

Rafael Freitas dos Santos
ul. Gen. W. Andersa 24/7
00-201 Warszawa

Streszczenie rozprawy doktorskiej
***“Certification of quantum states and measurements
in contextuality scenarios”***

Teoria kwantowa to teoria probabilistyczna, która opisuje układy fizyczne o małej skali, takie jak atomy czy fotony, i jest jedną z najskuteczniejszych teorii fizycznych, które zostały zweryfikowane eksperymentalnie z dużą dokładnością. Jednocześnie przewiduje zjawiska takie jak splątanie kwantowe, nielokalność Bella czy bardziej ogólnie kontekstualność kwantową, które zostały przekute w zasoby dla pewnych zastosowań, które nie są dostępne w fizyce klasycznej. Co więcej, zjawiska te są odpowiedzialne za szybki rozwój nowych technologii kwantowych, który się w ostatnim czasie odbywa, żeby tylko wspomnieć komputery kwantowe. Z punktu widzenia możliwości pełnego wykorzystania technologii kwantowych, za tym rozwojem musi podążać tworzenie odpowiednich narzędzi certyfikujących, które umożliwiłyby klasycznemu użytkownikowi sprawdzenie lub poświadczenie, że dane urządzenie działa zgodnie ze swoją specyfikacją i generuje prawidłowy wynik. Takie narzędzia certyfikacji są szczególnie istotne w kontekście kryptografii kwantowej, gdzie komunikujące się strony muszą zweryfikować, czy stan udostępniany przez strony, jak również wykonane przez nie pomiary są prawidłowe.

Pomimo tego, że istnieją metody służące powyższemu celowi, jak na przykład dobrze znana tomografia kwantowa, opierają się one na pewnych założeniach, takich jak to, że urządzenia pomiarowe używane do badania stanu są w pełni scharakteryzowane i że użytkownik ma pewność, że wykonują prawidłowe pomiary. O ile w niektórych sytuacjach takie założenia są uzasadnione, o tyle przypadku takich zadań jak kryptografia kwantowa już nie. Jako remedium na ten problem, Mayers i Yao zaproponowali ideę samotestowania. Pozwala ono na niemal pełną charakteryzację układów kwantowych w oparciu o wytwarzane przez nie korelacje nieklasyczne, bez konieczności czynienia założeń na temat tych urządzeń. Samotestowanie jest zatem sposobem certyfikacji w wersji niezależnej od urządzeń (ang. *device-independent*), w której urządzenia kwantowe są traktowane jak czarne skrzynki, których wewnętrzne działanie jest nieznane dla użytkownika, a nieklasyczność, jaką generują, jest tym zasobem, który pozwala wyciągać nietrywialne wnioski na ich temat.

Samotestowanie, w swoim pierwotnym sformułowaniu opiera się na nielokalności Bella i umożliwia certyfikację stanów splątanych i wykonanych na nich pomiarów kwantowych. Choć powstało już wiele metod samotestowania splątanych stanów kwantowych zarówno w przypadku dwuciałowym, jak i wieloczęściowym, większość z nich, szczególnie w tym drugim przypadku, poświęcona jest układom składającym się z kubitów. Co więcej, metody certyfikacji tego typu są rzadko badane w przypadku układów, które nie mają podukładów oddzielonych przestrzennie i tym samym nie wykazują nielokalności Bella. Naszym celem jest wypełnienie powyższych luk. Z jednej strony badamy możliwość wykorzystania kontekstowości kwantowej do celów certyfikacji. W tym kierunku wprowadzamy klasę skalowalnych nierówności niekontekstualnych, których maksymalne łamanie kwantowe można wykorzystać do certyfikacji układów kwantowych składających się z N kubitów i zbiorów pomiarów binarnych, które spełniają pewne relacje komutacyjne i antykomutacyjne i generują N -kubitową grupę Pauliego. Po drugie, proponujemy schemat, który jest modyfikacją

standardowego scenariusza kontekstualności kwantowej, a który pozwala na formułowanie certyfikujących o układach kwantowych na podstawie zaobserwowanych korelacji, ale bez konieczności czynienia założeń na temat struktury kompatybilności wykonywanych pomiarów, które się standardowo czyni w przypadku metod certyfikacji opartych na standardowej kontekstualności. Z drugiej strony rozwijamy zastosowanie nielokalności Bella, która jest pewną szczególną formą kwantowej kontekstualności, w samotestowaniu. Wprowadzamy pierwszą, zgodnie z naszą najlepszą wiedzą, ogólną klasę nierówności Bella, które są maksymalnie łamane przez wielocząstkowe stany grafowe o dowolnym wymiarze lokalnym, który liczbą pierwszą, a także pokazujemy, że w przypadku kutrytowym maksymalne łamanie tych nierówności pozwala na samotestowanie stanów grafowych. Podobnie jak w powyższym przypadku nasze nierówności są skalowalne w tym sensie, że liczba wartości oczekiwanych, z których się składają skaluje się liniowo z liczbą podukładów co ma znaczenie z punktu widzenia ich zastosowań w eksperymencie.



Rafael Freitas dos Santos