Review of Master's Thesis

Student: Malík Viktor, Bc.
Title: Template-Based Synthesis of Heap Abstractions (id 19901)
Reviewer: Hruška Martin, Ing., UITS FIT VUT

1. Assignment complexity — **considerably demanding assignment**

Obtížnost zadání spočívá v následujícím
- Nastudování verifikační techniky, na které je založen rámec 2LS, což je relativně nový přístup k verifikaci software.
- Nastudovat jeho implementaci, která má zatím spíše charakter prototypu, tudíž není ideálně dokumentovaná a srozumitelná.
- Nastudovat nástroje, na kterých 2LS staví, tj. CBMC a MiniSAT.
- Navrhnout zcela novou doménu pro reprezentaci dynamických datových struktur v rámci 2LS.

2. Completeness of assignment requirements — **assignment fulfilled**

3. Length of technical report — **in usual extent**

4. Presentation level of technical report — **95 p. (A)**

Práce je psána srozumitelně a vhodně logicky strukturována. Popisované koncepty nejsou definovány pouze deklarativně pomocí formalismů, ale jsou vždy doprovezeny psedukódem a ve většině případů i příkladem. Tuto snahu studenta vše důkladně a názorně vysvětlit považuji za nadstandardní. Jedinou mojí výtkou je, že text občas působí poněkud úmorně, což je ovšem dáno snahou studenta vysvětlit vše do detailu.

5. Formal aspects of technical report — **90 p. (A)**

Práce je psána dobrou angličtinou. K typografii nemám připomínek.

6. Literature usage — **90 p. (A)**

Student uvedl všechny relevantní zdroje.

7. Implementation results — **95 p. (A)**

Výstupem je rozšíření nástroje 2LS pro verifikaci programů. K práci jsou dodány regresní testy umožňující ověření korektního přeložení nástroje. Nástroj je funkční a dle toho, co mohu posoudit, programátorská úroveň je vysoká.

8. Utilizability of results

Práce přináší nové poznatky v oblasti možnosti shape analýzy v rámci 2LS. Zatím je technika schopna zvládnout pouze seznamy, nicméně předpokládám, že by neměl být principiální problém v jejím rozšíření na komplikované datové struktury. Domnívám se, že práce bude publikovaná na některé kvalitní mezinárodní konferenci. Dosažené výsledky výrazně zlepšily výsledky nástroje 2LS na benchmarku mezinárodní soutěže ve verifikaci SV-COMP v kategorii týkající se dynamických datových struktur. Dá se tedy předpokládat, že práce přispěje k lepším výsledkům nástroje 2LS v dalších ročnících této soutěže. Dále také velmi oceňuji, že již od začátku práce na shape analýze v 2LS student předkládá algoritmy pro interprocedurální analýzu, která je do budoucna nezbytná k tomu, aby nástroj škáloval na větší systémy. To stejné platí i pro první náznaky kombinace domén, např. kombinace analýzy pro dynamické datové struktury s analýzou celočíselných proměnných.

9. Questions for defence

- Uvažoval jste, jak obtížné bude rozšířit navržený přístup na stromové struktury?

10. Total assessment — **95 p. excellent (A)**

Předloženou práci hodnotím velmi pozitivně. Jde o naprůměrně obtížný úkol, který byl splněn nadprůměrným způsobem. Student dokázal vyvinout nový přístup k shape analýze v rámci nástroje 2LS a pomocí implementace demonstroval jeho funkčnost. Jak jsem zmínil, práce má jistě dobrý publikační potenciál. Přepodložená práce zcela splňuje požadavky na inženýrské dílo: a) vychází z nastudování a uchopení potřebné teorie, b) teorii využívá k návrhu algoritmů řešících nový problém, c) algoritmy implementuje v nástroji, jehož dlouhodobým cílem je verifikace větších softwarových systému, nikoliv pouze prototypových příkladů. Proto navrhuji hodnotit práci za **A** a dávám komisi ke zvážení nominace na další ocenění za kvalitní diplomovou práci.

In Brno 9. June 2017

.....
signature