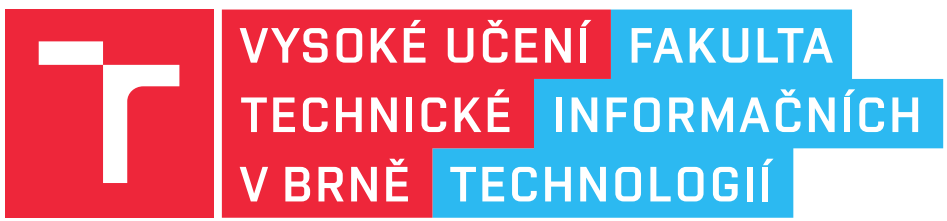
Optimalizace parametrů evoluce ohnutých booleovských funkcí

Karel Ondřej

Fakulta informačních technologií Vysokého učení technického v Brně
Božetěchova 1/2. 612 66 Brno - Královo Pole

xondre09@stud.fit.vutbr.cz



9. května 2019

Zadání

- Číslo zadání: 03
- Vedoucí: Ing. Jakub Husa
- Vlastní výběr evolučního algoritmu.
- Hledání booleovských funkcí o 10 vstupech dosahujících maximální možné nelinearity.
- Experimentovat s dvěma zvolenými parametry algoritmu.
- Zhodnocení výsledků experimentů ve formě tabulky.

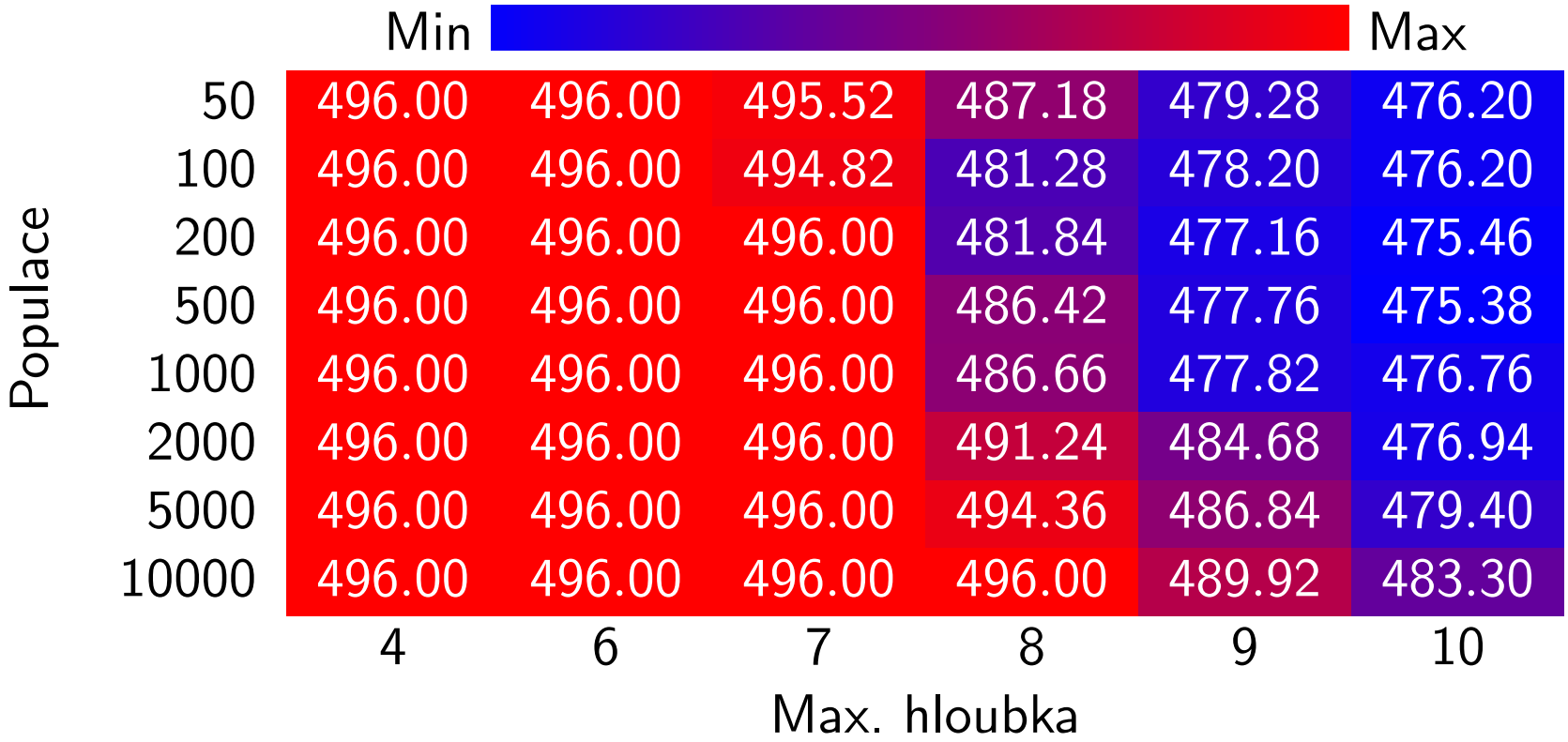
- Booleovské ohnuté funkce se využívají v kryptografii.
- Pro booleovské funkce o 10 vstupech existuje 2^{10} afinních funkcí (lineární funkce a jejich komplementy).
- Nelinearita je nejmenší Hammingova vzdálenost mezi libovolnou afinní funkcí.

- Genetické programování.
  - Parametry: hloubka stromu, velikost populace.
  - Množina operací: and, nand, or, nor, xor, nxor.
  - Inicializace populace: Ramped-half-and-half.
  - Výběr pomocí turnaje.
  - Jeden operátor křížení.
  - Dva operátory mutace.
- Programovací jazyk:
  - Python,
  - C++,
  - Framework[1].

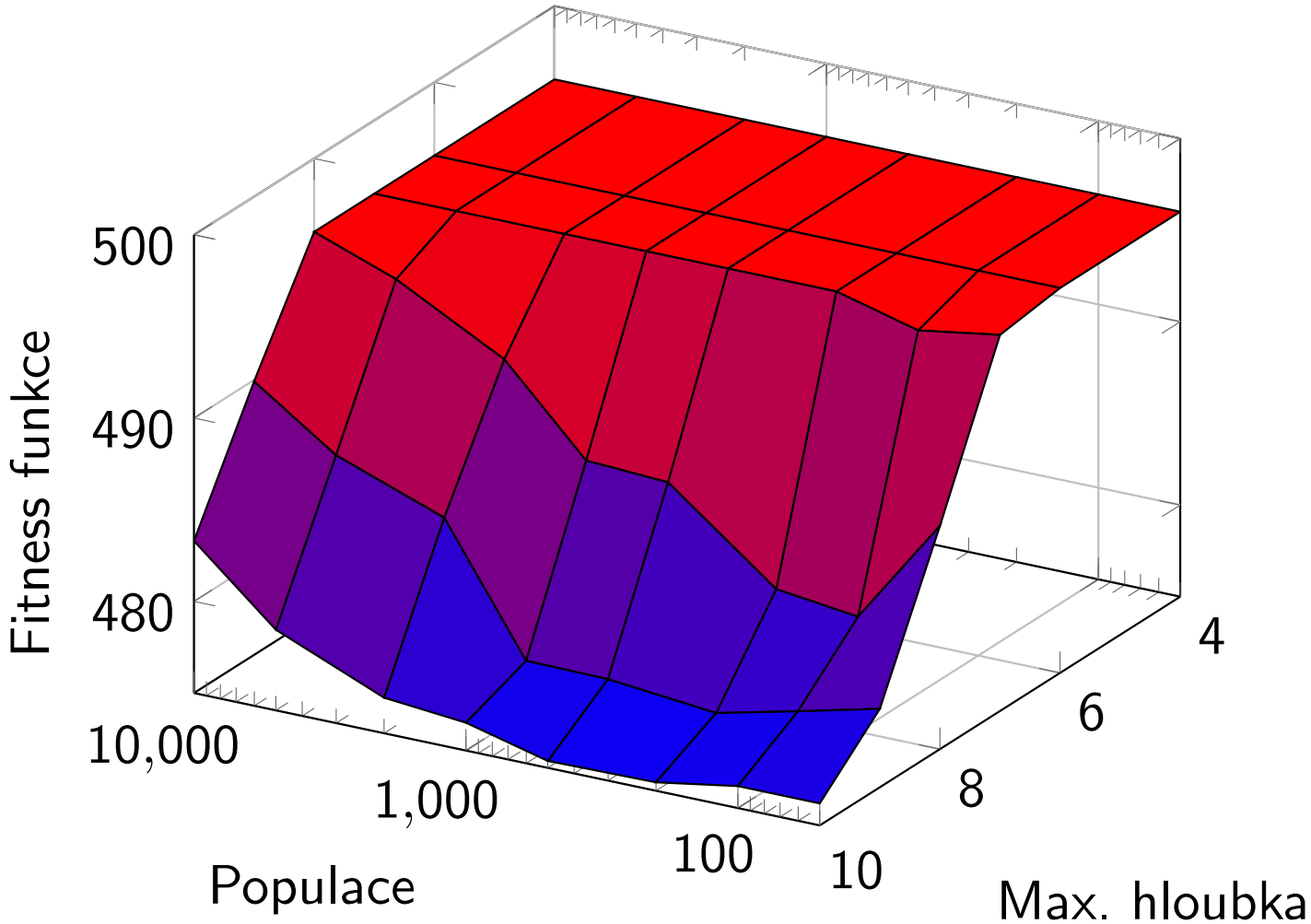
[1] ECF - Evolutionary Computation Framework (http://ecf.zemris.fer.hr/).

- Hloubka stromu $\{4, 6, 7, 8, 9, 10\}$.
- Velikost generace $\{50, 100, 200, 500, 1000, 2000, 5000, 10000\}$.
- Pro každou kombinaci parametrů 50 běhů.
- Ukončení po $0,5 \cdot 10^6$ evaluací nebo nalezení maximální možné nelinearity $N_f = 496$.

Výsledky experimentu – Heatmap



Výsledky experimentu – Graf



```
./bin-gp $1 $2 $3 $4 $5
```

```
$1      Minimální hloubka stromu.
$2      Maximální hloubka stromu.
$3      Velikost populace.
$4      Počet běhů.
$5      Maximální počet evaluací.
```

```
<?xml version="1.0" encoding="UTF-8"?>
<project>
  <batch population.size="50" deep.max="4" ... >
    <run number="1">
      <individual fitness="496" ... >
        <tree size="31" deep="4" notation="postfix">
          ...
        </tree>
      </individual>
    </run>
  </batch>
</project>
```

Zhodnocení

- Implementován evoluční algoritmus genetické programování pro hledání funkcí s velkou nelinearitou.
- Provedeny experimenty s parametry: velikost populace, maximální hloubka stromu.
- Maximální hloubka stromu má oproti velikosti populace významný vliv na kvalitu řešení.
- Ohodnocení jedince je časově náročné.