Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze

Autor práce	Martin Dvořák		
Název práce	Využití celulárních automatů pro šifrování dat		
Rok odevzdání	2017		
Studijní program	Informatika	**Studijní obor**	Obecná informatika

Autor posudku	Mgr. Otakar Trunda	**Role**	Vedoucí
Pracoviště	Katedra teoretické informatiky a matematické logiky		

Prosím vyplňte hodnocení křížkem u každého kritéria. Hodnocení *OK* označuje práci, která kritérium vhodným způsobem splňuje. Hodnocení *lepší* a *horší* označují splnění nad a pod rámec obvyklý pro bakalářskou práci, hodnocení *nevyhovuje* označuje práci, která by neměla být obhájena. Hodnocení v případě potřeby doplňte komentářem. Komentář prosím doplňte všude, kde je hodnocení jiné než *OK*.

K celé práci	lepší	OK	horší	nevyhovuje
Obtížnost zadání	☐	☒	☐	☐
Splnění zadání	☒	☒	☐	☐
Rozsah práce *... textová i implementační část, zohlednění náročnosti*	☒	☒	☐	☐
Komentář Obtížnost práce je standardní a zadání bylo v odpovídající míře splněné. Rozsahem textové části, experimentů i zdrojových kódů jde práce nad rámec standardní bakalářské práce.				

Textová část práce	lepší	OK	horší	nevyhovuje
Formální úprava *... jazyková úroveň, typografická úroveň, citace*	☐	☒	☐	☐
Struktura textu *... kontext, cíle, analýza, návrh, vyhodnocení, úroveň detailu*	☒	☒	☐	☐
Analýza	☐	☒	☐	☐
Vývojová dokumentace	☒	☒	☐	☐
Uživatelská dokumentace	☐	☒	☐	☐

Komentář Práce je psaná odborným stylem obvyklým pro tento typ práce a splňuje všechny formální náležitosti. Text je srozumitelný a neobsahuje zjevné gramatické ani stylistické chyby. V textu se vyskytuje jen několik překlepů a formálních prohřešků. Konkrétně:
Strana 11: "líče" místo "klíče", strana 19: "přijehorším" místo "přinejhorším", strana 21 "jejím" místo "jejich".
Obrázky v sekci 2.5.1 mají anglicky psané popisky.
Seznam zkratek není seřazený abecedně (v tomto případě nevadí, ale při větším počtu použitých zkratek by to ztěžovalo vyhledávání).
Stránka 5 i jinde: čárky na začátcích řádků u rovnic nevypadají hezky.
Stránky 34 - 39: některé obrázky nejsou v textu práce odkazované.

Tyto nedostatky však výrazně nesnižují čitelnost ani srozumitelnost textu práce.

Některé pasáže by snesly podrobnější vysvětlení, respektive upřesnění. Zejména:

Pořádně popsat motivaci: o co v práci jde a proč je zajímavé se o to snažit. Například v kapitole o celulárních automatech není žádná zmínka o možnostech využití v šifrování nebo o vlastnostech, které CA mají, a které by v šifrování mohly být výhodné. Motivace je zmíněná jen krátce v úvodní kapitole, ale zasluhovala by si víc prostoru.

Testování v kapitole 2.7: co přesně vlastně testujeme a jak? Bylo by vhodné ještě před kapitolou 2.7.1 jasně popsat, jaký algoritmus chceme testovat, co je jeho vstupem, co je jeho výstupem a jaké výstupy jsou považované za kvalitní a proč.
Algoritmus byl sice stručně popsaný v sekci 2.3, ale mezi kapitolami 2.3 a 2.7 bylo zmíněno několik dalších algoritmů, a není na první pohled zřejmé, který z nich se zde myslí.

Není jasné, jak přesně se používá 2D automat, například Amoeba universe. Kam přesně se píše počáteční zpráva a odkud se čte výsledek?

Autor se u některých výsledků snaží podat vysvětlení pozorovaných jevů, ale často je analýza výsledků pouze povrchní. Bylo by zajímavé aspoň u jednoho experimentu podrobně vysvětlit, co se v automatu děje a proč. Například: proč dává KeyExtenderSimpleQuadratic s automatem 110 špatné výsledky v testu Compress, ale dobré v ostatních testech. Bylo by také možné s výsledky experimentů dále pracovat a zjistit například, jestli existuje nějaká korelace mezi výsledky jednotlivých testovacích kritérii, a podobně.

U genetického algoritmu nejsou popsané žádné výsledky. Sice je zmíněný důvod - vysoké časové nároky provádění rozsáhlejších experimentů, ale bylo by vhodné aspoň některé výsledky zveřejnit, nebo slovně popsat.

Na některých místech jsou navržené postupy popsané jen slovně, přestože jsou poměrně složité. Slovní popis je sice správný a vyčerpávající, ale snazšímu pochopení by pomohly obrázky či ilustrační příklad.

Některé použité formulace nejsou příliš vhodné. Zejména:

strana 19: "diskuze na internetu naznačují.."
strana 5: "buňka uprostřed .. na neomezené ploše" chybí zde formální popis plochy, na které automat pracuje. Hodila by se i formální definice celulárního automatu obecně.

V kapitole 4, zejména na začátku, se zmiňuje mnoho technických detailů souvisejících s implementací. To se na tomto místě zdá zbytečné. Bylo by vhodnější všechny technické detaily popsat na jednom místě (například v kapitole 3) a poté se v kapitole 4 už věnovat pouze abstraktnímu popisu použitých procesů a případně experimentů a výsledků.

I přes výše zmíněné drobné nedostatky je textová část práce celkově na dobré úrovni, má vhodnou strukturu a i kvalita dokumentace odpovídá požadovaným standardům.

Implementační část práce	lepší	OK	horší	nevyhovuje
Kvalita návrhu *... architektura, struktury a algoritmy, použité technologie*	☒	☒	☐	☐
Kvalita zpracování *... jmenné konvence, formátování, komentáře, testování*	☒	☐	☐	☐
Stabilita implementace	☐	☒	☐	☐

Komentář Implementační část je celkově kvalitní a značně rozsáhlá, zvláště s přihlédnutím k tomu, že implementační činnost nebyla stěžejní náplní práce. Zdrojové kódy jsou dobře strukturované, při návrhu jsou vhodným způsobem používány návrhové vzory, kód je bohatě komentovaný a je psaný s využitím doporučených postupů a konvencí. Výjimkou je pouze metoda Totalistic2DAutomaton.Step(), která by zasluhovala rozdělení na několik menších metod, což by zlepšilo její čitelnost.

Pro reprezentaci funkcionality různých typů celulárních automatů je vhodným způsobem využitá hierarchie tříd a rozhraní, což zlepšuje přehlednost kódu. Bylo by přínosné podobnou hierarchii navrhnout i pro reprezentaci jednotlivých testovacích kritérií, aby bylo možné k testování a vyhodnocování výsledků přistupovat jednotně.

Co se týče experimentů: není příliš dobře popsané, jak dlouho se tyto experimenty prováděly a jaké přesně experimenty vůbec byly provedené. Dá se totiž tušit, že autor provedl daleko větší množství experimentů (například s více druhy automatů) a poté zveřejnil jen některé z výsledků. Zajímavá by byla také informace o tom, kolik výpočetního času celkem experimenty zabraly.

Drobné výhrady mám k některým jmenným konvencím. Například to, proč se KeyExtenderQuadratic jmenuje "Quadratic", se dozvídáme až na konci popisu a tímto důvodem je jeho kvadratická složitost. Vhodnější by bylo v názvech zohledňovat spíše náplň činnosti, kterou příslušná třída zajišťuje, než její složitost. Podobně například název KeyExtenderUncertain by mohl být zvolený lépe.

Celkové hodnocení Výborně
Práci navrhuji na zvláštní ocenění Ne

Datum 20.1.2017 **Podpis**