Dr hab. Inż. Jan kałuski
Ul.Kochanowskiego 27A/9
44-100 Gliwice

Gliwice, 11.10. 2025r.

RECENZJA

Pracy doktorskiej Pana mgr inż. Piotra Jóźwiaka
p.t." *Zastosowanie probabilistycznych metod do oceny losowości liczb otrzymanych z kwantowych generatorów liczb losowych",*

przygotowanej pod kierunkiem naukowym dr hab.inż. Krzysztofa Zatwarnickiego i dr hab.inż. Witolda Jacaka.

Celem sporządzonej recenzji jest odpowiedź na następujące pytania:
--czy przedłożona rozprawa doktorska prezentuje ogólną wiedzę teoretyczną kandydata oraz umiejętność samodzielnego prowadzenia pracy naukowo- badawczej?
-- czy przedmiotem rozprawy jest oryginalne rozwiązanie problem naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w dziedzinie informatyki kwantowej, kryptografii i pokrewnych dziedzinach.

W celu uzyskania odpowiedzi na powyższe pytania ocenie poddano w szczególności:
- konstrukcję pracy oraz sposób prezentowania wywodu naukowego,
- rozeznanie stanu wiedzy i umiejętność krytycznej analizy prezentowanych teorii
- oryginalność i znaczenie problemu badawczego,
- kompletność i poprawność sformułowania celów pracy,
- poprawność budowy i poziom weryfikacji hipotez i zadań badawczych,
- oryginalność, trafność i poprawność wykorzystania metod i narzędzi i zadań badawczych.

1. Konstrukcja pracy oraz sposób prowadzenia wywodu naukowego

Rozprawa doktorska mgr inż. Piotra Jóźwiaka dotyczy zastosowań probabilistycznych i statystycznych metod do oceny generowanych z generatorów kwantowych liczb losowych i obejmuje szeroki zakres tematyczny związany z:

-- mechaniką kwantową,
--teorią prawdopodobieństwa i statystyką matematyczną,
--informatyką klasyczną i kwantową i w głównej mierze
--kwantowymi generatorami ciągów liczb losowych.

Tematyka ta w sposób bardzo precyzyjny i spójny jest przedstawiona w pracy w formie pisemnej, liczącej 204 strony w tym; 69 rysunków, 22 tabele oraz 7 listingów. Spis cytowanej literatury wynosi 171 pozycji. Praca pisemna zawiera *Wstęp* (8 stron) i 7 rozdziałów o objętościach odpowiednio po (21, 16, 3, 42, 60, 20 i 7 stron) oraz 5 cio-stronicowego zakończenia.

Od razu chciałbym zaznaczyć, że dysproporcja w objętościach stron dla poszczególnych rozdziałów nie razi i według mojej opinii jest uzasadniona. Również sądzę, że w pracy zawarta jest gruntowna i potrzebna wiedza z informatyki i mechaniki kwantowej oraz probabilistyki i statystyki matematycznej i zastała w umiejętny sposób wykorzystana w pracy dla zbudowania wywodu naukowego, który to wywód, w całej pracy jest stosowany bardzo logicznie i prowadzi do precyzyjnego sformułowania celów pracy i zadań do wykonania.

2. Ocena tematu, celów pracy oraz innych założeń badawczych

Temat pracy, dotyczący oceny generatorów kwantowych liczb losowych jest dziś jednym z głównych i aktualnych technicznych i naukowych problemów we współczesnej informatyce, ze względu na coraz intensywniej wprowadzanych komputerów kwantowych. Wiąże się to z nowymi możliwościami w kryptografii, związanymi przede wszystkim z ułatwioną kompromitacją dotychczasowych zabezpieczeń. Ważnym więc w tym względzie, jest testowanie wzorców do celów kryptografii.

Stąd uważam, że temat rozprawy doktorskiej jest naukowo uzasadniony i jest nietrywialny. W związku z realizacją tematu pracy, dotyczącego weryfikacji i oceny losowości generatorów kwantowych liczb losowych, sformułowano dwa obszerne cele:

1. **Opracowanie metody oceny losowości kwantowego generatora liczb losowych, wykorzystując splątanie kwantowe qubitów.**

   Sformułowano w związku z tym zadania w postaci;

1a. Analiza korelacji fotonów otrzymanych w nierówności Bella- CHSH dla wyznaczania rozkładu prawdopodobieństwa związanej z tym statystyki testowej.

1b. Opracowanie miary dla kwantowych generatorów liczb losowych, wykorzystujących splątanie kwantowe, identyfikując w ten sposób kwantowe źródła entropii.

1c. Opracowanie testu statystycznego do oceny kwantowego generatora z wykorzystaniem korelacji Bella-CHSH ze splątania kwantowego odnośnie referencyjnego lub idealnego generatora.

1d. Opracowanie symulatora kwantowego generatora, w celu dostarczenia korelacji odpowiadających stanom czystym w danym układzie. Symulator taki powinien dostarczyć niezbędne dane referencyjne do opracowania właściwego testu statystycznego generatora liczb losowych.

Drugim, przystającym do pierwszego celu pracy było:

2. **Określenie czy aktualnie stosowane algorytmy statystyczne są wystarczające oraz odpowiednie do badania kwantowych generatorów liczb losowych jako odrębnej klasy generatorów.**

W związku z powyższym w pracy sformułowano następujące zadania;

2a. Analiza krytyczna aktualnie stosowanych testów statystycznych oraz ich parametrów celem wyznaczenia warunków testowych dostosowanych do testowania kwantowych źródeł losowości. Przeanalizowano baterię testów NIST STS jako szeroko stosowany standard do oceny losowości różnej klasy generatorów liczb losowych. Zauważa się brak prac weryfikujących jakość testów statystycznych losowości kwantowych generatorów liczb, które posiadają inne cechy statystyczne niż generatory pseudolosowe.

2.b. Przeprowadzenie testów statystycznych baterią NIST STS na ciągach liczb otrzymanych z kwantowych generatorów liczb losowych w poszukiwaniu niedoskonałości algorytmicznych i implementacyjnych samej baterii testów NIST STS.

2c. Weryfikacja wykrywalności daleko zasięgowych deterministycznych korelacji w sekwencjach losowych, jakie mogą teoretycznie występować w kwantowych generatorach liczb losowych.

2.d. Opracowanie metody generowania liczb losowych, pozwalającej pokonać wybrane ograniczenia aktualnie stosowanego podejścia do testowania kwantowych generatorów liczb losowych, wykorzystując mechanizmy mechaniki kwantowej w procesie testowania. Została przedstawiona nowa metoda

generowania liczb prawdziwie losowych w oparciu o wielosplątaniowe stany kwantowe qubitów (np. fotonów), umożliwiająca bezpieczną ocenę losowości w oparciu o publiczną weryfikację ciągów liczb.

Nie sposób, rzecz jasna, komentować i oceniać szczegółowo, punkt po punkcie, wszystkie przyjęte cele do realizacji w recenzowanej pracy doktorskiej, jest to bowiem, autonomiczne prawo Autora. Można tylko stwierdzić, że tak sformułowane cele główne i cząstkowe, jako zadania do realizacji, są spójne i ściśle korespondują z tematem ocenianej pracy doktorskiej.

Tym niemniej, pozwolę sobie w tym miejscu na potwierdzenie aktualności wszystkich zaproponowanych przez Autora rozprawy doktorskiej, celów i zadań do realizacji. W końcowej części mojej recenzji spróbują zwięźle podsumować główne osiągnięcia Doktoranta, w związku z tym.

Biorąc pod uwagę, że główną metodą badawczą w recenzowanej pracy jest zastosowanie modeli probabilistycznych i statystycznych, Autor zasadnie zaczyna od prezentacji tych modeli. Ta dziś już obszerna dziedzina wiedzy nie jest w pracy przedmiotem badań. Tworzy niezbędne narzędzia badawcze w postaci testów statystycznych. Niemniej ważną częścią pracy jest zastosowanie mechaniki kwantowej a w szczególności nierówności Bella-CHSH do prowadzenia istotnych badań w zakresie testowania generatorów kwantowych liczb losowych.

W związku narastającą mocą komputerów kwantowych i potrzebą testowania różnych źródeł generowania liczb losowych, po dziś dzień właściwie nie istnieje technika generowania takich liczb losowych. Obecnie używane algorytmy generowania liczb losowych a raczej pseudolosowych, dokonywane są z użyciem algorytmów deterministycznych. Stosowanie ich w kryptografii kwantowej jest wręcz niebezpieczne, gdyż mogą z łatwością być kompromitowane. Problemy te w pracy są dokładnie badane i tworzą ważną część realizacji postawionych celów i zadań z nich wynikających.

3. Wykorzystanie metod i narzędzi badawczych

Podstawowymi metodami użytymi w pracy do realizacji sformułowanych celów głównych i cząstkowych należą;

1) Metody statystyki matematycznej w zakresie weryfikacji hipotez statystycznych oraz
2) Metody mechaniki kwantowej w oparciu o efekty splątania kwantowego dwóch i większej liczby qubitów oraz nierówności Bella- CHSH.

Metody statystyczne to, przede wszystkim, różnego rodzaju testy statystyczne do weryfikacji hipotez o postaci rozkładu prawdopodobieństwa lub wartości określonego parametru ciągu liczb losowych. W pracy posłużono się gotowym zestawem baterii tes towej NIST STS, będącym zestawem testów opracowanych przez *National Institute of*

Standards and Technology (s.10) w odniesieniu do kwantowych źródeł liczb losowych. W sumie testów tych jest 15 i służą do weryfikacji hipotez statystycznych o postaci rozkładu teoretycznego badanej próbki losowej lub określonych jego parametrów.

W tym zakresie Autor zwięźle i dużą znajomością przedmiotu, przedstawił niezbędne informacje na temat każdego testu. Uważam, że Doktorant postąpił właściwie, gdyż w tym przypadku odwoływanie się do literatury przedmiotu, zubożyłoby pracę doktorską i nie pozwoliłoby należycie ocenić przygotowanie Autora w zakresie metod statystyki matematycznej a też i modeli probabilistycznych.

Autor słusznie zwrócił uwagę na to, że po dziś dzień nie istnieją testy statystyczne do weryfikacji hipotez o losowości ciągu liczb losowych otrzymywanych z generatorów kwantowych. Stąd używanie testów obecnie istniejących, powinno być w szczególny sposób uzasadnione, Aczkolwiek różnica między ciągami liczb pseudolosowych i losowych (tu Autor mówi o prawdziwie losowych – choć nie wiadomo co to oznacza?) otrzymanych z generatorów kwantowych jest czasami nieduża, co upoważnia Autora do stosowania baterii testów NIST STS. Gwoli sprawiedliwości i Jego wiedzy omawiane są również ograniczenia w stosowaniu tych testów w badaniu ciągów liczb losowych z generatorów kwantowych. Podstawowym ograniczeniem jest tu długość generowanego ciągu pseudolosowych liczb według algorytmów deterministycznych . Jednym z takich głównych ograniczeń jest stosunkowo mała wydajność tych generatorów a przez to niedużych długości ciągu liczb. Nieduże ciągi liczb, nie pozwalają na wykrycie deterministycznych okresowych zaburzeń. Przy tym należy zauważyć, że żaden z testów NIST STS nie był przystosowany do wykrywania tego typu zaburzeń. Stąd potrzeba konstrukcji nowych testów. Autor pracy to zauważa i proponuje nowe rozwiązania w tym zakresie (rozdz.5).

W dalszej kolejności (rozdz.6) Autor wykorzystuje właściwości splątania qubitów do budowy szczególnego rodzaju testów weryfikujących ciągi liczb losowych z generatorów kwantowych. Testy te jak i sam generator są oparte na właściwościach mechaniki kwantowej i dotyczą znanego faktu łamania nierówności Bella-CHSH.

W pracy, w związku z tym, w rozdz.6 opracowano symulator takiego kwantowego układu oraz permutacyjny test statystyczny oceniający splątaniowy kwantowy generator liczb losowych.

Warto tu podkreślić, że działanie testu statystycznego w tym przypadku dotyczy wyłącznie sposobu generowania liczb losowych na podstawie analizy korelacji i nierówności Bella-CHSH. W ten sposób Autor rozprawy w pkt. 6.2. pracy dochodzi do zasadniczego i ważnego wniosku praktycznego mianowicie, że teoretyczne testowanie kwantowych generatorów można sprowadzić do wykazania dowodu na kwantową naturę źródła losowości (s.163, rozdz.6.2).

A w związku z tym, że splątaniowy generator liczb losowych generuje tylko liczby losowe co nie wymaga jak by dodatkowego testowania tego strumienia na losowość! W praktyce oczywiście tak nie jest, gdyż trudno jest otrzymać czyste splątanie kwantowe nawet dwóch qubitów. Stąd propozycję metody do tego celu oparto o system ERP S403 Quelle.

Rys.6.2 i 6.3. wyraźnie pokazuje działanie takiego systemu i obrazuje złamanie nierówności Bella- CHSH. A więc jest to bezpośredni dowód, że generator splątaniowy generuje ciąg liczb losowych.

Osobną wartością w pracy, powiedziałbym dodaną, jest wykorzystanie testu permutacyjnego, pochodzącego jeszcze z lat 30-tych ubiegłego wieku, opracowanego przez R.A. Fishera i E.Pitmana. W pracy Autor używa tego testu, wykorzystując nierówność Bella- CHSH (pkt. 6.4.).

4. Uwagi formalne do pracy

Recenzowana praca została napisana wyjątkowo starannie. Strona redaktorska pracy nie budzi moich żadnych zastrzeżeń. Układ rysunków i tablic jest umieszczony w tekście logicznie i zgodnie z narracją prowadzoną przez Autora. Wrażenie z lektury pracy jest bardzo pozytywne.

Uwagi, które pragnę zamieścić w tym miejscu nie będą miały zasadniczego wpływu na pozytywną ocenę pracy, którą w konkluzji wyrażę w całej rozciągłości. Tym niemniej pewne zwroty, definicje i określenia budzą moją ciekawość. Dlatego prosiłbym Doktoranta podczas obrony pracy ustosunkowanie się do nich.

1) Strona 7. Co to są „liczby prawdziwie losowe"? Według mnie liczby mogą być: *losowe, pseudolosowe lub deterministyczne.*
2) Strona 11, środkowy akapit zakończenie: ...Test ten umożliwia ocenę splątaniowych generatorów liczb losowych względem idealnej realizacji". Co to oznacza?
3) Strona 13, rozdz.1. Co to oznacza, że losowość wywodzi się z j. niemieckiego!? Wszak *losowość* to określenie pewnej cechy, np. ciągu liczb! A więc, jeżeli mówimy już o języku, to słowo LOSOWOŚĆ jest wyrazem czysto polskim.

   Owszem, używane często w j.polskim słowo szacowanie (czyli ocenianie) jest pochodzenia niemieckiego (od niem. Schatzung/schätzen).

   A tak na marginesie w j.polskim używa się wiele różnych słów na określenie losowości. Np. Stochastyczny, randomizacja (albo przypadkowość).

4) Strona 37. Tak naprawdę nie wiadomo z czym jest związane splątanie kwantowe! Natomiast MODELOWANE ONO jest liniową przestrzenią Hilberta i iloczynem tenzorowym odpowiednich wielkości. Stąd co to oznacza, że:" ...Pochodzenie splątania ma czysto matematyczne podstawy"?! Jest to wszak, proces czysto fizyczny, należący do fizyki kwantowej.

5) Strona 49. Co to oznacza „... fundamentalnie deterministyczne..." ?

6) Strona 119. (pod rys.5.22). Co to znaczy równomierny rozkład Poissone'a? Rozkład jest albo równomierny albo Poissone'a.

7) Strony 109,127,129,134,135,137 i 138. Na powyższych stronach, wyróżnionych przeze mnie, zamieszczono wartości P*value* oraz (delta alfa). Aż się prosi umieścić te wartości w odpowiednich tablicach! Chociażby dla łatwiejszego powoływania się na skądinąd ważne eksperymentalne wyniki badań.

8) Brak porządku alfabetycznego w spisie cytowanej literatury. I chociaż dziś to obserwuje się nagminnie, szczególnie w spisach literatury w publikacjach obcojęzycznych to jednak, moim zdaniem, alfabetyczny spis cytowanej literatury umożliwia szybki dostęp do odpowiedniej pozycji literatury. Szczególnie, gdy spis cytowane literatury jest duży.

9) Strona 172. Mówi się *Rozkład jednostronnie lub obustronnie* ***Uciety.***

10) Strona 198, cytowana pozycja literatury [84]. Czy tu chodzi o A.N. Kołmogorowa, rosyjskiego matematyka, twórcę aksjomatycznej teorii prawdopodobieństwa? Jeśli tak to skąd data publikacji 1998! Wszak On zmarł w 1987 roku.

11) Wobec tego, że recenzowana praca nosi charakter wybitnie eksperymentalno-badawczy interesuje mnie w jaki sposób w warunkach laboratoryjnych Politechniki Wrocławskiej uzyskano dwu-i więcej niż dwa splątanie qubitow? Wszak do tego są potrzebne specjalne warunki aby uzyskać stabilność stanów kwantowych a więc temperatury bliskie zera bezwzględnego i określonej próżni?!

5.Konkluzja i ocena pracy

Kończąc moją recenzję pracy doktorskiej Pana mgr inż. Piotra Jóźwiaka p.t." **Zastosowanie probabilistycznych metod do oceny losowości liczb otrzymanych z kwantowych generatorów liczb losowych**", pragnę podkreślić jej wybitny charakter eksperymentalno – badawczy. Biorąc zaś pod uwagę dobór tematyki rozprawy oraz jej aktualność, zrealizowane cele i zadania z tym związane, układ i logikę prowadzenia wywodu badawczo- naukowego, opracowane nowe metody oraz wykorzystanie metod i narzędzi już istniejących, **należy stwierdzić, że recenzowana rozprawa doktorska jest niezwykle udanym projektem**.

Oryginalne rezultaty pracy doktorskiej zostały podsumowane przez Autora na stronie 190 pracy. Całkowicie się z tym zgadzam! Należy w tym miejscu zwrócić uwagę, że zastosowanie probabilistycznych metod do oceny losowości liczb otrzymywanych z kwantowych generatorów liczb losowych, jest nie trywialne i nowatorskie. Jako wnikliwy eksperymentator w nowoczesnej i mało jeszcze zbadanej dziedzinie naukowej, a szczególnie technicznej, jaką jest mechanika kwantowa, komputery kwantowe oraz kryptografia coraz mocniej z tym zawiązana,

Doktorant wykazał swoją głęboką wiedzę teoretyczną i praktyczną. Dodatkowym atutem Jego użytkowych badań i otrzymanych wartościowych rezultatów w omawianej dziedzinie jest fakt Jego współpracy ze znanym nie tylko w Polsce ale i za granicą, Zespołem Naukowo -Badawczym z Politechniki Wrocławskiej.

Reasumując stwierdzam, że w mojej opinii oceniana rozprawa doktorska mgr inż. Piotra Jóźwiaka p.t. *„Zastosowanie probabilistycznych metod do oceny losowości liczb otrzymanych z kwantowych generatorów liczb losowych"* spełnia wymogi rozprawy promocyjnej na stopień doktora nauk technicznych, zgodnie z Ustawą z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* (Dz. U. 2018 poz.1668). Na podstawie powyższego uzasadnienia wnoszę o dopuszczenie recenzowanej pracy doktorskiej do jej publicznej obrony oraz o ustosunkowanie się Autora do zawartych w recenzji uwag i odpowiedzi na sformułowane pytania.

Dodatkowo do mojej bardzo wysokiej oceny rozprawy doktorskiej Pana mgr inż. Piotra Jóźwiaka, proponuję wyróżnić Jego pracę. Będzie to ukłon w stronę rzetelności, wytrwałości i umiejętności Doktoranta a także zachętą do uzyskiwania coraz lepszych wyników w pracy naukowej.

Gliwice, 11 października 2025 r.

Dr hab. Inż. Jan Kałuski