Gdańsk, 19.11.2024

Dr hab. Marcin Pawłowski, prof. UG
Międzynarodowe Centrum Teorii Technologii Kwantowych
Uniwersytet Gdański

Rada Naukowa Dyscypliny Nauki Fizyczne
Uniwersytet Warszawski

Recenzja

Rozprawa doktorska magister Gabriela Pereiry Alvesa zatytułowana jest „Nielokalność Bella i certyfikacja urządzeń kwantowych". Jej formą jest cykl publikacji, w którego skład wchodzą dwa artykuły opublikowane w recenzowanych czasopismach „Optimality of any pair of incompatible rank-one projective measurements for some nontrivial Bell inequality", oraz "Biased random access codes". Oba zostały opublikowane w Physical Review A. Oprócz tego w skład rozprawy wchodzi, opublikowana wyłącznie jako pre-print : "Machine Learning meets the CHSH scenario". Wszystkie wyżej wymienione prace dotyczą certyfikacji zasobów kwantowych i tworzą wewnętrznie spójną całość.

Rozprawa składa się z czterech części. W pierwszym rozdziale znajduje się ogólne wprowadzenie do tematyki certyfikacji zasobów kwantowych. Rozdział drugi uszczegóławia je odnosząc się bezpośrednio do problemów, które autor rozważał w publikacjach. Rozdział trzeci zawiera trzy wymienione w poprzednim akapicie prace wraz z krótkimi komentarzami oraz oświadczeniami o wkładzie autora w ich powstanie. Rozprawa zakończona jest krótkim podsumowaniem. Całość rozprawy napisana jest po angielsku w sposób zrozumiały bez zbędnego żargonu.

O ile styl samych publikacji stanowiących serce rozprawy nie budzi zastrzeżeń, biorąc pod uwagę niewielką objętość tekstu nie będącego publikacjami uważam, że autor mógł włożyć więcej wysiłku w lepszą prezentację wyników. Jest w rozprawie kilka zdań, które nic nie wnoszą, na przykład ustalenie, który stan kwantowy jest podstawowy, a który wzbudzony zaraz po równaniu (1.1). Nigdzie w dalszej części pracy nic od tego nie zależy, w dodatku w większości eksperymentów, które mogłyby wykorzystać wyniki tej rozprawy, oba stany miałby tę samą energię. Innym przykładem jest komentarz na temat algorymów kodowania i dekodowania na stronie 11. Ponieważ algorytm Ekreta dotyczy dystrybucji klucza, a nie całości bezpiecznej komunikacji, nie jest istotne w jaki sposób informacja jest szyfrowana. W dodatku cały ten komentarz (ostatnie 2 zdania pierwszego akapitu punktu 1.2) jest trudny do zrozumienia. Podobnie jest ze stwierdzeniem na następnej stronie: „In other words, Ekert's approach only requires the devices to be pre-tested." Nie jestem w stanie zrozumieć co autor mógł mieć przez nie na myśli. Ostatni rozdział, zatytułowany: „Concluding remarks" nie wnosi nic nowego tylko powtarza informacje, które już zostały wcześniej przekazane. Uważam, że dobrą praktyką jest zamieszczenie w tej części wpływu otrzymanych wyników oraz możliwym dalszych kierunków prac.

Nie wszystkie jednak moje uwagi dotyczące prezentacji są negatywne. Podoba mi się umieszczenie przed każdą publikacją krótkiego komentarza, gdzie nie tylko opisany jest wkład autora, ale także przedstawione jest krótkie streszczenie wyników łączące publikację z treścią rozdziału 2. Strona językowa pracy też jest dość dobra choć znalazłem parę literówek i niezręcznych sformułowań, których ze względu na to, że nie są zbyt istotne, nie będę tu wypisywał.

Przechodząc do komentarzy merytorycznych zacznę od wstępu, gdzie na stronie 6 autor pisze: „local causality, i.e., no effect can propagate faster than the speed of light". Lokalna przyczynowość to zasada, która mówi, że nie można przesłać informacji (każde wywarcie jakiegokolwiek wpływu wiąże się z przesłaniem informacji) bez nośnika. Prędkość światła wchodzi do gry dopiero wtedy, kiedy dodatkowo założymy, że jest to maksymalna prędkość, z którą mogą poruszać się te nośniki. Jest to oczywiście dość bezpieczne założenie, uzasadnione przez dekady prac naukowych i eksperymentów, ale to samo tyczy się kwantowej nielokalności. Jeśli prowadzimy rozważania na podstawowym poziomie dobrze jest rozdzielić lokalną przyczynowość od konkretnego ograniczenia na prędkość. Ma to szczególne znaczenie w kryptografii, gdzie w analizie bezpieczeństwa zakładamy, że kontrolujemy kanały boczne, czyli nie zachodzi niekontrolowany wyciek informacji z urządzeń. W takim wypadku użytkownicy protokołu opartego o łamanie nierówności Bella nie muszą być oddaleni przestrzennopodobnie, aby nie musieć martwić się o *locality loophole*. Gdyby zastosować taką definicję jak autor we wstępie miałoby to istotny, negatywny wpływ na praktyczne zastosowania kryptografii kwantowej niezależnej od urządzeń.

O samych publikacjach wchodzących z skład rozprawy mam bardzo dobrą opinię. Autor rozwiązuje w nich wysoce nietrywialne problemy wykazując się bardzo dobrym opanowaniem zarówno metod analitycznych jak i numerycznych.

W pierwszej z nich przedstawiona jest rodzina nierówności Bella, która pozwala na samo-testowanie szerokiego zestawu pomiarów kwantowych. Sprowadza się to do udowodnienia, że dla każdej pary pomiarów należących do określonego zbioru istnieje nierówność Bella, która jest przez nie maksymalnie łamana. Autorzy publikacji, już w tytule, twierdzą, że tym zbiorem są wszystkie niekompatybilne projektory rzędu 1, ale definicja niekompatybilności, którą stosują nie jest standardowa. Wymagają oni, aby każda para wektorów bazowych miała iloczyn skalarny ściśle mniejszy od 1. Pokazują ponadto, że jeśli to nie zajdzie to konkretna nierówność Bella z rodziny przez nich zaproponowanej nie będzie łamana, ale nie znaczy to, że nie istnieje inna nierówność dla której to zajdzie. Na publicznej obronie chciałbym dowiedzieć się czy autor widzi możliwość uogólnienia rezultatów na wszystkie pomiary spełniające standardową definicję niekompatybilności oraz jaki jest związek pomiędzy nimi.

Druga praca dotyczy kodów swobodnego dostępu (ang. *Random Access Codes* - RACs) czyli zadań, w których jedna strona musi skompresować informację tak aby zmaksymalizować prawdopodobieństwo poprawnej dekompresji konkretnych części wiadomości przez stronę drugą. Jest to dość dobrze zbadany obszar, w którym zwykle, jako miarę efektywności stosuje się średnie prawdopodobieństwo poprawnej dekompresji. Autorzy pracy "Biased random access codes", jak sam tytuł sugeruje, uogólnili problem poprzez rozważenie średniej ważonej. Publikacja zawiera zestaw wyników analitycznych i numerycznych dotyczących tego, uogólnionego zagadnienia. Co więcej autorzy udostępniają bibliotekę w Pythonie pozwalającą użytkownikom na usprawnienie innych prac nad kodami RAC.

Ostatnia praca dotyczy uczenia maszynowego, a dokładnie klasyfikacji czy dany rozkład prawodpodobieństwa może zostać uzyskany za pomocą kwantowych zasobów czy nie. W tym przypadku moje główne zastrzeżenie dotyczy celowości pracy. Aby przygotować zestaw danych treningowych wykorzystywane są konkretne algorytmy, a z praktyki wiadomo, że modele uczone na tak przygotowanych zbiorach nie są szczególnie dobre. Jednak efektywność algorytmu nie jest największym problemem. Jest nim to w jakiej sytuacji może być on stosowany. Trudno mi taką znaleźć. Jeśli w praktyce otrzymamy jakiś rozkład prawdopodobieństwa to powinien on być kwantowy, w innym przypadku byłoby to odkrycie na taką skalę, że dowód w postaci decyzji algorytmu ML byłby niewystarczający. Jeśli natomiast rozkład prawdopodobieństwa został wygenerowany przez określony algorytm, twórcy tego algorytmu, albo z góry wiedzą czy jest kwantowy, albo jest to istotą ich badań i znów dowód w postaci decyzji programu nie jest wystarczający, szczególnie jeśli jest to program nauczony na zbiorze treningowym wygenerowanym proceduralnie.

Pomimo moich licznych krytycznych komentarzy, moja ogólna ocena rozprawy jest pozytywna. Problemy rozwiązane w publikacjach (zwłaszcza tych opublikowanych w Phys. Rev. A) wnoszą istotny wkład w naszą wiedzę i pomagają rozwijać dziedzinę. Dlatego uważam, że rozprawa magister Gabriela Pereiry Alvesa spełnia wymogi zarówno formalne jak i zwyczajowe stawiane pracom doktorskim i wnioskuję o dopuszczenie jej do dalszych etapów przewodu doktorskiego.

Z poważaniem,

Marcin Pawłowski