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

Wrocław, 09.09.2017

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

Tytuł rozprawy:
„Wybrane metody weryfikacji modelowej wykorzystujące testery SAT i SMT"

Autor rozprawy: mgr Agnieszka Zbrzezny

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

Celem przygotowanej rozprawy było opracowanie nowych metod ograniczonej weryfikacji modelowej bazujących na testerach SAT i SMT do analizy i weryfikacji systemów współbieżnych a w szczególności systemów: czasu rzeczywistego i agentowych. Celem było również porównanie wydajności metod opartych na testerach SMT z bazującymi na testerach SAT.

Rośnie zakres systemów informatycznych w sterowaniu systemami związanymi z bezpieczeństwem ludzi, środowiska, sprzętu, np. systemy sterowania elektrowniami jądrowymi, ruchem lotniczym i kolejowym. Coraz więcej informacji jest przechowywanych i przetwarzanych ze wsparciem informatycznym. Wymagana jest ochrona informacji zgodnie z prawami dostępu do niej. Takie systemy charakteryzują się współbieżnością, a są wśród tych systemy: czasu rzeczywistego i agentowe. Podstawowym środkiem weryfikacji oprogramowania jest nadal testowanie, które jednak nie może służyć dowodowi poprawności. Innym podejściem do weryfikacji oprogramowania i sprzętu systemów informatycznych i automatyki jest weryfikacja modelowa. Podstawowym celem tej weryfikacji jest wykrycie zachowań projektowanego systemu niezgodnych ze specyfikacją wymagań nałożonych na system. W ograniczonej weryfikacji modelowej, problem spełnialności własności wyrażonej formułą logiki temporalnej w systemie tranzycyjnym jest badany poprzez jego redukcję do formuły klasycznego rachunku zdań (SAT) lub do formuły SMT ogólniejszej z wybranymi zmiennymi boolowskimi zastąpionymi przez predykaty np. różnych arytmetyk ze względu na parametry liczbowe czasu czy wag systemów tranzycyjnych. Aby ograniczoną weryfikację modelową można było efektywnie stosować niezbędne jest narzędzia programistyczne częściowo automatyzujące tę. Stąd dla nowych metod wymagane jest dowodzenie ich poprawności oraz opracowanie wydajnych narzędzi programistycznych. W pracy wykonano wiele badań wydajności rozmaitych metod rozwiązywania problemów ograniczonej weryfikacji modelowej systemów współbieżnych, w tym systemów: czasu rzeczywistego i agentowych opartych na testerach SAT lub SMT. Zatem cel naukowy został trafnie i jasno sformułowany.

2. Czy Autorka rozwiązała postawiony problem i czy użyła do tego właściwych metod?

Na opracowanie nowych metod ograniczonej weryfikacji modelowej bazujących na testerach SAT i SMT dla systemów współbieżnych oraz na porównanie wydajności tych metod składają się następujące osiągnięcia.

- W zakresie systemów współbieżnych:
  - Zdefiniowanie poprawionej w stosunku do wcześniej zdefiniowanej przez innych autorów translacji formuł języka RTECTL do formuł języka ECTL i udowodnienie poprawności tej translacji,
  - Opracowanie i implementacja trzech metod ograniczonej weryfikacji modelowej opartych na testerze SMT dla systemów tranzycyjnych a własnościach wyrażonych w logikach:
    - ECTL*,
    - RTECTL,
    - ECTL,
  - Badania eksperymentalne czasu wykonania i wymaganej pamięci oraz porównanie tych wielkości dla trzech powyższych metod ograniczonej weryfikacji modelowej w wariantach opartych na testerach SMT oraz metod bazujących na testerach SAT na przykładach systemów tranzycyjnych: Uszkodzonego Systemu Kontroli Pociągów, Uogólnionego Paradygmatu Przetwarzania Potokowego, Ucztujących Filozofów względem formuł w językach RTECTL, ECTL i ECTL*.
- W obszarze systemów czasu rzeczywistego:
  - Opracowanie i implementacja opartej na testerze SAT metody ograniczonej weryfikacji modelowej dla dyskretnych automatów czasowych i własności wyrażanych w języku EMTL z językiem pośrednim $ELTL_q$ między EMTL a SAT,
  - Badania eksperymentalne czasu wykonania i wymaganej pamięci oraz porównanie tych wielkości dla powyższej metody z metodą opartą na testerze SAT z językiem pośrednim HLTL.
- W zakresie systemów agentowych:
  - Opracowanie i implementacja opartych na testerach SMT metod ograniczonej weryfikacji modelowej dla:
    - Wagowych systemów interpretowanych i własności specyfikowanych w logice WECTLK (egzystencjalnym fragmencie wagowej logiki temporalnej czasu rozgałęzionego z komponentami epistemicznymi),
    - Wagowych systemów interpretowanych i własności specyfikowanych w logice WELTLK (egzystencjalnym fragmencie wagowej logiki temporalnej czasu liniowego z komponentami epistemicznymi),
    - Czasowo-wagowych systemów interpretowanych i własności wyrażonych w logice WECTLK,
    - Czasowo-wagowych systemów interpretowanych i własności wyrażonych w logice WELTLK,
    - Czasowych systemów interpretowanych i własności specyfikowanych w logice EMTLK (egzystencjalnym fragmencie metrycznej logiki temporalnej czasu liniowego z komponentami epistemicznymi),
  - Opracowanie i implementacja opartych na testerach SAT metod ograniczonej weryfikacji modelowej dla trzech ostatnich z powyższych pięciu przypadków,
  - Badania eksperymentalne czasu wykonania i wymaganej pamięci oraz porównanie tych wielkości dla ośmiu powyższych metod ograniczonej weryfikacji modelowej w wariantach opartych na testerach SMT oraz na testerach SAT na przykładach systemów.

Zatem recenzent stwierdza, że Doktorantka osiągnęła sformułowany cel i użyła do tego właściwych metod.

3. Czy tematyka rozprawy jest aktualna i dostatecznie ważna?

Opracowanie metod projektowania i implementacji systemów przechowywania, przetwarzania i przesyłania informacji czy sterowania spełniających wymagania funkcjonalne, dodatkowo pod warunkiem spełnienia wymagań niefunkcjonalnych jest fundamentalnym zagadnieniem inżynierii systemów. Weryfikacja formalna jest szczególnie ważna w przypadku systemów z wymaganiami na bezpieczeństwo ludzi, środowiska czy informacji. Takie systemy współbieżne są często zbyt skomplikowane aby analiza ich modeli mogła być przeprowadzana tylko przez człowieka na papierze. W celu weryfikacji projektu czy implementacji względem wymagań, potrzebne są metody analizy i programy komputerowe umożliwiające weryfikację zachowania systemów często o bardzo złożonych przestrzeniach stanów. Przykład standardu IEEE Protokołu koherencji pamięci podręcznej Futurebus+ wskazuje na użyteczność metod formalnych. Wiele błędów wykryto dzięki weryfikacji modelowej dopiero po sześciu latach od rozpoczęcia prac nad tym protokołem. Stąd tematyka rozprawy jest aktualna i dostatecznie ważna jako tematyka dysertacji doktorskiej.

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

Problematyka badawcza podjęta przez Autorkę jest aktualna i ważna. Doktorantka, prezentując swoje wyniki, wskazuje na jakich pracach innych badaczy opierała się.

Przydatność praktyczną dla techniki stanowią następujące rezultaty:

- Opracowanie dwunastu metod weryfikacji modelowej opartych w większości na testerach SMT, ale również na testerach SAT i ich zaprogramowanie w języku C++. Efektem powyższego jest rozbudowa programowego weryfikatora VerICS modeli systemów o metody oparte na testerach SMT jak również SAT,
- Implementacja metody ograniczonej weryfikacji modelowej dla dyskretnych automatów czasowych i własności wyrażanych w języku EMTL tłumaczonym na języki pośredni $ELTL_q$, która jest znacznie efektywniejsza niż metoda bazująca na translacji z EMTL do HLTL,
- Wyniki badań eksperymentalnych wskazują jak dobierać metody ograniczonej weryfikacji modelowej do problemów.

Na znaczenie poznawcze dla nauki składają się:

- Zdefiniowanie i udowodnienie poprawności translacji RTECTL/ECTL, EMTL/$ELTL_q$,
- Szereg twierdzeń charakteryzujących własności opracowanych metod weryfikacji modelowej.

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

Na dysertację składają się m.in. wyniki zawarte w 13 publikacjach, z których w 11 przypadkach Pani Agnieszka Zbrzezny jest jedyną lub pierwszą autorką.

Ogółem, Doktorantka jest autorką bądź współautorką trzydziestu 30 prac, w tym w przypadku 6 jedynym autorem. Pani jest współautorką jednej publikacji w czasopiśmie Fundamenta Informaticae, które jest na tzw. liście filadelfijskiej oraz 8 publikacji wydanych w seriach LNCS i LNAI wydawnictwa Springer.

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

Bibliografia rozprawy zawiera 109 pozycji, z których Doktorantka jest autorką lub współautorką 24 prac. Mgr Agnieszka Zbrzezny wykazała się szeroką wiedzą w obszarze formalnych metod weryfikacji modelowej systemów informatycznych. Stworzone implementacje w języku C++ dowodzą zaawansowanych umiejętności programistycznych Autorki.

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

Określmy problem weryfikacji modelowej jako parę: system tranzycyjny, formuła logiki temporalnej. Istnieją problemy weryfikacji modelowej, które dla konkretnych kombinacji operatorów rachunku zdań, operatorów temporalnych i kwantyfikatorów ścieżkowych można rozwiązać w czasie wielomianowym. Metody ograniczonej weryfikacji modelowej oparte na SAT-testerach czy SMT-testerach są ogólnymi stosowalnymi do rozwiązywania problemów, które są NP-zupełnymi jak również problemów rozwiązywalnych w czasie wielomianowym. Jednak szczególnie istotna jest wydajność metod weryfikacji dla problemów NP-zupełnych. Stąd pytanie do Autorki:

Czy wszystkie z badanych w pracy problemów są NP-zupełnymi?

Istnieją takie testery SAT, np. GRASP, SATO, które nie wymagają wykładniczej pamięci w funkcji rozmiaru problemu. W badaniach wydajności dla Wagowego Problemu Transmisji Bitów (Rys. 5.18 i 5.20) uzyskano zależności wymaganej pamięci w funkcji rozmiaru problemu, które na podstawie grafiki podejrzewając, mogą być wykładnicze. Zatem pytania do Doktorantki:

Czy jest to wykładnicza zależność wymaganej pamięci w funkcji rozmiaru problemu? Jeśli tak, to z czego to wynika?

Doktorantka prowadziła badania wymaganych czasu i pamięci dla wybranych systemów współbieżnych o różnych rozmiarach i własnościach wyrażonych formułami logik temporalnych. Na tej podstawie budowała wnioski szczegółowe odnośnie doboru metod weryfikacji do różnych problemów ograniczonej weryfikacji modelowej.

Czy możliwe jest sformułowanie ogólniejszych reguł doboru metod do problemów weryfikacji modelowej? Czy reguły oparte na metrykach strukturalno-liczbowych systemów tranzycyjnych i metrykach strukturalnych formuł logiki temporalnej są jedynym kierunkiem badawczym?

Uwagi szczegółowe

Str. 28 W ostatnim akapicie zamiast $G_I\alpha$ powinno być $EG_I\alpha$.

Str. 28, 29, 35 W definicjach syntaktyki i semantyki logiki RTECTL brakuje podformuły $EF_I\varphi$, pomimo, że takie napisy występują w formułach φ_1, φ_2 na str. 35 dla Uszkodzonego Systemu Kontroli Pociągów. W każdej z formuł φ_1, φ_2 jest o jedną parę nawiasów za dużo. Jeśli *albo on albo inny* jest intuicyjną interpretacją alternatywy wykluczającej (ang. exclusive or) , to zapis formuły φ_2 i jej interpretacja są sprzeczne.

Str. 36, 37 W formułach φ_3, φ_4, $tr(\varphi_3)$, $tr(\varphi_4)$, zamiast zmiennej zdaniowej $Received$ powinna być $ConsReceived$. W przypadku formuły φ_3 jest niezgodność między operatorem rachunku zdań a intuicyjną interpretacją.

Str. 18, 29, 41 Na str. 29 symbol s^0 oznacza jedyny stan początkowy systemu tranzycyjnego, natomiast na str. 41 w kodzie rozwinięcia relacji przejścia systemu

tranzycyjnego, ten symbol oznacza zbiór stanów początkowych, który w definicji systemu tranzycyjnego na str. 18 oznaczony jest I.

Str. 41 W opisie translacji formuł języka ECTL* do problemu SMT nie podano znaczenia funkcji g^l, g^r, h_k^U, h_k^G, zbioru A.

Str. 43 W formule α_2, górna granica zmiennej j przy uogólnionym iloczynie logicznym powinna być równa $\lfloor n/2 \rfloor$-1. Autorka przekazała mi, że obliczenia wykonała dla właściwej postaci tego wyrażenia. Podana w tekście interpretacja tej formuły nie jest poprawna.

Str. 44 W drugim akapicie od dołu, ostatnie zdanie nie jest dokończone.

Str. 63 Interpretacja każdej z formuł $\varphi_0, \ldots, \varphi_5$ budzi zastrzeżenia.

Str. 75 Przykład 5.2.1 Waga akcji $Consume$ na Rys. 5.1 jest inna niż podana w opisie tego przykładu.

Str. 103, 105 i 106 Dla Wagowego Problemu Transmisji Bitów, w opisach w tekście do rysunków 5.7, 5.8 oraz podpisach pod tymi rysunkami, podano, że badana jest zależność wydajności od liczby węzłów, natomiast badana jest zależność od liczby bitów, jak podano na rysunkach.

Powyższe pytania i uwagi szczegółowe nie podważają wysokiej oceny pracy.

7. Wniosek końcowy

Rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego. Doktorantka wykazała się umiejętnością samodzielnego rozwiązywania problemów naukowych w dyscyplinie Informatyka. Przedstawione uwagi dyskusyjne czy krytyczne nie mają znaczącego wpływu na pozytywną ocenę rozprawy, która zdaniem recenzenta z 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.