

dr Jędrzej Kaniewski
Wydział Fizyki, Uniwersytet Warszawski
Pasteura 5, 02-093 Warszawa

Autoreferat

1. Imię i nazwisko

Jędrzej Kaniewski

2. Posiadane dyplomy, stopnie naukowe lub artystyczne – z podaniem podmiotu nadającego stopień, roku ich uzyskania oraz tytułu rozprawy doktorskiej.

Licencjat z nauk ścisłych i przyrodniczych (ang. *Bachelor of Arts in Natural Sciences*) (Uniwersytet w Cambridge, 2011)

Magister z matematyki (ang. *Master of Advanced Study in Mathematics*) (Uniwersytet w Cambridge, 2011)

Doktorat z fizyki (Narodowy Uniwersytet w Singapurze, 2015)

Tytuł rozprawy: Relativistic quantum cryptography

3. Informacja o dotychczasowym zatrudnieniu w jednostkach naukowych lub artystycznych.

W roku 2011 ukończyłem 4-letnie studia na Uniwersytecie w Cambridge. W grudniu 2011 rozpocząłem studia doktoranckie na Narodowym Uniwersytecie w Singapurze pod opieką prof. Stephanie Wehner. Doktorat obroniłem w grudniu 2015 roku. Chociaż przez cały ten czas byłem formalnie doktorantem w Singapurze, to od października 2014 grupa badawcza, w której pracowałem, przeniosła się na Uniwersytet Techniczny w Delft w Holandii i tam spędziłem ostatni rok doktoratu.

W styczniu 2016 rozpocząłem zatrudnienie na stanowisku postdoka w grupie prof. Matthiasa Christandla na Uniwersytecie w Kopenhadze. Od marca 2017 do czerwca 2018 moje zatrudnienie było w całości finansowane z indywidualnego stypendium w ramach Marie Skłodowska-Curie Actions przyznanego przez Komisję Europejską.

Od lipca 2018 do czerwca 2019 byłem zatrudniony jako adiunkt w Centrum Fizyki Teoretycznej Polskiej Akademii Nauk, a moje zatrudnienie było w całości finansowane z grantu POLONEZ przyznanego przez Narodowe Centrum Nauki.

Od lipca 2019 jestem zatrudniony jako adiunkt na Wydziale Fizyki Uniwersytetu Warszawskiego, a moje zatrudnienie jest w całości finansowane z grantu HOMING przyznanego przez Fundację na Rzecz Nauki Polskiej. W 2020 roku zdobyłem grant SONATA z Narodowego Centrum Nauki, który pozwoli mi przedłużyć zatrudnienie na Uniwersytecie Warszawskim do końca 2023 roku.

4. Omówienie osiągnięć, o których mowa w art. 219 ust. 1 pkt. 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2020 r. poz. 85 z późn. zm.). Omówienie to winno dotyczyć merytorycznego ujęcia przedmiotowych osiągnięć, jak i w sposób precyzyjny określać indywidualny wkład w ich powstanie, w przypadku, gdy

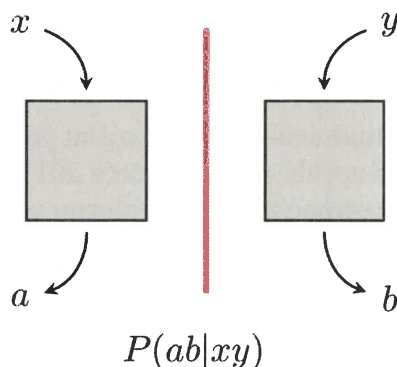
dane osiągnięcie jest dziełem współautorskim, z uwzględnieniem możliwości wskazywania dorobku z okresu całej kariery zawodowej.

Cykl habilitacyjny składa się z 9 prac naukowych opublikowanych w międzynarodowych czasopismach fizycznych, które koncentrują się na certyfikacji urządzeń kwantowych, a konkretniej dotyczą problemu samotestowania (ang. *self-testing*).

Certyfikacja urządzeń kwantowych skupia się na następującym pytaniu: jak w efektywny sposób zademonstrować, że dane urządzenie kwantowe działa zgodnie ze specyfikacją? Zagadnienie to występuje w wielu różnych formach w zależności od tego jakiego rodzaju urządzenia kwantowe chcemy badać (np. źródło stanów kwantowe, urządzenie pomiarowe albo kwantową bramkę logiczną), a także w jakim scenariuszu chcemy nasz proces testowania przeprowadzić (do jakich narzędzi mamy dostęp? jakie założenia chcemy przyjąć?).

Standardowym scenariuszem jest tzw. scenariusz tomograficzny, w którym chcemy przetestować nieznaną urządzenie kwantowe używając innych (zaufanego) urządzeń, np. testujemy źródło stanów kwantowych za pomocą zaufanego urządzenia pomiarowego. W tym przypadku certyfikacja staje się efektywnie problemem kalibracji i napotykamy na standardowy problem: jak skalibrować pierwsze urządzenie?

Okazuje się, że pewne formy certyfikacji są możliwe nawet jeśli nie mamy dostępu do żadnego zaufanego urządzenia. W naszym przypadku koncentrujemy się na tzw. scenariuszu Bella (patrz Rysunek 1), w którym mamy do dyspozycji dwa urządzenia kwantowe, które dzielą między sobą jakiś splątany stan kwantowy. Każde urządzenie może lokalnie wykonać jeden z kilku możliwych pomiarów kwantowych. Należy podkreślić, że nasza interakcja z każdym urządzeniem jest w pełni klasyczna: zarówno wybór, którego pomiaru dokonać jak i odczytanie jego wyniku odbywa się przez klasyczną wymianę informacji.



Rysunek 1: Dwuczęściowy scenariusz Bella. Dwa niekomunikujące się urządzenia kwantowe wykonują pomiary oznaczone przez x, y i generują wyniki oznaczone przez a, b . Konkluzje w tym scenariuszu bazują jedynie na obserwowanych statystykach oznaczonych przez $P(ab|xy)$ i założeniu, że w trakcie eksperymentu komunikacja między urządzeniami nie jest możliwa.

Zaletą scenariusza Bella jest możliwość przeprowadzenia eksperymentu, który pozwala odróżnić urządzenia kwantowe od klasycznych przy tylko jednym założeniu: że urządzenia w trakcie eksperymentu nie mogą się w żaden sposób komunikować. Jeśli zaobserwujemy korelacje, które nie mogą być wytłumaczone przez żadną teorię klasyczną, mówimy o łamaniu nierówności Bella i zjawisko to jest fundamentalne dla podstaw mechaniki

kwantowej. Te teoretyczne przewidywanie zostały wielokrotnie zweryfikowane w eksperymentach na różnych kwantowych platformach.

Oryginalnym celem testu Bella było znalezienie prostej sytuacji fizycznej, która przy minimalnych założeniach pozwoli nam odróżnić mechanikę kwantową od teorii klasycznych. Certyfikacja urządzeń kwantowych w scenariuszu Bella może być interpretowana jako następny krok w tym kierunku: jeśli jesteśmy w stanie wydedukować, że w naszym doświadczeniu dzieje się coś nieklasycznego, to jeśli przyjmiemy, że nasze urządzenia są kwantowe, powinniśmy być w stanie wyciągnąć dalsze wnioski na ich temat. Typowym zadaniem w scenariuszu Bella jest certyfikacja splątania pomiędzy urządzeniami (splątanie jest niezbędne do łamania nierówności Bella).

Samotestowanie jest najbardziej kompletną formą certyfikacji w scenariuszu Bella. W sytuacji bezszumowej pozwala nam jednoznacznie zidentyfikować stan kwantowy i pomiary na nim wykonane (z dokładnością do dwóch naturalnych, nieusuwalnych klas transformacji). Wynika to z faktu, że w scenariuszu Bella niektóre szczególnie silne korelacje kwantowe mogą być zrealizowane tylko w jeden sposób, co jest wysoce nietrywialnym stwierdzeniem.

W cyklu habilitacyjnym pracowałem nad następującymi pytaniami:

1. Jakie struktury kwantowe (stany, pomiary) mogą być samotestowane?
2. Jak zachowuje się zjawisko samotestowania w realistycznych scenariuszach, tzn. w obecności szumu?
3. Czy zjawisko samotestowania można rozszerzyć na inne scenariusze kwantowe i jeśli tak, to przy jakich założeniach?
4. Czy istnieją przypadki, w których zjawisko samotestowania nie zachodzi, i do poprawnego opisu należy wprowadzić nowe, słabsze formy certyfikacji?

Poniżej przedstawiam szczegółowy opis osiągnięć opisanych we wszystkich pracach z cyklu habilitacyjnego (kolejność chronologiczna).

W pracy [1] skupiam się na problemie samotestowania w relacji do nierówności Clauser-Horne-Shimony-Holt (CHSH) i Mermina. Wiadome jest, że maksymalne łamanie nierówności CHSH wymaga obecności maksymalnie splątanego stanu dwóch kubitów. Celem tej pracy była analiza w jakim stopniu samotestowanie stanu kwantowego jest odporne na szum. W pracy tej wprowadziłem nową metodę samotestowania opartą na nierównościach operatorowych i zademonstrowałem jej użyteczność w dwóch powyższych sytuacjach. W przypadku CHSH, gdzie maksymalna wartość kwantowa wynosi $2\sqrt{2} \approx 2.83$, a wartość klasyczna wynosi 2, pokazałem, że nietrywialna certyfikacja stanu jest możliwa jeśli obserwowane łamanie przekracza wartość ≈ 2.11 (wcześniej wiadomym było, że próg wynosi przynajmniej ≈ 2.39). Nierówność Mermina jest nierównością dla 3 układów kwantowych i maksymalne jej łamanie wymaga trzykubitowego stanu Greenberger-Horne-Zeilinger (GHZ). Kwantowa wartość nierówności Mermina wynosi 4, a w pracy pokazałem, że nietrywialna certyfikacja bliskości do stanu GHZ jest możliwa jeśli zaobserwowane łamanie przekracza wartość $2\sqrt{2}$. Ta wartość graniczna może być łatwo wyjaśniona zauważając, że jest ona osiągalna w sytuacji, kiedy tylko dwa urządzenia dzielą splątanie (dwuczęściowe splątanie nie może dać nietrywialnego wyniku w certyfikacji stanu GHZ, które zawiera splątanie trzyczęściowe). To pokazuje, że wynik samotestujący wyprowadzony dla nierówności Mermina jest optymalny.

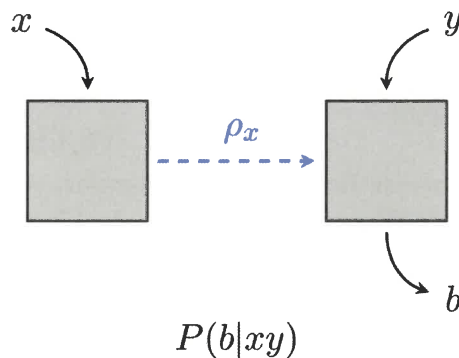
Wkład wnioskodawcy: Praca [1] jest pracą jednoautorską.

W pracy [2] rozważam problem samotestowania pomiarów kwantowych. Należy wspomnieć, że wcześniejsze prace z samotestowania skupiały się na samotestowaniu stanów, a samotestowanie pomiarów było traktowane jedynie jako mniej istotny wynik poboczny. W związku z tym nie było nawet jasną definicją należy przyjąć do problemu samotestowania pomiarów. Ja rozważyłem problem samotestowania dwóch pomiarów dwuwynikowych (binarnych) i zauważyłem, że definicję samotestowania takich obserwabli można oprzeć w całości na relacjach komutacyjnych między nimi. Wiadomym było, że im mocniej dwie obserwabli nie komutują, tym większa ich niekompatybilność. W tej pracy pokazałem, że dla pary binarnych obserwabli, spełnienie odpowiednich relacji komutacyjnych pozwala nam wydedukować, że obserwabli te są równoważne dwóm konkretnym pomiarom na kubicie. Z tych relacji komutacyjnych udało mi się zbudować miary, których potem użyłem do certyfikacji nieznanymi obserwabli. Głównym wynikiem tej pracy jest konkluzja, że każdą parę obserwabli na kubicie można samotestować, a ponadto samotestowanie według nowych definicji jest odporne na szum: nawet minimalne złamanie nierówności Bella prowadzi do ilościowej konkluzji na temat niekompatybilności nieznanymi pomiarów. Ponadto, nowe podejście pozwoliło mi zanalizować rodzinę wieloczęściowych nierówności Bella znanych jako nierówności Mermin-Ardehali-Belinskii-Klyshko (MABK). Rodzina ta jest indeksowana przez liczby całkowite $n \geq 2$. Dla $n=2$ otrzymujemy nierówność CHSH, a dla $n=3$ nierówność Mermina. W tej pracy pokazałem, że dla dowolnej liczby n nierówność ta ma własność samotestowania. Innymi słowami, do osiągnięcia maksymalnego łamania wymagany jest n -qubitowy stan GHZ, a lokalne pomiary muszą odpowiadać maksymalnie antykomutującym obserwabliom (np. obserwabli Pauliego X i Z).

Wkład wnioskodawcy: Praca [2] jest pracą jednoautorską.

W pracy [3] wraz ze współpracownikami z Uniwersytetu w Genewie, Instytutu Badań Nuklearnych w Debrecenie (Węgry) i Perimeter Institute w Waterloo (Kanada) pokazaliśmy, że koncept samotestowania można rozszerzyć do scenariuszy innych niż scenariusze Bella. Pokazaliśmy, że zjawisko samotestowania występuje w nietrywialnej formie w scenariuszach "przygotuj-i-zmierz" (ang. *prepare-and-measure*; patrz Rysunek 2) jeśli jako dodatkowe założenie wprowadzi się ograniczenie górne na wymiar układu kwantowego przesłanego między urządzeniami. W tej pracy skupiliśmy się na najprostszym możliwym przypadku czyli tzw. kwantowym kodzie losowego dostępu (ang. *quantum random access code*) w którym 2 klasyczne bity są kodowane w postaci pojedynczego kubitu. Pokazaliśmy, że optymalna kwantowa strategia w tym zadaniu jest unikalna (z dokładnością do wyboru bazy czyli operacji unitarnej) i polega na zakodowaniu czterech możliwych kombinacji w czterech stanach czystych, które geometrycznie tworzą kwadrat na sferze Blocha, a następnie wykonaniu pomiarów w dwóch bazach wzajemnie nieobciążonych (ang. *mutually unbiased bases*) na kubicie. Standardowa optymalna strategia zakłada wykonanie pomiarów w bazach własnych operatorów Pauliego X i Z , a wtedy przygotowane stany muszą odpowiadać wektorom własnym operatorów $(X \pm Z)$. W tej pracy pokazaliśmy również, że strategie, które osiągają wyniki bliskie optymalnym muszą być w dobrze zdefiniowanym znaczeniu bliskie strategii optymalnej. Aby to osiągnąć zbudowaliśmy dwa niezależne dowody pokazujące, że: (1) przygotowane stany kwantowe muszą być w przybliżeniu czyste i tworzyć kwadrat na sferze Blocha; (2) pomiary muszą być w przybliżeniu rzutowe i pierwszego rzędu i wzajemnie nieobciążone. Pierwszy z tych argumentów używał metody, którą zaproponowałem w pracy [1] do samotestowania w scenariuszu Bella.

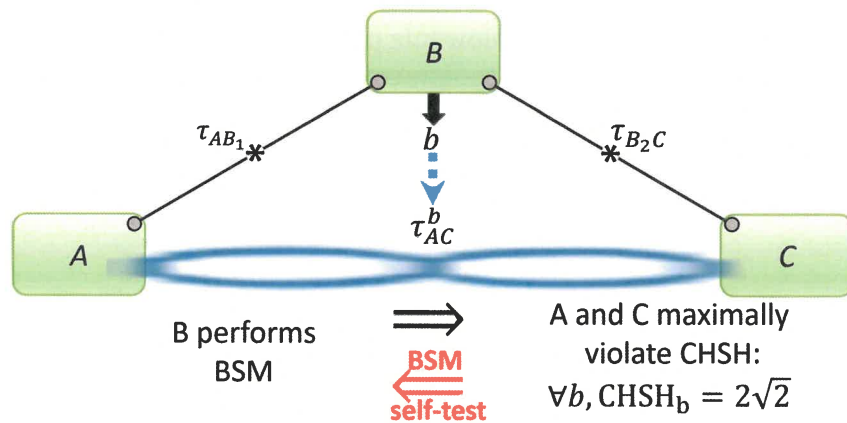
Wkład wnioskodawcy: Pomysł na zdefiniowanie pojęcia samotestowania w scenariuszach "przygotuj-i-zmierz" wyszedł ze strony współpracowników z Genewy, ja zostałem zaproszony do współpracy ze względu na moje doświadczenie w dziedzinie samotestowania. Razem z pierwszym autorem wyprowadziliśmy analityczne relacje samotestujące, byłem także odpowiedzialny za adaptację metody z pracy [1] do nowego scenariusza.



Rysunek 2: Scenariusz "przygotuj-i-zmierz". Źródło stanów kwantowych otrzymuje klasyczną informację x i generuje stan kwantowy o ustalonym wymiarze. Urządzenie pomiarowe wykonuje pomiar oznaczony przez y i zwraca wynik pomiarowy b . Konkluzje w tym scenariuszu bazują jedynie na obserwowanych statystykach oznaczonych przez $P(b|xy)$ i założeniu, że wymiar wymienionego układu kwantowego jest ograniczony.

W pracy [4] we współpracy z badaczami z Uniwersytetu w Genewie rozszerzyliśmy koncept samotestowania do scenariusza Bella, w którym biorą udział trzy urządzenia, a stany kwantowe są generowane przez dwa niezależne źródła (patrz Rysunek 3). Celem tego scenariusza było pokazanie przy minimalnych założeniach, że urządzenie B, które otrzymuje dwa układy kwantowe z dwóch różnych źródeł realizuje procedurę wymiany splątania (ang. *entanglement swapping*). Pokazaliśmy, że jeśli urządzenia A i C wskazują na maksymalne łamanie pewnego wariantu nierówności CHSH (wariant ten zależy od klasycznego wyniku uzyskanego przez urządzenie B), to rzeczywiście jesteśmy w stanie w całości scharakteryzować nieznaną układy kwantowe korzystając jedynie z założenia o niezależności źródeł. Rozważyliśmy także przypadek, w którym zaobserwowane łamanie CHSH nie jest maksymalne. Aby to zrobić musieliśmy zdefiniować co to znaczy, że pomiar kwantowy działający na iloczyn tensorowy dwóch przestrzeni Hilberta jest równoważny (albo chociaż podobny) pomiarowi w bazie Bella wykonanego na dwóch kubitach. Definicja, którą przyjęliśmy jest oparta na całkowicie dodatnich mapach unitalnych. Dla takiej definicji udało nam się pokazać, że jeśli urządzenia A i C obserwują wysokie (ale niekoniecznie maksymalne) łamanie nierówności CHSH to pomiar wykonany przez B musi być podobny do pomiaru w bazie Bella. Matematyczne wyprowadzenie tego wyniku wykorzystuje główny wynik z pracy [1] jako jeden ze składników.

Wkład wnioskodawcy: Razem z pierwszym autorem wyprowadziliśmy analityczną charakteryzację wszystkich urządzeń w przypadku braku szumu. Samodzielnie pokazałem jak zaadaptować metodę z pracy [1] do scenariusza z niezależnymi źródłami, co wymagało znalezienia analitycznego rozwiązania dla rodziny problemów dodatniookreślonych (ang. *semidefinite program*).



Rysunek 3: Scenariusz Bella z dwoma niezależnymi źródłami, w którym można certyfikować splątane pomiary kwantowe.

W pracy [5] wraz ze współpracownikiem z Uniwersytetu Gdańskiego (pan Mate Farkas; byłem promotorem pomocniczym jego pracy doktorskiej) pokazaliśmy, że samotestowanie w scenariuszach "przygotuj-i-zmierz" występuje także w przypadku wysokowymiarowych kwantowych kodów losowego dostępu. Rozważyliśmy standardowy przypadek, w którym 2 klasyczne dity (dit = jednostka klasycznej informacji przyjmująca d możliwych wartości) są kodowane w jednym kudicie (kudit = d -wymiarowy układ kwantowy). Poprzednio było wiadomo, że w takim zadaniu jeśli urządzenie pomiarowe jest ograniczone do pomiarów w bazie (tzn. wykonuje pomiary rzutowe, których operatory pomiarowe są pierwszego rzędu), to optymalne pomiary odpowiadają bazom wzajemnie nieobciążonym. Pierwszym wynikiem naszej pracy jest fakt, że lepszych wyników nie da się uzyskać używając najbardziej ogólnych pomiarów kwantowych. Ponadto, pokazaliśmy, że optymalny wynik jest możliwy wtedy i tylko wtedy jeśli użyte pomiary odpowiadają dwóm bazom wzajemnie nieobciążonym. Udało nam się też pokazać, że strategie, które osiągają wyniki bliskie optymalnym muszą być zbliżone do strategii optymalnej, m.in. pokazaliśmy, że w przybliżeniu: (1) operatory pomiarowe muszą być pierwszego rzędu, (2) ślady produktów operatorów pomiarowych muszą być rozłożone w sposób jednorodny, (3) pomiary muszą być tak niekompatybilne jak bazy wzajemnie nieobciążone i (4) pomiary muszą prowadzić do najsilniejszych możliwych relacji nieoznaczoności. Dla przypadków $d=3$ i $d=4$ certyfikacja jest możliwa przy realistycznym poziomie szumu i nasze wyniki teoretyczne zostały później potwierdzone w doświadczeniu ("Self-Testing Mutually Unbiased Bases in Higher Dimensions with Space-Division Multiplexing Optical Fiber Technology", Farkas et al., *Physical Review Applied* **15**, 014028 (2021)). Dowód matematyczny głównego wyniku jest oparty jedynie o proste właściwości macierzy, co sprawia, że nasz argument można stosować dla dowolnej wartości d i dla każdego d osiąga niezerową odporność na szum (aczkolwiek odporność na szum spada z rosnącym wymiarem). Warto też podkreślić, że choć nasza analiza dostarcza nam dokładnej wiedzy na temat pomiarów, nie jest to certyfikacja z dokładnością do operacji unitarnej (w wyższych wymiarach nie wszystkie pary baz wzajemnie obciążonych są równoważne). Ta obserwacja była kluczowa i doprowadziła nas do wyników opublikowanych później w pracy [9].

Wkład wnioskodawcy: Razem z pierwszym autorem wyprowadziliśmy analityczne relacje samotestowania.

W pracy [6] wraz ze współpracownikami z Uniwersytetu w Amsterdamie rozwinęliśmy metodę samotestowania zaproponowaną w pracy [1]. W oryginalnej pracy metoda ta była użyta, żeby uzyskać silną certyfikację stanu maksymalnie splątanego dwóch kubitów na podstawie łamania nierówności CHSH. W nowej pracy użyliśmy tej samej metody do samotestowania stanów częściowo splątanych dwóch kubitów na podstawie łamania przechylonej nierówności CHSH (ang. *tilted-CHSH inequality*). Pokazaliśmy, że także w tym przypadku nowa metoda daje wyniki w znacznej mierze odporne na szum. Ponadto, pokazaliśmy, że samotestowanie oparte na nierówności CHSH jest możliwe tylko jeśli obserwowane łamanie wynosi przynajmniej ≈ 2.0014 . Badania naukowe opublikowane w tej pracy mają swój początek w pracy magisterskiej pana Tima Coopmansa, której prof. Christian Schaffner i ja byliśmy współpromotorami.

Wkład wnioskodawcy: Byłem pomysłodawcą projektu, razem z pierwszym autorem wyprowadziliśmy zależności analityczne, a także nadzorowałem wykonanie obliczeń numerycznych przez pierwszego autora. Wspólnie zbudowaliśmy argument pokazujący niemożność samotestowania poniżej pewnego progu.

W pracy [7] wraz ze współpracownikami rozważaliśmy nowe nierówności Bella, skonstruowane w taki sposób, aby maksymalne łamanie było osiągalne za pomocą pomiarów w bazach wzajemnie nieobciążonych. Pokazaliśmy, że jeśli d jest liczbą pierwszą większą od 2, to możemy skonstruować nierówność Bella, której maksymalna wartość kwantowa jest osiągnięta przez stan maksymalnie splątany o lokalnym wymiarze d , a pomiary odpowiadają konkretnej konstelacji baz wzajemnie nieobciążonych (potrzebujemy d takich baz, których istnienie jest gwarantowane, ponieważ d jest liczbą pierwszą). Ponadto w najprostszym przypadku, tzn. $d=3$, pokazaliśmy dowód na samotestowanie. Jest to jeden z pierwszych dowodów, gdzie samotestowanie układów wielowymiarowych jest wyprowadzone bezpośrednio, bez użycia wyników samotestujących dla stanów dwu-kubitowych. W tym przypadku rozważając rozkład operatora Bella na sumę kwadratów, udało nam się w pełni scharakteryzować optymalne pomiary za pomocą relacji algebraicznych, które później mogliśmy rozwiązać *explicite* (argument ten jest uogólnieniem argumentu użytego w pracy [2] do analizy par obserwabli binarnych).

Wkład wnioskodawcy: Wraz z prof. Augusiakiem i dr. Turą wyprowadziliśmy konstrukcję nowych nierówności Bella. Samodzielnie wyprowadziłem wynik samotestowania dla $d=3$.

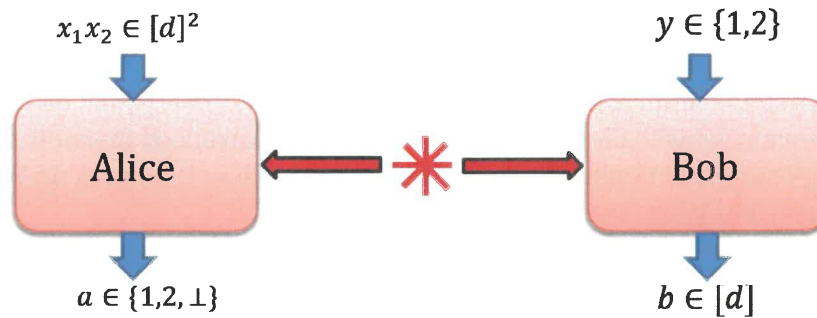
Praca [8] jest oparta na obserwacji dokonanej w trakcie badań nad geometrią zbioru korelacji kwantowych. Zauważyliśmy, że istnieją relatywnie proste nierówności Bella (3 ustawienia pomiarowe i 2 wyniki na każdym urządzeniu), których maksymalne łamanie jest osiągnięte przez wiele nierównoważnych realizacji kwantowych. Wszystkie te realizacje są oparte na stanie maksymalnie splątanych dwóch kubitów, ale różnią się stosowanymi pomiarami. W tej pracy udało mi się w pełni scharakteryzować kwantowe realizacje, które osiągają maksymalne łamanie. Dokonałem tego analizując rozkład operatora Bella na sumę kwadratów i wyprowadzając relacje algebraiczne, które muszą spełniać optymalne operatory pomiarowe. Następnie te relacje algebraiczne udało mi się rozwiązać, używając metody analogicznej do tej zaprezentowanej w pracy [2], ale ponieważ w nowym scenariuszu charakteryzujemy 3 obserwabli (zamiast dwóch), relacje algebraiczne nie prowadzą do jednego rozwiązania, a do 1-parametrowej rodziny rozwiązań (wszystkie wciąż realizowane na jednym kubicie). Mając w pełni scharakteryzowane obserwabli mogłem zbudować operator Bella i pokazać dla jakich kombinacji pomiarów możliwe jest maksymalne łamanie nierówności Bella. Okazało się, że w każdym przypadku maksymalne łamanie wymaga stanu maksymalnie splątanego

dwóch kubitów, co dowodzi istnienia nowej, słabszej formy samotestowania, w której możliwa jest certyfikacja stanu, mimo że nie możemy całkowicie scharakteryzować pomiarów. Zanalizowałem również sytuację w której obserwujemy niemaksymalne łamanie nierówności Bella. Okazało się, że również w tym przypadku przybliżona certyfikacja stanu jest możliwa, a wyniki numeryczne wskazują na podobieństwo do standardowych scenariuszy, w których pełne samotestowanie jest możliwe, np. scenariusza CHSH. Podobnie analiza losowości, którą możemy certyfikować nie wykazała znaczących różnic od standardowych przypadków. Sugeruje to, że słabsza forma samotestowania może wciąż być wystarczająca w wielu konkretnych zastosowaniach.

Wkład wnioskodawcy: Praca [8] jest pracą jednoautorską.

W pracy [9] wraz ze współpracownikami zaproponowaliśmy nową konstrukcję nierówności Bella. Konstrukcja ta pozwala otrzymać nierówności Bella, które są maksymalnie łamane przez konkretne symetryczne konstelacje pomiarów. Dla każdego wymiaru $d \geq 2$ jesteśmy w stanie skonstruować nierówności Bella, które są maksymalnie łamane przez: (1) dowolną parę baz wzajemnie nieobciążonych (patrz Rysunek 4) i (2) zestaw symetrycznych informacyjnie-kompletnych operatorów rzutowych (ang. *symmetric informationally-complete projectors*). W obu przypadkach wymaganym stanem jest stany maksymalnie splątany o lokalnym wymiarze d . Dla obu rodzin nierówności znaleźliśmy zastosowania w polu kryptografii niezależnej od urządzeń (ang. *device-independent cryptography*). Pokazaliśmy, że rodzina oparta o bazy wzajemnie nieobciążone pozwala na implementację protokołu kwantowej dystrybucji klucza (ang. *quantum key distribution*), a rodzina oparta na symetrycznych operatorach rzutowych pozwala na efektywne generowanie losowości. W obu przypadkach wykonaliśmy obliczenia numeryczne potwierdzające użyteczność tych protokołów dla $d=3$ przy realistycznym poziomie szumu. Pokazaliśmy też, że obie nierówności mogą być użyte do certyfikacji pomiarów, a w przypadku baz wzajemnie nieobciążonych także stanu kwantowego. Dzięki temu pokazaliśmy, że istnieją punkty ekstremalne (w znaczeniu geometrii wypukłej) zbioru kwantowego, które nie spełniają warunku samotestowania, co z punktu widzenia fundamentów korelacji kwantowych jest najważniejszym wynikiem tej pracy. Argument prowadzący do certyfikacji pokazuje, że w przypadku nierówności Bella dla baz wzajemnie nieobciążonych maksymalne łamanie jest osiągalne przez unikalny punkt ze zbioru kwantowego, co oznacza, że jest to punkt ekspanowany, a w konsekwencji także ekstremalny. Jednak ze względu na istnienie nierównoważnych par baz wzajemnie nieobciążonych w wyższych wymiarach (np. dla $d=4$), co zostało wspomniane w kontekście pracy [5], punkt ten może być zaimplementowany przez wiele nierównoważnych realizacji kwantowych. Nasz wynik pokazuje, że naturalne jest zdefiniowanie całej hierarchii warunków certyfikacji, w której standardowa definicja samotestowania stanowi najbardziej restrykcyjny wariant. Ponadto pokazaliśmy, że naturalna rodzina pomiarów, którą nazwaliśmy pomiarami wzajemnie nieobciążonymi jest nietrywialna i zawiera pomiary, które nie są sumą prostą baz wzajemnie nieobciążonych.

Wkład wnioskodawcy: Pomysł na konstrukcję nierówności Bella dla symetrycznych informacyjnie-kompletnych projektorów wyszedł od dr. Tavakoli. Ja pokazałem, że tę konstrukcję można zastosować również do baz wzajemnie nieobciążonych. Wraz z dr. Farkasem wyprowadziliśmy analityczne relacje certyfikujące, a także badaliśmy strukturę pomiarów wzajemnie nieobciążonych.



Rysunek 4: Scenariusz Bella, w którym skonstruowaliśmy nierówność Bella maksymalnie łamaną przez dowolną parę baz wzajemnie nieobciążonych w wymiarze d .

5. Informacja o wykazywaniu się istotną aktywnością naukową albo artystyczną realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej.

W trakcie mojej dotychczasowej kariery naukowej prowadziłem działalność badawczą w ramach następujących instytucji:

- Centrum Technologii Kwantowych, Narodowy Uniwersytet w Singapurze (od grudnia 2011 do września 2014)
- Techniczny Uniwersytet w Delft, Holandia (od października 2014 do grudnia 2015)
- Centrum Matematyki Teorii Kwantowej QMATH, Uniwersytet w Kopenhadze, Dania (od stycznia 2016 do czerwca 2018)
- Centrum Fizyki Teoretycznej PAN (od lipca 2018 do czerwca 2019)
- Wydział Fizyki Uniwersytetu Warszawskiego (od lipca 2019)

W każdej z tych instytucji byłem aktywnym uczestnikiem życia naukowego uczestnicząc w regularnych seminariach czy konferencjach lub warsztatach organizowanych lokalnie (także jako prelegent). Szczególnie istotne wydarzenia zostały wymienione w kolejnej sekcji.

6. Informacja o osiągnięciach dydaktycznych, organizacyjnych oraz popularyzujących naukę lub sztukę.

Aktywność dydaktyczna:

- W 2015 roku prowadziłem ćwiczenia z przedmiotu "Quantum computing and communication" na Uniwersytecie Technicznym w Delft (Holandia) prowadzonym przez prof. Stephanie Wehner.
- W październiku lat 2016 i 2017 prowadziłem całotygodniowy intensywny kurs LaTeXa na Uniwersytecie w Kopenhadze dla studentów pierwszego roku kierunku matematyka.
- W roku akademickim 2016/2017 opiekowałem się dwoma pracami magisterskimi: pan Zabulon Bucumi (African Institute for Mathematical Sciences, Senegal, współpraca na odległość) i pan Tim Coopmans (Uniwersytet w Amsterdamie; współpromotorem był prof. Christian Schaffner). Obie prace zostały obronione w 2017 roku.

- W lipcu 2018 roku prowadziłem mini-wykład "Randomness and device independence" w ramach Quantum Information Science Summer School w Seulu organizowanej przez Korea Institute of Advanced Study.
- W semestrze letnim roku akademickiego 2019/2020 wspólnie z dr. Alexem Streltsovem prowadziłem 30-godzinny wykład "Advanced quantum information: entanglement and nonlocality" dla studentów studiów II stopnia na Wydziale Fizyki Uniwersytetu Warszawskiego.
- W roku akademickim 2019/2020 opiekowałem się dwoma pracami licencjackimi, które zostały obronione we wrześniu 2020, a ponadto, byłem promotorem pomocniczym pracy doktorskiej pana Mate Farkas (Uniwersytet Gdański). Aktualnie jestem opiekunem dwóch prac licencjackich, jednej pracy magisterskiej i jestem także promotorem pomocniczym jednego doktoranta (pan Gabriel Pereira Alves).

Aktywność organizacyjna:

- W 2012 roku byłem członkiem komitetu organizacyjnego konferencji QCrypt 2012, samodzielnie zorganizowałem sesję plakatową.
- W 2018 roku byłem członkiem komitetu programowego konferencji CEQIP.

Aktywność popularyzacyjna:

- W 2012 roku prowadziłem pokazy doświadczalne dla uczestników Alumni Open Day na Narodowym Uniwersytecie w Singapurze.
- W 2012 roku byłem sędzią w konkursie International Mathematical Challenge organizowanym przez NUS High School of Mathematics and Science (Singapur).
- W 2015 roku zostałem zaproszony do wygłoszenia prelekcji na corocznym spotkaniu organizacji studenckiej Christiaan Huygens na Uniwersytecie Technicznym w Delft.
- W październiku 2016 byłem organizatorem "Kwantowego kącika" w ramach Kulturnatten (odpowiednik polskiego Festiwalu Nauki) na Uniwersytecie w Kopenhadze.

7. Oprócz kwestii wymienionych w pkt. 1-6, wnioskodawca może podać inne informacje, ważne z jego punktu widzenia, dotyczące jego kariery zawodowej.

Nie dotyczy.

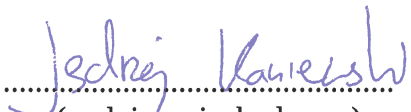
Cykl habilitacyjny składa się z następujących prac (porządek chronologiczny):

[1] J. Kaniewski, Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities, *Physical Review Letters* **117**, 070402 (2016)

[2] J. Kaniewski, Self-testing of binary observables based on commutation, *Physical Review A* **95**, 062323 (2017)

[3] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario, *Physical Review A* **98**, 062307 (2018)

- [4] M. O. Renou, J. Kaniewski, N. Brunner, Self-testing entangled measurements in quantum networks, *Physical Review Letters* **121**, 250507 (2018)
- [5] M. Farkas, J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, *Physical Review A* **99**, 032316 (2019)
- [6] T. Coopmans, J. Kaniewski, C. Schaffner, Robust self-testing of two-qubit states, *Physical Review A* **99**, 052123 (2019)
- [7] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, R. Augusiak, Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems, *Quantum* **3**, 198 (2019)
- [8] J. Kaniewski, A weak form of self-testing, *Physical Review Research* **2**, 033420 (2020)
- [9] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, J. Kaniewski, Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments, *Science Advances* **7**, eabc3847 (2021)


.....
(podpis wnioskodawcy)

