Abstrakte Temporale Eigenschaften

H. Peter Gumm

Philipps-Universität Marburg

Sommersemester 2007

Sicherheit und Lebendigkeit

- Sicherheitseigenschaften
  - Systeme nie gleichzeitig in kritischem Bereich
  - Nie beide Ampeln gleichzeitig grün
  - Variable x wird nicht gelesen bevor sie initialisiert wurde
- Lebendigkeitseigenschaften
  - Prozess i kann den kritischen Bereich erreichen
  - Ein Auto an der Ampel bekommt irgendwann grün
  - Variable x wird irgendwann initialisiert
- Safety ohne Liveness nutzlos
  - Ampeln immer rot
  - Kein System kommt in kritischen Bereich
  - Variable x wird nie gelesen
- Praktische Spezifikationen benötigen Sicherheit und Lebendigkei

Safety - Liveness

- Kann man Sicherheit und Lebendigkeit formal definieren ?
- Intuitive Definition (Leslie Lamport)
  - Safety: *Nothing bad will ever happen*
  - Liveness: *Something good will eventually happen*
- Gute umgangssprachliche Definition, aber
  - nicht formal genug
  - damit kann man keine Eigenschaften beweisen
- Mathematische Definition von Alpern & Schneider

Zustände, Folgen Eigenschaften

- S : Menge von Zuständen
  - S^* : Endliche Folgen
  - S^ω : unendliche Folgen
- Def.: Temporale Eigenschaft
  - Eine temporale Eigenschaft ist eine Teilmenge von S^ω
- Beispiele temporaler Eigenschaften für $S = \{ (c_1,c_2) \mid c_\iota \in \{rot,gelb,grün\}\}$
  - NoCrash = $\{ \sigma \in S^\omega \mid \sigma \models G\neg(c_1=c_2=grün) \} \subseteq S^\omega$
  - TooSafe = $\{ \sigma \in S^\omega \mid \sigma \models G\neg(c_1=grün) \wedge G\, \neg(c_2=grün) \} \subseteq S^\omega$
  - MalGrün = $\{ \sigma \in S^\omega \mid \sigma \models F(c_1=grün) \wedge F\,(c_2=grün) \} \subseteq S^\omega$
  - OftGrün = $\{ \sigma \in S^\omega \mid \sigma \models GF(c_1=grün) \wedge GF\,(c_2=grün) \} \subseteq S^\omega$
  - Riskant = MalGrün $\cap$ (S^ω - NoCrash)$\in$
  - LaissezFaire = S
  - NixDa = $\emptyset$
- Welche davon sind
  - Sicherheit
  - Lebendigkeit,
  - beides
  - weder noch
- Problem: Was ist „nothing bad“, „something good“

Beobachtbare und Sicherheitseigenschaften

- Beobachtbar:
  - Etwas, was nach endlicher Zeit konstatiert werden kann
  - Hintergrund:
    - Ein Unglück, das nicht nach endlicher Zeit eintritt, kann uns nicht beunruhigen
  - Idee zur Formalisierung:
    - (Un)glück ist endliche Folge $\alpha \in S^*$
    - auf Pfad σ passiert (Un)glück : $\alpha \prec \sigma$
    - Pfad σ ist sicher vor (Un)glück : $\neg(\alpha \prec \sigma)$
  - Menge von (Un)glücken $U \subseteq S^*$
    - $U \cdot S^\omega = \{ \alpha \cdot \sigma \mid \alpha \in P, \sigma \in S^\omega \} = \{ \pi \in S^\omega \mid \forall \alpha \in U . \alpha \pm \pi \})$
  - Definition: Eine Eigenschaft $P \subseteq S^\omega$ heißt beobachtbar, falls es eine Menge $U \subseteq S^*$ gibt, so daß $P = U \cdot S^\omega$.
  - Definition: Eine Eigenschaft Q heißt Sicherheitseigenschaft (safety property), falls S^ω-Q beobachtbar ist.
    - Fehlschlagen einer Sicherheitseigenschaft ist beobachtbar
  - Beispiel: NoCrash = $\{ \sigma \in S^\omega \mid \sigma \models G\neg(c_1=c_2=\text{grün}) \}$ ist safety
    - NoCrash = $S^\omega - U \cdot S^\omega$, wobei $U = \{ \alpha \in S^* \mid \exists i \in \mathbb{N} . \alpha(i)=(\text{grün},\text{grün}) \}$

Das System der beobachtbaren Mengen

1. $\emptyset$ und S^ω sind beobachtbar

   Beweis: $\emptyset \subseteq S^*$ und $\emptyset = \emptyset \cdot S^\omega$. Weiter: $S^* \subseteq S^*$ und $S^\omega = S^* \cdot S^\omega$

2. Sind P_i beobachtbar für alle $i \in I$, dann ist $\cup_{i \in I} P_i$ beobachtbar

   Beweis: $P_i = U_i \cdot S^\omega$ mit $U_i \subseteq S^*$ für jedes $i \in I$. Es folgt $\cup_{i \in I} U_i \subseteq S^*$ und $\cup_{i \in I} P_i = \cup_{i \in I} U_i \cdot S^\omega$.

3. Sind P_1 und P_2 beobachtbar, dann ist $P_1 \cap P_2$ beobachtbar

   Beweis: $P_1 = U_1 \cdot S^\omega$ und $P_2 = U_2 \cdot S^\omega$ mit $U_1, U_2 \subseteq S^*$. Definiere $U_1 \ominus U_2 := \{ \beta \in U_2 \mid \exists \alpha \in U_1 . \alpha \preceq \beta \}$ (erst passiert ein Unglück aus U_1 danach ein Unglück aus U_2). Dann gilt $P_1 \cap P_2 = ((U_1 \ominus U_2) \cup (U_2 \ominus U_1)) \cdot S^\omega$.

- Allgemeine mathematische Definition : Ein System τ von Teilmengen einer Menge X heißt Topologie, falls:
  - $\emptyset \in \tau, X \in \tau$
  - $P_1, P_2 \in \tau \Rightarrow P_1 \cap P_2 \in \tau$
  - $\forall i \in I. P_i \in \tau \Rightarrow \cup_{i \in I} P_i \in \tau$
- Die Mengen in τ heißen : Offene Mengen. Komplemente: Abgeschlossene Mengen
- In unserem Falle: $X = S^\omega$ und offen = beobachtbar, abgeschlossen = safety.

Sicherheitshülle – abgeschlossene Hülle

- Beobachtbare Mengen sind abgeschlossen gegen
  - endliche Schnitte
  - beliebige Vereinigungen
- Sicherheitseigenschaften sind abgeschlossen gegen
  - beliebige Schnitte
  - endliche Vereinigungen.
- Sei P irgendeine Eigenschaft. Definiere den Abschluß (closure) von P als
- $Cl(P) = \cap \{ Q \subseteq S^\omega \mid P \subseteq Q \text{ und } Q \text{ safety} \}.$
- Dann gilt:
  - Cl(P) ist die kleinste Safety-Eigenschaft, welche P umfasst.
  - Cl(P) heißt auch die abgeschlossene Hülle, oder kurz „der Abschluss" von P
- Cl ist ein „Abschlussoperator", d.h. für alle $P,Q \subseteq S^\omega$ gilt
  - $P \subseteq Cl(P)$ (extensiv)
  - $P \subseteq Q \Rightarrow Cl(P) \subseteq Cl(Q)$ (monoton)
  - $Cl(Cl(P)) = Cl(P)$ (idempotent)
- P safety $\Leftrightarrow Cl(P) = P$

Lebendigkeit - Liveness

- Lebendigkeitseigenschaften (liveness properties)
  - sagen etwas über die Zukunft voraus
  - sind unabhängig von bisher gewesenem
  - egal was bis zu einem Zeitpunkt gewesen ist, kann danach die Lebendigkeitseigenschaft noch erfüllt werden

- Definition: $P \subseteq S^\omega$ heißt liveness, falls $\forall \alpha \in S^*. \exists \sigma \in P. \alpha \prec \sigma$.

Aus der Definition folgen sofort:

- Lemma: $P=S^\omega$ ist die einzige Eigenschaft, die sowohl safety als auch liveness ist
- Lemma: Ist P liveness und $P \subseteq Q \subseteq S^\omega$, dann ist auch Q liveness.

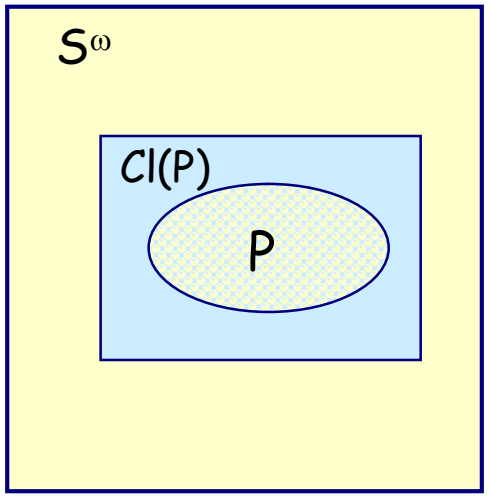
- Beispiel einer Lebendigkeitseigenschaft:
  - $OftGrün = \{ \sigma \in S^\omega \mid \sigma \models GF(c_1=grün) \wedge GF(c_2=grün) \} \subseteq S^\omega$

- Satz: P ist liveness, gdw. $Cl(P) = S^\omega$

  - Beweis: Sei P liveness. Wegen $P \subseteq Cl(P)$ ist Cl(P) sowohl safety als auch liveness, daher gilt $Cl(P) = S^\omega$.

  - Umgekehrt, sei $Cl(P) = S^\omega$. Wir müssen zeigen, dass P liveness ist.
  - Angenommen, es gäbe ein α aus S^* so daß für kein $\sigma \in \Sigma^\omega$ auch $\alpha \cdot \sigma \in P$ gilt.
  - Dann wäre die beobachtbare Menge $O = \{\alpha\} \cdot S^\omega$ disjunkt zu P, also $O \cap P = \emptyset$. Somit gilt $P \subseteq (S^\omega - O) \subset S^\omega$.
  - Da $(S^\omega - O)$ eine P enthaltene Sicherheitseigenschaft ist, folgt $P \subseteq Cl(P) \subseteq S^\omega - O$. Aus der Voraussetzung $Cl(P)=S^\omega$ folgt $O=\emptyset$.
  - Dieser Widerspruch widerlegt unsere Annahme.

Alpern-Schneider



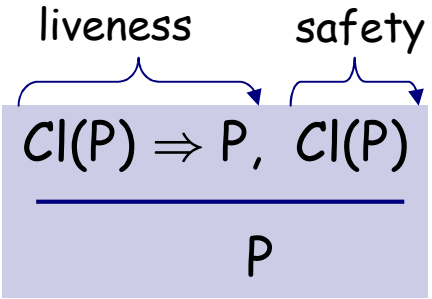
- Satz: Jede temporale Eigenschaft ist Konjunktion einer Sicherheitseigenschaft und einer Livenesseigenschaft

  Beweis:
  - $L := (S^\omega - C(P)) \cup P$ ist eine Lebendigkeitseigenschaft, denn
    - $L \supseteq S^\omega - Cl(P)$, also $C(L) \supseteq (S^\omega - C(P))$
    - $L \supseteq P$, also $C(L) \supseteq CL(P)$
    - folglich $C(L) \supseteq (S^\omega - C(P)) \cup Cl(P) = S^\omega$
  - $Cl(P)$ ist Sicherheitseigenschaft
  - $L \cap Cl(P) = ((S^\omega - Cl(P)) \cup P) \cap Cl(P) = \emptyset \cup P = P$

Spezialfall eines Satzes der Topologie:

- „Jede Teilmenge von X ist Durchschnitt einer abgeschlossenen und einer dichten Menge"

- Verwandschaft mit Modus-Ponens: ($\cup \approx \vee$, $\cap \approx \wedge$, $- \approx \neg$)
  - $(S^\omega - Cl(P)) \cup P \approx \neg Cl(P) \vee P \approx Cl(P) \Rightarrow P$



- Der Verdienst von Alpern & Schneider besteht darin, die richtige Modellierung, und die richtigen mathematischen Definitionen entdeckt zu haben.

Zerlegung

- Alpern-Schneider: Jede Eigenschaft P besteht aus einer Safety-Eigenschaft P_{safe} und einer Liveness-Komponente P_{live}.
- Diese Komponenten sind disjunkt, ausser für $P = S^{\omega}$.
  - Beispiel: Der Getränke-Automat gibt erst nur Fanta oder Cola aus, ab irgendeinem Zeitpunkt aber nur Bier.
    - $S = \{ \text{Bier}, \text{Cola}, \text{Fanta} \}$
  - Liveness: Versprechen, die nur im unendlichen eingelöst werden können
    - $P_{live} = S^* \cdot \{\text{Bier}\}^{\omega} = \{ \sigma \in S^{\omega} \mid \sigma \models FG\ \text{Bier} \}$
    - Liveness, weil jede endliche Folge zu einer Folge vervollständigt werden kann, die FG Bier erfüllt
  - Safety:
    - Verletzung in endlicher Zeit sichtbar
    - Verbotene Präfixe: $V = \{ \alpha \cdot \text{Bier} \cdot s \mid \alpha \in S^*, s \neq \text{Bier} \}$
    - $P_{safe} = S^{\omega} - V \cdot S^{\omega} = \{\text{Bier}\}^3 \cdot S^{\omega}$ (sowohl safety, als auch beobachtbar)
- Wie kann man allgemein die Zerlegung berechnen ?
  - $P_{safe} = Cl(P)$, $P_{live} = S^{\omega} - Cl(P) \cup P$
- Genügt zu wissen: Wie kann man Cl(P) bestimmen ?

Cl(P) durch verbotene Präfixe

- Leider ist die Definition

  $Cl(P) := \cap\{ Q \subseteq S^\omega \mid P \subseteq Q \text{ und } Q \text{ safety}\}$

  praktisch nicht handhabbar.

- Eine Methode: Verbotene Präfixe bestimmen
  - Andere Methode: Konvergenzabschluss – siehe folgende Folien.

- Für $P \subseteq S^\omega$ sei $V(P) = \{ \alpha \in S^* \mid \forall \sigma \in P. \neg(\alpha \prec \sigma) \}$

- Satz: $Cl(P) = S^\omega - V(P) \cdot S^\omega$.

  - Beweis: Offensichtlich ist $S^\omega - V(P) \cdot S^\omega$ abgeschlossen und umfasst P.
    Wir müssen zeigen, dass es die kleinste abgeschlossene Menge ist, die P umfasst.

  - Angenommen es gäbe eine weitere abgeschlossene Menge Q mit $P \subseteq Q \subseteq S^\omega - V(P) \cdot S^\omega$.
  - Dann ist Q von der Form $S^\omega - U \cdot S^\omega$, und es folgt $S^\omega - P \supseteq U \cdot S^\omega \supseteq V(P) \cdot S^\omega$

  - Sei $\alpha \in U$. Wegen $S^\omega - P \supseteq U \cdot S^\omega$ folgt für jedes $\tau \in S^\omega$, dass $\alpha \cdot \tau \in S^\omega - P$, daher gilt nach Definition $\alpha \in V(P)$. Somit ist auch $U \subseteq V(P)$, mithin $U \cdot S^\omega = V(P) \cdot S^\omega$, also $Q = S^\omega - V(P) \cdot S^\omega$.

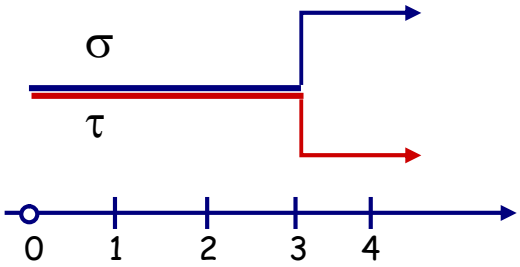
Beispiel: Alkoholentzug

- Der Getränke-Automat gibt erst nur Fanta oder Cola aus, ab irgendeinem Zeitpunkt aber nur Bier.
- $P = \{ \sigma \in S^{\omega} \mid \sigma \models [\neg \text{Bier } U \text{ } G \text{ Bier}] \}$
- Verbotene Präfixe:
  - $V(P) = \{ \alpha \in S^{*} \mid \exists\, i \in \mathbb{N}.\ \alpha(i) = \text{Bier}, \alpha(i+1) \neq \text{Bier} \}$
- $Cl(P) = S^{\omega} - V(P) \cdot S^{\omega} = \{ \sigma \in S^{\omega} \mid \sigma \models [\neg \text{Bier } W \text{ } G \text{ Bier}] \}$
- P_{safe} ist in diesem Beispiel also $P \cup (\text{Cola} \mid \text{Fanta})^{\omega}$
- Jede Bier-freie Folge ist in der Tat ein Grenzwert von Folgen in P
  - Das Bier gibt es später und später und später
  - Im Grenzwert nie.
- Was bedeutet genau: Im Grenzwert ?

Der ultrametrische Raum S^ω

- Auf S^ω lässt sich ein Abstand definieren:

$$d(\sigma,\tau) = \begin{cases} 0 & \text{falls } \sigma = \tau \\ \frac{1}{2^n} & \text{falls } n = min\{k \mid \sigma(k) \neq \tau(k)\} \end{cases}$$



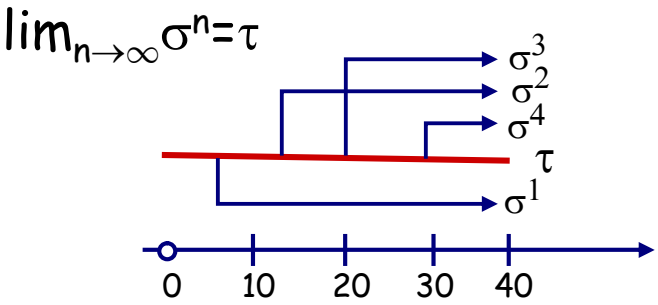
$d(\sigma,\tau)=\frac{1}{4}$

- damit erfüllt d: $S^\omega \times S^\omega \to \mathbb{R}^+$ die Gesetze:
  - d(x,y) = 0 $\Leftrightarrow$ x = y
  - d(x,y) = d(y,x)
  - d(x,z) $\leq$ d(x,y) + d(y,z)

  d.h. (S^ω,d) ist ein metrischer Raum

- Mehr noch, (S^ω,d) ist sogar ultrametrischer Raum, denn es gilt:
  - d(x,z) = max(d(x,y),d(y,z))

Konvergenz



- Eine Folge von Pfaden $(\sigma^n)_{n\in\mathbb{N}}$ konvergiert gegen τ gdw.

  $$\forall\varepsilon>0.\exists m\in\mathbb{N}.\forall k\geq m.\ d(\sigma^k,\tau) < \varepsilon.$$

  Schreibweise: $\lim_{n\to\infty}\sigma^n = \tau$.

- Äquivalent: Mit wachsendem m stimmen die σ^k auf immer längeren Präfixen mit τ überein.
  - $\forall r\in\mathbb{N}.\exists m\in\mathbb{N}.\forall k\geq m.\ \sigma^k_{<r}=\tau_{<r}$

- <u>Satz</u>: $P\subseteq S^\omega$ abgeschlossen $\Leftrightarrow$ für jede konvergente Folge $\lim_{n\to\infty}\sigma^n = \tau$ gilt:
  $$(\forall\, n\in\mathbb{N}.\ \sigma^n \in P) \Rightarrow \tau\in P$$

- <u>Beweis</u>: „$\Rightarrow$" Sei P abgeschlossen, dann gilt $P=S^\omega\text{-}V(P)\cdot S^\omega$ für $V(P) = \{\ \alpha \in S^* \mid \forall\sigma \in P.\neg(\alpha \prec \sigma)\ \}$.

  Angenommen $\lim_{n\in\mathbb{N}}\sigma^n=\tau$ aber $\tau\notin P$. Dann gilt $\tau = \alpha\cdot\sigma$ für ein $\alpha\in V(P)$. Sei r die Länge von α. Wegen $\lim_{n\to\infty}\sigma^n=\tau$ gibt es ein k, ab dem die σ^n mindestens auf den ersten r Gliedern mit τ übereinstimmen. Es folgt $\sigma^k\in V(P)\cdot S^\omega$, also $\sigma^k\notin P$.

  „$\Leftarrow$" : Es genügt zu zeigen: $P = S^\omega\text{-}V(P)\cdot S^\omega$ mit $V(P) = \{\ \alpha \in S^* \mid \forall\sigma \in P.\neg(\alpha \prec \sigma)\ \}$
  „$\subseteq$" folgt sofort aus der Definition.
  Sei $\sigma \in S^\omega\text{-}V(P)\cdot S^\omega$. Für jedes $d\in\mathbb{N}$ ist $\sigma_{<d}\notin V(P)$. Also gibt es für jedes $d\in\mathbb{N}$ ein $\sigma^d \in P$ mit $\sigma_{<d}\prec \sigma^d$.
  Es folgt, dass die so konstruierten $(\sigma^d)_{d\in\mathbb{N}}$ gegen σ konvergieren, also $\lim_{d\to\infty}\sigma^d = \tau$. Also ist $\tau \in P$.

Häufungspunkte

- Sei $P \subseteq S^\omega$. Ein Häufungspunkt von P ist eine Folge $\tau \in S^\omega$, so dass es eine Serie $(\sigma^n)_{n \in \mathbb{N}}$ gibt mit $\forall\, n \in \mathbb{N}.\sigma^n \in P$ und $\lim_{n\to\infty} \sigma^n = \tau$.

  Häufungspunkte von P sind also alle Grenzwerte von Serien von Elementen aus P.

- Sei lim(P) die Menge aller Häufungspunkte von P.

- Der vorige Satz besagt also: „P abgeschlossen $\Leftrightarrow$ P enthält alle seine Häufungspunkte"

- Satz: $\lim(P) = Cl(P)$

- Beweis: Wegen $P \subseteq Cl(P)$ und dem vorigen Satz folgt sofort $\lim(P) \subseteq \lim(Cl(P)) \subseteq Cl(P)$.
- Sei $\tau \in Cl(P) = S^\omega - V(P) \cdot S^\omega$. Dann ist kein Präfix von τ in V(P). Für jeden Präfix $\tau_{<k}$ von τ gibt es also ein $\sigma^k \in S^\omega$ mit $\tau_{<k} \cdot \sigma \in P$. Offensichtlich gilt $\tau = \lim_{k\to\infty} \tau_{<k} \cdot \sigma^k$, also $\tau \in \lim(P)$.

- Folgerung: $Cl(P) = S^\omega - V(P) \cdot S^\omega = \lim(P)$.

- Wir haben also zwei Wege, Cl(P) zu bestimmen:
  - über die verbotenen Präfixe und Komplementation
  - als Menge aller Häufungspunkte von P.

König's Lemma und Konvergenz

- Satz: Ist S endlich, so hat jede unendliche Folge von Pfaden eine konvergente Teilfolge

- Beweis: Sei $(\sigma^n)_{n\in\mathbb{N}}$ eine Folge von Pfaden und $T=Pref(\{\sigma^n \mid n\in\mathbb{N}\})$ die Menge aller endlichen Präfixe der Folgen σ^n.
  T ist ein unendlicher Baum. Wenn S endlich ist, dann ist T endlich verzweigend und König's Lemma garantiert einen unendlich langen Ast τ
  Für jeden Präfix $\tau_{<}d$ von τ existiert ein $\sigma^{n(d)}$ mit dem gleichen Präfix. Es folgt: $\lim_{d\in\mathbb{N}}\sigma^{n(d)}=\tau$

Anders ausgedrückt:

- Jede unendliche Folge σ^n hat einen Häufungspunkt.

$P = P_{safe} \cap P_{live}$

- Wir haben zwei Methoden, P_{safe} zu bestimmen
  - Psafe = Cl(P) = S^{ω}-V(P)·S^{ω}
  - Psafe = Cl(P) = lim(P)
- Daraus können wir P_{live} bestimmen als S^{ω}-Cl(P).
- Die Zerlegung $P = P_{safe} \cap P_{live}$ ist aber nicht eindeutig!
- Beispiel: S={Arbeit, Bier}.
  - ∅ und G Arbeit sind Sicherheitseigenschaften
  - S^{ω} und F Bier sind Lebendigkeitseigenschaften
  - ∅ = ∅ ∩ S^{ω} = G Arbeit ∩ F Bier sind verschiedene Zerlegungen von ∅.

Zusammenfassung

G F Ferien