Prof. dr hab. Marcin Szpyrka
Akademia Górniczo-Hutnicza
Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej
Katedra Informatyki Stosowanej
Al. Mickiewicza 30, 30-059 Kraków
tel.: 012 617 51 94
e-mail: mszpyrka@agh.edu.pl

Kraków, 10 lipca 2017 r.

Recenzja rozprawy doktorskiej mgr. inż. Agnieszki Zbrzezny pt. *Wybrane metody weryfikacji modelowej wykorzystujące testery SAT i SMT*

Rozprawa doktorska została opracowana w Instytucie Podstaw Informatyki Polskiej Akademii Nauk.

1. Cel i zakres rozprawy

Rozprawa doktorska mgr. inż. Agnieszki Zbrzezny dotyczy problemu opracowania nowych bazujących na testerach SAT i SMT algorytmów ograniczonej weryfikacji modelowej dla systemów współbieżnych, w tym systemów czasu rzeczywistego i systemów wieloagentowych. Ponadto w pracy wiele miejsca poświęcono problemowi porównania algorytmów bazujących na testerach SAT z ich odpowiednikami bazującymi na testerach SMT, w celu wskazania najbardziej wydajnych rozwiązań dla danej grupy systemów współbieżnych.
Praca ma charakter erudycyjny i bazuje na wysoce sformalizowanym aparacie logicznym i metalogicznym, odnoszącym się do pewnych egzystencjalnych rozszerzeń LTL, CTL lub CTL*. Model analizowanego systemu przedstawiany jest z użyciem struktur Kripkego i ich rozszerzeń lub systemów interpretowanych i ich rozszerzeń. Teza pracy nie została jawnie określona lecz przedstawiona jako ww cele do zrealizowania.

2. Struktura i zawartość rozprawy

Opiniowana rozprawa doktorska została przygotowana w języku polskim. Praca składa się z sześciu rozdziałów wliczając w to wstęp i podsumowanie. Zawiera ponadto streszczenie w języku polskim i angielskim, spis rysunków, spis tablic, indeks haseł oraz wykaz literatury. Praca liczy łącznie 187 stron. Wspomniany wykaz literatury zawiera łącznie 110 pozycji. Do rozprawy została dołączona płyta DVD, która zawiera elektroniczną wersję rozprawy doktorskiej wraz ze skryptami, które wykorzystano do realizacji przedstawionych w rozprawie testów.

- Rozdział 1 zawiera wprowadzenie do problematyki pracy, w szczególności przedstawiono w nim w zarysie główne wyniki rozprawy. Pewien niedosyt budzi brak jawnie określonej tezy rozprawy.
- Rozdział 2 zawiera opis wybranych pojęć związanych z problematyką weryfikacji modelowej. Zawarto w nim m.in. definicję systemu tranzycyjnego, składnię i semantykę logiki ECTL* (egzystencjalny fragment logiki CTL*), krótkie wprowadzenie do problemu ograniczonej weryfikacji modelowej oraz przegląd wybranych narzędzi do weryfikacji modelowej. Nie do końca

jasny jest cel ulokowania w tym rozdziale opisu logiki ECTL*. W kolejnych rozdziałach podawana jest logika temporalna, na której aktualnie skupia się autorka.

- Rozdział 3 poświęcono tematyce weryfikacji systemów współbieżnych. Rozdział rozpoczyna się od wprowadzenia logiki RTECTL (egzystencjalny fragment logiki RTCTL – Real-Time CTL). W logice tej semantyka operatorów U (until) i G (globally) definiowana jest dla określonego przedziału w zbiorze liczb naturalnych $\mathbb{N}$. Rozdział zawiera opis translacji formuł logiki RTECTL do formuł logiki ECTL (przy czym w pracy nie podano składni i semantyki dla logiki ECTL) oraz porównanie czasu realizacji obliczeń i zajętości pamięci w przypadku weryfikacji prawdziwości formuł RTECTL i ich odpowiedników w ECTL.

  Drugą część rozdziału poświęcono problemowi ograniczonej weryfikacji modelowej bazującej na testerach SMT dla logiki ECTL*. Zamieszczono w nim semantykę ograniczonej logiki ECTL*, metodę translacji formuł ECTL* do bezkwantyfikatorowej formuły pierwszego rzędu oraz wyniki eksperymentów porównującej wydajność nowej metody z wcześniejszymi rozwiązaniami.

- W rozdziale 4 przedstawiono metodę ograniczonej weryfikacji modelowej dla dyskretnych automatów czasowych i własności wyrażanych w logice EMTL. Rozdział zawiera opis: automatów czasowych, składni i semantyki logik EMTL (metryczny ELTL) i ELTL$_q$, translacji z EMTL do ELTL$_q$, translacji formuł ELTL$_q$ do problemu SAT i wyników eksperymentów obliczeniowych. W mojej ocenie rozdział ten można było całkowicie pominąć bez straty dla końcowej oceny rozprawy doktorskiej.

- Rozdział 5 swoją objętością zajmuje ponad połowę rozprawy doktorskiej. Poświęcono go problemom weryfikacji modelowej systemów wieloagantowych. Rozdział rozpoczyna się od wprowadzenia kilku wersji systemów interpretowanych (wagowy, czasowy, wagowo-czasowy), które w dalszej części rozdziału są używane do modelowania weryfikowanych systemów. Następnie przedstawiono logiki temporalne stosowane w tym rozdziale do opisywania własności systemów: WECTLK (ważony ECTLK), WELTLK (ważony ELTLK) i EMTLK (metryczny ELTLK).

  Główną część rozdziału stanowi opis metod ograniczonej weryfikacji modelowej dla systemów wieloagantowych. Schemat opisu rozwiązań jest następujący: wskazanie typu systemów interpretowanych i logiki temporalnej, której dotyczy dana sekcja, opis semantyki ograniczonej, przedstawienie translacji formuły do problemu SMT i SAT oraz eksperymentalne porównanie metod.

- Rozdział 6 zawiera krótkie podsumowanie rozprawy oraz pewne sugestie prac badawczych mających być jej kontynuacją.

Prezentacja materiału przedstawionego w pracy dokonana jest w sposób relatywnie poprawny z językowego punktu widzenia. W pracy trafiają się literówki i drobne błędy stylistyczne. W kilku miejscach przy wypunktowaniach po kropce używane są małe litery. Inne uwagi techniczno-redakcyjne przedstawiono w dalszej części recenzji.
Pewną dostrzegalną wadą pracy natury redakcyjno-merytorycznej jest (być może zamierzona) lapidarność definicyjna, utrudniająca lub uniemożliwiająca miejscami pełną weryfikację stwierdzeń i tez autorki pracy. Praca sprawia w tych miejscach wrażenie raczej pewnego *przewodnika* po pracach i wynikach autorki, zamieszczonych gdzie indziej, niż rozprawy niezależnej od tych prac.
W mojej ocenie całą rozprawę doktorską można było zbudować bazując wyłącznie na wynikach przedstawionych w rozdziale 5. W efekcie uzyskalibyśmy zdecydowanie bardziej spójne przedstawienie wartościowych wyników badań, ale pozbawione nadmiaru symboli i rozważanych logik temporalnych i formalnych metod opisu systemów informatycznych.

3. Ocena rozprawy

Praca podejmuje tematy naukowo aktualne i kluczowe dla informatyki teoretycznej, takie jak dyskutowana w niej taksonomia metod i narzędzi dla problemu SAT i SMT. Niewątpliwą zaletą rozprawy jest *eksperymentalna analiza komparatystyczna* zastosowanych metod weryfikacji. Godna podziwu jest szczegółowość, czy też stopień analityczności podejmowanych w pracy rozważań, przekraczający typowe standardy stawiane pracom z informatyki, nawet tym bardziej zmatematyzowanym. Warty podkreślenia jest znaczący dorobek publikacyjny autorki, na którym ta praca bazuje.
Do najistotniejszych osiągnięć przedstawionych w ocenianej rozprawie doktorskiej należy zaliczyć:

1. Zdefiniowanie i udowodnienie poprawności translacji z RTECTL do ECTL.

2. Opracowanie i implementacja metod ograniczonej weryfikacji modelowej dla rozważanych logik temporalnych i formalizmów (logika, formalizm, typ testera):

   a) RTECTL, TS, SMT
   b) ECTL, TS, SMT
   c) ECTL*, TS, SMT
   d) EMTL, DTA, SAT
   e) WECTLK, WIS, SMT
   f) WELTLK, WIS, SMT
   g) WECTLK, TWIS, SMT
   h) WECTLK, TWIS, SAT
   i) WELTLK, TWIS, SMT
   j) WELTLK, TWIS, SAT
   k) EMTLK, TIS, SMT
   l) EMTLK, TIS, SAT

3. Przeprowadzenie licznych testów z użyciem SMT i SAT-testerów, które wstępnie pozwalają ocenić skuteczność zaproponowanych metod lub pozwalają wybrać bardziej wydajne rozwiązanie dla danej konfiguracji: (logika, formalizm).

3.1. Uwagi ogólne

1. W rozprawie stosowanych jest szereg skrótów oznaczających stosowane przez autorkę logiki temporalne. Przy pierwszym użyciu takich skrótów powinno się podać pełną nazwę stosowanej logiki.

2. W rozdziale 3 nie podano składni i semantyki logiki ECTL. Krótka uwaga w rozdziale 2, że jest to podzbiór logiki ECTL* nie jest wystarczająca, biorąc pod uwagę istotne różnice składniowe między logikami CTL i CTL*.

3. Rozprawa doktorska jest wysoce sformalizowana, zawiera bardzo dużą liczbę oznaczeń, a kolejne rozdziały charakteryzują się zmianą kontekstu w sensie typu rozważanych logik, czy też formalizmów stosowanych do modelowania. Autorka rozprawy bardzo często pozostawia złożone formalne definicje bez jakiegokolwiek komentarza. To powoduje, że rozprawa pozostaje słabo czytelna (zwłaszcza dla mniej wprawnego czytelnika). Klasycznymi przykładami są: opis translacji z RTECTL do ECTL (strony 29–30), prezentacja stwierdzeń 1–4 na stronie 31, definicja 9 (str. 41) itd.

4. Przedstawione w rozprawie translacje do SMT nie są opisane w pełni. Rozważmy dla przykładu translację opisaną w sekcji 3.3.2. Czytelnik nie wie jak zaimplementowane są funkcje $p(\overline{\mathbf{w}})$, $I_s(\overline{\mathbf{w}})$, $\mathcal{T}(\overline{\mathbf{w}}, \overline{\mathbf{w}}')$, h_k^{U} itd. Uniemożliwia to np. ocenę poprawności definicji 9 (w której ponadto używany jest niezdefiniowany symbol A).

   Analogiczna sytuacja występuje w rozdziale 4 i 5.

5. Wprowadzając logiki do opisu własności systemów wieloagentowych, autorka konsekwencje unika wyjaśnienia znaczenia niektórych operatorów, pozostawiając czytelnikowi wyłącznie dalece nieintuicyjne definicje formalne. Szczególnym przypadkiem jest tutaj unikanie jakiegokolwiek opisu znaczenia operatora $\overline{K}$.

3.2. Uwagi szczegółowe

1. Str. 20 – Użycie symbolu $\pi[j..]$ do oznaczenia sufiksu zwiększyłoby czytelność pracy i byłoby to spójne ze stosowanym oznaczeniem prefiksu.

2. Str. 21 – W definicji operatora Release powinna być koniunkcja, a nie alternatywa: $\varphi \mathsf{R} \psi = \mathsf{G}\psi \vee \psi \mathsf{U}(\varphi \wedge \psi)$.

3. Str. 22 – W definicji brakuje określenia semantyki dla $\neg p$.

4. Str. 34 – Warto byłoby dodać wprost – dla jasności opisu – że dowód Twierdzenia 1 dla translacji z RTECTL do ECTL jest koniunkcją dowodów Lematu 1 oraz Lematu 2. Czytelnik po lekturze dowodu Lematu 2 może wciąż oczekiwać dowodu samego Twierdzenia 1, dowiedziawszy się wcześniej jedynie, że do dowodu twierdzenia potrzebny jest Lemat 1.

5. Str. 39 – W Definicji 7 nie jest wyjaśnione czym jest l. Z tekstu po definicji można się domyślać, że wskazuje indeks stanu, w którym rozpoczyna się pętla. Jaką rolę pełni l, jeżeli k-ścieżka nie jest pętlą?

6. Str. 40 – Pojęcie *semantyka przeplotowa* nie jest zdefiniowane w rozprawie.

7. Str. 41 – W Definicji 9 nie jest wyjaśnione czym jest zbiór A.

8. Str. 42 – Nie jest jasne z jakimi implementacjami bazującymi na SAT i SMT porównywane jest opisane w rozdziale rozwiązanie.

9. Str. 44 – Przedostatni akapit jest niekompletny. Brak jest wniosków ze zrealizowanych testów.

10. Str. 49 – Warto byłoby wyjaśnić sens nazwy *metryczny* ELTL.

11. Str. 53 – Twierdzenie 4 Dowód jest zbyt lapidarny. Nie o końca wiadomo, jak uzyskać tezę twierdzenia, zwłaszcza, że *słabo-czasowo-bisymulacyjna równoważność modeli* (jako pojęcie dalece nieelementarne z teorii modeli), nie zostało wcześniej zdefiniowane.

12. Str. 54 – Zdanie: „Problem egzystencjalnej weryfikacji modelowej pyta, czy $\widehat{\mathcal{M}} \vdash \mathsf{E}\psi$" powinno brzmieć inaczej, np. „Problem ezystencjalnej weryfikacji to pytanie, czy…" lub podobnie.

13. Str. 60 – Znów nie do końca jasne, w jaki sposób teza Twierdzenia 6 wynika *bezpośrednio* z Lematu 5 oraz Lematu 6.

14. Str. 70 – Początek podrozdziału 5.1 jest bardzo ciekawy, ale doktorat (nawet z teorii literatury) nie jest pamiętnikiem i osobiste wspomnienia, nawet jeśli wydają się sugestywne, nie powinny się tu znaleźć.

15. Str. 72 – Niejasne jest użycie nawiasów klamrowych w definicji systemu interpretowanego. Czy to nie powinny być krotki $(L_{\mathbf{i}}, Act_{\mathbf{i}}, P_{\mathbf{i}}, \mathcal{V}_{\mathbf{i}})$?

16. Str. 73 – W Definicji 21 brakuje „dla pewnego $\widetilde{a}_i \in Act$."

17. Str. 77 – Przy definicji $\mathcal{X}_{\mathbf{i}}$ brak jest informacji, że są to zegary agenta $\mathbf{i}$.

18. Str. 84 – Brak rozwinięcia skrótu WECTLK.

19. Str. 85 – W opisie semantyki logiki WECTLK nie jest wyjaśnione czym jest P.

20. Str. 86 – Brak rozwinięcia skrótu WELTLK.

21. Str. 88 – Co oznacza „EMTL4.2"?

22. Str. 96 – Dopiero w tym miejscu pojawia się przykład kodowania formuły dla SMT-testera. Szkoda, że podobne przykłady nie zostały zamieszczone we wcześniejszych rozdziałach.

23. Str. 109 – Sufiks jest tutaj oznaczany za pomocą symbolu $\rho[m..k]$. Wybrane tutaj oznaczenie wskazuje, że uwaga do str. 20 była zasadna.

24. Str. 157 – Być może lepszym miejscem na opis logiki ELTL$_q$K jest podrozdział 5.3.

25. Str. 165 – W przypadku wskazania podobieństwa dowodu, do dowodów zamieszczonych w literaturze, należałoby choć w zarysie przedstawić ideę takiego dowodu.

3.3. Uwagi techniczno-redakcyjne

Pod względem edytorskim oceniana rozprawa doktorska lokuje się zdecydowanie powyżej przeciętnej. Została dość starannie złożona z użyciem systemu składu LaTeX. Tym niemniej autorka nie ustrzegła się kilku „typowych" błędów, np.: używanie dwukropka zamiast polecenia `\colon` (np. przy definiownaiu funkcji), brak stosowania polecenia `\mathit{}` wokół wieloliterowych nazw w trybie matematycznym, symbol zbioru liczb naturalnych powinien być generowany z użyciem `\mathbb{N}` itp.

4. Wniosek końcowy

Przedstawiona w pracy problematyka dotyczy aktualnych i interesujących zagadnień naukowych związanych z problemem ograniczonej weryfikacji modelowej dla systemów współbieżnych, w tym systemów czasu rzeczywistego i systemów wieloagentowych. Rozprawa doktorska zawiera szereg interesujących oryginalnych wyników pracy badawczej autorki. Mimo przedstawionych wcześniej uwag krytycznych, rozprawę doktorską jako całość oceniam pozytywnie.

Biorąc pod uwagę opinie i uwagi zaprezentowane w poprzednich punktach oraz wymagania zdefiniowane przez artykuł 13 Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym (z późniejszymi zmianami, tekst jednolity Dz. U. z 2016 r. poz. 882, 1311), moja ocena rozprawy pod względem trzech podstawowych kryteriów jest następująca:

A. Czy rozprawa zawiera oryginalne rozwiązanie problem naukowego?

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

B. Czy po przeczytaniu rozprawy zgadzasz się, że kandydat posiada ogólną wiedzę teoretyczną w dyscyplinie?

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

C. Czy kandydat posiada umiejętność samodzielnego prowadzenia pracy naukowej?

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

Podsumowując, stwierdzam, że recenzowana rozprawa doktorska pt. *Wybrane metody weryfikacji modelowej wykorzystujące testery SAT i SMT* spełnia wymagania stawiane rozprawom doktorskim i wnoszę o dopuszczenie mgr. inż. Agnieszki Zbrzezny do dalszych etapów przewodu doktorskiego.