

Aufgabe 1: (Potenzrechnung) (3 Punkte)

Seien $a, b, c \in \mathbb{N}$. Verweise beziehen sich auf 2.1 - 2.3 und 3.3.

20. $(a^b)^c = a^{b \cdot c}$

(a) $c = 0$: $(a^b)^0 \stackrel{(12)}{=} 1 \stackrel{(12)}{=} a^0 \stackrel{(8)}{=} a^{b \cdot 0}$

(b) $c \rightarrow c + 1$: $(a^b)^{c+1} \stackrel{(13)}{=} (a^b)^c \cdot a^b \stackrel{IV}{=} a^{b \cdot c} \cdot a^b \stackrel{(18)}{=} a^{b \cdot c + b} \stackrel{(9)}{=} a^{b \cdot (c+1)}$

Aufgabe 2: (Zahlendarstellung 1) (6 Punkte)

Sei $a \in \{0, 1\}^m$; $m, n, i, j \in \mathbb{N}$; $m > n$. Beweise:

1. $\langle a, 0^i \rangle = \langle a \rangle \cdot 2^i$

$$\begin{aligned} \langle a[m-1:0], 0^i \rangle &= \sum_{k=i}^{i+m-1} a_{k-i} \cdot 2^k + \sum_{k=0}^{i-1} 0 \cdot 2^k \\ &= \sum_{k=0}^{m-1} a_k \cdot 2^{k+i} \\ &= 2^i \cdot \sum_{k=0}^{m-1} a_k \cdot 2^k \\ &= \langle a[m-1:0] \rangle \cdot 2^i \end{aligned}$$

2. $\langle 0^j, a \rangle = \langle a \rangle$

$$\begin{aligned} \langle 0^j, a[m-1:0] \rangle &= \sum_{k=m}^{j+m-1} 0 \cdot 2^k + \sum_{k=0}^{m-1} a_k \cdot 2^k \\ &= \langle a[m-1:0] \rangle \end{aligned}$$

3. $\langle a[m-1:0] \rangle \equiv \langle a[n-1:0] \rangle \pmod{2^n}$

$$\begin{aligned} &\langle a[m-1:0] \rangle \equiv \langle a[n-1:0] \rangle \pmod{2^n} \\ \Leftrightarrow &2^n \mid \langle a[m-1:0] \rangle - \langle a[n-1:0] \rangle \\ \Leftrightarrow &2^n \mid \sum_{k=0}^{m-1} a_k \cdot 2^k - \sum_{k=0}^{n-1} a_k \cdot 2^k \\ \Leftrightarrow &2^n \mid \sum_{k=n}^{m-1} a_k \cdot 2^k \\ \Leftrightarrow &2^n \mid \sum_{k=0}^{m-n-1} a_{n+i} \cdot 2^{n+i} \\ \Leftrightarrow &2^n \mid 2^n \cdot \sum_{k=0}^{m-n-1} a_{n+i} \cdot 2^i \end{aligned}$$

Aufgabe: (Modulorechnung 5) (6 Punkte)

Seien $a, x \in \mathbb{Z}$; $k \in \mathbb{N}$. Beweise:

Es existiert genau ein $x' \in \{a, \dots, a+k-1\}$ mit $x \equiv x' \pmod{k}$

1. Existenz

zu Zeigen: $\forall x' \in \mathbb{N} : \exists x' \in \{a, \dots, a+k-1\}, x \equiv x' \pmod{k}$

Zu jeder ganzen Zahl existiert eine eindeutige Zerlegung:

$$x - a = n \cdot k + m \quad \text{mit } m \in \{0, \dots, k-1\}$$

Sei $x' = a + m$, dann gilt:

$$\begin{aligned} k & \mid n \cdot k \\ \Leftrightarrow k & \mid (n \cdot k + m + a) - (a + n) \\ \Leftrightarrow k & \mid x - x' \\ \Leftrightarrow x & \equiv x' \pmod{k} \end{aligned}$$

2. Eindeutigkeit

Anname: $\exists x'' \in \{a, \dots, a+k-1\}, x'' \equiv x \pmod{k}, x'' \neq x'$

$$\begin{aligned} x' & \equiv x \equiv x'' \pmod{k} \\ \Rightarrow x' & \equiv x'' \pmod{k} \\ \Leftrightarrow k & \mid x' - x'' \\ \Leftrightarrow \exists q \in \mathbb{Z} - \{0\} : k \cdot -q & = x' - x'' \\ \Leftrightarrow \exists q \in \mathbb{Z} - \{0\} : x'' & = x' + k \cdot q \\ \Rightarrow x'' & \leq x' - k \vee x'' \geq x' + k \\ \Rightarrow x'' & \leq a + k - 1 - k \vee x'' \geq a + k \\ \Rightarrow x'' & \leq a - 1 \vee x'' \geq a + k \\ \Rightarrow x'' & \notin \{a, \dots, a+k-1\} \end{aligned}$$

Aufgabe 6: (Zahlendarstellung 2) (6 Punkte)

Sei $a \in \{0, 1\}^n$.

1. Hilfsbehauptung: Die Abbildung

$$\langle \rangle : \{0, 1\}^n \rightarrow \{-2^{n-1}, \dots, 2^{n-1} - 1\}; \langle a \rangle := \sum_{i=0}^{n-1} a_i 2^i$$

ist injektiv.

Seien $a, b \in \{0, 1\}^n$ und $a \neq b$.

Sei $k = \max\{i \mid a_i \neq b_i\}$ und oBdA. $a_k < b_k$.

$$a_k < b_k \Rightarrow a_k = 0 \wedge b_k = 1$$

Damit:

$$\begin{aligned}
\langle a \rangle - \langle b \rangle &= \sum_{i=0}^{n-1} a_i 2^i - \sum_{i=0}^{n-1} b_i 2^i \\
&= \sum_{i=k+1}^{n-1} a_i 2^i + a_k 2^k + \sum_{i=0}^{k-1} a_i 2^i \\
&\quad - \left(\sum_{i=k+1}^{n-1} b_i 2^i + b_k 2^k + \sum_{i=0}^{k-1} b_i 2^i \right) \\
&= \sum_{i=k+1}^{n-1} a_i 2^i - \sum_{i=k+1}^{n-1} b_i 2^i + a_k 2^k - b_k 2^k + \sum_{i=0}^{k-1} a_i 2^i - \sum_{i=0}^{k-1} b_i 2^i \\
&= 0 \cdot 2^k - 1 \cdot 2^k + \sum_{i=0}^{k-1} a_i 2^i - \sum_{i=0}^{k-1} b_i 2^i \\
&< 0
\end{aligned}$$

2. Beweise: Die Abbildung

$[] : \{0, 1\}^n \rightarrow \{-2^{n-1}, \dots, 2^{n-1} - 1\}$; $[a] := -a_{n-1} \cdot 2^{n-1} + \langle a[n-2 : 0] \rangle$
ist bijektiv.

(a) Injektivität

Seien $a, b \in \{0, 1\}^n$ und $a \neq b$.

i. $a_{n-1} = b_{n-1}$

$$\begin{aligned}
&a[n-2 : 0] \neq b[n-2 : 0] \\
\Rightarrow &\langle a[n-2 : 0] \rangle \neq \langle b[n-2 : 0] \rangle \\
\Rightarrow &-2^{n-1} a_{n-1} + \langle a[n-2 : 0] \rangle \neq -2^{n-1} b_{n-1} + \langle b[n-2 : 0] \rangle \\
\Rightarrow &[a] \neq [b]
\end{aligned}$$

ii. $a_{n-1} \neq b_{n-1}$, oBdA sei $a_{n-1} < b_{n-1}$

$$\begin{aligned}
&\langle a[n-2 : 0] \rangle \geq 0 \wedge \langle b[n-2 : 0] \rangle < 2^{n-1} \\
\Rightarrow &-2^{n-1} a_{n-1} + \langle a[n-2 : 0] \rangle \geq 0 > -2^{n-1} b_{n-1} + \langle b[n-2 : 0] \rangle \\
\Rightarrow &[a] \neq [b]
\end{aligned}$$

(b) Surjektivität

Da $\#(\{0, 1\}^n) = 2^n = \# \{-2^{n-1}, \dots, 2^{n-1} - 1\}$ und da $[]$ injektiv ist, ist $[]$ surjektiv.

Damit ist gezeigt, daß $[]$ bijektiv ist.