Częstochowa, 17 sierpnia 2020

dr hab. Bożena Woźna-Szcześniak, prof. UJD
Uniwersytet Humanistyczno-Przyrodniczy
im. Jana Długosza w Częstochowie
ul. Waszyngtona 4/8, 42-200 Częstochowa

RECENZJA

rozprawy doktorskiej

Tytuł rozprawy: Zastosowanie paradygmatu funkcyjnego do formalnej analizy systemów modelowanych w języku Alvis

Autor rozprawy: mgr inż. Jerzy Biernacki

Recenzja wykonana jest na zlecenie Rady Dyscypliny Informatyki Technicznej i Telekomunikacji, Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie, pismo z dnia 14 lipca 2020r.

Recenzowana rozprawa doktorska napisana została pod kierunkiem promotora prof. dr hab. Marcina Szpyrki (Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej, AGH). Praca lokuje się w dyscyplinie informatyka techniczna i telekomunikacja.

1. *Cel, zakres i charakter rozprawy.*

   Rozprawa doktorska mgra Jerzego Biernackiego dotyczy metod formalnej weryfikacji modeli systemów współbieżnych oraz tych zależnych od czasu wyspecyfikowanych w języku *Alvis*.

   Automatyczna weryfikacja systemów, również tych zależnych od czasu, realizowana przez analizę modeli jest bardzo ważnym tematem badań naukowych. Wynika to z rosnącego zapotrzebowania na weryfikację systemów o krytycznym znaczeniu dla bezpieczeństwa, których awaria może powodować dramatyczne konsekwencje dla ludzi i urządzeń. Do takich systemów zaliczają się systemy sterowania ruchem kolejowym/tramwajowym/lotniczym, kontrolery hamulcowe, systemy planowania lotów i wiele innych.

   Problemem większości popularnych narzędzi do formalnej weryfikacji systemów współbieżnych oraz tych zależnych od czasu jest ich nieprzystępność dla przeciętnych inżynierów oprogramowania. Narzędzie *Alvis* stworzone zostało z myślą o formalnej specyfikacji i weryfikacji takich systemów, ale w sposób przystępny dla przeciętnych inżynierów oprogramowania. Oceniana rozprawa zawiera dwa nowe rozwiązania umożliwiające formalną weryfikację modeli w języku *Alvis* i w ten sposób istotnie przyczynia się do rozszerzenia dotychczasowych możliwości narzędzia *Alvis*.

   Formalna teza rozprawy jest jasno i precyzyjnie sformułowana przez Autora. Cytując Autora, brzmi następująco:

   > „Możliwe jest opracowanie skutecznych algorytmów formalnej weryfikacji własności systemów współbieżnych rozwijanych w języku *Alvis* z wykorzystaniem paradygmatu funkcyjnego i pośredniej reprezentacji modelu wyrażonej w języku *Haskell*."

Na poparcie swojej tezy Autor:

- opracował i zaimplementował metodę formalnej analizy modeli w języku *Alvis* na podstawie ich postaci pośredniej w języku *Haskell*. W tym, opracował i zaimplementował język zapytań *Alvis Query Language*, który umożliwia analizę modeli systemów zawierających powyżej 10^6 stanów przy zastosowaniu komputera klasy PC.
- opracował i zaimplementował algorytm translacji przestrzeni stanów modeli *Alvis* zapisanych w postaci grafu LTS do języka SMV. Translacja ta umożliwia weryfikację modeli *Alvis* przy pomocy narzędzia *nuXmv*.
- opracował czasowy i współbieżny model systemu *centrali sygnalizacji pożarowej* oraz model *zwrotnicy tramwajowej*, a następnie przeprowadził ich formalną weryfikację przy wykorzystaniu proponowanych podejść.
- opracował proces weryfikacji modeli *Alvis* wykorzystujący rozwiązania chmurowe i pokazał jego efektywność poprzez przeprowadzenie weryfikacji modeli wybranych systemów współbieżnych i czasowych (tj. skalowalnego systemu typu producent-konsument, zwrotnicy tramwajowej oraz centrali sygnalizacji pożarowej) na instancjach *Google Cloud Compute*.
- Przeprowadził wydajnościową analizę porównawczą zaproponowanych podejść.

Ponieważ rozprawa ma rozbudowaną stronę aplikacyjną i w zasadzie nie zawiera strony analitycznej, a wyniki opisane w pracy bazują na znajomości i umiejętności stosowania metod formalnych oraz wyspecjalizowanych języków programowania, pracę zaliczam do rozpraw o charakterze aplikacyjnym.

2. *Struktura i zawartość rozprawy.* Opiniowana rozprawa doktorska została przygotowana w języku polskim i składa się ze wstępu, sześciu rozdziałów, podsumowania oraz jednego dodatku. Zawiera ponadto stronę tytułową w językach polskim i angielskim, stronę z podziękowaniami, streszczenia w językach polskim i angielskim, spis treści oraz bibliografię. Praca liczy łącznie 118 stron. Bibliografia obejmuje 122 pozycje, w tym pozycje książkowe, artykuły w czasopismach naukowych oraz recenzowanych materiałach konferencyjnych, a także dokumentacje techniczne. Treść poszczególnych rozdziałów daje syntetyczny pogląd na przedstawioną w nich zawartość merytoryczną. W szczególności:

   - Rozdział 1 stanowi wstęp do rozprawy. Zawiera motywację do prowadzonych badań oraz cele i obszar badań.
   - Rozdział 2 zawiera opis podstawowych koncepcji języka *Alvis*, krótko charakteryzuje metody modelowania systemów czasowych i tych bez czasu w tym formalizmie, wprowadza grafy LTS jako reprezentację przestrzeni stanów generowanej przez model systemu zapisanego w języku *Alvis*. W rozdziale zawarto również krótki opis środowiska *Alvis* oraz porównano język *Alvis* z innymi formalizmami o podobnym zastosowaniu, takimi jak sieci Petriego, algebry procesów, automaty czasowe, Statechart, czy też PRISM.
   - Rozdział 3 przybliża ogólną koncepcję paradygmatu programowania funkcyjnego, opisuje zalety języka *Haskell* oraz sposób reprezentacji postaci pośredniej modelu *Alvis* w języku *Haskell*, ze szczególnym uwzględnieniem sposobu reprezentacji stanów i dynamiki modelu. W rozdziale zawarto również krótki opis sposobu generowania grafu LTS oraz wybrane opcje narzędzia *Alvis Compiler*.
   - Rozdział 4 wprowadza do problemu weryfikacji modelowej, formalnie definiuje systemy tranzycyjne jako klasę modeli służąca do reprezentacji zachowania systemów współbieżnych i czasowych oraz wprowadza syntaktykę i semantykę dla następujących języków formalnych, które służą do opisu własności weryfikowanego systemu: LTL, CTL, RTCTL oraz rachunek μ. W rozdziale zawarto również przegląd literatury dotyczący obszaru badań oraz dokonano przeglądu najnowszych narzędzi do weryfikacji modelowej pod kątem możliwości integracji z istniejącym pakietem narzędziowym Alvisa.

- Rozdział 5 zawiera opis pierwszego podejścia proponowanego przez autora rozprawy, które umożliwia automatyczną weryfikację modeli zapisanych w języku *Alvis*. Podejście to polega na wykonaniu automatycznej translacji grafu LTS do języka SMV, a następnie weryfikacji przy zastosowaniu narzędzia *nuXmv*. W szczególności, w pierwszym podrozdziale krótko wprowadzono podstawową strukturę języka SMV na przykładzie prostego systemu tranzycyjnego. Następnie opisano algorytm translacji grafu LTS do języka SMV wraz z narzędziem go implementującym o nazwie *Alvis2ModelChecker*. W kolejnym podrozdziale opisano studium przypadków weryfikacji modeli rzeczywistych systemów współbieżnych, w tym zwrotnicy tramwajowej oraz centrali sygnalizacji pożarowej. Na koniec przedstawiono podsumowanie wyników testów wydajnościowych zaproponowanego podejścia oraz podano uzasadniono, dlaczego to podejście nie pozwala na komputerze klasy PC weryfikować modeli, których liczba stanów przekracza 10^5.
- Rozdział 6 zawiera opis koncepcji chmur obliczeniowych oraz sposobu ich wykorzystania w procesie automatycznej weryfikacji modelowej systemów współbieżnych i czasowych reprezentowanych za pomocą modeli *Alvis*, a weryfikowanych przy pomocy narzędzia *nuXmv*. W rozdziale zawarto również wyniki testów zaproponowanego w Rozdziale 5 podejścia na instancji *Google Cloud Compute*. Analiza wyników wydajnościowych pokazała, że zastosowanie chmur obliczeniowych pozwala weryfikować systemy posiadające więcej niż 10^5 stanów, jak również potencjalnie nawet 10^6, jeżeli tylko wykorzystane zostaną odpowiednio mocne instancje.
- Rozdział 7 zawiera opis drugiego podejścia proponowanego przez autora rozprawy, które umożliwia automatyczną weryfikację modeli zapisanych w języku *Alvis*. Podejście to wykorzystuje pośrednią reprezentację modelu zapisaną przy pomocy języka funkcyjnego *Haskell*. Na wstępie rozdziału opisana została koncepcja funkcji filtrujących wraz z ich wadami, będących podstawowym sposobem wykorzystania warstwy pośredniej do weryfikacji modelu. Następnie wprowadzono proces weryfikacji modeli *Alvis* przy pomocy języka zapytań *Alvis Query Language* (AQL), będącego zestawem funkcji pozwalających na weryfikację wybranych właściwości modeli *Alvis*. Język został opracowany i zaimplementowany przez autora rozprawy. W szczególności rozdział zawiera szczegółowy opis zaimplementowanych nakładek na funkcje filtrujące wraz z ich deklaracjami i przykładami użycia. Rozdział zawiera również analizę testów wydajnościowych zaproponowanego rozwiązania na przykładach modeli wprowadzonych w Rozdziale 5. Ponadto w rozdziale pokazano, że zastosowanie paradygmatu programowania funkcyjnego do postaci pośredniej w języku *Haskell* umożliwiło weryfikację modeli *Alvis* o rozmiarze znacznie przekraczającym 10^6.

Prezentacja materiału przedstawionego w pracy dokonana jest w sposób relatywnie poprawny z językowego punktu widzenia. W pracy trafiają się literówki i drobne błędy gramatyczne oraz stylistyczne. Inne uwagi techniczno–redakcyjne przedstawiono w dalszej części recenzji.

3. *Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczący o dostatecznej wiedzy Autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?*

   Motywacja dla podjęcia tematu rozprawy wynikała z dobrze przeprowadzonej przez Autora analizy źródeł w zakresie automatycznej weryfikacji modelowej i narzędzi z nią związanych. Dzięki erudycji autora odzwierciedlony został w pełni aktualny stan wiedzy w zakresie narzędzi inżynierskich służących do automatycznej weryfikacji modelowej systemów współbieżnych i tych zależnych od czasu. Zabrakło może jedynie odniesienia do narzędzia MCMAS (`https://vas.doc.ic.ac.uk/software/mcmas/`), przy pomocy którego można weryfikować systemy współbieżne bez czasu.

   Przeprowadzona analiza źródeł świadczy o dość szerokiej wiedzy Autora, zaś sformułowane w sposób jasny i przekonywujący wnioski z tej analizy pozwoliły Autorowi do poprawnego zdefiniowania tezy rozprawy, wychodzącej naprzeciw rzeczywistemu zapotrzebowaniu w inżynierii oprogramowania na przyjazne w użytkowaniu narzędzia do automatycznej weryfikacji modelowej.

4. *Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek Autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?*

   Rozwiązując postawione w tezie rozprawy zadanie Autor uzyskał cztery główne nowe rezultaty, stanowiące jego samodzielny i oryginalny dorobek. Osiągnięcia te zawarto w rozdziałach od piątego do siódmego:

   - opracowanie i implementacja języka zapytań *Alvis Query Language* (AQL) umożliwiającego weryfikację modelu *Alvis* operując na jego postaci pośredniej zapisanej w języku *Haskell*.
   - opracowanie i implementacja algorytmu translacji graf LTS do języka SMV umożliwiającego weryfikację modeli *Alvis* w narzędziu *nuXmv*.
   - rozszerzenie możliwości weryfikacji obu powyższych rozwiązań poprzez opracowanie procesu weryfikacji modeli *Alvis* wykorzystującego chmury obliczeniowe.
   - opracowanie dwóch modeli systemów współbieżnych i czasu rzeczywistego (tj. zwrotnicy tramwajowej oraz centrali sygnalizacji pożarowej), a następnie ich formalna weryfikacja przy wykorzystaniu proponowanych podejść.

   Warto również podkreślić całkiem dobry współczynnik Hirscha (h=4), który stanowi dodatkową ilustrację osiągnięć naukowych Autora, głównie tych zawartych w rozprawie. Oceniana rozprawa udanie wpisuje się w nurt badań światowych dotyczących opracowywania nowych metod automatycznej weryfikacji modelowej, a uzyskane rezultaty upoważniają do stwierdzenia o wysokiej pozycji rozprawy w relacji do stanu wiedzy w skali krajowej oraz umiarkowanej pozycji w relacji do stanu wiedzy w skali światowej.

5. *Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?*

   Autor w pełni rozwiązał postawione w tezie rozprawy zadanie stosując właściwe dla przedmiotu badań metody. Zastosowana metodologia to: (1) analiza dostępnych narzędzi do automatycznej weryfikacji modelowej systemów współbieżnych i czasowych oraz analiza rozwiązań chmurowych; (2) opracowanie języka zapytań AQL umożliwiającego weryfikację modelu *Alvis* przy wykorzystaniu jego postaci pośredniej w języku *Haskell*; (3) opracowanie translacji z grafu LTS, wygenerowanego dla modelu w *Alvis*, do języka SMV, bedącego wejściem dla narzędzia *nuXmv*; (4) opracowanie procesu weryfikacji modeli w *Alvis* z użyciem rozwiązań chmurowych; (5) implementacja zaproponowanych przez Autora algorytmów oraz przeprowadzenie badań eksperymentalnych/wydajnościowych zarówno na komputerze klasy PC, jak i przy użyciu chmur obliczeniowych. Taka metodologia postępowania jest moim zdaniem właściwa i okazała się efektywna. Przyjęte założenia do realizacji zadań postawionych w tezie rozprawy są także prawidłowe i merytorycznie uzasadnione.

6. *Czy Autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?*

   Jak już zostało napisane w punkcie 2 tej recenzji, rozprawa obejmuje 118 stron, dzieli się na wstęp, podsumowanie, 6 rozdziałów prezentujących cel rozprawy i rozwiązujących postawioną tezę, spis treści, bibliografię oraz 1 załącznik. Treść pracy odpowiada tematowi określonemu w tytule. Treść kolejnych rozdziałów stanowi logicznie powiązaną całość.

   Struktura rozprawy wynika z przyjętego planu pracy oraz podporządkowana jest stopniowemu realizowaniu przyjętych celów. Prezentowane zagadnienia tworzą harmonijną całość, przez co autor rozprawy konsekwentnie realizuje zamierzone zadanie badawcze. Eksperymenty zostały poprawnie zaprojektowane i metodycznie przeprowadzone, a otrzymane wyniki dobrze przeanalizowane.

   Rozprawa napisana jest poprawnie i przekonująco. Zastosowana terminologia i symbole nie budzą większych zastrzeżeń. Należy jednak zaznaczyć, że:

- Definicji 4.3.2. zawiera błąd przy koniunkcji oraz operatorze Until.
- Dziwi, że LTL definiowane jest na minimalnym zbiorze operatorów modalnych, a CTL i RTCTL już nie.

Pod względem edytorskim oceniana rozprawa doktorska jest napisana dobrze, w czym z pewnością Autorowi pomogła umiejętność posługiwania się systemem LaTeX. Niemniej jednak Autor zapomniał o dodaniu do rozprawy tak istotnych z punktu widzenia czytelnika elementów jak: spis tabel, spis rysunków, czy też spis listingów. Ponadto:

- Autor zamiast poprawnej formy „agenci aktywni", czy też „agenci pasywni", czy też po prostu „agenci", stosuje niepoprawną formę „agenty".
- brak jest konsekwencji w odwoływaniu się do rysunków. Raz Autor stosuje „Rys. x.x", a raz „rysunek x.x".
- brak jest konsekwencji w odwoływaniu się do listingów. Raz Autor stosuje „na Listingu x.x", a raz „na/w listingu x.x".
- rozmiary niektórych rysunków są przesadnie duże (np. Rys. 2.2.), a niektórych (np. Rys. 2.4, 2.5) zbyt małe i nie do końca czytelne.
- jeśli chodzi o interpunkcję, to brakuje dużej ilości przecinków przed wyrażeniami z zaimkiem przymiotnikowym „który".

7. *Jakie są słabe strony rozprawy i jej główne wady?*

   Rozprawa ma dwie istotne usterki merytoryczne, które wymagają komentarza w trakcie obrony pracy.

   Usterka nr. 1: przedstawiona w piątym rozdziale translacja etykietowanego systemu przejść wygenerowanego dla modelu Alvis do języka SMV powinna zostać opatrzona dowodem jej poprawności, a takowy w rozprawie jest pominięty. Wydaje się, że ta poprawność jest oczywista, ale pewien komentarz byłby mile widziany, zwłaszcza, że brak jest również odniesienia do opublikowanej pracy Autora, w której taki dowód poprawności można byłoby znaleźć.

   Usterka nr. 2: przedstawiony w siódmym rozdziale *Alvis Query Language (AQL)* przypomina bardziej dokumentację techniczną i przewodnik dla inżyniera niż opis nowo proponowanego mechanizmu weryfikacji. Mile widziany byłby tutaj szczegółowy opis, przynajmniej kilku wybranych, ciał funkcji stanowiących AQL z wykazaniem poprawności algorytmów w nich zaimplementowanych. Tego w rozprawie brakuje. Brak jest również odniesienia do opublikowanej pracy Autora, w której takie definicje funkcji wraz z dowodem ich poprawności można byłoby znaleźć.

   Wymienione tutaj usterki nie mają istotnego wpływu na pozytywną ocenę ogólną osiągnięć naukowych opisanych w rozprawie.

8. *Jaka jest przydatność rozprawy dla dyscypliny Informatyka Techniczna i Telekomunikacja ?*

   W ocenianej rozprawie Autor zaproponował i zaimplementował dwa alternatywnego podejścia do weryfikacji modeli *Alvis*. Jedno wykorzystujące postać pośrednią modelu *Alvis* w języku *Haskell*, a drugie wykorzystujące translację do SMV po to, aby móc zastosować dobrze znane w świecie weryfikacji modelowej niskopoziomowe narzędzie *nuXmv*. Realizacje tych zadań wymagały doskonalej znajomości metod formalnych (m.in., systemów tranzycyjnych, logik temporalnych), wysokich umiejętności w zakresie programowania funkcyjnego oraz wykorzystywania chmur obliczeniowych. Ponadto, oba zaproponowane algorytmy istotnie rozszerzają funkcjonalność narzędzia *Alvis* rozwijanego na Wydziale Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej w AGH przez zespół badawczy prof. dr hab. Marcina Szpyrki. Zatem uważam, że realizację wspomnianych wyżej zadań należy uznać jako znaczący wkład w rozwój dyscypliny Informatyka Techniczna i Telekomunikacja, o czym świadczą również publikacje Autora w czasopismach o zasięgu międzynarodowym, w tym, w czasopiśmie „*IEEE Access*", które zostało wycenione na 100pkt w ostatniej liście czasopism z MNiSW.

Za niemniej istotne i wielce przydatne naukowo uważam również opracowanie dwóch autorskich modeli systemów współbieżnych i czasu rzeczywistego, tj. zwrotnicy tramwajowej oraz centrali sygnalizacji pożarowej. Tego typu modele sa bardzo cenione w świecie naukowym związanym z automatyczną weryfikacja modelową, gdyż umożliwiają one porównawcze badania nowych algorytmów, a czas i praca związana z ich stworzeniem są niebagatelne.

9. *Konkluzja*

Ze względu na wagę podjętego w rozprawie problemu badawczego i znaczenie praktyczne, a przede wszystkim na pozytywną ocenę merytoryczną i metodologiczną, stwierdzam, że recenzowana rozprawa doktorska spełnia wymagania Ustawy stawiane rozprawom doktorskim. Wnioskuję zatem o dopuszczenie mgra inż. Jerzego Biernackiego do dalszych etapów postępowania w przewodzie doktorskim.

dr hab. Bożena Woźna-Szcześniak, prof. UJD