5.4 Abstrakte Semantik

<u>Ziel</u>: Imitiere die konkrete Semantik auf einer abstrakten Datendomäne.

<u>Definition</u>: Sichere Approximation von Funktionen

Sei (α, γ) eine Galois-Verbindung mit $L \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} M$.
Sei ferner $f: L \to L$ eine Funktion.

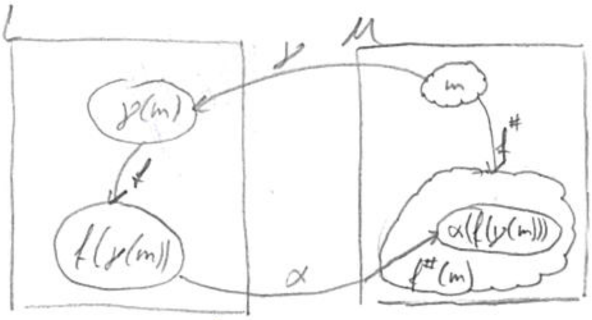
- Dann heißt $f^\#: M \to M$ <u>sichere Approximation</u> von f, falls gilt:

$$\alpha \circ f \circ \gamma \leq_M f^\#$$

also

$$\alpha(f(\gamma(m))) \leq_M f^\#(m)$$

für alle $m \in M$.



- Die Funktion $f^\#$ heißt <u>genaueste</u> sichere Approximation von f, falls gilt:

$$\alpha \circ f \circ \gamma = f^\#$$

- Oft sind $f, f^\#$ monoton.

<u>Lemma</u>:
Sind f und $f^\#$ monoton, gilt:

$$\alpha \circ f \circ \gamma \leq_M f^\# \quad \underline{\text{gdw.}} \quad \alpha \circ f \leq_M f^\# \circ \alpha$$

Beispiel 1

- Betrachte die Vorzeichenabstraktion, $\mathcal{P}(\mathbb{Z}) \underset{\gamma_{sign}}{\overset{\alpha_{sign}}{\rightleftarrows}} \mathcal{P}(\{-,0,+\})$.
- Sei $f_{-2} : \mathcal{P}(\mathbb{Z}) \longrightarrow \mathcal{P}(\mathbb{Z})$, $f_{-2}(Z) = \{z-2 \mid z \in Z\}$, die Subtraktion von 2 auf dem Potenzmengenverband $\mathcal{P}(\mathbb{Z})$.
- Definiere eine sichere Approximation von f_{-2} durch:

$$f_{-2}^{\#} : \mathcal{P}(\{-,0,+\}) \longrightarrow \mathcal{P}(\{-,0,+\})$$

$$f_{-2}^{\#}(A) := \begin{cases} \emptyset & \text{falls } A = \emptyset \\ \{-,0,+\}, & \text{falls } + \in A \\ \{-\} & \text{, sonst} \end{cases}$$

- Es ist zu zeigen, dass für alle $A \subseteq \{-,0,+\}$ gilt:

$$\alpha(f_{-2}(\gamma(A))) \subseteq f_{-2}^{\#}(A)$$

- Am Beispiel:

$$\begin{aligned} \alpha(f_{-2}(\gamma(\{0,+\}))) &= \alpha(f_{-2}(\{0,1,2,3,\dots\})) \\ &= \alpha(\{-2,-1,0,1,2,\dots\}) \\ &= \{-,0,+\} = f_{-2}^{\#}(\{0,+\}) \end{aligned}$$

- Definiere nun die operationelle Semantik von While-Programmen auf einer abstrakten Datendomäne
- Beachte, dass die Transitionsrelation nicht-deterministisch wird:

$$(\text{if } (x=0) \text{ then } c_1 \text{ else } c_2 \text{ end}, \{(x=\text{even})\})$$

Die Bedingung kann sowohl wahr als auch falsch sein.

- Betrachte eine Galois-Verbindung $\mathbb{P}(State) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} M$.
  Dabei ist $\mathbb{P}(State)$ der vollständige Verband der Mengen von Variablenbelegungen und M ein vollständiger Verband abstrakter Werte
- Die abstrakte Semantik sollte eine sichere Approximation der konkreten sein.
- Dazu müssen wir die konkrete Semantik als Funktion auf $\mathbb{P}(State)$ auffassen (State Transformer), wie folgt:

$$post_{c,c'},\ post_c : \mathbb{P}(State) \to \mathbb{P}(State)$$

für alle $c, c' \in Prog$, mit:

$$post_{c,c'}(S) := \{\sigma' \in State \mid \exists \sigma \in S.\ (c,\sigma) \to (c',\sigma')\}$$
$$post_c(S) := \{\sigma' \in State \mid \exists \sigma \in S.\ (c,\sigma) \to \sigma'\}$$

Definition: Abstrakte Semantik

Betrachte die Galois-Verbindung $\mathbb{P}(State) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} M$.

- Eine <u>abstrakte Semantik</u> ist gegeben durch eine Familie von Funktionen

$$post^{\#}_{c,c'},\ post^{\#}_c : M \to M$$

mit

$$\alpha \circ post_{c,c'} \circ \gamma \leq_M post^{\#}_{c,c'}$$
$$\alpha \circ post_c \circ \gamma \leq_M post^{\#}_c$$

- Sind alle $post^{\#}_{c,c'}, post^{\#}_c$ genaueste sichere Approximationen der $post_{c,c'}, post_c$, spricht man von der <u>genauesten</u> abstrakten Semantik.
- Die abstrakte Semantik induziert die <u>abstrakte Transitionsrelation</u>

$$\Rightarrow\ \subseteq (Prog \times M) \times ((Prog \times M) \cup M)$$

zwischen <u>abstrakten Konfigurationen</u> $(c,m) \in Prog \times M$ mittels:

$$(c,m) \Rightarrow (c', post^{\#}_{c,c'}(m)) \quad \text{und} \quad (c,m) \Rightarrow post^{\#}_c(m)$$

Beispiel: (Genaueste abstrakte Semantik)

- Betrachte $\mathbb{P}(\mathbb{Z}^{\{n\}}) \underset{\gamma_{parity}}{\overset{\alpha_{parity}}{\rightleftarrows}} \mathbb{P}(\{odd, even\}^{\{n\}})$, die ~~Gerade~~/Ungerade-Abstraktion für eine Variable, n:

•

$$(n = 3n+1, \{odd\}) \Rightarrow \{even\}$$
$$(n = 3n+1, \{even\}) \Rightarrow \{odd\}$$
$$(n = 3n+1, \{odd, even\}) \Rightarrow \{odd, even\}$$
$$(\text{while } n \neq 1 \text{ do } c \text{ end}, \{odd\}) \Rightarrow \{odd\}$$
$$(\text{while } n \neq 1 \text{ do } c \text{ end}, \{odd\}) \Rightarrow (c; \text{while } n \neq 1 \text{ do } c \text{ end}, \{odd\})$$
$$(\text{while } n \neq 1 \text{ do } c \text{ end}, \{even\}) \not\Rightarrow \{even\}$$
$$(\text{while } n \neq 1 \text{ do } c \text{ end}, \{even\}) \Rightarrow (c; \text{while } n \neq 1 \text{ do } c \text{ end}, \{even\})$$
$$\text{while } (n \neq 1 \text{ do } c \text{ end}, \{odd, even\}) \Rightarrow \{odd\}$$
$$\text{while } (n \neq 1 \text{ do } c \text{ end}, \{odd, even\}) \Rightarrow (c; \text{while } n \neq 1 \text{ do } c \text{ end}, \{odd, even\})$$

⋮

Lemma:

Die genaueste abstrakte Semantik ist im Allgemeinen nicht berechenbar.

Begründung:

- Betrachte die Galois-Verbindung $\mathbb{P}(State) \underset{\gamma_{sign}}{\overset{\alpha_{sign}}{\rightleftarrows}} \mathbb{P}(\{-, 0, +\})$.
- Sei die abstrakte Konfiguration:

$$\text{if } n > 2 \wedge x^n + y^n = z^n \text{ then } n = 1 \text{ else } n = -1 \text{ end}, \{(n=+, x=+, y=+, z=+)\}$$

- Um zu entscheiden, ob n auf - oder + gesetzt werden soll, muss man entscheiden, ob es Belegungen von x, y, z, n mit $\mathbb{N} \setminus \{0\}$ gibt, die die Bedingung erfüllt.
- "Letzter Satz" von Fermat besagt: nein. (Bewiesen 1994)
- Allgemein: (Hilberts 10. Problem 1900)
  Es ist unentscheidbar, ob eine Diophantische Gleichung
  $$p(x_1, \dots, x_n) = 0$$
  mit Polynom p und Koeffizienten in $\mathbb{Z}$ eine Lösung in $\mathbb{Z}$ hat.
  (Bewiesen 1970, Matiyasevich)

5.5 Herleitung einer abstrakten Semantik

Ziel: Berechne die abstrakte Semantik für Galois-Verbindungen $(\alpha_\beta, \gamma_\beta)$, die durch Liften einer Extraktionsfunktion $\beta : \mathbb{Z} \to D$ auf State entstanden sind.

Also: $$\mathbb{P}(State) = \mathbb{P}(\mathbb{Z}^{Vars}) \underset{\gamma_\beta}{\overset{\alpha_\beta}{\rightleftarrows}} \mathbb{P}(D^{Vars})$$

Problem:
- Werte Boolsche Ausdrücke auf der abstrakten Domain $\mathbb{P}(D)$ aus. — schon auf D problematisch
- Benötigt sichere Approximation von Prädikaten.

Lösung: Werte die Approximation in 3-wertiger Logik aus — à la Kleene

$(\mathbb{P}(\mathbb{B}) \setminus \{\emptyset\}, \wedge_3, \vee_3, \neg_3)$ mit

$\wedge_3$	$\{0\}$: 0	$\{1\}$: 1	$\{0,1\}$: $\frac{1}{2}$
0	0	0	0
1	0	1	$\frac{1}{2}$
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$

$\vee_3$	0	1	$\frac{1}{2}$
0	0	1	$\frac{1}{2}$
1	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$

$\neg_3$	
0	1
1	0
$\frac{1}{2}$	$\frac{1}{2}$

Definition!

Sei $p: \mathbb{Z}^n \to \mathbb{B}$ ein n-stelliges Prädikat, das auch auf Mengen verstanden werden kann:

$$p: \mathbb{P}(\mathbb{Z})^n \longrightarrow \mathbb{P}(\mathbb{B})$$

$$\underset{Z_i \in \mathbb{P}(\mathbb{Z})}{p((Z_1, \dots Z_n))} = \{ \underbrace{p(z_1, \dots, z_n)}_{\text{"Orginal } p\text{"}} \mid z_i \in Z_i \}$$

Dann heißt $p^\#: \mathbb{P}(D)^n \to \mathbb{P}(\mathbb{B})$ sichere Approximation von p, falls

$$p \circ \gamma_\beta^n \subseteq p^\#$$

↳ Komponentenweise Konkretisierung mit $\mathbb{P}(\mathbb{Z}) \underset{\gamma_\beta}{\overset{\alpha_\beta}{\rightleftarrows}} \mathbb{P}(D)$

Definition!

Sei $\mathcal{S} = (\mathbb{Z}, I)$ und $(\alpha_\beta, \gamma_\beta)$ die Galois-Verbindung $\mathbb{P}(\mathbb{Z}) \underset{\gamma_\beta}{\overset{\alpha_\beta}{\rightleftarrows}} \mathbb{P}(D)$, für Extraktionsfunktion $\beta: \mathbb{Z} \to D$.

Dann heißt $\mathcal{S}_{Abs} = (\mathbb{P}(D), I^\#)$ <u>abstrakte Sig-Struktur</u>, falls

$f_{I^\#}^\#: \mathbb{P}(D)^n \to \mathbb{P}(D)$ ist sichere Approximation von $f_I: \mathbb{Z}^n \to \mathbb{Z}$

$p_{I^\#}^\#: \mathbb{P}(D)^n \to \mathbb{P}(\mathbb{B})$ ist sichere Approximation von $p_I: \mathbb{Z}^n \to \mathbb{B}$

Die Semantik Boolscher Ausdrücke ist dabei: $(\sigma: Vars \to \mathbb{P}(D))$

$\cancel{f_I^\#(D_1, \dots, D_n)}$

$$\mathcal{S}_{Abs}[\![p(a_1, \dots, a_n)]\!](\sigma) := p_I^\#(\mathcal{S}_{Abs}[\![a_1]\!](\sigma), \dots, \mathcal{S}_{Abs}[\![a_n]\!](\sigma))$$

$$\mathcal{S}_{Abs}[\![b_1 \land b_2]\!](\sigma) := \mathcal{S}_{Abs}[\![b_1]\!] \land_3 \mathcal{S}_{Abs}[\![b_2]\!](\sigma)$$

$$\text{—— } \lor \text{ ——} \qquad \text{——} \lor_3 \text{——}$$

$$\text{—— } \neg \text{ —} \qquad \neg_3 \text{ ——}$$

Lemma:

Es gilt:

$$\beta(\mathcal{S}[\![a]\!](\sigma)) \in \mathcal{S}_{Abs} [\![a]\!] (\sigma')$$

$$\mathcal{S}[\![b]\!](\sigma) \in \mathcal{S}_{Abs} [\![b]\!] (\sigma')$$

mit

$$\sigma'(x) := \{ \beta(\sigma(x)) \}$$

Mögliche Definition für $f_I^{\#}$ und $p_I^{\#}$

$$f_I^{\#}(D_1, \dots, D_n) := \beta(f(\beta^{-1}(D_1), \dots, \beta^{-1}(D_n)))$$

$$p_I^{\#}(D_1, \dots, D_n) := \underbrace{p(\beta^{-1}(D_1), \dots, \beta^{-1}(D_n))}$$

0, falls $p(z_1, \dots, z_n) = 0$ für alle $z_i \in \beta^{-1}(D_i)$

1, falls $p(z_1, \dots, z_n) = 1$ für alle $z_i \in \beta^{-1}(D_i)$

½, sonst

Ist ein abstrakte Sig-Struktur gegeben, erhält man die <u>abstrakte Transitionsrelation</u>

$$\Rightarrow \; \in \left(Prog \times \mathcal{P}(D^{Vars})\right) \times \left(\left(Prog \times \mathcal{P}(D^{Vars})\right) \cup \mathcal{P}(D^{Vars})\right)$$

mit folgender Definition:

$$\frac{}{(x := a, Abs) \Rightarrow \{\sigma[x \mapsto d] \mid \sigma \in Abs,\ d \in \mathcal{S}_{Abs}[\![a]\!](\sigma')\}}$$

$$\sigma'(x) = \{\sigma(x)\}$$

$$\frac{}{(skip, Abs) \Rightarrow Abs}$$

$$\frac{(c_1, Abs) \Rightarrow Abs'}{(c_1; c_2, Abs) \Rightarrow (c_2, Abs')} \qquad \frac{(c_1, Abs) \Rightarrow (c_1', Abs')}{(c_1; c_2, Abs) \Rightarrow (c_1'; c_2, Abs')}$$

$$\frac{}{(\text{if } b \text{ then } c_1 \text{ else } c_2 \text{ end}, Abs) \Rightarrow (c_1, Abs \setminus \{\sigma \mid \mathcal{S}_{Abs}[\![b]\!](\sigma') = \{0\}\})}$$

$$\frac{}{(\text{if } b \text{ then } c_1 \text{ else } c_2 \text{ end}, Abs) \Rightarrow (c_2, Abs \setminus \{\sigma \mid \mathcal{S}_{Abs}[\![b]\!](\sigma') = \{1\}\})}$$

$$\frac{}{(\text{while } b \text{ do } c \text{ end}, Abs) \Rightarrow Abs \setminus \{\sigma \mid \mathcal{S}_{Abs}[\![b]\!](\sigma') = \{1\}\}}$$

$$\frac{}{(\text{while } b \text{ do } c \text{ end}, Abs) \Rightarrow (c; \text{while } b \text{ do } c \text{ end}, Abs \setminus \{\sigma \mid \mathcal{S}_{Abs}[\![b]\!](\sigma') = \{0\}\})}$$

Beachte:
- Bei bedingten Anweisungen werden die abstrakten Zustände σ entfernt, die auf jeden Fall die andere Verzweigung ~~gewählt~~ ausgeführt hätten.
- ~~Das~~ $\mathcal{S}_{Abs}[\![-]\!]$ erwartet Objekte vom Typ $\mathcal{P}(D)^{Vars}$, $\sigma \in Abs$ ist aber vom Typ ~~P~~ D^{Vars}. Deshalb verwenden wir σ'.

Definition:

$$\mathrm{post}^{\#}_{c,c'}(Abs) := \begin{cases} Abs', & \text{falls } (c, Abs) \Rightarrow (c', Abs') \\ \emptyset, & \text{sonst} \end{cases}$$

$$\mathrm{post}^{\#}_{c}(Abs) := \begin{cases} Abs', & \text{falls } (c, Abs) \Rightarrow Abs' \\ \emptyset & \end{cases}$$

Satz:

Die Familie der Funktionen $\mathrm{post}^{\#}_{c,c'}, \mathrm{post}^{\#}_{c}$ ist eine Abstrakte Semantik, also:

$$\alpha \circ \mathrm{post}_{c,c'} \circ \gamma \leq \mathrm{post}^{\#}_{c,c'}$$

$$\alpha \circ \mathrm{post}_{c} \circ \gamma \leq \mathrm{post}^{\#}_{c}$$