# Posudek oponenta bakalářské práce

**Student:** Michalisko Tomáš
**Téma:** Návrh hašovacích funkcí pomocí genetického programování (id 24915)
**Oponent:** Piňos Michal, Ing., UPSY FIT VUT

**1. Náročnost zadání** **průměrně obtížné zadání**

Cílem této práce byl automatizovaný návrh hašovacích funkcí s využitím genetického programování. Toto zadání obnášelo nastudování metod návrhu a evaluace hašovacích funkcí, společně se zpracováním studie využití evolučních algoritmů v kontextu návrhu hašovacích funkcí. V rámci této práce bylo implementováno kartézské genetické programování pro návrh hašovacích funkcí pro účely tzv. kukaččího hašování. Navržené řešení bylo dále otestováno a porovnáno s ostatními hašovacími funkcemi na zadaných trénovacích a testovacích datech. Jedná se o průměrně obtížné zadání, ovšem s výzkumným potenciálem.

**2. Splnění požadavků zadání** **zadání splněno s podstatným rozšířením**

Zadání bylo splněno v plném rozsahu.

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

Je v obvyklém rozmezí. Počet stran lehce převyšuje minimální počet normostran pro bakalářskou práci.

**4. Prezentační úroveň předložené práce** **85 b. (B)**

Celkově je práce dobře strukturována, rozsahy a návaznost jednotlivých kapitol jsou do jisté míry vyhovující. Na několika místech je ovšem text nepřehledný či hůře pochopitelný.
Například v sekci 2.1 je hašovací klíč označen symbolem "k", nicméně hned v další kapitole je označen symbolem "x". Dále je napříč několika sekcemi míchán pojem kandidát, kandidátní řešení, jedinec atd.
V popisu implementace programu v sekci 6.4 je řečeno, že jako rodič je zvolen jedinec s nejvyšší fitness, což je v rozporu s tím, že nižší fitness znamená lepší řešení.
Dále mi v technické zprávě chybí bližší popis využití hašovacích funkcí v kontextu síťového provozu.

**5. Formální úprava technické zprávy** **85 b. (B)**

Práce je psána spisovnou češtinou, nicméně se lze na několika místech setkat s překlepy, chybným skloňováním, nejastnostmi či chybějící čárkou.

**6. Práce s literaturou** **100 b. (A)**

Použitá literatura odpovídá problematice řešené v této práci. Seznam literatury obsahuje 36 položek, které jsou zapsané a použité v souladu s citačními zvyklostmi.

**7. Realizační výstup** **100 b. (A)**

Realizačním výstupem je implementace CGP algoritmu pro automatizovaný návrh hašovacích funkcí v jazyce C++. Student provedl velké množství experimentů, zahrnující experimenty s cílem nalézt vhodné nastavení parametrů kukaččiho hašování nebo experimenty hledající vhodné parametry CGP algoritmu (jako je velikost CGP mřížky, množina použitých funkcí nebo pravděpodobnost mutace). Student rovněž experimentoval s různými implementacemi mutací a způsobu vyhodnocení jedinců. V neposlední řadě student provedl experimenty porovnávající navržené hašovací funkce s existujícími state-of-the-art hašovacími funkcemi na poskytnuté trénovací a testovací sadě.
Zdrojové soubory jsou přehledné a dobře komentované. Převzaté části, zejména implementace hašovacích funkcí použitých pro porovnání s navrženými hašovacími funkcemi, byly řádně označeny a použity v souladu s licenčními podmínkami.

**8. Využitelnost výsledků**

Experimenty provedené na poskytnuté testovací sadě ukázaly, že implementovaná metoda je schopna navrhovat hašovací funkce, které jsou porovnatelné a v některých případech dokonce lepší, než obecně známé a ručně navržené hašovací funkce. Výsledky této práce mají bezpochyby výzkumný potenciál a mohly by být základem pro vědeckou publikaci.

**9. Otázky k obhajobě**

- Jak si vysvětlujete, že pro 16bitové a 32bitové bloky s verzí XOR Folding se jeví jako nejlepší množina funkcí F11 (tedy množina obsahující pouze sčítání)? Je toto zjištění nějakým způsobem uplatnitelné v praxi?
- Dalo by se Vaše řešení použít i pro návrh hašovacích funkcí pro jiné účely, například z oblasti bezpečnosti? Pokud ano, jaké změny v současném návrhu/implementaci by byly nutné?

**10. Souhrnné hodnocení** **90 b. výborně (A)**

Ikdyž se jednalo o průměrně obtížné zadání, tak bylo splněno nadstandardním způsobem. To se zejména

odrazilo na počtu experimentů, kterých bylo provedeno nepřeberné množství. Celkový dojem ovšem trošku kazí horší kvalita technické zprávy. Celkově hodnotím práci stupněm A - výborně.

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

V Brně dne: 30. května 2022

Piňos Michal, Ing.
oponent