Warszawa, 19 października 2020 r.

dr hab. inż. Grzegorz Borowik, prof. Uniwersytetu SWPS
Katedra Informatyki
Wydział Projektowania
SWPS Uniwersytet Humanistycznospołeczny

Recenzja rozprawy doktorskiej pt. Efektywne badanie nieprzywiedlności wielomianów binarnych o szczególnych postaciach

Autor rozprawy:
mgr inż. Paweł Jacek Augustynowicz

Promotor:
dr hab. inż. Andrzej Paszkiewicz, prof. WAT

Niniejsza recenzja została sporządzona na prośbę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja w przedłożonym przez dra hab. inż. Zbigniewa Piotrowskiego, prof. WAT piśmie (uchwała 22/RDN ITiT/2020). Przewód doktorski prowadzony jest zgodnie z klasyfikacją dziedzin i dyscyplin naukowych w latach 2011–2018, tj. w dziedzinie nauk technicznych, w dyscyplinie Informatyka.

Mechanizmy ochrony komunikacji cyfrowej realizowane za pomocą specjalnych protokołów bezpieczeństwa i w formie algorytmów kryptograficznych stały się częścią wielu standardowych rozwiązań. Eksplozja wzrostu usług internetowych w zakresie handlu i biznesu, w tym operacji finansowych i obrotu kapitałowego, spowodowała, że realizacja mechanizmów zabezpieczenia przed nieuprawnionym dostępem do informacji jest ogromnym i aktualnym wyzwaniem.

Celem pracy było przeprowadzenie badań podstawowych mających na celu systematyczne i empiryczne sprawdzenie wybranych własności trójmianów, wielomianów osadowych oraz rejestrów przesuwnych o nieliniowej funkcji sprzężenia zwrotnego. Przedstawione w recenzowanej rozprawie wyniki, przez ich potencjalne zastosowanie w praktyce, są ściśle związane z bezpieczeństwem informacji. Wyniki znajdują ważne zastosowania w kryptografii szyfrów strumieniowych np. do opisu rejestrów z liniowym sprzężeniem zwrotnym, schematach wymiany klucza, czy dynamicznego generowania nierozkładalnych wielomianów pierwotnych. Ponadto znajdują zastosowanie w teorii kodowania, testowaniu układów cyfrowych pod kątem uszkodzeń, ale można je również stosować w zagadnieniach związanych z generatorami liczb losowych wykorzystywanych w metodach Monte-Carlo.

Przeprowadzone przez Autora studia literaturowe dotyczące algorytmów badania nieprzywiedlności dla wielomianów szczególnych postaci nad ciałem binarnym oraz poszukiwań rejestrów przesuwnych o szczególnej, nieliniowej postaci funkcji sprzężenia zwrotnego i maksymalnym okresie pozwoliły na sformułowanie następujących tez pracy:

- Prowadzenie rozległych eksperymentów obliczeniowych pozwala na weryfikację prawdziwości znanych hipotez i sformułowanie nowych hipotez oraz twierdzeń.
- Możliwym jest skonstruowanie efektywnych algorytmów badania nieprzywiedlności wielomianów binarnych nad GF(2), uwzględniających specyfikę współczesnych systemów obliczeniowych, w tym procesorów umożliwiających przetwarzanie wektorowe oraz koprocesorów graficznych, jak również prowadzenie przy ich wykorzystaniu zaawansowanych eksperymentów obliczeniowych.

- Środowisko obliczeniowe kart graficznych pozwala na efektywne badanie pełności okresu rejestrów przesuwnych o szczególnych, nieliniowych postaciach funkcji sprzężenia zwrotnego.

Tezy rozprawy zostały sformułowane w sposób precyzyjny i jasny. Uwzględniając powyższe wyrażam przekonanie, że wybór tematu rozprawy doktorskiej mgr. inż. Pawła J. Augustynowicza uznać należy za ważny technicznie i 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 doktorskiej mieści się w nurcie badań światowych z zakresu teorii liczb i własności wielomianów. Charakter rozprawy można uznać za teoretyczno-eksperymentalny, wyraźnie ukierunkowany w stronę praktycznych zastosowań.

Na podkreślenie zasługuje dobre rozeznanie Autora w literaturze przedmiotu. Wykaz literatury obejmuje 83 pozycje (są to pozycje z okresu 1946–2020, z czego większość to publikacje z ostatniego dziesięciolecia, ale zamieszczenie pozycji starszych jest jak najbardziej uzasadnione), w tym 6 pozycji współautorskich mgr. inż. Pawła J. Augustynowicza (Autor nie ma w swoim dorobku publikacji samodzielnej). Wnioski z przeglądu stanu wiedzy oraz aktualnych badań w uznanych ośrodkach naukowych przedstawiono w sposób jasny i przekonujący. Autor w sposób właściwy odniósł się do dotychczasowego dorobku literaturowego i oceny stanu wiedzy w zakresie istotnych problemów zgodnych z tematyką pracy. Doktorant wykazał się również dobrym rozeznaniem w zakresie istniejących współczesnych jednostek procesorowych oraz obliczeniowych układów graficznych.

W trakcie prowadzonych badań Autor zaprojektował i zaimplementował rodzinę efektywnych algorytmów badania nieprzywiedlności wielomianów nad ciałem binarnym oraz poszukiwania rejestrów przesuwnych o nieliniowej funkcji sprzężenia zwrotnego o maksymalnym okresie.

Oryginalnym elementem rozprawy jest zaproponowana przez Autora modyfikacja podstawowego algorytmu badania nieprzywiedlności Ben-Ora. Zmodyfikowany algorytm pozwala na efektywne badania nieprzywiedlności wielomianów binarnych z wykorzystaniem współczesnych jednostek procesorowych oraz koprocesorów graficznych. Kluczowe w zaproponowanym rozwiązaniu jest przeorganizowanie reprezentacji wielomianów binarnych w pamięci przez transpozycję ich tablicy. Taka organizacja pozawala na równoległe przetwarzanie k bitów w jednym kroku algorytmu, a także wykorzystanie specyficznych dla procesorów operacji. W wyniku reorganizacji bitów następuje grupowanie współczynników wielomianów, dzięki czemu mogą być one przetwarzane w ramach jednej instrukcji. Dzięki zaproponowaniu struktury bryłki, operacja podnoszenia wielomianu do kwadratu jest efektywnie realizowana przez odpowiednie manipulacje pamięcią. Największymi zaletami zaimplementowanych rozwiązań jest ich wszechstronność i skalowalność. Mogą być dostosowane do niemal każdej platformy obliczeniowej, stopnia wielomianu lub jego postaci.

W wyniku opracowania algorytmów oraz ich implementacji w układach procesorowych oraz układach graficznych Autor:
- obliczył najmłodsze leksykograficznie wielomiany osadowe o stopniu mniejszym bądź równym wartości 513000;
- podał kompletną listę 25 kontrprzykładów do hipotezy Gao, Howella i Panario o stopniu wewnętrznym wielomianu osadowego. Należy zaznaczyć, że pierwszy kontrprzykład został podany w 2009 roku przez dr. hab. inż. A. Paszkiewicza, który do roku 2012 doprowadził badania wielomianów osadowych nad GF(2) do stopnia $n = 132000$;
- pokazał, że dla danego stopnia wewnętrznego może istnieć więcej niż jeden wielomian osadowy niespełniający hipotezy Gao, Howella i Panario;

- pokazał, że hipoteza zaproponowana przez dr. hab. inż. A. Paszkiewicza w ramach pracy „Nierozwiązane problemy dotyczące wielomianów nieprzywiedlnych nad ciałem skończonym GF(2)" jest górnym ograniczeniem do stopnia $n = 513000$;
- wyznaczył przybliżenie średniego stopienia wewnętrznego wielomianu osadowego dla badanego przedziału stopni wielomianów przez podanie odpowiedniej funkcji;
- zbadał rozkłady dla liczb wielomianów o danym stopniu wewnętrznym i pokazał, że rozpatrując zadany problem w różnych przedziałach o zadanej długości, uzyskuje się podobne rozkłady ilościowe;
- zaproponował alternatywny sposób poszukiwania rozpatrywanych struktur algebraicznych, który charakteryzuje się mniejszą złożonością praktyczną, ale nie w każdym przypadku daje w rezultacie rozwiązanie optymalne. W badaniu, oprócz powszechnie używanej metody poszukiwania zgodnego z porządkiem leksykograficznym, porównał przeszukiwanie wielomianów kandydujących do znalezienia pierwszego wielomianu osadowego w porządku odwrotnym leksykograficznym z wykorzystaniem zmodyfikowanej i obalonej hipotezy 3.1. oraz względem aproksymacji funkcji średniego stopnia – naprzemiennie zgodnie i przeciwnie do porządku leksykograficznego. Wykazał, że metoda oparta na wykorzystaniu funkcji średniego stopnia wielomianu osadowego pozwala na najszybsze odnalezienie wielomianu nierozkładalnego o pożądanej postaci, a znaleziony przez nią wielomian ma najniższy możliwy stopień wewnętrzny w 98% przypadków;
- przeprowadził eksperyment obliczeniowy mający na celu wyznaczenie wszystkich trójmianów nieprzywiedlnych do stopnia $n = 513000$ oraz trójmianów nierozkładalnych o szczególnej postaci $x^{2\cdot 3^l} + x^{3^l} + 1$ dla $l \in \{1,2,\ldots,13\}$. Zaimplementowany algorytm osiągnął wyniki wydajnościowe lepsze niż biblioteka NTL. Badania Autora pozwoliły na przedstawienie po raz pierwszy przykładów ośmiu i dziewięciu kolejnych stopni, dla których nie istnieje trójmian nierozkładalny;
- wyznaczył statystyki udziału wielomianów, dla których istnieje co najmniej jeden trójmian nierozkładalny oraz średnią liczbę trójmianów nierozkładalnych przypadających na stopień;
- przeprowadził badania wyczerpujące trójmianów nieprzywiedlnych nad GF(2), których stopień wyraża się liczbą postaci $2 \cdot 3^l$ dla $l \leq 13$. Wielomiany nieprzywiedlne tych stopni posiadają ciekawą własność, mianowicie ich stopnie wewnętrzne układają się (z wyjątkiem kilku sporadycznych przypadków) według pewnego wzorca. Autor rozprawy potwierdził istnienie tych wzorców dla wszystkich $l \leq 13$, weryfikując za pomocą techniki "double checking" wcześniejsze obserwacje promotora pracy, przeprowadzone w zakresie $l \leq 12$. Dzięki temu możliwe było znalezienie i dowiedzenie nierozkładalności dziewięciu nieskończonych klas trójmianów;
- zaproponował nowy algorytm weryfikacji maksymalności okresu rejestru przesuwnego o zadanej funkcji sprzężenia zwrotnego dostosowany do wymagań środowisk graficznych i najnowszych architektur procesorowych. W ramach eksperymentu znalazł wszystkie rejestry przesuwne o funkcji sprzężenia zwrotnego o zadanej postaci dla długości rejestrów $n \leq 30$ osiągając w ten sposób nowe wyniki w porównaniu do tych prezentowanych w literaturze światowej.

Wymienione elementy rozprawy stanowią samodzielny i oryginalny dorobek Autora.

Rozprawa stanowi spójną tematycznie całość. Następstwo rozdziałów i podrozdziałów oraz ich zawartość należy uznać za właściwe. Omawiane zagadnienia zostały uzupełnione przez algorytmy prezentowane w pseudokodzie. Zawartość poszczególnych rozdziałów i rozwój zawartych w nich myśli świadczy o dojrzałości naukowej Doktoranta, dobrym przygotowaniu do samodzielnego prowadzenia badań naukowych, jak również świadczy o popartych wyczuciem dużych umiejętnościach inżynierskich.

W zasadzie nie dostrzegam istotnych wad rozprawy, a gdyby chcieć wymienić „drobne", to wskazałbym jedynie na:

- brak publikacji wyników badań w czasopiśmie o szerokim zasięgu. Takie publikacje mogą skutecznie wpłynąć na wiedzę w wielu ośrodkach naukowych, takich jak Uniwersytet Kalifornijski w Santa Barbara, w którym pracuje Çetin Kaya Koç. Należy podkreślić że hipoteza 3.1. rozprawy została

obalona po raz pierwszy przez dr. hab. inż. A. Paszkiewicza w 2009 r., jednak brak odpowiedniej publikacji o szerokim zasięgu spowodował, że Çetin Kaya Koç wyróżnił hipotezę jako jeden z nierozwiązanych problemów matematyki obliczeniowej w swojej książce w roku 2015;
- brak wstępnych wprowadzających dyskusji, np. w rozdz. 2 omawiającym implementację zaproponowanej modyfikacji algorytmu; można pokusić się o proste stwierdzenie, że dokonano transpozycji współczynników wielomianów;
- brak dobrego omówienia tablic z wynikami; warto uzupełnić omówienie wyników wskazując i omawiając pojedynczy wiersz z tablicy (dotyczy tablicy na stronie 31 i kolejnych). Przykładowo na stronie 31 jest informacja, że "szczegółowe wyniki zawarto w tabelach 2.3, 2.4, 2.5, 2.6." Według recenzenta pożądane byłoby wyjaśnienie co znajduje się w przykładowym wierszu tabeli wskazując czytelnikowi na wadę i zaletę danego układu obliczeniowego;
- brak dyskusji dotyczącej przeniesienia zaproponowanej metody na inne układy procesorowe/graficzne. Rodzi się pytanie: Czy zaproponowana metoda jest generyczna i umożliwia implementację z wykorzystaniem najnowszych układów graficznych?;
- brak analizy statystycznej rozkładów; Autor rozprawy wskazuje jedynie, że dane charakteryzują się "podobnym rozkładem";
- wady redakcyjne – praca zawiera czterostopniowe indeksowanie sekcji; przy tej wielkości dokumentu zaleca się indeksowanie dwustopniowe.

Moje uwagi traktuję jako rzecz drugorzędną w odniesieniu do uzyskanych przez Doktoranta rezultatów.

Praca zawiera błędy stylistyczne i redakcyjne, które nie wpływają na jakość i wartość merytoryczną rozprawy:

str. 1, "interesujących pozycjach" – zbyt potoczne stwierdzenie

str. 2, brakuje nr strony

str. 2, "trójmianów nierozkładalnych towarzyszących wielomianów postaci" – niejasne

str. 2, praca jest napisana w formie bezosobowej, natomiast na stronie jest akapit w pierwszej osobie

str. 13, drugi wzór, zamiast f_i powinno być g_i

str. 13, "zachodzi dla jakiś" – zbyt potoczne stwierdzenie

str. 20, "rozkazów jednocześnie 4 elementach wektora zmiennych pojedynczej precyzji" – niejasne

str. 20, "Dlatego też istotnym jest, by obydwa rodzaje równoległości wziąć pod uwagę w trakcie konstrukcji i implementacji rozwiązań algorytmicznych, gdyż tylko takie podejście gwarantuje ich wysoką wydajność." – niejasne są rodzaje równoległości, nie wynikają z poprzedzającego tekstu

str. 20, sugestia zamiany słowa "wspiera" na słowo "umożliwia"

str. 22, "układ graficzny mikroarchitektury Pascal składa się z skalowalnej macierzy…" – niejasne

str. 24, "W obydwu przypadkach zaobserwowano znaczący wzrost wydajności porównaniu do tradycyjnych metod mnożenia wielomianów binarnych." – brakuje "w"

str. 25, “Nie brano pod uwagę, iż istnieją zastosowania arytmetyki ciał skończonych, takie jak badanie nieprzywiedlności, dla których to nie operacja mnożenia jest najbardziej czasochłonna.“ – niejasne, zdanie wymaga przeredagowania

str. 25 i kolejne, sugestia zmiany “opartą o” na “opartą na”, np. “opartą o wykorzystanie” na “opartą na wykorzystaniu”

str. 36, “poprzez dodatnie warunków” – literówka

str. 37, “potwierdza lub przeczy … hipotezie” – raczej “przeczy hipotezie”

str. 44, “rozkład … równomierny” – nie jasne jest użycie stwierdzenia

str. 44 i kolejne, niepoprawne użycie słowa “histogram”, to jest raczej wykres słupkowy

str. 50, “zgodnie ze wzorem” “zgodnie z wzorem”

str. 51, “Przedstawiony algorytm, …, powinna umożliwić na znalezienie” – literówka

str. 56, “problemu . Przestrzeń” – niepotrzebna spacja

str. 57, “… to można wówczas powyższe twierdzenie zastosowań do wielomianu” – literówka

str. 58, “… można skonstruowano algorytm” – literówka

str. 60, “… dla których istnieje trójmian nierozkładalny się stabilizuje wokół wartości …” – niejasne

str. 72, “Badania wyczerpujące pozwoliły na przedstawienie po raz pierwszy przykładów 8 i 9 kolejnych stopni n …” – nie jest jasne, zaleca się użycie liczebników w formie słownej, jeśli odnoszą się one do kontekstu pracy i są z przedziału 0-9.

str. 76, “rejestrów przesuwnych o maksymalnych okresie” – literówka

str. 76, “$B_n = 2^{2-1} - n$” – błąd

str. 76, “Jednym z najchętniej stosowanych i poznanych teoretycznie rodzajem sekwencji są tak zwane kwadratowe m-sekwencje.” – literówka

str. 76, “Kwadratową m-sekwencją rzędu n nazywamy ciąg bitów wygenerowaną …” – literówka

str. 76, “… rejestr przesuwny o funkcji sprzężenia zwrotnego będącego następującą formą kwadratową.” – literówka

str. 77 i dalsze, “matryc programowalnych bramek logicznych FPGA” – proponuję zmienić na “układów programowalnych FPGA”

str. 78, “… metoda konstrukcji rejestrów przesuwnych o nieliniowych funkcjach sprzężenia zwrotnego konstrukcyjnie przy wykorzystaniu logarytmów Zecha” – niejasne

str. 81, "… iż wątki działające w ramach jednej osnowy powinny zawsze wykonywać tę samą instrukcje …" – literówka

str. 82, "W początkowej fazie projektu wykonać implementacje dedykowaną jednostkom procesorowym …" – literówka

str. 83 i kolejne, dla liczebników o wartościach od jeden do dziewięć, które odnoszą się do kontekstu pracy (oprócz np. numerów rozdziałów, stron) zaleca się używanie w treści pracy liczebników w formie słownej

str. 83, str. 84, "uśredniony czas badania 1 pełnego" – niejasne

str. 85, "co według wiedzy autora rozprawy jest osiągnięciem wcześniej lepszym" – niejasne

str. 89, "znacznie przewyższały" – nieprecyzyjne określenie

str. 90-97, pozycje bibliograficzne wymagają redakcji pod względem interpunkcyjnym

Przeprowadzone przez Doktoranta prace mają charakter badań podstawowych na przecięciu dziedzin: matematyki – teorii liczb i własności wielomianów, telekomunikacji i informatyki. Wyniki badań znajdują duże zastosowanie w badaniach przemysłowych z zakresu bezpieczeństwa informacji i kryptografii. Jak pokazał Autor rozprawy, badania dotyczące własności wielomianów oraz poszukiwania wielomianów o określonych własnościach są nadal prowadzone w zespołach naukowo-badawczych na świecie. Pozwala to tym bardziej wysoko ocenić rezultaty uzyskane przez Doktoranta, który w wyniku realizacji rozprawy doktorskiej zaproponował oryginalne i efektywne metody poszukiwania wielomianów nieprzywiedlnych, a ponadto stworzył użyteczne narzędzia komputerowego wspomagania poszukiwania takich wielomianów. Mając na uwadze, że otrzymane przez Doktoranta wyniki w sposób znaczący mogą przyczynić się do poprawy wielu algorytmów ochrony informacji oraz istotnie poprawiają rezultaty osiągnięte i opublikowane w literaturze światowej, zachęcam Autora rozprawy do publikacji tych wyników w czasopismach o szerokim zasięgu.

Rozprawę mgr. inż. Pawła Jacka Augustynowicza oceniam jako wybitnie dobrą, zasługującą na wyróżnienie. Autor rozprawy wykazał się dogłębną wiedzą z zakresu zagadnień, które uczynił przedmiotem dociekań naukowych. Rozwiązał nietrywialne, aktualne i ważne technicznie problemy naukowe, użyteczne praktycznie i wszystko dobrze udokumentował. Wykazał się przy tym inicjatywą twórczą, umiejętnościami rozwiązywania złożonych problemów, bardzo dobrym opanowaniem warsztatu badawczego i przygotowaniem do samodzielnego prowadzenia badań naukowych. Uważam, że przedstawiona do recenzji praca mgr. inż. Pawła J. Augustynowicza pt.: „Efektywne badanie nieprzywiedlności wielomianów binarnych o szczególnych postaciach" spełnia z nadmiarem wymagania postanowień aktualnie obowiązującej „Ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki". Dlatego wnoszę o przyjęcie recenzowanej pracy jako rozprawy doktorskiej i dopuszczenie jej Autora do dalszych etapów przewodu doktorskiego. Jednocześnie, uwzględniając doniosłość uzyskanych rezultatów teoretycznych i praktycznych oraz formę ich udokumentowania, wnioskuję o wyróżnienie tej rozprawy.