Dr hab. Paweł Kurzyński, prof. UAM
Wydział Fizyki
Uniwersytet im. Adama Mickiewicza
w Poznaniu

Poznań, 31 sierpnia 2017

Recenzja rozprawy doktorskiej mgr. Ryszarda Veynara "Fizyczne ograniczenia na przetwarzanie informacji kwantowej"

Tematyka:

Badania podjęte przez mgr. Ryszarda Veynara poświęcone są fizycznym aspektom przetwarzania informacji w układach kwantowych. Powyższa tematyka badawcza rozwinęła się w bardzo krótkim czasie — od ściśle teoretycznych rozważań po komercyjne układy pozwalające na takie zadania jak kwantowa generacja klucza kryptograficznego. Problemy rozważane przez Doktoranta są w centrum zainteresowania wielu grup badawczych z całego świata, co potwierdza, że tematyka rozprawy jest niezwykle aktualna.

Sformułowanie problemów i hipotez badawczych:

Celem rozprawy jest zbadanie różnych protokołów przetwarzania informacji kwantowej w realnych sytuacjach, w których kluczową rolę odgrywają fizyczne ograniczenia narzucone na układy będące nośnikami informacji oraz na aparaturę pomiarową. Zadanie, którego podjął się Doktorant, jest ambitne, ponieważ otrzymane rezultaty mogą mieć wpływ na dalszy rozwój technologii kwantowych.

Problem badawczy jest jasno postawiony w tytule oraz trochę dokładniej omówiony w streszczeniu. Moim zdaniem mgr. Veynar mógłby również szczegółowo omówić tezę rozprawy we wstępie, tuż przed rysem historycznym, co pozwoliłoby czytelnikowi już na początku jednoznacznie zrozumieć jakie są cele i motywacje Doktoranta.

Rezultaty, ich znaczenie i oryginalność:

Wyniki zawarte w rozprawie ukazały się w czterech pracach, z których trzy zostały już opublikowane w cenionych recenzowanych czasopismach naukowych. Są to oryginalne wyniki naukowe, które pogłębiają nasze zrozumienie fizycznych aspektów przetwarzania informacji kwantowej oraz mogą znaleźć praktyczne zastosowanie w technologiach kwantowych.

W szczególności, w rozdziale trzecim omówiono wpływ efektywności detektorów na bezpieczeństwo protokołów kwantowej generacji klucza kryptograficznego opartych na kodach swobodnego dostępu. Pokazano, jak możliwość wygenerowania bezpiecznego klucza kryptograficznego zależy od możliwości ingerencji Ewy (podsłuchującego) w układy Alicji i Boba oraz od średniej efektywności ich detektorów. Zbadany problem jest istotny z punktu widzenia kryptografii kwantowej, zatem otrzymane wyniki mogą znaleźć praktyczne zastosowanie.

W rozdziale czwartym zbadano zależność efektywności procesu teleportacji od ilości klasycznej informacji przesyłanej od Alicji do Boba. Przede wszystkim, wyznaczono minimalną ilość informacji klasycznej, którą Alicja musi przesłać do Boba aby splątanie między nimi odegrało jakąkolwiek rolę. Powyższy wynik pokazuje silną relację pomiędzy klasyczną komunikacją i splątaniem, co pogłębia nasze zrozumienie podstawowych zasobów kwantowej teorii informacji.

W rozdziale piątym rozważono wersję protokołu kryptograficznego BBM92, w którym nie ograniczono się do założenia, że wiązka pompująca jest słaba. W takim procesie generowane są splątane stany wielofotonowe. W szczególności, zaprezentowano metodę pozwalającą na generację klucza kryptograficznego w oparciu o zdarzenia, w których wszystkie fotony wygenerowane w tym samym modzie przestrzennym padają na ten sam detektor. Co więcej, znaleziono optymalną wartość parametru opisującego intensywność wiązki pompującej. Podobnie jak w przypadku wyników z rozdziału trzeciego, przedstawiony wynik może znaleźć praktyczne zastosowanie w przyszłości.

Rozdział szósty dotyczy problemu detekcji splątania w sytuacji kiedy przeprowadzone pomiary nie dają nam pełnej informacji o stanie układu. Z reguły należy wykonać określoną ilość pomiarów i dopiero później na podstawie wyników można stwierdzić czy stan jest splątany. W rozprawie zaproponowano metodę pozwalającą na stwierdzenie czy stan jest splątany jeszcze zanim zrobimy wszystkie pomiary. Na bieżąco obliczamy pewną wielkość na podstawie otrzymanych wyników i jeśli przekroczy ona pewien próg graniczny to wiemy, że stan jest splątany i dalszych pomiarów nie musimy wykonywać. Przedstawiona metoda ma praktyczne znaczenie w teorii splątania, ponieważ pozwala ona na zaoszczędzenie czasu oraz zasobów potrzebnych do wykonania pomiaru.

Metody:

W rozprawie zastosowano standardowe techniki kwantowej teorii informacji, takie jak algebra liniowa, teoria grup, rachunek prawdopodobieństwa i statystyka, czy metody optymalizacyjne. Rozważane problemy zostały rozwiązane w sposób analityczny lub numeryczny. Rozprawa jednoznacznie pokazuje, że Doktorant biegle opanował wspomniane techniki.

Układ pracy i struktura treści:

Całość tekstu podzielona jest na siedem rozdziałów, streszczenie oraz spisu literatury. Pierwszy rozdział to wstęp, w którym przedstawiono rys historyczny kwantowej teorii informacji. W rozdziale drugim omówiono podstawowe pojęcia niezbędne do zrozumienia dalszej części pracy. Główne wyniki zebrano w rozdziałach od trzeciego do szóstego, a rozdział siódmy zawiera podsumowanie rozprawy. Moim zdaniem układ pracy jest prawidłowy, jednak mam drobne uwagi co do treści zawartych w dwóch pierwszych rozdziałach. Jak wspomniałem wcześniej, uważam, że poza rysem historycznym we wstępie należałoby również dokładniej omówić główne tezy pracy. Dodatkowo, w rozdziale drugim omówiłbym szczegółowiej takie pojęcia jak entropia warunkowa oraz ograniczenie Holevo.

Poprawność (formalna, językowa, stylistyczna):

Praca została spisana w języku polskim i zawiera rzetelnie sporządzone streszczenie w języku angielskim. Przedstawione wyniki są poprawne, jednakże sama rozprawa sprawia

wrażenie spisanej w pośpiechu ze względu na liczne literówki w tekście i we wzorach oraz błędy gramatyczne, ortograficzne i stylistyczne. Dodatkowo, rysunki 4.1 i 4.2 są niewłaściwe (są kopiami rysunków 5.1 i 5.2).

Dobór literatury:

Rozprawa zawiera rozsądny zbiór odnośników do literatury. Moim zdaniem Doktorant cytuje wszystkie ważniejsze prace, które poprzedziły i zainspirowały badania omówione w rozprawie. Mam tylko dwie uwagi odnośnie wstępu. W rysie historycznym Doktorant wspomina (str. 8), że protokół Ekerta jest równoważny protokołowi BB84, jednak dowód równoważności tych protokołów nie jest cytowany. Ponadto, Doktorant nie cytuje prac eksperymentalnych o teleportacji kubitów materii oraz o otrzymywaniu stanów splątanych dużych ilości atomów i fotonów (str. 10). Oczywiście, brak cytowań wspomnianych wyników nie jest istotnym uchybieniem, jednakże wiele innych osiągnięć jest dość szczegółowo cytowanych, przez co powyższe braki rzucają się w oczy.

Szczegółowe uwagi:

1) Ostatni paragraf na stronie 48 jest dla mnie niezrozumiały. Czy w równaniu (3.90) wielkość "C" nie powinna być indeksowana przez "e"? W tej sytuacji warunek bezpieczeństwa wynikający z nierówność (3.87) przybiera postać równania (3.72), które opisuje ogólny atak, a nie prostszy.

2) We wzorze (4.22) zostaje wprowadzona operacja U indeksowana przez i oraz j. Poniżej wspomniano, że ta operacja odpowiada za zmniejszenie wydajności zjawiska teleportacji ze względu na błędy w kanale kwantowym. Jaka jest postać tego operatora? Z kontekstu rozumiem, że jest to dowolny bezśladowy operator unitarny. Czy to prawda, czy może w pracy przyjęto konkretny model błędu? Ponadto, czy ten operator musi być unitarny?

3) W rozdziale 4.5 na stronie 71 wspomniano, że najlepszą strategią w przypadku wysyłania ograniczonej liczby bitów przez Alicję jest wysyłanie jedynie części informacji. Jednakże, wcześniej wspomniano, że może wystąpić sytuacja w której różne wyniki otrzymywane przez Alicję mogą mieć różne prawdopodobieństwa. Czy w tym przypadku lepszą strategią nie byłaby kompresja (być może stratna)?

4) W standardowym protokole BBM92 pomiary Alicji i Boba dokonywane są na pojedynczych fotonach. Lokalne obserwable są komplementarne, zatem prawdopodobieństwo przekrycia się stanów z różnych baz wynosi 1/2. W uogólnionym protokole rozważanym przez Doktoranta pomiary dokonywane są na wielu fotonach. Wydaje mi się, że w takiej sytuacji prawdopodobieństwo przekrycia różnych stanów się zmieni. Np. pomiary obserwabli X i Z na pojedynczym kubicie dają stany, których prawdopodobieństwo przekrycia wynosi 1/2, lecz te same pomiary na dwóch kubitach dadzą stany, których prawdopodobieństwo przekrycia wyniesie 1/4. Czy ten fakt ma jakiś wpływ na bezpieczeństwo protokołu?

5) W rozdziale 6.6.3 wprowadzono uogólnione macierze Pauliego "lambda". Dla d=3 są to macierze Gell-Manna. Jednakże macierze Pauliego mogą być uogólnione na wiele sposobów. Czy podobne wyniki można otrzymać stosując unitarne macierze o wartościach własnych będących pierwiastkami z jedynki?

Wniosek końcowy:

Przedstawiona rozprawa stanowi oryginalny i konkretny wkład do kwantowej teorii informacji oraz spełnia wszystkie ustawowe i zwyczajowe wymogi. W związku z powyższym, wnioskuję o dopuszczenie mgr. Ryszarda Veynara do dalszych etapów przewodu doktorskiego.

Paweł Kurzyński

Paweł Kurzyński