Diskrete Mathematik

Inhalte 4. Vorlesungswoche
Sebastian Iwanowski
FH Wedel

Referenzen zum Nacharbeiten:

Meinel 5.4
Meinel 10.2-10.4 (zur Vertiefung: 10.5-10.8 und Beutelspacher 10)
Meinel 3
Lang 4.1 (nur bis S. 43)
Meinel 7

2. Mengenlehre

2.3 Funktionen

Mächtigkeit von Mengen

Zwei endliche Mengen gelten als „gleich groß“,
wenn sie die gleiche Anzahl von Elementen enthalten.

Zwei unendliche Mengen gelten als „gleich groß“,
wenn es zwischen ihnen eine bijektive Funktion gibt.

- Diese Definition verallgemeinert die für endliche Mengen:
  Sie ist also auch auf endliche Mengen anwendbar.
- Cantorsches Diagonalverfahren für Mengen,
  die gleichmächtig zu $\mathbb{N}$ sind (*abzählbar unendliche Mengen*)
- $\mathbb{Q}$ ist abzählbar, $\mathbb{R}$ nicht

2. Mengenlehre

2.4 Boolesche Algebren

Konzept 1: Aussagenlogische Formeln und ihre Operationen:

Aussagenlogische Formeln
haben die Operatoren ¬ (einstellig) und ∧ und ∨ (jeweils zweistellig)
und die Konstanten ⊥ und ⊤, die folgenden Regeln genügen:

$$p \wedge q = q \wedge p$$
$$p \vee q = q \vee p$$
Kommutativgesetze

$$p \wedge (q \wedge r) = (p \wedge q) \wedge r$$
$$p \vee (q \vee r) = (p \vee q) \vee r$$
Assoziativgesetze

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$$
Distributivgesetze

$$p \wedge p = p$$
$$p \vee p = p$$
Idempotenz

$$\neg(p \wedge q) = \neg p \vee \neg q$$
$$\neg(p \vee q) = \neg p \wedge \neg q$$
deMorgansche Regeln

$$\neg\neg p = p$$
Doppelte Negation (Involution)

$$p \vee \bot = p$$
$$p \wedge \top = p$$
Neutrale Elemente

$$p \wedge \bot = \bot$$
$$p \vee \top = \top$$
“Nullmultiplikation”

$$p \wedge \neg p = \bot$$
$$p \vee \neg p = \top$$
Inverses Element (Komplement)

2. Mengenlehre

2.4 Boolesche Algebren

Konzept 2: Mengen eines Ereignisraums Ω und ihre Operationen:

Mengen eines Ereignisraums Ω
haben die Operatoren ¯ (einstellig) und ∩ und ∪ (jeweils zweistellig)
und die Konstanten ∅ und Ω, die folgenden Regeln genügen:

$$\mathbf{p \cap q = q \cap p}$$
$$\mathbf{p \cup q = q \cup p}$$
Kommutativgesetze

$$\mathbf{p \cap (q \cap r) = (p \cap q) \cap r}$$
$$\mathbf{p \cup (q \cup r) = (p \cup q) \cup r}$$
Assoziativgesetze

$$\mathbf{p \cap (q \cup r) = (p \cap q) \cup (p \cap r)}$$
$$\mathbf{p \cup (q \cap r) = (p \cup q) \cap (p \cup r)}$$
Distributivgesetze

$$\mathbf{p \cap p = p}$$
$$\mathbf{p \cup p = p}$$
Idempotenz

$$\mathbf{\overline{(p \cap q)} = \overline{p} \cup \overline{q}}$$
$$\mathbf{\overline{(p \cup q)} = \overline{p} \cap \overline{q}}$$
deMorgansche Regeln

$$\mathbf{\overline{\overline{p}} = p}$$
Doppelte Negation (Involution)

$$\mathbf{p \cup \emptyset = p}$$
$$\mathbf{p \cap \Omega = p}$$
Neutrale Elemente

$$\mathbf{p \cap \emptyset = \emptyset}$$
$$\mathbf{p \cup \Omega = \Omega}$$
“Nullmultiplikation”

$$\mathbf{p \cap \overline{p} = \emptyset}$$
$$\mathbf{p \cup \overline{p} = \Omega}$$
Inverses Element (Komplement)

2. Mengenlehre

2.4 Boolesche Algebren

Formale Zusammenfassung dieser beiden Konzepte:

Eine **Boolesche Algebra** ist eine Menge $\mathscr{B}$ aus Elementen mit den Operatoren ~ (einstellig) und $\oplus$ und $\odot$ (jeweils zweistellig) und den Konstanten 0 und 1, die folgenden Regeln genügen:

$$\mathbf{p \odot q = q \odot p}$$
$$\mathbf{p \oplus q = q \oplus p}$$

Kommutativgesetze

$$\mathbf{p \odot (q \odot r) = (p \odot q) \odot r}$$
$$\mathbf{p \oplus (q \oplus r) = (p \oplus q) \oplus r}$$

Assoziativgesetze

$$\mathbf{p \odot (q \oplus r) = (p \odot q) \oplus (p \odot r)}$$
$$\mathbf{p \oplus (q \odot r) = (p \oplus q) \odot (p \oplus r)}$$

Distributivgesetze

$$\mathbf{p \odot p = p}$$
$$\mathbf{p \oplus p = p}$$

Idempotenz

$$\mathbf{\sim(p \odot q) = \sim p \oplus \sim q}$$
$$\mathbf{\sim(p \oplus q) = \sim p \odot \sim q}$$

deMorgansche Regeln

$$\mathbf{\sim\sim p = p}$$

Doppelte Negation (Involution)

$$\mathbf{p \oplus 0 = p}$$
$$\mathbf{p \odot 1 = p}$$

Neutrale Elemente

$$\mathbf{p \odot 0 = 0}$$
$$\mathbf{p \oplus 1 = 1}$$

“Nullmultiplikation”

$$\mathbf{p \odot \sim p = 0}$$
$$\mathbf{p \oplus \sim p = 1}$$

Inverses Element (Komplement)

2. Mengenlehre

2.4 Boolesche Algebren

Was bringt uns der Formalismus ?

Sehr viel: Boolesche Algebren fassen mehrere Konzepte zusammen, die wir bereits kennen !

➔ Einmal verstanden, mehrmals angewendet

➔ Sachverhalte, die aus den Eigenschaften einer Booleschen Algebra folgen, gelten für alle Mengen, die zum Konzept der Booleschen Algebra gehören.

Beispiele für solche Sachverhalte:

Normalformen (KNF, DNF)

Ordnungsrelationen

Auswertungsalgorithmen

Komplexitätsanalysen

2. Mengenlehre

2.4 Boolesche Algebren für Faule

Der Nachweis folgender Eigenschaften einer Booleschen Algebra reicht aus:

Eine **Boolesche Algebra** ist bereits durch eine Menge $\mathscr{B}$ aus Elementen mit den Operatoren ~ (einstellig) und $\oplus$ und $\odot$ (jeweils zweistellig) und den Konstanten 0 und 1 gegeben, die folgenden Regeln genügen:

$$\mathbf{p} \odot \mathbf{q} = \mathbf{q} \odot \mathbf{p}$$

$$\mathbf{p} \oplus \mathbf{q} = \mathbf{q} \oplus \mathbf{p}$$

Kommutativgesetze

$$\mathbf{p} \odot (\mathbf{q} \oplus \mathbf{r}) = (\mathbf{p} \odot \mathbf{q}) \oplus (\mathbf{p} \odot \mathbf{r})$$

$$\mathbf{p} \oplus (\mathbf{q} \odot \mathbf{r}) = (\mathbf{p} \oplus \mathbf{q}) \odot (\mathbf{p} \oplus \mathbf{r})$$

Distributivgesetze

$$\mathbf{p} \oplus 0 = \mathbf{p}$$

$$\mathbf{p} \odot 1 = \mathbf{p}$$

Neutrale Elemente

$$\mathbf{p} \odot \sim\mathbf{p} = 0$$

$$\mathbf{p} \oplus \sim\mathbf{p} = 1$$

Inverses Element (Komplement)

Das heißt:
Bei Erfüllung dieser 4 Grundgesetze sind die anderen Gesetze *Assoziativgesetze*, *deMorgansche Regeln*, *Idempotenz*, *Nullmultiplikation* und *doppelte Negation* automatisch erfüllt.

2. Mengenlehre

2.4 Boolesche Algebren: Weitere Beispiele

1. Schaltfunktionen-Algebra

$\mathcal{B} = \{f:\{0,1\}^n \rightarrow \{0,1\}\}$

$\sim f(x_1,\ldots,x_n) = 1 - f(x_1,\ldots,x_n)$

$(f \oplus g)(x_1,\ldots,x_n) = \max\,\{f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)\}$

$(f \odot g)(x_1,\ldots,x_n) = \min\,\{f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)\}$

Nullelement, Einselement ?

2. Teiler-Algebra

$\mathcal{B} = \{m \in \mathbb{N}$: m teilt n$\}$ für ein festes $n \in \mathbb{N}$

$\sim p = n / p$

$p \oplus q = \text{ggt}\,(p,q)$

$p \odot q = \text{kgv}\,(p,q)$

Nullelement, Einselement ?

3. Beweisverfahren

3.1 Kernstrukturen der Mathematik

- **Voraussetzungen: Axiome**

  Axiome sind Forderungen, die nicht bewiesen werden müssen.
  Sie sind implizite (d.h. häufig nicht erwähnte) Voraussetzungen vieler Aussagen.

- **Benennungen: Definitionen**

  Definitionen sind vereinfachende Schreibweisen. Sie sind keine Aussagen oder Axiome, d.h. weder zu fordern noch zu beweisen.

- **Aussagen: Satz, Lemma, Korollar**

  Sätze, Lemmata oder Korollare sind als Aussagen wahr oder falsch.
  Ob es sich bei einem Sachverhalt um eine Aussage handelt (und nicht um eine Definition oder ein Axiom), ist meistens leicht einzusehen.
  Schwieriger ist es zu beweisen, ob es sich um eine wahre Aussage handelt.

- **Beweise**

  Kette von logischen Schlussfolgerungen, um die Wahrheit einer Aussage, ausgehend von einer Behauptung (häufig in Form von Axiomen) zu belegen.

3. Beweisverfahren

3.1 Kernstrukturen der Mathematik

Das Axiomensystem von Peano für die natürlichen Zahlen:

Gegeben sei eine Menge $\mathbb{N}$ und eine Nachfolgerelation $\sigma \subset \mathbb{N} \times \mathbb{N}$

1) $0 \in \mathbb{N}$
2) Die Nachfolgerelation ist eine Funktion.
3) Die Nachfolgerelation ist injektiv.
4) 0 ist nicht Nachfolger einer natürlichen Zahl.
5) Mit einer endlich oft hintereinandergeschalteten Anwendung der Nachfolgefunktion auf 0 kann man *jedes* Element von $\mathbb{N}$ erzeugen.

Satz: Das Axiomensystem von Peano ist minimal.

Die Wegnahme eines einzigen Axioms lässt auch andere Strukturen zu,
welche alle anderen Axiome erfüllen, aber nicht als Repräsentation von $\mathbb{N}$ gewünscht sind.

3. Beweisverfahren

3.2 Vollständige Induktion

Die vollständige Induktion ist ein systematisches Beweisverfahren, welches in der Informatik häufige Verwendung findet.

Grundprinzip (einfachste Variante):

Zu beweisen ist eine Aussage der Form A(n) für ein beliebiges $n \in \mathbb{N}$

1) **Induktionsverankerung:** Beweise: Es gilt A (0)
2) **Induktionsschluss:** Beweise: Aus A (n) folgt A (n+1)

   Der Beweis soll die Gültigkeit für A (n) nicht zeigen, sondern voraussetzen.
   Zu zeigen ist nur die Gültigkeit von A (n+1).

   Der Induktionsschluss muss für wirklich alle n > 0 gelten (keine Einschränkungen!)

Beispiele: Eigene Übung macht den Meister !