ETH Zürich, D-INFK
HS 2016, 29. September 2016

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik

Lösung 3

Teil 1: Prädikatenlogik

3.1 Quantoren und Prädikate

a)

i) $\forall m\, \forall n\, \big(0 < m \cdot n \rightarrow (0 < m \vee 0 < n)\big)$ *(2 Punkte)*
Diese Aussage ist falsch, da zum Beispiel $(-2) \cdot (-2) = 4$.

ii) $\forall m\, \exists n\, (m + n = 0)$ *(2 Punkte)*
Diese Aussage ist wahr für das Universum der ganzen Zahlen. Für das Universum der natürlichen Zahlen wäre die Aussage falsch.

iii) $\forall n\, \big(((\exists k\, n = 2 \cdot k) \wedge 2 < n) \rightarrow \exists p\, \exists q\, (\mathtt{prime}(p) \wedge \mathtt{prime}(q) \wedge n = p + q)\big)$ *(2 Punkte)*
Hierbei handelt es sich um die (starke) Goldbachsche Vermutung. Es ist nicht bekannt, ob die Aussage wahr oder falsch ist.

b) Es gibt mehrere Möglichkeiten, die Aussagen in Worte zu fassen. Zum Beispiel:

i) „Für jede ganze Zahl x gibt es eine ganze Zahl y so dass das Produkt xy gleich 1 ist.“ *(1 Punkt)*
oder kurz
„Jede ganze Zahl hat ein multiplikatives Inverses.“
Die Aussage ist falsch, da zum Beispiel 23 kein ganzzahliges multiplikatives Inverses hat. *(1 Punkt)*

ii) „Es gibt eine ganze Zahl x, so dass für jede ganze Zahl y das Produkt xy ungleich 1 ist und so dass es eine ganze positive Zahl gibt.“ *(1 Punkt)*
Die Aussage ist wahr, da für $x = 0$ und beliebiges y gilt, dass das Produkt $xy \neq 1$ ist und da 42 eine positive Zahl ist. *(1 Punkt)*
Vorsicht, die folgende Interpretation ist falsch (Warum?):
„Es gibt eine ganze Zahl x, so dass für jede ganze Zahl y das Produkt xy ungleich 1 ist und y positiv ist.“

3.2 Vertauschung von Quantoren

a) Nehmen wir an, $\exists y\, \forall x\, P(x, y)$ gilt. Nach Definition von $\exists$ existiert dann ein y, sodass $\forall x\, P(x, y)$ wahr ist. Sei y_0 ein solches y. Nach Definition von $\forall$ bedeutet dies, dass

$P(x, y_0)$ für alle x wahr ist. $\exists y\ P(x, y)$ gilt also auch für alle x, denn wir können stets y_0 als y wählen. Wenden wir erneut die Definition von $\forall$ an, erhalten wir $\forall x\ \exists y\ P(x, y)$.

b) Wir geben ein Gegenbeispiel an: Betrachte das Universum der natürlichen Zahlen und sei P das Prädikat `less`. Es gilt dann $\forall x\ \exists y \quad x < y$, aber $\exists y\ \forall x \quad x < y$ ist falsch.

3.3 Gewinnstrategie

a) Wir bemerken, dass die Zahlen von Alice nicht von b_1 und b_2 abhängig sein können. Die Aussage kann daher wie folgt als Formel geschrieben werden:

$$\exists a_1 \exists a_2 \forall b_1 \forall b_2 \ \ a_1 + (a_2 + b_1)^{|b_2|+1} = 1.$$

Diese Aussage ist falsch, denn für jedes Tupel (a_1, a_2) existiert das Tupel $(b_1, b_2) := (2 - a_2 - a_1, 0)$, so dass

$$a_1 + (a_2 + b_1)^{|b_2|+1} = a_1 + (a_2 + 2 - a_2 - a_1) = 2.$$

Somit gibt es keine Gewinnstrategie für Alice.

b) In diesem Fall kann Alice a_2 abhängig von b_1 wählen. Die Aussage kann wie folgt als Formel geschrieben werden:

$$\exists a_1 \forall b_1 \exists a_2 \forall b_2 \ \ a_1 + (a_2 + b_1)^{|b_2|+1} = 1.$$

Diese Aussage ist wahr, denn für $a_1 = 1$ und $a_2 = -b_1$ gilt

$$a_1 + (a_2 + b_1)^{|b_2|+1} = 1 + 0^{|b_2|+1} = 1.$$

Es gibt also eine Gewinnstrategie für Alice.

Teil 2: Beweistechniken

3.4 Direkter Beweis (2.4.3)

a) Seien n und m beliebige gerade natürliche Zahlen. Es gibt also natürliche Zahlen a und b, so dass $n = 2a$ und $m = 2b$. Wir erhalten $nm = (2a)(2b) = 4ab = 2(2ab)$. Das Produkt ist somit gerade, da es für die natürliche Zahl $c = 2ab$ die Form $nm = 2c$ hat.

Ausführliche Lösung:
Wir betrachten zwei Aussagen S und T und wollen zeigen, dass $S \implies T$ gilt. Bei einem direkten Beweis nehmen wir an, dass S wahr ist, und zeigen, dass dann T wahr ist.

Aussage S: n und m sind gerade natürliche Zahlen.

Aussage T: nm ist eine gerade Zahl.

Direkter Beweis:
n und m sind gerade natürliche Zahlen.
$\Rightarrow$ Es gibt natürliche Zahlen a und b, so dass $n = 2a$ und $m = 2b$.
$\Rightarrow$ Es gilt $nm = (2a)(2b) = 4ab = 2(2ab)$.
$\Rightarrow$ Es gibt eine natürliche Zahl c, so dass $nm = 2c$.
$\Rightarrow$ nm ist eine gerade Zahl.

3.5 Indirekter Beweis (2.4.4)

a) Wir nehmen an, dass n gerade ist und zeigen, dass dann $42^n - 1$ keine Primzahl ist. Falls n gerade ist, gibt es ein $k > 0$ mit $n = 2k$. Es folgt, dass $42^n - 1 = 42^{2k} - 1 = (42^k + 1)(42^k - 1)$. Da dies eine nicht trivial Faktorisierung ist, kann $42^n - 1$ keine Primzahl sein.

Ausführliche Lösung:
Wir betrachten zwei Aussagen S und T und wollen zeigen, dass $S \implies T$ gilt. Bei einem indirekten Beweis nehmen wir an, dass T falsch ist, und zeigen, dass dann auch S falsch ist.

Aussage S: $42^n - 1$ ist prim.

Aussage T: n ist ungerade.

Indirekter Beweis:
n ist nicht ungerade.
$\Rightarrow$ n ist gerade.
$\Rightarrow$ Es gibt ein $k > 0$ mit $n = 2k$.
$\Rightarrow$ Es gilt $42^n - 1 = 42^{2k} - 1 = (42^k + 1)(42^k - 1)$.
$\Rightarrow$ Es gibt eine nicht triviale Faktorisierung von $42^n - 1$.
$\Rightarrow$ $42^n - 1$ ist nicht prim.

b) Sei n gerade. Damit folgt mit Teilaufgabe **3.4a)**, dass auch $n \cdot n = n^2$ gerade ist.

3.6 Fallunterscheidung (2.4.7)

a) Wir unterscheiden zwei Fälle :

n **gerade:** Falls n gerade ist, so sind auch $5n^2$ und $3n$ gerade. Da die Summe gerader Zahlen gerade ist, ist auch $5n^2+3n+8$ gerade und die Behauptung gilt in diesem Fall.

n **ungerade:** Falls n ungerade ist, sind $5n^2$ und $3n$ ungerade. $5n^2 + 3n$ ist gerade, da die Summe zweier ungerader Zahlen immer gerade ist. Daher ist $5n^2 + 3n + 8$ gerade und die Behauptung gilt auch in diesem Fall.

Da diese Fälle alle ganzen Zahlen abdecken, gilt die Behauptung.

b) Wir bezeichnen im Folgenden mit $R_3(x)$ den Rest der ganzzahligen Division von x geteilt durch 3 (z.B. $R_3(5) = 2$). Für eine Primzahl p können wir nun drei Fälle betrachten:

Für $p = 2$ ist $p^2 + 2 = 6$ und somit nicht prim. Die Aussage stimmt also für $p = 2$.

Für $p = 3$ ist $p^2 + 2 = 11$ prim, aber auch $p^3 + 2 = 29$ ist prim. Die Aussage stimmt also für $p = 3$.

Für $p > 3$ ist $R_3(p) \in \{1, 2\}$, da 3 nicht p teilt. Damit gilt

$$R_3(p^2) = R_3(R_3(p) \cdot R_3(p)) = 1.$$

Es folgt

$$R_3(p^2 + 2) = R_3(R_3(p^2) + R_3(2)) = R_3(1 + 2) = 0$$

und somit muss 3 $p^2 + 2$ teilen. Für $p > 3$ ist $p^2 + 2$ daher nicht prim und die Aussage folgt auch für solche p.