

Rendszermodellezés

Időzített automata szorgalmi feladat

2012. tavasz

Az elkészítendő feladat

A szorgalmi feladat a házi feladathoz specifikált és elkészített üzletifolyamat-modell egy kellően érdekes részének elkészítése időzített automata (Timed Automaton) formalizmussal, illetve analízise az automatára felírt egyszerű temporális logika kifejezésekkel. A javasolt eszköz az UPPAAL, amely a honlapjáról (<http://uppaal.org/>) – kizárólag akadémiai célra – ingyenesen beszerezhető.

A modellezett folyamatrész ne tartalmazzon (fork-join) párhuzamosságot; ha pedig ciklust tartalmaz, akkor valamilyen módon (például ciklusszámláló segédváltozóval) biztosítani kell, hogy ne maradjon benne örökké. Legyenek elágazások a modellben (az üzletifolyamat-moddellel ellentétben itt segédváltozókat felhasználva összefüggéseket is könnyű teremteni köztük) és az elemi tevékenységek / taszkok versengjenek legalább két külön erőforrástípusért. A szorgalmi feladat keretei és az UPPAAL korlátai miatt elég 5-6 folyamatpéldányt indítani, és az egyéb méretek meghatározásakor sem érdemes túlzásokba esni.

A modell helyességéről (pl. deadlock-mentesség) való meggyőződés után vizsgálandó, hogy kihasználhatók-e az erőforrások, illetve hogy az elágazások minden lehetőségét számba véve milyen worst-case időkorlát adható az összes folyamat befejeződésére. Vizsgálandó továbbá (két-három próbálkozás erejéig) az erőforrás-kapacitások hatása erre az időkorlátra.

Az UPPAAL dióhéjban

1. Az UPPAAL modell állapotterképpel és állapotváltozókkal definiált automaták kompozíciójából épül fel. Az állapotváltozók C-szerű szintaxissal adhatók meg, az állapotterkép egy grafikus szerkesztővel. Az állapotátmenetek nem valószínűségi, hanem tisztán nemdeterminisztikus jellegűek. Lehetőség van *automata-sablonok* alkalmazására, amelyek több példányban, akár különböző paraméterezéssel épülhetnek be a rendszerbe.
2. Az automaták kompozíciója alapvetően aszinkron, de lehetőség van különböző automaták állapotátmeneteinek szinkron összeolvasztására randevú *csatornák* (chan) segítségével. Az adatfolyamháló formalizmussal ellentétben a csatornák nem FIFO jellegűek, nincs kapacitásuk, hanem szinkronizálják a „küldést” és „fogadást”. Különböző automatapéldányokban megtalálható *csatorna?* és *csatorna!* jelű állapotátmenet-párok egyszerre, egyetlen szinkron állapotátmenetként tudnak végbemenni, természetesen csak ha az egyéb kényszerek (kiinduló állapot, őrfeltétel) alapján nincsenek tiltva. A csatornák kezelése a változókéra hasonlít: tömbökbe szervezhetőek, paraméterként átadhatóak, stb.
3. Az idő múlása órákkal modellezhető. Az óra nulláról indul (de későbbi állapotátmenetekkel is nullázható) és folyamatosan növekedhet az összes többi órával szinkronban, de az állapotátmenetek *pillanatszerűek* maradnak. Őrfeltételekben fel lehet használni az órák pillanatnyi értékének vagy órák különbségének viszonyát egy időkorláttal, ilyen módon időlegesen engedélyezett állapotátmeneteket lehet készíteni. Az állapotterkép helyei úgynevezett *invariáns*ban írhatnak elő felső korlátot egy órára, ezzel meghatározva, hogy

meddig tartózkodhat azt automata bennük. Az ún. sürgős (urgent) helyekről az automata mindig idő eltelése nélkül lép tovább. Az ún. sürgős csatornán a szinkronizálás, ha engedélyezett, mindig végbemegy, mielőtt az időt telni hagyná (de az egyéb állapotátmenetekkel szemben nincs elsőbbsége).

4. Az elkészült modellen temporális logikai kifejezések segítségével igazolhatóak a helyességre és a teljesítményre vonatkozó követelmények. Az UPPAAL egy nagyon egyszerű logikát támogat, amelyben az útvonal- és temporális operátorok elválaszthatatlanok, és nem ágyazhatóak egymásba. Például azt az elvárást, hogy egy tulajdonság minden esetben örökké igaz, a következő TL kifejezés fejezi ki: $A[(tulajdonság)$, míg az $E\langle\langle tulajdonság \rangle\rangle$ azt jelenti, hogy legalább egyféle lefutás esetén, legalább egy időpontban igaz lesz.
5. További információk (pl. részletes szintaxis) az UPPAAL súgójában olvashatók. A

felkészüléshez érdemes lehet megnézni a honlapon közzétett tutorialt:

<http://www.it.uu.se/research/group/darts/papers/texts/new-tutorial.pdf>

További forrás a „Formális Módszerek” c. tárgy előadásai, különösen a temporális logika ill. a modellellenőrzés témájában:

<http://www.inf.mit.bme.hu/edu/courses/materials/formalis-modszer/2011-tavasz/ea02-temporalis-logikak>

<http://www.inf.mit.bme.hu/edu/courses/materials/formalis-modszer/2011-tavasz/ea03-modellellenorzés>

Folyamatmodellek megfogalmazása UPPAAL-ban

A folyamatból készüljön egy automata-sablon. Minden elemi tevékenység (taszk) leképezendő egy-egy állapothármasra; az első az erőforrásokra várakozást jelenti, a második a taszk végrehajtása közbeni állapot, a harmadik a taszk befejezése utáni átmeneti állapot (elágazásokhoz, stb.). Az erőforrások globálisan deklarált csatornákon kérhetőek el és szabadíthatók fel, ami a taszk állapotába belépéskor és kilépéskor történik. Erőforrástípusonként külön erőforrás-menedzser automaták felügyelik az elérhető kapacitást.

Egy globális óra tartja nyilván a rendszer kezdete óta eltelt időt, ezen kívül minden folyamatpéldány egy saját órával méri a taszkok végrehajtási idejét. A taszk állapotába lépve inicializálódik a lokális óra; a taszk invariánsként figyeli, hogy a befejeződése után a rendszer ne maradjon ebben az állapotban; a kimeneti él pedig csak az idő lejártakor kapcsol be, hogy a taszk idejét ki kelljen tölteni (ez a két határ lazítható, ha a taszk végrehajtási ideje nem fix). Az erőforrás-foglaló csatornák sürgős jelzésűek, hogy az erőforrás rendelkezésre állásakor azonnal elkezdődjön a taszk. A taszk befejezése utáni átmeneti állapot is sürgős, mert az idő a folyamat futása közben csak erőforrásra várva vagy taszk végrehajtás közben telhet. Az egész folyamat befejezésekor átmenetileg egy sürgős állapotban tartózkodik; ennek segítségével azonosítható az az időpont, amikor az utolsó folyamatpéldány épp befejeződik.

A segítségként mellékelt UPPAAL modell egy menzarendszert ír le, amelyben kanállal levest esznek, utána villával téstát; levest nem mindenki kér, de aki nem kér, az vehet téstából repetát; az egyes vendégek különböző késleltetéssel érkeznek az étterembe, és az evőeszközök száma korlátos. Az ellenőrzendő temporális logikai tulajdonságok a modell befejeződésére, holtponmentességére, az egyes erőforrások kihasználtságára vonatkoznak; ezen felül azt biztosítják, hogy legkésőbb a megadott időkorlátig mindenképpen befejeződjön a futás, de az időkorlátig bizonyos esetekben eltartson. Az éles időkorlátra e két utóbbi kifejezéssel alsó és felső korlátokat adhatunk, így

próbálkozásos úton (pontosabban fokozatos intervallumszűkítéssel) határozható meg a rendszer ezen jellemzője.

Leadandó:

Egy ZIP fájlba összeszerkesztve kell feltölteni

- a jegyzőkönyvet egy doc/pdf formátumú dokumentumban:
 - a választott (rész)feladat specifikációját
 - az elkészült időzített automata modell magyarázatát (a modell melyik része mit fejez ki, milyen üzleti folyamat elemek mivé képződtek le, modellezési döntések, stb.)
 - a temporális logikai kritériumokat és magyarázatukat
 - az elvégzett kísérletek leírását, a verifikáció eredményét, a különböző feltételek mellett garantálható időkorlátot
 - minden egyéb megjegyzést (nehézségek, felhasznált eszközök, stb.)
- az összes elkészült forrást (UPPAAL modell, temporális logikai kérdések)

A beadás módja: elektronikus feltöltés a tárgyhonlapon keresztül.

Határidő: 2012. május 13. 23:59

Kontakt

Vörös András, email: vori «kukac» mit «pont» bme «pont» hu

Konzultációt a félév folyamán egyetlen alkalommal fogunk biztosítani, mindenki érkezzen felkészülten, a feladat és az eszközök ismeretének birtokában, konkrét kérdésekkel.

Szerző

Bergmann Gábor, email: bergmann «kukac» mit «pont» bme «pont» hu