Modell transzformáció helyesség ellenőrzése

Önálló laboratórium feladat összefoglalója (1. félév)

Soproni Péter (NLFA6B)
Konzulens: Varró Dániel, Horváth Ákos
BME Méréstechnika és Információs Rendszerek Tanszék
Informatikai infrastruktúra tervezése szakirány, 2006/2007. I. félév

A félév során a cél az olyan alapvető ismeretek megszerzése volt, amelyek szükségesek lehetnek a későbbiekben a modell transzformáció helyesség ellenőrzésével kapcsolatos kutatások sikeres elvégzéséhez. Ennek megfelelően betekintést nyertem az általános modell leíró módszerek, transzformációs eszközök és a helyesség ellenőrzés témakörébe.

A félév első felében a transzformáció helyesség ellenőrzés két elterjedt módszerét vizsgáltam meg, remélve, hogy ezeket fel tudom használni a kutatás során. Ezek a következők voltak:

- A **weakest precondition** a módszer célja, hogy az ismert helyes kimeneti paraméter halmaz alapján meghatározzuk, hogy mi a bemeneti változók értékeinek az a legszélesebb halmaza, amely mellett az eredmény bele esik a kívánt tartományba. A módszer alapját az ún. Floyd-Horac logika képezi.

- A **design by contract** ezzel szemben a kérdésnek a program kódból le nem vezethető részére koncentrál, a priori tudást reprezentál. Ezen keresztül ellenőrzi a művelet helyességét. Mind a transzformáció bemenetére, mind a kimenetére vonatkoztatva alkalmazható, illetve a végrehajtás során bizonyos tulajdonságok invarianciáját kötheti meg.

Ezt követően a modell transzformációk során alkalmazott tudásreprezentációs módszereket vizsgáltam meg, különös tekintettel azok kifejező erejére, illetve a rajtuk értelmezett átalakítási módszerekre. A két legígéretesebb ezek közül:

- A **shapek** a hagyományos gráf reprezentáció kiterjesztése multiplicitás bevezetésével. A koncepció lényege, hogy a hagyományos gráfokkal szemben az egyes pontokra, illetve a pontokhoz tartozó bemenő címkézett élekre azok számosságára vonatkozó megkötéseket, kijelentéseket tesz lehetővé. Így egy-egy él, illetve csomópont a hagyományos értelemben vett társaiból képes többet is reprezentálni. Ezzel a reprezentáció kompaktságát nagymértékben növeli. Ugyanakkor a hurok éleken keresztül iteráció is bevezethető. A megfogalmazás hátránya, hogy nem ismert közvetlen shape-shape transzformáció.

- **A nested quantification** szintén a hagyományos gráfok kiterjesztése. Az egyszerű gráf tekinthető egy olyan logikai kifejezésnek, ahol az egyes élekkel összekötött elemek logikai ’és’ kapcsolatban állnak egymással. Ezt egészíti ki a módszer a minden, illetve a létezik kvantorral, valamint a negáció bevezetésével. A módszer lehetővé teszi a tudás általános reprezentációját, és gráfokra vonatkozó szabályok megfogalmazására is alkalmas.

A két megközelítés közül a második tűnik ígéretesebbnek, mivel ezáltal egy bevált eszköz halmazt, az elsőrendű logikai bizonyítás segéd eszközeit lehet bevetni. Természetesen figyelemmel kell lenni az elsőrendű logika félig eldönthetőségére is. Azaz egyes felmerülő problémák eldönthetetlenek lehetnek, ezeket se belátni, se megcáfolni nem lehet.

A félév utolsó időszakában a helyesség ellenőrzés során felhasználható szoftverek közül próbáltam meg minél többet megismerni, közülük a későbbiek során leginkább használhatót kiválasztani. Ezek a következők voltak:

- **PVS:** igen elterjedt, LISP alapú interaktív tételbizonyító. Széles körű támogatottsággal rendelkezik, korlátozottan képes autonóm, önálló bizonyításra is. Az esetek túlnyomó részben azonban szükség van az emberi beavatkozásra, ami egy későbbi automatikus eszköz kialakításnál hátrányos lehet.

- **ACL2:** igen széles lehetőségeket nyújtó eszköz. Szintén interaktív bizonyító.

- **E-SETHEO:** még a fejlesztés fázisában lévő eszköz, több korábbi megvalósítás egyesítése (SETHEO, E-prover). Képes mind interaktív, mind autonóm bizonyításra is. Több díjat is megnyert, ugyanakkor még nem kiforrott rendszer, használata nehézkes.

- **OTTER:** kiforrott, régi rendszer. Képes autonóm bizonyításra, ugyanakkor nem a legmodernebb. Bemeneti nyelve rokonságot mutat a Prolog nyelvével, emellett inputját más tételbizonyítók is képesek feldolgozni.

- **PROVER9:** Otter alapú eszköz, annál fejlettebb, nagyobb teljesítményre képes.

- **VAMPIRE:** több versenyt is megnyert, jelenleg nem elérhető autonóm bizonyító.

- **SPASS:** autonóm bizonyító eszköz, jó teljesítőképességgel.

Ezek alapján a SPASS és a Prover9 tűnik a legígéretesebbnek, de még további vizsgálatok szükségesek.