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

TECHNISCHE UNIVERSITÄT DARMSTADT

10. November, 2008

1. Hausaufgabe Formale Grundlagen der Informatik I
WS 2008/2009

Abgabe: Fr 21. November, in der Übung

Geben Sie bitte ihren Namen und die Nummer ihrer Übungsgruppe an.

(H1.1) [Äquivalenzrelationen]

Sei $\Sigma = \{a, b, c\}$ und sei Σ^* die Menge der Wörter über diesem Alphabet.

(i) Überprüfen Sie, ob die folgenden Relationen Äquivalenzrelationen auf Σ^+ sind.

$$\begin{array}{lcl} x \sim y & \Leftrightarrow & x \text{ und } y \text{ haben ein nicht-leeres Teilword gemeinsam} \\ x \sim y & \Leftrightarrow & x \text{ und } y \text{ haben ein nicht-leeres Anfangsstück gemeinsam} \\ x \sim y & \Leftrightarrow & x \text{ und } y \text{ haben gleichviel } a\text{'s} \end{array}$$

(ii) Zeigen Sie, dass die folgende Relation auf $\mathbb{N}_{>0} \times \mathbb{N}_{>0}$ eine Äquivalenzrelation ist:

$$(k, l) \sim (m, n) \Leftrightarrow kn = ml.$$

Musterlösung.

(i) Die erste Relation ist nicht transitiv (z.B. $a \sim ab$ und $ab \sim b$. aber nicht $a \sim b$), also keine Äquivalenzrelation.

Die zweite Relation ist eine Äquivalenzrelation (hier gilt $x \sim y$ genau dann wenn x und y denselben Anfangsbuchstabe haben).

Die dritte Relation ist auch eine Äquivalenzrelation.

(ii) Reflexivität: $(k, l) \sim (k, l)$, weil $kl = kl$.

Symmetrie: $(k, l) \sim (m, n) \Rightarrow kn = ml \Rightarrow ml = kn \Rightarrow (m, n) \sim (k, l)$.

Transitivität: $(k, l) \sim (m, n)$ und $(m, n) \sim (p, q) \Rightarrow kn = ml$ und $mq = pn \Rightarrow kq = knn^{-1}q = mln^{-1}q = mqn^{-1}l = pnn^{-1}l = pl \Rightarrow (k, l) \sim (p, q)$.

(Oder man bemerkt, dass $(k, l) \sim (m, n)$ gdw. $\frac{k}{l} = \frac{m}{n}$).

(H1.2) [Isomorphie]

In dieser Aufgabe betrachten wir gerichtete Graphen. Ein gerichteter Graph $\mathcal{G} = (G, E)$ besteht aus einer endlichen Menge G von Knoten und einer Teilmenge $E \subseteq G \times G$ von Kanten. Ein Beispiel:

$$\begin{tikzcd} a \arrow[r] \arrow[d] & b \arrow[d] \\ c \arrow[ur] & d \arrow[loop right] \end{tikzcd}$$

$$\begin{aligned} G &= \{a, b, c, d\} \\ E &= \{(a, b), (a, c), (b, d), (c, b), (d, d)\} \end{aligned}$$

(i) Finden Sie zwei Graphen $\mathcal{G}_1$ und $\mathcal{G}_2$, so dass es einen bijektiven Homomorphismus $f : \mathcal{G}_1 \to \mathcal{G}_2$ gibt, ohne dass $\mathcal{G}_1$ und $\mathcal{G}_2$ isomorph sind.

(ii) Kann es zwei Graphen $\mathcal{G}_1$ und $\mathcal{G}_2$ geben, so dass es bijektive Homomorphismen $f : \mathcal{G}_1 \to \mathcal{G}_2$ und $g : \mathcal{G}_2 \to \mathcal{G}_1$ gibt, ohne dass $\mathcal{G}_1$ und $\mathcal{G}_2$ isomorph sind? Begründen Sie Ihre Antwort!

Musterlösung.

(i) Das einfachste Gegenbeispiel ist folgendes: sei $\mathcal{G}_1$ ein Graph mit einem Knoten und keiner Kante, und $\mathcal{G}_2$ ein Graph mit einem Knoten und einem Loop. Ein Homomorphismus von Graphen $f : \mathcal{G}_2 \to \mathcal{G}_1$ hat die Eigenschaft, dass wenn a und b Knoten in $\mathcal{G}_2$ sind die durch eine Kante verbunden sind, die Knoten $f(a)$ und $f(b)$ in $\mathcal{G}_1$ auch verbunden sein müssen. Deshalb kann es keinen Homomorphismus $\mathcal{G}_2 \to \mathcal{G}_1$ geben und sind $\mathcal{G}_1$ und $\mathcal{G}_2$ nicht isomorph.

(ii) Nein! Ein bijektiver Homomorphismus $f : \mathcal{G}_1 \to \mathcal{G}_2$ bildet die Kanten in $\mathcal{G}_1$ injektiv auf die Kanten in $\mathcal{G}_2$ ab. Wenn es also einen bijektiven Homomorphismus $f : \mathcal{G}_1 \to \mathcal{G}_2$ gibt, hat $\mathcal{G}_1$ nicht mehr Kanten als $\mathcal{G}_2$. Gibt es bijektiven Homomorphismen $f : \mathcal{G}_1 \to \mathcal{G}_2$ und $g : \mathcal{G}_2 \to \mathcal{G}_1$, dann haben $\mathcal{G}_1$ und $\mathcal{G}_2$ gleichviel Kanten. Also bildet f die Kanten in $\mathcal{G}_1$ *bijektiv* auf die Kanten in $\mathcal{G}_2$ ab. (Hier verwenden wir das Schubfachprinzip: eine injektive Abbilding $f : A \to B$ zwischen endlichen Mengen A und B die gleichviel Elementen haben ist auch bijektiv.) Deshalb ist auch f^{-1} ein Homomorphismus und sind $\mathcal{G}_1$ und $\mathcal{G}_2$ isomorph.

(H1.3) [Aussagenlogik]

(i) Geben Sie eine binäre Wahrheitsfunktion $\Box : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ an, so dass sowohl $\neg$ als auch $\wedge$ sich aus $\Box$ definieren lassen. Geben Sie diese Definitionen explizit an und definieren Sie auch $\vee, \to$ mit Hilfe von $\Box$.

(ii) Wir legen $n+1$ Bücher in n Schubfächer. Seien p_{ij} $(1 \leqslant i \leqslant n+1, 1 \leqslant j \leqslant n)$ aussagenlogische Variablen, die ausdrücken, dass das i-te Buch sich im j-ten Schubfach befindet. Schreiben Sie das Schubfachprinzip

> ,,Wenn jedes Buch in ein Schubfach gelegt wird, dann gibt es ein Schubfach, das mehr als ein Buch enthält."

formal auf, wobei Sie nur die aussagenlogischen Variablen p_{ij} und aussagenlogische Operatoren verwenden.

Musterlösung.

(i) Es gibt genau zwei mögliche Lösungen, den Sheffer stroke | (NAND) und den Quine dagger † (NOR).

$$\begin{array}{c|cc} | & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \dagger & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 0 \end{array}$$

Die übliche Operatoren lassen sich dann wie folgt definieren:

$$\begin{array}{ccc} \neg p & p|p & p \dagger p \\ p \wedge q & \neg(p|q) & \neg p \dagger \neg q \\ p \vee q & \neg p|\neg q & \neg(p \dagger q) \\ p \rightarrow q & p|\neg q & \neg(\neg p \dagger q) \end{array}$$

(ii)

$$\bigwedge_i \Big(\bigvee_j p_{ij} \wedge \bigwedge_{j \neq j'} \neg(p_{ij} \wedge p_{ij'})\Big) \rightarrow \bigvee_j \bigvee_{i \neq i'} (p_{ij} \wedge p_{i'j})$$

(H1.4) [Induktion]

(i) Sei $A(n)$ eine bestimmte Eigenschaft der natürlichen Zahlen. Beweisen Sie durch Wertverlaufsinduktions, dass

$$(\exists n \in \mathbb{N})\, A(n) \rightarrow (\exists n \in \mathbb{N})\, [\, A(n) \wedge (\forall k < n)\, \neg A(k)\,].$$

(ii) Sei $f : \mathbb{N} \rightarrow \mathbb{N}$ eine Funktion. Beweisen Sie, dass

$$(\exists n \in \mathbb{N})\, (\forall m \in \mathbb{N})\, [f(n) \leqslant f(m)].$$

Musterlösung.

(i) Nehmen wir an, die Aussage sei falsch. Dann gibt es eine bestimmte Eigenschaft $A(n)$, so dass

(1) $(\exists n \in \mathbb{N})\, A(n)$, aber

(2) $\neg(\exists n \in \mathbb{N})\, [\, A(n) \wedge (\forall k < n)\, \neg A(k)\,]$.

Durch logische Umformungen bekommt man die zu (2) äquivalente Aussage:

$$
\begin{aligned}
\neg(\exists n \in \mathbb{N})\, [\, A(n) \wedge (\forall k < n)\, \neg A(k)\,] \quad &\leftrightarrow \quad (\forall n \in \mathbb{N})\, \neg[\, A(n) \wedge (\forall k < n)\, \neg A(k)\,] \\
&\leftrightarrow \quad (\forall n \in \mathbb{N})\, [\, \neg A(n) \vee \neg(\forall k < n)\, \neg A(k)\,] \\
&\leftrightarrow \quad (\forall n \in \mathbb{N})\, [\, (\forall k < n)\, \neg A(k) \rightarrow \neg A(n)\,]
\end{aligned}
$$

Mit Wertverlaufsinduktion folgt jetzt $(\forall n \in \mathbb{N}) \neg A(n)$, was (1) widerspricht.

(ii) Sei jetzt $A(n) := (\exists m \in \mathbb{N})\, f(m) = n$. Offensichtlich gilt $(\exists n \in \mathbb{N})\, A(n)$ (z.B. ist $A(f(0))$ wahr). Deshalb folgt mit (i), dass ein $l \in \mathbb{N}$ existiert, so dass $A(l)$ gilt, aber $A(k)$ nicht, falls $k < l$. Aus $A(l)$ folgt, dass ein $n \in \mathbb{N}$ existiert mit $f(n) = l$. So ein n hat die gewünschte Eigenschaft: wäre $f(m)$ nämlich kleiner als $f(n) = l$ für ein bestimmtes m, dann würde für $k = f(m) < l$ die Aussage $A(k)$ gelten, was aber nicht sein kann. Also ist die Aussage bewiesen.