Grundlagen der Programmierung

SS 05
Prof. Dr. K. Madlener
Lösungshinweise zu Übungsblatt 1

Aufgabe 1.1. Klar: $f(X \cap Y) \subseteq f(X) \cap f(Y)$.
Sei f injektiv. Seien weiter $X, Y \subseteq A$ und $z \in f(X) \cap f(Y)$. Es gibt also $x \in X$ mit $f(x) = z$ und $y \in Y$ mit $f(y) = z$. f injektiv $\rightsquigarrow$ aus $f(x) = z = f(y)$ folgt $x = y$. Also $x = y \in X \cap Y$ und $z = f(x) \in f(X \cap Y)$. Daher auch $f(X) \cap f(Y) \subseteq f(X \cap Y)$ und somit $f(X) \cap f(Y) = f(X \cap Y)$.
Sei umgekehrt $x, y \in A$ mit $f(x) = f(y)$. Sei $X = \{x\}$ und $Y = \{y\}$. Es gilt $f(x) = f(y) \in f(X) \cap f(Y) = f(X \cap Y)$. Also ist $f(X \cap Y) \neq \emptyset$ und so auch $X \cap Y \neq \emptyset$. Es folgt $x = y$.

Aufgabe 1.2. Seien E und F nicht-leere endliche Mengen. Wir treffen folgende Vereinbarung: $[n] := \{1, \ldots, n\}$.

(1) Seien $f : E \to [n]$ und $g : F \to [p]$ Bijektionen. Dann ist auch $h : E \cup F \to [n+p]$ mit $h(x) = f(x)$ für alle $x \in E$ und $h(x) = g(x) + n$ für alle $x \in F$ eine Bijektion.
$\rightsquigarrow |E \cup F| = n + p = |E| + |F|$.
$h(x)$ ist Bijektion weil sie eine Inverse $h^{-1}(x) : [n+p] \to E \cup F$ hat.
$h^{-1}(k) = \begin{cases} f^{-1}(k), & \text{wenn } k \leq n \\ g^{-1}(k-n), & \text{wenn } n < k \leq n+p \end{cases}$

(2) Seien $f : E \to [n]$ und $g : F \to [p]$ Bijektionen und $h : E \times F \to [n \cdot p]$ definiert durch $h(x, y) = p \cdot (f(x) - 1) + g(y)$ für alle $(x, y) \in E \times F$. Dann ist h Bijektion und $|E \times F| = |E| \cdot |F|$. Die Inverse von $h(x, y)$ ist

$$h^{-1}(k) = \big(f^{-1}(1 + \lfloor\frac{k-1}{p}\rfloor), g^{-1}(1 + (k-1) \mod p)\big)$$

mit $(k-1) \mod p$ der Rest der Division $(k-1)/p$.

(3) Mit der Darstellung $E = \{1, ..., n\}$ und $F = \{1, ..., p\}$ können wir die Funktionen von E nach F bzgl. der Basis p aufzählen, wir beginnen mit $\{(1,1), (2,1), \ldots, (n,1)\}$, $\{(1,1), (2,1), \ldots, (n,2)\}$, bis wir $\{(1,p), (2,p), ...(n,p)\}$ erreicht haben. Es gibt p^n viele Funktionen.
Die Bijektion $h : F^E \to [p^n]$ liefert für eine Funktion $s : E \to F$

$$h(s) = 1 + \sum_{k=1}^{n} p^{n-k} \cdot (s(k) - 1)$$

und die Inverse $h^{-1}(k)$ liefert eine Funktion, die für i $(1 \leq i \leq n)$ wie folgt definiert ist:

$$h^{-1}(k)(i) = 1 + \lfloor\frac{k-1}{p^{n-i}}\rfloor \mod p$$

.

(4) Die Abbildung, die mit jeder Teilmenge $A \subseteq E$ ihre charakteristische Funktion χ_A assoziiert, ist eine Bijektion.

$\rightsquigarrow |\mathcal{P}(E)| = |\{0,1\}^E| = 2^{|E|}$ (mit (3).

Oder so: Induktion über $|E| =: n$.

$n = 0$: $E = \emptyset$. $\mathcal{P}(E) = \{\emptyset\}$. $|\mathcal{P}(E)| = 1 = 2^0 = 2^{|E|}$.

$n \to n+1$: Sei $E = \{a_1, \ldots, a_n, a_{n+1}\}$ und $E' = \{a_1, \ldots, a_n\}$. (Anders: $|E| = n+1 \rightsquigarrow \exists E' \subseteq E : E = E' \cup \{a_{n+1}\}$ und $|E'| = n$).
$\rightsquigarrow |E'| = n \overset{\text{I.V.}}{\rightsquigarrow} |\mathcal{P}(E')| = 2^{|E'|} = 2^n$.
Für jede Teilmenge $A \subseteq E$ gilt: entweder $a_{n+1} \in A$ oder $a_{n+1} \notin A$.
Ist $a_{n+1} \notin A$, so ist $A \subseteq E'$. Solche Teilmengen gibt es 2^n Stück (I.V.).
Ist $a_{n+1} \in A$, so gibt es genau eine Teilmenge A' von E mit $A = A' \cup \{a_{n+1}\}$ und $A' \subseteq E'$. Solche Teilmengen gibt es also auch 2^n Stück (da $A_1 \neq A_2 \to A_1' \neq A_2'$). $2^n + 2^n = 2^{n+1} \rightsquigarrow |\mathcal{P}(E)| = 2^{n+1} = 2^{|E|}$.

Aufgabe 1.3. Gilt für ein Wort $w \in \Sigma^*$ die Gleichung $w = w^{mi}$, nennt man w ein *Palindrom*. Beispiele sind etwa *abba* oder *ababa*. Aus der Spiegelungssymmetrie folgt für Palindrome, deren Länge größer als 1 sind, die Übereinstimmung von Anfangs- und Endbuchstaben. Sei also $w \in \Sigma^*$ ein Palindrom mit $|w| > 1$. Dann lässt sich w schreiben als $w = xvx$, wobei $x \in \Sigma$ ein Buchstabe und $v \in \Sigma^*$ ein Wort ist. Aus der Spiegelungssymmetrie folgt nun, dass auch v ein Palindrom sein muss.

ad (1). Es gilt:

$$\begin{aligned} \mathrm{dom}(f) &= \{w \in \Sigma^* : f(w) \downarrow\} \\ &= \{w \in \Sigma^* : \exists v : (w,v) \in \mathrm{graph}(f)\} \\ &= \{w \in \Sigma^* : \exists v : f(w) = v\} \\ &= \{w \in \Sigma^* : \exists v : w = xvx, x \in \Sigma \text{ und } w = w^{mi}\} \\ &= \{w \in \Sigma^* : w = w^{mi} \text{ und } |w| > 1\} \end{aligned}$$

Es gilt:

$$\begin{aligned} \mathrm{im}(f) &= \{f(w) \in \Sigma^* : w \in \mathrm{dom}(f)\} \\ &= \{f(w) \in \Sigma^* : w = w^{mi} \text{ und } |w| > 1\} \end{aligned}$$

Nach obiger Argumentation ist $f(w)$ selber ein Palindrom. Sei $u \in \Sigma^*$ ein Palindrom. Dann ist auch aua ein Palindrom und es gilt $f(aua) = u$. Im Wertebereich der Funktion f finden wir also alle Palindrome, d.h.

$$\mathrm{im}(f) = \{w \in \Sigma^* : w = w^{mi}\}$$

ad (2). Anschaulich schneidet f^2 allen Palindromen w mit $|w| > 3$ jeweils die ersten zwei und die letzten zwei Buchstaben ab. Der Definitionsbereich verkleinert sich also im Vergleich zu f.

$$\mathrm{dom}(f^2) = \{w \in \Sigma^* : w = w^{mi} \text{ und } |w| > 3\}$$

Aufgabe 1.4. Sei: $\Sigma = \{S, a, b\}$.
$\Pi = \{S \to aSa, S \to bSb, S \to \varepsilon\}$.
$M := \{uS\rho(u) \mid u \in (\Sigma \backslash \{S\})^*\} \cup \{u\rho(u) \mid u \in (\Sigma \backslash \{S\})^*\}$.

Zeige:
a) $\forall x \in M : S \vdash_\Pi x$ (d. h. $\{S\} \vdash_{K(\Sigma,\Pi)} x$).
b) $\forall x \in \Sigma^* : S \vdash_\Pi x \rightsquigarrow x \in M$.
Bezeichnung: $\Gamma := \Sigma \backslash \{S\}$.
Beweis:

a) Wir zeigen die Aussage zunächst für jedes Wort $uS\rho(u)$ mit $u \in \Gamma^*$.
Induktion über $|u|$:
$|u| = 0$: Klar, da $S \vdash^0_\Pi S$.
$|u| \to |u| + 1$: Es ist $|u| \geq 1$. D. h. $u = u'c$ mit $u' \in \Gamma^*$ und $c \in \Gamma$.
$uS\rho(u) = u'cS\rho(u'c) = u'cSc\rho(u')$ (Eigenschaft von ρ).
Nach I.V. gilt $\{S\} \vdash_{K(\Sigma,\Pi)} u'S\rho(u')$, da $|u'| < |u|$.
Da sowohl $\dfrac{u'S\rho(u')}{u'aSa\rho(u')}$ als auch $\dfrac{u'S\rho(u')}{u'bSb\rho(u')}$ Regeln des Kalküls $K(\Sigma,\Pi)$ sind, folgt $\{S\} \vdash_{K(\Sigma,\Pi)} uS\rho(u)$ für alle $u \in \Gamma^*$ mit $u = u'c$ und $c \in \Gamma$.

Da für $u \in \Gamma^*$ $\dfrac{uS\rho(u)}{u\rho(u)}$ eine Regel von $K(\Sigma,\Pi)$ ist, folgt auch noch $\{S\} \vdash_{K(\Sigma,\Pi)}$ $u\rho(u)$ für alle $u \in \Gamma^*$.

b) Sei M_i für $i \in \mathbb{N}$ die Menge der Wörter aus Σ^*, die in genau i Schritten in (Σ,Π) aus S ableitbar sind. (Beachte: $M = \bigcup_{i \geq 0} M_i$.)
Behauptung:
$M_0 = \{S\}$.
$M_i = \{uS\rho(u) \mid u \in \Gamma^* \text{ und } |u| = i\} \cup \{u\rho(u) \mid u \in \Gamma^* \text{ und } |u| = i - 1\}$ für $i > 0$.
Beweis:
$i = 0$: klar.
$i = 1$: $M_1 = \{aSa, bSb, \varepsilon\}$ (wg. Π)
$= \{uS\rho(u) \mid u \in \Gamma^*, |u| = 1\} \cup \{u\rho(u) \mid u \in \Gamma^*, |u| = 0\}$.

$i \to i+1$: I.V.: $M_i = \{uS\rho(u) \mid u \in \Gamma^* \text{ und } |u| = i\} \cup \{u\rho(u) \mid u \in \Gamma^* \text{ und } |u| = i-1\}$.

Auf $u\rho(u)$ mit $u \in \Gamma^*$ ist keine Produktion anwendbar, da S in $u\rho(u)$ nicht vorkommt.

Sei nun $uS\rho(u) \in M_i$, d. h. $u \in \Gamma^*$ und $|u| = i$.

Damit sind in einem Schritt aus $uS\rho(u)$ ableitbar:

$$\begin{array}{ll} uaSa\rho(u) = uaS\rho(ua) & (\text{mit } S \to aSa), \\ ubSb\rho(u) = ubS\rho(ub) & (\text{mit } S \to bSb), \\ u\rho(u) & (\text{mit } S \to \varepsilon). \end{array}$$

Sonst gibt es keine in einem Schritt ableitbaren Wörter.

$\rightsquigarrow M_{i+1} \subseteq \{uS\rho(u) \mid u \in \Gamma^* \text{ und } |u| = i+1\} \cup \{u\rho(u) \mid u \in \Gamma^* \text{ und } |u| = i\}$.

Sei andererseits $x = uS\rho(u)$ für beliebiges $u \in \Gamma^*$ mit $|u| = i+1$.

$$\begin{array}{ll} \rightsquigarrow x = u'cS\rho(u'c) & (\text{mit } u' \in \Gamma^*,\ c \in \Gamma \text{ und } u = u'c). \\ \quad = u'cSc\rho(u'). & \end{array}$$

Dies ist in einem Schritt aus $u'S\rho(u')$ ableitbar. Da $u'S\rho(u') \in M_i$ (wg. $|u'| = i$ und I.V.), ist $x \in M_{i+1}$.

Sei zuletzt $x = u\rho(u)$ für beliebiges $u \in \Gamma^*$ mit $|u| = i$.

Dies ist ein einem Schritt aus $uS\rho(u)$ ableitbar. Da $uS\rho(u) \in M_i$ ist (wg. $|u| = i$ und I.V.), ist $x \in M_{i+1}$.

Lösungsalternative für Punkt 2:

Behauptung: Jedes von S ableitbare Wort ist ein Element von M.

Beweis: **Erinnerung**:

Ein Objekt φ ist in einem Kalkül K ableitbar, falls es eine Folge $(\varphi_1, \ldots, \varphi_n)$ von Objekten gibt, so dass für alle $i = 1, \ldots, n$ Objekt φ_i die Konklusion einer Regel von K ist, deren Prämissen alle in $\{\varphi_1, \ldots, \varphi_{i-1}\}$ ($\emptyset$ für $i = 1$) enthalten sind und $\varphi_n = \varphi$ ist. Wir sagen dann, dass φ in $n-1$ Schritten ableitbar ist.

Also: w ist aus S ableitbar gdw. w ist aus S in i Schritten ableitbar für ein $i \in \mathbb{N}$.

Der Kalkül:

$$\frac{uSv}{uaSav} \quad (u, v \in \Sigma^*)$$

$$\frac{uSv}{ubSbv} \quad (u, v \in \Sigma^*)$$

$$\frac{uSv}{uv} \quad (u, v \in \Sigma^*)$$

$$\frac{}{S}$$

Wir zeigen: Für alle $i \in \mathbb{N}$ gilt: w aus S im Kalkül in i Schritten ableitbar $\rightsquigarrow w \in M$.

$i = 0$: $\quad w = S = \varepsilon S \varepsilon$, $\varepsilon = \rho(\varepsilon)$ und $\varepsilon \in \{a, b\}^*$.

$i \to i+1$: Sei w also aus S in $i+1$ Schritten ableitbar.

1. Letzte angewandte Kalkülregel: $\frac{uSv}{uv}$ für $u, v \in \Sigma^*$ geeignet.
$\rightsquigarrow w = uv$.
uSv ist also in i Schritten aus S ableitbar.

$\overset{I.V.}{\rightsquigarrow} v = \rho(u)$ und $u, v \in \{a, b\}^*$ (da nach I.V. $uSv \in M$).
$\rightsquigarrow w \in M$.

2. Letzte angewandte Kalkülregel: $\frac{uSv}{uaSav}$ für $u, v \in \Sigma^*$ geeignet.
$\rightsquigarrow w = uaSav$.
uSv ist also in i Schritten aus S ableitbar.

$\overset{I.V.}{\rightsquigarrow} v = \rho(u)$ und $u, v \in \{a, b\}^* \rightsquigarrow av = a\rho(u) = \rho(ua)$
$\rightsquigarrow w \in M$.

3. Analog für $\frac{uSv}{ubSbv}$.