Posudek oponenta bakalářské práce

Student: Vasilišin Maroš
Téma: Knihovna pro boolovské funkce v algebraické normální formě (id 19103)
Oponent: Mrázek Vojtěch, Ing., UPSY FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Zadání očekává vytvoření knihovny pro reprezentaci a manipulaci s boolovskými funkcemi. Práce vychází z teoretických znalostí reprezentace boolovských funkcí a výsledkem by měla být knihovna použitelná pro reprezentaci obvodů pro kryptografii.

2. Splnění požadavků zadání **zadání splněno pouze částečně**

Student teoreticky analyzoval reprezentaci boolovských funkcí a zaměřil se na knihovny pracující s binárními rozhodovacími diagramy. Navržená knihovna však splňuje pouze minimální požadavky na manipulaci s funkcemi reprezentované v ANF. Největší problém vidím v pouze částečně splněném bodu zadání 4, protože student navrženou knihovnu vyhodnotil pouze na základních obvodech a nedemonstroval tak schopnost knihovny pracovat s komplexními obvody, pro které byla určena.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Práce má obvyklý rozsah.

4. Prezentační úroveň předložené práce **60 b. (D)**

Teoretická část popisuje reprezentaci boolovských funkcí a analýzu knihoven pro práci s nimi. Text práce je v určitých ohledech nepřesný - např. v kapitole 2.2 jsou vynechány důležité reprezentace funkcí (grafová reprezentace - která se v práci využívá, reprezentace pomocí diagramů). Vyhodnocení výsledků v textu je někdy neúplné - např. v kapitole 4.3 jsou sice knihovny pro implementaci hashovací tabulky kompletně popsány, ale chybí výsledky, na jejichž základě došlo k porovnání. V popisu realizačního výstupu by mohlo být více ilustrací datové reprezentace místo výpisů kódu. Celková struktura práce je však odpovídající a až na výjimky prezentuje požadované informace.

5. Formální úprava technické zprávy **70 b. (C)**

Typografická úroveň práce je dobrá, některé obrázky jsou však ve špatném rozlišení pro tisk. Jazyková stránka nemohla být kvůli použití slovenského jazyka hodnocena.

6. Práce s literaturou **75 b. (C)**

Autor vybíral odpovídající literaturu z konferenčních, časopisových i knižních publikací zejména z oblasti reprezentace funkcí.

7. Realizační výstup **50 b. (E)**

Realizačním výstupem je knihovna pracující se stromovou reprezentací ANF. Základní manipulační funkce, které knihovna umožňuje, jsou vytváření uzlů, přidávání proměnných do uzlů a manipulace s hodnotami uzlů - tzn. evaluace funkce pomocí zadání hodnot jednotlivým vstupům a zjištění výsledku funkce. Tato reprezentace může být transformována do různých formátů určených pro vizualizaci grafů. Knihovna obsahuje 6 vlastních zdrojových souborů a 7 vlastních hlavičkových souborů. Kód je přehledný a dostatečně komentovaný. Autor implementoval 9 testů, které slouží k demonstraci vytváření struktury ANF a práci s hashovací tabulkou. Testuje ANF reprezentaci a evaluaci jednoduchých boolovských funkcí se 4 vstupy přes všechny vstupní proměnné.
Největší slabinu realizačního výstupu vidím v tom, že knihovna nebyla použita pro návrh většího obvodu (viz bod 4 zadání). Knihovna neumožňuje provádět další operace, které by se u takového typu aplikace dalo předpokládat: transformace do CNF pro SAT solvery, implementace Gaussovy eliminační metody pro určení SAT, umožnění přidávání dalších typů uzlů (AND, NAND, OR, NOR). Dále se domnívám, že porovnání výkonnosti vůči knihovně CUDD (kapitola 6), která pracuje s binárními rozhodovacími stromy, které nemají nativní podporu XOR uzlů, je nevhodné. Tato knihovna musí řešit transformace a binární rozhodovací stromy reprezentují XOR funkce s velkým počtem uzlů.

8. Využitelnost výsledků

Výsledná knihovna vytváří základní datovou strukturu pro práci s rovnicemi v ANF. Pro praktické využití v oblasti kryptografie, kde tyto rovnice mají velký význam, však chybí manipulace s těmito stromy.

9. Otázky k obhajobě

1. Jaké jsou cílové aplikace, ve kterých je výhodné navrženou knihovnu použít?
2. Jak je potřeba knihovnu rozšířit, aby byl bod 4 zadání splněn?

10. Souhrnné hodnocení **51 b. dostatečně (E)**

Realizační výstup této práce splňuje minimální požadavky dané zadáním. Největší slabina této práce je

nedostatečné vyhodnocení funkčnosti knihovny dané bodem 4 zadání. Tento bod zadání byl splněn pouze částečně. Autor však v technické zprávě poměrně detailně (na 10 vysázených stranách) diskutuje možnosti reprezentace logických funkcí a čerpá z relevantní literatury. Vlastní knihovna je funkční, otestovaná, ovšem funkčnost je menší, než by se u práce tohoto druhu očekávalo. Proto navrhuji po zodpovězení otázky k obhajobě hodnocení **E - dostatečně**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 28. května 2017

.....
podpis