Posudek oponenta diplomové práce

Student: Kidoň Marek, Bc.
Téma: Evoluční návrh hašovacích funkcí (id 18335)
Oponent: Bidlo Michal, Ing., Ph.D., UPSY FIT VUT

1. Náročnost zadání

průměrně obtížné zadání

Práce se zabývá nekonvenční technikou návrhu hašovacích funkcí pomocí genetického programování (GP). Klíčovým prvkem byla volba funkcí, na nichž budou hašovací algoritmy postaveny, a návrh fitness funkce. Uvažované koncepty hašování i GP jsou již dobře zavedené techniky, z toho důvodu považuji téma za průměrně náročné.

2. Splnění požadavků zadání

zadání splněno

3. Rozsah technické zprávy

je v obvyklém rozmezí

4. Prezentační úroveň předložené práce

78 b. (C)

Práce má celkově vhodnou logickou stavbu, jednotlivé kapitoly i prezentace výsledků jsou dobře pochopitelné. Nedostatky jsou následující:

- V sekci 2.1 jsou faktické chyby u popisu principů hašování (zjevně nesprávné symboly v prvním odstavci této sekce, dále nepřesnosti ve vyjádření funkce na str. 5).
- Sekce 3.2 dle nadpisu popisuje evoluční algoritmy (EA) -- to je však celá třída různých technik, ve skutečnosti je až do sekce 2.5 popisován genetický algoritmus (GA).
- Jelikož bylo použito pouze GP, stačilo detailně popsat pouze tuto techniku se stručným uvedením vztahu ke třídě EA.
- V technické zprávě chybí jakékoliv ukázky nalezených hašovacích funkcí, jejich podrobnější analýza a zhodnocení (očekával bych alespoň jeden nejlepší výsledek z každé sady experimentů), jediný exemplář lze spatřit v přiloženém článku z konference Excel@FIT. Výsledky v DP tak shrnují pouze celkové statistické vyhodnocení experimentů.
- Další méně závažné nepřesnosti jsou v textu vyznačeny.

5. Formální úprava technické zprávy

70 b. (C)

Formální stránka je na poměrně slušné úrovni až na jisté množství pravopisných chyb a překlepů (v textu vyznačeny).

6. Práce s literaturou

70 b. (C)

Seznam literatury obsahuje relevantní zdroje, na které je z příslušných míst v textu odkazováno. Na několika málo místech však citace chybí (v textu vyznačeno), případně je uveden obecnější zdroj namísto původního článku (např. u popisu GA či evoluční strategie, původní literatura v seznamu chybí).

7. Realizační výstup

80 b. (B)

Diplomant realizoval celkem tři sady experimentů řešících problematiku hašování v doméně IP adres. Konkrétně se jednalo o přímý návrh hašovacích algoritmů z dané množiny elementárních funkcí, dále optimalizace modifikovaného MD schématu a návrh kukaččího hašování se dvěma hašovacími funkcemi. Bylo provedeno základní statistické vyhodnocení evoluce, vlastností výsledných hašovacích algoritmů a jejich vzájemné porovnání.

Na přiloženém CD jsou uvedeny pouze dva soubory s výsledky hašovacích funkcí (další zde nelze dohledat). Vzhledem k množství provedených experimentů a statistikám v technické zprávě bych očekával, že bude tento hodnotný materiál shrnut pro případné další studium. Adresáře, v nichž by se dle popisu výsledky měly nacházet, jsou však prázdné.

8. Využitelnost výsledků

Práce přináší původní vědecké výsledky, jejichž předběžná verze byla publikována na studentské akci Excel@FIT, kde získal příspěvek dvě ocenění. Po dopracování a rozšíření budou výsledky publikovatelné i na mezinárodní konferenci či v časopisu.

9. Otázky k obhajobě

1. Jaký je význam četnosti 0.05 u elitismu v tabulce 4.1 na str. 27?
2. Jakým způsobem byly získány trénovací datasety a v čem se zásadně odlišují, když v řadě případů dávají značně různé výsledky při vyhodnocování výsledných hašovacích funkcí?
3. Kolik operací (řádově) obsahují Vámi nalezené hašovací funkce?
4. Je možné výrazy hašovacích funkcí, nalezené pomocí CGP, dále optimalizovat (zjednodušit) např. pomocí vhodného matematického SW?

10. Souhrnné hodnocení

77 b. dobře (C)

Jedná se o kvalitní DP s publikovatelnými výsledky, jejichž úroveň byla již potvrzena oceněním na akci Excel@FIT. Vzhledem k některým nepřehlédnutelným nedostatkům v technické zprávě a absenci ukázek nalezených hašovacích technik navrhuji hodnocení známkou C.

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

V Brně dne: 6. června 2016

.....
podpis