# Eine direkte Definition der *predicate transformer*-Semantik für nichtdeterminisch-probabilistische Programme

Artus Ph. Rosenbusch

Diplomarbeit betreut von den
Herren Professoren Klaus Keimel und Thomas Streicher
am Fachbereich Mathematik
der TU Darmstadt

FB 4
Technische Universität Darmstadt
Schloßgartenstr. 7
64287 Darmstadt
Deutschland

08. Februar 2007

## Abstract

Wir führen zwei direkte Semantiken sowie die *weakest preexpectation*-Semantik und die *weakest liberal preexpectation*-Semantik als zugehörige *predicate transformer*-Semantiken für die imperative Programmiersprache pGCL ein, die sowohl probabilistischen Nondeterminismus als auch Nondeterminismus im üblichen Sinne erlaubt.
Um totale Korrektheitsaussagen zu treffen, definieren wir eine direkte Semantik im Smyth-Powerdomain auf dem Raum der Subverteilungen. Die direkte Semantik, auf der partielle Korrektheitsüberlegungen aufsetzen, nutzt den Hoare-Powerdomain auf dem Raum der Subverteilungen.
Beide *predicate Transformer*-Semantiken für pGCL werden aus der entsprechenden direkten Semantik heraus definiert, erfüllen aber bestimmte Gleichungen, die es erlauben, sie auf äquivalente Weise rekursiv über den Termaufbau zu definieren.
Die *predicate Transformer*-Semantiken von `while`-Schleifen berechnen sich im Fall von wp als kleinster und im Fall von wlp als größter Fixpunkt. So erlaubt die *weakest liberal preexpectation*-Semantik partielle Korrektheitsbeweise via Invariantenkalkül.


### Eidesstattliche Erklärung

Ich erkläre an Eides statt, daß ich die vorliegende Diplomarbeit selbständig und ohne fremde Hilfe verfaßt, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Einleitung

Gleichzeitig mit der Bedeutung der Informatik wächst auch die Komplexität der in allen Bereichen eingesetzten IT-Systeme. Nur über Modularisierung und klare Definition von Schnittstellen kann man heute noch große Softwareprojekte realisieren und den vielerorts extrem hohen Sicherheitsanforderungen gerecht werden.

Beweisbare Korrektheit von Programmen oder Programmteilen ist vor diesem Hintergrund ein interessantes Thema. Um aber mit mathematischen Methoden über Programme zu diskutieren, muß man diesen zunächst eine Semantik zuweisen.

Während es schon lange eine umfassende Theorie zur Semantik von imperativen deterministischen Programmiersprachen gibt, beschäftigt sich diese Arbeit mit solchen Sprachen, die zwei unterschiedliche Formen des Nondeterminismus erlauben. Für eine solche Sprache wird zunächst eine direkte Semantik mit Hilfe des Smyth-Powerdomains und später eine weitere mit Hilfe des Hoare-Powerdomains entwickelt. Dann wird auch eine rekursive Charakterisierung für die beiden assoziierten *predicate transformer*-Semantiken wp und wlp angegeben.

Kapitel 0 klärt Notationen und bietet Platz für allgemeine Sätze über Bereiche, Verbände und Infima in $\mathbb{R}$.

Im ersten Kapitel werden mathematischen Begriffe und Ergebnisse aus [TKP05] vorgestellt, auf denen diese Arbeit aufbaut. Im Wesentlichen sind dies der erweiterte probabilistische Powerdomain und der Smyth- Powerdomain auf einer Teilmenge davon, den Subverteilungen. Das Kapitel schließt mit einer Charakterisierung des Smyth-Powerdomain als Menge der $T_2$-abgeschlossenen saturierten, konvexen, nichtleeren Mengen von Subverteilungen.

Das zweite Kapitel stellt die beiden behandelten Formen des Nondeterminismus vor und gibt einen ersten Eindruck davon, wie wir sie semantisch fassen wollen. Es endet mit der Definition der Syntax der Programmiersprache pGCL, für die wir eine denotationelle Semantik entwickeln wollen.

Kapitel 3 führt eine direkte denotationelle Semantik für pGCL ein, die Programme durch Funktionen aus dem Zustandsraum $S$ in den Smyth-Powerdomain auf den Subverteilungen von $S$, also durch Funktionen $f : S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ interpretiert.

Im vierten Kapitel wird eine assoziierte *predicate transformer*-Semantik der *weakest pre-expectation* definiert, die Dijkstras wp-Semantik nach [Dij75] entspricht. Die Definition ist direkt, das heißt wp ist eine Abbildung, die der direkten Semantik eines Programms eine Selbstabbildung des Raums der Prädikate zuordnet. Es wird gezeigt, wie wp auf äquivalente Weise rekursiv über den Termaufbau definiert werden kann.

Die wp-Semantik einer `while`-Schleife ist dabei ein kleinster Fixpunkt. Will man partielle Korrektheitsbeweise mit dem etablierten Invariantenkalkül führen, so benötigt man jedoch einen größten Fixpunkt.

Deswegen wird in Kapitel 5 eine weitere direkte denotationelle Semantik definiert, die Programme durch Funktionen aus dem Zustandsraum $S$ in den Hoare-Powerdomain auf den Subverteilungen von $S$, also durch Funktionen $f : S \longrightarrow \mathfrak{P}_{\text{H}}\mathcal{V}(S)$ interpretiert.

Die direkte Semantik im Hoare-Powerdomain erlaubt die Definition einer assoziierten *predicate transformer*-Semantik, die der *weakest liberal preexpectation*. Diese wlp-Semantik entspricht der wlp-Semantik bei Dijkstra. Sie ist Gegenstand von Kapitel 6. Wir zeigen, daß wieder Gleichungen gelten, die eine äquivalente Definition rekursiv über den Termaufbau erlauben und im Zuge dessen, daß Schleifen in dieser Semantik als größte Fixpunkte interpretiert werden.

An dieser Stelle möchte ich gerne all jenen danken, die am Gelingen dieser Diplomarbeit maßgeblich beteiligt waren: Zuallererst den Herren Professoren Klaus Keimel und Thomas Streicher, die nicht müde wurden, meine vielen Fragen zu diskutieren und mir stets wertvolle Anregungen geben konnten. Insbesondere in der Schlußphase der Arbeit haben Sie sehr viel Zeit investiert, um mir detailliert Feedback über den Status der Arbeit zu geben und viele Vorschläge zur Verbesserung der Darstellung gemacht, wofür ich besonders dankbar bin. Ben S. Cohen gilt mein Dank für ausführliches Korrekturlesen, Hinweise zum Design und unzählige Stunden der fachlichen Diskussion. Meinen Eltern Gisela und Artus W. Rosenbusch danke ich dafür, daß sie mein Studium großzügig unterstützt haben. Mathias Kegelmann hat mich nicht nur in seiner Vorlesung in den Grundlagen der Bereichstheorie unterrichtet und die Begeisterung für dieses mathematische Gebiet entfacht, sondern auch große Unterstützung im Umgang mit LaTeX gegeben.

Dank gilt auch den Betreibern und den Nutzern der Webseiten `wikipedia.com` und `dict.leo.org`, ohne die ich mir effizientes Arbeiten heute nicht mehr vorstellen könnte.

*Among the maxims on Lord Naoshige's wall, there was this one: "Matters of great concern should be treated lightly." Master Ittei commented, "Matters of small concern should be treated seriously."*

## Grundlegende Begriffe und Notationen

Diese Arbeit setzt grundlegende Kenntnisse in der Bereichstheorie voraus. Begriffe und Bezeichnungen übernehmen wir aus [AJ94]. Ein Bereich ist in dieser Arbeit eine dcpo.

Für zwei Bereiche $X$ und $Y$ bezeichnet $\left[X \longrightarrow Y\right]$ die Menge der Scott-stetigen Funktionen von $X$ nach $Y$, die mit der punktweisen Ordnung selbst wieder ein Bereich ist.

Für eine Teilmenge $D$ eines Bereichs $X$ bedeutet die Gleichung

$$\bigvee\nearrow D = d$$

zweierlei, erstens, daß $D$ gerichtet ist und zweitens, daß $d$ das Supremum von $D$ ist.

Es ist $\mathbb{R}_+ := \left\{r \in \mathbb{R} \;\middle|\; r \geq 0\right\}$ mit der gewöhnlichen linearen Ordnung.

Der Abschluß $\overline{\mathbb{R}}_+$ enthält zusätzlich ein Element $\infty$ mit $r \leq \infty$ für alle $r \in \mathbb{R}_+$. Auf dem dcpo $\overline{\mathbb{R}}_+$ betrachten wir, soweit nicht anders vermerkt, stets die Scott-Topologie.

Wir verwenden die übliche Semantikklammer $[\![\cdot]\!]$, um zwischen Syntax und Semantik zu unterscheiden.

In einem Poset $X$ schreiben wir für die Saturierung $\uparrow\{x\}$ eines Punkts $x \in X$ kurz $\uparrow x$.

**Satz 0.1.** *Es sei $(D_i)_{i\in I}$ eine Menge von stetigen Bereichen mit kleinstem Element $\bot$.*

(i) *Das direkte Produkt $\Pi(D_i)$ mit der punktweisen Ordnung ist ein stetiger Bereich, dessen way-below-Relation charakterisiert wird duch*

$$(a_i) \ll (b_i) \quad \Longleftrightarrow \quad \begin{cases} \left(\forall i \in I\right) a_i \ll b_i & \textit{und} \\ a_i = \bot & \textit{für alle bis auf endlich viele } i. \end{cases}$$

(ii) *Die Topologie, die sich als Produkttopologie der Scott-Topologien auf den $D_i$ ergibt, ist gerade die Scott-Topologie auf $\Pi(D_i)$.*

(iii) *Sind ferner $X_i \subseteq D_i$ Scott-kompakte Teilmengen, so ist auch $\Pi(K_i)$ eine Scott-kompakte Teilmenge von $\Pi(D_i)$.*

**Beweis.**

(i) Siehe [GHK+03, Proposition I-2-1]

(ii) Aus (i) folgt $\pi_i^{-1}(\uparrow a_i) = \uparrow(\bot, \ldots, \bot, a_i, \bot, \ldots, \bot)$. Da Mengen der Form $\uparrow x$ eine Basis der Scott-Topologie auf stetigen Bereichen sind, folgt die Behauptung.

(iii) Die Kompaktheit des Produkts folgt mit (ii) aus dem Satz von Tychonoff.

□

**Satz 0.2.** *Für einen vollständigen Verband $L$ und ein dcpo $A$ ist der dcpo der Scott-stetigen Funktionen $\left[A \longrightarrow L\right]$ wieder ein vollständiger Verband.*

**Beweis.** Es sei $F$ eine Menge von Scott-stetigen Funktionen in $\left[A \longrightarrow L\right]$.
In $L^A$ existiert das Supremum

$$f = \bigvee F = \lambda x. \bigvee_{g \in F} g(x).$$

Es ist zu prüfen, ob dieses Supremum Scott-stetig ist.
Sei hierfür $(x_i)_{i \in I}$ eine gerichtete Menge in $A$. So ist

$$f\Big(\bigvee\nolimits^{\nearrow}_{i} x_i\Big) = \bigvee_{g \in F} g\Big(\bigvee\nolimits^{\nearrow}_{i} x_i\Big) = \bigvee_{g} \bigvee\nolimits^{\nearrow}_{i} g(x_i) = \bigvee\nolimits^{\nearrow}_{i} \bigvee_{g} g(x_i) = \bigvee\nolimits^{\nearrow}_{i} f(x_i).$$

Da nun in $\left[A \longrightarrow L\right]$ beliebige Suprema existieren, existieren beliebige Infima über

$$\wedge F := \bigvee \underbrace{\bigcap_{g \in F} (\downarrow g)}_{\substack{\text{untere Schranken} \\ \text{von } F}} .$$

□

**Korollar 0.3.** *Unter den Voraussetzungen von Satz 0.2 ist auch $\left[A \longrightarrow L\right]^{\mathsf{op}}$ ein vollständiger Verband*

Stillschweigend werden wir das folgende Lemma verwenden:

**Lemma 0.4.** *Es sei $S$ eine abzählbare Menge. Für $A_t \subseteq [0,1]$ sei die reelle Summe $\sum_{t \in S} \bigwedge A_t$ beschränkt. Dann gilt*

$$\bigwedge \sum_{t \in S} A_t = \sum_{t \in S} \bigwedge A_t.$$

**Beweis.** Für $m \in \sum A_t$ ist $m = \sum m_t$ mit $m_t \in A_t$. Es ist für alle $t$ stets $m_t \geq \bigwedge A_t$ und deswegen ist $m \geq \sum \bigwedge A_t$, also ist $\bigwedge \sum A_t \geq \sum \bigwedge A_t$.
Zeigen wir als nächstes, daß $\bigwedge \sum A_t \leq \sum \bigwedge A_t$ gilt:
Es sei $N : S \longrightarrow \mathbb{N}$ eine Bijektion (hier ist $0 \notin \mathbb{N}$) und $z > 0$ gegeben.

Wegen der Approximationseigenschaft von $\mathbb{R}$ gibt es für jedes $t \in S$ stets ein $a_t \in A_t$ mit

$$\bigwedge A_t + \frac{z}{2^{N(t)}} > a_t.$$

Dann ist

$$\sum_{t\in S} a_t - \sum_{t\in S} \bigwedge A_t < \sum_{n\in\mathbb{N}} \frac{z}{2^n} = z.$$

Da $z > 0$ beliebig war, gilt $\bigwedge \sum A_t \leq \sum \bigwedge A_t$. □

Für die Scott-Topologie auf stetigen Bereichen gilt das folgende Lemma.

**Lemma 0.5.** *Sei $X$ ein stetiger Bereich und $A$ eine Teilmenge von $X$. Dann ist der Scott-Abschluß $\overline{A}$ gegeben durch*

$$\overline{A} = \left\{ \bigvee\nearrow D \;\middle|\; D \subseteq {\downarrow}A \right\}.$$

**Beweis.** Offensichtlich gilt $A \subseteq \left\{ \bigvee\nearrow D \;\middle|\; D \subseteq {\downarrow}A \right\} \subseteq \overline{A}$. Es ist also hinreichend, zu zeigen, daß $L \coloneqq \left\{ \bigvee\nearrow D \;\middle|\; D \subseteq {\downarrow}A \right\}$ eine Scott-abgeschlossene Menge ist.

Hierzu zeigen wir zunächst, daß $L$ eine untere Menge ist.

Sei $D \subseteq {\downarrow}A$, $x = \bigvee\nearrow D \in L$ und $x' \leq x$ ein Punkt darunter. Dann sehen wir zunächst wie folgt ein, daß ${\downarrow}x'$ eine Teilmenge von ${\downarrow}A$ ist:

$$\begin{aligned} a \ll x' \Longrightarrow a \ll x = \bigvee\nearrow D \Longrightarrow \left(\exists d \in D\right) a \leq d \\ \Longrightarrow \left(\exists d \in {\downarrow}A\right) a \leq d \Longrightarrow a \in {\downarrow}A. \end{aligned}$$

Da $X$ ein stetiger Bereich ist, ist $x' = \bigvee\nearrow{\downarrow}x'$. Und da ${\downarrow}x' \subseteq {\downarrow}A$ ist, ist per definition $x' \in L$.

Schließlich überzeugen wir uns, daß $L$ unter dem Bilden gerichteter Suprema abgeschlossen ist. Sei hierfür $\{d_i = \bigvee\nearrow D_i\}$ eine gerichtete Teilmenge von $L$ und sei $U_i \coloneqq {\downarrow}D_i$. Dann ist $\bigvee\nearrow\{d_i\} = \bigvee \cup D_i = \bigvee \cup U_i$ und $\cup U_i$ ist eine Teilmenge von ${\downarrow}A$.

Es bleibt zu zeigen, daß $\cup U_i$ gerichtet ist. Seien hierfür zwei Elemente $u_1 \in U_1, u_2 \in U_2$ gegeben. Wir suchen nun ein $u_3 \in U_3$ mit $u_j \leq u_3 (j = 1, 2)$.

Da $\{d_i\}$ gerichtet ist, gibt es ein $d_3$, das über $d_1$ und $d_2$ liegt. Somit ist auch $u_1 \ll d_3$ und $u_2 \ll d_3$.

Die Interpolationseigenschaft stetiger Bereiche garantiert nun die Existenz eines $d_3$ mit $u_j \ll u_3 \ll d_3 (j = 1, 2)$. Nochmalige Interpolation liefert ein $x$ mit $u_3 \ll x \ll d_3$.

Ist $d_3 = \bigvee\nearrow D_3$, so ist per definition der $\ll$-Relation $x \in {\downarrow}D_3$. Es folgt sofort $u_3 \in U_3$, was den Beweis abschließt. □

*Jedem Anfang wohnt ein Zauber inne, der*
*uns beschützt und der uns hilft, zu leben.*
*(Hermann Hesse)*

# 1 Der Smyth-Powerdomain

Bevor wir uns der Syntax und Semantik von pGCL zuwenden, widmen wir uns den auftretenden Räumen und ihren Eigenschaften.

Zunächst gibt es einen Zustandsraum, der die Systemzustände eines Rechners modelliert. Da wir keine Sprache mit höheren Typen untersuchen, sind zwei Systemzustände stets unvergleichbar. Die Ordnung auf dem Zustandsraum ist also trivial und jede Teilmenge ist Scott-offen.

**Definition 1.1.** Der **Zustandsraum** $S$ ist ein abzählbarer diskreter Raum.

Implizit tritt auch der Systemzustand $\bot$ auf, der für Nichtterminierung reserviert ist. Der dcpo $S_\bot$ ist das Lifting von $S$.

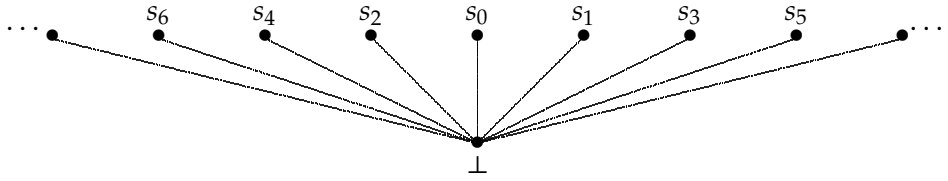


Abbildung 1: Der flache Bereich $S_\bot$

In den nächsten Abschnitten stelle ich Begriffe und Ergebnisse aus [TKP05] vor, auf denen diese Arbeit aufbaut.

## 1.1 d-Kegel

**Definition 1.2.** Einen Menge $C$ heißt **Kegel**, wenn sie mit einer Addition $+ : C \times C \longrightarrow C$ und einer Skalarmultiplikation $\cdot : \mathbb{R}_+ \times C \longrightarrow C$ ausgestattet ist, so daß die folgenden Bedingungen erfüllt sind:

(i) Es gibt ein neutrales Element $0 \in C$ für die Addition, so daß $(C, +, 0)$ ein kommutatives Monoid ist, das heißt für $a, b, c \in C$ gilt:

$$(a + b) + c = a + (b + c)$$
$$a + b = b + a$$
$$a + 0 = a$$

(ii) Die Skalarmultiplikation verhält sich wie bei Vektorräumen: Für $a, b \in C$ und $r, s \in \mathbb{R}_+$ gilt

$$\begin{aligned} 1 \cdot a &= a \\ 0 \cdot a &= 0 \\ (r \cdot s) \cdot a &= r \cdot (s \cdot a) \\ r \cdot (a + b) &= (r \cdot a) + (r \cdot b) \\ (r + s) \cdot a &= (r \cdot a) + (s \cdot a). \end{aligned}$$

Eine Funktion $f : C \longrightarrow D$ zwischen Kegeln heißt **linear**, falls für alle $a, b \in C$ und $r \in \mathbb{R}_+$ folgende Bedingungen gelten:

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(r \cdot a) &= r \cdot f(a) \end{aligned}$$

Ein Kegel $C$ heißt **geordneter Kegel**, wenn er mit einer partiellen Ordnung $\leq$ ausgestattet ist, so daß die Addition und die Skalarmultiplikation als Abbildungen $C \times C \longrightarrow C$ bzw. $\mathbb{R}_+ \times C \longrightarrow C$ in beiden Variablen odnungserhaltend sind.

Ein Kegel mit einer Topologie darauf, bezüglich der die Addition und Skalarmultiplikation stetig sind, heißt **topologischer Kegel**.

Wenn die Ordnung $C$ zu einem dcpo macht und die Addition und Skalarmultiplikation Scott-stetig sind, dann heißt $C$ auch **d-Kegel**.

Ist $C$ darüberhinaus ein stetiger Bereich, so heißt $C$ auch **stetiger d-Kegel**.

Mit $\mathsf{conv}(A)$ bezeichnen wir die konvexe Hülle einer Teilmenge $A$ eines Kegels. Konvexität wird hier stets geometrisch verstanden; Konvexität im Sinne der Ordnungstheorie spielt in dieser Arbeit keine Rolle.

**Lemma 1.3.** *Es seien $P, Q$ Teilmengen eines Kegels $C$ und $r \in \mathbb{R}_+$. Dann folgt*

(i) *Die konvexe Hülle eines skalaren Vielfachen ist gegeben durch* $\mathsf{conv}(r \cdot P) = r \cdot \mathsf{conv}\ P$.

(ii) *Die konvexe Hülle der Summe ist gegeben durch* $\mathsf{conv}(P + Q) = \mathsf{conv}\ P + \mathsf{conv}\ Q$.

(iii) *Wenn $P, Q$ konvex sind, so sind auch $r \cdot P$ und $P + Q$ konvex.*

(iv) *Mit der so definierten Addition und Skalarmultiplikation ist die Menge der konvexen Teilmengen von $C$ selbst wieder ein Kegel.*

(v) *Wenn $P$ und $Q$ konvex sind, so ist die konvexe Hülle der Vereinigung von $P$ und $Q$ gegeben durch* $\mathsf{conv}(P \cup Q) = \left\{ r \cdot p + (1 - r) \cdot q \;\middle|\; p \in P,\, q \in Q,\, r \in [0, 1] \right\}$.

**Beweis.** Siehe [TKP05, Lemma 2.8]. □

**Lemma 1.4.** *Für kompakte konvexe Teilmengen $P$ und $Q$ eines topologischen Kegels ist die konvexe Hülle* $\mathsf{conv}(P \cup Q)$ *der Vereinigung selbst wieder kompakt. Das gilt insbesondere für stetige d-Kegel mit der Scott-Topologie.*

**Beweis.** Siehe [TKP05, Lemma 2.9]. □

## 1.2 Subverteilungen im erweiterten probabilistischen Powerdomain

Wir haben einige Eigenschaften von Kegeln vorgestellt. In diesem Abschnitt betrachten wir den Kegel, der in unserer denotationellen Semantik von probabilistischen Programmen die zentrale Rolle spielt.

**Definition 1.5.** Es sei $S$ der diskrete Zustandsraum und $\mathcal{O}(S) = \mathfrak{P}(S)$ das System der Teilmengen von $S$. Eine Funktion $\mu : \mathcal{O}(S) \longrightarrow [0,1]$ heißt **Bewertung** auf $S$, falls für alle $U, V \in \mathcal{O}(S)$ gilt:

- $\mu(\varnothing) = 0$ ($\mu$ ist **strikt**)
- $U \subseteq V \Longrightarrow \mu(U) \leq \mu(V)$ ($\mu$ ist **monoton**)
- $\mu(U) + \mu(V) = \mu(U \cup V) + \mu(U \cap V)$ ($\mu$ ist **modular**)

Ist ferner $\mu$ Scott-stetig, das heißt es gilt

- $\mu\left(\bigvee\!\!\nearrow_{i\in I} U_i\right) = \bigvee\!\!\nearrow_{i\in I} \mu(U_i)$ für alle per $\subseteq$ gerichteten Familien $(U_i)_{i\in I}$ in $\mathcal{O}(S)$,

so heißt $\mu$ **stetige Bewertung** und wird wegen $\mu(S) \leq 1$ auch **Subverteilung** auf $S$ genannt.

Die Menge der Subverteilungen auf $S$ bildet mit der punktweisen Ordung eine dcpo. Mit $\mathcal{V}(S)$ bezeichnen wir diesen Raum der Subverteilungen auf $S$ mit der Scott-Topologie.

Der **erweiterte probabilistische Powerdomain** $\mathcal{V}_\infty(S)$ ist der Raum der stetigen Bewertungen $\mu : \mathcal{O}(S) \longrightarrow \overline{\mathbb{R}}_+$ mit der punktweisen Ordnung und der Scott-Topologie.

**Proposition 1.6.** *Für abzählbare diskrete Zustandsräume $S$ kann $\mathcal{V}(S)$ durch den folgenden Isomorphismus von Posets charakterisiert werden:*

$$\mathcal{V}(S) \cong \left\{ f : S \longrightarrow [0,1] \;\middle|\; \sum_{s\in S} f(s) \leq 1 \right\}$$

$$\mu \longmapsto f_\mu, \quad \textit{mit} \quad f_\mu(s) = \mu(\{s\}) \qquad \text{und invers:}$$

$$f \longmapsto \mu_f, \quad \textit{mit} \quad \mu_f(U) = \sum_{s\in U} f(s), \textit{ für } U \in \mathcal{O}(S)$$

**Beweis.** Striktheit, Monotonie, Modularität und Stetigkeit von $\mu_f$ sind offenbar gegeben. Beide Funktionen sind also wohldefiniert.

Die Monotonie von $\mu \longmapsto f_\mu$ folgt direkt aus der Definition der Ordnung auf $\mathcal{V}(S)$:

$$\begin{aligned} \mu \leq \mu' &\Longrightarrow \mu(U) \leq \mu'(U) && \text{für alle } U \in \mathcal{O}(S) \\ &\Longrightarrow \mu(\{s\}) \leq \mu'(\{s\}) && \text{für alle } s \in S \\ &\Longrightarrow f_\mu(s) \leq f_{\mu'}(s) && \text{für alle } s \in S \\ &\Longrightarrow f_\mu \leq f_{\mu'} \end{aligned}$$

Die Monotonie der Umkehrabbildung $f \longmapsto \mu_f$ sieht man analog. Da beide Abbildungen monoton und zueinander invers sind, sind die Räume ordnungsisomorph. Statten wir beide mit der Scott-Topologie aus, so sind sie auch homöomorphe topologische Räume. □

Im Folgenden werden wir, auch die einer Subverteilung $\mu$ zugeordnete Funktion $f_\mu$ selbst wieder mit $\mu$ bezeichnen, wenn aus dem Typ des Funktionsarguments ersichtlich wird, was gemeint ist.

Definieren wir einige spezielle Subverteilungen:

**Definition 1.7.** Für $s \in S$ ist die **Punktverteilung** $\eta_s \in \mathcal{V}(S)$ gegeben durch

$$\eta_s(U) := \begin{cases} 1 & \text{für } s \in U \\ 0 & \text{für } s \notin U. \end{cases}$$

Die **Nullverteilung** $\perp \in \mathcal{V}(S)$ ist gegeben durch

$$\perp (U) := 0.$$

**Bemerkung 1.8.** Die Nullverteilung $\perp$ ist das kleinste Element von $\mathcal{V}(S)$. Die Punktverteilungen $\eta_s$ sind maximale Elemente von $\mathcal{V}(S)$. Die Wahrscheinlichkeitsverteilungen sind genau die maximalen Elemente von $\mathcal{V}(S)$.

**Theorem 1.9.** *Der erweiterte probabilistische Powerdomain $\mathcal{V}_\infty(S)$ ist ein stetiger d-Kegel mit der punktweisen Addition und Skalarmultiplikation.*

**Beweis.** Siehe [TKP05, Theorem 2.10] □

Um eine Semantik für nichtdeterministische Auswahl zu definieren, werden wir das folgende Resultat benötigen. Mit den Ergebnissen aus dem nächsten Abschnitt ist Theorem 1.10 ein Korollar des vorherigen Theorems, wir beweisen es hier aber direkt.

**Theorem 1.10.** *Es seien $A$ und $B$ zwei Scott-kompakte, konvexe Teilmengen von $\mathcal{V}(S)$. Dann ist die Menge* $\mathsf{conv}(A \cup B)$ *Scott-kompakt in $\mathcal{V}(S)$.*

**Beweis.** Die Abbildung

$$\begin{aligned}[0,1]\times[0,1]\times A\times B &\longrightarrow \mathcal{V}(S)\\ (p,q,a,b) &\longmapsto p\cdot a+q\cdot b\end{aligned}$$

ist Scott-stetig.

Wenn wir nun $q = 1 - p$ setzen, so entspricht dies der Abbildung

$$\begin{aligned}[0,1]\times A\times B &\longrightarrow \mathcal{V}(S)\\ (p,a,b) &\longmapsto p\cdot a+(1-p)\cdot b,\end{aligned}$$

wobei $[0,1]$ als Teilmenge $\left\{(p,1-p)\in[0,1]^2 \;\middle|\; p\in[0,1]\right\}$ zu verstehen ist und die übliche Hausdorfftopologie trägt.

Bezüglichdieser ist die Abbildung stetig. Entsprechend ist $\mathsf{conv}(A\cup B)$ kompakt, da es das Bild der kompakten Menge $[0,1]\times A\times B$ unter einer stetigen Abbildung ist. □

Die Subverteilungen $\mathcal{V}(S)$ entsprechen durch Einbettung der durch die Ungleichung $\mu(S)\leq 1$ begrenzten kompakten konvexen Teilmenge von $\mathcal{V}_\infty(S)$. Deswegen können wir Aussagen über stetige d-Kegel oft auch auf $\mathcal{V}(S)$ übertragen, obwohl $\mathcal{V}(S)$ selbst kein d-Kegel ist.

## 1.3 $\mathcal{V}(S)$ als Unterraum von $\mathcal{V}_\infty(S)$

Wir untersuchen nun, wie wir Scott-offene Mengen in $\mathcal{V}(S)$ aus Scott-offenen Mengen in $\mathcal{V}_\infty(S)$ erzeugen können und umgekehrt. Wir unterscheiden dabei in der Notation nicht zwischen $\mathcal{V}(S)$ als Raum und $\mathcal{V}(S)$ als Teilmenge von $\mathcal{V}_\infty(S)$.

**Lemma 1.11.** *$\mathcal{V}(S)$ ist ein abgeschlossener Unterraum von $\mathcal{V}_\infty(S)$, das heißt offene Mengen in $\mathcal{V}(S)$ und $\mathcal{V}_\infty(S)$ kann man wie folgt auseinander erzeugen:*

(i) *Sei $O$ Scott-offen in $\mathcal{V}(S)$. Dann ist $O\cup\mathcal{V}(S)^{\mathsf{c}}$ Scott-offen in $\mathcal{V}_\infty(S)$.*

(ii) *Sei $U$ Scott-offen in $\mathcal{V}_\infty(S)$. Dann ist $U\cap\mathcal{V}(S)$ Scott-offen in $\mathcal{V}(S)$.*

*Diese wechselseitige Erzeugung von offenene Mengen wird in Abb. 2 und 3 illustriert.*

**Beweis.**

(i) Sei $O$ Scott-offen in $\mathcal{V}(S)$. Das heißt $O = \uparrow O$ in $\mathcal{V}(S)$ und für alle gerichteten Mengen $\{f_i \mid i\in I\}\subseteq\mathcal{V}(S)$ mit $\bigvee\!\!\nearrow f_i\in O$ gibt es einen Index $j$ mit $f_j\in O$.

Betrachten wir nun die Menge $O\cup\mathcal{V}(S)^{\mathsf{c}}$ in $\mathcal{V}_\infty(S)$.

Da $\uparrow O$ in $O\cup\mathcal{V}(S)^{\mathsf{c}}$ liegt, ist

$$O\cup\mathcal{V}(S)^{\mathsf{c}} = \uparrow O\cup\mathcal{V}(S)^{\mathsf{c}}$$

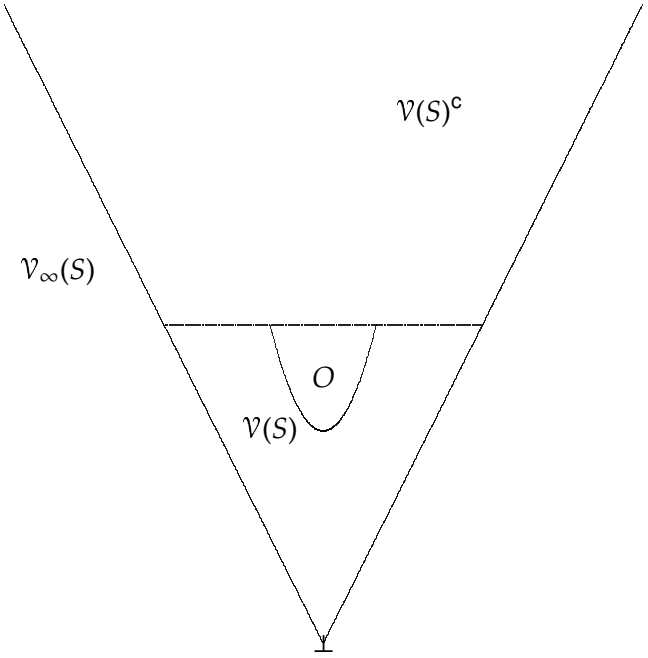


Abbildung 2: Übergang von $\mathcal{OV}(S)$ zu $\mathcal{OV}_\infty(S)$

und Vereinigungen saturierter Mengen sind saturiert. Es bleibt zu zeigen, daß für gerichtete Teilmengen $\{f_i \mid i \in I\} \subseteq \mathcal{V}_\infty(S)$ stets

$$\bigsqcup_{i\in I}^{\nearrow} f_i \in O \cup \mathcal{V}(S)^{\mathsf{c}} \Longrightarrow \big(\exists j \in I\big)\, f_j \in O \cup \mathcal{V}(S)^{\mathsf{c}}$$

gilt.

Ist $\bigsqcup^{\nearrow} f_i \in O$, so sind alle $f_i \in \mathcal{V}(S)$ und es folgt die Behauptung, da $O$ offen in $\mathcal{V}(S)$ ist.

Ist andererseits $\bigsqcup^{\nearrow} f_i \in \mathcal{V}(S)^{\mathsf{c}}$, so ist auch $\bigsqcup^{\nearrow} f_i(S) \in (1, \infty]$. Dieses Intervall ist eine Scott-offene Teilmenge von $\overline{\mathbb{R}}_+$, also gibt es ein $j$ mit $f_j(S) > 1$. Dann ist aber auch $f_j \in \mathcal{V}(S)^{\mathsf{c}}$. Tatsächlich ist also $O \cup \mathcal{V}(S)^{\mathsf{c}}$ Scott-offen in $\mathcal{V}_\infty(S)$.

(ii) Sei nun andererseits eine offene Menge $U$ in $\mathcal{V}_\infty(S)$ gegeben. Betrachten wir die Menge $U \cap \mathcal{V}(S)$. Trivialerweise ist $U \cap \mathcal{V}(S) = \uparrow\big(U \cap \mathcal{V}(S)\big)$ in $\mathcal{V}(S)$.

In einer gerichtete Menge $\{f_i\}$ in $\mathcal{V}(S)$ mit $\bigsqcup^{\nearrow} f_i \in U \cap \mathcal{V}(S)$ gibt es stets eine Element $f_j$ mit $f_j \in U$, denn $U$ ist offen in $\mathcal{V}_\infty(S)$. Da $f_j$ Element von $\mathcal{V}(S)$ ist, ist auch $f_j \in U \cap \mathcal{V}(S)$.

□

**Korollar 1.12.** *Eine Scott-kompakte Menge $A \subseteq \mathcal{V}(S)$ ist auch Scott-kompakt in $\mathcal{V}_\infty(S)$.*

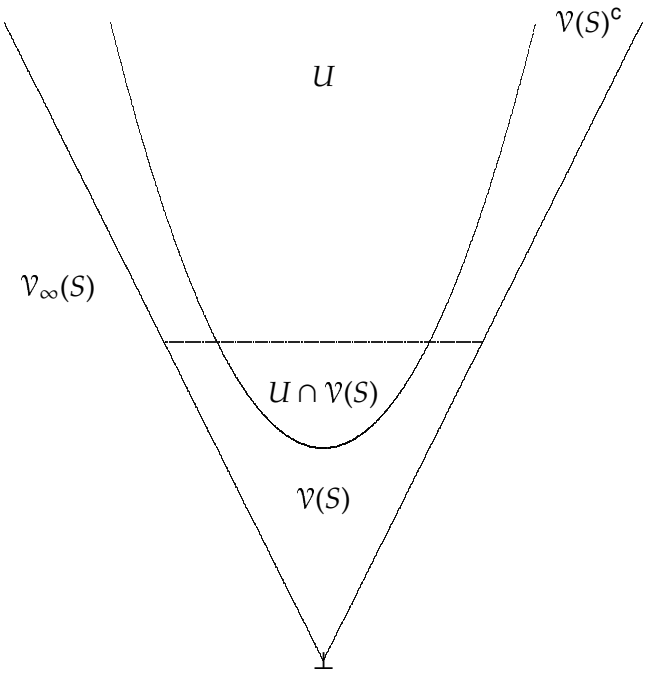


Abbildung 3: Übergang von $\mathcal{OV}_\infty(S)$ zu $\mathcal{OV}(S)$

**Beweis.** Es sei eine offene Überdeckung $(U_i)_{i\in I}$ von $A$ in $\mathcal{V}_\infty(S)$ gegeben. Dann sind $O_i \coloneqq U_i \cap \mathcal{V}(S)$ offene Teilmengen von $\mathcal{V}(S)$, die $A$ überdecken, da $A$ selbst Teilmenge von $\mathcal{V}(S)$ ist. Da $A$ in $\mathcal{V}(S)$ kompakt ist, gibt es eine endliche Indexmenge $F \subseteq_{\mathsf{fin}} I$ mit $A \subseteq \bigcup_{f\in F} O_f$. Daraus ergibt sich aber auch $A \subseteq \bigcup_{f\in F} U_f$. □

**Korollar 1.13.** *Für eine Scott-kompakte Menge $A \subseteq \mathcal{V}_\infty(S)$ ist $A \cap \mathcal{V}(S)$ Scott-kompakt in $\mathcal{V}(S)$.*

**Beweis.** Es sei eine offene Überdeckung $(O_i)_{i\in I}$ von $A \cap \mathcal{V}(S)$ in $\mathcal{V}(S)$ vorgegeben. Dann sind $U_i \coloneqq O_i \cup \mathcal{V}(S)^{\mathsf{c}}$ offene Teilmengen von $\mathcal{V}_\infty(S)$, die $A$ überdecken, denn $A \subseteq (A \cap \mathcal{V}(S)) \cup \mathcal{V}(S)^{\mathsf{c}}$. Da $A$ in $\mathcal{V}_\infty(S)$ kompakt ist, gibt es eine endliche Indexmenge $F \subseteq_{\mathsf{fin}} I$ mit $A \subseteq \bigcup_{f\in F} U_f$. Daraus ergibt sich aber auch $A \cap \mathcal{V}(S) \subseteq \bigcup_{f\in F} O_f$. □

**Bemerkung.** Mit der Theorie aus diesem Abschnitt können wir Theorem 1.10 auch als Korollar von Theorem 1.9 auffassen:

Da $A, B$ kompakt in $\mathcal{V}(S)$ sind, sind sie auch kompakte, konvexe Teilmengen von $\mathcal{V}_\infty(S)$. Somit ist wegen Theorem 1.9 und Lemma 1.4 auch $\mathsf{conv}(A \cup B)$ kompakt in $\mathcal{V}_\infty(S)$, und also $\mathsf{conv}(A \cup B) \cap \mathcal{V}(S) = \mathsf{conv}(A \cup B)$ kompakt in $\mathcal{V}(S)$.

**Bemerkung.** Tatsächlich ist die Scott-Topologie auf $\mathcal{V}(S)$ gerade die Topologie, die von der Scott-Topologie auf $\mathcal{V}_\infty(S)$ auf $\mathcal{V}(S)$ induziert wird.

## 1.4 Der Smyth-Powerdomain über $\mathcal{V}(S)$

Wir können nun den Smyth-Powerdomain über $\mathcal{V}(S)$ definieren, der totale Korrektheit modelliert.

**Definition 1.14.** Der **Smyth-Powerdomain** über $\mathcal{V}(S)$ besteht aus den nichtleeren konvexen kompakten saturierten Teilmengen von $\mathcal{V}(S)$ und wird mit $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ bezeichnet.

Wir betrachten als Ordnung auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ die **umgekehrte** Mengeninklusion. Dadurch entsteht eine dcpo. Als Topologie darauf betrachten wir die aus dieser Ordnung resultierende Scott-Topologie.

Der Smyth-Powerdomain $\mathfrak{P}_{\text{Sm}}\mathcal{V}_\infty(S)$ über dem erweiterten probabilistischen Powerdomain ist wieder ein topologischer Kegel, aber nicht mit der punktweisen Addition und Skalarmultiplikation. Vielmehr muß man $A +_S B := \uparrow(A + B)$ und $r \cdot_S A := \uparrow(r \cdot A)$ wählen.

Wir werden auch auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ addieren und mit Skalaren multiplizieren. Der Raum $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ ist aber weder unter Addition noch unter Multiplikation mit Skalaren $r > 1$ abgeschlossen.

Es ist allerdings für unsere Zwecke hinreichend, Konvexkombinationen von Elementen aus $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ zu bilden. Daß dies in $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ immer möglich ist, zeigt das folgende Lemma.

**Lemma 1.15.** *Für $r \in [0,1]$ und $A, B \in \mathfrak{P}_{Sm}\mathcal{V}(S)$ ist $r \cdot A + (1-r) \cdot B$ eine obere Menge, es gilt also die Gleichheit*

$$r \cdot A + (1-r) \cdot B = \uparrow\Big(r \cdot A + (1-r) \cdot B\Big).$$

*Ferner ist $r \cdot A + (1-r) \cdot B \in \mathfrak{P}_{Sm}\mathcal{V}(S)$.*

**Beweis.** Für $r \in \{0,1\}$ ist nichts zu zeigen.

Sei nun $x \in A, y \in B$ und $r \in (0,1)$ gegeben und $p = r \cdot x + (1-r) \cdot y$. Es ist zu zeigen, daß $\uparrow p$ in $r \cdot A + (1-r) \cdot B$ enthalten ist. Sei hierfür $p' \geq p$.

Nun sei $d := p' - p$. In Kegeln gibt es a priori keine Subtraktion, wir können jedoch die Differenz formal bilden (durch punktweise Differenz in $\mathbb{R}$ und wegen $p' \geq p$ ist auch $d \in \mathcal{V}(S)$.

Dann gilt $r \cdot (x+d) + (1-r) \cdot (y+d) = p'$. Hierbei sind $x+d$ und $y+d$ zunächst Elemente von $\mathcal{V}_\infty(S)$ und es ist unklar, ob sie auch Elemente von $\mathcal{V}(S)$ sind. Ist dies der Fall, so wählen wir $a = (x+d) \geq x$ und $b = (y+d) \geq y$. Somit ist $a \in A$ und $b \in B$ und wir haben die gewünschte Darstellung für $p'$.

Sei andernfalls o.B.d.A. $(x+d)(S) > 1$. In diesem Falle existiert wegen $x(S) \leq 1$ ein $\alpha \in [0,1)$ mit $(x + \alpha d)(S) = 1$.

Es ist $r < 1$, so daß wir

$$\beta := \frac{1 - r\alpha}{1-r} \quad ,$$

setzen können. Damit gilt

$$\begin{aligned} r(x + \alpha d) + (1-r)(y + \beta d) &= rx + r\alpha d + (1-r)y + (1-r)\beta d \\ &= p + d \\ &= p'. \end{aligned}$$

Für $a := x + \alpha d$ gilt $a \in \mathcal{V}(S)$ und $a \geq x$, entsprechend ist $a \in A$. Weiterhin ist $b := y + \beta d \geq y$. Wenn wir nun zeigen, daß $b(S) \leq 1$ gilt, so ist $b \in B$ und wir haben $p'$ in der gewünschten Form als Konvexkombination dargestellt.

Wäre $b(S) > 1$, so wäre wegen $a(S) = 1$ und $r > 0$ auch $p'(S) > 1$. Das ist aber widersprüchlich dazu, daß $p' \in \mathcal{V}(S)$ ist. Also ist $b(S) \leq 1$, was den Beweis dafür, daß $r \cdot A + (a - r) \cdot B$ eine obere Menge ist, abschließt.

Abbildung 4 veranschaulicht die Situation.

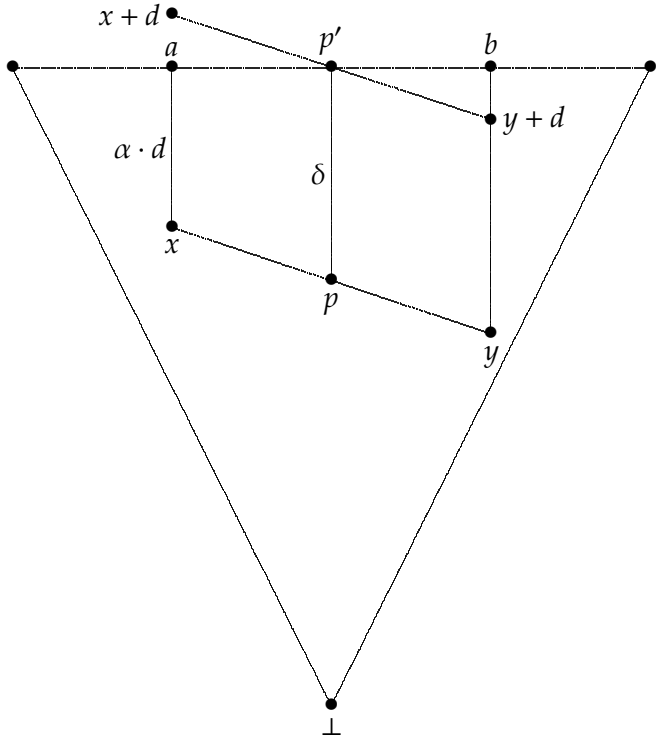


Abbildung 4: Konvexkombinationen von Smyth-Mengen sind saturiert.

Aus dem Bisherigen folgt $r \cdot A + (1 - r) \cdot B = r \cdot_S A +_S (1 - r) \cdot_S B$. Da $\cdot_S$ und $+_S$ stetig sind, ist $r \cdot A + (1 - r) \cdot B$ schon eine kompakte saturierte Menge. Trivialerweise ist die Menge auch konvex und nichtleer. □

Um *worst-case*-Aussagen über das Verhalten von Programmen zu treffen, werden wir Infima verwenden.

Wir betrachten nun deswegen die Stetigkeit von Infimumsabbildungen.

Ein stetiger Bereich, in dem binäre Infima extistieren und die Infimumsbildung Scott-stetig ist, heißt **stetiger Infimumshalbverband**. Mit der üblichen Ordnung ist $[0, 1]$ ein stetiger Infimumshalbverband.

Wegen Satz 0.1 ist dann auch $\mathcal{V}(S)$ ein stetiger Infimumshalbverband.

**Proposition 1.16.** *Die Infimumsabbildung aus dem Smyth-Powerdomain über einem Infimumshalbverband in diesen Halbverband*

$$\begin{aligned}\mathsf{INF} \;:\; \mathfrak{P}_{Sm}\mathcal{Y}(S) &\longrightarrow \mathcal{V}(S)\\ Q &\longmapsto \bigvee\nolimits^{\uparrow}\Big\{\inf F \;\Big|\; F \text{ ist endlich und } Q \subseteq \mathsf{int}{\uparrow}F\Big\}\end{aligned}$$

*ist wohldefiniert und Scott-stetig.*

**Beweis.** Siehe [TKP05, Lemma 4.21]. □

**Lemma 1.17.** *Für eine Scott-stetige Funktion $f : \mathcal{V}(S) \longrightarrow [0,1]$ ist*

$$\begin{aligned}\mathsf{INF}\, f \;:\; \mathfrak{P}_{Sm}\mathcal{Y}(S) &\longrightarrow [0,1]\\ P &\longmapsto \bigwedge f[P] = \min f[P]\end{aligned}$$

*stetig.*

**Beweis.** Für stetiges $f$ ist $f[P]$ Scott-kompakt in $[0,1]$, das heißt $f[P]$ hat ein kleinstes Element $a$, so daß $\bigwedge f[P] = \min f[P] = a$ gilt.

Die Infimumsabbildung ist monoton, denn für $P \leq P'$ gilt $P' \subseteq P$, also $f[P'] \subseteq f[P]$. Das kleinste Element $a'$ von $f[P']$ ist also Element von $f[P]$ und somit gilt $a \leq a'$.

Gerichtete Suprema in $\mathfrak{P}_{Sm}\mathcal{Y}(S)$ sind gerichtete Schnitte, somit folgt das Erhalten gerichteter Suprema direkt, denn $f[\bigcap_i P_i] \neq \bigcap_i f[P_i]$ aber $\wedge f[\bigcap_{i}^{\downarrow} P_i] = \bigvee_i^{\uparrow} \wedge f[P_i]$. □

**Lemma 1.18.** *Seien $X, Y$ Bereiche und $f : X \times Y \longrightarrow [0,1]$ Scott-stetig. Dann ist die Abbildung*

$$\begin{aligned}\mathsf{INF}_X\, f \;:\; Y &\longrightarrow [0,1]\\ y &\longmapsto \bigwedge_{x \in X} f(x,y)\end{aligned}$$

*Scott-stetig.*

**Beweis.** Der Fall $X = \varnothing$ ist trivial. Andernfalls betrachten wir das Urbild der offenen Menge $(r,1] \subseteq [0,1]$.

$$\Big(\mathsf{INF}_X\, f\Big)^{-1}\Big((r,1]\Big) = \left\{ y \in Y \;\middle|\; \bigwedge_{x \in X} f(x,y) > r \right\} =: M.$$

Es ist $M = {\uparrow}M$, da $f$ monoton ist.

Sei $D \subseteq Y$ gerichtet mit $\bigvee^{\uparrow} D \in M$, dann gibt es ein $x \in X$ mit $f(x, \bigvee^{\uparrow} D) > r$. Da $f$ stetig ist, gilt $\bigvee^{\uparrow}_{d \in D} f(x,d) = f(x, \bigvee^{\uparrow} D) > r$. Man kann die Scott-offene Menge nicht nurch gerichtete Suprema erreichen, also gibt es auch ein $d \in D$ mit $d(x,d) > r$, deshalb ist $d \in M$.

Also ist $D$ Scott-offen und somit ist $\mathsf{INF}_X\, f$ Scott-stetig. □

**Lemma 1.19.** *Es sei $f : X \longrightarrow Y$ eine Scott-stetige Funktion zwischen zwei Bereichen. Dann ist für beliebige Teilmengen $A \subseteq X$ stets*

$$\bigwedge f[A] = \bigwedge f[\uparrow A].$$

**Beweis.** Wegen $A \subseteq \uparrow A$ gilt sofort $\bigwedge f[A] \geq \bigwedge f[\uparrow A]$. Für $a' \in \uparrow A$ gibt es stets ein $a \in A$ mit $a \leq a'$. Da $f$ monoton ist, gilt $f(a) \leq f(a')$ und wegen $\bigwedge f[A] \leq f(a)$ folgt, daß $\bigwedge f[A]$ eine untere Schranke von $f[\uparrow A]$ ist, also gilt auch $\bigwedge f[A] \leq \bigwedge f[\uparrow A]$. □

Es werden in der Semantik zunächst Mengen auftreten, die kompakt und konvex, nicht aber saturiert sind. Es ist wichtig, daß ihre Saturierung wieder kompakt und konvex ist, so daß der Operator $\uparrow$ aus diesen Mengen Elemente von $\mathfrak{P}_{\mathrm{Sm}}\mathcal{V}(S)$ macht.

**Satz 1.20.** *Für eine nichtleere kompakte konvexe Teilmenge $A \subseteq \mathcal{V}(S)$ ist $\uparrow A \in \mathfrak{P}_{Sm}\mathcal{V}(S)$.*

**Beweis.** Offenbar ist $\uparrow A$ nichtleer und saturiert.

Jede offene Überdeckung von $A$ ist auch eine offene Überdeckung von $\uparrow A$ und umgekehrt, da Scott-offene Mengen saturiert sind. Also sind auch endliche Teilüberdeckungen von $A$ endliche Teilüberdeckungen von $\uparrow A$, weshalb $\uparrow A$ kompakt ist.

Um die Konvexität von $\uparrow A$ nachzuweisen, seien $a, b \in \uparrow A$ gegeben. Wir müssen nun zeigen, daß die Verbindungsstrecke, also die Menge

$$\Big\{ r \cdot a + (1-r) \cdot b \;\Big|\; r \in [0,1] \Big\}$$

in $\uparrow A$ enthalten ist.

Da $a$ und $b$ in $\uparrow A$ liegen, gibt es $a', b' \in A$ mit $a' \leq a$ und $b' \leq b$. Für $r \in [0,1]$ ist stets $x_r := r \cdot a' + (1-r) \cdot b' \in A$ und es ist $x_r \leq r \cdot a + (1-r) \cdot b$. Deswegen ist $r \cdot a + (1-r) \cdot b \in \uparrow A$. □

## 1.5 Die Hausdorfftopologie auf $\mathcal{V}(S)$

In diesem Abschnitt betrachten wir die übliche Hausdorfftopologie auf $[0,1]$ und die durch sie induzierte Topologie auf $\mathcal{V}(S)$. Wir werden zeigen, daß $\mathcal{V}(S)$ mit dieser Topologie ein kompakter $T_2$-Raum ist und der Smyth-Powerdomain gerade die in dieser Topologie abgeschlossenen saturierten konvexen und nichtleeren Mengen enthält.

**Definition 1.21.** Die übliche Hausdorfftopologie auf $[0,1]$ definiert durch die Produkttopologie eine Hausdorfftopologie auf $\big[S \longrightarrow [0,1]\big] \cong \prod_{s \in S} [0,1]$. Durch diese wird auch auf dem Teilraum $\mathcal{V}(S)$ eine $T_2$-Topologie induziert.

Diese Topologie nennen wir $\mathcal{H}$.

**Satz 1.22.** *Der Raum $\big(\mathcal{V}(S), \mathcal{H}\big)$ ist kompakt.*

**Beweis.** Da $[0,1]$ mit der üblichen $T_2$-Topologie kompakt ist, ist der Produktraum $\Big[S \longrightarrow [0,1]\Big]$ kompakt (Satz von Tychonoff).
Da $f \longmapsto \mu_f(S) : \mathcal{V}(S) \longrightarrow [0,1]$ bezüglich der Hausdorfftopologie stetig ist, definiert die Einschränkung

$$\sum_{s \in S} f(s) \leq 1$$

als Urbild der abgeschlossnen Menge $[0,1]$ eine abgeschlossene Teilmenge dieses Produktraums. Deswegen ist $\mathcal{V}(S)$ als abgeschlossener Teilraum eines kompakten Raums selbst kompakt. □

Wir werden das folgende Lemma benötigen, das direkt aus [GHK+03, Thm VI-6.18] folgt.

**Lemma 1.23.** *Sei $\mathcal{H}$ eine $T_2$-Topologie auf einem stetigen Bereich $D$, die feiner ist als die Scott-Topologie. Ferner gebe es für jedes Paar $x, y \in D$ mit $y \not\leq x$ stets zwei Mengen $U \in \Sigma\Big(\mathcal{V}(S)\Big)$ und $V \in \mathcal{H}$ mit $y \in U, x \in V$ und $U \cap V = \emptyset$.*

*Dann stimmt $\mathcal{H}$ mit der Patch-Topologie der Scott-Topologie überein.*

**Beweis.** Siehe [GHK+03, Thm VI-6.18] □

**Theorem 1.24.** *Der Smyth-Powerdomain $\mathfrak{P}_{Sm}\mathcal{V}(S)$ besteht genau aus den saturierten konvexen und nichtleeren Teilmengen von $\mathcal{V}(S)$, die bezüglich $\mathcal{H}$ abgeschlossen sind.*

**Beweis.** Wir zeigen zunächst, daß saturierte konvexe nichtleere und $\mathcal{H}$-abgeschlossene Teilmengen von $\mathcal{V}(S)$ stets Scott-kompakt, also auch Mengen in $\mathfrak{P}_{Sm}\mathcal{V}(S)$ sind:

Abgeschlossene Mengen in $(\mathcal{V}(S), \mathcal{H})$ sind stets $\mathcal{H}$-kompakt, denn $\mathcal{V}(S)$ selbst ist $\mathcal{H}$-kompakt. Die Hausdorff-Topologie auf $[0,1]$ ist feiner, als die Scott-Topologie, also ist auch die induzierte $T_2$-Topologie $\mathcal{H}$ feiner als die Scott-Topologie auf $\mathcal{V}(S)$. Entsprechend impliziert $\mathcal{H}$-kompakt auch Scott-kompakt.

Nun zeigen wir, daß Mengen in $\mathfrak{P}_{Sm}\mathcal{V}(S)$ stets $\mathcal{H}$-abgeschlossen, also $\mathcal{H}$-kompakt sind:

Hierfür überprüfen wir die Voraussetzungen des obigen Lemmas. Seien $x, y \in \mathcal{V}(S)$, $y \not\leq x$ und sei

$$S_y := \Big\{ s \in S \;\Big|\; y(s) > x(s) \Big\}.$$

Wegen $y \not\leq x$ ist $S_y$ nicht leer. Ferner sei $S_0 \subseteq S_y$ eine nichtleere endliche Teilmenge.
Wir setzen nun

$$U = \left\{ \mu \in \mathcal{V}(S) \;\middle|\; s \in S_0 \Longrightarrow \mu(s) > \frac{x(s) + y(s)}{2} \right\}$$
$$V = \left\{ \mu \in \mathcal{V}(S) \;\middle|\; s \in S_0 \Longrightarrow \mu(s) < \frac{x(s) + y(s)}{2} \right\}.$$

Es ist wegen $S_y \neq \emptyset$ der Schnitt von $U$ und $V$ leer, $U$ ist Scott-offen und $V$ ist $\mathcal{H}$-offen, was man sofort erkennt, wenn man die entsprechenden Projektionen auf ein $s \in S$ betrachtet.

Nach Lemma 1.23 ist $\mathcal{H}$ also die von der Scott-Topologie und von deren co-kompakter Topologie erzeute Topologie, die Patch-Topologie der Scott-Topologie.

Das Komplement einer Scott-kompakten oberen Menge $A \in \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ ist also offen in $\mathcal{H}$, somit sind die Mengen im Smyth-Powerdomain stets $\mathcal{H}$-abgeschlossen. □

*In my experience, there is no such thing as luck.*
*(Obi-Wan Kenobi)*

# 2 Dämonen, Würfel und pGCL

## 2.1 Überblick

Im Gegensatz zur Semantik von deterministischen Programmiersprachen, die man mittels Topologie, Bereichstheorie und Kategorientheorie bereits seit den 70er Jahren untersucht, sind die ersten Arbeiten über Powerdomains (in deutschsprachigen Veröffentlichungen auch Potenzbereiche genannt) erst um 1980 erschienen.

Wenn deterministische Programme auf einer Maschine mit Zustandsraum $S$ ausgeführt werden, dann entsprechen sie Scott-stetigen Abbildungen in $\left[S \longrightarrow S_\perp\right]$. Je nachdem in welchem Zustand ein Programm startet, liefert seine Ausführung einen neuen Zustand – oder es terminiert nicht. Diese Möglichkeit der Divergenz wird durch Hinzufügen des Infimums-Elementes $\perp$ zum Zustandsraum eingeräumt.

Eine nondeterministische imperative Programmiersprache beinhaltet Befehle, deren Ausgang man nicht vorhersehen kann. Das ist auf zwei verschiedenen Ebenen möglich. Zunächst könnte die Sprache einen Befehl anbieten, der nach dem Zufallsprinzip mit einer gewissen Wahrscheinlichkeit A ausführt und ansonsten B. Programmiersprachen, die Zufallszahlen produzieren können, bieten im Grunde diese Form von Nondeterminismus an. Es handelt sich in gewissem Sinne um die Möglichkeit zu würfeln. Man nennt diese Möglichkeit auch *probabilistischen* Nondeterminismus. Vorteile und Anwendungen eines solchen Kommandos liegen auf der Hand: Viele Netzwerkprotokolle, kryptographische Algorithmen und selbst einfachste Spiele kommen ohne das Erzeugen von Zufallszahlen nicht aus. Auch der Miller-Rabin-Test, der effizienteste Primzahltest, der zur Zeit bekannt ist, setzt Zufallszahlen ein. Mit den Mitteln der Wahrscheinlichkeitstheorie und der Statistik kann man Aussagen über solche Programme treffen.

Hier soll darüber hinaus eine zweite Form des Nondeterminismus betrachtet werden, der *nichtprobabilistische* Nondeterminismus. Dabei handelt es sich um die Möglichkeit, an einer gewissen Stelle im Programmtext den Befehl „führe A oder B aus" zu geben. Dabei wird nicht spezifiziert, auf welcher Grundlage die Entscheidung fallen soll, was genau tatsächlich passiert.

Um Programme zu modellieren, die mit einem größeren System interagieren (zum Beispiel dem Betriebssystem oder dem Benutzer) oder um Parallelität zu modellieren, in der man nicht weiß in welcher Reihenfolge verschiedene Programmteile abgearbeitet werden, ist diese Form des Nondeterminismus nützlich.

Die Form, in der wir nichtprobabilistischen Nondeterminismus behandeln, orientiert sich zunächst an Smyth und heißt auch *dämonischer* Nondeterminismus. Andere Ansätze sind der *erratische* Nondeterminismus (Plotkin) und der *angelische* Nondeterminismus (Hoare). Letzterer wird uns später beschäftigen, wenn wir uns partiellen Korrektheitsaussagen widmen.

Smyths Nondeterminismus heißt *dämonisch*, weil wir bei seinem Auftreten stets davon ausgehen, daß zwischen den beiden Alternativen diejenige gewählt wird, die für unser derzeitiges Interesse weniger erstrebenswert ist. Man rechnet meist mit worst-case-Szenarien. Wenn ein solches Programm bei einer der nichtprobabilistischen Abzweigungen unter gewissen Voraussetzungen die Möglichkeit hat, einen Weg zu wählen, der es zur Divergenz bringt, dann gehen wir davon aus, daß dies jedesmal geschieht. Wir stellen uns vor, daß ein bösartiger Dämon in der Maschine sitzt, genau weiß, was uns nicht gefallen würde und eben diese Verzweigung im Programmablauf wählt.

Die beiden Formen des Nondeterminismus interagieren zusätzlich, wenn man erwartet, daß jede probabilistische Auswahl mit den konkreten jeweiligen Wahrscheinlichkeiten $p$ und $1 - p$ zwischen A und B in der Spezialisierungsordnung auf dem Raum der Programme *besser* ist als die dämonische Auswahl zwischen A und B.

Das Programm „wähle beliebig zwischen A und B" wird durch jede konkrete Instanz „Führe A mit Wahrscheinlichkeit $p$ aus, sonst führe B aus" implementiert und somit verfeinert.

Wenn deterministische Programme in ihrer direkten denotationellen Semantik gerade Scott-stetige Funktionen von $S$ nach $S_\perp$ sind, was ist dann die direkte denotationelle Semantik nondeterministischer Programme? Diese Frage wurde auf unterschiedliche Arten beantwortet. Drei *Powerdomains* werden heute verwendet, um nichtprobabilistischen Nondeterminismus zu modellieren. Plotkin veröffentlichte 1976 seine Powerdomain-Konstruktion [Plo76], die Smyth 1978 vereinfachte [Smy78]. Der Hoare-Powerdomain wird gebraucht, um partielle Korrektheit zu modellieren. Da diese Form der Korrektheit „optimistischer" ist, als totale Korrektheit, wird der dämonische Nondeterminismus im Hoare-Fall auch häufig als nicht dämonisch, sondern als *engelsartig* (englisch: *angelic*) bezeichnet.

Um sowohl probabilistischen als auch dämonischen Nondeterminismus zu fassen, verwenden wir für totale Korrektheitsaussagen den in Definition 1.14 eingeführten Smyth-Powerdomain über dem Raum der Subverteilungen auf einem diskreten, abzählbaren Zustandsraum. Später werden wir dann den Hoare-Powerdomain über dem Raum der Subverteilungen verwenden, um über partielle Korrektheit zu sprechen.

Bevor wir die Syntax von pGCL definieren, deuten wir an, wie wir die beiden Formen des Nondeterminismus syntaktisch und semantisch handhaben wollen.

## 2.2 Probabilismus

Um probabilistischen Nondeterminismus zu fassen, gibt es in pGCL ein syntaktisches Konstrukt $P \,{}_p\!\oplus\, Q$, wo $p$ eine Zahl zwischen 0 und 1 ist und $P$ und $Q$ zwei pGCL-Programme sind.

Von einer pGCL-Maschine erwarten wir, daß sie beim Auftreten dieses Konstrukts mit der Wahrscheinlichkeit $p$ das Programm $P$ ausführt und ansonsten das Programm $Q$ ausführt.

**Bemerkung.** Es ist durch wiederholte Anwendung von

$$\texttt{a:=0} \underset{\frac{1}{2}}{\oplus} \texttt{a:=1}$$

möglich, beliebig lange zufällige 0/1-Ketten zu erzeugen. Somit läßt sich ein Meta-Befehl `random`$(m, M)$ definieren, der eine ganze Zufallszahl $r$ mit $m \leq r \leq M$ erzeugt.

Die Wahrscheinlichkeitsrechnung beantwortet die Frage, wie man die denotationelle Semantik eines probabilistischen Programms definieren sollte. Während ein deterministisches Programm bei Termination jedem Startzustand einen Endzustand zuordnet, wird ein probabilistisches Programm aus einem Startzustand eine Subverteilung $\mu$ auf dem Zustandsraum erzeugen. Die Größe $\mu(S) \leq 1$ ist dabei die Terminierungswahrscheinlichkeit.

Die direkte denotationelle Semantik eines solchen Programmes $P$ ist (notwendigerweise eine Scott-stetige) Funktion $[\![P]\!] : S \longrightarrow \mathcal{V}(S)$.

## 2.3 Nondeterminismus

Um nichtprobabilistischen Nondeterminismus zu fassen, gibt es in pGCL ein syntaktisches Konstrukt $P \sqcap Q$, wo $P$ und $Q$ zwei pGCL-Programme sind.

Von einer pGCL-Maschine erwarten wir, daß sie beim Auftreten dieses Konstrukts entweder das Programm $P$ ausführt oder das Programm $Q$ ausführt.

Wenn $P$ und $Q$ zwei probabilistische Programme sind, die aus gegebenem Startzustand $s \in S$ die beiden Verteilungen $\mu$ und $\nu$ erzeugen, so müssen wir damit rechnen, daß $P \sqcap Q$ von diesen beiden Verteilungen diejenige liefert, die uns in der jeweiligen Anwendung weniger gelegen kommt. Jede konkrete probabilistische Entscheidung zwischen den beiden soll auch eine zulässige Implementierung des dämonischen Auswahloperators sein.

Um die Unsicherheit darüber zu fassen, welche Verteilung nach dem Auftreten von dämonischem Nichtdeterminismus gilt, liefert die direkte denotationelle Semantik eines dämonischen nondeterministischen Programms die Menge von Verteilungen, die aus dem Startzustand $s$ hervorgehen *können*. Diese Mengen sind, solange wir totale Korrektheit modellieren, nichtleer, kompakt, konvex und saturiert. Die Semantik ist dann eine Scott-stetige Funktion $[\![P]\!] : S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$.

## 2.4 pGCL

Wir führen die gleiche (turingmächtige) Programmiersprache ein wie McIver und Morgan in [MM04]. Sie heißt **pGCL** und ist eine Anreicherung von Dijkstras *guarded command language* GCL um die beiden vorgestellten Operationen, die die beiden Probabilismus und Nondeterminismus erlauben.

Wenn wir die Syntax unserer Programmiersprache angeben, ist diese schon an zwei Stellen eng mit der direkten Semantik der Sprache verwandt: Erstens definieren wir

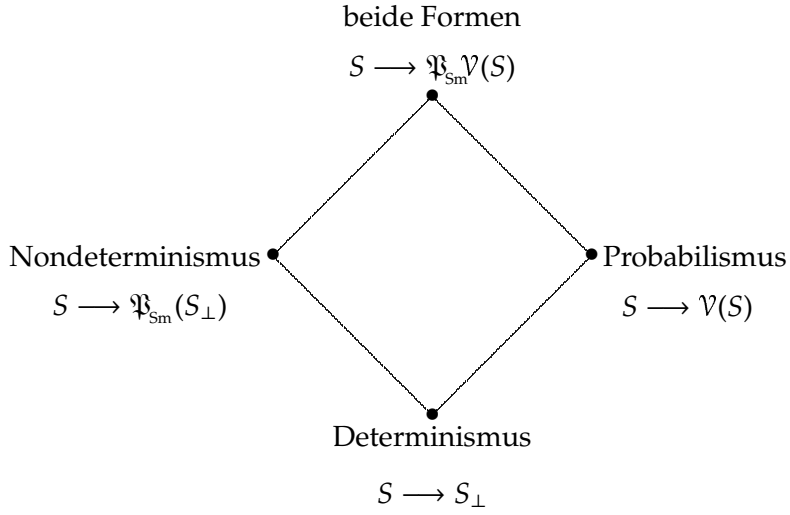


Abbildung 5: Nondeterminismus im Smyth-Powerdomain

keine Syntax für die booleschen Ausdrücke im Schleifenkopf bzw. der bedingten Verzweigung. Solche booleschen Ausdrücke könnten so aussehen:

```
(x-y>3) and z=7
```

Von allen Zuständen in $S$ werden gerade einige diese boolesche Bedingung erfüllen und andere nicht. Boolesche syntaktische Ausdrücke entsprechen also semantisch echten Attributen $b \subseteq S$. Wir vereinfachen die folgende Arbeit, indem wir für einen syntaktischen Ausdruck zum Attribut $b$ einfach auch $b$ schreiben.

Auch Wertzuweisungen wie `x := x + a;` wollen wir nicht komplett syntaktisch behandeln sondern identifizieren sie direkt mit den bewirkten Scott-stetigen Funktionen $f : S \longrightarrow S$ und wir führen wie bei [TKP05] einen Befehl $\texttt{assign}_f$ für einfache Operationen $f$ ein. Dabei wird bewußt von einer Definition der *einfachen Operationen* abgesehen – obwohl in diesen Programmzeilen die „eigentliche Arbeit" erfolgt, stellen die Basisbefehle weder für die direkte Semantik noch für die *predicate transformer*-Semantiken eine Herausforderung dar.

Um diese beiden Ungenauigkeiten in der Unterscheidung von Syntax und Semantik auszuräumen, müßte man syntaktisch boolesche und ganzzahlige Ausdrücke, Operationen, Variablen, natürliche Konstanten etc. definieren. Glynn Winskel tut dies beispielsweise in [Win93]. Uns soll die folgende Definition der Syntax von pGCL genügen.

**Definition 2.1.** Die Menge der syntaktisch nach den folgenden Regeln geformten pGCL-Terme heißt **Programme** und wird mit Prog bezeichnet.

Basisfälle:

| | |
|---|---|
| $\texttt{assign}_f$ | für Scott-stetige Funktionen $f : S \longrightarrow S$. |
| `abort` | |
| `skip` | |

Rekursiver Termaufbau

| | |
|---|---|
| $P\,\texttt{;}\,Q$ | für zwei Programme $P$ und $Q$. |
| `if` $b$ `then` $P$ `else` $Q$ `fi` | für Programme $P$, $Q$ und ein echtes Prädikat $b$. |
| `while` $b$ `do` $P$ `od` | für ein Programm $P$ und ein echtes Prädikat $b$. |
| $P \,{}_p\!\oplus\, Q$ | für Programme $P$, $Q$ und $0 < p < 1$. |
| $P \sqcap Q$ | für Programme $P$ und $Q$. |

Die direkte Semantik dieser Befehle wird im nächsten Kapitel definiert.

**Bemerkung.** Die Sprache ist nicht dadurch eingeschränkt, daß $b$ in den Konstruktionen `if` und `while` ein echtes, also kein probabilistisches Prädikat sein darf. Es ist eine einfache Fingerübung, durch Einführung einer Hilfsvariablen, die in jedem Schleifendurchlauf eine neue Zufallszahl zugewiesen bekommt, probabilistische Prädikate als Schleifenabbruchbedingung zu simulieren. Ebenso einfach läßt sich die Fallunterscheidung mittels einer zufälligen Hilfsgröße zwischen 0 und 1 auf probabilistische Prädikate erweitern.

Beispielsweise läßt sich dieses Programm (nicht pGCL Syntax)

$$\texttt{while } \tfrac{1}{3} \texttt{ do } P \texttt{ od}$$

in pGCL wie folgt realisieren:

$$\texttt{a=1} \,{}_{\frac{1}{3}}\!\oplus\, \texttt{a=0;}$$
$$\texttt{while (a=1) do } P\texttt{; a=1} \,{}_{\frac{1}{3}}\!\oplus\, \texttt{a=0 od}$$

*I'm offering you my body and you're offering me semantics?*
*(Caitlin in Clerks)*

# 3 Direkte Semantik von pGCL

## 3.1 Verkettung von Programmen

Der Zustandsraum $S$, auf dem unsere Programme operieren, ist ein abzählbarer diskreter Bereich.

Der Endzustand eines Programmes ist jedoch eine Menge $M \in \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ von Subverteilungen auf $S$, zwischen denen dann der Dämon wählt.

Die direkte denotationelle Semantik eines Programms ist also eine Funktion von $S$ nach $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$.

In dieser Form kann man der Hintereinanderausführung zweier Programme $P$ und $Q$ nicht ohne Weiteres eine Semantik zuweisen, da $[\![Q]\!]$ als Eingabe einen Zustand erwartet, $[\![P]\!]$ als Ausgabe aber ein Element des Smyth-Powerdomains liefert. Dementsprechend ist es notwendig, $[\![Q]\!]$ auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ fortzusetzen.

Hierzu überlegen wir uns zunächst, wie $S$ als Teilmenge von $\mathcal{V}(S)$ und $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ verstanden werden kann.

**Definition 3.1.** Wir definieren die folgenden Funktionen:

$$\begin{aligned} \eta \,:\, S &\longrightarrow \mathcal{V}(S) \\ \sigma &\longmapsto \eta_\sigma \\ i \,:\, \mathcal{V}(S) &\longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S) \\ \mu &\longmapsto \uparrow\mu. \end{aligned}$$

Daß $i$ wohldefiniert ist, beweisen wir im folgenden Lemma:

**Lemma 3.2.** *Sei $\mu \in \mathcal{V}(S)$, dann ist die Menge $\uparrow\mu$ Element von $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$, also kompakt, saturiert und konvex.*

**Beweis.** Per Definition sind Mengen der Form $\uparrow\mu$ saturiert.

Wir zeigen nun die Konvexität: Seien $a, b \in \uparrow\mu$, also $\mu \sqsubseteq a$, $\mu \sqsubseteq b$. Dann ist

$$r \cdot a + (1-r) \cdot b \geq r \cdot \mu + (1-r) \cdot \mu = \mu.$$

Die Scott-Kompaktheit folgt aus der Existenz eines kleinsten Elements. □

**Proposition 3.3.** *Die Funktion $\eta$ ist eine Einbettung von $S$ nach $\mathcal{V}(S)$, die Funktion $i$ ist eine Einbettung von $\mathcal{V}(S)$ nach $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$.*

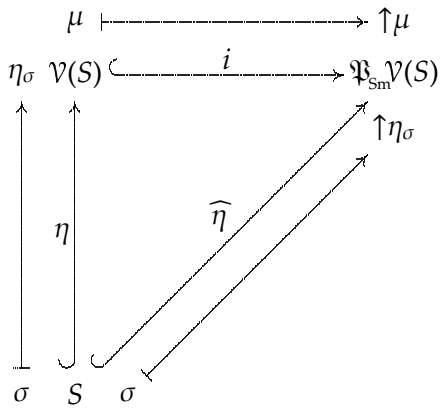


Abbildung 6: Einbettung von $S$ in $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$

**Beweis.** Zwei Punktauswertungen $\eta_\sigma$ und $\eta_{\sigma'}$ sind unterschiedlich, falls $\sigma \neq \sigma'$. Ebenso gilt in einem $T_0$-Raum offenbar $\uparrow\mu \neq \uparrow\mu'$ für $\mu \neq \mu'$. Also sind die Funktionen $\eta$ und $i$ injektiv.

Per Definition ist $\eta_\sigma \in \mathcal{V}(S)$.

Somit wäre geklärt, daß $\eta$ eine Injektion von $S$ nach $\mathcal{V}(S)$ ist, und auch daß $i$ eine Injektion von $\mathcal{V}(S)$ nach $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ ist.

Die Scott-Stetigkeit von $\eta$ steht nicht in frage, da $S$ diskret ist. Betrachten wir nun die Einbettung $i$:

Für $\mu \leq \mu'$ gilt $\uparrow\mu' \subseteq \uparrow\mu$ und somit $\uparrow\mu \leq \uparrow\mu'$, denn die Ordnung auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ ist durch umgekehrte Inklusion definiert.

Für $\mu = \bigvee\!\!\!\nearrow \mu_j$ haben wir $\uparrow\mu \subseteq \bigcap \uparrow\mu_j$, denn $\mu \geq \mu_j$ für alle $j \in J$. Ist andererseits $\nu \in \bigcap \uparrow\mu_j$, dann ist $\nu$ eine obere Schranke aller $\mu_j$, also $\nu \geq \mu$ bzw. $\nu \in \uparrow\mu$.

Dementsprechend gilt

$$i\Big(\bigvee\!\!\!\nearrow \mu_j\Big) = i(\mu) = \uparrow\mu = \bigcap \uparrow\mu_j = \bigvee\!\!\!\nearrow i(\mu_j),$$

so daß auch $i$ Scott-stetig ist. □

**Bemerkung.** Wie im Diagramm bezeichnen wir die Einbettung $i \circ \eta : S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ mit $\widehat{\eta}$ – wo keine Verwechslungsgefahr besteht gegebenenfalls auch kurzerhand mit $\eta$.

**Bemerkung.** Es gilt $\uparrow\eta_\sigma = \uparrow\{\eta_\sigma\} = \{\eta_\sigma\}$, da Punktauswertungen maximale Elemente in $\mathcal{V}(S)$ sind.

Nun wollen wir Funktionen $f : S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ auf $\mathcal{V}(S)$ und auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ fortsetzen. Wir benötigen hierfür eine spezielle Interpretation des kartesischen Produkts von Mengen als „Auswahlfunktionen".

**Definition 3.4.** Für ein System von Mengen $(A_i)_{i\in I}$ ist das **Produkt** der $A_i$ definiert als:

$$\prod_{i\in I}(A_i) \coloneqq \left\{ g \,:\, I \longrightarrow \bigcup A_i \;\middle|\; \big(\forall i \in I\big)\; g(i) \in A_i \right\}$$

**Proposition 3.5.** *Die folgenden Eigenschaften übertragen sich von $A_i$ auf $\prod_{i\in I} A_i$:*

(i) *Wenn alle $A_i$ nichtleer sind, ist $\prod_{i\in I} A_i$ nichtleer (Auswahlaxiom).*

(ii) *Wenn alle $A_i$ als Teilmengen eines Posets $X$ saturiert sind, so ist auch $\prod_{i\in I} A_i$ eine saturierte Teilmenge der punktweise geordneten Funktionen von $I$ nach $X$.*

(iii) *Wenn alle $A_i$ als Teilmengen eines Kegels $C$ konvex sind, dann ist auch $\prod_{i\in I} A_i$ als Teilmenge des Kegels $C^I$ konvex.*

(iv) *Wenn alle $A_i$ als Teilmengen eines stetigen Bereichs $X$ mit $\bot$ Scott-kompakt sind, so ist auch $\prod_{i\in I} A_i$ als Teilmenge von $\prod_{i\in I} X$ Scott-kompakt.*

**Beweis.**

(i) Diese Aussage ist das Auswahlaxiom, das wir hier voraussetzen.

(ii) Es sei $p \in \prod_{i\in I} A_i$ ein Element des Produkts. Es sei $f : I \longrightarrow A$ eine Funktion mit $p \leq f$. Dann ist für jedes $i \in I$ stets $p(i) \leq f(i)$. Da $A_i$ saturiert ist, ist auch $f(i) \in A_i$. Dies gilt für alle $i$, also ist $f \in \prod_{i\in I} A_i$.

(iii) Seien $g$ und $g'$ Elemente von $\prod_{i\in I} A_i$. Für jedes $i$ sind $g(i)$ und $g'(i)$ Elemente der konvexen Menge $A_i$. Deswegen ist auch $p \cdot g(i) + (1-p) \cdot g'(i)$ ein Element von $A_i$. Also ist $p \cdot g + (1-p) \cdot g' \in \prod_{i\in I} A_i$.

(iv) Siehe Satz 0.1 (iii).

□

**Definition 3.6.** Für eine mengenwertige Funktion $f : X \longrightarrow \mathfrak{P}(Y)$ schreiben wir

$$\Pi(f) \coloneqq \prod_{x\in X} f(x).$$

Wir haben nun die nötige Theorie aufgebaut, um die direkte Semantik eines Programms zunächst auf $\mathcal{V}(S)$ fortzusetzen.

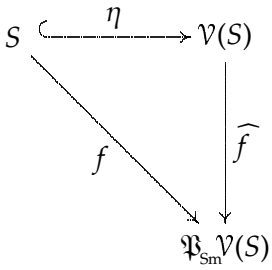


Abbildung 7: Fortsetzung von $f$ auf $\mathcal{V}(S)$

**Definition 3.7.** Sei $f : S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ eine Scott-stetige[1]Funktion. Dann definieren wir die **Fortsetzung von** $f$ **auf** $\mathcal{V}(S)$ als:

$$\begin{aligned}\widehat{f} : \mathcal{V}(S) &\longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)\\ \mu &\longmapsto \uparrow \left\{ \lambda s.\ \sum_{t\in S} g(t)(s)\cdot\mu(t) \;\middle|\; g \in \Pi(f) \right\}.\end{aligned}$$

Hierbei ist $g$ als Funktion $g : S \longrightarrow \mathcal{V}(S)$ aufzufassen.

Jetzt zeigen wir, daß das wohldefiniert und wirklich eine Forsetzung ist.

**Lemma 3.8.** *Betrachten wir die Hausdorfftopologie $\mathcal{H}$ auf $\mathcal{V}(S)$ und die von ihr induzierte Produkttopologie auf $\left[S \longrightarrow \mathcal{V}(S)\right]$, so ist für festes $\mu \in \mathcal{V}(S)$ die Funktion*

$$\begin{aligned}\Phi_\mu : \left[S \longrightarrow \mathcal{V}(S)\right] &\longrightarrow \mathcal{V}(S)\\ g &\longmapsto \lambda s. \sum_{t\in S} g(t)(s)\cdot\mu(t)\end{aligned}$$

*wohldefiniert und stetig.*

**Beweis.** Wegen $g(t) \in \mathcal{V}(S)$ gilt definitionsgemäß

$$\sum_{s\in S} g(t)(s) \leq 1.$$

Somit folgt direkt

$$\begin{aligned}\sum_{s\in S}\sum_{t\in S} g(t)(s)\cdot\mu(t) &= \sum_{t\in S}\mu(t)\cdot\sum_{s\in S} g(t)(s)\\ &\leq \sum_{t\in S}\mu(t)\cdot 1 \leq 1.\end{aligned}$$

[1]wieder dient die Forderung lediglich der Konformität mit anderen Quellen. Jede solche Funktion ist Scott-stetig.

Es bleibt zu zeigen, daß für festes $s \in S$ und $U \in \mathcal{O}([0,1])$ die Menge

$$\Big\{ g : S \longrightarrow \mathcal{V}(S) \;\Big|\; \Phi_\mu(g)(s) \in U \Big\}$$

offen ist.

Zu diesem Zweck sei $g_0$ gegeben mit $\Phi_\mu(g_0)(s) \in U$.

Da $U$ offen ist, gibt es ein $\epsilon > 0$, so daß das Intervall $\Big(\Phi_\mu(g_0)(s) - \epsilon, \Phi_\mu(g_0)(s) + \epsilon\Big)$ (oder gegebenenfalls der Schnitt dieses reellen Intervalls mit [0,1]) eine Teilmenge von $U$ ist.

Da $\mu$ eine Subverteilung ist, gilt $\sum_{t \in S} \mu(t) \leq 1$, also gibt es eine endliche Menge $S_F \subseteq_{\mathsf{fin}} S$ mit $\sum\limits_{t \in {S_F}^{\mathsf{c}}} \mu(t) < \frac{\epsilon}{3}$.

Sei nun $n \coloneqq |S_F|$ die Anzahl der Elemente von $S_F$.

Für $t \in S_F$ setzen wir $\delta_t \coloneqq \min\Big(1, \frac{\epsilon}{3n}\Big)$.

Nun sei $I_t \coloneqq \Big(g_0(t)(s) - \delta(t), g_0(t)(s) + \delta_t\Big) \cap [0,1]$. Wir werden jetzt sehen, daß die Menge $\Big\{ g : S \longrightarrow \mathcal{V}(S) \;\Big|\; \Big(\forall t \in S_F\Big)\; g(t)(s) \in I_t \Big\}$, eine basisoffene Umgebung von $g_0$, im Urbild von $U$ enthalten ist:

Sei hierfür $g$ aus dieser Menge. Dann ist

$$\begin{aligned}
\Phi_\mu(g)(s) &= \sum_{t \in S} g(t)(s) \cdot \mu(t) \\
&= \sum_{t \in S_F} g(t)(s) \cdot \mu(t) + \underbrace{\sum_{t \notin S_F} g(t)(s) \cdot \mu(t)}_{\leq \frac{\epsilon}{3}}
\end{aligned}$$

Da für zwei Zahlen $x, y \in [0, \frac{\epsilon}{3}]$ stets $|x - y| \in [0, \frac{\epsilon}{3}]$ ist, folgt

$$\left| \sum_{t \notin S_F} g(t)(s) \cdot \mu(t) - \sum_{t \notin S_F} g_0(t)(s) \cdot \mu(t) \right| \leq \frac{\epsilon}{3}$$

und somit

$$\begin{aligned}
\Big|\Phi_\mu(g)(s) - \Phi_\mu(g_0)(s)\Big| &\leq \frac{\epsilon}{3} + \sum_{t \in S_F} \Big(g(t)(s) - g_0(t)(s)\Big) \cdot \mu(t) \\
&\leq \frac{\epsilon}{3} + \sum_{t \in S_F} \frac{\epsilon}{3n \cdot \mu(t)} \cdot \mu(t) \\
&= \frac{\epsilon}{3} + \frac{\epsilon}{3} < \epsilon,
\end{aligned}$$

was den Beweis abschließt. □

Die Funktion $\Phi$ ist im übrigen auch Scott-stetig, wie wir in Proposition 4.2 sehen werden.

**Satz 3.9.** *Die Funktion $\widehat{f}$ aus Definition 3.7 ist*

(i) *wohldefiniert,*

(ii) *Scott-stetig und*

(iii) *erhält Konvexkombinationen, d.h.*

$$\widehat{f}\left(r \cdot \mu + (1-r) \cdot \mu'\right) = r \cdot \widehat{f}(\mu) + (1-r) \cdot \widehat{f}(\mu').$$

**Beweis.**

(i) Für alle $s \in S$ ist $f(s) \in \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$, also nichtleer, kompakt, saturiert und konvex. Somit ist auch $\Pi(f)$ nichtleer. Die auftretenden Integrale haben stets Werte in $[0,1]$, da $0 \leq g(t)(s) \leq 1$ ist und schon

$$\int_S 1 \,\mathrm{d}\mu(t) \leq 1$$

gilt. Also ist $\widehat{f}(\mu)$ nichtleer.

Die Abbildung

$$g \longmapsto \int_S g(t)(s) \,\mathrm{d}\mu(t)$$

ist für festes $\mu$ und $s$ stets Scott-stetig und linear. Wir können Proposition 4.2 verwenden, denn die Funktion $B_{s,g} : t \longmapsto g(t)(s)$ ist für alle $s$ und $g$ Scott-stetig [2].

Dann ist aber auch die Abbildung

$$g \longmapsto \lambda s. \int_S g(t)(s) \,\mathrm{d}\mu(t)$$

Scott-stetig und linear, denn die Ordnung ist punktweise definiert und gerichtete Suprema werden punktweise ausgerechnet. Entsprechend ist das Bild der saturierten, konvexen und kompakten Menge $\Pi(f)$ unter dieser Abbildung wieder konvex und kompakt.

Wenn aber

$$\left\{ \lambda s. \int_S g(t)(s) \,\mathrm{d}\mu(t) \;\middle|\; g \in \Pi(f) \right\}$$

konvex, nichtleer und kompakt ist, so folgt mit Satz 1.20, daß $\widehat{f}(\mu)$ tatsächlich ein Element von $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ ist.

[2] Vorwärtsverweise auf diese Proposition sind unbedenklich, da sie nicht mit Ergebnissen aus diesem Abschnitt bewiesen, sondern aus anderer Quelle zitiert wird.

(ii) Seien zwei Verteilungen $\mu, \nu \in \mathcal{V}(S)$ mit $\mu \sqsubseteq \nu$ gegeben. Dann haben wir für jeden Zustand $s \in S$ und jede Auswahl $g \in \Pi(f)$

$$\int_S g(t)(s)\,\mathrm{d}\mu(t) \leq \int_S g(t)(s)\,\mathrm{d}\nu(t).$$

Entsprechend gilt $\widehat{f}(\mu) \sqsubseteq \widehat{f}(\nu)$, also ist $\widehat{f}$ monoton.

Sei $\mu_j$ eine gerichtete Menge von Verteilungen und $\mu$ ihr Supremum.

Nun ist zu zeigen, daß $\widehat{f}(\mu) = \bigsqcup\nearrow \widehat{f}(\mu_i)$ gilt. Dabei folgt $\geq$ bereits aus der Monotonie. Es gilt per Definition

$$\widehat{f}(\mu) \sqsubseteq \bigsqcup\nearrow \widehat{f}(\mu_i) \quad\Longleftrightarrow\quad \widehat{f}(\mu) \sqsupseteq \bigsqcap\nolimits_{\downarrow} \widehat{f}(\mu_i)$$

Das bedeutet gerade, daß wir die folgende Implikation beweisen wollen:

$$\big(\forall i \in I\big)\; a \in \widehat{f}(\mu_i) \Longrightarrow a \in \widehat{f}(\mu).$$

Das ist äquivalent zu

$$\begin{aligned}\big(\forall i \in I\big)\,\big(\exists g \in \Pi f\big)\; a \geq \lambda s.\ &\int_S g_i(t)(s)\,\mathrm{d}\mu_i(t)\\ \Longrightarrow \big(\exists g \in \Pi f\big)\; a \geq \lambda s.\ &\int_S g(t)(s)\,\mathrm{d}\mu(t).\end{aligned}$$

Sei

$$M_i \coloneqq \left\{ g \in \Pi f \;\middle|\; a \geq \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu_i(t) \right\},$$

so sind alle $M_i$ nichtleer. Weiterhin sind die Mengen $M_i$ gefiltert, da $(\mu_i)_{i\in I}$ gerichtet ist und für $\mu_i \leq \mu_j$ stets $M_j \subseteq M_i$ gilt.

Da alle $f(s) \in \mathfrak{P}_{\mathrm{Sm}}\mathcal{V}(S)$ in der Hausdorfftopologie $\mathcal{H}$ abgeschlossen und kompakt sind, ist auch $\Pi f$ mit der Produkttopologie ein kompakter Raum (Satz von Tychonoff). Wegen der $\mathcal{H}$-Stetigkeit des Integrals (siehe Lemma 3.8) sind ferner die Mengen $M_i$ als Produkte von Urbildern von Mengen der Form $[a(s), 1]$ $\mathcal{H}$-abgeschlossene Mengen in einem kompakten $T_2$-Raum (Kompaktheit des Produktraums folgt wieder mit dem Satz von Tychonoff).

Der gefilterte Schnitt nichtleerer abgeschlossener Mengen in einem kompakten Raum ist aber nichtleer (der Beweis hierfür ist eine einfache Übung).

Für $g^* \in \bigcap_{\downarrow} M_i$ ist

$$\big(\forall i \in I\big)\; a \geq \lambda s.\ \int_S g^*(t)(s)\,\mathrm{d}\mu_i(t).$$

Damit ist aber auch

$$a \geq \bigsqcup_{i \in I}{}^{\nearrow} \lambda s.\ \int_S g^*(t)(s)\,\mathrm{d}\mu_i(t) = \lambda s.\ \int_S g^*(t)(s)\,\mathrm{d}\mu(t)$$

Die letzte Gleichheit folgt aus der Beschaffenheit des de facto abzählbaren Integrals (siehe Lemma 0.4), gilt aber auch allgemein (siehe Proposition 4.2).

(iii) Für beliebige Funktionen $B : S \longrightarrow [0,1]$ ist die Abbildung

$$\mu \longmapsto \int_S B(t)\,\mathrm{d}\mu(t)$$

linear (siehe Proposition 4.2).

Für jedes $s$ und jedes $g \in \Pi(f)$ ist die Abbildung $t \longmapsto g(t)(s)$ eine solche Abbildung $B$, so daß auch die Abbildung

$$\mu \longmapsto \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu(t)$$

linear ist.

Zeigen wir nun, daß $\widehat{f}$ Konvexkombinationen erhält:

$$\begin{aligned}
&\widehat{f}\left(r \cdot \mu + (1-r) \cdot \mu'\right) \\
&= \uparrow \left\{ \lambda s.\ r \cdot \int_S g(t)(s)\,\mathrm{d}\mu(t) + (1-r) \cdot \int_S g(t)(s)\,\mathrm{d}\mu'(t) \;\middle|\; g \in \Pi(f) \right\} \\
&= \uparrow \bigcup_{g \in \Pi(f)} \left( r \cdot \left\{ \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu(t) \right\} + (1-r) \cdot \left\{ \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu'(t) \right\} \right) \\
&\subseteq \uparrow \bigcup_{\substack{g \in \Pi(f) \\ g' \in \Pi(f)}} \left( r \cdot \left\{ \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu(t) \right\} + (1-r) \cdot \left\{ \lambda s.\ \int_S g'(t)(s)\,\mathrm{d}\mu'(t) \right\} \right) \\
&= r \cdot \widehat{f}(\mu) + (1-r) \cdot \widehat{f}(\mu').
\end{aligned}$$

Die Mengeninklusion in der dritten Zeile gilt aber auch umgekehrt, denn für $g, g' \in \Pi(f)$ können wir stets auch $h \in \Pi(f)$ finden mit

$$\begin{aligned}
& r \cdot \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu(t) + (1-r) \cdot \lambda s.\ \int_S g'(t)(s)\,\mathrm{d}\mu'(t) \\
= \quad & r \cdot \lambda s.\ \int_S h(t)(s)\,\mathrm{d}\mu(t) + (1-r) \cdot \lambda s.\ \int_S h(t)(s)\,\mathrm{d}\mu'(t).
\end{aligned}$$

Dabei gehen wir wie folgt vor. Für $\mu(t) = 0$ wählen wir $h(t) = g'(t)$.
Für $\mu(t) > 0, \mu'(t) = 0$ wählen wir $h(t) = g(t)$. Im verbleibenden Fall ist $\mu(t) \cdot \mu'(t) > 0$ und wir wählen

$$h(t) = \frac{r \cdot \mu(t) \cdot g(t) + (1-r) \cdot \mu'(t) \cdot g'(t)}{r \cdot \mu(t) + (1-r) \cdot \mu'(t)}.$$

Im letzten Fall ist $h(t) \in f(t)$, da $f(t)$ konvex ist und

$$\frac{(1-r) \cdot \mu'(t)}{r \cdot \mu(t) + (1-r) \cdot \mu'(t)} = 1 - \frac{r \cdot \mu(t)}{r \cdot \mu(t) + (1-r) \cdot \mu'(t)}$$

gilt.

□

**Bemerkung.** Für $\sigma \in S$ haben wir

$$\widehat{f}(\eta_\sigma) = \uparrow \left\{ \lambda s.\ g(\sigma)(s) \;\middle|\; g \in \Pi(f) \right\} = \uparrow f(\sigma) = f(\sigma),$$

also wird $\widehat{f}$ zu Recht als Fortsetzung bezeichnet.

Machen wir uns nun daran, $\widehat{f}$ noch weiter auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ fortzusetzen.

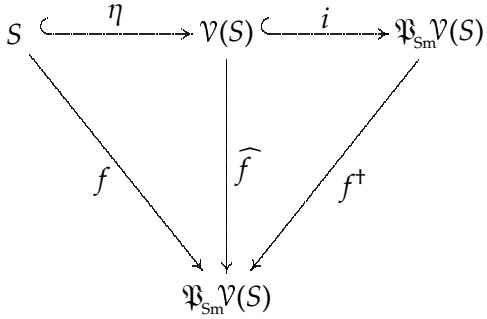


Abbildung 8: Fortsetzung von $f$ auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$

**Definition 3.10.** Es sei wiederum $f : S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ eine Scott-stetige[3]Funktion. Dann definieren wir die **Fortsetzung von $f$ auf $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$** als:

$$\begin{aligned} f^\dagger : \mathfrak{P}_{\text{Sm}}\mathcal{V}(S) &\longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S) \\ P &\longmapsto \bigcup \widehat{f}[P] \end{aligned}$$

**Satz 3.11.** *Die Funktion $f^\dagger$ aus Definition 3.10 ist*

[3]wieder dient die Forderung lediglich der Konformität mit anderen Quellen. Jede solche Funktion ist Scott-stetig.

(i) *wohldefiniert und*

(ii) *Scott-stetig.*

**Beweis.**

(i) Zunächst zeigen wir, daß $\widehat{f}[P]$ eine nichtleere, konvexe, saturierte kompakte Teilmenge von $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ ist. Im nächsten Schritt sehen wir dann, daß deswegen die Vereinigung $f^\dagger(P)$ selbst nichtleer, konvex, saturiert und kompakt ist.

Da die Vereinigung von nichtleeren bzw. oberen Mengen wieder eine nichtleere bzw. obere Menge ist und $\widehat{f}(\mu)$ diese Eigenschaften für alle $\mu \in P$ besitzt, ist $\widehat{f}[P]$ eine nichtleere obere Menge.

Die Konvexität von $\widehat{f}[P]$ folgt direkt aus der Konvexität von $P$, da $\widehat{f}$ Konvexkombinationen erhält (siehe Satz 3.9 (iii)).

Da $\widehat{f}$ Scott-stetig ist, ist das Bild der Scott-kompakten Menge $P$ wieder Scott-kompakt.

Daß nun die Vereinigung $f^\dagger(P)$ einer konvexen Menge konvexer saturierter und nichtleerer Mengen selbst saturiert und nichtleer ist, ist klar. Die Konvexität sehen wir leicht:

Sei $x \in X \in f^\dagger(P)$, $y \in Y \in f^\dagger(P)$ und $r \in [0,1]$. Für $z \coloneqq r \cdot x + (1-r) \cdot y$ ist dann $z \in r \cdot X + (1-r) \cdot Y \in f^\dagger(P)$, da $f^\dagger(P)$ selbst konvex ist.

Es bleibt zu zeigen, daß $f^\dagger(P)$ kompakt ist. Der folgende Beweis stammt von Prof. Klaus Keimel und Prof. Gordon Plotkin und ist einem noch zu erscheinenden Paper entnommen. Er wurde von mir lediglich leicht angepaßt und übersetzt.

Sei $U_i$ eine gerichtete Familie von offenen Mengen, die $f^\dagger(P)$ überdecken. Dann gibt es für jedes $X \in \widehat{f}[P]$ einen Index $i_X$, so daß $X \subseteq U_{i_X}$ ist.

Nach [TKP05] enthält $U_{i_X}$ eine kompakte konvexe saturierte Menge $Y_X$, die eine Umgebung von $X$ ist. Also ist $\uparrow Y_X$ eine Umgebung von $X$ in $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$.

Da $\widehat{f}[P]$ eine kompakte Teilmenge von $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ ist, gibt es eine endliche Auswahl $X_1, \ldots, X_n \in \widehat{f}[P]$, so daß $\widehat{f}[P] \supseteq \uparrow Y_{X_1} \cup \ldots \uparrow Y_{X_n}$ ist.

Entsprechend gibt es also für jedes $X \in \widehat{f}[P]$ einen Index $j$, so daß $Y_{X_j} \ll X$ ist.

Wir schließen, daß $X$ im Innern von $Y_{X_j}$ liegt und entsprechend $X \subseteq U_{X_j}$ ist. Also gilt $f^\dagger(P) \subseteq U_{X_1} \cup \ldots \cup U_{X_n}$.

(ii) Für $P \subseteq Q$ ist auch $\widehat{f}[P] \subseteq \widehat{f}[Q]$, also ist $f^\dagger$ monoton.

Sei nun $P_i$ ein gerichtetes System von Elementen von $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$.

Für $x \in \mathcal{V}(S)$ gilt die Äquivalenz

$$\left(\exists a \in \bigcap\nolimits_{\downarrow} P_i\right) x \in \widehat{f}(a) \quad \Longleftrightarrow \quad \left(\forall i \in I\right)\left(\exists a \in P_i\right) x \in \widehat{f}(a).$$

Die Implikation von links nach rechts ist trivial.

Die andere Richtung gilt, da $\widehat{f}^{-1}(\{a\})$ und $P_i$ auch $\mathcal{H}$-abgeschlossen sind. Somit sind alle $\widehat{f}^{-1}(\{a\}) \cap P_i$ auch $\mathcal{H}$-kompakt und der gefilterte Schnitt nichtleerer kompakter Mengen ist wieder nichtleer.

Daraus folgt sofort die Gleichheit der Mengen

$$\bigcup \widehat{f}\left[\bigcap\nolimits_{\downarrow} P_i\right] = \bigcap\nolimits_{\downarrow} \bigcup \widehat{f}[P_i]$$

und somit ist

$$\begin{aligned} f^\dagger(\swarrow P_i) &= \bigcup \widehat{f}\left[\bigcap\nolimits_{\downarrow} P_i\right] \\ &= \bigcup \bigcap\nolimits_{\downarrow} \widehat{f}[P_i] \\ &= \bigcap_{i\in I\downarrow} \bigcup \widehat{f}[P_i] \\ &= \bigcap\nolimits_{\downarrow} f^\dagger(P_i) \\ &= \swarrow f^\dagger(P_i). \end{aligned}$$

□

Die Funktion $f^\dagger$ ist also eine stetige Fortsetzung von $\widehat{f}$, und somit auch von $f$. In der Tat gilt

$$f^\dagger(\{\eta_s\}) = \widehat{f}(\eta_s) = f(s).$$

## 3.2 Interpretation von Attributen

Ein wichtiges Element von klassischen Programmiersprachen sind Attribute auf dem Zustandsraum. Wir haben bereits die pGCL-Befehle `if` und `while` gesehen, die beide mit echten Attributen arbeiten. Solche klassischen Attribute sind Teilmengen des Zustandsraums. Ein Zustand erfüllt dann entweder das Attribut, das heißt er liegt in der entsprechenden Teilmenge, oder er erfüllt es nicht.

Tatsächlich beobachtbar sind sogar nur offene Teilmengen von $S$, für diskreten Zustandsraum sind aber alle Teilmengen offen.

Für ein echtes Attribut $b$ definieren wir eine Semantik der Auswertung, sowie eine Semantik der Auswertung von $\neg b$ in konkreten Systemzuständen $\sigma \in S$:

**Definition 3.12.** Es sei $S$ ein diskreter Zustandsraum und $b$ ein echtes Attribut auf $S$,

also $b \subseteq S$, dann ist

$$[\![b]\!] \coloneqq \chi_b \,:\, S \longrightarrow \{0,1\} \quad \sigma \longmapsto \begin{cases} 1 & \text{für } \sigma \in b \\ 0 & \text{sonst.} \end{cases}$$

$$[\![\neg b]\!] \coloneqq \chi_{b^c} \,:\, S \longrightarrow \{0,1\} \quad \sigma \longmapsto \begin{cases} 0 & \text{für } \sigma \in b \\ 1 & \text{sonst.} \end{cases}$$

Wenn wir nach dem Auftreten von Nondeterminismus nicht wissen, in welchem Zustand sich die Maschine befindet, nicht einmal sicher sind, welche Subverteilung den Zustand beschreibt, dann können wir auch nicht mit Sicherheit entscheiden, ob ein gewisses Attribut erfüllt ist.

Zunächst überlegen wir uns, was es für ein Attribut bedeutet, in einer Verteilung zu gelten oder nicht. Tun wir das an einem Beispiel:

**Beispiel 3.13.** Es sei $S \coloneqq \{s,t\}$ ein Zustandsraum mit zwei Elementen und $b$ das echte Attribut $b \coloneqq \{s\} \subseteq S$. Das Attribut ist genau dann erfüllt, wenn der aktuelle Systemzustand gerade $s$ ist (und nicht $t$ oder gar $\bot$).

Wenn nun $\mu$ eine Subverteilung auf dem Zustandsraum ist, zum Beispiel $\mu(s) = 0,3$ und $\mu(t) = 0,5$ und wir postulieren, daß der Maschinenzustand zum Zeitpunkt der Auswertung von $b$ gerade der Verteilung $\mu$ folgt, dann ergibt es Sinn zu sagen, daß das Attribut $b$ mit einer Wahrscheinlichkeit von 30% erfüllt ist. Diese Zahl errechnet sich durch $\mu(s) \cdot \chi_b(s) + \mu(t) \cdot \chi_b(t)$.

Wir müssen zumindest für Zwischenergebnisse sogar noch einen Schritt weiter gehen und Attribute betrachten, die schon auf einzelnen Zuständen nur unter Umständen gelten. Das heißt sie gelten mit gewissen Wahrscheinlichkeiten. Allerdings sind sie keine Wahrscheinlichkeitsverteilungen.

Solche Attribute entsprechen dann beliebigen Funktionen von $S$ nach $[0,1]$. Wir nennen die Menge aller dieser Funktionen $\mathcal{E}(S)$. Durch punktweise Ordnung wird $\mathcal{E}(S)$ zu einem vollständigen Verband, auf dem wir die Scott-Topologie betrachten. Die klassischen Attribute sind durch diese Verallgemeinerung nicht verloren gegangen, denn die charakteristischen Funktionen auf beliebigen Teilmengen von $S$ haben Werte in $[0,1]$.

**Definition 3.14.** Ein **probabilistisches Attribut** $B$ über dem Zustandsraum $S$ ist ein Element von $\mathcal{E}(S)$. Die **denotationelle Interpretation** des probabilistischen Attributs in einem Systemzustand $\sigma \in S$ ist dann gerade die Funktion $B$ selbst, also $[\![B]\!](\sigma) = B(\sigma)$.

Die **denotationelle Interpretation** eines solchen Attributs $[\![B]\!]$ im probabilistischen Systemzustand $\mu$ ist dann:

$$[\![B]\!](\mu) \coloneqq \int_{\sigma \in S} B(\sigma)\, \mathrm{d}\mu = \sum_{\sigma \in S} \mu(\sigma) \cdot B(\sigma).$$

Die **dämonische semantische Auswertung** eines solchen Attributs in einem Systemzustand, in dem eine Menge von Verteilungen $M \in \mathfrak{P}_{\mathrm{Sm}}\mathcal{V}(S)$ gelten könnten, ist dann

$$[\![B]\!](M) \coloneqq \bigwedge_{\mu \in M} [\![B]\!](\mu).$$

## 3.3 Definition der direkten Semantik

Für ein pGCL-Programm $P$ ist $[\![P]\!] : S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ eine Scott-stetige Funktion. Diese direkte Semantik können wir nun definieren:

**Definition 3.15.** Die **direkte Semantik** von pGCL-Programmen ist über den Termaufbau rekursiv folgendermaßen definiert:

$$\begin{aligned}
[\![\texttt{assign}_f]\!](s) &\coloneqq \widehat{\eta}(f(s)) = \uparrow \eta_{f(s)} \overset{\text{(Bem.1.8)}}{=} \{\eta_{f(s)}\} \\
[\![\texttt{abort}]\!](s) &\coloneqq \bot \\
[\![\texttt{skip}]\!](s) &\coloneqq \widehat{\eta}(s) = \uparrow \eta_s \overset{\text{(Bem.1.8)}}{=} \{\eta_s\} \\
[\![P\,;Q]\!](s) &\coloneqq [\![Q]\!]^\dagger\Big([\![P]\!](s)\Big) \\
[\![\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi}]\!](s) &\coloneqq [\![b]\!](s) \cdot [\![P]\!](s) + [\![\neg b]\!](s) \cdot [\![Q]\!](s) \\
&= ([\![b]\!](s) \wedge [\![P]\!](s)) \vee ([\![\neg b]\!](s) \wedge [\![Q]\!](s)) \\
[\![P \,{}_p\!\oplus\, Q]\!](s) &\coloneqq p \cdot [\![P]\!](s) + (1-p) \cdot [\![Q]\!](s) \\
[\![P \sqcap Q]\!](s) &\coloneqq \bigcup_{0 \le p \le 1} p \cdot [\![P]\!](s) + (1-p) \cdot [\![Q]\!](s) = \mathsf{conv}\Big([\![P]\!](s) \cup [\![Q]\!](s)\Big) \\
[\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!] &\coloneqq \mu f.\lambda s.[\![b]\!](s) \cdot f^\dagger\Big([\![P]\!](s)\Big) + [\![\neg b]\!](s) \cdot \eta_s \\
&= \mu f.\lambda s.\Big([\![b]\!](s) \wedge f^\dagger\Big([\![P]\!](s)\Big)\Big) \vee ([\![\neg b]\!](s) \wedge \eta_s)
\end{aligned}$$

Dabei ist $\mu(f) = \bigsqcup_{n=0}^{\infty} f^n(\bot)$.

Die Gleichheit zwischen der punktweisen Multiplikation und der Infimumsbildung, bzw. der Addition und der Supremumsbildung gilt, da $[\![b]\!]$ echt, also $\{0,1\}$-wertig ist.

**Proposition 3.16.** *Die Semantik aus Definition 3.15 ist wohldefiniert, insbesondere ist*

$$\begin{gathered}
[\![P\,;Q]\!](s) \in \mathfrak{P}_{\text{Sm}}\mathcal{V}(S), \\
[\![P \,{}_p\!\oplus\, Q]\!](s) \in \mathfrak{P}_{\text{Sm}}\mathcal{V}(S) \textit{ und} \\
[\![P \sqcap Q]\!](s) \in \mathfrak{P}_{\text{Sm}}\mathcal{V}(S).
\end{gathered}$$

**Beweis.** Die Menge $[\![P \,{}_p\!\oplus\, Q]\!]$ ist saturiert (siehe Lemma 1.15). Sie ist weiterhin konvex nach Lemma 1.3 und kompakt, da Addition und Skalarmultiplikation stetig sind.

Die Menge $[\![P \sqcap Q]\!](s)$ ist gerade die konvexe Hülle der beiden Mengen $[\![P]\!](s)$ und $[\![Q]\!](s)$. Diese Mengen sind beide kompakte und konvexe Teilmengen des topologischen Kegels $\mathcal{V}(S)$, deswegen ist nach Theorem 1.10 auch $[\![P \sqcap Q]\!](s)$ wieder kompakt und konvex. Als Vereinigung saturierter Mengen ist sie selbst wieder saturiert.

Die Wohldefiniertheit von $[\![Q]\!]^\dagger([\![P]\!](s))$ haben wir in Satz 3.11 gezeigt.

Die Wohldefiniertheit der anderen Fälle ist leicht einzusehen. □

**Bemerkung.** Tatsächlich ist $[\![P \sqcap Q]\!](s)$ in $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ das Infimum von $[\![P]\!](s)$ und $[\![Q]\!](s)$, wie durch die Notation nahegelegt wird. Eine Smyth-Menge, die $[\![P]\!](s)$ und $[\![Q]\!](s)$ enthält, enthält nämlich zumindest $\mathsf{conv}\Big([\![P]\!](s) \cup [\![Q]\!](s)\Big) = [\![P \sqcap Q]\!](s)$.

*The basics of optimism is sheer terror.*
*(Oscar Wilde)*

# 4 wp-Semantik von pGCL

## 4.1 wp-Semantik

### 4.1.1 Klassisch, deterministisch

Die direkte Semantik identifiziert deterministische Programme mit Abbildungen in $\left[S \longrightarrow S_\perp\right]$. Darüberhinaus können wir ein Programm auch beschreiben, indem wir erklären, wie es auf der Menge der Attribute auf dem Zustandsraum operiert.

Die wp-Semantik hilft, totale Korrektheitsaussagen zu treffen. Das Kürzel wp steht dabei für *weakest precondition* (oder im probabilistischen Falle dann *weakest preexpectation*) also schwächste Vorbedingung (bzw. -erwartung). Es ist eine Funktion, die jedem Programm eine Selbstabbildung des Raums der Attribute auf $S$ zuordnet. Diese Form der Semantik heißt deswegen auch *predicate transformer*-Semantik.

Dabei wird einem Programm jene Abbildung zugeordnet, die jeder möglichen Nachbedingung $b$ gerade exakt das Attribut zuordnet, das eben nötig ist, um bei Ausführung des Programmes die Termination und auch die Nachbedingung zu gewährleisten.

Sei $[\![P]\!] : S \longrightarrow S_\perp$ die Semantik eines deterministischen Programmes und $b \subseteq S$ ein echtes Attribut. Dann ist

$$\mathsf{wp}([\![P]\!])(b) \quad = \quad [\![P]\!]^{-1}(b).$$

### 4.1.2 Nondeterministisch

Im nondeterministischen probabilistischen Falle interpretieren wir $[\![P]\!](s)$ als Element des Smyth-Powerdomains, also eine Menge von Verteilungen, von denen zum Zeitpunkt der Ausführung eine ausgewählt wird, die dann die Wahrscheinlichkeiten des Auftretens der verschiedenen Maschinenzustände beschreibt.

Wenn unser Programm aus dem Startzustand $s$ gerade die Verteilung $\mu$ erzeugt, so können wir bestimmen, *wie wahrscheinlich* es ist, daß in der Verteilung $\mu$ die Nachbedingung oder ein probabilistisches Prädikat $B \in \mathcal{E}(S)$ gilt, indem wir den Erwartungswert berechnen:

$$[\![B]\!](\mu) = \int_S B(t)\,\mathrm{d}\mu(t)$$

Probabilistische Nachbedingungen werden nicht *post-condition*, sondern *post-expectation* genannt.

Entsprechend verfahren wir nun mit der Menge von möglicherweise geltenden Verteilungen und wählen dann risiko-konservativ das *Infimum* der auftauchenden Werte als *weakest preexpectation*.

**Definition 4.1.** Sei Prog die Menge der pGCL-Programme. Sei $S$ der Zustandsraum und sei $P \in \mathsf{Prog}$ ein Programm. Dann ist $[\![P]\!] : S \longrightarrow \mathfrak{P}_{\mathrm{Sm}}\mathcal{Y}(S)$ eine Abbildung. Sei generell $f : S \longrightarrow \mathfrak{P}_{\mathrm{Sm}}\mathcal{Y}(S)$ gegeben. Sei weiterhin $B \in \mathcal{E}(S)$ ein probabilistisches Attribut, das nach Ausführung von $P$ erfüllet sein soll. Dann ist die **weakest preexpectation** von $B$ unter $P$ definiert als

$$\begin{aligned}\mathcal{E}(S) \ni \mathsf{wp}(f)(B) \ &: S \longrightarrow [0,1] \\ &s \longmapsto \bigwedge_{\mu \in f(s)} \int_S B(t)\,\mathrm{d}\mu(t).\end{aligned}$$

**Proposition 4.2.** *Die Funktion*

$$\begin{aligned}\mathcal{V}(S) \times \mathcal{E}(S) &\longrightarrow [0,1] \\ (\mu, B) &\longmapsto \int_s B(t)\,d\mu(t)\end{aligned}$$

*ist komponentenweise Scott-stetig und bilinear.*

*Dabei (und im folgenden) meinen wir, daß alle Linearkombinationen durch die Funktion erhalten werden, die in $\mathcal{V}(S)$ bzw. in $\mathcal{E}(S)$ existieren. Insbesondere wird die Null und jede Konvexkombination erhalten.*

**Beweis.** Siehe [TKP05, Satz 4.4]. □

In diesem Sinne ist folgende Schreibweise zu verstehen:

**Definition 4.3.** Sei $\mu \in \mathcal{V}(S)$ und $B \in \mathcal{E}(S)$, dann definieren wir die an das Skalarprodukt angelehnte **Schreibweise**:

$$\langle \mu, B \rangle \coloneqq \int_S B(t)\,\mathrm{d}\mu(t)$$

Wir können also kurz schreiben:

$$\mathsf{wp}([\![P]\!])(B)(s) = \bigwedge_{\mu \in [\![P]\!](s)} \langle \mu, B \rangle$$

Es ist wichtig anzumerken, daß wp mit dieser Definition eine Scott-stetige Funktion von $[\![\mathsf{Prog}]\!]$ nach $\Big[\mathcal{E}(S) \longrightarrow \mathcal{E}(S)\Big]$ ist.

**Lemma 4.4.** *Die Funktion* $\mathsf{wp} : \Big[S \longrightarrow \mathfrak{P}_{Sm}\mathcal{Y}(S)\Big] \times \mathcal{E}(S) \times S \longrightarrow [0,1]$ *ist in jedem ihrer Parameter $[\![P]\!]$, $B$ und $s$ separat und simultan in den drei Parametern Scott-stetig.*

**Beweis.** Da $S$ diskret ist, ist wp in $s$ stetig.

Da $\mu \longmapsto \langle \mu, B \rangle$ Scott-stetig ist, ist mit Lemma 1.17 auch die Funktion

$$[\![P]\!](s) \longrightarrow \mathsf{wp}([\![P]\!])(B)(s)$$

Scott-stetig.

Da $[\![P]\!]$ eine stetige Funktion ist, ist trivialerweise $s \longmapsto [\![P]\!](s)$ stetig. Also ist die Hintereinanderausführung $s \longmapsto \mathsf{wp}([\![P]\!])(B)(s)$ Scott-stetig.

Da auch $[\![P]\!] \longmapsto [\![P]\!](s)$ Scott-stetig ist, ist aus dem selben Grund auch die Funktion $[\![P]\!] \longmapsto \mathsf{wp}([\![P]\!])(B)(s)$ Scott-stetig.

Die Stetigkeit von $B \longmapsto \mathsf{wp}([\![P]\!])(B)(s)$ folgt aus der Stetigkeit des Skalarprodukts und Lemma 1.18.

Simultane Stetigkeit folgt direkt aus der separaten Stetigkeit, da die auftretenden Räume stetige Bereiche sind. □

## 4.2 Rekursive Definition von wp in pGCL

In der Sprache pGCL können wir wp rekursiv über den Termaufbau definieren. Wir beweisen, daß sich die Funktion wp, wie sie in 4.1 definiert ist *natürlich* auf den definierenden Termen von pGCL verhält.

**Theorem 4.5.** *Die Funktion* wp *erfüllt die folgenden Gleichungen:*

$$\mathsf{wp}([\![\texttt{abort}]\!])(B) = \bot \tag{1}$$

$$\mathsf{wp}([\![\texttt{skip}]\!])(B) = B \tag{2}$$

$$\mathsf{wp}([\![\texttt{assign}_f]\!])(B) = B \circ f \tag{3}$$

$$\mathsf{wp}([\![\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi}]\!])(B) = ([\![b]\!] \wedge \mathsf{wp}([\![P)]\!](B)) \vee ([\![\neg b]\!] \wedge \mathsf{wp}([\![Q]\!])(B)) \tag{4}$$

$$\mathsf{wp}([\![P;Q]\!])(B) = \mathsf{wp}([\![P]\!])(\mathsf{wp}([\![Q]\!])(B)) \tag{5}$$

$$\mathsf{wp}([\![P \,{}_p\!\oplus\, Q]\!])(B) = p \cdot \mathsf{wp}([\![P]\!])(B) + (1-p) \cdot \mathsf{wp}([\![Q]\!])(B) \tag{6}$$

$$\mathsf{wp}([\![P \sqcap Q]\!])(B) = \mathsf{wp}([\![P]\!])(B) \wedge \mathsf{wp}([\![Q]\!])(B) \tag{7}$$

$$\mathsf{wp}([\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!])(B) = \mu X.\, \Big(([\![b]\!] \wedge \mathsf{wp}([\![P]\!])(X)) \vee ([\![\neg b]\!] \wedge B)\Big) \tag{8}$$

*Wobei* $\vee$ *und* $\wedge$ *von Subverteilungen bei* (4) *und* (8) *natürlich punktweise zu verstehen sind und wegen der* $\{0,1\}$*-Wertigkeit von* $[\![b]\!]$ *mit* $+$ *und* $\cdot$ *übereinstimmen.*
*Wieder ist* $\mu(f) = \bigsqcup_{n=0}^{\infty} f^n(\bot)$.

Das Theorem wird im folgenden Abschnitt nach und nach bewiesen.

**Bemerkung.** Theorem 4.5 läßt sich als rekursive Definition der wp-Semantik von pGCL verstehen, bzw als Kommutativität von Diagramm 9

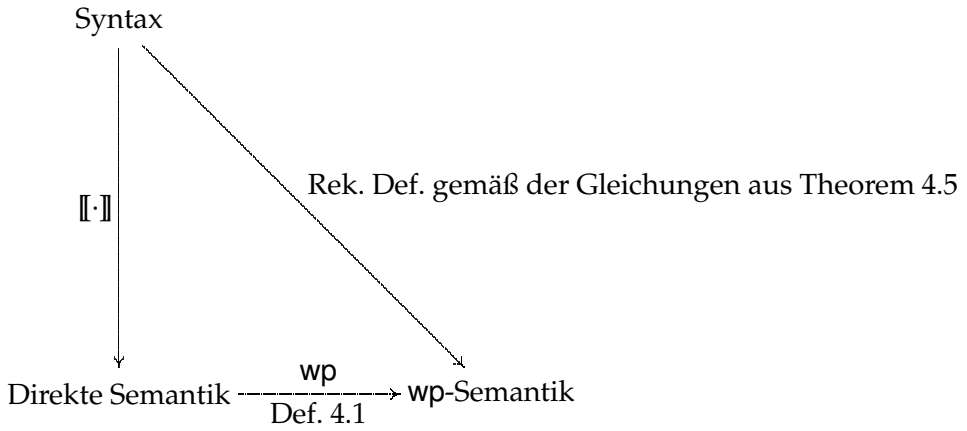


Abbildung 9: Interpretation von Theorem 4.5

## 4.3 Beweis des Theorems 4.5

### 4.3.1 Die einfachen Fälle

Zunächst werden die Punkte (1) bis (7) bewiesen, die alle nicht schwer zu sehen sind. Ohne Ausnahme folgt die Behauptung hier durch Einsetzen von $[\![P]\!]$ in die Definition von $\mathsf{wp}(P)(B)(s)$.

(1) Da `abort` jede Verteilung erzeugen kann, ist das Infimum des Skalarprodukts stets 0.

(2) Auch `skip` ist schnell behandelt: Da $[\![\texttt{skip}]\!]$ stets die Punktverteilung $\eta_s$ erzeugt, ist $\mathsf{wp}([\![\texttt{skip}]\!])(B)(s)$ tatsächlich nichts anderes, als $B(s)$.

(3) Ebenso problemlos ist das Anwenden einer deterministischen Funktion $f$ auf dem Zustandsraum. Da $[\![\texttt{assign}_f]\!](s) = \uparrow\left\{\eta_{f(s)}\right\}$ ist, gilt gemäß der Definition von wp:

$$\mathsf{wp}([\![\texttt{assign}_f]\!])(B) = \lambda s. \bigwedge_{\mu\in\{\eta_{f(s)}\}} \langle \mu, B\rangle = \lambda s.\langle \eta_{f(s)}, B\rangle = \lambda s.B(f(s)) = B \circ f.$$

(4) Untersuchen wir nun die Semantik der `if`-Verzweigung:
Die direkte Semantik der Fallunterscheidung ist definiert als

$$[\![\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi}]\!]s = [\![b]\!]s \cdot [\![P]\!](s) + [\![\neg b]\!]s \cdot [\![Q]\!](s).$$

Deswegen gilt

$$\begin{aligned}
\mathsf{wp}(\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi})(B) &= \lambda s. \bigwedge_{\mu\in[\![b]\!]s\cdot[\![P]\!](s)+[\![\neg b]\!]s\cdot[\![Q]\!](s)} \langle \mu, B\rangle \\
&= \lambda s.[\![b]\!]s \cdot \bigwedge_{\mu\in[\![P]\!](s)} \langle \mu, B\rangle + [\![\neg b]\!]s \cdot \bigwedge_{\mu\in[\![Q]\!](s)} \langle \mu, B\rangle \\
&= \lambda s.[\![b]\!]s \cdot \mathsf{wp}([\![P]\!])(B)s + [\![\neg b]\!]s \cdot \mathsf{wp}([\![Q]\!])(B)s.
\end{aligned}$$

(5) Auch die Regel für die Hintereinanderausführung läßt sich direkt nachprüfen. Wir wollen zeigen, daß $\mathsf{wp}(P;Q)(B)$ dasselbe ist wie $\mathsf{wp}(\llbracket P \rrbracket)(\mathsf{wp}(\llbracket Q \rrbracket)(B))$.
Nun ist

$$\begin{aligned}
\llbracket P;Q \rrbracket(s) &= \llbracket Q \rrbracket^{\dagger}(\llbracket P \rrbracket(s)) \\
&= \bigcup \left\{ \widehat{\llbracket Q \rrbracket}(\mu) \;\middle|\; \mu \in \llbracket P \rrbracket(s) \right\} \\
&= \Big\uparrow \underbrace{\bigcup_{\substack{\mu \in \llbracket P \rrbracket(s) \\ g \in \Pi(\llbracket Q \rrbracket)}} \left\{ \lambda z.\ \int_S g(t)(z)\, \mathrm{d}\mu(t) \right\}}_{A}.
\end{aligned}$$

Lemma 1.19 garantiert $\bigwedge f[\uparrow A] = \bigwedge f[A]$ für stetige $f$. Somit ist:

$$\begin{aligned}
\mathsf{wp}(P;Q)(B)(s) &= \bigwedge_{\mu \in \llbracket P;Q \rrbracket(s)} \sum_{t' \in S} B(t') \cdot \mu(t') \\
&= \bigwedge_{\mu \in A} \sum_{t' \in S} B(t') \cdot \mu(t') \\
&= \bigwedge_{g,\mu} \sum_{t' \in S} B(t') \cdot \Big( \lambda z.\ \sum_{t \in S} \mu(t) \cdot g(t)(z) \Big)(t') \\
&= \bigwedge_{g,\mu} \sum_{t' \in S} B(t') \cdot \sum_{t \in S} \mu(t) \cdot g(t)(t') \\
&= \bigwedge_{g,\mu} \sum_{t \in S} \sum_{t' \in S} g(t)(t') \cdot B(t') \cdot \mu(t) \\
&= \bigwedge_{\mu \in \llbracket P \rrbracket(s)} \sum_{t \in S} \mu(t) \cdot \bigwedge_{g \in \Pi \llbracket Q \rrbracket} \sum_{t' \in S} g(t)(t') \cdot B(t') \\
&= \bigwedge_{\mu \in \llbracket P \rrbracket(s)} \sum_{t \in S} \mu(t) \cdot \bigwedge_{\nu \in \llbracket Q \rrbracket t} \sum_{t' \in S} \nu(t') \cdot B(t') \\
&= \mathsf{wp}(\llbracket P \rrbracket)\Big(\mathsf{wp}(\llbracket Q \rrbracket)(B)\Big)(s).
\end{aligned}$$

Hierbei können wir in der vorletzten Gleichheit $\bigwedge_g$ durch $\bigwedge_\nu$ ersetzen, da

$$\left\{ g(s) \;\middle|\; g \in \Pi(f) \right\} = f(s)$$

gilt.
Die Summen über $t$ bzw. $t'$ vertauschen, da absolute Konvergenz vorliegt.

(6) Für die probabilistische Auswahl zwischen zwei Programmen gilt

$$\begin{aligned}
[\![P \,{}_p\!\oplus Q]\!](s) &= p \cdot [\![P]\!](s) + (1-p) \cdot [\![Q]\!](s) \\
\mathsf{wp}([\![P \,{}_p\!\oplus Q]\!])(B)(s) &= \bigwedge_{\mu \in [\![P \,{}_p\!\oplus Q]\!](s)} \langle \mu, B \rangle \\
&= \bigwedge_{\nu \in [\![P]\!](s), \nu' \in [\![Q]\!](s)} \langle p \cdot \nu + (1-p) \cdot \nu', B \rangle \\
&= p \cdot \bigwedge_{\nu \in [\![P]\!](s)} \langle \nu, B \rangle + (1-p) \cdot \bigwedge_{\nu' \in [\![Q]\!](s)} \langle \nu', B \rangle \\
&= p \cdot \mathsf{wp}([\![P]\!])(B)(s) + (1-p) \cdot \mathsf{wp}([\![Q]\!])(B)(s),
\end{aligned}$$

da das Skalarprodukt linear ist.

(7) Für die nondeterministische Auswahl haben wir:

$$\begin{aligned}
\mathsf{wp}([\![P \sqcap Q]\!])(B)(s) &= \bigwedge_{\mu \in \left\{ p \cdot [\![P]\!](s) + (1-p) \cdot [\![Q]\!](s) \;\middle|\; p \in [0,1] \right\}} \langle \mu, B \rangle \\
&= \bigwedge_{p \in [0,1]} p \cdot \mathsf{wp}([\![P]\!])(B)(s) + (1-p) \cdot \mathsf{wp}([\![Q]\!])(B)(s) \\
&= \mathsf{wp}([\![P]\!])(B)(s) \wedge \mathsf{wp}([\![Q]\!])(B)(s)
\end{aligned}$$

Die letzte Gleichheit gilt, da von zwei Elementen aus $[0,1]$ stets eines das Größere und eines das Kleinere ist. Dementsprechend ist die kleinste Konvexkombination der beiden auch gerade das kleinere Element.

### 4.3.2 Die while-Schleife

(8) Schließlich widmen wir uns dem schwierigsten Teil des Beweises. Wir wollen im Folgenden zeigen, daß die folgende Gleichheit gilt:

$$\mathsf{wp}([\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!])(B) = \mu X. \left( [\![b]\!] \cdot \mathsf{wp}([\![P]\!])(X) + [\![\neg b]\!] \cdot B \right)$$

Hier ist die direkte Semantik definiert als:

$$[\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!](s) = \mu f. \lambda s. [\![b]\!](s) \cdot f^{\dagger}\Big( [\![P]\!](s) \Big) + [\![\neg b]\!](s) \cdot \eta_s$$

Beim Beweis hilft das folgende Lemma, das ein Spezialfall des ,,Least Fix Point Theorem for Scott Continuous Functions (Prop II-2.4)'' aus [GHK+03] ist.

**Lemma 4.6.** *Es seien $k$ eine Scott-stetige Selbstabbildung von $\Big[S \longrightarrow \mathfrak{P}_{Sm}\mathcal{Y}(S)\Big]$, $g$ eine Scott-stetige Selbstabbildung von $\mathcal{E}(S)$ und $h : \Big[S \longrightarrow \mathfrak{P}_{Sm}\mathcal{Y}(S)\Big] \longrightarrow \mathcal{E}(S)$ Scott-stetig und strikt. Aus $g \circ h = h \circ k$ folgt dann $h(\mu(k)) = \mu(g)$, wobei $\mu$ der kleinste-Fixpunkt-Operator ist:*

$$\mu(f) = \bigsqcup_{n=0}^{\infty} f^n(\bot)$$

**Beweis.** Vergleiche [GHK+03, Prop II-2.4].
Sowohl $\left[S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)\right]$ als auch $\mathcal{E}(S)$ sind Bereiche mit $\bot$. □

Um das Theorem zu beweisen, wollen wir das Lemma auf diese Funktionen anwenden:

$$\begin{aligned} h_B(f) &\coloneqq \mathsf{wp}(f)(B) \\ k(f) &\coloneqq \lambda s.[\![b]\!](s) \cdot f^{\dagger}\Big([\![P]\!](s)\Big) + [\![\neg b]\!](s) \cdot \eta_s \\ g(X) &\coloneqq [\![b]\!] \cdot \mathsf{wp}([\![P]\!])(X) + [\![\neg b]\!] \cdot B \end{aligned}$$

Diagramm 10, von dem wir sehen werden, daß es kommutiert, veranschaulicht die Situation.

$$\begin{array}{ccc} \left[S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)\right] & \xrightarrow{\quad h_B \quad} & \mathcal{E}(S) \\ \Big\downarrow k & & \Big\downarrow g \\ \left[S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)\right] & \xrightarrow{\quad h_B \quad} & \mathcal{E}(S) \end{array}$$

Abbildung 10: Fixpunkte in der direkten und der wp-Semantik der `while`-Schleife

Wir überprüfen die Voraussetzungen von Lemma 4.6 in diesem Kontext.
Tatsächlich sind $k$ und $g$ Scott-stetige Abbildungen, die einen kleinsten Fixpunkt haben. Das Diagramm kommutiert:

$$\begin{aligned} \Big(h_B \circ k\Big)(s) &= \mathsf{wp}\Big(\lambda s.\Big([\![b]\!](s) \cdot f^{\dagger}\Big([\![P]\!](s)\Big) + [\![\neg b]\!](s) \cdot \eta_s\Big)\Big)(B)(s) \\ &= [\![b]\!](s) \cdot \mathsf{wp}\Big(f^{\dagger}\Big([\![P]\!](s)\Big)\Big)(B)(s) + [\![\neg b]\!](s) \cdot B(s) \\ &= [\![b]\!](s) \cdot \mathsf{wp}([\![P]\!])\Big(\mathsf{wp}(f)(B)\Big)(s) + [\![\neg b]\!](s) \cdot B(s) \\ &= g(\mathsf{wp}(f)(B))(s) \\ &= \Big(g \circ h_B\Big)(s). \end{aligned}$$

Die Striktheit von $h_B$ ist leicht einzusehen, denn das Bottom-Element von $\left[S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)\right]$ ist $[\![\texttt{abort}]\!]$ und wir haben bereits gesehen, daß $h_B(\bot) = \mathsf{wp}(\texttt{abort})(B) = \bot$ gilt.
$h_B$ ist Scott-stetig, denn es ist eine Projektion der Scott-stetigen Funktion

$$\mathsf{wp} \;:\; \left[S \longrightarrow \mathfrak{P}_{\text{Sm}}\mathcal{V}(S)\right] \longrightarrow \left[\mathcal{E}(S) \longrightarrow \mathcal{E}(S)\right].$$

Die Bedingungen des Lemmas sind also alle erfüllt und somit ist

$$\begin{aligned}\mathsf{wp}([\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!])(B) &= h_B(\mu(k)) \\ &= \mu(g) \\ &= \mu X.\, \Big([\![b]\!] \cdot \mathsf{wp}([\![P]\!])(X) + [\![\neg b]\!] \cdot B\Big),\end{aligned}$$

was den Beweis des Theorems abschließt. □

## 4.4 Das Bild von wp

Es erhebt sich die Frage, welche predicate transformer $p : \mathcal{E}(S) \longrightarrow \mathcal{E}(S)$ als Bild von wp auftauchen.

Gordon Plotkin hat diese Frage in [Plo79] für nondeterministische nichtprobabilistische Programme $f : S \longrightarrow \mathfrak{P}_{\text{Sm}}(S_\perp)$ beantwortet.

In diesem Fall sind die Abbildungen der Gestalt $\mathsf{wp}(f)$ genau diejenigen Scott-stetigen $p : \mathfrak{P}(S) \longrightarrow \mathfrak{P}(S)$, die binäre Schnitte erhalten. Diese $p$ erhalten dann auch nichtleere Schnitte, da für $s \in \mathsf{wp}(f)(B)$ eine kleinste endliche Teilmenge $B_0$ von $B$ existiert mit $s \in \mathsf{wp}(f)(B_0)$.

Plotkin und Keimel arbeiten derzeit an einer derartigen Charakterisierung im nondeterministischen probabilistischen Fall.

*De mortuis nihil nisi bene.*
*Bzw: Endlosschleife, na und?*

# 5 Semantik im Hoare-Powerdomain

Es gibt Situationen, in denen Divergenz eines Programmes keine gravierenden Folgen hat und lediglich gewisse Ausgaben vermieden werden müssen. Man denke an einen Bargeldautomaten. Es ist ärgerlich, wenn dieser sich aufhängt. Es beruhigt uns allerdings ein Aufkleber:

Sollte es zu einem Systemfehler kommen, wird Ihre Karte nicht zu einem späteren Zeitpunkt unkontrolliert ausgegeben.

Diese *partielle Korrektheitsaussage* interessiert uns. „Vielleicht terminiert das hier nicht. Aber *falls* es terminiert: Meine Karte ist sicher."

Betrachten wir das folgende pGCL-Programm, das nondeterministische, aber keine probabilistische Auswahl verwendet.

$$
\begin{array}{l}
x := 0; \\
a := 0 \sqcap a := 1; \\
\texttt{while } (a = 0) \texttt{ do} \\
\quad x := x + 2; \\
\quad a := 0 \sqcap a := 1 \\
\texttt{od}
\end{array}
$$

Gibt man für dieses Programm eine Semantik in $(S \longrightarrow \mathfrak{P}_{\text{Sm}}(S_\perp))$ an, so wäre diese gegeben durch $(\sigma \longmapsto S_\perp)$, denn das Programm kann potentiell divergieren und die einzige saturierte Menge, die $\perp$ enthält, ist $S_\perp$ selbst.

Hier erkennt man, daß eine Semantik im Smyth-Powerdomain für partielle Korrektheitsaussagen nicht hinreichend ist. Es ist durchaus vernünftig, über das Programm zu sagen: „Wenn es terminiert, so liefert es für $x$ eine gerade Zahl." Die Smyth-Powerdomain-Semantik läßt aber jede Ausgabe zu, also auch Termination mit ungeradem $x$.

Deswegen definieren wir eine weitere direkte Semantik, die auf partielle Korrektheitsaussagen abzielt und aus der wir dann eine *predicate transformer*-Semantik wlp erzeugen werden.

Die Powerdomain-Konstruktion, die wir hierfür verwenden, geht auf Hoare zurück.

## 5.1 Der Hoare-Powerdomain

Wie gehabt sei $S$ ein abzählbarer flacher Zustandsraum und $\mathcal{V}(S)$ die Menge der Subverteilungen auf $S$.

**Definition 5.1.** Der **Hoare-Powerdomain** $\mathfrak{P}_{\mathrm{H}}$ über $\mathcal{V}(S)$ besteht aus den nichtleeren konvexen Scott-abgeschlossenen Teilmengen von $\mathcal{V}(S)$ und wird mit $\mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ bezeichnet.

Auf $\mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ betrachten wir als Ordnung die Mengeninklusion (im Gegensatz zur umgekehrten Mengeninklusion auf $\mathfrak{P}_{\mathrm{Sm}}\mathcal{V}(S)$).

Der Hoare-Powerdomain $\mathfrak{P}_{\mathrm{H}}\mathcal{V}_\infty(S)$ über dem erweiterten probabilistischen Powerdomain ist wieder ein topologischer Kegel, und zwar mit der Summe

$$A +_H B := \overline{A + B}$$

und dem Skalarprodukt

$$r \cdot_H A := \overline{r \cdot A}.$$

Wieder ist durch die Einschränkung von $\mathcal{V}_\infty(S)$ auf $\mathcal{V}(S)$ die Abgeschlossenheit unter beiden Operationen verletzt, allerdings ist es wieder möglich, Konvexkombinationen von Elementen aus $\mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ zu bilden:

Aus einer nichtleeren Teilmenge $M \subseteq \mathcal{V}(S)$ kann man ein Element von $\mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ erzeugen, indem man den Scott-Abschluß der konvexen Hülle von $M$ bildet.

**Lemma 5.2.** *Für nichtleere $M \subseteq \mathcal{V}(S)$ ist stets $\overline{\mathsf{conv}\, M} \in \mathfrak{P}_H\mathcal{V}(S)$.*

**Beweis.** Per Definition ist $\overline{\mathsf{conv}\, M}$ abgeschlossen und als Obermenge von $M$ auch nichtleer.

Tix, Keimel und Plotkin zeigen in [TKP05, Prop 2.7], daß der Scott-Abschluß konvexer Teilmengen von $\mathcal{V}_\infty(S)$ konvex ist. Das gilt also insbesondere für konvexe Teilmengen von $\mathcal{V}(S)$. □

Ebenfals aus [TKP05] übernehmen wir das folgende Ergebnis:

**Proposition 5.3.** *Für eine gerichtete Familie von Mengen $A_i \in \mathfrak{P}_H\mathcal{V}(S)$ gilt*

$$\bigdownarrow \bigcup\nolimits^{\uparrow} A_i = \overline{\bigcup\nolimits^{\uparrow} A_i}.$$

**Lemma 5.4.** *Für eine Menge $A \subseteq \mathcal{V}(S)$ gilt*

$$\overline{A} = \left\{ \bigdownarrow D \;\middle|\; D \subseteq \downarrow A \right\}.$$

**Beweis.** Da $\mathcal{V}(S)$ ein stetiger Bereich ist, gilt Lemma 0.5. □

Es folgen einige Ergebnisse für Infima:

**Satz 5.5.** *Es sei $f : \mathcal{V}(S) \longrightarrow [0,1]$ Eine Scott-*op*-stetige Funktion, also eine antitone Funktion mit $f(\bigdownarrow D) = \bigwedge_{\downarrow} f(D)$. Dann ist die Infimumsfunktion*

$$\begin{aligned} \mathsf{INF}_f \;&:\; \mathfrak{P}_H\mathcal{V}(S) \longrightarrow [0,1] \\ A &\longmapsto \bigwedge_{\mu \in A} f(\mu) \end{aligned}$$

*Scott-*op*–stetig und für Teilmengen $A \subseteq \mathcal{V}(S)$ gilt stets*

$$\bigwedge f\left[\overline{A}\right] = \bigwedge f[A].$$

**Beweis.** Zeigen wir zunächst den letzten Teil des Satzes.

Für antitones $f$ ist $\bigwedge f[A] = \bigwedge f[{\downarrow}A]$. Es genügt also, $\bigwedge f[{\downarrow}A] = \bigwedge f[\overline{{\downarrow}A}]$ zu zeigen. Einerseits ist

$$\bigwedge_{\mu \in \overline{{\downarrow}A}} f(\mu) = \bigwedge_{D \subseteq {\downarrow}A} f(\swarrow\!\!\!\nearrow D) = \bigwedge_{D \subseteq {\downarrow}A} \bigwedge_{a \subseteq D} f(a) \leq \bigwedge_{a \in {\downarrow}A} f(a),$$

da die einelementigen Mengen $\{a\}$ gerichtete Teilmengen von ${\downarrow}A$ sind. Andererseits ist aber auch $\left(\forall D \subseteq {\downarrow}A\right) f[D] \subseteq f[{\downarrow}A]$und deswegen $\bigwedge f[D] \geq \bigwedge f[{\downarrow}A]$.
Sei schließlich für die Stetigkeit von $\mathsf{INF}_f$ eine gerichtete Menge $A_i \subseteq \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ gegeben. Wir rechnen nun leicht nach:

$$\begin{aligned}\mathsf{INF}_f\,(\swarrow\!\!\!\nearrow_i A_i) = \mathsf{INF}_f\left(\overline{\textstyle\bigcup_i^{\uparrow} A_i}\right) &= \bigwedge f\left(\overline{\textstyle\bigcup_i^{\uparrow} A_i}\right) = \bigwedge f\left(\textstyle\bigcup_i^{\uparrow} A_i\right) \\ &= \bigwedge \textstyle\bigcup_i^{\uparrow} f(A_i) = \bigwedge_i^{\downarrow} \bigwedge f(A_i) = \bigwedge_i^{\downarrow} \mathsf{INF}_f\,(A_i),\end{aligned}$$

was den Beweis abschließt. □

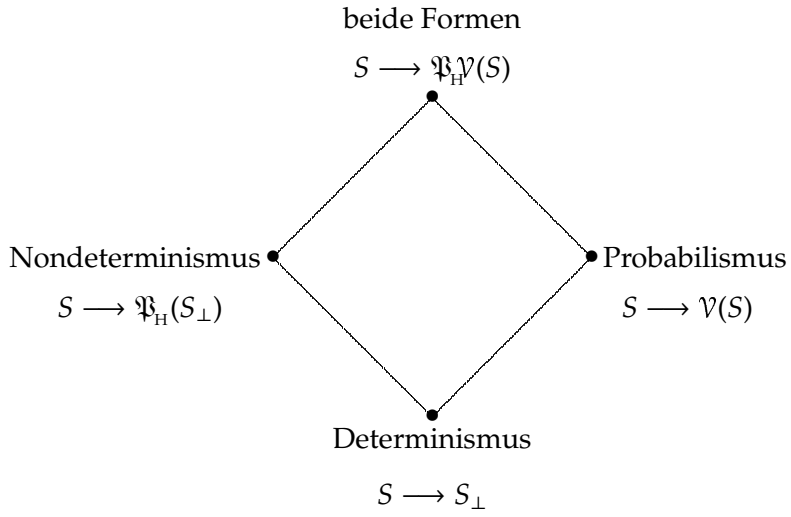


Abbildung 11: Nondeterminismus im Hoare-Powerdomain

Wir erinnern uns an Abbildung 5, die veranschaulicht, wie wir mit dem Smyth-Powerdomain nichtprobabilistischen Nondeterminismus fassen. Faßt man nichtprobabilistischen Nondeterminismus mit dem Hoare-Powerdomain, ergibt sich entsprechend Abbildung 11.

## 5.2 Verkettung von Programmen

Auch wenn wir die denotationelle Semantik eines pGCL-Programms als Funktion in $\left[S \longrightarrow \mathfrak{P}_{\text{H}}\mathcal{V}(S)\right]$ definieren, ist es zunächst nicht möglich, solche Funktionen zu verketten. Wieder benötigen wir eine Fortsetzung wie im Diagramm 12.

**Proposition 5.6.** *Die Funktion* $i : \mathcal{V}(S) \longrightarrow \mathfrak{P}_{H}\mathcal{V}(S) : \mu \longrightarrow \downarrow\mu$ *ist eine stetige Einbettung.*

**Beweis.** Der Beweis ist eine einfache Übung. □

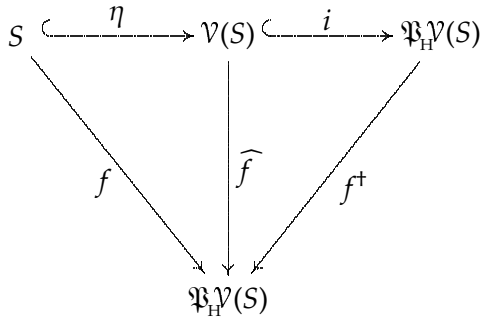


Abbildung 12: Fortsetzung von $f$ auf $\mathfrak{P}_{\text{H}}\mathcal{V}(S)$

**Definition 5.7.** Sei $f : S \longrightarrow \mathfrak{P}_{\text{H}}\mathcal{V}(S)$ eine Scott-stetige[4] Funktion. Dann definieren wir die **Fortsetzung von** $f$ **auf** $\mathcal{V}(S)$ als:

$$\begin{aligned}\widehat{f} : \mathcal{V}(S) &\longrightarrow \mathfrak{P}_{\text{H}}\mathcal{V}(S)\\ \mu &\longmapsto \overline{\left\{ \lambda s. \int_S g(t)(s)\,\mathrm{d}\mu(t) \;\middle|\; g \in \Pi(f) \right\}} =: \overline{A_\mu}.\end{aligned}$$

**Satz 5.8.** *Die Funktion* $\widehat{f}$ *aus Definition 5.7 ist*

(i) *wohldefiniert,*

(ii) *Scott-stetig und*

(iii) *erhält Konvexkombinationen, d.h.*

$$\widehat{f}\left(r \cdot \mu + (1-r) \cdot \mu'\right) = r \cdot_H \widehat{f}(\mu) +_H (1-r) \cdot_H \widehat{f}(\mu').$$

[4] wieder dient die Forderung lediglich der Konformität mit anderen Quellen. Jede solche Funktion ist Scott-stetig.

**Beweis.**

(i) Wie in Kapitel 3 ist $A_\mu \subseteq \mathcal{V}(S)$.

Da $g \longmapsto \lambda s.\ \int g(t)(s)\,\mathrm{d}\mu(t)$ linear (im sinne von Proposition 4.2) ist, ist $A_\mu$ eine konvexe Menge. Entsprechend ist gemäß Lemma 5.2 auch $\overline{A_\mu} \in \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$.

(ii) Die Monotonie von $\widehat{f}$ weist man direkt nach:

$$\begin{aligned}\mu \leq \mu' &\Longrightarrow \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu(t) \leq \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu'(t)\\ &\Longrightarrow A_\mu \subseteq {\downarrow}A_{\mu'} \subseteq \widehat{f}(\mu')\\ &\Longrightarrow \widehat{f}(\mu) \leq \widehat{f}(\mu').\end{aligned}$$

Sei nun $(\mu_i)_{i\in I}$ gerichtet. Schon aus der Monotonie folgt $\widehat{f}\left(\bigvee^{\uparrow}\mu_i\right) \geq \bigvee^{\uparrow}\widehat{f}(\mu_i)$.

Zeigen wir nun $\widehat{f}\left(\bigvee^{\uparrow}\mu_i\right) \leq \bigvee^{\uparrow}\widehat{f}(\mu_i) \quad\Longleftrightarrow\quad \overline{A_{\bigvee^{\uparrow}\mu_i}} \leq \overline{\bigcup^{\uparrow} A_{\mu_i}}$.

Hierfür genügt es, zu zeigen, daß $A_{\bigvee^{\uparrow}\mu_i} \subseteq \overline{\bigcup^{\uparrow} A_{\mu_i}}$ ist. Sei $x \in A_{\bigvee^{\uparrow}\mu_i}$, also

$$x = \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\Big(\bigvee^{\uparrow}\mu_i\Big)(t).$$

Dann ist nach Proposition 4.2

$$\begin{aligned}x = \bigvee^{\uparrow} &\underbrace{\lambda s.\ \int_S g(t)(s)\,\mathrm{d}\Big(\mu_i\Big)(t)}_{\in A_{\mu_i}}\\ \Longrightarrow\quad x &\in \overline{\bigcup^{\uparrow} A_{\mu_i}}.\end{aligned}$$

(iii) Für beliebige Funktionen $B : S \longrightarrow [0,1]$ ist die Abbildung

$$\mu \longmapsto \int_S B(t)\,\mathrm{d}\mu(t)$$

linear im sinne von Proposition 4.2.

Für jedes $s$ und jedes $g \in \Pi(f)$ ist die Abbildung $t \longmapsto g(t)(s)$ eine solche Abbildung $B$, so daß auch die Abbildung

$$\mu \longmapsto \lambda s.\ \int_S g(t)(s)\,\mathrm{d}\mu(t)$$

linear ist.

Zeigen wir nun, daß $\widehat{f}$ Konvexkombinationen erhält:

$$\begin{aligned}
&\widehat{f}\Big(r \cdot \mu + (1-r) \cdot \mu'\Big) \\
&= \overline{\left\{ \lambda s. r \cdot \int_S g(t)(s)\,\mathrm{d}\mu(t) + (1-r) \cdot \int_S g(t)(s)\,\mathrm{d}\mu'(t) \;\middle|\; g \in \Pi(f) \right\}} \\
&= \overline{\bigcup_{g \in \Pi(f)} \left( r \cdot \left\{ \lambda s. \int_S g(t)(s)\,\mathrm{d}\mu(t) \right\} + (1-r) \cdot \left\{ \lambda s. \int_S g(t)(s)\,\mathrm{d}\mu'(t) \right\} \right)} \\
&\subseteq \overline{\bigcup_{\substack{g \in \Pi(f) \\ g' \in \Pi(f)}} \left( r \cdot \left\{ \lambda s. \int_S g(t)(s)\,\mathrm{d}\mu(t) \right\} + (1-r) \cdot \left\{ \lambda s. \int_S g'(t)(s)\,\mathrm{d}\mu'(t) \right\} \right)} \\
&= r \cdot_H \widehat{f}(\mu) +_H (1-r) \cdot_H \widehat{f}(\mu').
\end{aligned}$$

Die Mengeninklusion in der dritten Zeile gilt aber auch umgekehrt, denn für $g, g' \in \Pi(f)$ können wir stets auch $h \in \Pi(f)$ finden mit

$$\begin{aligned}
&\left( r \cdot \lambda s. \int_S g(t)(s)\,\mathrm{d}\mu(t) + (1-r) \cdot \lambda s. \int_S g'(t)(s)\,\mathrm{d}\mu'(t) \right\} \\
=&\left( r \cdot \lambda s. \int_S h(t)(s)\,\mathrm{d}\mu(t) + (1-r) \cdot \lambda s. \int_S h(t)(s)\,\mathrm{d}\mu'(t) \right).
\end{aligned}$$

Dabei gehen wir wie folgt vor. Für $\mu(t) = 0$ wählen wir $h(t) = g'(t)$.

Für $\mu(t) > 0, \mu'(t) = 0$ wählen wir $h(t) = g(t)$. Im verbleibenden Fall ist $\mu(t) \cdot \mu'(t) > 0$ und wir wählen

$$h(t) = \frac{r \cdot \mu(t) \cdot g(t) + (1-r) \cdot \mu'(t) \cdot g'(t)}{r \cdot \mu(t) + (1-r) \cdot \mu'(t)}.$$

Im letzten Fall ist $h(t) \in f(t)$, da $f(t)$ konvex ist und

$$\frac{(1-r) \cdot \mu'(t)}{r \cdot \mu(t) + (1-r) \cdot \mu'(t)} = 1 - \frac{r \cdot \mu(t)}{r \cdot \mu(t) + (1-r) \cdot \mu'(t)}$$

gilt.

□

**Bemerkung.** Für $\sigma \in S$ haben wir

$$\begin{aligned}
\widehat{f}(\eta_\sigma) &= \overline{\left\{ \lambda s. \int_S g(t)(s)\,\mathrm{d}\eta_\sigma(t) \;\middle|\; g \in \Pi(f) \right\}} \\
&= \overline{\left\{ \lambda s. \int_{\uparrow\{\sigma\}} g(t)(s)\,\mathrm{d}\eta_\sigma(t) + \int_{S\setminus\uparrow\{\sigma\}} g(t)(s)\,\mathrm{d}\eta_\sigma(t) \;\middle|\; g \in \Pi(f) \right\}} \\
&= \overline{\left\{ \lambda s. \int_{\uparrow\{\sigma\}=\{\sigma\}} g(t)(s)\,\mathrm{d}\eta_\sigma(t) + 0 \;\middle|\; g \in \Pi(f) \right\}} \\
&= \overline{\left\{ \lambda s.\, g(\sigma)(s) \;\middle|\; g \in \Pi(f) \right\}} = \overline{\left\{ g(\sigma) \;\middle|\; g \in \Pi(f) \right\}} \\
&= \overline{f(\sigma)} = {\downarrow} f(\sigma) = f(\sigma),
\end{aligned}$$

die Bezeichnung „Fortsetzung" ist also angemessen.

**Definition 5.9.** Es sei wiederum $f : S \longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ eine Scott-stetige[5] Funktion. Dann definieren wir die **Fortsetzung von** $f$ **auf** $\mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ als:

$$\begin{aligned}
f^\dagger : \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S) &\longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S) \\
P &\longmapsto \overline{\cup \widehat{f}[P]}
\end{aligned}$$

**Satz 5.10.** *Die Funktion $f^\dagger$ aus Definition 5.9 ist*

(i) *wohldefiniert und*

(ii) *Scott-stetig.*

**Beweis.**

(i) Nach Satz 5.8 (iii) ist $\widehat{f}[P]$ konvex, da $P$ konvex ist. Also ist auch $\cup\widehat{f}[P]$ konvex und somit $f^\dagger(P) \in \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ (Lemma 5.2).

(ii) Es ist $P \leq Q \Longrightarrow P \subseteq Q \Longrightarrow \widehat{f}[P] \subseteq \widehat{f}[Q] \Longrightarrow f^\dagger(P) \leq f^\dagger(Q)$.
Sei nun $(A_i)_{i\in I}$ eine gerichtete Menge in $\mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$. Wegen Lemma 5.4 ist zunächst

$$\overline{\bigcup\nolimits^{\uparrow}_i \widehat{f}[A_i]} = \overline{\widehat{f}\left[\bigcup\nolimits^{\uparrow}_i A_i\right]},$$

somit folgt aber direkt

$$\bigsqcap_i f^\dagger(A_i) = \overline{\bigcup\nolimits^{\uparrow}_i f^\dagger(A_i)} = \overline{\bigcup\nolimits^{\uparrow}_i \overline{\cup\widehat{f}(A_i)}} = \overline{\cup\overline{\bigcup\nolimits^{\uparrow}_i \widehat{f}(A_i)}} = \overline{\cup\widehat{f}\left(\bigsqcap_i A_i\right)} = f^\dagger\left(\bigsqcap_i A_i\right).$$

[5] wieder dient die Forderung lediglich der Konformität mit anderen Quellen. Jede solche Funktion ist Scott-stetig.

□

## 5.3 Direkte Semantik in $\mathfrak{P}_{\mathsf{H}}\mathcal{V}(S)$

Für ein pGCL-Programm $P$ ist $[\![P]\!]_{\mathrm{H}} : S \longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ eine Scott-stetige Funktion. Diese direkte Semantik können wir nun definieren:

**Definition 5.11.** Die **direkte (Hoare-)Semantik** von pGCL-Programmen ist über den Termaufbau rekursiv folgendermaßen definiert:

$$
\begin{aligned}
[\![\texttt{assign}_f]\!]_{\mathrm{H}}(s) &:= \widehat{\eta}(f(s)) = \downarrow \eta_{f(s)} \\
[\![\texttt{abort}]\!]_{\mathrm{H}}(s) &:= \bot = \{\mathbf{0}\} \\
[\![\texttt{skip}]\!]_{\mathrm{H}}(s) &:= \widehat{\eta}(s) = \downarrow \eta_s \\
[\![P\,;Q]\!]_{\mathrm{H}}(s) &:= [\![Q]\!]^{\dagger}_{\mathrm{H}}\big([\![P]\!]_{\mathrm{H}}(s)\big) \\
[\![\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi}]\!]_{\mathrm{H}}(s) &:= [\![b]\!](s) \cdot [\![P]\!]_{\mathrm{H}}(s) + [\![\neg b]\!](s) \cdot [\![Q]\!]_{\mathrm{H}}(s) \\
&= ([\![b]\!](s) \wedge [\![P]\!]_{\mathrm{H}}(s)) \vee ([\![\neg b]\!](s) \wedge [\![Q]\!]_{\mathrm{H}}(s)) \\
[\![P \,{}_p\!\oplus\, Q]\!]_{\mathrm{H}}(s) &:= p \cdot_H [\![P]\!]_{\mathrm{H}}(s) +_H (1-p) \cdot_H [\![Q]\!]_{\mathrm{H}}(s) \\
[\![P \sqcap Q]\!]_{\mathrm{H}}(s) &:= \overline{\bigcup_{0 \le p \le 1} p \cdot_H [\![P]\!]_{\mathrm{H}}(s) +_H (1-p) \cdot_H [\![Q]\!]_{\mathrm{H}}(s)} \\
[\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!]_{\mathrm{H}} &:= \mu f.\lambda s.[\![b]\!](s) \cdot_H f^{\dagger}\big([\![P]\!]_{\mathrm{H}}(s)\big) +_H [\![\neg b]\!](s) \cdot_H \downarrow \eta_s
\end{aligned}
$$

Dabei ist $\mu(f) = \bigsqcup_{n=0}^{\infty} f^n(\bot)$.

**Proposition 5.12.** *Die Semantik aus Definition 5.11 ist wohldefiniert, insbesondere ist*

$$
\begin{gathered}
[\![P\,;Q]\!]_H(s) \in \mathfrak{P}_H\mathcal{V}(S), \\
[\![P \,{}_p\!\oplus\, Q]\!]_H(s) \in \mathfrak{P}_H\mathcal{V}(S) \textit{ und} \\
[\![P \sqcap Q]\!]_H(s) \in \mathfrak{P}_H\mathcal{V}(S).
\end{gathered}
$$

**Beweis.** Da $[\![P]\!]_{\mathrm{H}}s$ und $[\![Q]\!]_{\mathrm{H}}s$ in jedem Fall Elemente des Hoare-Powerdomains sind, sind sie konvex. Mengen der Form $r \cdot [\![P]\!]_{\mathrm{H}}s + (1-r) \cdot [\![Q]\!]_{\mathrm{H}}s$ sind dann wieder konvex und nichtleer. Entsprechend ist ihr Abschluß jeweils ein Element des Hoare-Powerdomains. Deswegen ist $[\![P \,{}_p\!\oplus\, Q]\!]_{\mathrm{H}}(s) \in \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$.

Als konvexe Vereinigung konvexer nichtleerer Mengen ist auch

$$
\bigcup_{0 \le p \le 1} p \cdot_H [\![P]\!]_{\mathrm{H}}(s) +_H (1-p) \cdot_H [\![Q]\!]_{\mathrm{H}}(s)
$$

konvex und nichtleer; entsprechend ist $[\![P \sqcap Q]\!]_{\mathrm{H}}(s) \in \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$.

Die Wohldefiniertheit von $[\![Q]\!]^{\dagger}_{\mathrm{H}}([\![P]\!]_{\mathrm{H}}(s))$ haben wir in Satz 5.10 gezeigt.

Die Wohldefiniertheit der anderen Fälle ist leicht einzusehen. □

**Bemerkung.** Im Gegensatz zum Smyth-Fall, wo $[\![P \sqcap Q]\!](s)$ gerade das Infimum in $\mathfrak{P}_{\mathrm{Sm}}\mathcal{V}(S)$ war, ist hier $[\![P \sqcap Q]\!]_{\mathrm{H}}(s)$ das Supremum von $[\![P]\!]_{\mathrm{H}}(s)$ und $[\![Q]\!]_{\mathrm{H}}(s)$ in $\mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$. Das motiviert dazu, den Nondeterminismus im Hoare-Falle auch als *angelischen* Nondeterminismus zu bezeichnen.

*Alles ist richtig, auch das Gegenteil.*
*Nur „zwar – aber", das ist nie richtig.*
*(Kurt Tucholsky)*

# 6 wlp-Semantik

## 6.1 Motivation

Wir haben in Theorem 4.5 gesehen, daß wp uns eine *predicate transformer*-Semantik liefert, die auf intuitive Weise rekursiv über den Termaufbau definiert werden kann. Dabei wird die while-Schleife, wie in der direkten Semantik auch, durch einen kleinsten Fixpunkt interpretiert.

Um die etablierten Methoden der Schleifenverifikation mittels Invariantenkalkül anwenden zu können, braucht man jedoch eine *predicate transformer*-Semantik, die für die Schleife einen größten Fixpunkt liefert.

Es sei $I \in \mathcal{E}(S)$ ein probabilistisches Prädikat und $I \leq \Big([\![b]\!] \wedge \mathsf{wp}([\![P]\!])(I)\Big) \vee ([\![\neg b]\!] \cdot B)$. Dann ist

$$I \leq \nu X.\ \Big((([\![b]\!] \wedge \mathsf{wp}(P)(X)) \vee ([\![\neg b]\!] \wedge B)\Big),$$

wobei $\nu$ nun der Größter-Fixpunkt-Operator ist. Entsprechend ist der größte Fixpunkt gerade das Supremum all dieser $I$.

Aus diesem Grunde schlagen McIver und Morgan in [MM04] eine Variante der *predicate transformer*-Semantik vor, die *partielle Korrektheit* faßt und Schleifen als größte Fixpunkte interpretiert. Diese Variante heißt bei ihnen wie bei uns wlp. Sie geben allerdings keinen Beweis dafür, daß wlp, wie es als Funktion auf der direkten Semantik von Programmen definiert ist, unseren Ansprüchen genügt und die Gleichungen einer rekursiven Definition über den Termaufbau erfüllt.

Die Definition von wlp wird sich sehr eng an der Definition von wp orientieren. Der Unterschied der beiden wird vor allem deutlich, wenn man den Befehl `abort` betrachtet. Der *predicate transformer* $\mathsf{wp}([\![\texttt{abort}]\!])$ ordnet jedem probabilistischen Prädikat $B$ das $\bot$-Element zu, während $\mathsf{wlp}([\![\texttt{abort}]\!]_{\mathrm{H}})(B)$ für beliebiges $B$ stets erfüllt ist. Während wp monoton ist, ist wlp über flachem Zustandsraum antiton.

Wir entwickeln nacheinander eine wlp-Semantik für deterministische Programme, probabilistische Programme und nichtdeterministische probabilistische Programme und beweisen in allen drei Fällen, daß $\mathsf{wlp}([\![\texttt{while}\ b\ \texttt{do}\ P\ \texttt{od}]\!]_{\mathrm{H}})(B)$ für jede Nachbedingung $B$ der gewünschte größte Fixpunkt ist. Im dritten und allgemeinen Fall formulieren wir dann in Theorem 6.14 die Gleichungen, die wlp erfüllt und mittels derer es als Funktion rekursiv auf dem Termaufbau aufgefaßt werden kann.

Hierbei treten die Räume $[0,1]$, $\Big[\mathfrak{P}S \longrightarrow \mathfrak{P}S\Big]$ und $\Big[\mathcal{E}(S) \longrightarrow \mathcal{E}(S)\Big]$ jeweils mit der umgekehrten Ordnung auf.

Auch diese drei Räume $[0,1]^{\mathsf{op}}$, $\Big[\mathfrak{P}(S) \longrightarrow \mathfrak{P}(S)\Big]^{\mathsf{op}}$ und $\Big[\mathcal{E}(S) \longrightarrow \mathcal{E}(S)\Big]^{\mathsf{op}}$ sind Bereiche, bei allen dreien handelt es sich sogar um vollständige Verbände (siehe Lemma 0.3).

## 6.2 wlp-Semantik im deterministischen Fall

Beschränken wir uns zunächst auf den deterministischen Fall, wo die direkte Semantik eines Programms gerade eine Scott-stetige Funktion in $\left[S \longrightarrow S_\perp\right]$ ist und Prädikate nichts anderes als Teilmengen des Zustandsraumes. Die Rolle von $\mathcal{E}(S)$ übernimmt hier also $\mathfrak{P}(S)$ mit der Inklusionsordnung.

Wir definieren im deterministischen Falle wie folgt:

**Definition 6.1.** Es sei $f \in \left[S \longrightarrow S_\perp\right]$, dann ist die **weakest liberal precondition** von $f$ bezüglich $B$ definiert als

$$\mathsf{wlp}(f)(B) = f^{-1}\left(B \cup \{\perp\}\right).$$

**Bemerkung.** Durch diese Definition ergibt sich die Äquivalenz

$$\begin{aligned} s \in \mathsf{wlp}(f)(B) \quad &\Longleftrightarrow \quad f(s) \in B \cup \{\perp\} \\ &\Longleftrightarrow \quad \Big(f(s) \neq \perp \Longrightarrow f(s) \in B\Big), \end{aligned}$$

so daß wlp der oben angegebenen intuitiven Bedeutung entspricht. „Falls es terminiert, so garantiert es mir $B$."

Offenbar erhält wlp beliebige Vereinigungen und nichtleere Schnitte und ist antiton.

**Lemma 6.2.** *Für jede aufsteigende $\omega$-Kette $(f_n)_{n\in\mathbb{N}}$ in $\left[S \longrightarrow S_\perp\right]$ gilt:*

$$\mathsf{wlp}\Big(\bigvee_{n\in\mathbb{N}} f_n\Big)(B) = \bigcap_{n\in\mathbb{N}} \mathsf{wlp}(f_n)(B).$$

**Beweis.**

$$\begin{aligned} s \in \mathsf{wlp}\Big(\bigvee f_n\Big)(B) \quad &\Longleftrightarrow \quad \Big(\big(\exists n \in \mathbb{N}\big)\, f_n(s) \in B\Big) \vee \Big(\big(\forall n \in \mathbb{N}\big)\, f_n(s) = \perp\Big) \\ &\Longleftrightarrow \quad \Big(\forall n \in \mathbb{N}\Big)\, \Big(\Big(\big(\exists n \in \mathbb{N}\big)\, f_n(s) \in B\Big) \vee f_n(s) = \perp\Big) \\ &\Longleftrightarrow \quad \Big(\forall n \in \mathbb{N}\Big)\, \Big(f_n(s) \neq \perp \Longrightarrow \big(\exists n \in \mathbb{N}\big)\, f_n(s) \in B\Big) \\ (*) \quad &\Longleftrightarrow \quad \Big(\forall n \in \mathbb{N}\Big)\, \big(f_n(s) \neq \perp \Longrightarrow f_n(s) \in B\big) \\ &\Longleftrightarrow \quad \Big(\forall n \in \mathbb{N}\Big)\, s \in \mathsf{wlp}(f_n)(B) \\ &\Longleftrightarrow \quad s \in \bigcap_{n\in\mathbb{N}} \mathsf{wlp}(f_n)(B). \end{aligned}$$

Die Äquivalenz bei $(*)$ folgt daraus, daß $S$ ein flacher Bereich und $(f_n)$ eine Kette ist. □

Wir schließen, daß die Funktion wlp von $\left[S \longrightarrow S_\perp\right]$ nach $\left[\mathfrak{P}(S) \longrightarrow \mathfrak{P}(S)\right]^{\mathsf{op}}$ im deterministischen Fall Scott-stetig ist.

Wir wollen nun sehen, daß in diesem deterministischen Falle die wlp-Semantik der `while`-Schleife die gewünschte Gleichheit

$$\mathsf{wlp}(\texttt{while}\ b\ \texttt{do}\ P\ \texttt{od})(B) = \nu X.([\![b]\!] \cap \mathsf{wlp}([\![P]\!])(X)) \cup ([\![\neg b]\!] \cap B)$$

erfüllt. Im deterministischen Kontext ist $[\![b]\!] \subseteq S$ und $[\![\neg b]\!] = S \setminus [\![b]\!]$.
Zur Vereinfachung der Notation definieren wir

$$\begin{aligned}
\Psi : \left[S \longrightarrow S_\perp\right] &\longrightarrow \left[S \longrightarrow S_\perp\right] \\
g &\longmapsto \left( s \longmapsto \begin{cases} g([\![P]\!](s)) & \text{für } s \in [\![b]\!] \\ s & \text{sonst.} \end{cases} \right) \\
\Phi_B : \mathfrak{P}(S) &\longrightarrow \mathfrak{P}(S) \\
X &\longmapsto ([\![b]\!] \cap \mathsf{wlp}([\![P]\!])(X)) \cup ([\![\neg b]\!] \cap B).
\end{aligned}$$

**Lemma 6.3.** *Die Funktion $\Phi_B$ erhält Infima absteigender Ketten.*

**Beweis.** Es sei eine absteigende Kette $(X_n)_{n\in\mathbb{N}}$ in $\mathfrak{P}(S)$ gegeben. Dann ist

$$\begin{aligned}
\Phi_B\left(\bigcap_{n\in\mathbb{N}} X_n\right) &= \left([\![b]\!] \cap \mathsf{wlp}([\![P]\!])\left(\bigcap_{n\in\mathbb{N}} X_n\right)\right) \cup ([\![\neg b]\!] \cap B) \\
&= \left([\![b]\!] \cap [\![P]\!]^{-1}\left(\bigcap_{n\in\mathbb{N}} X_n\right)\right) \cup \underbrace{([\![\neg b]\!] \cap B) \cup \left([\![b]\!] \cap [\![P]\!]^{-1}(\{\perp\})\right)}_{M} \\
&= \left([\![b]\!] \cap [\![P]\!]^{-1}\left(\bigcap_{n\in\mathbb{N}} X_n\right)\right) \cup M \\
&= \left([\![b]\!] \cap \bigcap_{n\in\mathbb{N}} [\![P]\!]^{-1}(X_n)\right) \cup M \\
&= \bigcap_{n\in\mathbb{N}} \left([\![b]\!] \cap [\![P]\!]^{-1}(X_n)\right) \cup M \\
&= \bigcap_{n\in\mathbb{N}} \left([\![b]\!] \cap [\![P]\!]^{-1}(X_n) \cup M\right) = \bigcap_{n\in\mathbb{N}} \Phi_B(X_n).
\end{aligned}$$

□

Zeigen wir nun das wesentliche Resultat:

**Satz 6.4.** *Für alle $B \subseteq S$ gilt:*

$$\mathsf{wlp}([\![\texttt{while}\ b\ \texttt{do}\ P\ \texttt{od}]\!])(B) = \nu\Phi_B,$$

**Beweis.** Per Definition ist

$$\mathsf{wlp}([\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!])(B) = (\mu\Psi)^{-1}(B \cup \{\bot\}).$$

Es ist $\mu\Psi$ das Supremum der aufsteigenden Kette $\Psi^n(\bot)$, wobei $\bot$ in diesem Kontext die Funktion $\lambda s.\lambda s'.0$ ist.

Andererseits ist wegen Lemma 6.3 $\nu\Phi_B$ das Infimum der absteigenden Kette $\Phi_B^n(S)$, denn $S$ ist das größte Prädikat.

Es genügt also zu zeigen, daß

$$(\Psi^n(\lambda s.\ \bot))^{-1}(B \cup \{\bot\}) = \Phi_B^n(S)$$

gilt. Dies tun wir per Induktion über $n$.

Für $n = 0$ erhält man $(\lambda s.\ \bot)^{-1}(B \cup \{\bot\}) = S = \Phi_B^0(S)$.

Gelte nun als Induktionshypothese die Aussage bereits für $n = i$. Dann haben wir

$$\begin{aligned}(\Psi^{i+1}(\lambda s.\ \bot)^{-1}(B \cup \{\bot\}) &= (b \cap f^{-1}((\Psi^i(\lambda s.\ \bot))^{-1}(B \cup \{\bot\})) \cup (\neg b \cup B)\\ &\overset{\text{(I.H.)}}{=} (b \cap f^{-1}(\Phi_B^i(S)) \cup (\neg b \cup B)\\ &= \Phi_B^{i+1}(S).\end{aligned}$$

□

## 6.3 wlp-Semantik im probabilistischen Fall

Als nächstes betrachten wir Programme mit probabilistischem, aber ohne nichtprobablisitischen Nondeterminismus, für welche die direkte Semantik gegeben ist durch Scott-stetige Funktionen $f : S \longrightarrow \mathcal{V}(S)$. Für diese definieren wir die wlp-Semantik wie folgt:

**Definition 6.5.** Für eine Scott-stetige Funktion $f : S \longrightarrow \mathcal{V}(S)$ definieren wir die **weakest liberal preexpectation** als Funktion in $\left[\mathcal{E}(S) \longrightarrow \mathcal{E}(S)\right]$ durch

$$\mathsf{wlp}(f)(B)(s) = \mathsf{wp}(f)(B)(s) + f(s)(\bot).$$

**Lemma 6.6.** *Die Funktion* wlp *erfüllt die zu erwartende Gleichheit*

$$\mathsf{wlp}(f)(B) = 1 - \mathsf{wp}(f)(1 - B).$$

**Beweis.** Wir rechnen direkt nach:

$$\begin{aligned}\mathsf{wlp}(f)(B)(s) &= \mathsf{wp}(f)(B) + f(s)(\bot)\\ &= \sum_{t \in S} B(t) \cdot f(s)(t) + 1 - \sum_{t \in S} f(s)(t)\\ &= 1 - \sum_{t \in S} (1 - B(t)) \cdot f(s)(t)\\ &= 1 - \mathsf{wp}(f)(1 - B)(s)\end{aligned}$$

□

Da $\mathsf{wp}(f)$ stetig ist, folgt die Stetigkeit von $\mathsf{wlp}(f)$ unmittelbar aus der Definition. Aus dem Lemma folgt die Antitonie von $\mathsf{wlp}$.

Ferner ist $\mathsf{wlp}\big(\bigvee_{n\in\mathbb{N}} f_n\big)$ das punktweise Infimum der absteigenden Folge $\mathsf{wlp}(f_n)$:

$$\begin{aligned}\mathsf{wlp}\Big(\bigvee_{n\in\mathbb{N}} f_n\Big)(B)(s) &= 1 - \sum_{t\in S}(1-B(t))\cdot\Big(\bigvee_{n\in\mathbb{N}} f_n(s)(t)\Big)\\ &= 1 - \bigvee_{n\in\mathbb{N}}\sum_{t\in S}(1-B(t))\cdot f_n(s)(t)\\ &= \bigwedge_{n\in\mathbb{N}}\left(1-\sum_{t\in S}(1-B(t))\cdot f_n(s)(t)\right)\\ &= \bigwedge_{n\in\mathbb{N}}\mathsf{wlp}(f_n)(B)(s).\end{aligned}$$

Seien nun $[\![b]\!] \subseteq S$ und $[\![P]\!] = f : S \longrightarrow \mathcal{V}(S)$ gegeben, so ist die direkte Semantik von `while` $b$ `do` $P$ `od` durch den kleinsten Fixpunkt von $\Psi$ gegeben, wobei

$$\begin{aligned}\Psi : \big[S \longrightarrow \mathcal{V}(S)\big] &\longrightarrow \big[S \longrightarrow \mathcal{V}(S)\big]\\ \Psi(g)(s) &= \begin{cases}(f;g)(s) & \text{für } s \in [\![b]\!] = b\\ \eta_s & \text{sonst}\end{cases}\end{aligned}$$

mit

$$\begin{aligned}(f;g)(s)(s') &= \sum_{t\in S} g(t)(s')\cdot f(s)(t),\\ \eta_s(s') &= \begin{cases}1 & \text{für } s = s'\\ 0 & \text{sonst.}\end{cases}\end{aligned}$$

Es sei

$$\begin{aligned}\Phi_B : \mathcal{E}(S) &\longrightarrow \mathcal{E}(S)\\ X &\longmapsto ([\![b]\!] \wedge \mathsf{wlp}(f)(X)) \vee ([\![\neg b]\!] \wedge B).\end{aligned}$$

Wir werden die folgenden drei Lemmata benötigen:

**Lemma 6.7.** *Die Funktion $\Phi_B$ erhält Infima absteigender Ketten.*

**Beweis.** Für eine absteigende Kette $(X_i)_{n\in\mathbb{N}}$ in $\mathcal{E}(S)$ haben wir

$$\begin{aligned}\Phi_B\left(\bigwedge_{n\in\mathbb{N}} X_n\right)(s) &= \mathsf{wp}(f)\left(\bigwedge_{n\in\mathbb{N}} X_n\right)(s) + f(s)(\bot)\\ &= \int_S \bigwedge_{n\in\mathbb{N}} X_n(t)\,\mathrm{d}f(s)(t) + f(s)(\bot)\\ &= \bigwedge_{n\in\mathbb{N}} \int_S X_n(t)\,\mathrm{d}f(s)(t) + f(s)(\bot)\\ &= \bigwedge_{n\in\mathbb{N}} \Phi_B(X_n)(s)\end{aligned}$$

□

**Lemma 6.8.** *Für die* wlp *von der Hintereinanderausführung zweier Programme gilt*

$$\mathsf{wlp}(f\,;g)(B)(s) = \mathsf{wlp}(f)(\mathsf{wlp}(g)(B))(s).$$

**Beweis.** Mit den Ergebnissen von Kapitel 4 sieht man ein, daß auch im probabilistischen Fall die Gleichung $\mathsf{wp}(f\,;g)(B) = \mathsf{wp}(f)(\mathsf{wp}(g)(B))$ gilt. Damit folgt

$$\begin{aligned}\mathsf{wlp}(f\,;g)(B)(s) &= 1 - \mathsf{wp}(f\,;g)(1-B)(s)\\ &= 1 - \mathsf{wp}(f)(\mathsf{wp}(g)(1-B))(s)\\ &= \mathsf{wlp}(f)(1 - \mathsf{wp}(g)(1-B))(s)\\ &= \mathsf{wlp}(f)(\mathsf{wlp}(g)(B))(s).\end{aligned}$$

□

**Lemma 6.9.** *Für alle g gilt*

$$\mathsf{wlp}(\Psi(g))(B) = \Phi_B(\mathsf{wlp}(g)(B))$$

**Beweis.**

$$\begin{aligned}\mathsf{wlp}(\Psi(g))(B) &= \lambda s.1 - \sum_{\sigma\in S}(1-B(\sigma))\cdot(b(s)\cdot(f;g)(s)(\sigma) + (1-b(s))\eta_s(\sigma))\\ &= s \mapsto \begin{cases}1 - \sum_{\sigma\in S}(1-B(\sigma))\cdot(f;g)(s)(\sigma) & \text{für } b(s)=1\\ 1 - \sum_{\sigma\in S}(1-B(\sigma))\cdot\eta_s(\sigma) & \text{sonst. } (\Longrightarrow b(s)=0)\end{cases}\\ &= s \mapsto \begin{cases}\mathsf{wlp}(f)(\mathsf{wlp}(g)(B))(s) & \text{für } b(s)=1\\ 1 - \sum_{\sigma\in\{s\}}(1-B(\sigma)) & \text{sonst.}\end{cases}\\ &= s \mapsto \begin{cases}\mathsf{wlp}(f)(\mathsf{wlp}(g)(B))(s) & \text{für } b(s)=1\\ B(s) & \text{sonst.}\end{cases}\\ &= b\cdot\mathsf{wlp}(f)(\mathsf{wlp}(g)(B)) + ((1-b)\cdot B)\\ &= \Phi_B(\mathsf{wlp}(g)(B)),\end{aligned}$$

wobei die dritte Gleichheit gerade in Lemma 6.8 nachgewiesen wurde. □

Es gilt nun wieder, die gewünschte Gleichheit zu beweisen:

**Satz 6.10.** *Für alle $B \in \mathcal{E}(S)$ gilt:*

$$\mathsf{wlp}(\texttt{while}\ b\ \texttt{do}\ P\ \texttt{od})(B) = \nu(\Phi_B)$$

**Beweis.**
Da $\Phi_B$ Infima absteigender Ketten erhält, genügt es wiederum zu zeigen, daß

$$\mathsf{wlp}(\Psi^n(\lambda s.\lambda s'.0))(B) = \Phi_B^n(S)$$

gilt. Dies tun wir per Induktion über $n$.
Für $n = 0$ erhält man wie gewünscht $\mathsf{wlp}([\![\texttt{abort}]\!])(B) = \lambda s.1$.
Gelte nun als Induktionshypothese die Aussage bereits für $n = i$. Dann haben wir

$$\begin{aligned}
\mathsf{wlp}(\Psi^{i+1}(\lambda s.\lambda s'.0)(B) &= \mathsf{wlp}(\Psi\Psi^i(\lambda s.\lambda s'.0))(B) \\
&= \Phi_B(\mathsf{wlp}(\Psi^i(\lambda s.\lambda s'.0))(B)) && \text{(wegen 6.9)} \\
&= \Phi_B\Phi_B^i(\lambda s.1) && \text{(IH)} \\
&= \Phi_B^{i+1}(\lambda s.1).
\end{aligned}$$

□

## 6.4 wlp-Semantik im allgemeinen Fall

Schließlich betrachten wir wieder den allgemeinen Fall, in dem sowohl nicht probabilistischer, als auch probabilistischer Nondeterminismus zugelassen sind. Nun ist die direkte Semantik eines Programms $[\![P]\!]_{\mathrm{H}}$ gegeben durch eine Funktion $f : S \longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$. Wir definieren die wlp-Semantik in Anlehnung an Definition 6.5:

**Definition 6.11.** Für eine Scott-stetige Funktion $f : S \longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{V}(S)$ definieren wir die **weakest liberal preexpectation** von $f$ als Funktion in $\left[\mathcal{E}(S) \longrightarrow \mathcal{E}(S)\right]$ durch

$$\mathsf{wlp}(f)(B)(s) = \bigwedge_{\mu \in f(s)} 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t).$$

Es ist

$$1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) = \mu(\bot) + \langle B, \mu \rangle,$$

also entspricht die Funktion wlp der Intuition.

**Proposition 6.12.**

(i) *Für $B \in \mathcal{E}(S)$ ist die Abbildung*

$$\begin{aligned} \mathcal{V}(S) &\longrightarrow [0,1]^{\mathsf{op}} \\ \mu &\longmapsto 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \end{aligned}$$

*monoton und Scott-stetig.*

(ii) *Die Funktion $\mathsf{wlp}(f) : \mathcal{E}(S) \longrightarrow \mathcal{E}(S)$ ist Scott-stetig.*

(iii) *Die Funktion $\mathsf{wlp}$ ist antiton und für eine aufsteigende Kette $(f_n)_{n \in \mathbb{N}}$ ist*

$$\mathsf{wlp}\left(\bigvee_{n \in \mathbb{N}} f_n\right) = \bigwedge_{n \in \mathbb{N}} \mathsf{wlp}(f_n).$$

**Beweis.**

(i) Da nach Proposition 4.2 für $B' \coloneqq (1 - B)$ die Abbildung

$$(B', \mu) \longmapsto \sum_{t \in S} B'(t) \cdot \mu(t)$$

Scott-stetig ist, ist auch

$$\mu \longmapsto \sum_{t \in S} (1 - B(t)) \cdot \mu(t)$$

eine monotone Scott-stetige Funktion von $\mathcal{V}(S)$ nach $[0,1]$.
Da in $[0,1]$ die Gleichung

$$1 - \bigvee_{a \in A} a = \bigwedge_{a \in A} (1 - a)$$

gilt, ist

$$\mu \longmapsto 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t)$$

eine Scott-stetige Abbildung von $\mathcal{V}(S)$ nach $[0,1]^{\mathsf{op}}$.

(ii) Die Monotonie sieht man direkt:

$$\begin{aligned} B \leq C &\Longrightarrow \Big(\forall t \in S\Big)\, B(t) \leq C(t) \\ &\Longrightarrow \Big(\forall t \in S\Big)\Big(\forall \mu \in \mathcal{V}(S)\Big)\, (1 - B(t)) \cdot \mu(t) \geq (1 - C(t)) \cdot \mu(t) \\ &\Longrightarrow \Big(\forall \mu \in \mathcal{V}(S)\Big) \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \geq \sum_{t \in S} (1 - C(t)) \cdot \mu(t) \\ &\Longrightarrow \Big(\forall \mu \in \mathcal{V}(S)\Big)\, 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \leq 1 - \sum_{t \in S} (1 - C(t)) \cdot \mu(t) \\ &\Longrightarrow \mathsf{wlp}(f)(B) \leq \mathsf{wlp}(f)(C). \end{aligned}$$

Sei nun $(B_i)_{i\in I}$ gerichtet.

$$\begin{aligned}
\mathsf{wlp}(f)(\bigvee\!\!\!\nearrow_i B_i) &= \lambda s.\ \bigwedge_{\mu\in f(s)} 1 - \sum_{t\in S}(1 - \bigvee\!\!\!\nearrow_i B_i(t))\cdot\mu(t)\\
&= \lambda s.\ \bigwedge_{\mu\in f(s)} 1 - \sum_{t\in S}\bigwedge_i (1 - B_i(t))\cdot\mu(t)\\
&= \lambda s.\ \bigwedge_{\mu\in f(s)} 1 - \bigwedge_i \sum_{t\in S}(1 - B_i(t))\cdot\mu(t) && \text{Lemma 0.4}\\
&= \lambda s.\ \bigwedge_{\mu\in f(s)} \bigvee\!\!\!\nearrow_i 1 - \sum_{t\in S}(1 - B_i(t))\cdot\mu(t)\\
&= \lambda s.\ \bigvee\!\!\!\nearrow_i \bigwedge_{\mu\in f(s)} 1 - \sum_{t\in S}(1 - B_i(t))\cdot\mu(t) && \text{Satz 5.5}\\
&= \bigvee\!\!\!\nearrow_i \mathsf{wlp}(f)(B_i).
\end{aligned}$$

(iii) Es seien $f \le f' \in \left[S \longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{Y}(S)\right]$ gegeben. Dann ist für alle $s \in S$ stets $f(s) \le f'(s)$, das bedeutet $f(s) \subseteq f'(s)$. Es folgt

$$\begin{aligned}
\mathsf{wlp}(f)(B)(s) &= \bigwedge_{\mu\in f(s)} 1 - \sum_{t\in S}(1 - B(t))\cdot\mu(t)\\
&\ge \bigwedge_{\mu\in f'(s)} 1 - \sum_{t\in S}(1 - B(t))\cdot\mu(t)\\
&= \mathsf{wlp}(f')(B)(s).
\end{aligned}$$

Sei nun eine aufsteigende Kette $(f_n)_{n\in\mathbb{N}}$ in $\left[S \longrightarrow \mathfrak{P}_{\mathrm{Sm}}\mathcal{Y}(S)\right]$ gegeben. Dann ist wegen Satz 5.5 und (ii)

$$\mathsf{wlp}\Big(\bigvee_{n\in\mathbb{N}} f_n\Big) = \bigwedge_{n\in\mathbb{N}} \mathsf{wlp}(f_n).$$

□

Wieder führen wir Notation ein, um die auftauchenden Fixpunkte bei der `while`-Schleife abzukürzen:

$$\begin{aligned}
\Psi\ :\ \left[S \longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{Y}(S)\right] &\longrightarrow \left[S \longrightarrow \mathfrak{P}_{\mathrm{H}}\mathcal{Y}(S)\right]\\
\Psi(g)(s)\ &=\ \Big(b(s) \wedge g^{\dagger}\big(f(s)\big)\Big) \vee \big((1 - b(s)) \wedge \downarrow\eta_s\big),\\
\Phi_B\ :\ \mathcal{E}(S) &\longrightarrow \mathcal{E}(S)\\
X &\longmapsto (\llbracket b\rrbracket \wedge \mathsf{wlp}(\llbracket P\rrbracket)(X)) \vee (\llbracket\neg b\rrbracket \wedge B).
\end{aligned}$$

Wieder zeigen wir als Lemma:

**Lemma 6.13.** *Für beliebiges $B \in \mathcal{E}(S)$ erhält die Funktion $\Phi_B$ Infima absteigender Ketten.*

**Beweis.** Es gilt

$$\begin{aligned}
\mathsf{wlp}([\![P]\!])\left(\bigwedge_{n\in\mathbb{N}} X_n\right) &= \lambda s.\ \bigwedge_{\mu\in[\![P]\!](s)} 1 - \sum_{t\in S}\left(1 - \bigwedge_{n\in\mathbb{N}} X_n(t)\right)\cdot\mu(t)\\
&= \lambda s.\ \bigwedge_{\mu\in[\![P]\!](s)} 1 - \bigvee_{n\in\mathbb{N}}\sum_{t\in S}(1 - X_n(t))\cdot\mu(t)\\
&= \lambda s.\ \bigwedge_{n\in\mathbb{N}}\bigwedge_{\mu\in[\![P]\!](s)} 1 - \sum_{t\in S}(1 - X_n(t))\cdot\mu(t)\\
&= \bigwedge_{n\in\mathbb{N}} \mathsf{wlp}([\![P]\!])(X_n),
\end{aligned}$$

somit ist

$$\begin{aligned}
\Phi_B\left(\bigwedge_{n\in\mathbb{N}} X_n\right) &= \left([\![b]\!] \wedge \mathsf{wlp}([\![P]\!])\left(\bigwedge_{n\in\mathbb{N}} X_n\right)\right) \vee ([\![\neg b]\!] \wedge B).\\
&= \left([\![b]\!] \wedge \bigwedge_{n\in\mathbb{N}} \mathsf{wlp}([\![P]\!])\,(X_n)\right) \vee ([\![\neg b]\!] \wedge B).\\
&= \bigwedge_{n\in\mathbb{N}} \Phi_B(X_n).
\end{aligned}$$

□

Wir können nun das zentrale Theorem dieses Kapitels beweisen. Es besagt, daß alle für den Termaufbau in pGCL erlaubten Konstruktionen sich natürlich mit wlp verhalten.

Dabei ist die predicate transformer-Semantik der `while`-Schleife durch einen größten Fixpunkt gegeben, so daß partielle Korrektheitsaussagen bewiesen werden können.

**Theorem 6.14.** *Der Operator* wlp *erfüllt die folgenden Gleichungen:*

$$\mathsf{wlp}([\![\texttt{abort}]\!]_H)(B) = \top = \lambda s.1 \tag{1}$$

$$\mathsf{wlp}([\![\texttt{skip}]\!]_H)(B) = B \tag{2}$$

$$\mathsf{wlp}([\![\texttt{assign}_f]\!]_H)(B) = B \circ f \tag{3}$$

$$\mathsf{wlp}([\![\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi}]\!]_H)(B) = ([\![b]\!] \wedge \mathsf{wlp}([\![P]\!]_H)(B)) \vee ([\![\neg b]\!] \wedge \mathsf{wlp}([\![Q]\!]_H)(B)) \tag{4}$$

$$\mathsf{wlp}([\![P\,;Q]\!]_H)(B) = \mathsf{wlp}([\![P]\!]_H)(\mathsf{wlp}([\![Q]\!]_H)(B)) \tag{5}$$

$$\mathsf{wlp}([\![P \mathrel{{}_p\!\oplus} Q]\!]_H)(B) = p\cdot\mathsf{wlp}([\![P]\!]_H)(B) + (1-p)\cdot\mathsf{wlp}([\![Q]\!]_H)(B) \tag{6}$$

$$\mathsf{wlp}([\![P \sqcap Q]\!]_H)(B) = \mathsf{wlp}([\![P]\!]_H)(B) \wedge \mathsf{wlp}([\![Q]\!]_H)(B) \tag{7}$$

$$\mathsf{wlp}([\![\texttt{while } b \texttt{ do } P \texttt{ od}]\!]_H)(B) = \nu\Phi_B \tag{8}$$

*Dabei ist* $\nu(f) = \bigsqcap_{n=0}^{\infty} f^n(\top)$.

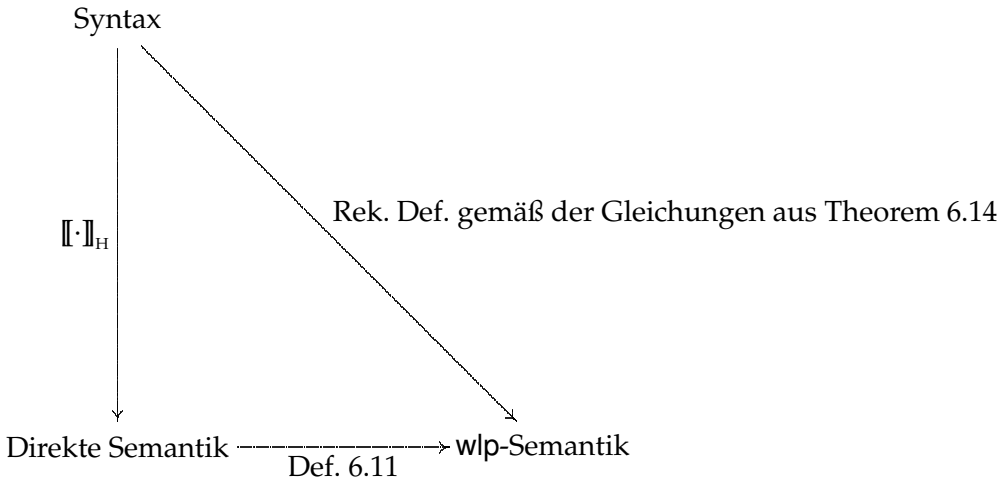


Abbildung 13: Interpretation von Theorem 6.14

**Bemerkung.** So wir wir Theorem 4.5 als rekursive Definition der wp-Semantik verstehen konnten, können wir Theorem 6.14 als rekursive Definition der wlp-Semantik verstehen, Diagramm 9 können wir zu Diagramm 13 modifizieren.

**Beweis.**
(1) Es gilt

$$\begin{aligned}\mathsf{wlp}([\![\texttt{abort}]\!]_{\mathrm{H}})(B)(s) &= \bigwedge_{\mu\in[\![\texttt{abort}]\!]_{\mathrm{H}}(s)} 1-\sum_{t\in S}(1-B(t))\cdot\mu(t)\\ &= \bigwedge_{\mu\in\{\bot\}} 1-\sum_{t\in S}(1-B(t))\cdot\mu(t)\\ &= 1-\sum_{s\in S}(1-B(s))\cdot 0 = 1,\end{aligned}$$

also ist tatsächlich $\mathsf{wlp}([\![\texttt{abort}]\!])(B) = \lambda s.1$.

(2) Wir haben

$$\begin{aligned}\mathsf{wlp}([\![\texttt{skip}]\!]_{\mathrm{H}})(B) &= \lambda s.\bigwedge_{\mu\in\downarrow\eta_s} 1-\sum_{t\in S}(1-B(t))\cdot\mu(t)\\ &= \lambda s.1-\sum_{t\in S}(1-B(t))\cdot\eta_s(t)\\ &= \lambda s.1-(1-B(s))\\ &= B.\end{aligned}$$

Da `skip` sicher terminiert ist es nicht überraschend, daß $\mathsf{wp}([\![\texttt{skip}]\!]) = \mathsf{wlp}([\![\texttt{skip}]\!]_{\mathrm{H}})$ gilt.

(3) Bei der Anwendung einer Scott-stetigen Funktion $f$ ist

$$\begin{aligned}
\mathsf{wlp}([\![\texttt{assign}_f]\!]_{\mathrm{H}})(B) &= \lambda s. \bigwedge_{\mu \in \downarrow\{\eta_{f(s)}\}} 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \\
&= \lambda s. \bigwedge_{\mu \in \{\eta_{f(s)}\}} 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \\
&= \lambda s. 1 - \sum_{t \in S} (1 - B(t)) \cdot \eta_{f(s)}(t) \\
&= \lambda s. 1 - (1 - B(f(s)) \\
&= B \circ f.
\end{aligned}$$

(4) Für die Untersuchung der `if`-Verzweigung erinnern wir an die direkte Semantik der Fallunterscheidung:

$$[\![\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi}]\!]_{\mathrm{H}} s = [\![b]\!] s \cdot [\![P]\!]_{\mathrm{H}} s + [\![\neg b]\!] s \cdot [\![Q]\!]_{\mathrm{H}} s.$$

Entsprechend ist

$$\begin{aligned}
\mathsf{wlp}([\![\texttt{if } b \texttt{ then } P \texttt{ else } Q \texttt{ fi}]\!]_{\mathrm{H}})(B) &= \lambda s. \bigwedge_{\mu \in [\![b]\!] s \cdot [\![P]\!]_{\mathrm{H}} s + [\![\neg b]\!] s \cdot [\![Q]\!]_{\mathrm{H}} s} 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \\
&= \lambda s. \quad [\![b]\!] s \cdot \bigwedge_{\mu \in [\![P]\!]_{\mathrm{H}} s} 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \\
&\qquad + [\![\neg b]\!] s \cdot \bigwedge_{\mu \in [\![Q]\!]_{\mathrm{H}} s} 1 - \sum_{t \in S} (1 - B(t)) \cdot \mu(t) \\
&= ([\![b]\!] \wedge \mathsf{wlp}([\![P]\!]_{\mathrm{H}})(B)) \vee ([\![\neg b]\!] \wedge \mathsf{wlp}([\![Q]\!]_{\mathrm{H}})(B)) \,.
\end{aligned}$$

(5) Zunächst erkennen wir, daß im vollständigen Verband $[0,1]$ für konvexe Teilmengen $A$ die Operationen $\bigvee, \bigwedge$ und $x \longmapsto 1 - x$ auf die folgende Weise miteinander vertauschen:

$$\begin{aligned}
1 - \bigvee_{a \in A} a &= \bigwedge_{a \in A} (1 - a) \\
1 - \bigwedge_{a \in A} a &= \bigvee_{a \in A} (1 - a)
\end{aligned}$$

Es ist

$$[\![P\,;Q]\!] s = \overline{\bigcup_{\substack{\mu \in [\![P]\!]_{\mathrm{H}} s \\ g \in \Pi([\![Q]\!]_{\mathrm{H}})}} \left\{ \lambda z. \int_S g(t)(z) \,\mathrm{d}\mu(t) \right\}} =: \overline{A}$$

Satz 5.5 erlaubt uns die Vereinfachung $\bigwedge f[\overline{A}] = \bigwedge f[A]$. Wir rechnen also nach:

$$\begin{aligned}
\mathsf{wlp}([\![P\,;Q]\!]_{\mathrm{H}})(B)(s) &= \bigwedge_{\mu\in\overline{A}} 1-\sum_{t'\in S}(1-B)(t)\cdot\mu(t') \\
&= \bigwedge_{\mu\in A} 1-\sum_{t'\in S}(1-B)(t)\cdot\mu(t') \\
&= \bigwedge_{\mu\in[\![P]\!](s)}\ \bigwedge_{g\in\Pi[\![Q]\!]} 1-\sum_{t'\in S}(1-B)(t)\cdot\sum_{t\in S}\mu(t)\cdot g(t)(t') \\
&= \bigwedge_{\mu\in[\![P]\!](s)}\ \bigwedge_{g\in\Pi[\![Q]\!]} 1-\sum_{t\in S}\sum_{t'\in S}(1-B)(t)\cdot\mu(t)\cdot g(t)(t') \\
&= \bigwedge_{\mu\in[\![P]\!](s)}\ \bigwedge_{g\in\Pi[\![Q]\!]} 1-\sum_{t\in S}\mu(t)\cdot\left(1-\left(1-\sum_{t'\in S}(1-B)(t)\cdot g(t)(t')\right)\right) \\
&= \bigwedge_{\mu\in[\![P]\!](s)} 1-\sum_{t\in S}\mu(t)\cdot\left(1-\bigwedge_{g\in\Pi[\![Q]\!]}\left(1-\sum_{t'\in S}(1-B)(t)\cdot g(t)(t')\right)\right) \\
&= \bigwedge_{\mu\in[\![P]\!](s)} 1-\sum_{t\in S}\mu(t)\cdot\left(1-\bigwedge_{\nu\in[\![Q]\!](t)}\left(1-\sum_{t'\in S}(1-B)(t)\cdot\nu(t')\right)\right) \\
&= \mathsf{wlp}([\![P]\!])\Big(\mathsf{wlp}([\![Q]\!])(B)\Big)(s).
\end{aligned}$$

Hierbei können wir in der vorletzten Gleichheit $\bigwedge_{g}$ durch $\bigwedge_{\nu}$ ersetzen, da

$$\Big\{g(s)\;\Big|\;g\in\Pi(f)\Big\} = f(s)$$

gilt.

Die Summen über $t$ bzw. $t'$ vertauschen, da absolute Konvergenz vorliegt.

(6) Bei probabilistischen Auswahlen ist

$$\begin{aligned}
\mathsf{wlp}([\![P\,{}_p\!\oplus Q]\!]_{\mathrm{H}})(B) &= \bigwedge_{\mu\in[\![P\,{}_p\!\oplus Q]\!]_{\mathrm{H}}} 1-\sum_{t\in S}(1-B(t))\cdot\mu(t) \\
&= \bigwedge_{\nu\in[\![P]\!]_{\mathrm{H}},\nu'\in[\![Q]\!]_{\mathrm{H}}} 1-\sum_{t\in S}(1-B(t))\cdot(p\cdot\nu+(1-p)\cdot\nu')(t) \\
&= p\cdot\mathsf{wlp}([\![P]\!]_{\mathrm{H}})(B)+(1-p)\cdot\mathsf{wlp}([\![Q]\!]_{\mathrm{H}})(B).
\end{aligned}$$

(7) Für die nondeterministische Wahl gilt

$$[\![P\sqcap Q]\!]_{\mathrm{H}}(s) = \overline{\bigcup_{0\le p\le 1}[\![P\,{}_p\!\oplus Q]\!]_{\mathrm{H}}(s)}.$$

Es folgt mit $\bigwedge f[\overline{A}] = \bigwedge f[A]$:

$$\begin{aligned}\mathsf{wlp}([\![P \sqcap Q]\!]_{\mathrm{H}})(B) &= \bigwedge_{p\in[0,1]} p \cdot \mathsf{wlp}([\![P]\!]_{\mathrm{H}})(B) + (1-p)\cdot \mathsf{wlp}([\![Q]\!]_{\mathrm{H}})(B)\\ &= \mathsf{wlp}([\![P]\!]_{\mathrm{H}})(B) \wedge \mathsf{wlp}([\![Q]\!]_{\mathrm{H}})(B),\end{aligned}$$

da in $[0,1]$ die kleinste Konvexkombination zweier Zahlen stets die kleinere Zahl ist.

(8) Wegen Lemma 6.13 genügt es zu zeigen, daß

$$\mathsf{wlp}(\Psi^n(\lambda s.\{\lambda s'.0\}))(B) = \Phi_B^n(\lambda s.1)$$

gilt.

Für den Induktionsanfang $n = 0$ haben wir

$$\begin{aligned}\mathsf{wlp}(\Psi^0(\lambda s.\{\lambda s'.0\}))(B) &= \mathsf{wlp}(\lambda s.\{\lambda s'.0\})(B)\\ &= \lambda s.1\\ &= \Phi_B^0(\lambda s.1).\end{aligned}$$

Induktionsschritt:

Wie im probabilistischen Falle gilt für alle $g$ und $B$

$$\mathsf{wlp}(\Psi(g))(B) = \Phi_B(\mathsf{wlp}(g)(B)) \qquad (\star)$$

Es ist nämlich

$$\begin{aligned}\mathsf{wlp}(\Psi(g))(B) &= \lambda s. \bigwedge_{\mu\in(b(s)\cdot g^{\dagger}(f(s))+(1-b(s))\cdot\downarrow\eta_s)} 1 - \sum_{t\in S}(1-B(t))\cdot\mu(t)\\ &= s \mapsto \begin{cases}\bigwedge\limits_{\mu\in g^{\dagger}(f(s))} 1-\sum_{t\in S}(1-B(t))\cdot\mu(t) & \text{für } b(s)=1\\ \bigwedge\limits_{\mu\in\downarrow\eta_s} 1-\sum_{t\in S}(1-B(t))\cdot\mu(t) & \text{sonst.}\end{cases}\\ &= s \mapsto \begin{cases}\mathsf{wlp}(f)(\mathsf{wlp}(g)(B))(s) & \text{für } b(s)=1\\ 1-\sum_{t\in\{s\}}(1-B(t)) & \text{sonst.}\end{cases}\\ &= s \mapsto \begin{cases}\mathsf{wlp}(f)(\mathsf{wlp}(g)(B))(s) & \text{für } b(s)=1\\ B(s) & \text{sonst.}\end{cases}\\ &= b\cdot\mathsf{wlp}(f)(\mathsf{wlp}(g)(B)) + ((1-b)\cdot B)\\ &= \Phi_B(\mathsf{wlp}(g)(B)),\end{aligned}$$

wobei wir die dritte Gleichheit gerade unter (5) nachgewiesen haben.

Gelte nun als Induktionshypothese die Aussage bereits für $n = i$. Dann haben wir

$$\begin{aligned}
\mathsf{wlp}(\Psi^{i+1}(\lambda s.\{\lambda s'.0\})(B) &= \mathsf{wlp}\Big(\Psi\Big(\Psi^i(\lambda s.\{\lambda s'.0\})\Big)\Big)(B) \\
&\overset{(\star)}{=} \Phi_B\Big(\mathsf{wlp}\Big(\Psi^i(\lambda s.\{\lambda s'.0\})\Big)(B)\Big) \\
&\overset{\text{(I.H.)}}{=} \Phi_B(\Phi_B^i(\lambda s.1)) \\
&= \Phi_B^{i+1}(\lambda s.1),
\end{aligned}$$

was den Beweis des Theorems abschließt. □

**Bemerkung.** Dieses Resultat erlaubt uns die Anwendung des üblichen Invariantenkalküls zum Nachweis der partiellen Korrektheit von Schleifen.

*But then again, all good things must come to an end . . .*

*(Q in Star Trek TNG)*

# 7 Zusammenfassung und Ausblick

Um Systemzustände zu modellieren und dabei sowohl probabilistischen als auch dämonischen Nichtdeterminismus zu fassen, wurde der Smyth- und der Hoare-Powerdomain über dem Raum der Subverteilung auf einem flachen Zustandsraum definiert.

Ich habe nun jeweils eine direkte Semantik im Smyth- und im Hoare-Powerdomain definiert, und auf der Basis dieser direkten denotationellen Semantiken die *predicate transformer*-Semantiken wp und wlp gerade so konstruiert, daß sie die Gleichungen der natürlichen Definition per Rekursion auf dem Termaufbau erfüllen.

Während die wp-Semantik `while`-Konstruktionen gerade einen kleinsten Fixpunkt zuordnet, werden diese in der wlp-Semantik als größte Fixpunkte interpretiert, was Invariantenkalkül im herkömmlichen Sinne erlaubt.

Nicht jede Teilmenge von $\mathcal{V}(S)$ ist auch Element von $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$. Im Allgemeinen können unschöne Effekte auftreten, wenn man aus beliebigen Teilmengen von $\mathcal{V}(S)$ Elemente von $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ erzeugen will. Überraschend und gleichzeitig sehr hilfreich war die Entdeckung der Tatsache, daß man einer Auseinandersetzung mit diesen Phänomenen weitestgehend aus dem Wege gehen kann, da für alle in der hier betrachteten Semantik auftretenden Mengen $M$ bereits die Saturierung $\uparrow M$ in $\mathfrak{P}_{\text{Sm}}\mathcal{V}(S)$ liegt.

Abschließend möchte ich noch auf einen möglichen weiteren Schritt in diesem Fachgebiet hinweisen.

Beschäftigt man sich eingehender mit der direkten Semantik, so erwartet man, daß $[\![\texttt{(P ; Q) ; R}]\!] = [\![\texttt{P ; (Q ; R)}]\!]$ gilt. Bisher wurden die entsprechenden Lifting- bzw. Monadeneigenschaften hierfür aber nicht nachgewiesen.

Für $\mathfrak{P}_{\text{Sm}}\mathcal{V}_\infty$ und $\mathfrak{P}_{\text{H}}\mathcal{V}_\infty$ sind diese bereits untersucht (vergleiche [TKP05]), dort kann man sich der Theorie der Kegel bedienen. Der richtige Raum für die Anwendung ist aber $\mathcal{V}(S)$, nicht $\mathcal{V}_\infty(S)$.

Um den Rahmen der Arbeit nicht zu sprengen, haben wir hier nur diejenigen Eigenschaften nachgerechnet, die für die *predicate transformer*-Semantik der Hintereinanderausführung unerlässlich waren. Es wäre sinnvoll, die Gedanken aus [TKP05] für $\mathfrak{P}_{\text{Sm}}\mathcal{V}$, bzw $\mathfrak{P}_{\text{H}}\mathcal{V}$ anstelle von $\mathfrak{P}_{\text{Sm}}\mathcal{V}_\infty$ und $\mathfrak{P}_{\text{H}}\mathcal{V}_\infty$ zu wiederholen, die richtigen Kategorien in diesem Kontext anzugeben und die universellen Eigenschaften entsprechend neu zu beweisen.

# Index

# Literatur

[AJ94] S. Abramsky and A. Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, pages 1–168. Clarendon Press, 1994.

[Dij75] Edsger W. Dijkstra. Guarded commands, nondeterminacy and formal derivation of programs. *Communications of the ACM*, 18:453–457, 1975.

[GHK+03] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. W. Mislove, and D. S. Scott. *Continuous Lattices and Domains*, volume 93 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2003.

[MM04] Annabelle McIver and Carroll Morgan. *Abstraction, Refinement and Proof for Probabilistic Systems.* Monographs in Computer Science. Springer-Verlag, 2004.

[Plo76] Gordon Plotkin. A powerdomain construction. *SIAM Journal of Computing*, September 1976.

[Plo79] Gordon Plotkin. Dijkstras predicate transformers & smyth's power domains. *Springer Lecture Notes In Computer Science*, 86:527–553, 1979.

[Smy78] Michael Smyth. Power domains. *Journal of Computer and System Sciences*, 1978.

[TKP05] Regina Tix, Klaus Keimel, and Gordon Plotkin. Semantic domains for combining probability and non-determinism. *Electronic Notes in Theoretical Computer Science*, 129:1–104, 2005.

[Win93] Glynn Winskel. *The Formal Semantics of Programming Languages: an introduction*. The MIT Press, Cambridge, Massachusetts, 1993.