Dr hab. inż. Remigiusz Augusiak
Centrum Fizyki Teoretycznej PAN
Al. Lotników 32/46
02-668 Warszawa

Warszawa, 12.05.2020

Recenzja rozprawy doktorskiej mgr. Jakuba Jana Borkały
pt. „Applications of Quantum Random Access Codes in Quantum Information"

Struktura. Rozprawa pt. *„Application of Quantum Random Access Codes in Quantum Information"* autorstwa mgr. inż. Jakuba Borkały została przygotowana pod kierunkiem dr hab. Marcina Pawłowskiego, prof. UG. Zawarta jest na 89 stronach włączając całkiem obszerny spis literatury bo zawierający aż 174 pozycje i została napisana w języku angielskim na całkiem dobrym poziomie.

Rozprawa składa się z pięciu rozdziałów. Pierwszy to krótki wstęp zawierający wprowadzenie do dziedziny, sformułowanie głównego celu badawczego oraz streszczenie pozostałych rozdziałów. Celem drugiego rozdziału jest wprowadzenie podstawowych scenariuszy kwantowej teorii informacji, które są rozpatrywane w rozprawie, czyli scenariusza komunikacyjnego przygotuj i zmierz (ang. *prepapre-and-measure scnario*) oraz scenariusza, w którym obserwatorzy mogą współdzielić stany kwantowe. Przytoczono tutaj także wszystkie najważniejsze pojęcia i narzędzia używane w kwantowej teorii informacji jak i samej mechanice kwantowej takie jak stan i pomiar kwantowy, kanał kwantowy, czy bazy wzajemnie komplementarne (ang. *mutually unbiased bases*). W rozdziale drugim autor zamieścił także krótki opis metod optymalizacji wypukłej takich jak programowanie liniowe czy programowanie dodatnio pół-określone oraz nakreślił zasadę działania opartych na tym ostatnim metod typu *see-saw,* a także hierarchii Navascués-Pironio-Acín i jej modyfikacji sformułowanej przez Navascuésa i Vértesi'ego dla układów kwantowych o ustalonym wymiarze, którą w dalszych częściach recenzji będę nazywał metodą NV.

Trzeci rozdział zawiera definicje kodów swobodnego dostępu (ang. *random access codes*) wraz z ich dwiema modyfikacjami na przypadek kwantowy zwanymi kwantowymi kodami swobodnego dostępu (ang. *quantum random access codes*) oraz kodami dostępu wspomaganymi splątaniem (ang. *entanglement-assisted random access codes*); za Autorem będę je dalej oznaczał przez, odpowiednio, RAC, QRAC oraz EARAC. Omówiono wreszcie ideę samotestowania. Ponadto w rozdziale 3 pojawiają się pierwsze oryginalne wyniki Autora: definicja kwantowych kodów swobodnego dostępu z obietnicą (ang. *promise-QRAC*), lematy 1 i 2 wykorzystywane później w podrozdziale 4.1, a także uogólnienia protokołu RAC na przypadek wielocząstkowy będące filarem podrozdziału 4.3.

Zasadnicza część rozprawy, zawierająca główne i oryginalne wyniki naukowe otrzymane przez mgr. Borkałę to rozdział czwarty. Został on podzielony na trzy podrozdziały, z których każdy odpowiada jednemu z artykułów naukowych, których współautorem jest mgr. Borkała:

[R1] E. A. Aguilar, J. J. Borkała, P. Mironowicz, M. Pawłowski, *Connections Between Mutually Unbiased Bases and Quantum Random Access Codes*, Phys. Rev. Lett. **121**, 050501 (2018),

[R2] N. Miklin, J. J. Borkała, M. Pawłowski, *Self-testing of unsharp measurements*, arXiv:1903.12533,

[R3] D. Saha, J. J. Borkała, *Multiparty random access codes*, Europhys. Lett. **128**, 30005 (2020).

RA

Warto tutaj podkreślić, że pierwszy z artykułów został opublikowany w bardzo dobrym czasopiśmie fizycznym Physical Review Letters, a trzeci w dobrym Europhysics Letters. Drugi natomiast został umieszczony w bazie preprintów i zapewne wysłany do czasopisma.

Rozprawę wieńczy krótkie podsumowanie zawarte w rozdziale piątym, które z jednej strony streszcza wszystkie wyniki zawarte w pracy, a z drugiej nakreśla możliwe kierunki dalszych badań.

Rozdziały wstępne (1,2,3) wraz z podsumowaniem (rozdział 4 omawiam w dalszych częściach tej recenzji) zostały napisane w przystępny sposób i poza pewnymi wyjątkami, o których piszę poniżej, pozawalają zorientować się w pojęciach i metodach używanych w rozprawie bez konieczności posiłkowania się dodatkową literaturą. Udało mi się znaleźć tutaj kilka potknięć głównie natury językowej takich jak powtórzenia, literówki, czy zdania, które są trudne do zrozumienia. Nie ma sensu żebym je wszystkie wypisywał tutaj, toteż załączam je na końcu recenzji. Mam jednak dwie uwagi dotyczące rozdziałów 2 i 3, o których warto tutaj wspomnieć.

1.1. Uważam, że opis metody NV zamieszony w podrozdziale 2.5.4 jest zbyt powierzchowny. Została ona użyta do uzyskania wielu wyników zamieszczonych w rozprawie i czytelnikowi, który nie ma rozeznania w tego typu metodach, część podrozdziału 4.1 dotycząca jej implementacji staje się mało czytelna.

1.2. Podobny problem jest z podrozdziałem 3.7, który dotyczy idei samotestowania. Zamieszczony tam opis jest zbyt ogólny i głównie dotyczy scenariusza Bella. W szczególności brakuje w nim jawnej, matematycznej definicji samotestowania w scenariuszu przygotuj i zmierz, co może skutkować problemami ze zrozumieniem wyników zamieszczonych w podrozdziale 4.2. Ponadto, nie zrozumiałem jak ze zdania „Compared to the nonlocal scenarios ..." autor wnioskuje „That is why we can conclude that all outcome statistics are invariant under unitary transformations". Myślę, że Autor chciał tutaj powiedzieć, że owe rozkłady prawdopodobieństw opisujące scenariusz przygotuj i zmierz są niezmiennicze na działanie operacji unitarnych, toteż w tym scenariuszu można samotestować stany i pomiary kwantowe z dokładnością działania do operacji unitarnych.

Tematyka. Rozprawa poświęcona jest kodom swobodnego dostępu, a w zasadzie ich wersjom kwantowym, które są rodzajem zadań rozproszonych, w których dwoje lub wielu obserwatorów współpracują aby osiągnąć pewien zadany cel. Zazwyczaj są formułowane w scenariuszu przygotuj i zmierz (ang. *prepare-and-measure scenario*), który jest jednym z najbardziej podstawowych scenariuszy komunikacyjnych rozpatrywanych w ramach kwantowej teorii informacji. Jego główną zaletą jest to, że pomimo swojej prostoty pozwala na stawianie nietrywialnych problemów, w rozwiązaniu których korelacje kwantowe dają przewagę nad korelacjami klasycznymi. Jest to zatem bardzo ciekawa tematyka o znaczeniu fundamentalnym i dlatego jest ona (a w tym owe kody swobodnego dostępu) intensywnie badana w ostatnich latach. Promotor dr hab. M. Pawłowski jest w niej z pewnością jednym z wiodących badaczy. Badania zaprezentowane w rozprawie mgr. Borkały bardzo dobrze wpisują się w ten nurt badań, a co więcej mają niemały wkład w jego rozwój. Ich celem nadrzędnym jest eksploracja zastosowań kodów swobodnego dostępu w różnych gałęziach kwantowej teorii informacji i tym samym wykazanie, że są one bardzo użytecznym narzędziem w tej dziedzinie. Cel ten jest bardzo ogólny, toteż Autor formułuje kilka celów szczegółowych, które są następnie w rozprawie realizowane, a o których w bardziej szczegółowy sposób wypowiadam się poniżej.

Wyniki. Podrozdział 4.1 zawiera dość brawurową próbę odpowiedzi na pytanie, czy w przestrzeniach Hilberta o wymiarze sześć istnieją cztery bazy wzajemnie komplementarne. Hipoteza sformułowana przez Zaunera mówi, że w szcześciowymiarowych przestrzeniach Hilberta istnieją tylko 3 takie bazy i celem autora było potwierdzenie tej hipotezy. Warto tutaj podkreślić, że istnieje już dość obszerna literatura na ten temat, wymieniona zresztą w rozprawie, która potwierdza, że problem ten pomimo tego, że na pierwszy rzut oka wygląda dość niewinnie, jest w istocie bardzo trudny do rozstrzygnięcia.

RA

Zaproponowano bardzo oryginalną i jednocześnie ogólną metodę weryfikacji, czy w przestrzeni Hilberta o skończonym wymiarze d istnieje n baz wzajemnie niejednoznacznych, która oparta jest na zmodyfikowanej wersji standardowego protokołu QRAC, nazwana QRAC z obietnicą (ang. *promise QRAC*). To co odróżnia go od standardowego protokołu QRAC, a jednocześnie stanowi trzon metody to Lemat 2, który podaje ograniczenie górne na maksymalne średnie prawdopodobieństwo sukcesu oraz mówi, że owo ograniczenie jest osiągane wtedy i tylko wtedy, gdy pomiary kwantowe wykonywane przez Boba tworzą bazy wzajemnie niejednoznaczne; Obserwacja 1 sformułowana na stronie 34 pokazuje, że w przypadku standardowego QRAC implikacja zachodzi tylko w jedną stronę.

Druga część metody zaproponowanej w pracy [R1] to dwie metody numeryczne, które pozwalają nałożyć ograniczenia górne i dolne na średnie prawdopodobieństwo sukcesu (3.12) i tym samym zweryfikować czy w danym przypadku scharakteryzowanym wymiarem przestrzeni Hilberta d i ilością baz n może ono osiągać wartość ograniczenia (3.13). Obie oparte są na programowaniu dodatnio pół-określonym i wykorzystują fakt, że prawdopodobieństwo (3.12) jest funkcją liniową stanu kwantowego jak i operatorów pomiaru. Pierwsza z metod to hierarchia NV nakreślona w podrozdziale 2.5. Pozwala ona wyznaczyć nieskończony ciąg ograniczeń górnych na owo prawdopodobieństwo maksymalne, które zbiegają to jego wartości ścisłej. Główną zaletą tej metody to fakt, że na każdym poziomie zawsze zwraca globalne maksimum (z numeryczną dokładnością), dzięki czemu unika się „problemu lokalnych maksimów". Zatem jeżeli metoda NV na jednym z jej poziomów zwróciłaby ograniczenie górne na (3.12), które miałoby wartość niższą niż (3.13), oznaczałoby to, że w danej p. Hilberta nie istnieje n baz wzajemnie komplementarnych. Z drugiej strony jej złożoność bardzo szybko rośnie wraz ze wzrostem wymiaru p. Hilberta i/lub ilością baz co sprawia, że metodę tą można efektywnie stosować tylko w najprostszych przypadkach. W szczególności tabelka 4.3 sugeruje, że w przypadku protokołu $(4,2)^6$, który dotyczy postawionego problemu, Autor nie był w stanie użyć tej metody nawet na jej podstawowym poziomie. W celu usprawnienia działania hierarchii NV skorzystano z pewnych symetrii wbudowanych w scenariusz oparty na QRAC takich jak np. to, że zamiana wyników pomiarów Boba nie zmienia wartości prawdopodobieństwa sukcesu. Jak wynika z tabelki 4.3 to znacznie usprawniło działanie hierarchii NV, a w szczególności pozwoliło zastosować ją do przypadku kodów z obietnicą $(4,2)^6$ nawet na kilku poziomach. Niestety wartość otrzymana na najwyższym z tych poziomów z dokładnością do numerycznej precyzji w zasadzie odpowiada wartości (3.13), co nie pozwoliło wykluczyć istnienia czterech baz komplementarnych i tym samym potwierdzić powyższej hipotezy.

Druga z metod to tzw. metoda typu see-saw, również oparta na programowaniu dodatnio pół-określonym. Pozwala ona numerycznie wyznaczyć ograniczenie dolne na maksymalne średnie prawdopodobieństwo sukcesu (3.12). Zaletą tego podejścia w kontekście poszukiwania baz wzajemnie niejednoznacznych w p. Hilbertach to fakt, że w przypadku osiągnięcia wartości (3.13) zwraca ona również stan kwantowy oraz poszukiwane bazy, dla których wyrażenie (3.12) osiąga wartość maksymalną. Metoda ta została przetestowana na kilku przykładach kwantowych kodów z obietnicą $(n,m)^d$. Otrzymane wartości zebrane są w tabeli 4.2 i w najprostszych przypadkach metoda w zasadzie potwierdza istnienie znanych już baz wzajemnie komplementarnych. Natomiast w najbardziej interesującym przypadku kodów $(4,2)^6$ otrzymana wartość zbytnio odbiega od wartości maksymalnej aby można było wnioskować o istnieniu czterech baz wzajemnie komplementarnych.

Dodatkowym wynikiem zaprezentowanym w podrozdziale 4.1 jest nowa miara wzajemnej komplementarności baz w skończenie wymiarowych przestrzeniach Hilberta oparta o prawdopodobieństwo sukcesu sformułowane dla kodów kwantowych z obietnicą.

Sformułowaną metodę uważam za bardzo ciekawą i oryginalną. Pokazuje ona, że czysto-matematyczny problem jakim jest jest poszukiwanie baz wzajemnie komplementarnych w przestrzeniach Hilberta można „zaatakować" używając narzędzi stworzonych w ramach kwantowej informacji. Nawet jeżeli nie udało się potwierdzić powyższej hipotezy to należy docenić fakt, że mgr Borkała postawił sobie za cel rozwiązanie tak ambitnego problemu. Ponadto, podobało mi się zastosowanie teorii grup do opisu symetrii w rozważanym scenariuszu, co miało duży wpływ na przyspieszenie działania metod numerycznych. Szkoda, że Autorzy nie pociągnęli tego

RA

wątku dalej, a w szczególności w zastosowaniu do scenariuszy Bella, tak jak się to zasugerowane w referencjach pracy [R1]. Praca o podobnej tematyce autorstwa A. Tavakoli i współpracowników ukazała się niedawno w Physical Review Letters. Mam jednak kilka pomniejszych uwag dotyczących podrozdziału 4.1.

2.1. Jako że Autor nie opisał w szczegółach metody NV, to część podrozdziału 4.1 dotycząca implementacji tej metody staje się mało czytelna dla mniej zorientowanych osób.

2.2. Uważam, że lepiej byłoby zamieścić dowód Obserwacji 1 zaraz po niej, a nie odnosić czytelnika do tekstu, który znajduje się gdzieś dalej.

2.3. Zabrakło mi uzasadnienia dlaczego w dowodzie lematu 1 Autorzy biorą pod uwagę tylko pomiary projektywne.

Głównym celem podrozdziału 4.2 jest zastosowanie protokołów QRAC do samotestowania dwuwynikowych pomiarów kwantowych, które nie są projektywne. Pomiary tego typu znalazły wiele ciekawych zastosowań w informatyce kwantowej, a szczególności w protokołach sekwencyjnych, w których na danym układzie fizycznym pomiar kwantowy jest wykonywany kilkukrotnie. Przykładem takiego protokołu jest wprowadzony w rozprawie sekwencyjny protokół QRAC, w którym stan przygotowany przez Alicję jest mierzony przez dwóch obserwatorów, Boba i Charliego, a nie jednego jak to ma miejsce w przypadku standardowych protokołów QRAC. Obaj obserwatorzy starają się odgadnąć zadany bit wejściowy Alicji i globalne prawdopodobieństwo sukcesu w tym zadaniu jest kombinacją wypukłą prawdopodobieństw sukcesu każdego z nich (4.24).

Pierwszym celem badań zaprezentowanych w podrozdziale 4.2 jest charakteryzacja prawdopodobieństwa sukcesu (4.24). Wpierw Autorzy wyznaczają jego wartość maksymalną w przypadku, gdy Bob wykonuje pomiary projektywne, uwzględniając też szczególny przypadek, gdy jeden lub oba pomiary mają tylko jeden wynik (Proposition 1 na stronie 49). Następnie numerycznie wyznaczono jego wartość maksymalną kwantową, tzn. wartość maksymalną w przypadku, gdy Bob może wykonywać dowolne pomiary kwantowe (Proposition 2 na stronie 50). Stany oraz pomiary kwantowe osiągające tę wartość znaleziono przy pomocy metody typu *see-saw*, a następnie, wykorzystując hierarchię NV zweryfikowano ją dla skończonej liczby wartości parametru α. Co ciekawe, pomiary, które Bob musi wykonać, aby osiągnąć ową maksymalną wartość to pomiary nieprojektywne (zwane również uogólnionymi) i właśnie ten fakt pozwolił Autorom pracy [R2] na zaproponowanie metody samotestowania tego typu pomiarów. Co więcej, analiza numeryczna przedstawiona w podrozdziale 4.2.10 sugeruje, że w zasadzie można w ten sposób samotestować dowolne pomiary tego typu wykonane przez Boba. Wystarczy w tym celu odpowiednio dobrać parametr α w funkcji (4.73). Przebadano także przypadek „nieidealny", w którym obserwowana wartość (4.24) nie osiąga wartości optymalnej, ale jest do niej bliska.

Dodatkowo w podrozdziale 4.2 wyprowadzono relację monogamii pomiędzy prawdopodobieństwami sukcesu obu obserwatorów wykonujących pomiary w scenariuszu sekwencyjnym, która pozwala oszacować jaki wpływ ma pomiar wykonany przez pierwszego z tych obserwatorów na prawdopodobieństwo sukcesu drugiego. Użyto również tego scenariusza do przeanalizowania bezpieczeństwa klucza kryptograficznego wytwarzanego w w schemacie dystrybucji klucza z pracy [117], poprawiając wyniki uzyskane we wcześniejszych pracach. Wreszcie, wyprowadzone zostało ograniczenie górne na prawdopodobieństwo sukcesu w standardowym protokole QRAC w przypadku, gdy na stan przygotowany przez Alicję działa kanał defazujący. Pozwala ono ocenić jak obniży się prawdopodobieństwo sukcesu w przypadku gdy kanał kwantowy pomiędzy Alicją i Bobem jest „zaszumiony".

Podrozdział 4.2 zawiera dużą liczbę oryginalnych wyników, z których za najważniejszy i najciekawszy uważam definicję protokołu sekwencyjnego QRAC wraz z odpowiadającą mu funkcją celu jaką jest uśrednione prawdopodobieństwo sukcesu z wagą, dogłębną jego analizę oraz wynikająca z niej możliwość samotestowania uogólnionych dwuwynikowych pomiarów kwantowych, choć co do tego ostatniego mam pewne zastrzeżenia.

RA

3.1. Sformułowanie „and their probabilistic mixtures" pojawiające się w Proposition 1 jest niefortunne ponieważ dowolny dwuwynikowy pomiar nieprojektywny można wyrazić jako mieszaninę dwóch pomiarów projektywnych.

3.2. Jak już wcześniej wspomniałem uważam, że w podrozdziale 4.2 lub 3.7 powinna znaleźć się jawna definicja samotestowania w scenariuszu przygotuj i zmierz. Co prawda na stronie 58 pojawia się tekst, który w zasadzie określa co Autor rozumie przez samotestowanie, a w następnym paragrafie pojawia się również wyrażenie matematyczne, które niejako definiuje problem samotestowania w „przypadku z szumem". Brak takiej definicji sprawia, że czytelnikowi niezaznajomionemu z problemem samotestowania może być trudno zrozumieć zawartość podrozdziału 4.2.

3.3. Ponadto, nie zrozumiałem dlaczego owo wyrażenie matematyczne, które służy za definicję samotestowania dopuszcza zawiera inną operację unitarna dla każdego z pomiarów Boba. Moim zdaniem powinna pojawić się tutaj tylko jedna operacja unitarna, co zresztą potwierdza pierwsze zdanie wcześniejszego paragrafu: „*Formally, self-testing of measurements states that for all measurements compatible with the observed statistics there exist an isometry between these measurements and the target measurements*.", a także formuła (3.15), w której niezmienniczość rozkładów prawdopodobieństw rozpatrywanych w tym scenariuszu na działanie operacji unitarnych jest pokazana. Fakt, że Autorzy dopuszczają użycie dwóch operacji unitarnych potwierdzony jest rozważaniami w podrozdziale 4.2.4, które sprowadzają problem samotestowania do określenia norm operatorów dodatnich reprezentujących wyniki „0" obu pomiarów, będących w zgodzie z obserwowaną wartością funkcji (4.24). Podejście to nie pozwala jednak wykluczyć możliwości, w której oba pomiary wykonywane przez Boba są reprezentowane przez takie same normy.

3.4. Mam wrażenie, że układ części podrozdziału 4.2 ma nieco przypadkowy charakter. Przykładowo rozważania dotyczące samotestowania są rozdzielone opisami innych wyników takich jak np. wspomniana już relacja monogamii, czy analiza prawdopodobieństwa sukcesu w przypadku kanału z szumem. Swoją drogą nie jest dla mnie jasne, dlaczego ta analiza została w tym rozdziale w ogóle umieszczona.

W ostatniej pracy [R3], której współautorem jest mgr Borkała zaproponowano uogólnienia klasycznych i kwantowych protokołów swobodnego dostępu na przypadek dowolnej liczby obserwatorów. Następnie opierając się na znanych protokołach kwantowych takich jak *(4,4)*-QRAC, *(6,6)*-QRAC, czy tych wspomaganych splątaniem, skonstruowano protokoły wieloobserwatorowe, dla których pokazano, że różnica pomiędzy wartościami kwantowymi i klasycznymi wzrasta w stosunku do przypadku dwóch obserwatorów. Uważam, że jest to ciekawa obserwacja, która może mieć duże znaczenie z aplikacyjnego punktu widzenia. Mam jednak kilka uwag dotyczących podrozdziału 4.3.

4.1. Ta część rozprawy jest najkrótsza, ale jednocześnie najtrudniejsza do przebrnięcia. Myślę, że Autor mógł skorzystać z okazji jaką niesie możliwość napisania pełnej rozprawy i opisać swoje wyniki w nieco obszerniejszy sposób. W szczególności, można było przenieść opisy protokołów z podpisów pod rysunkami do głównego tekstu i nieco je rozwinąć.

4.2. Najważniejszym zarzutem jaki mam do tej części to brak wyjaśnienia dlaczego rozważane uogólnienia jak np. to zawarte podrozdziale 3.3 Autor nazywa wieloobserwatorowymi. Przypominają one raczej protokoły sekwencyjne, w których jeden z obserwatorów wykonuje pomiary jeden po drugim, używając różnych danych wejściowych oraz wyników poprzedniego pomiaru. Ponadto w podrozdziale 3.3 zabrakło omówienia dlaczego pierwszy obserwator otrzymuje wiele bitów wejściowych, a pozostali tylko dwa.

4.3. W części dotyczącej protokołów wspomaganych splątaniem zabrakło mi omówienia otrzymanych formuł oraz wykresu przedstawionego na Rys. 4.11, z którego wynika, ze zwiększanie n skutkuje zwiększeniem różnicy pomiędzy wartościami kwantowymi i klasycznymi prawdopodobieństwa sukcesu.

RA

Konkluzja. Podsumowując uważam, że rozprawa mgr. Borkały zawiera wiele ciekawych i nowatorskich wyników naukowych, który mają wkład w rozwój kwantowej teorii informacji oraz podstaw teorii kwantów. Pomimo pewnych braków i niedociągnięć dotyczących głównie strony redakcyjnej rozprawy, jestem przekonany, że spełnia ona ustawowe i zwyczajowe wymogi stawiane rozprawom doktorskim i wnoszę o dopuszczenie mgr. Jakuba Borkały do dalszych etapów przewodu doktorskiego.

Remigiusz Augusiak

Inne uwagi:

1. Strona 3: zamiast „state to much" powinno być „state too much".

2. Strona 3: „gap may serve" lub „gap serves" zamiast „gap may serves"

3. Strona 3: „asigned" zamiast „asign" oraz „it proves" zamiast „it proofs".

4. Strona 8: nie jest jasne dlaczego w zdaniu „... by the action of completely positive map on a state 2.3.1, but ..." pojawia się odniesienie do podrozdziału 2.3.1. Jeżeli Autor chciał odnieść czytelnika do definicji stanu kwantowego, mógł to zrobić pisząc „... maps on a state (for the definition of quantum states see chapter 2.3.1)".

5. Strona 8: zamiast „known form the classical" powinno być „known from the classical".

6. Strona 8: zamiast „preparation devise" powinno być „preparation device".

4. Strony 8 i 9: w kilku miejscach powinno być „what we can" zamiast „what can we".

5. Strona 10: zamiast „Language of quantum mechanics" powinno być „The language of quantum mechanics".

6. Strona 10: zamiast „with finite degrees of freedom" powinno raczej być „with a finite number of degrees of freedom".

7. Czasami Autor używa „positive", a czasami „positive semi-definite" na określenie operatorów dodatnich, co nie jest błędem bo oba pojęcia są używane w literaturze, ale dla przejrzystości lepiej używać tylko jednego z nich.

8. Strona 10: w zdaniu „The set S(H) ... corresponds to a third state ..." nie jest jasne do czego odnosi się czasownik „corresponds".

9. Strona 10: Po wzorze (2.2) powinno być „which" zamiast „witch".

10. Strona 11: zdanie „We also require for the eigenvalues of an effect to be real, therefore E=E^dag." jest niepotrzebne i błędne. Niepotrzebne bo warunek dodatniości operatora E pojawił się dwa zdania wcześniej i z tego warunku wynika, że operator E jest samosprzężony oraz ma nieujemne wartości własne. Błędne bo z faktu, że operator ma nieujemne wartości własne nie można wnioskować, że jest operatorem samosprzężonym.

11. Strona 11: zdanie „The duality of states and effects means ... the probability distribution." jest niezrozumiałe ponieważ mając stan kwantowy oraz jeden operator pomiaru E nie da się wyznaczyć rozkładu

RA

prawdopodobieństwa; można jedynie wyliczyć prawdopodobieństwo otrzymania wyniki reprezentowanego przez E w danym stanie kwantowym. Chyba że, Autor miał na myśli pomiar dwuwynikowy wyznaczony przez E.

12. Strona 11: Warunek (2.7) pojawia się już wcześniej dwa razy.

13. Strona 11: zamiast „This express" powinno być „This expresses".

14. Strona 12: w równaniu (2.12) przy przejściu z jednej strony równania na drugą, indeks zmienia się z „i" na „j". Ponadto, formuła (2.12) jest prawdziwa niezależnie od tego, czy stan jest czysty czy mieszany, a mam wrażenie, że Autor chciał pokazać jak wyraża się prawdopodobieństwo otrzymania wyniku reprezentowanego przez operator E_i w stanie czystym. Wówczas formuła (2.12) powinna wyglądać inaczej.

15. Strona 12: zdanie „To summarize our introduction on the topic of measurements." nie ma zakończenia.

16. Strona 13: W zdaniu „But first the map ... is positive map", drugie słowo „map" nie jest potrzebne.

17. Strona 13: w zdaniu „This form of CP map is motivated on the..." nie jest jasne, o którą postać chodzi, a ponadto zamiast „on" powinno być „by".

18. Strona 13: w zdaniu „Quantum channel is a operation that acts from the state of states S(H) into the state of states S(H) ..." zamiast „state of states" powinno być chyba „set of states", a ponadto zamiast rodzajnika „a" powinien być rodzajnik „an".

19. Strona 14: w zdaniu „First system enters ..." nie jest jasne czy chodzi o to, że pierwszy układ wchodzi do urządzenia pomiarowego, czy że najpierw układ wchodzi do urządzenia pomiarowego. Optuję za drugą możliwością.

20. Strona 14: zamiast „Afterwords" powinno być „Afterwards" bo Autorowi nie chodziło tutaj raczej o posłowie.

21. Definicja na stronie 15 jest nieco niefortunna bo nie wiadomo jaką rolę odgrywa w niej równanie (2.15a) skoro operacja Phi jest niezdefiniowana. Jak rozumiem Autor chciał w ten sposób powiedzieć, że suma odwzorowań w (2.15a) tworzy kanał kwantowy; wówczas jednak warunek (2.15b) jest zbędny.

22. Strona 15: myślę, że zamiast Corollary 1 lepiej byłoby użyć Theorem 1 bo słowo „corollary" oznacza raczej wniosek do twierdzenia lub innego faktu matematycznego, którego tutaj nie ma.

23. Strona 16: w zdaniu „than the collection ..." powinno być „then".

24. Strona 16: zamiast „is a Kraus decomposition the effect F_i" powinno być „is a Kraus decomposition of the effect F_i".

25. Strona 16: w definicji instrumentów Lüdersa zabrakło doprecyzowania czym są operatory F_i. Zakładam, że są to operatory dodatnie, ponieważ formalnie pierwiastek operatorowy definiuje się dla takich operatorów. Wtedy jest pewna niejednoznaczność pomiędzy wzorami (2.21) i (2.23), ponieważ w (2.23) występują dowolne operatory K_i, natomiast pierwiastek z operatora dodatniego w (2.21) jest również operatorem dodatnim. Chciałbym tutaj zauważyć, że z faktu, że $F_i=K_iK_i\text{^}dag$ nie wynika, że pierwiastek z F_i to K_i, a tak to chyba rozumie Autor.

RA

26. Strona 16: we wzorze (2.25) zamiast macierzy gęstości powinna być jej transpozycja względem bazy standardowej.

27. Strona 17: w zdaniu „... if each vector of the first basis has the same inner product with every vector of the second." brakuje wartości bezwzględnej. Ponadto, powinno być „the second one" zamiast „the second".

28. Strona 18: notacja użyta we wzorach (2.27)-(2.30) jest niejasna; w szczególności nie wiadomo co oznaczają indeksy *k* i *l*.

29. Strona 19: sformułowanie problemu liniowego w (2.32) jak i dodatnio pół-określonego nie jest najbardziej ogólne albowiem w warunkach obu problemów dopuszcza się także nierówności.

30. Strona 19: w zdaniu „In worlds x ..." powinno być „words".

31. Strona 20: we drugiej linii wyrażenia (2.36) powinno być $Tr(A_iX)$.

32. Strona 20: sformułowanie „and constraints being some matrices with variables are positive semi-definite" jest niefortunne. Z jednej strony warunki problemu liniowego nie są macierzami, lecz są zapisywane w postaci macierzowej. Z drugiej strony, brakuje jakiegoś słowa po „variables" przez co zdanie jest niejasne. Wreszcie, macierze o których mowa nie muszą być dodatnie.

33. Strona 21: W zdaniu „If some stopping criteria ..." brakuje słowa „go" przed „back".

34. Strona 21: trudno zrozumieć o co chodzi we wzorze (2.38).

35. Strona 23: sformułowanie „we focus on protocols that exchange information ... to provide certain information" jest niefortunne.

36. Strona 23: zdanie „The main idea behind ... all parties." jest nieczytelne; w szczególności pierwsze słowo „required" wydaje się niepotrzebne.

37. Strona 23: nie rozumiem dlaczego zdanie „Nevertheless, the RAC protocols ..." zaczyna się od słowa „nevertheless".

38. Strona 25: w tekście powinno być P_q-P_c zamiast P_c-P_q; w przeciwnym wypadku zdanie zawierające to wyrażenie nie ma sensu, ponieważ największa wartość jaką może przyjąć P_c-P_q to zero.

39. Strona 26: średnie prawdopodobieństwo sukcesu oznaczone jest we wzorze (3.3) małą literą *p*, podczas gdy w innych miejscach Autor używa dużego *P*.

40. Strona 27: przed wzorem (3.4) suma pojawiająca się w tekście powinna być po x_0 i x_1, a nie *X*, a ponadto λ_{max} powinna być indeksowana przez x_0 i x_1.

41. Strona 27: w równaniu (3.9) brakuje nawiasów.

42. Strona 27: bardzo podobało mi się użycie majoryzacji i funkcji Schura wklęsłej w znalezieniu wartości maksymalnej (3.4), ale wydaje mi się, że wystarczyło skorzystać z wklęsłości funkcji pierwiastkowej.

43. Strona 28: zamiast „pomisce" pownno być „promise".

RA

44. Strona 29: nie rozumiem dlaczego w podrozdziale 3.5 Autor nie podał ogólnej definicji kodów swobodnego dostępu wspomaganych splątaniem nawet w najprostszym scenariuszu (2,1), a jedynie przedstawił konkretną strategię, która maksymalizuje prawdopodobieństwo sukcesu (3.14).

45. Strona 31: zdanie „Strong violation of Bell inequality implies that that measured system is non-local ..." jest niefortunne bo dowolne łamanie nierówności Bella implikuje nielokalność.

46. Strona 32: zdanie „That is why we can conclude that all outcome statistics are invariant under unitary transformations" jest błędne bo niezmienniczość rozkładów prawdopodobieństw $p(b|x,y)$ na działanie operacji unitarnych nie wynika ze zdania poprzedniego, ale z reguły Borna. Myślę, że Autor tutaj chciał powiedzieć, że w przeciwieństwie do scenariusza Bella jedyną klasą równoważności w scenariuszu przygotuj i zmierz jest niezmienniczość na operacje unitarne. To jest ważna informacja i szkoda, że nie wybrzmiała tutaj.

47. Strona 35: Nie jest jasne do czego odnosi się „It" w pierwszym zdaniu podrozdziału 4.1.2: „It turned out that it can be used together with Lemma 1 ...". Wydaje się, że chodzi tutaj o nową miarę zapowiedzianą w tytule podrozdziału.

48. Strona 35: w tekście pod wzorem (4.6) jest inna notacja $p(b=x_y)$ niż w równaniu (4.1).

49. Strona 37: nie jest jasne do czego odnosi się sformułowanie „cf. remark below (2) of the main text".

50. Strona 38: w zdaniu „If one considers a set of basis ..." zamiast „basis" powinno być „bases".

51. Strona 40: powinno być „can find" zamiast „have can find".

52. Strona 42: w równaniu (4.19b) jest niepotrzebny nawias.

53. Strona 46: zamiast „slef-testing" powinno być „self-testing". Ponadto, w paragrafie przed podrozdziałem 4.2.1 omyłkowo znalazły się odniesienia do materiałów dodatkowych publikacji [R1].

54. Strona 57: sformułowanie „described in Section 4.2.6 of this SM" nie powinno się tutaj znaleźć.

55. Strona 58: zamiast zdania „For the definition of quantum instrument see e.g. [71]." powinno być zdanie odnoszące czytelnika do podrozdziału 2.3.2.

56. Strona 59: w podrozdziale 4.2.5 omyłkowo znalazło się podsumowanie z pracy [R1]. Ponadto, podrozdział 4.2.6 rozpoczyna się wyrażeniem „In this paper".

57. Na stronie 63 znowu pojawia się odniesienie do „supplementary material".

58. Strona 68: powinno być „The guess is correct if either all" zamiast „The guess is correct either all".

59. Strona 71: zamiast „explicate" powinno być „explain".

60. Wydrukowana wersja rozprawy, którą otrzymałem urywa się na stronie 84.

RA