Posudek bakalářské práce

předložené na Matematicko-fyzikální fakultě
Univerzity Karlovy v Praze

☐ ~~posudek vedoucího~~ ☒ posudek oponenta

Autor:	**Luboš Turek**
Název práce:	**Použití ACO algoritmu na řešení jednoduché substituční šifry**
Studijní program a obor:	**Obecná informatika**
Rok odevzdání:	**2012**

Jméno a tituly oponenta:	**RNDr. Pavel Surynek, Ph.D.**
Pracoviště:	**Katedra teoretické informatiky a matematické logiky**

	excelentní	**odpovídající**	**slabší**	**nevyhovující**
Náročnost zadaného tématu		X	X	
Míra splnění zadání		X		
Struktura textové části práce			X	
Jazyková a typografická úroveň				X
Analýza				X
Vývojová dokumentace		X		
Uživatelská dokumentace		X		
Kvalita zpracování softwarové části		X		
Stabilita aplikace		X		

Předložená práce se zabývá využitím techniky Ant Colony Optimization (ACO) na prolomení substituční šifry. Využití techniky ACO je implementováno formou jednoduchého softwaru. Řešitel rovněž srovnal techniku ACO na daném problému s genetickým algoritmem.

Bohužel téma práce je slabě motivováno, není provedena žádná analýza toho, proč by mělo být vhodné použít pro řešení substituční šifry zrovna ACO. Vzhledem k tomu, že existují jednodušší efektivní – polynomiální – algoritmy pro danou úlohu, jako je frekvenční analýza, nevidím žádný důvod nasazovat ACO, které je vhodné spíše pro NP-těžké úlohy (klasické využití je TSP). Z tohoto pohledu je práce nevědecká.

Samotný text práce je napsán velmi ledabyle, obsahuje řadu nepřesností a to zejména v důležitých definicích. Domnívám se, že v tomto stavu práce neměla být odevzdána k obhajobě.

Nejvýznamnější klady:

Oceňuji srovnání s genetickým algoritmem. Jedná se o jediný aspekt, který práci činí ještě stále obhajitelnou. Vhodnější by však bylo srovnání s algoritmem z jiné kategorie, např. s frekvenční analýzou.

Nejzávažnější nedostatky:

Práce má řadu konkrétních nedostatků, které popisuji v další sekci. Za nejvážnější však považuji celkově nevhodné pojetí práce – jedná se o pouhé cvičení na aplikaci ACO na jednoduchou úlohu bez ambice zodpovědět nějakou, byť dílčí, vědeckou otázku.

Další poznámky:

Domnívám se, že řešitel podceňuje možnosti současné výpočetní techniky, když předpokládá, že ověření správnosti klíče trvá na současné výpočetní technice jednu milisekundu (tj. 0.001s) [strana 10]. Není jasné, co úkol ověření klíče představuje a jakou výpočetní techniku řešitel uvažuje (komoditní PC, superpočítač, speciální HW, GPU), uvedený časový údaj tedy považuji za nepodložený.

V práci se vyskytuje řada termínů, které do tohoto druhu textu (vědecké pojednání) nepatří – např. „našroubovat“ problém [strana 7, strana 21], „zaseknout“ se v minimu [strana 12], chování „se dá lehce“ simulovat [strana 14], “nějakým způsobem vidět rozložení” [strana 28], „je vyhozená výjimka” [strana 28].

Dále v práci narazíme na několik vyjádření, které považuji za poněkud překvapivá a doporučil bych je nahradit jinou formou – „pod pojmem mravenec k myslím agenta …“ [strana 16], „snažím se být maximálně stručný, jelikož detailní popis by se rozsahem vyrovnal zbytku práce“ [strana 46], název sekce 3.11 “Další” – působí nedbale, „uvědomil jsem si, že jediné, co po této třídě požaduji, je …“ [strana 31], „je třeba umět zpracovat i texty ze života” [strana 33].

V části „Biologická inspirace“ [strana 13] by bylo vhodné k faktům z biologie uvádět zdroj, aby bylo možné fakta ověřit a to z důvodu, že lze předpokládat, že práci bude oponovat nikoli biolog.

Definice optimalizačního problému je evidentně chybná, neboť množina omezení Ω nehraje žádnou roli [strana 14]. Formulace „f je v s^* minimální“ je nejasná – jaký obor pro hledání minima se uvažuje? Zde by pravděpodobně měla přijít ke slovu množina omezení Ω.

Popis reprezentace optimalizačního problému [strana 15] se zdá být pouze přibližný. Například jednou je množina přípustných řešení označována jako S [bod 5 a bod 6], později je jako množina přípustných řešení označována množina $\tilde{S}$ [bod 8], pro kterou má platit, že $\tilde{S} \in S$, což je evidentně nesmysl. Navíc S v původní definici optimalizačního problému označuje množinu možných řešení, takže je velmi těžké se v definicích vyznat (nutno říci, že S v pů-

vodní definici používá jiný font, takže se možná jedná o jinou množinu, v tom případě se ale smysl ztrácí úplně). Celkově bych sekci reprezentace optimalizačního problému označil za chaotickou.

Sekce Ant Systém vysvětluje proměnné α, β, $\eta_{a,b}$ vystupující ve vzorci [strana 18], tak že „α, β jsou parametry“ a „$\eta_{a,b}$ je heuristická informace“. Tento popis považuji za ekvivalentní žádnému popisu.

Pokud je práce v češtině, doporučil bych být konzistentní a rovněž v obrázcích používat český popis [obrázek 4.1] – pouhé zkopírování z originálu působí ledabyle.

Na začátku kapitoly 5 [strana 27] se dozvíme, čím vším tato kapitola není – není referenční příručkou k API ani uživatelskou příručkou. Pozitivní vyjádření by bylo vhodnější.

Často v práci narazíme na přesah nerozděleného slova mimo stránku (práce je pravděpodobně psána v systému TeX).

Shrnutí:

Práce má potenciál k tomu být kvalitní bakalářskou prací na MFF, ovšem v současné podobě tento potenciál naplňuje jen z části, proto navrhuji hodnocení **dobře**. O výsledku nechť rozhodne obhajoba.

	výborně	**velmi dobře**	**dobře**	**neprospěl/a**
Návrh známky			**X**	

V Kobe, dne 8. června 2012

RNDr. Pavel Surynek, Ph.D.