Prof. dr hab. inż. Olgierd Hryniewicz

Instytut Badań Systemowych PAN, Warszawa

Warszawa, 2025-09-01

RECENZJA

rozprawy doktorskiej mgr. inż. Piotra Jóźwiaka

nt. „ Zastosowanie probabilistycznych metod do oceny losowości liczb otrzymanych z kwantowych generatorów liczb losowych"

Niniejsza recenzja została opracowana na prośbę JM Rektora Politechniki Opolskiej dr. hab. inż. Marcina Lorenca, przekazaną pismem z dn. 15.07.2025.

1. Opis zawartości rozprawy

Recenzowana rozprawa została wykonana pod kierunkiem dr. hab. inż. Krzysztofa Zatwarnickiego, profesora Politechniki Opolskiej, jako promotora oraz dr. hab. inż. Witolda Jacaka, profesora Politechniki Wrocławskiej, jako drugiego promotora. Jej Autor, mgr inż. Piotr Jóźwiak (zwany dalej: Doktorantem) jest pracownikiem Politechniki Wrocławskiej.

Rozprawa została napisana w języku polskim i ma postać rękopisu liczącego 204 str. Składa się ze Wstępu, siedmiu zasadniczych rozdziałów, stanowiącego podsumowanie rozprawy Zakończenia oraz bibliografii liczącej 171 pozycji. Cel pracy jest złożony i zgodnie z deklaracją Doktoranta można podzielić go na dwie części: **„Opracowanie metody oceny losowości kwantowego generatora liczb losowych wykorzystującego splątanie kwantowe qubitów"** oraz **„Określenie czy aktualnie stosowane algorytmy statystyczne są wystarczające oraz odpowiednie do badania kwantowych generatorów liczb losowych jako odrębnej klasy generatorów".** Określony przez Doktoranta powyższy cel pracy został osiągnięty przez realizację ośmiu zadań szczegółowych wymienionych we Wstępie do rozprawy.

Problem generacji liczb losowych jest znany od blisko osiemdziesięciu lat (metody Monte Carlo). Wykorzystywano do tego celu zarówno pomiary fizyczne (np. rozpadu promieniotwórczego), obserwacje rzeczywistych procesów mających w powszechnym odczuciu charakter losowy oraz algorytmy wyznaczające ciągi liczb losowych w sposób deterministyczny. W tym ostatnim przypadku uzyskiwane ciągi liczb nazywane są ciągami liczb pseudo-losowych. Istotną cechą liczb losowych jest brak możliwości przewidzenia ich przyszłych wartości (jest to „operacyjna" definicja losowości, zaproponowana przez von Misesa). Warunku tego, z oczywistych powodów, nie spełniają liczby pseudo-losowe. Opracowano jednak generatory takich liczb, w przypadku których identyfikacja algorytmu ich wyznaczania jest niezmiernie trudna, a w praktyce, przy wykorzystaniu klasycznych środków

obliczeniowych, niemożliwa. Sytuacja ta jest akceptowalna w przypadku wykorzystania generatorów liczb pseudo-losowych w klasycznych zadaniach symulacji komputerowej. Sytuacja ta może ulec zmianie, gdy do analizy ciągów liczb traktowanych jako ciągi liczb losowych i wykorzystywanych w zadaniach kryptografii zostaną użyte komputery kwantowe. W takim przypadku stanie się koniecznym wykorzystanie liczb rzeczywiście losowych, do których generacji można wykorzystać efekty kwantowe. Zgodnie z aktualnym stanem wiedzy, efekty kwantowe pozwalają uzyskać ciągi liczb idealnie losowych. Jednakże fizyczna implementacja generatorów kwantowych może wprowadzać dodatkowe efekty o charakterze deterministycznym. W rezultacie konieczne jest opracowanie metod weryfikacji jakości takich rzeczywistych generatorów, czemu poświęcona jest recenzowana rozprawa.

Recenzowaną rozprawę doktorską mgr. inż. Piotra Jóźwiaka można podzielić na trzy zasadnicze części. Rozprawę rozpoczyna rozbudowany Wstęp, w którego pierwszej części Doktorant wprowadza czytelnika do problemu generacji ciągów liczb losowych z wykorzystaniem zarówno liczb pseudo-losowych (deterministycznych) jak i czysto losowych (bazujących na zaobserwowanych zjawiskach kwantowych). Następnie przedstawione zostały ogólne i szczegółowe cele pracy oraz w sposób skrótowy omówiono jej zawartość.

Pierwsza z wymienionych powyżej części rozprawy, składająca się z jej trzech pierwszych rozdziałów, ma charakter wstępu do omawianej problematyki, mającego charakter rozbudowanego przeglądu literatury. W pierwszym rozdziale przedstawiono wyniki teoretycznych rozważań dotyczących pojęcia losowości. Przedstawiono rezultaty prac twórców nowoczesnej probabilistyki (von Misesa, Kołmogorowa), a także wyniki najnowszych badań (wykorzystano tu wyniki prac pochodzącego z Rosji wybitnego matematyka Khrennikova). Drugi rozdział pracy poświęcony jest omówieniu klasycznej i kwantowej teorii informacji. W szczególności omówiono zagadnienie kwantowej informacji, której zrozumienie jest niezbędne w analizie kwantowych generatorów liczb losowych. Trzeci rozdział pracy poświęcony jest wprowadzeniu do zagadnienia tworzenia generatorów liczb losowych oraz metod weryfikacji wyników ich działania.

Druga część pracy poświęcona została analizie statystycznej generatorów liczb losowych z wykorzystaniem stanowiącego obecnie nieformalny standard międzynarodowy zestawu testów statystycznych (zwanego baterią testów) opracowanego i oprogramowanego w amerykańskim instytucie standaryzacyjnym NIST. Ta część pracy składa się z dwu rozdziałów, z których rozdział czwarty oparty jest na raporcie amerykańskiego instytutu standaryzacyjnego NIST, w którym opisano wspomniany powyżej zestaw testów statystycznych wykorzystywanych do analizy ciągów generowanych zero-jedynkowych liczb losowych. Zestaw testów opracowanych i oprogramowanych w NIST jest obecnie powszechnie przyjętym standardem wykorzystywanym do certyfikacji stosowanych w praktyce generatorów. Osobistym wkładem Doktoranta jest uwzględnienie w opisie baterii testów NIST wyników najnowszych badań teoretycznych, w których poddano krytyce niektóre z proponowanych przez NIST rozwiązań.

Piąty rozdział rozprawy poświęcony jest opisowi wyników przeprowadzonego przez Doktoranta dużego eksperymentu, w którym wykorzystano zestaw testów NIST do

empirycznej weryfikacji jakości działania dwu generatorów kwantowych liczb losowych. Pierwszy z badanych generatorów (JUR02), wykorzystujący efekty kwantowe obserwowane w złączach półprzewodnikowych, został opracowany w Narodowym Laboratorium Technologii Kwantowych Politechniki Wrocławskiej, którego pracownikiem jest mgr inż. Piotr Jóźwiak. Ma on postać zminiaturyzowanego urządzenia, które może być wykorzystywane w praktyce kryptograficznej. Drugi z badanych generatorów (EPR S405 Quelle) jest opracowanym w Austrii zestawem wykorzystującym do generacji kwantowych liczb losowych zjawisko splątania kwantowego fotonów. Przeprowadzone eksperymenty potwierdziły przydatność zestawu testów NIST do badania generowanych przez te generatory sprzętowe ciągów liczb losowych, a w szczególności zgodność wygenerowanych przez oba generatory zestawów liczb losowych z kryteriami losowości określonymi w standardzie NIST. Opracowanie i wdrożenie generatora JUR02 może być interpretowane świetle treści Art.187 Ustawy „Prawo o szkolnictwie wyższym i nauce" w jego części dotyczącej warunków jakie musi spełniać rozprawa doktorska („praca projektowa, konstrukcyjna, technologiczna, wdrożeniowa"). Mgr. inż. Piotr Jóźwiak nie jest zapewne głównym autorem tego osiągnięcia, ale jest współautorem artykułów, w których zostało ono opisane. Można więc uznać, że jego udział w opracowaniu i wdrożeniu tego nowatorskiego urządzenia, a w szczególności w przeprowadzeniu badań eksperymentalnych weryfikujących poprawność jego działania i opisanych w rozdziale 5 rozprawy doktorskiej był udziałem istotnym. Można to, moim zdaniem, uznać za jego oryginalne osiągnięcie naukowo-techniczne uwzględniane w ocenie rozprawy doktorskiej.

W trzeciej części rozprawy, obejmującej rozdziały 5.5, 5.6, 6 oraz 7, zawarte są najważniejsze indywidualne osiągnięcia Doktoranta. W rozdz. 5.5 Doktorant przedstawił oryginalną analizę krytyczną zaobserwowanej anomalii w działaniu algorytmu NIST realizującego test nienakładających się wzorców. Wyniki tej analizy zostały opublikowane w materiałach ważnej konferencji międzynarodowej. Ponadto został zaproponowany pomysłowy sposób symulacyjnego badania wykrywalności deterministycznych dalekozasięgowych korelacji. Wyniki przeprowadzonych eksperymentów, a także wyciągnięte z ich analizy wnioski, mogą mieć istotne znaczenie w ocenie jakości kwantowych generatorów liczb losowych. Rozdział 6 rozprawy zawiera opis oryginalnej metody statystycznej weryfikacji niezwykle istotnej w ocenie kwantowych generatorów liczb losowych nierówności Bella-CHSH. W zaproponowanym rozwiązaniu Doktorant wykorzystał opracowany przez siebie programowy symulator kwantowej generacji liczb losowych, a także zaproponował pewną miarę określającą jakość kwantowych generatorów liczb losowych wykorzystujących efekt splątania kwantowego. W szczególności, Doktorant zaproponował wykorzystanie znanych testów statystycznych (test normalności, test permutacyjny) do weryfikacji hipotez o występowaniu efektu splątania w rzeczywistych generatorach, co ma, moim zdaniem, duże znaczenie praktyczne. W ostatnim, siódmym, rozdziale pracy doktorant przedstawia wyniki pracy współautorskiej, w której zaproponowano protokół kryptograficzny z publiczną weryfikacją losowości. Kompetencje autora niniejszej recenzji nie pozwalają mu ocenić wagi tego rezultatu, jednakże fakt jego opublikowania w liczącym się czasopiśmie (100 pkt. na liście MNiSW) oraz to, że Doktorant jest jego pierwszym autorem, a lista autorów nie jest listą

alfabetyczną, wskazuje na to, że uzyskany wynik naukowy w istotny sposób wzbogaca dorobek naukowy Doktoranta, a w tym jego rozprawę doktorską.

4. Ocena rozprawy – uwagi krytyczne i dyskusyjne

Oceniając całość recenzowanej rozprawy mgr. inż. Piotra Jóźwiaka należy uznać, że określone w jej Wstępie zadania badawcze zostały zrealizowane. Rozprawa zawiera wyniki istotnych dla praktyki badań eksperymentalnych oraz wyniki oryginalnych krytycznych analiz dotyczących weryfikacji jakości działania kwantowych generatorów liczb losowych. Zawiera więc ona wyniki naukowe upoważniające niniejszego recenzenta do sformułowania jej pozytywnej oceny,

Lektura recenzowanej rozprawy nasuwa jednak szereg przedstawionych poniżej uwag o charakterze krytycznym i dyskusyjnym.

Podstawowa uwaga dotyczy interpretacji wyników wszystkich eksperymentów z wykorzystaniem pojęcia *p-value*. W polskiej terminologii statystycznej nie ma powszechnie przyjętego odpowiednika tego terminu; stosuje się np. nazwę „istotność" (nie mylić z „poziomem istotności"). Pojęcie to jest powszechnie stosowane w praktyce stosowania testów statystycznych, a w obszarze prezentacji wyników analiz badań medycznych jest wręcz standardem. Jest też ono stosowane w raporcie NIST. Występują niestety istotne problemy z jego interpretacją. Na przykład, na pewno nie jest to prawdopodobieństwo prawdziwości testowanej hipotezy statystycznej. W rzeczywistości jest to największa wartość poziomu istotności testu statystycznego, który dla zaobserwowanych danych nie wskazuje na konieczność odrzucenia testowanej hipotezy statystycznej. Jest to więc własność konkretnej statystyki, a nie charakteru opisywanych przez tę statystykę danych. W związku z tym przyjęcie pewnej hipotezy statystycznej nie musi świadczyć o losowości analizowanych danych (jest to stwierdzenie spełnienia warunku koniecznego, a niekoniecznie wystarczającego), co sugeruje interpretacja stosowana w raporcie NIST. Zwrócił na to uwagę Doktorant, opisując w rozdz.4 test monobitowy. Istotną własnością charakterystyki *p-value* jest to, że w przypadku słuszności weryfikowanej hipotezy statystycznej jest to realizacja zmiennej losowej o rozkładzie równomiernym na przedziale [0,1]. W praktyce oznacza to, że w przypadku powtarzanych wielu niezależnych eksperymentów i odpowiadającym testowanej hipotezie statystycznej rozkładzie prawdopodobieństwa stosowanej statystyki testowej zaobserwowane w tych eksperymentach wartości *p-value* opisane są rozkładem równomiernym. Wydaje się, że niespełnienie powyższych warunków mogło być powodem zaobserwowanych przez Doktoranta anomalii.

Takie anomalie zaobserwował Doktorant analizując w rozdz. 5 wyniki działania znajdującego się w zestawie testów NIST testu występowania nienakładających się wzorców. Po przeprowadzeniu dogłębnej analizy doszedł on do słusznego wniosku, że powód występowania zaobserwowanych anomalii jest związany z zalecanym przez NIST algorytmem obliczeniowym i zaproponował konkretne ograniczenie określające zakres stosowalności tego testu. Możliwym jednak powodem jest wskazany w cytowanej przez Doktoranta pracy Iwasakiego problem z wyznaczeniem rozkładu prawdopodobieństwa

testowanej statystyki, który pojawia się w praktyce dopiero w przypadku długich wzorców. Ten sam problem może wystąpić w przypadku testu występowania nakładających się wzorców, w przypadku którego postać stosowanego przez NIST rozkładu statystyki testowej została zakwestionowana w cytowanej przez Doktoranta pracy Hamano i Kaneko.

Pewien problem z interpretacją wyników przeprowadzonych eksperymentów pojawia się natomiast w rozdziale 5.4.7. Obserwowana w Tab.5.2 wyraźnie zwiększona liczba negatywnych przypadków dla m=15 nie musi być wynikiem błędnego działania algorytmu, ale zwiększonej liczby rozpatrywanych konfiguracji; procent przypadków pozytywnych nie odbiega tu od oczekiwanej przy założeniu słuszności testowanej hipotezy wartości 99%. Również zaobserwowane na Rys. 5.24-5.25 nierównomierności dadzą się prosto wytłumaczyć niedużą liczbą (np. 48) rozpatrywanych wzorców. Natomiast histogram przedstawiony na Rys.5.26 wskazuje na niezgodność z rozkładem równomiernym, co może być różnie interpretowane. Zastanawia jednak pewna niezgodność tego histogramu z danymi przedstawionymi w Tab.5.2, gdzie liczba zaobserwowanych przypadków negatywnych nie przeczy założeniu o równomierności rozkładu zaobserwowanych wartości *p-value*. Ta przypuszczalna niezgodność wymaga jakiegoś wyjaśnienia.

Wątpliwości budzi też prezentacja wyników opisanych w rozdziale 5.5.3. Jak wiadomo, rozkład wartości *p-value* nie zależy od przyjętego poziomu istotności. Tymczasem w Tab.5.7, w jej części dotyczącej Próbki 1 i rozkładu *P-value* mamy dwie kolumny wartości. Powstaje więc np. pytanie, co te różne wartości oznaczają dla przypadku dotyczącego częstości monobitów w bloku. Test ten jest przecież uogólnieniem testu częstości monobitów, dla którego w Tab.5.7 podano tylko jedną wartość?

Jeśli chodzi o ocenę technicznego aspektu prezentacji recenzowanej rozprawy, to zauważono niewiele drobnych niedociągnięć (np. „literówek"). Jedynym istotnym niedociągnięciem jest brak zdefiniowania (choćby przez podanie odnośników do innych fragmentów rozprawy) wzoru (6.1). Wygląda na to, że został on przekopiowany z będącej autorstwa Doktoranta pracy [101], w której korzystano z innych oznaczeń występujących w tym wzorze wielkości.

Podsumowując powyższą ocenę należy podkreślić, że część podniesionych wątpliwości jest konsekwencją inherentnych problemów związanych z interpretowalnością wskaźnika *p-value*, a odnoszące się do tego uwagi mają charakter dyskusyjny. Również uwagi dotyczące sposobu wyjaśnienia zaobserwowanych anomalii należy traktować nie jako zarzut, ale jako wskazania możliwości prowadzenia dalszych badań.

3. Ocena końcowa

Przedstawiona do recenzji rozprawa doktorska mgr. inż. Piotra Jóźwiaka zawiera niewątpliwie szereg oryginalnych wyników naukowych o charakterze aplikacyjnym i teoretycznym, co jest podstawowym wymogiem stawianym rozprawom doktorskim. Przeprowadzone szerokie eksperymenty i analizy dostarczyły cennych wskazówek dotyczących projektowania badań jakości kwantowych generatorów liczb losowych. Na pozytywną ocenę zasługuje praktyczna weryfikacja zaproponowanego podejścia dla przypadku dwu konkretnych kwantowych generatorów liczb losowych, a zwłaszcza

generatora JUR02, będącego oryginalnym osiągnięciem technicznym. Sformułowane w recenzji uwagi o charakterze polemicznym, a także krytycznym, nie zmniejszają wartości zawartych w rozprawie oryginalnych wyników Doktoranta.

Dokonując całościowej oceny rozprawy, po uwzględnieniu jej zalet i nielicznych wad, można stwierdzić, że spełnia ona wymagania stawiane w odpowiednich przepisach rozprawom doktorskim w zakresie informatyki technicznej i telekomunikacji. W związku z tym wnoszę o dopuszczenie mgr. inż. Piotra Jóźwiaka do dalszych, przewidzianych przepisami, etapów przewodu doktorskiego.

Prof. dr hab. inż. Olgierd Hryniewicz