Review of Master's Thesis

Student: Martiček Štefan, Bc.
Title: Synthesizing Non-Termination Proofs from Templates (id 13436)
Reviewer: Fiedor Tomáš, Ing., UITS FIT VUT

1. Assignment complexity **considerably demanding assignment**

Zadání považuji za značně obtížné a přesahující požadavky na běžné magisterské studenty.

1. Implementace vyžaduje důkladné pochopení architektury nástroje 2LS a rovněž praktické použití knihovny MiniSAT.
2. Řešení neterminace programu je obecně nerozhodnutelný problém a aktuálně málo zmapovaná oblast formální analýzy a verifikace. Pochopení metod jejího dokazování vyžaduje nastudování řady akademických zdrojů.
3. Splnění bodu 5. pak vyžaduje efektivní implementaci, která bude fungovat na rozsáhlem benchmarku soutěže SV-COMP.

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

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

Technická zpráva čítá 42 stran vysázených v LaTeXu (tzn. cca 63 normostran). I přes menší počet normostran, považuji rozsah zprávy za dostačující.

4. Presentation level of technical report **70 p. (C)**

Práce má logickou strukturu. Místy je však velice těžce uchopitelná; řada pojmů by zasloužila illustraci pomocí praktických příkladů. Kapitola 2. popisující nástroj 2LS by výrazně ocenila konceptuální diagram a popis celkové architektury nástoje. Není zcela jasné, jak funguje hlavní smyčka nástroje. Mimo popisu samotného nástroje 2LS by určitě bylo vhodné i stručně představit některé jiné nástroje zaměřené na verifikaci neterminace (Ultimate Automizer, HipTNT+). Kapitola 3 je mírně stručná, chybí v ní převážně intuice významu dobrého uspořádání a konečnosti běhu a větší důraz na souvislost se zbytkem práce. Popis implementace v Kapitole 7 je velice strohý. Některé klíčové pojmy nejsou včas a dostatečně vysvětleny (např. phi node).

5. Formal aspects of technical report **100 p. (A)**

Práce je psána velice dobrou angličtinou. Drobné výhrady mám k špatně používané pomlčce (místo toho je používán spojovník) a prezentaci číselných dat v tabulkách (měly by být zarovnané na pravý okraj tabulky).

6. Literature usage **90 p. (A)**

Práce cituje 13 zdrojů, z toho se jedná výhradně o vědecké články. Pro oblast verifikace neterminace tento počet považuji za dostačující. Bibliografické citace jsou v souladu se zvyklostmi verifikační komunity. Nejsem si vědom porušení citační etiky.

7. Implementation results **80 p. (B)**

Výstupem práce jsou dva nové algoritmy pro dokazování neterminace aritmetických programů v jazyce C ve formě modulu v nástroji 2LS. Výsledná realizace má kolem 600 LOC, nicméně vzhledem k tomu, že se jedná o netriviální kód a nové myšlenky, považuji takový rozsah za dostačující. Kód je přeložitelný a funkční.

Výhrady však mám k podobě kódu. Výstup není dostačně komentovaný, je nevhodně strukturovaný (funkce o 200+ LOC), obsahuje nevhodné pojmenování (metoda implementujici algoritmus SRS je ve funkci check_properties, metoda pro algoritmus PRS pak ve check_properties_linear). Je zvláštní, že i když nástroj úspěšně dokáže neterminaci, tak nástroj vypisuje "verification failed".

Namísto srovnání s nástrojem AProVE by bylo vhodnější se zaměřit na nástroj CPAChecker, který byl sice v soutěži v kategorii Terminace pouze bronzový, ale zvládl zverifikovat více neterminačních příkladů než AProVE.

8. Utilizability of results

Práce přináší zcela nové poznatky: (i) metodu hledání tzv. singleton recurrence set---"jednoduchý" princip dokazování neterminace, který očividně v praxi funguje na široké škále příkladů a (ii) hledání tzv. periodic recurrence set, který je využitelný pro další třídu netriviálních příkladů. Práce je realizována v rámci nástroje 2LS, který je pod záštitou firmy DiffBlue, a je aktuálně jeden z nejslibnějších verifikačních nástrojů, který má potenciál být využíván v praxi. Výstupy práce výrazně posouvají nástroj 2LS do medailových příček v soutěži SV-COMP. Očekávám publikaci v rámci SV-COMP sekce konference TACAS'18.

9. Questions for defence

1. Výsledná strategie využívá metodu SRS a po určitém počtu kroků (v kódu se jedná o magickou konstantu 51) se jednou použije metoda PRS a pak zas pokračuje přes SRS. Na základě čeho jste zvolil tento prah (51 kroků)?
2. Stručně diskutujte potenciální rozšíření Vašeho přístupu na programy manipulující s dynamickými datovými strukturami.

10. Total assessment **90 p. excellent (A)**

Práce přináší nové výsledky v oblasti verifikace neterminace a implementuje je v rámci nástroje 2LS, čímž výrazně rozšiřuje jeho stávající schopnosti. Student prokázal schopnost řešit netriviální úkol přesahující požadavky na magisterské studenty a přišel s metodami, které v praxi fungují a dosáhl reálných výsledků. I když vidím nedostatky v technické zprávě a ve výsledné implementaci, vzhledem k obtížnosti práce, dosaženým výsledkům a využití v praxi se přikláním k hodnocení **90 (A)**.

In Brno 7. June 2017

.....
signature