Trinity College
HARTFORD CONNECTICUT

RECENZJA ROZPRAWY DOKTORSKIEJ

Autor rozprawy: mgr inż. Krzysztof Mańk
Tytuł rozprawy: *Pakiet testów losowości do badania prymitywów kryptograficznych*
Promotor: dr hab. inż. Marek Kojdecki, prof. WAT
Promotor pomocniczy: dr inż. Michał Wroński
Jednostka: Wydział Cybernetyki, Wojskowa Akademia Techniczna

Recenzent: Ewa Syta, Charles A. Dana Research Associate Professor and Chair of Computer Science
Stopień naukowy: Ph.D.
Afiliacja: Trinity College, Hartford, CT, USA
Data sporządzenia recenzji: 6 października 2025

1. Wymogi prawne

Zgodnie z art. 13 ust. 1 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki, rozprawa doktorska przygotowana pod opieką promotora powinna stanowić oryginalne rozwiązanie problemu naukowego oraz wykazywać ogólną wiedzę doktoranta w danej dyscyplinie naukowej, a także umiejętność samodzielnego prowadzenia pracy naukowej.

Recenzja rozprawy doktorskiej, zgodnie z §6 ust. 4 rozporządzenia MNiSW z dnia 19 stycznia 2018 r. w sprawie szczegółowego trybu przeprowadzania czynności w przewodach doktorskim i habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora, powinna zawierać szczegółowo uzasadnioną ocenę, czy rozprawa ta spełnia warunki określone w art. 13 cytowanej ustawy.

2. Tematyka rozprawy

Przedmiotem rozprawy doktorskiej *"Pakiet testów losowości do badania prymitywów kryptograficznych"* jest opracowanie metody konstrukcji pakietu testów statystycznych służących do oceny losowości prymitywów kryptograficznych, w szczególności generatorów liczb losowych i pseudolosowych. Autor podejmuje próbę formalnego uporządkowania i oceny istniejących testów losowości oraz metod ich łączenia w zintegrowane pakiety.

COMPUTER SCIENCE DEPARTMENT
300 SUMMIT STREET, HARTFORD, CT 06106-3100
TEL (860) 297-2517 FAX (860) 297-2531 www.trincoll.edu

Celem pracy jest określenie zbioru testów oraz odpowiadających im parametrów, które pozwalają uzyskać zestaw charakteryzujący się poprawnością statystyczną wyników, ograniczoną nadmiarowością oraz kontrolowaną korelacją pomiędzy testami. Proponowane podejście zakłada wykorzystanie wielostopniowej procedury weryfikacyjnej, obejmującej zarówno ocenę pojedynczych testów, jak i analizę ich wzajemnych zależności.

W rozprawie autor analizuje szereg istniejących pakietów testowych, w tym Knuth, DIEHARD, NIST SP 800-22, TestU01, Dieharder i Crypt-X, zestawiając ich strukturę i zastosowane procedury. Na tle tych rozwiązań przedstawia własny sposób selekcji i walidacji testów, a także kryteria pozwalające na ograniczenie liczby testów przy zachowaniu szerokiego zakresu diagnostycznego. Praca ma charakter metodologiczno-analityczny, a jej rezultatem jest opis procedury konstrukcji i oceny pakietu testowego, który może stanowić podstawę do implementacji narzędzia wspierającego badania nad losowością w kontekście kryptograficznym.

3. Zawartość pracy

Przedstawiona rozprawa podzielona została na 8 rozdziałów, w tym wstęp i podsumowanie oraz dwa załączniki.

Rozdział I zawiera wprowadzenie do tematyki testowania losowości oraz ogólną charakterystykę testów statystycznych stosowanych do oceny generatorów liczb losowych i pseudolosowych. W końcowej części rozdziału autor formułuje cel i zakres pracy.

Rozdziały II i III stanowią przegląd i klasyfikację istniejących testów oraz ogólnodostępnych pakietów testowych, takich jak Knuth, DIEHARD, NIST SP 800-22, TestU01 czy Dieharder. Opracowanie ma charakter kompendium, w którym autor przedstawia podstawy teoretyczne poszczególnych testów, ich interpretację oraz ograniczenia praktyczne. W kilku miejscach wprowadza także własne uwagi i drobne analizy porównawcze dotyczące skuteczności i redundancji testów, zwłaszcza w odniesieniu do pakietów NIST STS i Dieharder.

Rozdział IV dotyczy wyboru źródeł danych oraz sposobu ich przekształcenia na potrzeby analiz statystycznych. Opisano w nim procedurę generowania ciągów testowych oraz test badania równomierności rozkładu na przedziale $[0; 1]$, który został następnie wykorzystany jako punkt odniesienia w ocenie poprawności innych testów.

W rozdziale V autor przedstawia wielostopniową procedurę oceny testów losowości, obejmującą m.in. weryfikację ich stabilności, porównanie wyników dla różnych długości ciągów oraz analizę zgodności rozkładów wartości p. Rozdział kończy podsumowanie wyników i wskazanie testów spełniających przyjęte kryteria wiarygodności. Szczegółowe wyniki, o charakterze wyliczeniowym i obejmujące liczne zestawienia tabelaryczne, zostały przedstawione w załącznikach A i B, liczących łącznie około 100 stron. Dane te stanowią podstawę empiryczną do oceny wiarygodności testów, choć ich pełna weryfikacja wymagałaby dostępu do środowiska obliczeniowego autora.

Rozdział VI poświęcony jest analizie współzależności pomiędzy testami zakwalifikowanymi

do dalszego wykorzystania. Autor przedstawia metody i wyniki badań korelacyjnych, obejmujących analizy liniowe, nieliniowe i wielowymiarowe, których celem było ograniczenie liczby testów przy zachowaniu ich diagnostycznej różnorodności oraz wskazanie zestawu rekomendowanego do implementacji w projektowanym pakiecie.

Ostatnie rozdziały (VII–VIII) zawierają podsumowanie uzyskanych wyników, omówienie ograniczeń opracowanej metody oraz wskazania kierunków dalszych prac.

4. Ocena merytoryczna pracy

Rozprawa jest obszerna, lecz przejrzyście zorganizowana, co ułatwia śledzenie toku rozumowania autora i odnajdywanie kluczowych fragmentów. Struktura pracy odpowiada logicznemu porządkowi działań badawczych: od przeglądu literatury, przez analizę istniejących pakietów testowych, po opracowanie własnych procedur weryfikacyjnych i analizę wyników.

Rozdziały II i III świadczą o gruntownym i krytycznym przeglądzie literatury dotyczącej testowania losowości ciągów liczbowych i binarnych. Autor zestawia klasyczne i nowoczesne pakiety testowe, w tym Knuth, DIEHARD, NIST SP 800-22, TestU01, Dieharder i CryptX, wskazując ich ograniczenia i obszary możliwego usprawnienia. W kilku przypadkach przedstawia także własne uzupełniające obliczenia lub interpretacje, mające znaczenie dla porównania efektywności testów. Część tych wyników została zaprezentowana w publikacjach i na konferencjach naukowych.

Wspierając się ugruntowanym aparatem statystycznym, autor wykazał eksperymentalnie, że część testów, które weszły w skład dostępnych pakietów losowości, nie powinna była się tam znaleźć, choć temu aspektowi poświęcił zbyt mało miejsca. Przeprowadzone analizy sugerują również, że możliwe jest rozszerzenie zbioru testów poza zestawy standardowe, takie jak NIST STS czy Dieharder, przy jednoczesnym utrzymaniu spójności metodologicznej.

Uzyskane wyniki stanowią uporządkowany materiał porównawczy i mogą służyć jako podstawa do dalszych badań nad optymalizacją pakietów testowych oraz nad metodami oceny prymitywów kryptograficznych. Praca jest starannie przygotowana pod względem redakcyjnym i technicznym, a opis procedur i rezultatów jest wystarczająco szczegółowy, aby umożliwić zrozumienie zastosowanej metodyki.

5. Uwagi krytyczne

Rozprawa jest poprawna pod względem strukturalnym i językowym, jednak można wskazać kilka elementów wymagających doprecyzowania lub rozwinięcia.

Głównym zastrzeżeniem wobec przedstawionej rozprawy jest fakt, że pozostaje ona poza głównym nurtem współczesnych badań w dziedzinie kryptologii, co skutkuje ograniczonym zakresem literatury z ostatniej dekady oraz brakiem odniesień do najnowszych publikacji autora. Szersze uwzględnienie współczesnych źródeł mogłoby wzmocnić kontekst teoretyczny pracy.

W rozprawie brakuje szczegółowych informacji dotyczących oprogramowania powstałego w ramach realizacji badań. Dopiero w podsumowaniu pojawia się wzmianka o pakiecie *TeStat*, jednak dane mają charakter głównie statystyczny, a nie dokumentacyjny. Nie zostało również jasno określone, jakie dodatkowe oprogramowanie wykorzystano (np. Statistica, pakiet R), ani jakie narzędzia posłużyły do realizacji testów opisanych w punktach IV.3, V.1.1, VI.1.1 oraz w analizie metody Hellwiga. Na podstawie informacji zawartych na stronie 180 można stwierdzić, że nie przeprowadzono pełnego przeglądu przestrzeni rozwiązań w tej metodzie, gdyż w jednym z przypadków miałaby ona rozmiar 2^{538}.

Na stronie 154 brakuje wyjaśnienia sposobu obliczania prawdopodobieństw zaprezentowanych na rysunkach VI.4–VI.6. Nie przedstawiono również uzasadnienia przyjętej wartości 0,001 jako prawdopodobieństwa nieprzejścia testu równomierności przez procedurę skorelowaną. Podobnych arbitralnych decyzji można wskazać w pracy kilka, bez wystarczającego omówienia ich wpływu na wyniki:

- w rozdziale IV: długości ciągów użytych podczas weryfikacji generatorów i testów,
- w rozdziale V: długości ciągów rozpatrywanych w testach pierwszego poziomu oraz zestawy parametrów tych testów (przesunięcia, długości bloków itp.), liczby powtórzeń testów pierwszego poziomu i poziomy istotności w testach trzeciego poziomu,
- w rozdziale VI: poziomy istotności w testach korelacyjnych, kryteria przejścia do modelu liniowego oraz długości korelowanych wektorów.

W rozdziale V autor odnosi uzyskane wyniki do zawartości pakietu STS, jednak zabrakło analogicznego porównania w odniesieniu do pozostałych pakietów omówionych w rozdziale III oraz zestawienia wyników przedstawionych w rozdziale VI.

Praca została napisana poprawnym i spójnym językiem, z dużą starannością redakcyjną. Autor unika błędów ortograficznych i gramatycznych, jednak częste stosowanie zdań wielokrotnie złożonych utrudnia miejscami odbiór treści. Układ rozdziału II jest miejscami niejednolity, co utrudnia orientację w prezentowanym materiale. Przykładowo, warianty testu autokorelacyjnego występują w punktach 2.4, 2.5 i 2.28, natomiast niektóre grupy testów są rozwinięte w podpunktach czwartego poziomu (np. testy momentów), podczas gdy inne (np. testy odstępów) pozostają bez analogicznego podziału.

6. Przydatność rozprawy dla nauk inżynieryjno-technicznych

Część analityczna rozprawy może, po wprowadzeniu poprawek redakcyjnych, zostać przekształcona w skrypt wprowadzający do zagadnień testowania losowości.

Zaproponowane w punktach 5 załączników A i B zestawy procedur mogą stanowić podstawę do opracowania metod badania generatorów pod kątem losowości wytwarzanych przy ich pomocy ciągów binarnych. W celu uzyskania szerszego niż lokalny zasięgu warto rozważyć opublikowanie raportu w języku angielskim streszczającego główne wyniki rozprawy.

7. Podsumowanie

Rozprawa mgr inż. Krzysztofa Mańka pt. *„Pakiet testów losowości do badania prymitywów kryptograficznych”* jest pracą obszerną, wymagającą i metodycznie dobrze opracowaną. Autor wykazał się dużą wiedzą z zakresu statystyki, metod testowania losowości oraz znajomością narzędzi analizy empirycznej. Pomimo uwag krytycznych, praca spełnia wymagania określone w art. 13 ustawy o stopniach naukowych i tytule naukowym.

Wnoszę o dopuszczenie autora do publicznej obrony rozprawy doktorskiej.

Ewa Syta, Ph.D.
Associate Professor and Chair of Computer Science