Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Übungsblatt 6

Aufgabe 1
Zeigen Sie, dass die Menge der natürlichen Zahlen nicht in der reellen Arithmetik definierbar ist (ohne zu verwenden, dass $\mathrm{Th}(\mathbb{N}, +, \cdot)$ unentscheidbar ist).

Lösung
Angenommen die Formel F mit einer freien Variable x definiert $\mathbb{N}$ in $(\mathbb{R}, +, \cdot, <, 0, 1, -1)$, d.h. $(\mathbb{R}, +, \cdot, <, 0, 1, -1) \models F[n/x]$ genau dann wenn $n \in \mathbb{N}$. Durch Quantorenelimination kann man F in eine äquivalente quantorenfreie Formel F' umwandeln. Wir können annehmen, dass F' die Form

$$(s(x) = 0) \wedge \bigwedge_{i=1}^{m} (t_i(x) > 0)$$

hat, wobei $s, t_1, \ldots, t_m \in \mathbb{Z}[x]$ Polynome über $\mathbb{R}$ sind (in der Vorlesung wird dies für G in einer Formel $\exists x G$ angenommen). Sei $d(p)$ der Grad eines Polynoms p. Es gilt, dass $s(x) = 0$ entweder für alle reellen Zahlen gilt, wenn s das Nullpolynom ist, oder es gibt höchstens $d(s(x))$ viele Lösungen für $s(x) = 0$. Die Menge aller x mit $s(x) = 0$ ist also entweder ein Intervall über ganz $\mathbb{R}$ oder die Vereinigung aus $d(s(x))$ vielen einelementigen Intervallen. Analog gilt für jedes i ($1 \leq i \leq m$), dass man die Menge aller x mit $t_i(x) > 0$ ebenso als Vereinigung von höchstens $d(t_i(x))$ vielen Intervallen schreiben kann. Bool'sche Kombinationen (z.B. der Schnitt) von endlich vielen Intervallen über $\mathbb{R}$ lassen sich wieder mit Hilfe von endlich vielen Intervallen über $\mathbb{R}$ beschreiben. Falls also F die natürlichen Zahlen beschreibt, so müsste sich $\mathbb{N}$ durch endlich viele Intervalle über $\mathbb{R}$ beschreiben lassen, was ein Widerspruch ist.

Aufgabe 2
Zeigen Sie, dass $\mathrm{Th}(\mathbb{Z}, +, \cdot)$ unentscheidbar ist.
Hinweis: Verwenden Sie dazu den Satz von Lagrange: Jede natürliche Zahl lässt sich als Summe vierer Quadratzahlen schreiben.

Lösung
Im Gegensatz zur Arithmetik über $\mathbb{R}$ (siehe Aufgabe 1), lässt sich $\mathbb{N}$ mit Hilfe von $(\mathbb{Z}, +, \cdot)$ definieren: Sei N die folgende Formel mit der freien Variablen x:

$$N = \exists a \exists b \exists c \exists d (x = a \cdot a + b \cdot b + c \cdot c + d \cdot d)$$

Nach dem Satz von Lagrange gilt $(\mathbb{Z}, +, \cdot) \models N[z/x]$, wenn $z \in \mathbb{N}$. Da die negativen ganzen Zahlen $\mathbb{Z} \setminus \mathbb{N}$ sich nicht als Summe von Quadratzahlen schreiben lassen, gilt außerdem $(\mathbb{Z}, +, \cdot) \not\models N[z/x]$, wenn $z \in \mathbb{Z} \setminus \mathbb{N}$. Somit könnte man, wenn $\mathrm{Th}(\mathbb{Z}, +, \cdot)$ entscheidbar wäre, auch $\mathrm{Th}(\mathbb{N}, +, \cdot)$ entscheiden in dem man sich m.H. der Formel N auf die natürlichen Zahlen beschränkt. Wir wissen bereits, dass $\mathrm{Th}(\mathbb{N}, +, \cdot)$ unentscheidbar ist und somit muss auch $\mathrm{Th}(\mathbb{Z}, +, \cdot)$ unentscheidbar sein.