Dr hab. Paweł Kurzyński, prof. UAM
Wydział Fizyki UAM,
Umultowska 85, 61-614 Poznań
email: pawel.kurzynski@amu.edu.pl

Poznań, 4 września 2018

Recenzja rozprawy doktorskiej magistra Edgara Alexisa Aguilara Lozano „Device Independent and Semi Device Independent Protocols for Quantum Information Processing"

Tematyka:

Pan magister Edgar Alexis Aguilar Lozano w swojej pracy doktorskiej podjął się rozwiązania kilku problemów z dziedziny kwantowej teorii informacji. Jego badania dotyczyły komunikacji kwantowej: sprzętowo-niezależnej (DI – device-independent) dystrybucji klucza kwantowego oraz quasi-sprzętowo-niezależnego (SDI – semi-device-independent) protokołu kodu losowego dostępu (RAC - random access code). Tematyka badawcza przedstawionej rozprawy cieszy się obecnie bardzo dużą popularnością wśród wielu międzynarodowych grup badawczych, zarówno tych pracujących na uczelniach, jak i w wielkich koncernach technologicznych.

Sformułowanie problemów i hipotez badawczych:

Rozprawa składa się z trzech prac i każda z nich oparta jest na innej hipotezie badawczej. Pierwsza praca [PRA 94, 022305 (2016)] ma na celu rozwiązanie ważnego problemu w kryptograficznych protokołach DI, którym jest dostęp do początkowej losowości. Druga praca [PRL 120, 230503], która jest teoretyczno-eksperymentalna, ma na celu zbadanie czy kwantowy protokół RAC można wykorzystać do zagwarantowania, że otrzymywane w laboratorium stany kwantowe są wielowymiarowe (tzn. można całkowicie wykorzystać fakt, że ich stan jest opisywany przez d-wymiarową przestrzeń Hilberta). Celem trzeciej pracy [arXiv1709.04898] jest sprawdzenie, czy kwantowy protokół RAC może być zastosowany do wykluczania ilości baz wzajemnie komplementarnych (MUB – mutually unbiassed bases) w układach o zadanym wymiarze.

Omówione zagadnienia zostały zarysowane w streszczeniu i dokładniej przedstawione w podsumowaniu otrzymanych wyników, które jest wstępem do trzech prac, zatem czytelnik zapoznaje się z nimi już na początku lektury. Uważam, że powyższe problemy są ambitne i ważne dla rozwoju kwantowej teorii informacji i podstaw fizyki kwantowej, zatem jak najbardziej mogą stanowić podstawę pracy doktorskiej.

Rezultaty, ich znaczenie i oryginalność:

Postawione problemy zostały rozwiązane. W pracy [PRA 94, 022305 (2016)] zaproponowano prosty, lecz błyskotliwy, pomysł na rozwiązanie problemu początkowej losowości. Okazuje się, że taka losowość jest naturalnie zawarta w samej informacji, którą Alicja chce w bezpieczny sposób przekazać Bobowi. Powyższy fakt jest wręcz oczywisty, jednak przez lata był on kompletnie niezauważany, a przynajmniej nie

wykorzystywany. Losowość w początkowej wiadomości można następnie przetworzyć w ciąg prawie idealnie losowych bitów, korzystając z protokołów ekstrakcji i ekspansji losowości (Trevisan's extractor, Miller-Shi expansion). Bezpieczeństwo przedstawionego protokołu opisuje twierdzenie 4.2, które jest głównym wynikiem tej pracy. Otrzymany wynik pozwala na całkowicie sprzętowo-niezależną dystrybucję klucza kwantowego.

W pracy [PRL 120, 230503] pokazano, że kwantowy protokół RAC posiada różne ograniczenia górne na prawdopodobieństwo średniego sukcesu, w zależności od tego, czy dany układ ma strukturę produktową, czy też jest niepodzielny (ze względu na operacje i pomiary na nim dokonywane). Ponadto, powyższe ograniczenia zależą też od tego, czy ewentualne podukłady są klasyczne, czy kwantowe. Ten wynik pozwolił na skonstruowanie „wielowartościowego" świadka wymiaru („gamut" dimension witness), ponieważ jeśli w kwantowym protokole RAC osiągamy sukces z prawdopodobieństwem powyżej pewnej wartości, to automatycznie otrzymujemy ograniczenie dolne na wymiar używanego przez nas układu kwantowego. Wspomniany świadek wymiaru został następnie wykorzystany do eksperymentalnej weryfikacji wymiaru układu, w którym 1024 stany kwantowe są kodowane na różnych poprzecznych stanach pędowych pojedynczego fotonu. Jest to wynik naprawdę niesamowity, ponieważ o takich układach trudno mówić, że są mikroskopowe. W szczególności, takie układy dają nadzieję na zbadanie granicy pomiędzy światami kwantowym i klasycznym.

W ostatniej pracy [arXiv1709.04898] najpierw pokazano, że optymalne prawdopodobieństwo sukcesu w kwantowym protokole RAC, w którym Bob ma odgadnąć jeden z dwóch „ditów", powiązane jest z wzajemną komplementarnością baz pomiarowych Boba, a następnie zauważono, że zależność ta nie zachodzi w uogólnionym protokole, w którym Bob ma odgadnąć jeden z n ditów. To skłoniło autorów pracy do zaproponowania nowej wersji protokołu, w którym Alicja jest zapewniona o tym, że dit Boba będzie należał do pewnego podzbioru. Dzięki temu Alicja może opracować nową strategię kodowania zależną od otrzymanego zapewnienia. Okazuje się, że w przypadku kiedy podzbiory Boba składają się z dwóch ditów, optymalność tej strategii jest już ściśle powiązana z ilością baz komplementarnych (lemat 2). Zatem, poprzez optymalizację prawdopodobieństwa sukcesu można wykryć istnienie szukanej ilości baz komplementarnych. Niestety, nieudana optymalizacja nie oznacza, że szukana ilość baz nie istnieje. Jednakże, powyższy problem został „dopełniony" poprzez zastosowanie SDP hierarchii Navascuesa i Vertesiego. W tym przypadku sukces pozwala na wykrycie braku szukanej ilości baz. Pokazano, że powyższe podejście działa w znanych przypadkach i choć nie udało się rozwiązać problemu ilości baz w sześciowymiarowej przestrzeni, wydaje się, że zaproponowana metoda może pozwolić na to w przyszłości.

Otrzymane wyniki oceniam bardzo wysoko, gdyż wnoszą one istotny wkład do wspomnianych wcześniej dziedzin wiedzy. Ponadto, należy zwrócić uwagę na fakt, że prace poddane ocenie zostały opublikowane w prestiżowych międzynarodowych czasopismach naukowych, co świadczy o tym, że wyniki Doktoranta i jego współpracowników zostały już wcześniej wysoko ocenione przez recenzentów i edytorów, którzy są światowej klasy specjalistami w danych dziedzinach.

Wkład Doktoranta:

Doktorant jest pierwszym autorem wszystkich trzech prac wchodzących w skład ocenianego dzieła. Ponadto, z dostarczonych oświadczeń współautorów wyraźnie wynika, że wkład magistra Aguilara Lozano w powstanie każdej z prac był znaczący, lub wręcz wiodący. Zatem, przedstawione wyniki mogą śmiało stanowić podstawę do nadania stopnia doktora.

Metody:

Chociaż badania Doktoranta są głównie natury teoretycznej, jedna z przedstawionych prac zawiera również wyniki doświadczalne, gdyż magister Aguilar Lozano ściśle współpracował z grupą fizyków doświadczalnych z Chile, którzy dokonali eksperymentalnej weryfikacji teoretycznych rezultatów. Same metody teoretyczne to techniki stosowane w teorii informacji i teorii informacji kwantowej. Użyto protokołów ekstrakcji i ekspansji losowości, algebry liniowej, optymalizacji oraz metod numerycznych.

Układ pracy i struktura treści:

Rozprawa została złożona w postaci kolekcji trzech prac uzupełnionej o streszczenie i dość obszerne podsumowanie otrzymanych wyników. Wspomniane podsumowanie składa się z czterech części, w których jasno przedstawiono motywacje Doktoranta i jego współpracowników, omówiono główne wyniki wszystkich trzech prac i przedyskutowano możliwe kierunki rozwoju przyszłych badań.

Układ pracy, szczególnie jej pierwszej części, jest bardzo dobry. Podsumowanie napisano językiem prostym i przystępnym, a wszystkie kroki rozumowania prowadzące od założeń, przez wyniki do wniosków, zostały przedstawione w sposób logiczny. Ponadto, większość ważnych pojęć pojawiających się w tej części jest jasno wytłumaczonych. Czytelnik może łatwo zrozumieć główne tezy pracy oraz wagę otrzymanych wyników.

Same trzy prace składają się z części głównej i dodatków, w których zawarto bardziej szczegółowe wyprowadzenia i inne szczegółowe informacje, a układ ich treści odzwierciedla wymogi czasopism, w których zostały opublikowane. Myślę, że pierwsza praca [PRA 94, 022305 (2016)] skorzystałaby, gdyby była nieco dłuższa i autorzy dokładniej opisaliby podprotokoły i podaliby kilka przykładów obrazujących działanie ich protokołu.

Poprawność (formalna, językowa, stylistyczna):

Rozprawa została spisana w języku angielskim i zawiera streszczenie w języku polskim i angielskim. Całość jest napisana w sposób staranny i przystępny. Poza kilkoma literówkami, których nie sposób uniknąć w obszernych rozprawach doktorskich, nie zauważyłem błędów językowych i stylistycznych. Dodatkowo, należy podkreślić fakt, że w podsumowaniu Doktorant stara się unikać żargonu, który jest dość rozwinięty w tej dziedzinie badań, dzięki czemu nawet osoba nie będąca specjalistą w tej dziedzinie może zrozumieć główne idee rozprawy. Żargon pojawia się w samych pracach, lecz jest to nieuniknione w specjalistycznych publikacji naukowych.

Dobór literatury:

Każda z trzech przedstawionych prac zawiera własny zbiór literatury, a najważniejsze pozycje są również przytoczone w podsumowaniu. Uważam, że Doktorant cytuje wszystkie ważne prace, które w istotny sposób są powiązane z tematyką poruszaną w rozprawie. Chciałbym również wspomnieć, że bardzo spodobała mi się anegdota z książki Kahna, która została przytoczona na samym początku rozprawy. Wspomniana anegdota w bardzo obrazowy sposób motywuje potrzebę prac nad protokołami DI. Drobna uwaga (przeoczenie) – w pracy [arXiv1709.04898] pozycje literatury [4] i [10] są identyczne.

Inne uwagi:

1) W pracy [PRA 94, 022305 (2016)] wielokrotnie wspomina się grę GHZ (jako element protokołu ekspansji losowości), jednak brakuje prostego wytłumaczenia, choćby w kilku zdaniach, czym ona jest. Myślę, że warto aby czytelnik mógł to zrozumieć bez potrzeby odnoszenia się do innych pozycji literatury. Domyślam się, że chodzi o uogólnienie gry CHSH na większą liczbę graczy (lub bitów wejściowych i wyjściowych) przy użyciu wielocząstkowego paradoksu GHZ. Jednak, jak dokładnie w tym przypadku formułuje się paradoks GHZ w języku teorii gier?

2) W pracy [PRL 120, 230503] autorzy poszukują tzw. nieredukowalnych (irreducible) świadków wymiaru i wspominają, że takie narzędzia pozwalają na stwierdzenie, czy badany układ jest rozkładalny (decomposable) – np. w abstrakcie. Myślę jednak, że pojęcie rozkładalności w tym kontekście wprowadza trochę czytelnika w błąd, gdyż problem rozkładalności w większości problemów informatyki kwantowej wiąże się ze stwierdzeniem, czy dany układ składa się z więcej niż jednej części. W tym przypadku, układ może składać się z wielu części, lecz zakłada się (co zostało wspomniane w tekście, lecz moim zdaniem nie zostało wystarczająco podkreślone) produktowe operacje i pomiary – brak możliwości splątania układów.

3) Kolejne pytanie do pracy [PRL 120, 230503] odnosi się do układu eksperymentalnego, lecz chodzi mi o konkretną interpretację teoretyczną pomiarów. Zakłada się, że do implementacji użyto pojedynczych fotonów, które w efekcie generują pojedyncze kliki na detektorze. Gdyby jednak użyto klasycznej wiązki światła, to w zasadzie wyniki byłyby takie same (tak na dobrą sprawę autorzy sami przyznają, że nie zawsze generują pojedyncze fotony). Mielibyśmy zatem klasyczny układ, który daje nam ograniczenie kwantowe, a nie klasyczne. Jak to zinterpretować?

4) W pracy [arXiv1709.04898] pokazano, że zmodyfikowana wersja kwantowego protokołu RAC może być wykorzystana do poszukiwania ilości baz wzajemnie komplementarnych w danym wymiarze. Jednakże, wspomniano również bazy, które są w przybliżeniu wzajemnie komplementarne (np. w pracach [20,21]). Choć to nie jest celem pracy, myślę, że przydałaby się dyskusja praktycznego znaczenia istnienia takich baz. Dokładniej, czy istnienie baz wzajemnie komplementarnych może nam dać w praktyce coś więcej niż istnienie baz w przybliżeniu wzajemnie komplementarnych?

Wniosek końcowy:

Wyniki przedstawione w rozprawie są ważnym i oryginalnym wkładem do kwantowej teorii informacji i podstaw fizyki kwantowej. Rozprawa spełnia z nawiązką wszystkie ustawowe i zwyczajowe wymogi, zatem wnioskuję o dopuszczenie mgr. Edgara Alexisa Aguilara Lozano do dalszych etapów przewodu doktorskiego. Ponadto, ze względu na doskonałą jakość otrzymanych wyników, wnioskuję o wyróżnienie rozprawy.

Paweł Kurzyński

Paweł Kurzyński