Warszawa, 17.12.2025

dr hab. inż. Remigiusz Augusiak
Centrum Fizyki Teoretycznej
Polskiej Akademii Nauk
al. Lotników 32/46, 02-668 Warszawa

Recenzja rozprawy doktorskiej
mgr. Chithry Raj
pt. *,,Information Processing Tasks as a Toolbox for Quantum Information"*

Uwagi ogólne. Rozprawa pt. ,,*Information Processing Tasks as a Toolbox for Quantum Information*" została przygotowana w Międzynarodowym Instytucie Teorii Technologii Kwantowych Uniwersytetu Gdańskiego pod kierunkiem dr hab. inż. Marcina Pawłowskiego oraz dr. Pedra Ruasa Diegueza. Praca oparta jest na wynikach zawartych w trzech pracach artykułach naukowych, z czego dwie zostały opublikowane w dobrych renomowanych czasopismach naukowych *Physical Review A* oraz *Open Systems and Information Dynamics*, a jedna jest w trakcie recenzji; wszystkie prace można znaleźć w bazie preprintów arXiv.org.

Doktorat został napisany po angielsku na bardzo dobrym poziomie co ułatwia czytanie. Struktura pracy jest następująca: doktorat otwiera wstęp, w którym nakreślono kontekst badań, zdefiniowano główne cele, a także podsumowano zawartość pozostałych rozdziałów. Kolejny rozdział wprowadza najważniejsze pojęcia używane w dalszych częściach pracy oraz objaśnia najważniejsze wyniki literaturowe, które stanowią punkt wyjścia do wyników przedstawionych w pracy jak np. relacje monogamie dla splątania oraz nielokalności. Tą część pracy czyta się dobrze. Zawiera ona jednak szereg wpadek i niedociągnięć, z których — z obowiązku recenzenckiego — część wymieniam poniżej:

1. Po wzorze (2.6) pojawia się stwierdzenie: *„The trace distance has an operational interpretation as the maximum probability of distinguishing … with a single measurement.", które* można literalnie zrozumieć tak, jakby wzór (2.6) podawał wyrażenie na to prawdopodobieństwo, co nie jest ścisłe. W rzeczywistości, maksymalne prawdopodobieństwo rozróżnienia dwóch stanów kwantowych jest określone znaną formuła Helstroma i wyraża się poprzez odległość w normie śladowej.

2. Podając definicję stanu separowalnego, Doktorantka odwołała się do pracy [50], podczas gdy powinna była wskazać pracę Wernera z 1989 roku. Nawiasem mówiąc praca ta nie pojawia się w spisie literatury.

3. Na stronie 10 po wzorze (2.13) pojawia się stwierdzenie, które sugeruje, że Bell pokazał, że istnieją korelacje, które pozwalają złamać nierówność Bella CHSH, co jest pewną nieścisłością.

4. Zasada Niesygnalizowania jest zdefiniowana w pracy kilkukrotnie (zupełnie niepotrzebnie), we wzorach (2.15), (2.33) oraz (2.54). Ponadto wzory (2.15) oraz (2.33) nie definiują owej zasady w pełni bo brakuje podobnego wzoru do (2.15) czy (2.33) dla sumy po wynikach Alicji.

5. We wzorze (2.46), zapewne przez pomyłkę, entropia $H(A|B)$ pojawia sie po obu stronach, a więc można ją z tego wzoru wyrugować.

6. Nie rozumiem dlaczego wzór (2.48) nie jest symetryczny ze względu na zamianę obserwabli $X \leftrightarrow Z$. Ponadto, po wstawieniu (2.49) do (2.50) nie otrzymuje się (2.48), a zapewne taka była intencja.

7. Szereg pojęć oraz oznaczeń użytych w pracy pozostaje niezdefiniowanych, co w niektórych miejscach utrudnia zrozumienie wywodu. Przykładowo, nie podano definicji wyrażenia $X(S)$ pojawiającego się we

wzorze (2.58). Podobnie, po wzorze (2.48) nie zdefiniowano entropii minimalnej i maksymalnej. Za taką definicję można uznać wzór (2.49), ale wtedy brakuje definicji prawdopodobieństwa odgadnięcia, które się w tym wzorze pojawia.

W następnych trzech rozdziałach zawarte zostały wyniki rozprawy, przy czym każdy rozdział odpowiada jednej z publikacji. Pracę kończy krótki rozdział podsumowujący zaprezentowane wyniki oraz omawiający w bardzo skrótowy sposób możliwe kierunki dalszych badań. Uważam, że autorka mogła poświęcić owym kierunkom więcej uwagi i opisać je szerzej. Co ciekawe, rozdział ten zaweria któtki wyjaśnienie wyboru tytułu pracy, którego znaczenie bądź co bądź było dla mnie na początku trudne do uchwycenia.

Badania. Rozprawa bada relacje pomiędzy fundamentalnymi zasadami teorii kwantowej a ich konsekwencjami operacyjnymi. Celem pracy jest wykazanie, że zasady te mogą być bezpośrednio powiązane z zastosowaniami efektów i zjawisk kwantowych w przetwarzaniu informacji. Z jednej strony nakładają one ograniczenia na stopień użyteczności tych efektów w różnych zastosowaniach, takich jak kryptografia kwantowa czy metrologia kwantowa. Z drugiej strony same zadania informacyjne dostarczają podstaw do formułowania i uzasadniania owych zasad, co w ostatnich latach stało się intensywnie badanym obszarem, motywowanym potrzebą sformułowania zasad pozwalających wyodrębnić korelacje kwantowe spośród korelacji spełniających Zasadę Niesygnalizowania, bez konieczności odwoływania się do matematycznego formalizmu mechaniki kwantowej. Dobrym przykładem takiego podejścia jest Zasada Przyczynowości Informacyjnej, która wyłoniła się bezpośrednio z analizowanego w rozprawie scenariusza „przygotuj i zmierz" oraz z konkretnych zadań o charakterze teorio-informacyjnym rozważanych w tym kontekście, która jednocześnie nakłada silniejsze więzy na korelacje kwantowe niżli Zasada Niesygnalizowana. Autorka płynnie porusza się po tych obszarach, a jej rozprawa prezentuje szereg oryginalnych wyników, które zostały przeze mnie w skrócie opisane poniżej.

Rozdział 1. Celem pierwszego „badawczego" rozdziału rozprawy jest wykazanie, że pewne wielocząstkowe uogólnienie Zasady Przyczynowości Informacyjnej, której oryginalną wersję w przypadku dwóch obserwatorów zaproponował już pewien czas temu promotor niniejszej pracy wraz ze swoimi współpracownikami, gwarantuje bezpieczeństwo kryptograficzne w protokole opartym na nierówności CHSH. W pierwszej kolejności wyprowadzono odpowiednie sformułowanie tej zasady w taki sposób, aby mogła ona zostać skutecznie zastosowana do korelacji powstających w scenariuszu z trzema obserwatorami, z uwzględnieniem obecności podsłuchiwacza. Następnie wykazano, że zasada ta nakłada silniejsze ograniczenia na korelacje trójobserwatorowe niż sama Zasada Niesygnalizowania. Silniejsza monogamia z kolei przekłada się na bardziej restrykcyjne warunki dotyczące korelacji, jakie podsłuchiwacz może współdzielić z jednym z obserwatorów, co z kolei zapewnia bezpieczeństwo nawet przy słabszym łamaniu nierówności CHSH; wartość łamania obniżono tutaj z 0.881 (dla Zasady Niesygnalizowania) do 0.8471 Kluczowym narzędziem jest lemat, który stwierdza, że do wyznaczenia relacji monogamii wystarczy ograniczyć się do pewnej dwuparametrowej klasy korelacji niesygnalizujących, uzyskanych poprzez operację „twirlingu" pomiędzy Alicją i Bobem oraz pomiędzy Bobem a podsłuchiwaczem.

Uważam tę część pracy za szczególnie interesującą i wartościową. Wykazano w niej możliwość sformułowania wieloobserwatorowej wersji Zasady Przyczynowości Informacyjnej w taki sposób, aby nakładała ona silniejsze ograniczenia na korelacje wielociałowe niż sama Zasada Niesygnalizowania, a ponadto ukazano jej użyteczność w kontekście zapewniania bezpieczeństwa kryptograficznego. Uzyskany rezultat ma istotne znaczenie dla zrozumienia roli Zasady Przyczynowości Informacyjnej w odtwarzaniu korelacji kwantowych.

Mam kilka uwag/pytań do tej części pracy:

1. Zabrakło kilku słów wyjaśnienia, w jaki sposób relacja monogamii typu (2.36) przekłada się na warunek bezpieczeństwa kryptograficznego wyrażony wzorem (2.37). Ponadto, w podrozdziale 3.6, poświęconym analizie bezpieczeństwa kryptograficznego na podstawie otrzymanej relacji monogamii, nie sprecyzowano, jaki model ataku podsłuchiwacza jest rozważany. Przed wzorem (2.37) atak ten określony jest jako indywidualny, natomiast na stronie 25, w części „Key rate and security", pojawia się ograniczenie na „key

rate" wyrażone poprzez wartość funkcjonalu CHSH dla ataków kolektywnych. Czy Doktorantka może doprecyzować, dla jakiego typu ataków sformułowane są wyniki tego rozdziału, a jeśli dotyczą one ataków indywidualnych, to z jakiego powodu w pracy pojawia się wzór (2.58)?

2. Czy Autorka dostrzega możliwości ulepszenia otrzymanej zasady lub wynikającej z niej relacji monogamii? W szczególności, czy można oczekiwać odtworzenia „kwantowej" relacji monogamii (2.34)?

3. Czy Doktorantka badała zastosowanie innych zasad takich jak np. Zasada Lokalnej Ortogonalności w kontekście monogamii bądź kwantowej kryprografii?

Rozdzial 2. Kolejny rozdział dotyczy scenariusza typu „przygotuj i zmierz", w którym jeden z obserwatorów przygotowuje stan kwantowy z pewnego zbioru i wysyła go do drugiego obserwatora, który wykonuje na nim jeden z dostępnych pomiarów. Jest to scenariusz nieco prostszy do badania w stosunku do rozważanego w poprzednim rozdziale scenariusza Bella. Wciąż jednak pozwala on na stawianie nietrywialnych problemów, w rozwiązaniu których korelacje kwantowe pozwalają uzyskać przewagę nad korelacjami klasycznymi; w szczególności można w nim badać jak efekty kwantowe przekladaja się na bezpieczeństwo kryptograficzne. W pracy pokazano jak pewien konretny scenariusz określany równiez jaok QRAC 2→1 można sformułować w terminach eksperymentu interferometrycznego Macha-Zehndera. W pracy pokazano jak pewien świadek nieklasyczności, rozważany we wcześniejszej pracy [30] w kontekście analizy bezpieczeństwa kryptograficznego w scenariuszu typu QRAC 2→1, można wyrazić w postaci sumy dwóch kluczowych wielkości charakteryzujących eksperyment Macha-Zehndera, tzn. rozróżnialności oraz widzialności, które odpowiadają korpuskularnej oraz falowej naturze światła.

Uzyskano w ten sposób bardzo ciekawą interpretację scenariusza typu przygotuj i zmierz w kontekście jednego z najbardziej fundamentalnych eksperymentów interferometrycznych oraz pokazano, że wartość owego świadka jest miarą Dualizmu korpuskularno-falowego. Co więcej, pokazano, że wysokie wartości obu parametrów gwarantują nieklasyczność korelacji, a co więcej, zapewniają bezpieczeństwo kryptograficzne, co pozwoliło na powiązanie zasady Dualizmu korpuskularno-falowego z bezpieczeństwem kryptograficznym. Jednocześnie znana relacja komplementarności dla widzialności i rozróżnialności nakłada ograniczenie na wartość świadka.

Co ważne, przewidywania teoretyczne zostały również przetestowane w eksperymencie zrealizowanym we współpracy międzynarowowej. Dodatkowym wynikiem zaprezentowanym w tej części pracy jest bardziej rygorystyczne, w porównaniu z pracą [30], ograniczenie na wartość świadka gwarantujące bezpieczeństwo kryptograficzne w scenariuszu typu QRAC 2→1.

1. Rozważany w pracy bardzo szczególny przypadek jakim jest scenariusz typu RAC 2→1 z dwoma bitami wejściowymi po stronie Alicji oraz dwoma binarnymi pomiarami po stronie Boba bardzo dobrze pasuje do eksperymentu Macha-Zehndera. Z czystej ciekawości chciałbym zapytać, czy scenariusze z większą liczbą bitów/ditów wejściowych po stornie Alicji (oraz odpowiednich pomiarach po stronie Boba) da się również zaimplemetować przy pomocy optyki liniowej, zwiększając np. liczbę fotonów?

2. Czy Doktorantka mogłaby wyjaśnić, na czym polega różnica między wyprowadzeniem ograniczeń (4.39) i (4.40) a wyprowadzeniem przedstawionym w oryginalnej pracy [30]? Samo wyprowadzenie jest dość elementarne od strony matematycznej, dlatego chciałbym zrozumieć, jakie dodatkowe techniki pozwoliły na uzyskanie lepszych ograniczeń.

Rozdział 3. W ostatnim rozdziale badano Dualizm korpuskularno-falowy w eksperymencie typu interferometrycznego z opóźnionym wyborem, gdzie decyzja o pomiarze zachowania falowego bądź korpuskularnego jest odroczona w czasie. Celem było wyjście poza standardowy eksperyment i zbadanie zachowania "cząstki zanim dotrze ona do detektora", czyli przed dokonaniem pomiaru na badanym układzie. W pracy rozważano wersję, w której układ kontrolujący stanowi część splątanego stanu kwantowego, co dodatkowo ubogaca eksperyment i pozwala analizować, w jaki sposób ta forma korelacji wpływa na właściwości układu przed i po wyborze pomiaru. Obie cechy mierzono przy pomocy miary zwanej

realizmem, która określa ile realizmu jest w danym pomiarze względem zadanego stanu kwantego, przy czym za zachowanie korpuskularne odpowiada pomiar w bazie standardowej, natomiast zastronę falową odpowiada pomiar w bazie komplementarnej z nietrywialną fazą.

Przeanalizowano kilka scenariuszy w zależności od tego, jaka operacja jest wykonywana na jednym z podukładów kontrolującego stanu splątanego (ślad częściowo, postselekcja lub brak operacji) oraz od tego kiedy operacja kontrolowana jest zastosowana na badany kubit. Na tej podstawie poczyniono kilka obserwacji, z których najbardziej interesującą wydaje się fakt, że w przypadku eksperymentu, w którym na podukładzie C nie wykonuje się żadnej operacji, wartości realizmu dla obu obserwabli spełniają zasadę komplementarności: suma obu wartości jest ograniczona z góry przez funkcję liniową splątania pomiędzy badanym kubitem, a kubitami kontrolującymi.

O ile nie mam większych uwag do tej części pracy, to chciałbym zapytać, czy Doktorantka przeanalizowała sytuację, w której cząstka wejściowa *A* bądź cały układ są w stanie mieszanym. W szczególności, czy da się wyprowadzić podobną relację komplementarności do (5.19) w sytuacji, w której całkowity stan obejmujący kubity *A, B i C* jest mieszany.

Konkluzja. Uważam, że rozprawa doktorska Chithry Raj zawiera szereg oryginalnych wyników naukowych. Za najciekawsze uważam rezultaty przedstawione w Rozdziale 3, dotyczące Zasady Przyczynowości Informacyjnej oraz jej implikacji dla bezpieczeństwa kryptograficznego w scenariuszu niezależnym od urządzeń, a także wyniki z Rozdziału 4, w którym Autorka wykazuje analogię pomiędzy interferometrem Macha–Zehndera a pewnym szczególnym scenariuszem typu RAC. Uważam, że to właśnie te osiągnięcia mogą wywrzeć największy wpływ na społeczność naukową. Jednocześnie Autorka udowodniła, że posiada wiedzę teoretyczną niezbędną do uzyskania stopnia doktora w dyscyplinie nauki fizyczne. Co prawda znalazłem w pracy pewne uchybienia o charakterze redakcyjnym, jednak nie wpływają one na ocenę merytoryczną rozprawy. W związku z tym stwierdzam, że rozprawa doktorska Chitry Raj spełnia wymogi ustawowe i wnoszę o dopuszczenie Kandydatki do dalszych etapów postępowania doktorskiego, w tym do publicznej obrony.

Remigiusz Michał Augusiak

Elektronicznie podpisany przez Remigiusz Michał Augusiak
Data: 2025.12.17 14:09:44 +01'00'