1, \ldots, a_n)$. Paare sind 2-Tupel. Das leere Tupel oder 0-Tupel wird durch () bezeichnet.

Zwei Tupel $(a_1, \ldots, a_n)$ und $(b_1, \ldots, b_m)$ sind genau dann gleich, wenn $n = m$ und $a_i = b_i$ für $i = 1, \ldots, n$ gilt.

Zeichenketten (Strings) sind spezielle Tupel, zum Beispiel "Wort" = ("W", "o", "r", "t"). Hierbei ist die Grundmenge ein Alphabet { "a", "b", "c", …}.

Das *kartesische Produkt* zweier Mengen ist die Menge aller Paare von Elementen der Mengen:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Beispiel: $A = \{1, 2, 3\}, B = \{4, 5\}$: $A \times B = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$
Distributivgesetze::

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C) \\ A \times (B \cap C) &= (A \times B) \cap (A \times C) \\ A \times (B \setminus C) &= (A \times B) \setminus (A \times C) \end{aligned}$$

Das *mehrfache kartesische Produkt* von n Mengen ist analog dazu die Menge aller n-Tupel von Elementen der Mengen

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } i = 1, \ldots, n\}$$

Speziell ist das n-fache kartesische Produkt einer Menge A mit sich selbst

$$\underbrace{A \times \ldots \times A}_{n-mal} = A^n = \{(a_1, \ldots, a_n) \mid a_i \in A \text{ für } i = 1, \ldots, n\}$$

Für die Mächtigkeit des kartesichen Produkts gilt dann: $|A^n| = |A|^n$. Wichtige Beispiele sind die Euklidische Ebene $\mathbb{R}^2$ und der Euklidische Raum $\mathbb{R}^3$.

2.3 Aussagen

Eine *Aussage* ist eine sprachliche Feststellung, die entweder wahr oder falsch ist. Wir betrachten hierzu die Menge $\{w, f\}$ (auch $\{true, false\}$, $\{1, 0\}$, ...).

Beispiele:

- 2 ist eine gerade Zahl (w)
- 1004 ist durch 3 teilbar (f)
- $2^{999999999-1}$ ist eine Primzahl (unbekannt, aber w oder f)

Verknüpfungen (*Junktoren*) von Aussagen A, B:

- *Negation*: $\neg A$ (nicht A): genau dann wahr, wenn A falsch ist
- *Konjunktion*: $A \wedge B$ (A und B): genau dann wahr, wenn A und B wahr sind
- *Alternative*: $A \vee B$ (A oder B): genau dann falsch, wenn A und B falsch sind
- *Implikation*: $A \Rightarrow B$ (wenn A dann B): genau dann falsch, wenn A wahr und B falsch ist
- *Äquivalenz*: $A \Leftrightarrow B$ (A genau dann wenn B): genau dann falsch, wenn A und B beide wahr oder falsch sind

Die zugehörigen Wahrheitstafeln sind:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	f	w	w	f
f	f	f	f	w	w

A	$\neg A$
w	f
f	w

Rechenregeln:

- *Kommutativität*: $A \wedge B \Leftrightarrow B \wedge A$
  $A \vee B \Leftrightarrow B \vee A$
- *Assoziativität*: $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$
  $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$
- *Distributivität*: $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$
  $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
- *Verschmelzung*: $A \wedge (A \vee B) \Leftrightarrow A$
  $A \vee (A \wedge B) \Leftrightarrow A$

Beweis zur Verschmelzung über Wahrheitstafeln:

A	B	$A \vee B$	$A \wedge (A \vee B)$	$A \wedge B$	$A \vee (A \wedge B)$
w	w	w	w	w	w
w	f	w	w	f	w
f	w	w	f	f	f
f	f	f	f	f	f

Der *Beweis* eines mathematischen Satzes mit Voraussetzung V und Behauptung B ist formal eine Kette von Implikationen:

$$V \Rightarrow \ldots \Rightarrow B$$

Es gilt $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$. Ein *Widerspruchsbeweis* ist eine Kette

$$(V \wedge \neg B) \Rightarrow \ldots \Rightarrow f$$

Ist $V = V_1 \vee V_2$, dann zeigt man bei einem *Beweis durch Fallunterscheidung*:

$$V_1 \Rightarrow \ldots \Rightarrow B \quad \text{und} \quad V_2 \Rightarrow \ldots \Rightarrow B$$

Kapitel 3

Relationen und Abbildungen

3.1 Relationen

Eine *binäre (zweistellige) Relation* zwischen zwei Mengen A und B ist eine Teilmenge des kartesischen Produkts

$$R \subseteq A \times B$$

Man schreibt: $a\ R\ b \Leftrightarrow (a, b) \in R$. Analog dazu ist eine n-stellige Relation zwischen n Mengen $A_1, \ldots, A_n$

$$R \subseteq A_1 \times \ldots \times A_n$$

Zum Beispiel sei $A = B = \{1, 2, 3\}$. Es ist $A \times B = \{(1, 1), \ldots, (3, 3)\}$. Die Kleiner-Relation und die Kleiner-Gleich-Relation sind dann

$$\begin{aligned} < &= \{(1, 2), (1, 3), (2, 3)\} \\ \leq &= \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\} \end{aligned}$$

Die Umkehrrelation R^{-1} zu einer Relation R ist dann

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

Zum Beispiel ist die Umkerrelation der Kleiner-Relation die Größer-Relation

$$<^{-1} \ = \{(2, 1), (3, 1), (3, 2)\} = \ >$$

Eine *Äquivalenzrelation* auf einer Menge A ist eine Relation $R \subseteq A \times A$, die folgende Axiome erfüllt:

- *Reflexivität*: $(a, a) \in R$ für alle $a \in A$
- *Symmetrie*: $(a, b) \in R \Rightarrow (b, a) \in R$
- *Transitivität*: $(a, b), (b, c) \in R \Rightarrow (a, c) \in R$

Man schreibt $a \sim_R b$ oder $a \overset{R}{\sim} b$ oder, wenn klar ist um welche Äquivalenzelation es sich handelt, $a \sim b$.

Zum Beispiel ist eine Äquivelenzrelation, die die Menge $A = \{0, \ldots, 9\}$ in gerade und ungerade Zahlen einteilt

$$\begin{aligned} R &= \{(a,b) \mid a \text{ und } b \text{ gerade oder } a \text{ und } b \text{ ungerade}\} \\ &= \{(0,0),(0,2),\ldots,(8,8),(1,1),(1,3),\ldots,(9,9)\} \end{aligned}$$

Eine *Äquivalenzklasse* eines Elements $a \in A$ ist die Menge der Elemente, die äquivalent zu a sind:

$$[a]_R = \{b \in A \mid a \sim_R b\}$$

Das Element a heißt dann Repräsentant von $[a]_R$. Zum Beispiel ist

$$[0]_R = \{0,2,4,6,8\} \text{ und } [1] = \{1,3,5,7,9\}$$

Es gilt

$$[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow a \in [b] \Leftrightarrow b \in [a] \Leftrightarrow [a] \cap [b] \neq \emptyset$$

Eine *Ordnungsrelation* (wie die Kleiner-Relation) ist eine Relation, die zumindest transitiv ist.
Wichtige Eigenschaften von Relationen.

- *linkstotal*: $\forall a \in A\ \exists b \in B$ sodass $(a,b) \in R$
- *rechtstotal (surjektiv)*: $\forall b \in B\ \exists a \in A$ sodass $(a,b) \in R$
- *linkseindeutig (injektiv)*: $\forall a,c \in A\ \forall b \in B$ gilt: $(a,b) \in R$ und $(b,c) \in R \Rightarrow a = c$
- *rechtseindeutig*: $\forall a \in A\ \forall b,c \in B$ gilt: $(a,b) \in R$ und $(a,c) \in R \Rightarrow b = c$

Anschaulich:

- linkstotal: jedes $a \in A$ hat einen mindestens einen Partner in B
- rechtstotal: jedes $b \in B$ hat einen mindestens einen Partner in A
- linkseindeutig: jedes $b \in B$ hat einen maximal einen Partner in A
- rechtseindeutig: jedes $a \in A$ hat einen maximal einen Partner in B

Eine Relation heißt eineindeutig (bijektiv), wenn jedes $b \in B$ genau einen Partner $a \in A$ hat.

3.2 Abbildungen

Eine *Abbildung* ist eine linkstotale und reichtseindeutige Relation. Eine Abbildung f von A nach B ist demnach eine Vorschrift, die jedem $a \in A$ genau ein Abbild $b \in B$ zuordnet, das $f(a)$ genannt wird. Die Menge A heißt *Definitionsbereich* und die Menge B *Zielbereich* der Abbildung $f\colon A \to B$.

Der *Graph* einer Abbildung ist die Menge

$$G(f) = \{(a,b) \in A \times B \mid a \in A, b = f(a)\}$$

Die Menge

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

heißt *Bildmenge* oder kurz *Bild* von A und die Menge

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

heißt *Urbildmenge* oder kurz *Urbild* von B.

Zwei Abbildungen $f\colon A \to B$ und $g\colon C \to D$ heißen gleich, wenn gilt

$$A = C, B = D \text{ und } f(x) = g(x) \forall x \in A$$

Sind A und B Zahlenmengen, spricht man häufig von *Funktionen* statt von Abbildungen.

Beispiele:

- Identität: $id\colon A \to A \quad x \mapsto x$
- Projektion auf den ersten Faktor eines Paares: $\pi_1\colon A \times B \to A \quad (a, b) \mapsto a$
- Projektion auf den zweiten Faktor eines Paares: $\pi_2\colon A \times B \to A \quad (a, b) \mapsto b$

Regeln:

- $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$
- $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
- $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

Die *Hintereinanderausführung (Komposition)* zweier Abbildungen $f\colon X \to Y$ und $g\colon Y \to Z$ ist

$$g \circ f\colon X \to Z \quad x \mapsto (g \circ f)(x) = g(f(x))$$

Beispiel: Sind $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x + 1$ und $g\colon \mathbb{R} \to \mathbb{R}, x \mapsto 2x$, dann ist

$$\begin{array}{ll} g \circ f\colon \mathbb{R} \to \mathbb{R} & x \mapsto g(f(x)) = g(x + 1) = 2(x + 1) \\ f \circ g\colon \mathbb{R} \to \mathbb{R} & x \mapsto f(g(x)) = f(2x) = 2x + 1 \end{array}$$

Die Hintereinanderausführung von Abbildungen ist also im Allgemeinen nicht kommutativ (selbst wenn die Mengen passen sollten).

Regeln: Sind $f\colon X \to Y$, $g\colon Y \to Z$ und $h\colon Z \to W$, dann gilt

- $id_Y \circ f = f \circ id_X$
- $h \circ (g \circ f) = (h \circ g) \circ f$

Die *inverse Abbildung (Umkehrfunktion)* einer bijektiven Abbildung $f\colon X \to Y$ ist die eindeutig definierte Abbildung $f^{-1}\colon Y \to X$ mit

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

Die inverse Abbildung bildet damit jedes $y \in Y$ auf das eindeutig definierte $x \in X$ ab, für das mit $f(x) = y$ gilt.

Sind $f\colon X \to Y$ und $f\colon Y \to Z$ beide bijektiv, dann ist auch $g \circ f\colon X \to Z$ bijektiv und es gilt

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Beispiel: Sind wieder $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x + 1$ und $g\colon \mathbb{R} \to \mathbb{R}, x \mapsto 2x$, dann ist

$$\begin{aligned}
f^{-1}\colon \mathbb{R} \to \mathbb{R} &\qquad x \mapsto x - 1 \\
g^{-1}\colon \mathbb{R} \to \mathbb{R} &\qquad x \mapsto \frac{x}{2} \\
(g \circ f)^{-1}\colon \mathbb{R} \to \mathbb{R} &\qquad x \mapsto f^{-1}(g^{-1}(x)) = \frac{x}{2} - 1 \\
(f \circ g)^{-1}\colon \mathbb{R} \to \mathbb{R} &\qquad x \mapsto g^{-1}(f^{-1}(x)) = \frac{x - 1}{2}
\end{aligned}$$

Kapitel 4

Operationen und Strukturen

4.1 Operationen

Eine *zweistellige Operation* (innere zweistellige Verknüpfung) auf einer Menge A ist eine Abbildung $*\colon A \times A \to A,\ (a,b) \mapsto a * b$.

Beispiele für zweistellige Operationen: Grundrechenarten:

- Addition $+$ für $A \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$
- Subtraktion $-$ für $A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$
- Multiplikation $*$ für $A \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$
- Division $/$ für $A \in \{\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}\}$

Junktoren:

- Konjunktion $\wedge$ für $A \in \{w, f\}$
- Alternative $\vee$ für $A \in \{w, f\}$
- Implikation $\Leftarrow$ für $A \in \{w, f\}$
- Äquivalenz $\Leftrightarrow$ für $A \in \{w, f\}$

Komposition $\circ$ für $A = Abb(X) = \{f\colon X \to X\}$ (Menge der Selbsabbildungen einer Menge X)

Mengenoperationen:

- Vereinigung $\cup$ für $A = \mathcal{P}(X)$
- Durchschnitt $\cap$ für $A = \mathcal{P}(X)$ für eine beliebige Menge X

Verknüpfungstafeln dienen zur Visualisierung der Funktionsweise zweistelliger Operationen. Beispiele sind das „Einspluseins“ und das „Einmaleins“

$+$	1	2	3	$\cdots$
1	2	3	4	$\cdots$
2	3	4	5	$\cdots$
3	4	5	6	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$*$	1	2	3	$\cdots$
1	1	2	6	$\cdots$
2	2	4	9	$\cdots$
3	3	6	12	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

oder die Wahrheitstafeln der Junktoren.

Zweistellige Operationen können folgende Eigenschaften haben:

- Assoziativität: $(a * b) * c = a * (b * c)$ für alle $a, b, c \in A$
- Kommutativität: $a * b = b * a$ für alle $a, b \in A$

Bezüglich einer Operation $*$ können Elemente in der Menge A folgendermaßen ausgezeichnet sein:

- Ein Element $e \in A$ heißt *neutrales Element* falls $a * e = e * a$ für alle $a \in A$ gilt.
- Ein Element $b \in A$ heißt *inverses Element zu* a falls $a * b = b * a = e$ gilt.

Das inverse Element zu a wird meist mit a^{-1} bezeichnet.

Für zwei zweistellige Operationen $*$, $\circ$ kann auch noch gelten:

- Distributivität: $(a * b) \circ c = (a * c) \circ (b * c)$ und $a * (b \circ c) = (a * b) \circ (a * c)$ für alle $a, b, c \in A$

4.2 Strukturen

Eine *algebraische Struktur* $\mathcal{A} = (A, *_1, *_2, \ldots)$ besteht aus einer Menge A mit ein oder mehreren Operationen $*_1, *_2, \ldots$, für die eine Reihe von Eigenschaften gelten, die als Axiome festgelegt werden.

Wichtige algebraische Strukturen sind:

- Halbgruppe $(A, *)$, mit Assoziativgesetz
- Gruppe $(A, *)$, mit Assoziativgesetz, neutralem Element und inversem Element
- Kommutative Gruppe $(A, *)$, mit Assoziativgesetz, Kommutativgesetz, neutralem Element und inversem Element
- Ring $(A, *, \circ)$, wobei $(A, *)$ eine kommutative Gruppe und $(A, \circ)$ eine Halbgruppe ist
- Kommutativer Ring $(A, *, \circ)$, wobei $(A, *)$ eine kommutative Gruppe und $(A, \circ)$ eine kommutative Halbgruppe ist
- Körper $(A, *, \circ)$, wobei $(A, *)$ eine kommutative Gruppe und $(A \setminus \{0\}, \circ)$ eine kommutative Gruppe ist und das Distributivgesetz gilt

Beispiele für algebraische Strukturen sind:

- $(\mathbb{N}, +)$ und $(\mathbb{N}, *)$ sind kommutative Halbgruppen
- $(\mathbb{Z}, *)$ ist eine kommutative Gruppe
- $(\mathbb{Z}, +, *)$ ist ein kommutativer Ring
- $(\mathbb{Q}, +, *)$, $(\mathbb{R}, +, *)$ und $(\mathbb{C}, +, *)$ sind Körper
- $(\mathit{Abb}(R), +, *)$, wobei R ein Ring ist, ist wieder ein Ring (der Endomorphismenring)
- $(\mathit{Abb}(M), \circ)$ ist eine Halbgruppe (die Endomorphismenhalbgruppe)
- $(\{f \in \mathit{Abb}(M) : f \text{ bijektiv}\}, \circ)$ ist eine Gruppe (die Automorphismengruppe)

Das neutrale Element $e \in A$ in einer Gruppe ist eindeutig. Wäre nämlich e' ein weiteres neutrales Element, dann gilt

$$e' = e' * e = e$$

und somit Gleichheit. Das zu a inverse Element a^{-1} ist ebenfalls eindeutig. Wäre nämlich $\bar{a}^{-1}$ ein weiteres zu a inverses Element, dann folgt aus

$$a * a^{-1} = a^{-1} * a = e \text{ und } a * \bar{a}^{-1} = \bar{a}^{-1} * a = e$$

über die Assoziativität die Gleichheit

$$\bar{a}^{-1} = \bar{a}^{-1} * e = \bar{a}^{-1} * (a * a^{-1}) = (\bar{a}^{-1} * a) * a^{-1} = e * \bar{a} = \bar{a}$$

4.3 Modulare Arithmetik

Die *modulare Arithmetik* beschreibt das Rechnen im *Restklassenring*

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

wobei m der gewählte *Modul* ist und

$$[i] = \{n \in \mathbb{Z} | n = qm + i \text{ für ein } q \in \mathbb{Z}\}$$

die *Restklasse* zur Zahl i ist. Die Restklassen beschreiben Äquivalenzklassen bezüglich der Äquivalenzrelation „Division mit Rest„. Die gleiche Restklasse kann dabei durch verschiedene Repräsentanten beschrieben werden, so gilt

$$\ldots = [-2m+1] = [-m+1] = [1] = [m+1] = [2m+1] = \ldots.$$

Für diese Restklassen werden nun die folgenden Rechenoperationen definiert:

- Addition: $[i] + [j] = [i + j]$
- Multiplikation: $[i] * [j] = [i * j]$

Diese Operationen sind wohldefiniert denn aus $[i] = [j], [i'] = [j']$ folgt $[i+j] = [i'+j']$ und $[i*j] = [i'*j']$. Auf diese Weise erhält man den *Restklassenring* $(\mathbb{Z}_m, +, *)$, wobei $[0]$ das neutrale Element der Addition, $[1]$ das neutrale Element der Multiplikation und $[m-i]$ das inverse Element zu $[i]$ bezüglich der Addition ist.

Ist p eine Primzahl, so besitzt auch jedes Element in $\mathbb{Z}_p \setminus \{[0]\}$ auch ein inverses Element bezüglich der Multiplikation (das aber nicht so einfach angebbar ist) und $(\mathbb{Z}_p, +, *)$ bildet einen Körper.

Beispiel: Verknüpfungstafeln für $\mathbb{Z}_5$:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

*	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

4.4 Permutationen

Eine *Permutation* ist eine bijektive Abbildung $\pi\colon \{1,\dots,n\} \to \{1,\dots,n\}$. Eine Permutation ist damit eine Selbstabbildung der Menge $\{1,\dots,n\}$, bei der jede Zahl genau einmal als Abbild vorkommt. Man notiert Permutationen typischerweise in Zweizeilenform

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

Kompakter ist die Tupelschreibweise $\pi = (\pi(1), \pi(2), \dots, \pi(n))$, bei der nur die zweite Teile der Zweizeilenform notiert wird. Dies ist aber nur möglich, wenn die Reihenfolge der Zahlen der ersten Zeile bekannt ist (i.d.R. die natürliche Reihenfolge).

Die Permutationen fester Länge n bilden mit der Hintereinanderausführung $\circ$ als Verknüpfung eine Gruppe, die *symmetrische Gruppe* S_n. Die Hintereinanderausführung von zwei Permutationen erfolgt durch Verfolgen der Wege der Zahlen. Zum Beispiel ist

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

denn man verfolgt die Wege $1 \mapsto 1 \mapsto 3$, $2 \mapsto 3 \mapsto 2$ und $3 \mapsto 2 \mapsto 1$.

Das neutrale Element in der symmetrischen Gruppe ist die *identische Permutation* $\mathrm{id} = (1, 2, \dots, n)$ und das inverse Element ist die *inverse Permutation* π^{-1} mit $\pi^{-1} \circ \pi = \pi \circ \pi^{-1} = \mathrm{id}$. Die inverse Permutation lässt sich durch Vertauschen der beiden Zeilen der Zweizeilenform bestimmen:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Ein *Fehlstand* in einer Permutation ist ein Zahlenpaar, deren Ordnung durch die Permutation umgekehrt wird, also ein Paar (i, j), mit $i, j \in \{1, \dots, n\}$ für das

$$i < j \quad \text{und} \quad \pi(i) > \pi(j)$$

gilt. Die Menge der Fehlstände in einer Permutation π ist dann

$$\mathrm{inv}(\pi) = \{(i, j) \in \{1, \dots, n\}^2 \mid i < j \quad \text{und} \quad \pi(i) > \pi(j)$$

Die Fehlstandszahl $|\,\mathrm{inv}(\pi)|$ kann als Maß für die Unordnung der durch die Permutation vertauschten Zahlen angesehen werden. Zum Beispiel hat die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

die Fehlstände $\mathrm{inv}(\pi) = \{(1, 3), (2, 3), (1, 4), (2, 4), (2, 5)\}$. Man findet die Fehlstände, indem man für jede Zahl in der zweiten Zeile alle Zahlen findet, die größer sind und links von der Zahl stehen. Die Fehlstände sind dann die Zahlenpaare in der ersten Zeile.

Eine *Nachbarvertauschung* ist eine Permutation, die zwei benachbarte Zahlen $i, i+1$ miteinander vertauscht, also $\pi(i) = i+1$, $\pi(i+1) = i$ und $\pi(j) = j$ für $j \in \{1, \dots, n\} \setminus \{i, i+1\}$. Zum Beispiel vertauscht die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

die beiden Zahlen 3 und 4. Eine Nachbarvertauschung erzeugt genau einen Fehlstand. Eine *Vertauschung* ist eine Permutation, die zwei beliebige Zahlen i, j mit $j > i$ miteinander vertauscht, also $\pi(i) = j$, $\pi(j) = i$ und $\pi(k) = k$ für $k \in \{1, \dots, n\} \setminus \{i, j\}$. Zum Beispiel vertauscht die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$$

die beiden Zahlen 1 und 4. Jede Vertauschung erzeugt die $2(j-i)-1$ Fehlstände

$$\{(i,j)\} \cup \{(i,k) \mid k = i+1, \dots, j-1\} \cup \{(k,j) \mid k = i+1, \dots, j-1\}$$

Ein *k-Zyklus* ist eine Permutation, die k verschiedene Zahlen $\{i_1, \dots, i_k\}$ im Kreis vertauscht und die übrigen Zahlen festhält, also $\pi(i_1) = i_2, \pi(i_2) = i_3, \dots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1$ und $\pi(j) = j$ für $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\}$. Zum Beispiel ist die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}$$

ein 3-Zyklus, der die Zahlen 2, 3 und 4 im Kreis vertauscht. Zyklen werden durch $(i_1\ i_2\ \dots\ i_k)$ notiert. Jede Permutation zerfällt in disjunkte Zyklen. In der Zykelnotation einer Permutation beginnt man mit einer beliebigen Zahl a und notiert den Zyklus, der mit der Zahl a beginnt. Dann wählt man eine Zahl b, die bislang noch nicht vorgekommen ist, notiert den Zyklus, der mit der Zahl b beginnt und so weiter bis alle Zahlen genau einmal vorkommen.

$$(a\ \pi(a)\ \pi^2(a) \dots \pi^k(a))(b\ \pi(b)\ \pi^2(b) \dots \pi^l(b)) \dots$$

Einerzyklen können anschließend auch weggelassen werden. Zum Beispiel ist die Zykelnotation der Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 1 & 2 \end{pmatrix} = (1\ 4\ 5)(2\ 6)(3) = (1\ 4\ 5)(2\ 6)$$

Das *Vorzeichen* (*Signum*) einer Permutation ist definiert als

$$\operatorname{sgn}(\pi) = (-1)^{|\operatorname{inv}(\pi)|}.$$

Das Vorzeichen ist also $+1$, wenn die Anzahl der Fehlstände gerade ist und -1, wenn die Anzahl ungerade ist. Im ersten Fall spricht man von einer *geraden*, im zweiten Fahl von einer *ungeraden* Permutation.
Für das Vorzeichen der Hintereinanderausführung zweier Permutationen τ, π gilt die folgende Verkettungseigenschaft:

$$\operatorname{sgn}(\tau \circ \pi) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\pi)$$

Beweis: Es gilt:

$$\begin{aligned} \operatorname{sgn}(\tau \circ \pi) &= \prod_{i<j} \frac{\tau(\pi(j)) - \tau(\pi(i))}{j-i} = \prod_{i<j} \frac{\tau(\pi(j)) - \tau(\pi(i))}{\pi(j) - \pi(i)} \cdot \prod_{i<j} \frac{\pi(j) - \pi(i)}{j-i} = \\ &= \prod_{\pi^{-1}(i) < \pi^{-1}(j)} \frac{\tau(j) - \tau(i)}{j-i} \cdot \prod_{i<j} \frac{\pi(j) - \pi(i)}{j-i} = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\pi) \end{aligned}$$

Nachdem sich jeder k-Zyklus $(i_1\ i_2\ \dots\ i_k)$ als Hintereinanderausführung von $k-1$ Vertauschungen schreiben lässt

$$(i_1\ i_2\ \dots\ i_k) = (i_1\ i_2) \circ (i_2\ i_3) \circ \dots \circ (i_{k-1}\ i_k)$$

gilt für das Vorzeichen eines k-Zyklus

$$\operatorname{sgn}((i_1\ i_2\ \dots\ i_k)) = (-1)^{k-1}$$

Aus der Zykeldarstellung einer Permutation lässt sich demnach das Vorzeichen direkt ablesen: das Vorzeichen ist genau dann gerade, wenn die Anzahl der Zyklen gerader Länge gerade ist.

Die Ordnung einer Permutation π ist die kleinste natürliche Zahl k, sodass die k-malige Hintereinanderausführung von π die identische Permutation ergibt:

$$\operatorname{ord}(\pi) = \min\{k \in \mathbb{N} \mid \pi^k = \mathrm{id}\}$$

Die Ordnung einer Permutation ergibt sich als das kleinste gemeinsame Vielfache der Längen der disjunkten Zyklen der Permutation.

Kapitel 5

Algorithmen und Programme

5.1 Algorithmen

Ein *Algorithmus* für eine vorgegebene bestimmte Art von Aufgaben ist eine endliche Abfolge von wohldefinierten, ausführbaren Vorschriften, die bei Abarbeitung, ausgehend von einem Eingangszustand (Input) nach einer endlichen Anzahl von Verarbeitungsschritten einen Ausgangszustand (Output) bestimmen, der als Lösung der durch den Eingangszustand charakterisierten Aufgabe angesehen werden kann.

Beispiele für Algorithmen sind (im Idealfall) Bedienungsanleitungen und Kochrezepte.

Die folgende Liste von Anweisungen

Eingabe: Natürliche Zahl n
Schritt 1: Setze $k := 1, a := n$
Schritt 2: Ist $a = 1$ gehe zu Ausgabe
Schritt 3: Setze $a := \begin{cases} 3a+1 & \text{falls } a \text{ ungerade} \\ a/2 & \text{falls } a \text{ gerade} \end{cases}$
Schritt 4: Setze $k := k + 1$ und gehe zu Schritt 2
Ausgabe: k als Länge der erzeugten Zahlenfolge

stellt jedoch keinen Algorithmus dar, denn es ist nicht sichergestellt, dass die Abarbeitung der Anweisungen für jede Eingabezahl terminiert (Collatz-Problem).

Bei dem Entwurf von Algorithmen sind folgende Fragen zu beantworten:

- Komplexität: Wie lässt sich der Aufwand abschätzen, der betrieben werden muss, um die Aufgabe zu lösen?
- Korrektheit: Wie lässt sich nachweisen, dass der Algorithmus die Aufgabe auch tatsächlich löst?
- Robustheit: Wie groß ist die Problemklasse, für die der Algorithmus funktioniert?
- Genauigkeit: Wie groß ist der Berechnungsfehler (bei numerischen Algorithmen)?
- Berechenbarkeit: Gibt es Aufgaben, für die kein Algorithmus (oder kein effizienter Algorithmus) existiert?

Bei der Effizienzuntersuchung von Algorithmen werden folgende Komplexitäten unterschieden:

- Worst-Case-Komplexität: Obere Schranke für den Aufwand in Abhängigkeit vom Input
- Average-Case-Komplexität: Obere Schranke für den mittleren Aufwand in Abhängigkeit vom Input (unter bestimmten Annahmen über die Wahrscheinlichkeitsverteilung der Aufgaben in der Problemklasse)
- Untere Komplexität: Untere Schranke für den Aufwand zur Lösung eines Problems in einer Problemklasse unabhängig vom konkreten Algorithmus.

Komplexitätsklassen werden mit Hilfe der *Landau-Symbole* angegeben:

- $f = O(g)$ wenn $f(x) \leq Cg(x)$ mit $C > 0$ für alle $x > x_0$ (f wächst nicht wesentlich schneller als g)
- $f = \Omega(g)$ wenn $f(x) \geq Cg(x)$ mit $C > 0$ für alle $x > x_0$ (f wächst nicht wesentlich langsamer als g)

Wichtige Komplexitätsklassen für den Aufwand C zur Lösung eines Problems der Größe N sind

- Lineare Komplexität: $C = O(N)$
- Quadratische Komplexität: $C = O(N^2)$
- Kubische Komplexität: $C = O(N^3)$
- Exponentielle Komplexität: $C = O(2^N)$
- Logarithmische Komplexität: $C = O(\log N)$

Neben der Laufzeitkomplexität wird häufig auch die Speicherkomplexität eines Algorithmus betrachtet.

Ein *Computerprogramm* ist eine Implementierung eines Algorithmus in einem Computer mit Hilfe einer Programmiersprache. Hierzu werden heute meist höhere Programmiersprachen wie C, C++, Java oder Softwarepakete wie Mathematica, Maple oder Sage verwendet.

5.2 Sortieralgorithmen

5.3 Rekursion

Literaturverzeichnis

[1] Tilo Arens, Frank Hettlich, Christian Karpfinger Ulrich Kockelkorn, Klaus Lichtenegger, Hellmuth Stachel: *Mathematik*, Spektrum Akademischer Verlag, 2010.

[2] Dorothea Bahns, Christoph Schweigert: *Softwarepraktikum - Analysis und Lineare Algebra*. Vieweg Verlag, 2008.

[3] Thomas H. Cormen, Charles E. Leiserson, Ronald Rivest, Clifford Stein, Paul Molitor: *Algorithmen – eine Einführung*, Oldenbourg Verlag, 2010

[4] Winfrid Hochstättler: *Algorithmische Mathematik*, Springer Verlag, 2010

[5] Sage Development Team: *Sage Documentation*, http://www.sagemath.org/doc/

[6] Thomas Sonar: *Angewandte Mathematik, Modellbildung und Informatik*, Vieweg Verlag, 2001.

[7] Thorsten Theobald, Sadik Iliman: *Einführung in die computerorientierte Mathematik mit Sage*, Springer Verlag, 2016.