Posudek oponenta diplomové práce

Student: Mikuš Dávid, Bc.
Téma: Distribuované generování hesel pomocí pravděpodobnostních gramatik (id 21694)
Oponent: Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Zadání se zaměřuje na optimalizaci procesu generování a distribuci vět jazyka popsaného prostředky PCFG. Přestože cílem je reimplementace existujícího řešení, bylo nutné nastudovat potřebnou teorii a provést experimentální vyhodnocení vytvořené metody a její srovnání s původním přístupem.

2. Splnění požadavků zadání **zadání splněno**

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

4. Prezentační úroveň předložené práce **80 b. (B)**

Práce má vhodnou strukturu, jenž čtenáře nejprve uvádí do řešené problematiky a představuje existující systémy pro hledání hesel. Dále se pak práce již věnuje generování hesel pomocí PCFG a distribuce gramatik na klientské uzly. Hlavní výsledek práce, kterým je implementace distribuovaného generátoru hesel je uvedena v kapitole 5 a následně vyhodnocena v kapitole 6.

Práce je dobře pro čtenáře pochopitelná snad krom kapitol 3.2.1 a 3.2.2, kde je popsána funkce Next. Zde není z textu jasné jak tato funkce pracuje a jaký je význam prioritní fronty. Dále se pak objevují drobné chyby:

- Rovnice 2.3 na straně 7 není správně.
- Definice funkce generátoru hesel na straně 8 dole má být $g: N \to P$.

Celkově je prezentační úroveň práce na velmi dobré úrovni.

5. Formální úprava technické zprávy **90 b. (A)**

Typografická úprava práce a také její jazyková stránka je téměř bezchybná. Místy se objevují pouze drobné nedostatky, například mezery před "." či ",".

6. Práce s literaturou **95 b. (A)**

Autor použil množství relevantních informačních zdrojů sestávajících se zejména z vědeckých článků souvisejících s problematikou generování hesel. Ačkoliv se jedná o relevantní informace, bylo by vhodné uvést také nějaký aktuálnější zdroj, pokud existuje.

7. Realizační výstup **90 b. (A)**

Realizačním výstupem je implementace generátoru hesel s podporou jejich distribuce napsaná v jazyce Go. Jedná se o klient-server aplikaci, která podle zadaných parametrů dokáže generovat na serverové části preterminální struktury, které jsou distribuovány na aktivní klienty, kde jsou dále použity pro generování hesel.

Implementace je funkční a její vlastnosti byly demonstrovány v rámci různých experimentech, které ukázaly škálovatelnost systému.

8. Využitelnost výsledků

Práce volně navazuje na disertaci C.M.Weira z roku 2010 vytvořením nové implementace generátoru hesel pro PCFG. Nově vytvořená implementace má zajímavé vlastnosti, které lze s výhodou použít v praxi.

9. Otázky k obhajobě

- V tabulce 3.5 je několik příkladů odvození preterminálních struktur. Proč věta asd1234qw odpovídá K3D4L2 a ne K3K4K2?
- V práci je zmíněna možnost distribuce generování preterminálních struktur (4.2), což je v textu demonstrováno pouze jednoduchým příkladem. Jak by toto bylo možné pro složitější gramatiku a více klientský uzlů (100+)?

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

Jedná se o zajímavé téma, kde se využívá teorie PCFG pro vytvoření gramatiky popisující množinu, které jsou pak v distribuovaném prostředí generovány a pomocí nástroje Hashcat ověřovány.

Textová část práce je na velmi dobré úrovni, kdy veškeré uvedené informace jsou relevantní a až na jedno místo

i výborně vysvětleny, takže je práce, ač se jedná o poměrně komplikované téma, pro čtenáře srozumitelná.

Implementační část je funkční a bylo dostatečně demonstrováno, že má vhodné vlastnosti pro praktické použití.

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

V Brně dne: 5. června 2019

Ryšavý Ondřej, doc. Ing., Ph.D.
oponent