

Prof. dr hab. inż. Bolesław Pochopień
Katedra Grafiki, Wizji Komputerowej i Systemów Cyfrowych
Wydział Automatyki, Elektroniki i Informatyki
Politechnika Śląska

Gliwice, 05.07.2021

RECENZJA ROZPRAWY DOKTORSKIEJ

Tytuł rozprawy: Synteza logiczna funkcji boolowskich szczególnej postaci

Autor rozprawy: mgr inż. Tomasz Mazurkiewicz

Promotor rozprawy: prof. dr hab. inż. Tadeusz Łuba

(Recenzję opracowano na podstawie otrzymanego pisma Przewodniczącego Rady Dyscypliny Naukowej „Informatyka Techniczna i Telekomunikacja” dr. hab. inż. Zbigniewa Tarapaty, prof. WAT-pismo WYCH/N/00216/2021 z dnia 14.05.2021-działającego w oparciu o uchwałę nr 32/RDN ITiT/2021 z dnia 11 maja 2021)

1. Cel, zakres i charakter rozprawy

Wydarzenia w ostatnich miesiącach potwierdziły jak ważnym problemem jest cyberbezpieczeństwo aby skutecznie bronić się przed destabilizacją i dezinformacją wywołaną cyberatakami. Najlepszym gwarantem bezpieczeństwa jest podejmowanie działań związanych z ciągłym doskonaleniem systemów teleinformatycznych w celu zwiększenia skuteczności ich działania. Jedną z podstawowych operacji realizowanych w takich systemach jest wyszukiwanie danych reprezentujących różnorodne informacje statyczne i dynamiczne w dużym zbiorze, jak również ich klasyfikacja. Liczne możliwości stwarza zastosowanie funkcji boolowskich szczególnej postaci, zwanych też funkcjami generowania indeksów. Funkcje generowania indeksów okazują się użyteczne w realizacji m.in. skanerów antywirusowych, tablic adresów IP, kontrolerów TAC, konwerterów danych cyfrowych, zoptymalizowanych postaci białych list. W ostatnich latach prowadzone są intensywne badania nad sprzętową realizacją generatorów indeksów, czyli układów cyfrowych, które realizują funkcje generowania indeksów.

Zasadniczym celem badawczym recenzowanej pracy jest realizacja funkcji generowania indeksów, pozwalająca ograniczyć wykorzystanie pamięci. W aspekcie aplikacyjnym tematyka recenzowanej pracy dotyczy istotnych i aktualnych problemów.

W rozdziale 1 Doktorant sformułował zasadnicze tezy pracy:

- 1) Zbiory niezgodności wykorzystane mogą być do poszukiwania dekompozycji liniowej funkcji generowania indeksów.
- 2) Możliwa jest realizacja funkcji generowania indeksów z wykorzystaniem struktur probabilistycznych, charakteryzująca się niewielkim wykorzystaniem pamięci.

- 3) Dekompozycja funkcjonalna pozwala na realizację funkcji generowania indeksów, dla których nie istnieje optymalna dekompozycja liniowa.

Wyrażam przekonanie, że wybór tematu rozprawy doktorskiej uznać należy za poprawny, interesujący, ważny technicznie i wciąż aktualny, a stopień trudności i zakres podjętego zadania, jego znaczenie naukowe oraz przydatność praktyczna odpowiadają ustawowym i zwyczajowo przyjętym kryteriom jakie zwykło się wiązać z rozprawą doktorską. Tematyka rozprawy jest bardzo ambitna i mieści się w nurcie istotnych badań światowych w tej tematyce. Zakres pracy jest stosunkowo obszerny.

2. Zawartość rozprawy

Jednym z ważniejszych zadań w analizie danych jest zadanie wyodrębniania właściwych danych z ogromnej masy danych niepotrzebnych – w literaturze przedmiotu obejmowane nazwą generatorów adresu. Metodom syntezy takich układów poświęca się coraz większą liczbę prac naukowych publikowanych w artykułach i referatach konferencyjnych. Jedną z przyczyn takiej sytuacji jest specyfika działania takich układów sprowadzająca ich syntezę do syntezy silnie nieokreślonych funkcji boolowskich, których cechą charakterystyczną jest ogromna liczba zmiennych, a w konsekwencji potrzeba stosowania pamięci stałych typu ROM. Zastosowanie bloków pamięci (wbudowanych lub zewnętrznych) w systemach klasyfikacji danych otwiera więc nowe możliwości, jednak efektywne wykorzystanie tych możliwości wymaga zaawansowanego oprogramowania do redukcji, kompresji i dekompozycji zbiorów danych. Obszerny przegląd tych metod przedstawiono w książce o charakterystycznym tytule: „Memory based logic synthesis” [T. Sasao]. W książce tej wyraźnie podkreśla się nowe zadania syntezy logicznej, obejmujące: redukcję argumentów, dekompozycję liniową, dekompozycję funkcjonalną - niestety nie podając żadnych konkretnych rozwiązań tych problemów. Z powyższego wynika, że zagadnienia klasyfikacji danych i wykrywania wzorców w przypadku realizacji sprzętowych dystrybucji adresów IP, skanowania wirusów oraz wykrywania niepożądanych danych, wymagają obszernych badań w zakresie algorytmów syntezy logicznej. Badania te obejmują: dekompozycję liniową, realizację sprzętową oraz dekompozycję funkcjonalną.

W ramach badań związanych z dekompozycją liniową, Doktorant zaproponował metodę pozwalającą na reprezentację funkcji jako złożenia funkcji liniowej (realizowanej z wykorzystaniem bramek XOR) oraz funkcji ogólnej (realizowanej z wykorzystaniem pamięci ROM/RAM). Metoda ta wykorzystuje zbiory niezgodności reprezentujące argumenty funkcji wyznaczone przez niezgodne wartości binarne w analizowanej parze wektorów. W celu zwiększenia efektywności czasowej oprogramowania, dane wejściowe są wstępnie przetwarzane z wykorzystaniem algorytmu redukcji argumentów. Opracowane do tego celu oprogramowanie umożliwiło przeanalizowanie efektywności uzyskiwanego rozwiązania pod względem liczby zmiennych dla wybranych funkcji – koderów M z 16 i M z 20. Otrzymane rezultaty okazały się konkurencyjne z wynikami innych autorów, których publikacje przedstawiono w literaturze rozprawy. Ze względu na iteracyjny charakter działania algorytmu, w dalszych pracach przeanalizowano możliwość innego wyboru funkcji rozdzielającej. Na podstawie przeprowadzonych badań Doktorant zaproponował obliczanie dodatkowego parametru R oraz wybór funkcji, która cechuje się jego najmniejszą wartością. Podejście to nazwano MinR, podczas gdy wcześniej stosowano - First-Fit. Wartość ta równa jest liczbie różnych wektorów powstałych po usunięciu z tablicy prawdy funkcji tych

zmiennych, które wykorzystywane są w funkcji rozdzielającej. Zaproponowana metoda pozwoliła uzyskać lepsze wyniki dla koderów M z 16 i M z 20. Efektywność algorytmu zweryfikowano także z wykorzystaniem losowo wygenerowanych funkcji generowania indeksów i porównano z wynikami uzyskanymi z wykorzystaniem (własnej) implementacji metody wielomianowej Jaakko Astoli oraz wynikami dostępnymi w literaturze. Zaproponowany algorytm gwarantuje uzyskanie wyników równie dobrych, jak najlepsze algorytmy dostępne w literaturze.

Równoległe do prac nad algorytmem dekompozycji liniowej, Doktorant analizował możliwości sprzętowej realizacji generatora indeksów z wykorzystaniem dedykowanej architektury. Motywacją do badań dotyczących wykrywania wzorców była architektura IGU (Index Generation Units) zaproponowana przez Sasao. Wykorzystuje ona moduł transformacji liniowej, dwie pamięci, a także komparator oraz bramkę AND. Pamięć podstawowa przechowuje informację o generowanej wartości indeksu. Pamięć dodatkowa wykorzystywana jest z kolei do określenia, czy otrzymany wektor wejściowy należy do zbioru wektorów funkcji. Mając na uwadze fakt, że zajętość tej pamięci zależy od liczby zmiennych po transformacji liniowej poszukuje się takiej transformacji liniowej, która gwarantuje uzyskanie jak najmniejszej liczby zmiennych. Jednak im mniejsza ta liczba, tym wykorzystanie pamięci dodatkowej jest większe. W rezultacie może to doprowadzić do sytuacji, w której pamięć dodatkowa będzie większa niż pamięć podstawowa. W celu uniknięcia tego zjawiska Doktorant zaproponował zastosowanie struktur probabilistycznych - filtr Blooma oraz filtr Cuckoo – co umożliwiło zastąpienie pamięci dodatkowej. Przeprowadzone badania potwierdziły, że dzięki tej realizacji możliwe jest uzyskanie mniejszego wykorzystania pamięci, kosztem niewielkiego prawdopodobieństwa wyniku fałszywie pozytywnego. Wykorzystanie pamięci w proponowanej architekturze nie zależy od liczby zmiennych po transformacji liniowej. Przeprowadzono również badania uwzględniające analizę możliwości zastosowania filtru Blooma z pojedynczą funkcją skrótu.

W ramach badań związanych z dekompozycją funkcjonalną należy zwrócić uwagę na fakt, że dekompozycja liniowa gwarantuje efektywną realizację funkcji generowania indeksów, ale nie wszystkie funkcje posiadają optymalną dekompozycję liniową. W takich przypadkach stosuje się dekompozycję funkcjonalną. Niestety stosowane do tej pory algorytmy dekompozycji funkcjonalnej (Sasao) mają istotne ograniczenie do tzw. dekompozycji rozłącznej, co w przypadku trudniejszych zadań uniemożliwia uzyskanie jakiegokolwiek rozwiązania. Nie mniej istotnym mankamentem aktualnych metod dekompozycji funkcji generowania indeksów jest stosowanie tzw. tablic dekompozycji. Istotą metody zastosowanej w niniejszej rozprawie jest zastosowanie rachunku podziałów. Rachunek ten umożliwia sformułowanie wygodnych w praktyce twierdzeń, znacząco upraszczających dekompozycję funkcji generowania indeksów. I co najważniejsze, uzyskanie skutecznej metody obliczania dekompozycji nierozłącznej umożliwiającej znajdowanie reprezentacji funkcji jako złożenia dwóch funkcji w taki sposób, że $F(X) = H(U, G(VUW))$, gdzie $W \subseteq U, U \cap V = \emptyset$ oraz $U \cup V = X$. Możliwość takiej realizacji zapewnia odpowiednie przydzielenie zmiennych do zbiorów U i V, czyli określenie liczby zmiennych wejściowych do funkcji H oraz znalezienie postaci funkcji G i zbioru W. Ze względu na to, że rachunek podziałów oraz pojęcie r-przydatności pozwalają rozwiązać dwa pierwsze problemy, Doktorant skupił się na zadaniu znajdowania postaci zbioru W. W szczególności zaproponowane zostały dwa algorytmy: heurystyczny oraz dokładny. W ramach badań przeanalizowano również inne metody wyboru zmiennych i ich wpływ na efektywność czasową i jakość rozwiązania. Zastosowanie heurystycznych algorytmów kolorowania grafu umożliwiło efektywną dekompozycję funkcji o dużej liczbie wektorów. W ramach badań zaproponowano też algorytm dokładny dekompozycji funkcjonalnej. W tym celu

wykorzystano problem spełnialności modulo teorie (SMT). Na podstawie tablicy prawdy funkcji utworzono model, który wykorzystuje komendy zgodne ze standardem SMT-LIB. Następnie z wykorzystaniem narzędzia Z3 poszukiwane jest rozwiązanie, które spełnia ten model. Uzyskane w ramach badań wyniki potwierdziły efektywność zaproponowanego algorytmu pod względem jakości uzyskiwanego rozwiązania. Niestety, jego efektywność czasowa jest znacznie niższa niż w przypadku algorytmu heurystycznego. Co istotne, inni autorzy w ramach swoich prac skupiali się jedynie na znajdowaniu dekompozycji rozłącznej. Otrzymane w tych badaniach wyniki udowodniły jednak, że dla wielu funkcji podejście to jest niewystarczające. Na przykład, dla koderów 2 z 20 oraz 4 z 20 Doktorant znalazł dekompozycję nierozłączną, która pozwoliła na zmniejszenie wykorzystania pamięci o kilkadziesiąt procent.

Recenzowana praca ma stosunkowo zwarty charakter i stanowi spójną tematycznie całość. Następstwo rozdziałów i podrozdziałów jest właściwe, lecz ich zawartość i proporcje mogą być dyskusyjne. Praca ma stosunkowo dobry układ logiczny i wyraźnie pokazuje w jaki sposób kolejno formułowane i rozwiązywane w niej problemy częściowe składają się na kompletną całość. Praca liczy 95 stron, zawiera w kolejności streszczenie spisy treści, rysunków i tabel, sześć rozdziałów oraz wykaz bibliograficzny. Rozdział 6 stanowi podsumowanie i propozycje dalszych kierunków badań.

3. Analiza źródeł

Wykaz bibliograficzny obejmuje w zasadzie najważniejsze pozycje związane z tematyką i rozpatrywanym zakresem pracy. Lista cytowanych w pracy źródeł obejmuje 100 pozycji, w tym: 3 (z lat:1957, 1962, 1967), 3 (1970, 1974, 1979), 9 (1989-1997), 13 (2001-2010), 30 (2001-2016) i 42 (2017-2020). Na szczególne podkreślenie zasługuje fakt, że Doktorant jest samodzielnym autorem sześciu publikacji (w tym pięciu anglojęzycznych), głównym współautorem w 2-osobowych czterech publikacjach (w tym 2 anglojęzycznych) i 3-osobowej anglojęzycznej publikacji oraz współautorem w 2-osobowych dwóch polskojęzycznych publikacjach. Jest też już autorem anglojęzycznej publikacji w 2021 roku, nie cytowanej w pracy. Wyszczególnione powyżej prace Doktoranta zostały opublikowane odpowiednio:

- Na konferencjach o charakterze międzynarodowym:
 - International Conference on Systems Engineering (ICSEng),
 - International Conference Mixed Design of Integrated Circuits and Systems (MIXDES),
 - IEEE-SPIE Joint Symposium Wilga,
 - IEEE International Symposium on Multiple-Valued Logic (ISMVL),
 - International Business Information Management Association (IBIMA) Conference.
- Na konferencjach o charakterze krajowym:
 - Krajowe Sympozjum Telekomunikacji i Teleinformatyki (KSTiT).
- W czasopismach naukowych:
 - Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne,
 - Technical Sciences,
 - Journal of Telecommunications and Information Technology (JTIT),
 - Journal of Software and Systems Development.

Liczba publikacji Doktoranta, indeksowana w bazach międzynarodowych¹: *Web of Science* - 4, *Scopus* - 6, *IEEE Xplore* - 4, *Google Scholar* - 17.

Doktorant podejmuje w pracy, moim zdaniem, udaną próbę uporządkowania i usystematyzowania dotychczasowego dorobku publikacyjnego z zakresu objętego tematyką rozprawy, co świadczy o Jego bardzo dobrym rozeznaniu w literaturze przedmiotu, a także umiejętnym jej studiowaniu. Wnioski z przeglądu źródeł sformułowane są w sposób jasny i przekonujący.

4. Ocena uzyskanych rezultatów

Recenzowana praca zawiera wiele oryginalnych elementów. Za szczególnie istotne osiągnięcia Doktoranta uważam zaproponowane:

- Autorskie metody modyfikacji algorytmu dekompozycji liniowej wykorzystującego zbiory niezgodności – iteracyjny algorytm oraz 2 metody wyboru funkcji rozdzielającej: First-Fit oraz MinR.
- Autorska architektura wykorzystująca struktury probabilistyczne.
- Autorskie 2 metody (heurystyczna, dokładna) poszukiwania nierozłącznej dekompozycji funkcjonalnej funkcji generowania indeksów.

Praca jest starannie zredagowana, zawiera wszystkie elementy dobrej rozprawy naukowej, a mianowicie: krytyczny przegląd literatury, przedstawienie tezy i celu pracy, wskazanie zagadnień wymagających rozwiązania, krytyczne spojrzenie na uzyskane rezultaty, przedstawienie uzasadnionych i trafnych propozycji związanych z dalszą kontynuacją prowadzonych badań. Nie znalazłem w pracy błędów merytorycznych. Tezy i cele pracy zostały sformułowane w sposób jasny i precyzyjny. Sposób podejścia do rozwiązywania postawionego zadania uważam za metodologicznie prawidłowy. Doktorant doprowadził do realizacji postawionych celów i wykazania prawdziwości sformułowanych w pracy tez. Uzyskane rezultaty wzbogacają stan wiedzy światowej w obszarze tematyki, której dotyczy oceniana praca. Zawartość poszczególnych rozdziałów i rozwój zawartej w niej myśli świadczy o dojrzałości naukowej Doktoranta.

Podczas lektury pracy nasunęło mi się kilka pytań do Doktoranta, w tym m.in.:

- 1) Celem syntezy logicznej jest znalezienie dokładnej reprezentacji funkcji, która minimalizuje zajętość zasobów logicznych. Pana generator indeksów wykorzystuje jednak struktury probabilistyczne, które wprowadzają niezerowe prawdopodobieństwo wyniku fałszywie pozytywnego. Czy mógłby Pan ocenić, jak występowanie tego rodzaju błędu wpływa na możliwość stosowania zaproponowanego przez Pana rozwiązania?
- 2) Analizując literaturę można zauważyć, że większość artykułów na temat syntezy logicznej funkcji generowania indeksów dotyczy algorytmów dekompozycji liniowej. Z czego, Pana zdaniem, wynika brak większego zainteresowania innych autorów algorytmami dekompozycji funkcjonalnej? W Pana rozprawie tematyka ta jest ważnym zagadnieniem.

Interesującym byłoby, aby Doktorant, podczas obrony rozprawy doktorskiej, zechciał ustosunkować się do tych pytań.

5. Wniosek końcowy

Podsumowując recenzję pragnę stwierdzić, co następuje:

- Doktorant wykazał się dogłębną wiedzą z zakresu zagadnień, które uczynił przedmiotem dociekań naukowych.
- Rozwiązał nietrywialny, stosunkowo trudny, aktualny i ważny technicznie problem naukowy, użyteczny praktycznie i dobrze go udokumentował.
- Wykazał się przy tym dużą inicjatywą twórczą, umiejętnością rozwiązywania złożonych problemów, bardzo dobrym opanowaniem warsztatu badawczego i przygotowaniem do samodzielnego prowadzenia badań naukowych.

Uważam, że recenzowana praca mgr. inż. Tomasza Mazurkiewicza pt. „Synteza logiczna funkcji boolowskich szczególnej postaci” spełnia z wyraźnym nadmiarem wszystkie wymagania postanowień ustawowych stawianych rozprawom doktorskim. Dlatego stawiam wniosek o przyjęcie recenzowanej pracy jako rozprawy doktorskiej i dopuszczenie jej Autora do dalszych etapów przewodu doktorskiego. Uwzględniając liczny i wartościowy dorobek publikacyjny Autora oraz fakt, że praca jest nowatorska i wybitnie dobra, wnioskuję o jej wyróżnienie.

Wniosek przyjęty