Recenzja rozprawy doktorskiej

mgr Tushity Prasad

pt.

Operational approaches to quantum resources in communication and security

przygotowanej pod opieką

dr. hab. Marcina Pawłowskiego, prof. UG

Recenzent: dr hab. inż. Gniewomir Sarbicki, prof. UMK

Toruń, 8 lipca 2026

Rozprawa doktorska pani Tushity Prasad pt. „Operational approaches to quantum resources in communication and security" została przygotowana jako tzw. rozprawa zszywkowa: składa się z rozdziału wprowadzającego oraz rozdziałów zawierających omówienie trzech artykułów naukowych, których autorka rozprawy jest współautorką; pełne wersje tych prac zostały dołączone do rozprawy.

Rozprawa dotyczy operacyjnego znaczenia zasobów kwantowych — przede wszystkim splątania i komplementarności — w zadaniach komunikacji oraz kryptografii kwantowej. Autorka analizuje nie tylko to, kiedy zasoby te dają przewagę nad metodami klasycznymi, lecz także kiedy okazują się niewystarczające w realistycznych warunkach.

Rozdział wprowadzający przedstawia punktowo kilka zagadnień kluczowych dla dalszych części rozprawy. Niestety, czyni to w sposób zbyt skrótowy i nie w pełni spójny. Pojęcie *shared randomness* powinno zostać zdefiniowane. Zdarza się także mieszanie pojęć stanu i wektora stanu. Brakuje ponadto wyjaśnienia różnicy między splątaniem a „kwantową nielokalnością", niezależnie od tego, jak niefortunna jest ta druga nazwa. Kluczowe dla rozprawy jest pojęcie przepustowości kanału kwantowego dla informacji klasycznej: jedno- i wieloużyciowej, asymptotycznej oraz przepustowości wspomaganej splątaniem. Brak wprowadzenia tych definicji i ich krótkiej dyskusji uważam za istotne niedociągnięcie pracy.

W opisie interferometru Macha-Zehndera wprowadzone są wielkości rozróżnialności dróg i widzialności prążków. Ta druga nazwa nie jest całkiem jasna w odniesieniu do tego układu: brakuje odwołania do historycznego eksperymentu z dwiema szczelinami oraz krótkiego omówienia jego równoważności z interferometrem Macha-Zehndera.

W przypadku dwóch dróg mamy jednoparametrową rodzinę baz wzajemnie nieobciążonych (MUB) względem bazy obliczeniowej, parametryzowaną przesunięciem fazowym w jednej z gałęzi interferometru. Podobnie w uogólnieniu wyżejwymiarowym otrzymujemy wieloparametrową rodzinę baz parametryzowaną różnicami faz na poszczególnych drogach. Z tego powodu sformułowanie *this complementary basis is given by the Fourier transform of the computational basis* w paragrafie *Higher dimensional generalisation* wydaje się zbyt uproszczone.

Sformułowanie *(...) entanglement and complementarity were identified as resources* w rozdziale 2.2 jest nieco na wyrost. Wielkości te zostały zdefiniowane, ale nie zostały formalnie zidentyfikowane jako zasoby w sensie teorii zasobu.

Wprowadzenie do teorii kodowania jest napisane efektywnie i zrozumiale. Niedociągnięciem jest jednak użycie pojęcia minimalnej odległości kodu na stronę przed jego zdefiniowaniem. Definicja kodów Reeda-Solomona jest bardzo zwarta, lecz poprawna. Zdecydowanie zbyt skrótowy jest natomiast opis rozszerzenia ciała. Moim zdaniem należałoby zacząć od zdefiniowania go jako ciała reszt wielomianów nad $\mathbb{F}_q$ modulo wielomian nierozkładalny stopnia 2, a dopiero następnie wprowadzić izomorfizm z parami, definiując γ jako pierwiastek tego wielomianu w rozszerzeniu. Brakuje także wprowadzenia automorfizmu Frobeniusa oraz wyjaśnienia tożsamości $f(\gamma^q) = f(\gamma)^q$.

W podrozdziale 2.3, w paragrafie *Prepare-and-measure QKD*, w ogólnej definicji występuje tylko jedno wejście a po stronie Alicji. Dobrze byłoby odnieść ten zapis do protokołu BB84, w którym a w naturalny sposób zawiera zarówno przesyłany bit, jak i wybór bazy.

W paragrafie *Convex combination attacks* zamiast określać Λ_E jako *arbitrary information*, należałoby nazwać je klasycznym kanałem. Podobnie mianownik $N - 1$ w równaniu (2.37) wymaga komentarza.

Paragraf *Quantum Repeaters and QKD* pokazuje, że użycie repetera pozwala z dwóch stanów izotropowych o widzialności v otrzymać jeden stan na dłuższym dystansie o widzialności v^2. Należałoby jednak porównać ten wynik z pojedynczym stanem izotropowym łączącym A i B przy założeniu określonego modelu skalowania widzialności z odległością; dopiero wtedy takie porównanie ma pełny sens. Co więcej, na stronie 38 oraz w trzecim artykule pojawia się stwierdzenie, że jeżeli pomiędzy A i B znajduje się n repeaterów, to widzialność wynosi v^{2n}, gdzie v jest widzialnością na jednym odcinku. Przy standardowym liczeniu, w którym n oznacza liczbę repeaterów pośrednich, poprawne skalowanie powinno mieć postać v^{n+1}, chyba że n oznacza nie liczbę repeaterów, lecz liczbę iteracji podziału odcinka na dwie części.

Pierwszy z artykułów dotyczy klasycznej komunikacji wspomaganej splątaniem w skończonym reżimie zasobów. Zaproponowano w nim jawne konstrukcje kodów pozwalających korygować błędy lub wymazania przy zmiennej ilości współdzielonego splątania. Pokazano, że odpowiednie, adaptacyjne wykorzystanie splątania może poprawić wydajność transmisji, a współczynnik transmisji może przekroczyć 1. Wynik ten wydaje się jednak częściowo artefaktem definicyjnym: w mianowniku uwzględnia się liczbę użyć kanału, ale nie liczbę ebitów zużytych do supergęstego kodowania. Interesujący jest także niewypukły kształt obszaru osiągalnych parametrów; użycie time-sharingu powinno pozwolić na wysycenie *quantum bound*.

Drugi artykuł bada związek między komplementarnością falowo-korpuskularną a bezpieczeństwem w kryptografii kwantowej w modelu pół-niezależnym od urządzeń. Wynik polega na wyrażeniu świadka bezpieczeństwa przez wielkości interferometryczne: widzialność interferencji i rozróżnialność dróg. Dzięki temu bezpieczeństwo można certyfikować za pomocą parametrów mierzalnych eksperymentalnie. Nie jest jednak jasne, dlaczego stany BB84 (wzór 15 w artykule) są kodowane „skośnie", tj. w taki sposób, że jeden bit nie koduje bazy, a drugi położenia w bazie, co implikuje użycie operacji XOR w deltach Kroneckera. Jaka jest korzyść z takiego numerowania stanów Alicji? W tekście znajduje się wyjaśnienie *this parity mapping provides a clear separation between experiments testing distinguishability and those testing visibility*, ale nie jest ono wystarczające.

Trzeci artykuł pokazuje ograniczenia splątania jako zasobu kryptograficznego. Autorka wykazuje, że samo splątanie nie wystarcza do zagwarantowania bezpiecznej dystrybucji klucza, jeśli występuje choćby niewielki klasyczny wyciek informacji bocznej. Oznacza to fundamentalne rozdzielenie między obecnością splątania a jego użytecznością do generowania tajnego klucza. Wspomniałem już wyżej o błędnym, moim zdaniem, skalowaniu widzialności wraz z liczbą repeaterów.

Podsumowując, rozprawa opiera się na rozwiązaniu trzech problemów związanych z komunikacją kwantową i kwantowym uzgadnianiem klucza. Jej słabszą stroną jest rozdział wprowadzający, który ma charakter punktowego zestawienia pojęć i nie zawsze dostatecznie dba o ich wzajemne powiązanie. Niezależnie od powyższych uwag krytycznych, wysoko oceniam naukową wartość wyników składających się na rozprawę. Na podkreślenie zasługuje fakt, że dwa spośród trzech artykułów wchodzących w skład rozprawy zostały opublikowane w czasopiśmie *npj Quantum Information*, a trzeci jest dostępny jako preprint. Świadczy to o tym, że zasadnicze wyniki rozprawy zostały już poddane zewnętrznej ocenie środowiska naukowego lub są w obiegu naukowym. Prace te dotyczą aktualnych i istotnych problemów teorii informacji kwantowej: skończonych konstrukcji kodów wspomaganych splątaniem, operacyjnego znaczenia komplementarności w scenariuszach pół-niezależnych od urządzeń oraz ograniczeń splątania jako zasobu kryptograficznego. Szczególnie wartościowe jest

konsekwentne przyjęcie perspektywy operacyjnej, w której zasoby kwantowe oceniane są nie przez sam fakt ich występowania, lecz przez zadania informacyjne, które umożliwiają, oraz przez ograniczenia, którym podlegają w realistycznych warunkach. Wyniki rozprawy pokazują zarówno przewagi wynikające z użycia splątania i komplementarności, jak i granice ich użyteczności. Świadczy to o dojrzałości naukowej autorki i jej dobrej orientacji w nowoczesnych metodach teorii informacji kwantowej.

Podsumowując, stwierdzam, że recenzowana rozprawa spełnia wymagania określone w art. 187 ustawy z dnia 20 lipca 2018 r. — Prawo o szkolnictwie wyższym i nauce (t.j. Dz.U. z 2024 r. poz. 1571, z późn. zm.) i wnioskuję o dopuszczenie jej do dalszych etapów postępowania w sprawie nadania stopnia doktora w dziedzinie nauk ścisłych i przyrodniczych, w dyscyplinie nauki fizyczne.

Gniewomir Sarbicki