

1 OBECNÉ POJMY

1.1 GRAFY

- Neorientovaný graf (V, E) kde $e \in E$ sú dvojprvkové podmnožiny V (neusporiadané).
- Orientovaný graf (V, E) kde $E \subseteq V \times V$.
- Izomorfizmus grafov $G \simeq H: f: V(G) \rightarrow V(H)$ t.ž. $(u, v) \in E(G)$ iff $(f(u), f(v)) \in E(H)$.
- Planárny (rovinný) graf: Dá sa nakresliť do roviny bez pretínania hrán.
- (Silno) súvislá komponenta — zo všetkých vrcholov viem dosiahnuť všetky vrcholy.

1.2 VÝROKOVÁ LOGIKA

- Booleovská funkcia $F: [0, 1]^n \rightarrow [0, 1]$. Operátory $\wedge, \vee, \neg, \implies, \dots$ sú funkcie.
- Formula v systéme $\mathcal{L}(F_0, \dots, F_n)$: $\varphi ::= x \in Var \mid F_i(\varphi_0, \dots, \varphi_m)$
- Modelom formule je valuácia literálov $v: Var \rightarrow [0, 1]$: $v \models \varphi$
- Pravdivá/nepravdivá $v \models \varphi$, splniteľná $\exists v: v \models \varphi$, tautológia $\forall v: v \models \varphi$ ($\models \varphi$)
- φ je tautologický dôsledok: $T \models \varphi$ (bez ohľadu na model)
- Normálny tvar: CNF/DNF (klauzula, duálna klauzula, literál)

1.3 LOGIKA PRVÉHO RÁDU

- Premenné $Var: x, \dots$, funkčné symboly $F: f_0, \dots$, predikátové symboly $\mathcal{P}: P_0, \dots$
- Jazyk: Sada funkčných a predikátových symbolov
- Realizácia \mathcal{M} : Univerzum M , relácie $P_i \subseteq M^m$, funkcie $f_i: M^m \rightarrow M$
- **S rovnosťou vs. bez rovnosti**
- Term: $t ::= x \in Var \mid f_i(t_0, \dots, t_m)$
- Formula $\varphi ::= P_i(t_0, \dots, t_m) \mid (t_0 = t_1) \mid \varphi_0 \rightarrow \varphi_1 \mid \neg \varphi_0 \mid \exists x: \varphi$
- Modelom formule je realizácia a valuácia $v: Var \rightarrow M$: $(\mathcal{M}, v) \models \varphi$
- Pravdivá $\mathcal{M} \models \varphi$ (bez ohľadu na valuáciu)
- φ je sémantický dôsledok: $T \models \varphi$ (bez ohľadu na model)
- Teória T je množina axiémov. Teória má model \mathcal{M} ak sú v nej všetky axiémy T pravdivé.

1.4 ODVODZOVACIE SYSTÉMY

- Sada (generických) axiémov a syntaktických odvodzovacích pravidiel.
- Dôkaz: Postupnosť $\varphi_0, \varphi_1, \dots$ kde φ_i je axióm, alebo φ_i vznikne pravidlom z $\varphi_j: j < i$.
- Dokázateľná formula: $\vdash \varphi$, Dokázateľná z predpokladu: $T \vdash \varphi$
- Korektnosť: Dokázateľné je pravdivé ($\vdash \varphi \implies \models \varphi$)
- Úplnosť: Pravdivé je dokázateľné ($\models \varphi \implies \vdash \varphi$)
- Sporná = všetky formule sú dokázateľné.

1.5 LTS A KRIPKEHO ŠTRUKTÚRA

- $LTS = (S, A, \Delta)$ — stavy, akcie a prechody $\Delta \subseteq S \times A \times S$
- $K = (S, T, s_0, L)$ — kde $T \subseteq S \times S$, inícálny stav s_0 a proposition labelling $L : S \rightarrow 2^{AP}$. Väčšinou chceme T totálnu.
- Prechodový systém — T je množina prechodov kde prechod je deterministická funkcia ($T \subseteq \mathcal{P}(S \rightarrow S)$). Interpretujem ako že mám pomenované prechody.

1.6 TRACE EKVIVALENCIA A BISIMULÁCIA

- Trace: jeden beh v LTS
- Trace ekvivalencia = množiny behov systémov sú rovnaké.
- Relácia R je bisimulácia ak spĺňa, že ak $(s, t) \in R$ a $(s, a, s') \in \Delta_0$, tak musí existovať $(t, a, t') \in \Delta_1$ t.ž $(s', t') \in R$ a to isté opačne.
- Dva stavy sú bisimulačne ekvivalentné ak existuje nejaké bisimulácia v ktorej sú v relácii.
- Relácia bisimilarity \sim je najväčšia ekvivalencia ktorá je súčasne bisimulácia.
- Pozn.: Môžem mať situáciu kedy p simuluje q a q simuluje p , ale rôznymi reláciami a teda neviem zostrojiť jednu bisimuláciu ktorá ich zjednotí (Príklad: jeden proces sa rozhodne neskôr a druhý sa rozhodne buď hneď alebo neskôr.)

1.7 OMEGA AUTOMATY

- Omega regulárne jazyky sú tvaru $U.V^\omega$ kde U a V sú regulárne jazyky.
- Buchi automat $(Q, \Sigma, \delta, s_0, F)$ — stavy, abeceda, prechodová relácia (nedeterministická), inícálny stav, akceptujúce stavy.
- Automat akceptuje ak sa v slove nachádza stav z F nekonečne často.
- Zobecnený Buchiho automat: Miesto F mám množinu množín stavov a akceptujem ak prejdem každou z nich nekonečne často.

1.8 CPO A FIXED POINT

- Complete lattice (úplný svaz): Každá podmnožina má suprérum aj infimum.
- Complete partial order (CPO): Každá nekonečná postupnosť $a_0 \sqsubseteq a_1 \sqsubseteq \dots$ má v množine suprérum.
- Directed complete partial order (DCPO): Každá directed množina má suprérum. Directed množina je taká že po dvoch tam majú prvky upper bound.
- Pozn.: každý complete lattice je aj CPO, každý konečný complete lattice je aj DCPO.
- Veta o pevnom bode (Knaster-Tarski): Pre complete lattice (L, \leq) a monotónnu funkciu $f : L \rightarrow L$ platí, že aj fixed pointy f tvoria complete lattice.
- Veta o pevnom bode (Kleene): Pre DCPO (L, \leq) a Scott-spojité (monotónnu) funkciu $f : L \rightarrow L$ existuje najmenší pevný bod ktorý je suprérom postupnosti $f^n(\perp)$. (Zjednodušenie je pre konečný complete lattice a monotónnu funkciu)

1.9 LTL

- $\varphi ::= \text{true} \mid p \mid \neg\varphi \mid \varphi \vee \varphi \mid X \varphi \mid \varphi U \psi$
- Iné operátory: $F\varphi = \text{true} U \varphi$, $G = \neg F\neg\varphi$, $\varphi R \psi = \neg(\neg\varphi U \neg\psi)$ a $\varphi W \psi = (\varphi U \psi) \vee G\varphi$
- Formula ktorú nevyjadrim v CTL: $F(G(\phi))$

1.10 CTL

- $\varphi ::= \text{true} \mid p \mid \neg\varphi \mid \varphi \vee \varphi \mid AX \varphi \mid E/A[\varphi U \psi]$
- Iné operátory: $EX\varphi = \neg AX\neg\varphi$, $E/AF\varphi = E/A[\text{true} U \varphi]$, $E/AG\varphi = \neg A/EF\neg\varphi$
- Formula ktorú nevyjadrim v LTL: $AG(EF(\phi))$

1.11 REAL TIME SYSTEMS

- Procesor (aktívny), zdroj (pasívny), job (jednotka práce), task (periodicky sa opakujúci job)
- Release time r , execution time e , relative/absolute deadline d/D , period p , completion time C , response time $C - r$, utilization $\frac{e}{p}$, density tasku $\frac{e}{\min(p,D)}$ ($\frac{e}{d-r}$ pre job)
- Hard: verification, Soft: validation
- Tasks: Periodic (hard), Aperiodic (soft), Sporadic (hard)

1.12 DISTRIBUOVANÉ SYSTÉMY

- Komunikujúce procesy prepojené sieťou (Iné modely: MapReduce).
- Sieť je buď synchronná alebo asynchronná (všeobecnejšie).
- Komunikácia je drahá — Komunikačná zložitosť (počet, res. veľkosť správ)
- Sieť môže mať rôznu topológiu: ring, star, grid, hypercube, torus, tree, complete graph, unknown
- Zlyhania procesov: nečakaný delay, jednorázové zlyhanie, zlyhanie a zotavenie, bizantínske zlyhanie
- Zlyhania siete: nečakaný delay, packet loss, packet duplication, packet reordering, bizantínske zlyhanie

2 ADVANCED POJMY

2.1 GRAFOVÉ PROBLÉMY

- Nezávislá množina: žiadne dva vrcholy v množine nie sú spojené hranou.
- Vrcholové pokrytie: každá hrana končí vo vrchole ktorý je v pokrytí.
- Dominujúca množina: každý vrchol má suseda v množine.
- Ofarbenie grafu: Každý vrchol má medzi susedmi unikátnu farbu.
- Hamiltonovský cyklus/cesta.
- Reprezentácia grafov: Matica susednosti, Incidenčná matica, zoznam následníkov (hrán), implicitne.

2.2 LOGIKA

- Úplný systém logických spojok: dá sa pomocou neho vyjadriť ľubovoľná logická funkcia. (Dôkaz pre ano/or/not - ľubovoľnú funkciu zakódujem do veľmi hnusného DNF)
- Shefferovská funkcia: úplná sama o sebe (zhruba 1/3 funkcií je shefferovská)
- Lukasiewicz (odvodzovací systém pre výrokovú logiku):
 - A1: $A \rightarrow (B \rightarrow A)$
 - A2: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
 - A3: $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$
 - MP (modus ponens): Z $A \rightarrow B$ a A vyvod' B
- First order logic (odvodzovací systém):
 - A1-A3 + MP
 - $\forall x. \varphi \rightarrow \varphi[x/t]$ (špecifikácia)
 - $\forall x.(A \rightarrow B) \rightarrow (A \rightarrow \forall x.B)$ (ak x nemá voľný výskyt v A , distribúcia)
 - Generalizácia: Z A odvod' $\forall x.A$
 - Rovnosť: $x = x$, ak $x = y$, tak $f(x) = f(y)$ a ak $x = y \wedge P(x)$, tak $P(y)$.
- Veta o dedukcii: Ak $T \vdash (A \rightarrow B)$ tak $T \cup A \vdash B$.
- Veta o kompaktnosti: Nekonečná teória má model práve keď každá konečná podteória má model.
- Löwenheim-Skolem: Ak pre ľubovoľné n existuje model s nosičom mohutnosti n , tak existuje aj nekonečný model.

2.3 GÖDEL

- Peanova aritmetika — axiomy aritmetiky celých čísel v predikátovej logike.
- Gödelov predikát — $\beta(a, b, i, x) \iff x = a \bmod (1 + b(1 + i))$ — kóduje unikátnu (konečnú) postupnosť čísel.
- 1. Veta o neúplnosti: Existuje formula pravdivá v \mathcal{N} ktorá nie je dokázateľná v Peanovej aritmetike.
- Proof sketch: Dôkazy sa dajú kódovať ako čísla, teda môžem mať predikát $proof(x, y)$ ak x je dôkaz y , z tohoto dostanem predikát pre "x je dokázateľné". Na základe toho potom skonštruujem formulu typu $\varphi = \neg provable(\varphi)$. Formula sa nazýva Gödel sentence.
- 2. Veta o neúplnosti: Formula $consis = \neg provable(a \wedge \neg a)$ (ekvivalentné dôkazu bezspornosti) nie je dokázateľná v Peanovej aritmetike pre ľubovoľné a (ani iných podobne silných systémoch).
- Proof sketch: Použijem Gödel sentence g ako a a ukážem že ak $\vdash g$, tak aj $\vdash provable(g)$ a súčasne $\vdash \neg provable(g)$ (toto sa dá dokázať v PA, keďže g je nedokázateľná). Potom ale z $\vdash provable(g)$ plynie $\neg consis$.

2.4 LOGIKY NAD SLOVAMI

- Predikátová logika — kvantifikujem nad pozíciami v slove a mám dva predikáty $Q_a(x)$ (na pozícii x je znak a) a $x < y$.
- Pomerne slabá logika, nevie vyjadriť ani jazyk slov párnej dĺžky.
- Second order logic — pridávam kvantifikáciu nad množinami pozícií a predikát $x \in X$.
- Populárne predikáty: *next*, *last*, *first*... Množiny potom väčšinou definujem induktívne (existuje množina taká že jej prvok je prvý v slove a všetky jej prvky sú o dva za iným prvkom)
- FA to MSOL:
 - Definujem si "partície" do ktorých sa mi rozpadnú pozície slova podľa toho či skončím v tom stave keď prečítam danú pozíciu.
 - Inicializácia: Po prečítaní prvého znaku skončím v množine danej týmto znakom.
 - Množiny pozícií sú dizjunktné a každá pozícia patrí do jednej množiny.
 - Pozície zachovávajú prechodovú funkciu.
 - Potom už stačí napísať že posledná pozícia leží v množine ktorá odpovedá akceptujúcemu stavu.
- MSOL to FA:
 - Postupujem induktívne po formuli. Konštruujem automat ktorý akceptuje slová abecedy $\Sigma \times [0, 1]^n$ kde n je počet voľných premenných a hovorí či je pozícia v danej premennej alebo nie (FO premenné budú mať v celom slove len jednu jednotku).
 - Preklad predikátov je triviálny (proste sa presuniem keď na razím na vhodné kombo znak-príslušnosť)
 - Negácia — nemôžem robiť hlúpy komplement, musím ešte zabezpečiť že nebudem akceptovať malformed slová (FO premenné s viac jednotkami). Viem ale urobiť jazyk validných slov, takže urobím komplement a spriemnikujem s týmto jazykom.
 - Dizjunkcia — rozšírim abecedy jazykov na rovnakú doménu (jeden prechod zdvojam aby šiel bez ohľadu na novú premennú). Potom môžem robiť union.
 - Kvantifikácia — proste useknem celú pozíciu premennej z abecedy.
 - Výsledný automat môže byť veľký — "veža exponentov" vzhľadom k počtu negácií.

2.5 OMEGA AUTOMATY

- Uzavretosť na zjednotenie (blbý union), zretáženie regulárny+omega, res. regulárny^ω
- Prienik: Konštrukcia ako pre prevod zobecneneho automatu: Vytvorím vrstvy pre každý prienikovaný automat a behám medzi vrstvami pri prechode cez koncový stav.
- Komplement: Ano, ale dôkaz je fuj ??????
- Neprázdnosť jazyka je NLOG úplná (Reachability), Ne-univerzálnosť je PSPACE.
- Muller — množiny stavov, akceptujem ak $\inf(w)$ presne matchuje jednu z množín.
- Rabin — páry množín, akceptujem ak existujú pár t.ž. $\inf(w)$ má prienik s prvou ale nie s druhou.
- Street — páry množín, akceptujem ak pre všetky páry $\inf(w)$ má prienik s prvou implikuje že má prienik s druhou.

2.6 OPERAČNÁ SÉMANTIKA

2.7 DENOTAČNÁ SÉMANTIKA

2.8 AXIOMATICKÁ SÉMANTIKA (HOAREHO LOGIKA)