Einbettungen und Projektionen auf Kleene-Algebren

Roland Glück

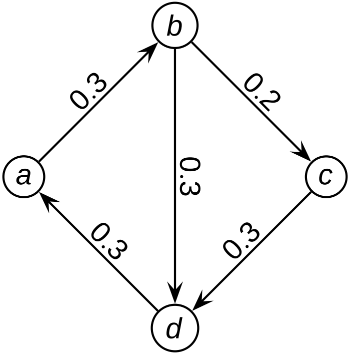
Universität Augsburg

21.05.2008
Sion

Vorschau

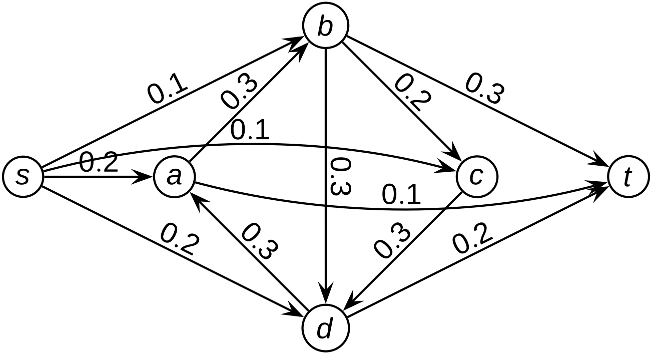
Am Anfang war ...

Wurzel allen Übels:



Am Anfang war ...

Wurzel allen Übels:



Allgemeine Problemstellung

- kleine/untergeordnete Struktur vs. große übergeordnete Struktur
- was in der kleinen Struktur geht, soll in der großen auch gehen
- umgekehrt nicht unbedingt
- z.B. eingeschränkte User-/Zugriffsrechte
- Agenten sehen nur einen Teil der Welt, können nur Teil der Welt beeinflussen

erste Definition

Definition

Für zwei Mengen A und B heißt ein Paar (e, p) von Funktionen $e : A \to B$ und $p : B \to A$ ein *Einbettungs-Projektionspaar* (oder kurz *EPP*) zwischen A und B, falls $p \circ e = id_A$ gilt. e heißt die *Einbettung*, p die *Projektion* des EPPs (e, p).

Beispiel

Ein einfaches Beispiel:

- $A = \{a, b, c, d\}$
- $B = \{a, b, c, d, s, t\}$
- $e = \{(a, a), (b, b), (c, c), (d, d)\}$
- $p = \{(a, a), (b, b), (c, c), (d, d), (s, a), (t, a)\}$

einfache Folgerungen

- Jede Einbettung ist eine injektive Funktion
- Damit gilt $|A| \leq |B|$
- Für $b \in e(A)$ gilt $p(b) = a \Leftrightarrow e(a) = b$
- p ist also durch e teilweise festgelegt

zweifache Folgerungen

- Wenn (e_1, p_1) ein EPP zwischen A und B ist und (e_2, p_2) ein EPP zwischen B und C ist, dann ist $(e_2 \circ e_1, p_1 \circ p_2)$ ein EPP zwischen A und C
- so ist für ein EPP (e, p) zwischen A und B und eine bijektive Funktion $f : B \to B$ auch $(f \circ e, p \circ f^{-1})$ ein EPP zwischen A und B
- Hierarchien von EPPs möglich
- Ist ein EPP wirklich das, was wir wollen?

Halbringe I

Definition

Ein *Halbring* ist eine Struktur $S = (M, +, 0, \cdot, 1)$ mit:

- $(M, +, 0)$ ist ein kommutatives Monoid
- $(M, \cdot, 1)$ ist ein Monoid
- 0 ist ein Annihilator bezüglich $\cdot$: $0 \cdot m = 0 = m \cdot 0 \, \forall m \in M$
- Es gilt Links- und Rechtsdistributivität
- also $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ und $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Halbringe II

- Falls $m + m = m$ gilt, dann heißt S *idempotent*
- In diesem Fall natürlich Ordung $\leq$ gegeben durch $x \leq y \Leftrightarrow x + y = y$
- Beispiele Relationen, Fuzzyrelationen, formale Sprachen, Mengensysteme, Programmabläufe ...
- $+$ repräsentiert Auswahl, $\cdot$ Komposition

Kleene-Algebren I

Definition

Eine *Kleene-Algebra* ist eine Struktur $K = (M, +, 0, \cdot, 1, ^*)$, wobei $(M, +, 0, \cdot, 1)$ ein Halbring ist und * ein Operator auf M mit folgenden Eigenschaften:

- $1 + aa^* \leq a^*$
- $1 + a^*a \leq a^*$
- $b + ax \leq x \Rightarrow a^*b \leq x$
- $b + xa \leq x \Rightarrow ba^* \leq x$

Kleene-Algebren II

- * modelliert endliche Iteration
- entspricht auf formalen Sprachen dem Stern
- dient auch zum Modellieren von Schleifen
- Zusammenhang in Graphen
- ...

Definition

Definition

Ein *Einbettungs-Projektionspaar* (kurz *EPP*) zwischen einer Kleene-Algebra $K_A = (A, +_A, 0_A, \cdot_A, 1_A, ^{*_A})$ und einer Kleene-Algebra $K_B = (B, +_B, 0_B, \cdot_B, 1_B, ^{*_B})$ ist ein EPP (e, p) zwischen A und B mit den zusätzlichen Eigenschaften

- $e(x +_A y) = e(x) +_B e(y)$
- $e(x \cdot_A y) = e(x) \cdot_B e(y)$

Ein einfaches Beispiel:

- Wähle $A = \{a, b, c\}$ und $B = \{a, b, c, d\}$
- Für K_A wähle $Rel(A)$, für K_B wähle $Rel(b)$ mit den bekannten Verknüpfungen und Operatoren
- Setze $e(a) = a$ (betrachte Relationen als Mengen)
- Setze $p(a) = \{p'(x, y) | (x, y) \in a\}$ mit $p'(x, y) = (x, y)$, falls $x, y \in \{a, b, c\}$ und $p'(x, y) = (a, a)$ sonst

einfache Folgerungen

- $x \leq_A y \Rightarrow e(x) \leq_B e(y)$
- $e(x^{*_A}) = e(x)^{*_B}$
- kann als Sicherheitseigenschaft interpretiert werden
- es gelten i.a. *nicht* $e(0_A) = 0_B$ und $e(1_A) = 1_B$
- wähle hierzu $A = \{a\}$ und $B = \{0, 1\}$

- Aussagen über Projektion sind schwieriger
- für $p|_{Im(e)}$ gelten aber analoge Aussagen
- So gilt zum Beispiel $x \leq_B y \Rightarrow p(x) \leq_A p(y)$ für $x, y \in Im(e)$