Prof. Dr. Rolf Drechsler, drechsler@informatik.uni-bremen.de, MZH 4330
Christina Plump, cplump@uni-bremen.de, MZH 4206

7. Übungsblatt zur Vorlesung

# Technische Informatik 1

**Aufgabe 1** (4 + 3 Punkte)

a) Sei $\mathcal{B} = (M, \cdot, +, \overline{\phantom{x}})$ eine Boolesche Algebra. Zeigt durch ausschließliche Anwendung der in der Vorlesung vorgestellten Axiome (Kommutativität, Assoziativität, Distributivität, Absorption, Auslöschung), dass für $\mathcal{B}$ die folgenden Gesetze gelten:

   a) $\exists!\mathbf{0} \in M, \forall m \in M : m \cdot \mathbf{0} = \mathbf{0}$ und $m + \mathbf{0} = m$ sowie $\exists!\mathbf{1} \in M, \forall m \in M : m \cdot \mathbf{1} = m$ und $m + \mathbf{1} = \mathbf{1}$

   b) $\forall m \in M : \overline{\overline{m}} = m$

   c) $\forall m, n \in M \; : \; m \cdot n = \mathbf{0}$ und $m + n = \mathbf{1} \Rightarrow n = \overline{m}$

   Schreibweise 1: „$\exists!m \in M$“ heißt: „es gibt genau ein Element $m$ in der Menge $M$“

   Schreibweise 2: „$\forall m \in M$“ heißt: „für alle Elemente $m$ der Menge $M$“

   **Hinweis:** Man darf bei den Teilaufgaben b) und c) davon ausgehen, dass der Beweis in a) erbracht wurde.

b) Eine Menge $M$ zusammen mit einer zweistelligen Verknüpfung $\circ : M \times M \to M$ heißt *Gruppe*, wenn es ein Element $e \in M$ (*neutrales Element*) gibt mit den folgenden Eigenschaften:

$$\forall m \in M : m \circ e = m = e \circ m \tag{1}$$

$$\forall m \in M \; \exists m^{-1} \in M : m \circ m^{-1} = e = m^{-1} \circ m \tag{2}$$

   Man zeige, dass für jede Boolesche Algebra $\mathcal{B} = (M, \cdot, +, \overline{\phantom{x}})$ mit $\mathbf{0} \neq \mathbf{1}$ die Menge $M$ mit keiner der beiden Verknüpfungen $\cdot$ und $+$ eine Gruppe bildet.

**Aufgabe 2** (5 Punkte)

Zeigt oder widerlegt, dass das Tupel $(\mathcal{B}_n, \cdot, +, \overline{\phantom{x}})$ mit

$$\begin{array}{lcll}
\mathcal{B}_n & = & \{f \mid f : \mathbb{B}^n \to \mathbb{B}\} & (\textit{Boolesche Funktionen in } n \textit{ Variablen}) \\
\forall \alpha \in \mathbb{B}^n,\ f, g \in \mathcal{B}_n & : & (f \cdot g)(\alpha) = f(\alpha) \wedge g(\alpha) & (\textit{Konjunktion}) \\
\forall \alpha \in \mathbb{B}^n,\ f, g \in \mathcal{B}_n & : & (f + g)(\alpha) = f(\alpha) \vee g(\alpha) & (\textit{Disjunktion}) \\
\forall \alpha \in \mathbb{B}^n,\ f \in \mathcal{B}_n & : & f(\alpha) = 1 \iff \overline{f}(\alpha) = 0 & (\textit{Negation})
\end{array}$$

eine Boolesche Algebra ist.

**H**inweis: Es darf davon ausgegangen werden, dass $(\mathbb{B}, \wedge, \vee, \overline{\phantom{x}})$ eine Boolesche Algebra ist.

**Aufgabe 3** (1 + 1 Punkte)

Betrachtet die folgenden Mengen ($n, m \in \mathbb{N}_0$):

$$\mathcal{B}_n = \{f \mid f : \mathbb{B}^n \to \mathbb{B}\}$$
$$\mathcal{B}_{n,m} = \{f \mid f : \mathbb{B}^n \to \mathbb{B}^m\}$$

Berechnet die Kardinalität dieser Mengen, d. h. ermittelt:

a) $|\mathcal{B}_n|$

b) $|\mathcal{B}_{n,m}|$

**Aufgabe 4** (4 + 2 Punkte)

a) Zeigt, dass es für jede Boolesche Funktion $f \in \mathcal{B}_n$ eine *Ringsummendarstellung* gibt, die keine negativen Literale enthält. Beweist dazu folgende Aussage: Jede Funktion $f \in \mathcal{B}_n$ lässt sich darstellen als

$$f = \bigoplus_{i=1}^{m} x_{i_1} \dots x_{i_{l_i}}$$

mit

- $\forall 1 \leq i \leq m\colon (l_i = 1 \wedge x_{i_1} = 1) \vee \big(\forall 1 \leq j, k \leq l_i\colon x_{i_j} \in \{x_1, \dots, x_n\} \wedge (j \neq k \implies x_{i_j} \neq x_{i_k})\big)$, d. h. ein Monom ist entweder die Konstante 1 oder besteht vollständig aus positiven Literalen und kein Literal kommt zweimal in einem Monom vor,
- $x_{i_1} \dots x_{i_{l_i}} \neq x_{j_1} \dots x_{j_{l_j}}$ für $i \neq j$, d. h. jedes Monom darf maximal einmal auftreten.

b) Zeigt oder widerlegt: Die in obiger Gleichung angegebene Darstellung ist für jedes $f \in \mathcal{B}_n$ eindeutig (bis auf die Reihenfolge der Monome).

**Notation:** Analog zum Summensymbol ist $\oplus_{i=1}^{0}$ definiert als 0.

**Bemerkung:** Die Ringsummendarstellung ist auch bekannt unter dem Namen *Positive-Polarity-Reed-Muller*-Darstellung, die nach den amerikanischen Mathematikern Reed und Muller benannt ist. Zuvor in den 30er Jahren des 20. Jahrhunderts wurde diese Darstellung von dem russischen Mathematiker Zhegalkin beschrieben und entsprechend *Zhegalkin-Polynom* genannt.

**Zusatzaufgabe** (Einzelbearbeitung; bis zu 10 Bonuspunkte)

Die Ringsummendarstellung aus Aufgabe 5) wird „Positive Polarity Reed Muller“-Darstellung (PPRM) genannt, weil zu jeder Variable $x_i$ nur das *positive* Literal $x_i$, nicht aber das negative Literal $\overline{x}_i$ in der Darstellung einer Funktion vorkommt. Eine Erweiterung stellt die „Fixed Polarity Reed Muller“-Darstellung (FPRM) dar. Hierbei wird für jede Variable $x_i$ separat gewählt, ob jeweils *nur* das positive Literal $x_i$ oder *nur* das negative Literal $\overline{x}_i$ zur Darstellung verwendet wird, aber nicht beide.

a) Gib analog zur Definition eines Ausdrucks in PPRM-Darstellung in Aufgabe 5 a) eine Definition der FPRM-Darstellung an.

b) Gib einen Algorithmus zur Konvertierung eines FPRM-Ausdrucks in einen äquivalenten PPRM-Ausdruck an. Begründe dabei die Äquivalenz der Ein- und Ausgabe des Algorithmus.

c) Die Größe einer FPRM-Darstellung wird in der Anzahl der Monome gemessen (in der vorigen Aufgabe mit $m$ bezeichnet). Die Wahl der Polarität beeinflusst die Größe sehr stark (vgl. die Funktion $f = \overline{x}_1 \dots \overline{x}_n$ in PPRM-Darstellung). Gib einen Algorithmus zur optimalen Wahl der Polaritäten für eine beliebige Boolesche Funktion an.

d) Beschränkt man sich auf symmetrische Boolesche Funktionen, lässt sich die optimale Wahl in polynomial vielen Schritten (in Abhängigkeit von $n$) treffen. Gib einen entsprechenden Algorithmus an.

**Definition:** Eine Boolesche Funktion $f \in \mathcal{B}_n$ heißt genau dann *symmetrisch*, wenn man ein Tupel $v = (v_0, \ldots, v_n) \in \{0,1\}^{n+1}$ finden kann, so dass

$$\forall (\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n, i \in \{0,1,\ldots,n\} \colon \Big( |\{j \mid 1 \leq j \leq n, \alpha_j = 1\}| = i \Big) \implies f(\alpha_1, \ldots, \alpha_n) = v_i$$

Der Funktionswert einer symmetrischen Funktion ist also nur von der Anzahl der Einsen im Argument, nicht aber von deren Position abhängig.

**Abgabe:** Gebt Eure (individuelle) Lösung zu dieser Zusatzaufgabe bitte bis zum 29. Juni 2022 08:15 Uhr per Mail an Christina ab.

**Abgabe: bis Donnerstag, den 08.06.2023, 08:15 Uhr per e-Mail an den Tutor und Christina Plump mit folgendem Betreff: [TI-Abgabe] <Tutorium> - <Gruppe>: Blatt <Blatt>**