**Fachbereich Mathematik**
Prof. Dr. Ulrich Kohlenbach
Dr. Benno van den Berg

TECHNISCHE UNIVERSITÄT DARMSTADT

7. November, 2008

# 2. Übungsblatt Formale Grundlagen der Informatik I
WS 2008/2009

**(E2.1) [Funktionen]**

Wir definieren die Funktion $P : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ durch

$$P(x,y) = \max(x^2, y^2) + x + \begin{cases} 0 & \text{falls } x \leqslant y, \\ x - y & \text{falls } y < x. \end{cases}$$

Zeigen Sie, dass $P$ eine Bijektion ist.

Hinweis: Berechnen Sie die Einträge in der folgenden Tabelle.

| $P(x,y)$ | $x=0$ | $x=1$ | $x=2$ |
|---|---|---|---|
| $y=0$ | | | |
| $y=1$ | | | |
| $y=2$ | | | |

**Musterlösung.**

| $P(x,y)$ | $x=0$ | $x=1$ | $x=2$ |
|---|---|---|---|
| $y=0$ | 0 | 3 | 8 |
| $y=1$ | 1 | 2 | 7 |
| $y=2$ | 4 | 5 | 6 |

Jetzt folgt ein sehr formaler (und nicht so einfacher) Beweis für die Bijektivität von $P$.

Erst beweisen wir die Surjektivität. Sei $n \in \mathbb{N}$ gegeben. Wir suchen $(x,y)$ so, dass $P(x,y) = n$. Erst wählen wir $p \in \mathbb{N}$ so, dass $p^2 \leqslant n < (p+1)^2$. Sei

$$q = \frac{p^2 + (p+1)^2 - 1}{2} = p^2 + p.$$

Bemerke, dass auch $p^2 \leqslant q < (p+1)^2$. Jetzt gibt es zwei Möglichkeiten: $n \leqslant q$, und $n > q$.

**Fall 1:** $n \leqslant q$. Dann wählen wir $y = p, x = n - p^2$.

Es folgt, dass $x = n - p^2 \leqslant q - p^2 = p = y$, d.h. $x \leqslant y$. Daher $P(x,y) = y^2 + x = p^2 + n - p^2 = n$.

**Fall 2:** $n > q$. Dann wählen wir $x = p, y = p - (n - q)$.

Es folgt, dass $y = p - (n - q) < p = x$, d.h. $y < x$. Daher $P(x, y) = x^2 + x + (x - y) = p^2 + p + (n - q) = n$.

Jetzt die Injektivität: wir nehmen an, dass $P(x_0, y_0) = n$, und versuchen zu beweisen, dass $x_0 = x$ und $y_0 = y$, wobei $x$ and $y$ oben definiert sind. Seien auch $p$ und $q$ wie oben. Wir unterscheiden wieder zwei Fälle, aber jetzt $x_0 \leqslant y_0$ und $y_0 < x_0$.

**Fall 1:** $x_0 \leqslant y_0$. Jetzt gilt $n = P(x_0, y_0) = y_0^2 + x_0$. Daraus folgt $y_0^2 \leqslant n < (y_0 + 1)^2$ und $y_0 = p$. Dann haben wir $n = y_0^2 + x_0 \leqslant p^2 + p = q$, und deshalb $y = p = y_0$ und $x = n - p^2 = n - y_0^2 = x_0$.

**Fall 2:** $x_0 > y_0$. Jetzt gilt $n = P(x_0, y_0) = x_0^2 + x_0 + (x_0 - y_0)$. Daraus folgt $x_0^2 \leqslant n < (x_0 + 1)^2$ und $x_0 = p$. Dann haben wir $n = x_0^2 + x_0 + (x_0 - y_0) > p^2 + p = q$, und deshalb $x = p = x_0$ und $y = p - (n - q) = p - ((p^2 + p + (p - y_0)) - (p^2 + p)) = y_0$.

## (E2.2) [Äquivalenzrelationen]

Seien $f, g : \mathbb{N} \to \mathbb{N}$ Funktionen. Wir sagen „$f$ ist in $\mathcal{O}(g)$" (kurz „$f \in \mathcal{O}(g)$"), falls es Konstanten $K, n_0$ gibt, so dass

$$f(n) \leqslant K \cdot g(n) \text{ für alle } n \geqslant n_0.$$

Wir schreiben $f \sim g$, falls $f \in \mathcal{O}(g)$ und $g \in \mathcal{O}(f)$. $f \sim g$ besagt, dass $f$ und $g$ dieselbe Wachstumsrate haben.

Zeigen Sie, dass $f \sim g$ eine Äquivalenzrelation auf der Menge aller Funktionen $\mathbb{N} \to \mathbb{N}$ ist.

**Musterlösung.**

Wir bemerken zuerst, dass $f \in \mathcal{O}(f)$, weil wir einfach $K = 1$ und $n_0 = 0$ wählen können.

Weiter gilt, dass

$$f \in \mathcal{O}(g) \text{ und } g \in \mathcal{O}(h) \text{ impliziert } f \in \mathcal{O}(h). \tag{1}$$

Nehmen wir an, dass $f(n) \leqslant K_0 \cdot g(n)$ für alle $n \geqslant n_0$ und $g(n) \leqslant K_1 h(n)$ für alle $n \geqslant n_1$. Dann folgt, dass $f(n) \leqslant K_0 K_1 h(n)$ wenn $n \geqslant n_0$ und $n \geqslant n_1$, d.h., wenn $n \geqslant \max(n_0, n_1)$.

Jetzt beweisen wir, dass $f \sim g$ eine Äquivalenzrelation ist. Die Reflexivität $f \sim f$ ist klar, da $f \in \mathcal{O}(f)$; die Symmetrie is auch klar, weil $f \sim g$ heißt, dass $f \in \mathcal{O}(g)$ und $g \in \mathcal{O}(f)$, woraus folgt, dass $g \sim f$.

Um die Transitivität zu beweisen, nehmen wir an, dass $f \sim g$ und $g \sim h$. Daraus folgt, dass $f \in \mathcal{O}(g)$ und $g \in \mathcal{O}(h)$. Dann folgt mit (1), dass $f \in \mathcal{O}(h)$. Analog beweist man $h \in \mathcal{O}(f)$.

## (E2.3) [Boolesche Algebren]

Sei $(B, 0, 1, +, \cdot, ')$ eine Boolesche Algebra. Zeigen Sie die folgende Regeln, wobei Sie nur die folgende Axiome verwenden:

**BA1:** $+$ und $\cdot$ sind assoziativ und kommutativ, d.h. für alle $x, y, z \in B$:

$$\begin{aligned} (x+y)+z = x+(y+z), &\quad x+y = y+x, \\ (x \cdot y) \cdot z = x \cdot (y \cdot z), &\quad x \cdot y = y \cdot x. \end{aligned}$$

**BA2:** $+$ und $\cdot$ sind distributiv, d.h. für alle $x, y, z \in B$:

$$x \cdot (y+z) = x \cdot y + x \cdot z, \quad x + (y \cdot z) = (x+y) \cdot (x+z).$$

**BA3:** 0 und 1 sind neutrale Elemente bzgl. $+$ und $\cdot$:

$$x + 0 = x, \quad x \cdot 1 = x \text{ für alle } x \in B.$$

**BA4:** Komplement: $0 \neq 1$ und $x \cdot x' = 0$ und $x + x' = 1$ für alle $x \in B$.

(i) $0 \cdot 0 = 0$,

(ii) $1 + 1 = 1$,

(iii) $x + x = x$,

(iv) $x \cdot x = x$,

(v) $x \cdot 0 = 0$,

(vi) $x + 1 = 1$,

(vii) $x + (x \cdot y) = x$,

(viii) $x \cdot (x + y) = x$.

**Musterlösung.**

(i)

$$\begin{aligned} 0 &= 0 \cdot 1 \\ &= 0 \cdot (1+0) \\ &= 0 \cdot 1 + 0 \cdot 0 \\ &= 0 + 0 \cdot 0 \\ &= 0 \cdot 0 + 0 \\ &= 0 \cdot 0. \end{aligned}$$

(ii) Analog zu (i):

$$\begin{aligned}1 &= 1+0\\ &= 1+(0\cdot 1)\\ &= (1+0)\cdot(1+1)\\ &= 1\cdot(1+1)\\ &= (1+1)\cdot 1\\ &= 1+1.\end{aligned}$$

(iii) $x+x = x\cdot 1 + x\cdot 1 = x\cdot(1+1) = x\cdot 1 = x$.

(iv) Analog zu (iii): $x\cdot x = (x+0)\cdot(x+0) = x+0\cdot 0 = x+0 = x$.

(v) $x\cdot 0 = x\cdot(x\cdot x') = (x\cdot x)\cdot x' = x\cdot x' = 0$.

(vi) Analog zu (v).

(vii) $x+(x\cdot y) = x\cdot 1 + x\cdot y = x\cdot(1+y) = x\cdot(y+1) = x\cdot 1 = x$.

(viii) Analog zu (vii).

**(E2.4) [Boolesche Algebren]**

Seien $(B,0,1,+,\cdot,')$ und $(\overline{B},\overline{0},\overline{1},\overline{+},\bar{\cdot},\bar{'})$ zwei Boolesche Algebren, und sei $f: B\to\overline{B}$ eine Funktion.

Zeigen Sie, dass die folgende Aussagen äquivalent sind:

(i) $f$ ist ein Homomorphismus.

(ii) $f(x') = f(x)^{\bar{'}}$ und $f(x+y) = f(x)\overline{+}f(y)$ für alle $x,y\in B$.

Hinweis: Sie dürfen verwenden, dass in jeder Booleschen Algebra gilt:

$$x\cdot y = (x'+y')'.$$

**Musterlösung.**

Die Definition sagt, dass $f$ ein Homomorphismus ist, genau dann wenn

$$\begin{array}{rrcl} 1. & f(x+y) & = & f(x)\overline{+}f(y)\\ 2. & f(x\cdot y) & = & f(x)\bar{\cdot}f(y)\\ 3. & f(x') & = & f(x)^{\bar{'}}\\ 4. & f(0) & = & \overline{0}\\ 5. & f(1) & = & \overline{1}\end{array}$$

(i) $\Rightarrow$ (ii) folgt unmittelbar aus der Definition.

Wir beweisen jetzt (ii) $\Rightarrow$ (i). (1) und (3) sind gegeben, also brauchen wir nur noch (2), (4) und (5) zu beweisen.

Für (2), verwenden wir den Hinweis:

$$f(x \cdot y) = f((x' + y')') = f(x' + y')^{\bar{\prime}} = (f(x') \mathbin{\overline{+}} f(y'))^{\bar{\prime}} = (f(x)^{\bar{\prime}} \mathbin{\overline{+}} f(y)^{\bar{\prime}})^{\bar{\prime}} = f(x) \mathbin{\bar{\cdot}} f(y).$$

(4) kann man wie folgt beweisen:

$$f(0) = f(0 \cdot 0') = f(0) \mathbin{\bar{\cdot}} f(0') = f(0) \mathbin{\bar{\cdot}} f(0)^{\bar{\prime}} = \bar{0},$$

und (5) geht analog.