Prof. dr hab. inż. Jan Magott
Katedra Informatyki Technicznej
Wydział Elektroniki
Politechniki Wrocławskiej

Wrocław, 10.01.2016

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA INSTYTUTU PODSTAW INFORMATYKI
POLSKIEJ AKADEMII NAUK
w Warszawie

Tytuł rozprawy: „Parametryczna weryfikacja modelowa"

Autor rozprawy: mgr Michał Knapik

1. Jaki jest cel rozprawy i czy został on trafnie i jasno sformułowany?

Synteza parametrów ma na celu wyznaczenie wszystkich lub części takich wartościowań parametrów, dla których zachowanie modelu jest zgodne ze specyfikacją. Celem rozprawy było opracowanie teorii syntezy parametrów dla wybranych metod specyfikacji wymagań oraz weryfikacja praktycznej stosowalności tej teorii. Doktorant podjął się syntezy parametrów dla modeli z czasem dyskretnym i z czasem ciągłym.

W coraz większym stopniu wytwarzanie oprogramowania oparte jest na modelowaniu. Modelowanie ma szczególne znaczenie w początkowych fazach cyklu życia oprogramowania systemów związanych z bezpieczeństwem w znaczeniach angielskich słów „Safety" i „Security". W tych fazach wiele elementów projektu nie jest jeszcze określonych. Stąd uzasadnione jest badanie zakresu rozwiązań dopuszczalnych tzn. zgodnych ze specyfikacją wymagań funkcjonalnych, spośród których wybór będzie dokonany na podstawie kryteriów niefunkcjonalnych. Praca podejmuje problematykę syntezy zbiorów rozwiązań dopuszczalnych. Aby parametryczną weryfikację modelową można było efektywnie stosować niezbędne jest narzędzie programistyczne częściowo automatyzujące tę. Zatem cel naukowy został trafnie i jasno sformułowany.

2. Czy autor rozwiązał postawiony problem i czy użył do tego właściwych metod?

Na opracowanie teorii syntezy parametrów dla wybranych metod specyfikacji wymagań oraz weryfikację praktycznej stosowalności tej teorii dla modeli z czasem dyskretnym składają się następujące osiągnięcia:

- Algorytm syntezy parametrów i narzędzie programistyczne o nazwie SPATULA dla Parametrycznej Logiki Czasu Rozgałęzionego z Akcjami,
- Dwa algorytmy syntezy parametrów dla systemów agentowych specyfikowanych za pomocą Parametrycznej Logiki Czasu Rozgałęzionego z Wiedzą i Parametrycznej Logiki Czasu Alternującego,
- Rozbudowa narzędzia weryfikatora modelowego systemów wielo-agentowych MCMAS w kierunku syntezy parametrów,
- Analiza teoretycznej złożoności obliczeniowej powyższych trzech algorytmów poprzez wyznaczenie górnego ograniczenia złożoności czasowej,

- Badanie eksperymentalne praktycznej złożoności czasowej z uwzględnieniem czasu działania algorytmu, wymaganej pamięci, rozmiaru wynikowego binarnego drzewa decyzyjnego, liczby wartościowań.

Na opracowanie teorii syntezy parametrów dla problemu osiągalności stanu dla modeli z czasem ciągłym oraz weryfikację praktycznej stosowalności tej teorii składają się następujące osiągnięcia:

- Pojęcie Parametrycznego Grafu Regionów dla Parametrycznego Automatu Czasowego i relacje między ścieżkami (sekwencjami przejść) w Grafie i Automacie,
- Dla Parametrycznego Automatu Czasowego z Dolnym albo Górnym Ograniczeniem, opracowanie teorii i na jej podstawie translatora Problemu Parametrycznej Osiągalności Stanu o zadanej formule stanowej do Problemu Syntezy Modeli Bezkwantyfikatorowej Arytmetyki Liniowej.

Zatem recenzent stwierdza, że Doktorant osiągnął sformułowany cel i użył do tego właściwych metod.

3. Czy tematyka rozprawy jest aktualna i dostatecznie ważna?

Opracowanie metod projektowania i implementacji systemów informatycznych czy sterowania spełniających wymagania funkcjonalne, dodatkowo pod warunkiem spełnienia wymagań niefunkcjonalnych jest fundamentalnym zagadnieniem inżynierii systemów. Nierzadko specyfikacja systemu, niekompletna na początkowych etapach procesu wytwarzania jest uzupełniania równolegle z tym procesem. Model systemu w budowie jest niekompletny. Stąd w procesie wytwarzania, niektóre parametry specyfikacji i modelu mogą być określone precyzyjnie, natomiast dla innych znane mogą być tylko zakresy ich wartości. Weryfikacja formalna jest szczególnie ważna w przypadku systemów z wymaganiami na bezpieczeństwo oraz mechanizmów współpracy procesów współbieżnych. Takie systemy są często zbyt skomplikowane aby analiza ich modeli mogła być przeprowadzana tylko przez człowieka na papierze. Potrzebne są metody analizy i programy komputerowe umożliwiające weryfikację zachowania systemów często o bardzo złożonych przestrzeniach stanów, w celu weryfikacji projektu czy implementacji względem wymagań. Stąd tematyka rozprawy jest aktualna i dostatecznie ważna jako tematyka dysertacji doktorskiej.

4. Na czym polega oryginalny dorobek Autora i jakie jest jego znaczenie poznawcze lub przydatność praktyczna dla nauki bądź techniki?

Bardzo dobre wrażenie robi rozległość tematyki badawczej podjętej przez Autora. Podjął się on parametrycznej weryfikacji modelowej systemów z czasem dyskretnym i ciągłym. Zakres uzyskanych oryginalnych wyników jest większy dla systemów z czasem ciągłym ze względu na ograniczenia rozstrzygalności problemów parametrycznej weryfikacji modelowej systemów z czasem ciągłym. Wśród systemów z czasem dyskretnym podjął badania systemów z przejściami etykietowanymi akcjami jak i systemów agentowych Wśród systemów agentowych analizował problematykę indywidualnej i grupowej wiedzy, ale również strategie współpracy agentów. Rozważał trzy kategorie wiedzy grupowej. Doktorant bardzo efektywnie spożytkował szanse rozwoju w dwu szkołach naukowych Prof. Wojciecha Penczka i Prof. Alessio Lomuscio.

Najważniejszymi oryginalnymi rezultatami uzyskanymi przez mgra Knapika w ramach modeli czasu dyskretnego są trzy twierdzenia dowodzące poprawności algorytmów syntezy dla trzech logik. Każde z tych twierdzeń jest podsumowaniem kilku lematów dowodzących własności procedur wchodzących w skład tych algorytmów.

Kolejnym znaczącym wynikiem są: nowe narzędzie programistyczne SPATULA do syntezy parametrów modeli Kripkego z akcjami i dobudowana do narzędzia MCMAS część służąca syntezie parametrów dla systemów agentowych.

W obszarze modeli z czasem ciągłym, problem syntezy parametrycznej jest nierozstrzygalny. Dwa uzyskane przez Autora częściowe rozwiązania tego problemu są wartościowymi rezultatami.

Przydatność metod w naukach technicznych zweryfikowano poprzez analizę wielu przykładów praktycznych zaczerpniętych głównie z informatyki. Przykłady charakteryzują się bardzo wysokimi wymaganiami ich poprawności co wymaga weryfikacji modelowej.

Podsumowując recenzent stwierdza, że Autor opracował metody i moduły programowe umożliwiające częściową automatyzację parametrycznej weryfikacji systemów.

Wszystkie dziewięć publikacji Doktoranta jest współautorskimi, jednak zasadnicze wyniki pracy doktorskiej pochodzą z publikacji, których jest autorem wiodącym. Jeden artykuł został opublikowany w czasopiśmie ACM Transactions on Embedded Computing Systems, które jest na tzw. liście filadelfijskiej. Dwie w podserii Transactions on Petri Nets and Other Models of Concurrency w ramach serii Lecture Notes in Computer Science. Pozostałe publikacje zostały wydane w materiałach prestiżowych konferencji.

5. Czy rozprawa świadczy o dostatecznej wiedzy Autora i znajomości współczesnej literatury z dyscypliny naukowej, której dotyczy?

Bibliografia rozprawy zawiera 116 pozycji, z których Doktorant jest współautorem 10 prac, 9 publikacji i jednego raportu, oraz autorem dwu narzędzi programistycznych do syntezy parametrów badanych przez niego modeli systemów. Mgr Michał Knapik wykazał się szeroką wiedzą w obszarach: formalnych metod weryfikacji modelowej systemów z dyskretnym i ciągłym czasem. Stworzone implementacje dowodzą zaawansowanych umiejętności programistycznych Autora.

6. Jakie są wady i słabe strony rozprawy oraz pytania ze strony recenzenta?

Przyśpieszenie w syntezie parametrów dla parametrycznej Logiki Czasu Rozgałęzionego z Akcjami wykonywanej z użyciem narzędzia SPATULA względem algorytmu siłowego w jednym z badanych przykładów sięga nawet 8.000. Jednak w innym przypadku, narzędzie SPATULA wymaga większego czasu działania niż podejście siłowe. Problematyka badana poprzez Classen'a i współpracowników w pracy *Symbolic model checking of software product lines* jest analogiczna. Ich metoda daje przyśpieszenie do około 800. Autor nie porównał swojej metody oraz podejścia Classen'a i współpracowników. Zatem pytanie:

Czy Autor jest w stanie porównać te dwie metody?

W teorii systemów dynamicznych o zdarzeniach dyskretnych istnieje pojęcie sterowania z nadzorem (ang. supervisory control) wprowadzone przez Ramadge'a i Wonham'a. W tym modelu analizowane są przejścia sterowane i niesterowane, przejścia obserwowalne i nieobserwowalne. Autor nie wspomniał o tym podobnym a bardzo szerokim obszarze badawczym. Stąd pytanie do Autora:

Czy opracowane przez Doktoranta podejście dla parametrycznej Logiki Czasu Rozgałęzionego z Akcjami można po modyfikacjach zastosować również w tym przypadku?

Praktyczna czasowa złożoność obliczeniowa badana jest poprzez zwiększanie liczby elementów o tym samym modelu. W praktyce, np. w automatycznym sterowaniu ruchem kolejowym, często elementy nie są identyczne, np. przełączniki między torami, po których jeżdżą pociągi. Automatyczne sterowanie ruchem kolejowym jest jednym z obszarów zastosowań logiki temporalnej. Trudności rozwiązania problemu sterowania ruchem

kolejowym wynikają ze złożoności obliczeniowej. Jednym z przykładów badanych przez Doktoranta jest sterowanie dostępem pociągów, z których jeden jest uszkodzony, do tunelu, w którym może być co najwyżej jeden pociąg. Przewaga metody Autora nad podejściem siłowym jest w tym przypadku bardzo duża. Stąd pytanie do Doktoranta:

Czy parametryczna weryfikacja modelowa może być drogą do uzyskania metody weryfikacji projektów sterowania ruchem kolejowym względnie efektywnej obliczeniowo?

Specjaliści od sterowania ruchem kolejowym operują graficzną reprezentacją torów kolejowych z przełącznikami inną niż model Kripke'go. Zatem kolejne pytanie skierowane do Autora brzmi:

Czy można zbudować względnie efektywny syntezator, którego interfejs byłby dopasowany do sposobu postrzegania eksperta sterowania ruchem kolejowym, ale synteza byłaby wykonywana z użyciem Parametrycznej Logiki Czasu Rozgałęzionego z Akcjami?

Doktorant nie przeanalizował teoretycznej złożoności obliczeniowej Algorytmu 15. syntezy parametrów dla Parametrycznego Automatu Czasowego z Dolnym albo Górnym Ograniczeniem. Algorytm ten korzysta z narzędzi typu SMT-solver, które zwykle bazują na metodzie Simpleksów. Metoda ta ma złożoność czasową wykładniczą. Istnieją wielomianowe algorytmy programowania liniowego np. algorytm Karmarkar'a. Zatem następne pytanie kierowane do Doktoranta brzmi:

Czy dla proponowanego przez Autora algorytmu częściowej syntezy parametrów można zbudować algorytm wielomianowy?

Uwagi szczegółowe

Str. 19, Definicja 2.1.3 Symbol zbioru akcji jest niepotrzebny.

Str. 19, akapit na temat rozmiaru formuł Zamiast $E(\phi U\psi)$ powinno być $|\, E(\phi U\psi \,|$.

Str. 20, 6g Powinno być $[\![\phi \vee \psi]\!]=[\![\phi]\!] \cup [\![\psi]\!]$. Linia od góry.

Str. 21, wyrażenie (2.10) Zamiast G powinno być H.

Str. 26, przykład 2.3.2 Obie formuły ϕ mają tę samą postać.

Str. 29, wyrażenie (2.20) Symbolu ω nie powinno być.

Str. 31, 6d Powinno być „equivalence 2.4".

Str. 36, 3d Zamiast st_n+1 powinno być st_1.

Str. 46, Tabela 2.1 Jedno z przyśpieszeń podano z pięcioma cyframi po przecinku.

Str. 46, Rys. 2.12 W jaki sposób synchronizowane są akcje *ret* wobec ich różnych dolnych indeksów?

Str. 50, trzeci akapit Przeciwdziedzina funkcji τ_e jest L_e.

Powyższe pytania i uwagi szczegółowe nie podważają wysokiej oceny pracy.

Sformalizowana postać dysertacji sprzyja popełnianiu błędów formalnych, których recenzent zauważył niewiele, co jest rezultatem wysokiej kultury matematycznej Doktoranta.

7. Wniosek końcowy

Rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego. Doktorant wykazał się umiejętnością samodzielnego rozwiązywania problemów naukowych w dyscyplinie Informatyka oraz dużą wiedzą praktyczną. Przedstawione uwagi dyskusyjne czy krytyczne nie mają znaczącego wpływu na pozytywną ocenę rozprawy, która zdaniem recenzenta z dużym nadmiarem przekracza wymagania stawiane pracom doktorskim. Biorąc pod uwagę powyższe fakty, stwierdzam, że recenzowana rozprawa w pełni spełnia wymagania Ustawy o Stopniach Naukowych i Tytule Naukowym i wnoszę o dopuszczenie jej do publicznej obrony.