Warszawa, 01.09.2022

Shubhayan Sarkar
Centrum Fizyki Teoretycznej PAN
Aleja Lotników 32/46
02-668 Warszawa

Streszczenie rozprawy doktorskiej

"Certification of entangled quantum states and quantum measurements in Hilbert spaces of arbitrary dimension"

Powstanie teorii kwantów na początku XX wieku zmieniło nasz pogląd na świat mikroskopowy i doprowadziło do powstania takich zastosowań efektów kwantowych jak teleportacja kwantowa, kwantowe generowanie liczb losowych i obliczenia kwantowe. Żadne z nich nie mogło by zostać zrealizowane w ramach fizyki klasycznej. Jednym z takich zastosowań, które przyciągnęło ostatnio wiele uwagi, jest certyfikacja złożonych układów kwantowych w wersji niezależnej od urządzeń (ang. *device-independent*). Podstawową jej ideą jest traktowanie danego urządzenia jak czarną skrzynkę, która po podaniu danych wejściowych generuje dane wyjściowe, a następnie wykorzystane obserwowanych statystyk do sprawdzenia, czy urządzenie to działa zgodnie z oczekiwaniami. Nowatorskość schematów certyfikacji tego typu polega na tym, że można prawie całkowicie scharakteryzować urządzenie (z dokładnością do pewnych równoważności) przy minimalnych, dobrze umotywowanych fizycznie założeniach, takich jak to, że urządzenie działa zgodnie z zasadami fizyki kwantowej. Zasobem kwantowym wykorzystywanym przez większość tych schematów certyfikacji jest nielokalność Bella.

Wiele pracy włożono ostatnio w stworzenie schematów certyfikacji w wersji niezależnej od urządzeń dla złożonych układów kwantowych. Większość z nich stosuje się jednak do układów o relatywnie niskich wymiarach lokalnych, w szczególności do stanów dwukubitowych. W tej pracy rozważamy problem projektowania ogólnych schematów, które mają zastosowanie do układów kwantowych o dowolnych wymiarach lokalnych. Najpierw konstruujemy w schemat certyfikacji, znany również jako samotestowanie, który pozwala certyfikować uogólnione stany Greenbergera-Horne'a-Zeilingera (GHZ) o dowolnym wymiarze lokalnym dzielony przez dowolną liczbę obserwatorów na podstawie maksymalnego łamania pewnej rodziny nierówności Bella; w szczególnym przypadku dwóch podukładów stan GHZ sprowadza się do stanu maksymalnie splątanego dwóch kuditów. Co ważne, jest to pierwszy przypadek, w którym takie stany kwantowe mogą być certyfikowane przy użyciu tylko dwóch pomiarów przez każdego z obserwatorów, co jest w rzeczywistości minimalną liczbą pomiarów wymaganą do zaobserwowania nielokalności Bella.

Choć w ostatnich latach dokonano znacznego postępu w projektowaniu schematów certyfikacji w wersji niezależnej od urządzeń, większość z nich dotyczy splątanych stanów kwantowych. Jednocześnie problem certyfikacji pomiarów kwantowych pozostaje w dużej mierze niezbadany. Brakuje w szczególności ogólnego schematu pozwalającego na certyfikację dowolnego zestawu niekompatybilnych pomiarów kwantowych. Ponieważ stworzenie takiego schematu w scenariuszu niezależnym od urządzeń jest trudnym zadaniem, w rozprawie rozważamy pewien uproszczony scenariusz, znany jako scenariusz jednostronnie niezależny od urządzeń (1SDI). W tym scenariuszu czynimy dodatkowe założenie, że jedno z urządzeń pomiarowych jest w pełni scharakteryzowane i wykonuje znane pomiary kwantowe. Proponujemy schemat certyfikacji ogólnej klasy pomiarów rzutowych, określanych tu jako prawdziwie niekompatybilne. W tym celu konstruujemy rodzinę nierówności sterowania (ang. *steering inequalities*), których maksymalna wartość kwantowa osiągana jest przez dowolny zbiór prawdziwie niekompatybilnych pomiarów. Co ciekawe, do tej klasy pomiarów kwantowych zaliczają się te, które odpowiadają bazom wzajemnie

niejednoznacznym. Wreszcie, w scenariuszu 1SDI, konstruujemy rodzinę nierówności sterowania, których maksymalne łamanie może być wykorzystane do certyfikacji dowolnego czystego, splątanego stanu dwucząstkowego przy użyciu minimalnej liczby dwóch pomiarów wykonywanych przez obu obserwatorów. Opierając się na tym wyniku, podajemy następnie metodę certyfikacji dowolnego ekstremalnego pomiaru kwantowego rzędu jeden, włączając w to pomiary nierzutowe.

Co ciekawe, metody samotestowania stanów oraz pomiarów kwantowych mogą być wykorzystane do stworzenia schematów poświadczania, że wyniki pomiarów wykonywanych na stanach kwantowych są losowe w tym sensie, że nie mogą być przewidziane przez żadnego zewnętrznego obserwatora. To sprawia, że nasze wyniki stają się użyteczne w zadaniach kryptograficznych. Najpierw pokazujemy, że ze splątanych stanów kwantowych o dowolnym wymiarze lokalnym można generować losowość w scenariuszu niezależnym od urządzeń używając pomiarów rzutowych. Następnie, w scenariuszu 1SDI, konstruujemy schemat poświadczający optymalną ilość losowości, która może być wygenerowana przy użyciu układu kwantowego o dowolnym wymiarze i nierzutowych pomiarów ekstremalnych, która równa jest dwukrotności maksymalnej ilości losowości, którą można wygenerować przy użyciu pomiarów rzutowych.

Shubhayan Sarkar.

Shubhayan Sarkar