Kvantové svazy a jejich aplikace v informatice

Jan Paseka

Masarykova Univerzita Brno

Abstrakt přednášky

V přednášce uvedeme základní příklady kvantových svazů a nastíníme metody pro jejich použití v teoretické informatice.
Jedním z těchto příkladů budou tzv. relační kvantové svazy, které tvoří bezespornou a úplnou třídu modelů pro nekomutativní intucionistickou lineární logiku. Dalším pak budou ideály Kleeneho algeber, které jsou studovány v rámci teorie jazyků.

Obsah přednášky

Obsah

Motivace I

1 Úvod a motivace, základní pojmy

Buď X množina (abeceda). Systém konečných posloupností nad X značíme X^* (volný monoid nad X vzhledem k operaci zřetězení $\cdot$). Systém všech podmnožin (jazyků) v X^* značíme $\mathcal{P}(X^*)$ a evidentně platí

$$\bigvee_{i\in I} A_i \cdot B = (\bigvee_{i\in I} A_i) \cdot B \tag{1}$$

$$\bigvee_{i\in I} B \cdot A_i = B \cdot (\bigvee_{i\in I} A_i) \tag{2}$$

$A_i, B \subseteq X^*$. Zde $A \cdot B = \{a \cdot b : a \in A, b \in B\}$.

Motivace II

Úplným polosvazem budeme rozumět uspořádanou množinu S tak, že pro každou její podmnožinu T bude existovat její supremum $\bigvee T$.

Homomorfismem mezi úplnými polosvazy bude zobrazení zachovávající suprema, zejména bude tedy zachováván nejmenší prvek 0. Největší prvek S budeme značit 1.

Motivace III

Označme $\mathcal{Q}(S_1, S_2)$ úplný polosvaz homomorfismů úplných polosvazů z S_1 do S_2 resp. $\mathcal{Q}(S) = \mathcal{Q}(S, S)$, zde S, S_1, S_2 jsou úplné polosvazy. Všimněme si, že $\mathcal{Q}(S)$ je asociativní pologrupa vůči operaci skládání, ve které platí následující distributivní zákony

$$\bigvee_{i\in I} f_i \circ g \;=\; (\bigvee_{i\in I} f_i) \circ g \tag{3}$$

$$\bigvee_{i\in I} g \circ f_i \;=\; g \circ (\bigvee_{i\in I} f_i) \tag{4}$$

pro všechna $f_i, g \in \mathcal{Q}(S)$.

Motivace IV

Kvantovým svazem (*kvantálem*) pak budeme rozumět úplný polosvaz Q opatřený asociativní operací násobení $\cdot$ splňující následující distributivní zákony

$$\bigvee_{i \in I} a_i \cdot b = \Big(\bigvee_{i \in I} a_i\Big) \cdot b \tag{5}$$

$$\bigvee_{i \in I} b \cdot a_i = b \cdot \Big(\bigvee_{i \in I} a_i\Big) \tag{6}$$

pro všechna $a_i, b \in Q$. Homomorfismem mezi kvantovými svazy bude homomorfismus úplných polosvazů zachovávající násobení.

Motivace V

Svazy ideálů v okruzích

Pojem kvantového svazu můžeme vystopovat již v pracech M. Warda a R.P. Dilwortha z 30. let, kteří si uvědomili, že teorii ideálů v okruzích lze vhodně formulovat pomocí pojmu *svazu ideálů* opatřeného asociativní operací násobení. Jsou to například práce

- M. Ward, Residuations in structures over which a multiplication is defined, Duke Mathematical Journal 3 (1937), 627-636.
- M. Ward, Structure residuation, Annals of Mathematics 39 (1938), 558-568.
- M. Ward and R.P. Dilworth, Residuated lattices, Trans. Amer. Math. Soc. 45 (1939), 335–354.
- R.P. Dilworth, Non-commutative residuated lattices, Trans. Amer. Math. Soc. 46 (1939), 426–444.

Motivace VI

Operace reziduace $\to_r - : Q \times Q \to Q$ and $\to_l - : Q \times Q \to Q$ jsou definovány v kvantových svazech předpisem

$$a \to_r x = \bigvee_{a \cdot y \leq x} y \quad \text{a} \quad a \to_l x = \bigvee_{y \cdot a \leq x} y.$$

Pro komutativní kvantový svaz Q je

$$a \to_r x = a \to_l x.$$

Motivace VII

Svazy relací

Další motivace ke studiu kvantových svazů pochází ze studia relačního kalkulu - viz. např. práce

- A. Andréka, Representations of distributive lattice-ordered semigroups, Algebra Universalis, vol. 28 (1991), 12–25.
- A. Andréka and D.A. Bredikhin, The equational theory of union-free algebras of relations, Algebra Universalis, vol. 33 (1995), 516–532.
- C. J. Mulvey, J. W. Pelletier, A Quantisation of the Calculus of Relations, Canadian Mathematical Society Conference Proceeding, vol. 13 (1992), 345–360.

Totiž, pro danou množinu X, množina $\mathcal{R}(X)$ relací na X tvoří kvantový svaz, ve kterém je spojení definováno jako sjednocení a násobení je obvyklé skládání relací.

Motivace VIII

Označme $M = (X, Q, \delta, q_0, F)$ nedeterministický automat s přechodovou relací $\delta : Q \times X \to \mathcal{P}(Q)$.

To nám jednoznačně určuje zobrazení $\delta^* : \mathcal{P}(Q) \times \mathcal{P}(X^*) \to \mathcal{P}(Q)$ předpisem $\delta^*(B, \lambda) = B$, $\delta^*(B, \{v \cdot x\}) = \delta(\delta^*(B, \{v\}), x)$. δ^* má pak následující vlastnosti:

$\delta^*(\bigcup_i B_i, Y) = \bigcup_i \delta^*(B_i, Y)$, $\delta^*(B, \bigcup_i Y_i) = \bigcup_i \delta^*(B, Y_i)$,
$\delta^*(B, Y \cdot Z) = \delta^*(\delta^*(B, Y), Z)$.

Motivace IX

$\mathcal{P}(Q)$ je pak pravý $\mathcal{P}(X^*)$-modul. Mluvíme o tzv. ”klasickém” systému, $\mathcal{P}(X^*)$ je nahrazen libovolným kvantovým svazem a chápeme jej jakožto množinu *konečných pozorování*.

V případě, že nahradíme $\mathcal{P}(Q)$ systémem uzavřených lineárních podprostorů Hilbertova prostoru mluvíme o ”kvantovém systému”.

Motivace X

Pro kvantový svaz Q nazveme *pravým modulem nad* Q úplný polosvaz M společně s akcí $\_\otimes\_ : M \times Q \to M$ splňující

$$(m \otimes a) \otimes b = m \otimes (a \cdot b) \tag{7}$$

$$\left(\bigvee X\right) \otimes a = \bigvee \{x \otimes a : x \in X\} \tag{8}$$

$$m \otimes \bigvee S = \bigvee \{m \otimes s : s \in S\} \tag{9}$$

pro všechna $a, b \in Q$, $m \in M$, $S \subseteq Q$, $X \subseteq M$.

Lineární logika I

2 Lineární logika a kvantové svazy

Girard, 1987 logický operátor $\otimes$ a !, základ pro studium paralelismu v computer science

Identity group

$$\frac{}{A \vdash A}\,\text{axm} \qquad \frac{\Gamma \vdash A \quad A, \Delta \vdash B}{\Gamma, \Delta \vdash B}\,\text{Cut}$$

Logical group

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}\,\multimap \qquad \multimap\,\frac{\Gamma \vdash A \quad B, \Delta \vdash C}{\Gamma, A \multimap B, \Delta \vdash C}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A\&B}\,\& \qquad \&1\,\frac{\Gamma, A \vdash C}{\Gamma, A\&B \vdash C} \qquad \&2\,\frac{\Gamma, B \vdash C}{\Gamma, A\&B \vdash C}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall X A}\,\forall \qquad \forall\,\frac{\Gamma, A[B/X] \vdash C}{\Gamma, \forall X A \vdash C}$$

(X not free in Γ)

$$\frac{!\Gamma \vdash A}{!\Gamma \vdash !A}\,\text{!-box} \qquad \text{der}\,\frac{\Gamma, A \vdash C}{\Gamma, !A \vdash C}$$

Structural Group

$$\text{w}\,\frac{\Gamma \vdash C}{\Gamma, !A \vdash C} \qquad \text{ctr}\,\frac{\Gamma, !A, !A \vdash C}{\Gamma, !A \vdash C}$$

Lineární logika II

Fázová sémantika

Fázový prostor je uspořádaná dvojice $(M, \perp)$, kde M je komutativní monoid a $\perp \subseteq M$.

Klademe $X \cdot Y = \{x \cdot y : x \in X, y \in Y\}$, $X \multimap Y = \{z \in M : X \cdot \{z\} \subseteq Y\}$, $X^{\perp} = X \multimap \perp$. Pokud $X^{\perp\perp} = X$, říkáme, že X je fakt.

Zejména $X \subseteq X^{\perp\perp}, X^{\perp\perp} \cdot Y^{\perp\perp} \subseteq (X \cdot Y)^{\perp\perp}$ a $X \subseteq Y \implies Y^{\perp} \subseteq X^{\perp}$.

${}^{\perp\perp} : \mathcal{P}(M) \to \mathcal{P}(M)$ je uzávěrový operátor, který indukuje na $Fix({}^{\perp\perp})$ strukturu kvantového svazu - fázový kvantový svaz.

Lineární logika III

Fázová sémantika - nekomutativní verze, D. Yetter, 1990

Girardův kvantový svaz je kvantový svaz opatřený cyklickým ($(a \rightarrow_r \perp = a \rightarrow_l \perp)$) dualizujícím ($((a \rightarrow_r \perp) \rightarrow_l \perp = ((a \rightarrow_l \perp) \rightarrow_r \perp)$) prvkem $\perp$.

Girardův kvantový svaz = fázový kvantový svaz

současný stav - studium fázových prostorů - Light Affine Logic (TCS), ap.

Dynamická epistemic logika (DEL) I

3 Dynamická epistemic logika a kvantové svazy

Baltag, Coecke, Sadrzadeh, 2004 - zaměřeno na epistemic programy, tj. programy, který mění informační stav agentů (modelování toku informací, výměna informací mezi agenty). Bezpečná komunikace, umělá inteligence, e-obchod.

Dynamická epistemic logika (DEL) II

Stavový model, trojice $\mathbf{S} = (S, \xrightarrow{A}, \mu)_{A \in \mathcal{A}}$
S množina stavů, $\mathcal{A}$ konečná množina agentů,
$\xrightarrow{A} \subseteq S \times S$ relace dostupnosti každého agenta $A \in \mathcal{A}$, Φ množina možných skutečností,
$\mu : S \to \mathcal{P}(\Phi)$ ohodnocení tj. $s \models \phi$ právě tehdy, když $\phi \in \mu(s)$.
Každé relaci dostupnosti odpovídá zobrazení
$f_A : S \to \mathcal{P}(S)$; $s \mapsto f_A(s) = \{t \in S : s \xrightarrow{A} t\}$, tj. agent A ve stavu s považuje stav t za možný svět.

Dynamická epistemic logika (DEL) II

Epistemic tvrzení P pro stavový model je podmnožina $P \subseteq S$ - stavy, ve kterém je tvrzení pravdivé

$$\mu(P) := \bigcap \{\mu(s) : s \in P\} \in \mathcal{P}(\Phi),$$

$$f_A(P) := \bigcup \{f_A(s) : s \in P\} \in \mathcal{P}(S).$$

Dynamická epistemic logika (DEL) IV

Model akcí, trojice $\Sigma = (\Sigma, \xrightarrow{A}, \mu)_{A \in \mathcal{A}}$

Σ množina akcí, $\xrightarrow{A} \subseteq \Sigma \times \Sigma$ relace dostupnosti každého agenta $A \in \mathcal{A}$, $\mu : \Sigma \to \mathcal{P}(S)$, akci se přiřadí předpoklady pro její uskutečnění.

Epistemic program π pro model akcí je podmnožina $\pi \subseteq \Sigma$

$$\mu(\pi) := \bigcup \{\mu(\sigma) : \sigma \in \pi\} \in \mathcal{P}(S),$$

$$f_A(\pi) := \bigcup \{f_A(\sigma) : \sigma \in \pi\} \in \mathcal{P}(\Sigma).$$

Dynamická epistemic logika (DEL) V

Update produkt $\mathbf{S} \otimes \Sigma$ - stavový model

$S \otimes \Sigma = \bigcup_{\sigma \in \Sigma} \mu(\sigma) \times \{\sigma\} \subseteq S \times \Sigma$

$f_A(s, \sigma) := f_A(s) \times f_A(\sigma), \mu(s, \sigma) := \mu(s).$

Update produkt tvrzení P a programu π

$P \otimes \pi = \bigcup_{\sigma \in \pi} (\mu(\sigma) \cap P) \times \{\sigma\} \subseteq P \times \pi$

Dynamická epistemic logika (DEL) V

Modality

$\Box_A P := \{s \in S : f_A(s) \subseteq P\}$ - agent A ví, že platí P nebo tomu věří - epistemic modalita

$[\pi]P := \{s \in S : \{s\} \otimes \pi \subseteq P\}$ - pro každý stav v $[\pi]P$ bude tvrzení P pravdivé po proběhnutí programu π - dynamická modalita

Dynamická epistemic logika (DEL) V

Sekvenční skládání modelů akcí - $\Sigma_1 \bullet \Sigma_2$

$\Sigma_1 \bullet \Sigma_2 := \Sigma_1 \times \Sigma_2$, $f_A(\sigma_1, \sigma_2) := f_A(\sigma_1) \times f_a(\sigma_2)$, $\mu(\sigma_1, \sigma_2) := \mu(\sigma_1) \cap \bigcup\{[\sigma_1]\psi : \psi \in \mu(\sigma_2)\}$.

Sekvenční skládání programů - $\pi_1 \bullet \pi_2$

$\pi_1 \bullet \pi_2 := \pi_1 \times \pi_2$.

Akční model se skipem - beze změny

$\mu(\text{skip}) = S$, $f_A(\text{skip}) = \{\text{skip}\}$

$S \otimes \text{skip} = S, \Sigma \bullet \text{skip} = \Sigma$.

Dynamická epistemic logika (DEL) V

DEL model - dvojice (S, Σ), S stavový model, Σ model akcí tak, že skip $\in \Sigma$, $S \otimes \Sigma \subseteq S$ a $\Sigma \bullet \Sigma \subseteq \Sigma$.

konkrétní epistemic systém - viz předchozí popis - dvojice $(\mathcal{P}(S), \mathcal{P}(\Sigma))$.

Systém (Abramsky, Vickers 1993) - dvojice (M, Q), Q kvantový svaz, M pravý Q-modul.

Dynamická epistemic logika (DEL) IX

Endomorfismus systému $f : (M, Q) \to (M, Q)$ je dvojice

$$(f^M : M \to M,\ f^Q : Q \to Q),$$

kde f^M je morfismus sup-polosvazů, f^Q je morfismus kvantových svazů a platí $f^M(m \otimes q) = f^M(m) \otimes f^Q(q)$.

Epistemic systém je tvaru $(M, Q, \{f_A\}_{A \in \mathcal{A}})$, (M, Q) systém, $\{f_A\}_{A \in \mathcal{A}}$ systémové endomorfismy.