Autor w swojej pracy rozważa różne wersje protokołu kodu losowego dostępu (RAC - *Random Access Code*). Protokół polega na zakodowaniu pewnej liczby bitów (lub ogólniej - ditów) w stan (klasyczny lub kwantowy) jednego bitu/qbitu, a odbiorca ma za zadanie odczytać wartość jednego, losowo wybranego zakodowanego bitu. Protokół może być klasyczny lub kwantowy, może być modyfikowany do wersji wielocząstkowej (M) lub w sytuacji gdy przesyłane układy kwantowe są splątane z układami posiadanymi przez odbiorcę (EA - *entanglement assisted*). Nową wersją protokołu jest protokół pQRAC (promise QRAC) - gdy nadawca ma obiecane, o które zakodowane bity może zapytać odbiorca. Nowy protokół pozwala zreformułować sławny problem istnienia 4 baz wzajemnie nieobciążonych (MUB's - *mutually unbiased bases*) w $\mathbb{C}^6$ w sposób ilościowy i dostarcza operacyjnej miary nieobciążenia zbioru baz.

Następną rozważaną modyfikacją protokołu QRAC jest rozbicie strony mierzącej (odbiorcy) na dwóch odbiorców B oraz C. Obaj odbiorcy nie mogą wydobyć pełnej chcianej informacji - występuje *tradeoff* pomiędzy informacją uzyskaną przez B i zaburzeniem stanu wysyłanego do C. Optymalność jest definiowana poprzez parametr α, opisujący z jaką wagą prawdopodobieństwa udanego odczytu w B i w C wchodzą do miary sukcesu protokołu. Optymalną strategią okazuje się być użycie POVM-a przez użytkownika B, a rozdźwięk pomiędzy tą wartością a maksymalną możliwą do uzyskania wartością przy używaniu pomiarów projektywnych pozwala na samocertyfikację użytych POVM-ów.

W końcu, rozważaną modyfikacją były dwie strony wysyłające, gdzie pierwsza przygotowuje stan na podstawie jej k bitów, a druga wykonuje na nim jedną z 2^{n-k} operacji unitarnych, produkując 2^n stanów, które następnie są mierzone przez odbiorcę. Dwa podane przykłady używają brył platońskich wpisanych w sferę Blocha.

Metody programowania półokreślonego (*semidefinite programming*) w szczególności metoda Navascués-Vertesi (NV) odgrywają centralną rolę w prezentowanych przewidywaniach numerycznych.

Rozprawa pokazuje szeroką wiedzę na temat protokołów komunikacji kwantowej (wliczając koncepcje Niezależności od Urządzeń (*Device Independence*) i Pół-Niezależności od Urządzeń (*Semi-Device Independence*)), narzędzi matematycznych Informatyki Kwantowej i metod numerycznych optymalizacji wypukłej. Rozważania o Shannonie, Turringu, von Neumannie, roli informacji w rozwoju cywilizacji, komentarz na temat dylematy Platona-Arystotelesa we wstępie, jak również rozważanie, czy problem istnienia czterech baz wzajemnie nieobciążonych w wymiarze 6 jest problemem typu hipotezy Riemanna (centralny), czy raczej twierdzenia Fermata (poboczny), ukazuje dojrzałość naukową i głębokie rozumienie prezentowanych problemów w szerszym kontekście.

Mimo wszystko, rozprawa ma pewne niedomagania, które wypunktuję w dalszym ciągu recenzji.

Chapter 2 Przywołane metody (NPA i NV) pozwalają wykonać optymizację wypukłą poprzez hierarchię problemów programowania półokreślonego (SDP), przypominając metodę Doherty'ego rozstrzygania o separowalności stanu. Pomimo, że nie jest ona używana w pracy, mogła być wspomniana, dla szerszego kontek-

stu, jako przykład podobnej metody o dużym znaczeniu dla dziedziny.

Inne uwagi:

- Ponad wzorem (2.1) występuje nieścisłość w definiowaniu stanów: wektor stanu tylko reprezentuje stan, w niejednoznaczny sposób, a przestrzeń Hilberta układu nie jest przestrzenią stanów - prowadziłoby to do sprzeczności ze wzorem (2.1), który jest już poprawny. To samo powyżej (2.2) - stan czysty, w notacji Diraca to $|\psi\rangle\langle\psi|$, nie $|\psi\rangle$. Również "Przestrzeń Hilberta o skończonej liczbie stopi swobody" nie jest dobrym sformułowaniem, powinno to brzmieć jak: przestrzeń Hilberta układu skończenie-poziomowego.

- Ponad wzorem (2.3), autor napisał:

  operator E_i *(...) has to be (...)* $0 \leq E_i \leq \mathbb{I}$ *(...) We also require for the eigenvalues of* E_i *to be real ...*

  - to nie jest dodatkowy warunek. Warunek $0 \leq E_i \leq \mathbb{I}$ wymaga hermitowskości operatorów E_i, w przeciwnym wypadku warunek nie miałby sensu.

- Wzór (2.16) mógłby być przepisany poprzez pomiar projektywny na rozszerzonym układzie. Dalej, użycie słowa *evolution* nie jest szczęśliwe, ponieważ sugeruje jednoparametrową rodzinę odwzorowań CPTP. Brakuje tam słów *between two time instants.*

- Jeżeli autor ogranicza nieznormalizowany izomorfizm Jamiołkowskiego do kanałów kwantowych, wtedy jego wartości nie są unormowane i nie powinny być nazywane *Choi states*, ale lepiej: *Choi operators.*

Chapter 3

- Strona 25: operatory M_b^y to nie POVM-y ale efekty i dalej, odpowiednio, nie pomiary projektywne ale projektory.

- Byłoby bardziej czytelnie, gdyby wzór (3.3) poprzedzała reguła Bayes'a, jak w (3.14).

- Zakończenie rozdziału 3.5 - byłoby lepiej zilustrować opisane bazy w kuli Blocha. Nie ma dowodu postulowanej optymalności wybranych baz.

- Rozdział 3.6 - nieklasyczne zachowanie nie powinno być nazywane nielokalnością (o szczegóły proszę pytać prof. Marka Żukowskiego).

Chapter 4

- W podrozdziale 4.1.1 mamy następujący wzór na prawdopodobieństwo sukcesu:

$$\max \sum_{ijk} \lambda_1(m_{ijk}, n_{ijk}),$$

gdzie parametr m_{ijk} jest maksymalny dla baz wzajemnie nieobciążonych. Nie widzę tu konieczności, że maksimum jest osiągane na zbiorze baz wzajemnie nieobciążonych - mamy również zależność od drugiego parametru i nie ma dyskusji o monotoniczności λ_1 ze względu na jej argumenty.

- Tablica 4.1 powinna być dalej, po odniesieniu do niej w tekście.
- Termin *collapse probability* nie jest wyjaśniony.
- Wzory 4.7 i 4.9 w przypadku baz obciążonych zależą od permutacji wewnątrz baz. Powinno być dodane w definicji maksimum.
- 4.1.3 - sformułowanie *the state is in the subspace* nie jest ściśle poprawne. Powinno to być wyrażone jako: *the state lives in a subspace* lub *range of the state is contained in a subspace*
- W podrozdziale 4.1.3: W takim eksperymencie numerycznym bazy ortonormalne Boba powinny być losowane z miary Haara na grupie macierzy unitarnych. W przeciwym wypadku, pewne regiony będą nadreprezentowane, a pewne niewystarczająco przeszukane, co zaburza statystykę w metodach Monte Carlo. By to zrobić, w opisanej procedurze wyrazy macierzy A powinny być losowane z rozkładu normalnego (tzw. **Ginibre ensemble**). Łotewska szkoła informatyki kwantowej to nie tylko intensywnie cytowany w pracy Andris Ambainis, ale również Māris Ozols, który napisał ładną pracę na ten temat.
- Kiedy hierarchia jest implementowana (przed wzorem (4.13)), wzory na wyrazy macierzy momentów zawierają stany w drugiej potędze, podczas gdy w oryginalnym sformułowaniu metody N-V są one wartościami oczekiwanymi łańcuchów projektorów, zatem są liniowe w stanach. Czy stany i efekty pełnią tutaj inną rolę? To powinno być wyjaśnione.
- Poziomy hierarchi $1 + succ$, $1 + succ + BB$ i potem $1 + AB$ nie są zdefiniowane w rozprawie.
- W podrozdziale 4.1.5 brakuje analizy, w jaki sposób użycie symetrii redukuje złożoność czasową algorytmu.
- Jakie jest uzasadnienie terminu *unbiased* wprowadzonego w podrozdziale 4.2.1 dla POVM-a o efektach o jednostkowym śladzie?
- Dowód optymalności ortogonalnych $|\phi\rangle$ and $|\psi\rangle$ pod (4.33) jest zawiły i niezrozumiały. Wystarczyłoby ograniczyć A do jej części symetrycznej A_{sym} i optymizować każdy składnik wartości oczekiwanej niezależnie dostając, że ψ jest wektorem własnym A_{sym} przy największej wartości własnej a ϕ jest wektorem własnym przy najmniejszej wartości własnej A_{sym}. Rezultat wynika z ortogonalności wektorów własnych macierzy symetrycznej.
- Nietrywialne rozwiązanie układu (4.46) - (4.48) istnieje dla $x_1 \neq 0, z_1 \neq \pm 1$ wtw gdy obrazem macierzy Lambd jest span$\{e_2, e_3\}$, co implikuje, że $\lambda_1 = \lambda_4 = \lambda_5 = 0$ i stąd: $y_4 = y_5 = 0, x_4 = x_1/(2\lambda_2), x_5 = -x_1/(2\lambda_3), z_4 = (1 + z_1)/(2\lambda_2), z_5 = (1 - z_1)/(2\lambda_3)$. Wydaje się, że podzbiór optymalnych rozwiązań został pominięty.
- Dowód Wniosku 2 i wyniki o samotestowaniu W podrozdziałach 4.2.3, 4.2.4 i 4.2.8 są bardzo słabo przedstawione w bardzo zawiły sposób, który uniemożliwia podążanie. Wyniki wyprzedzają swoje wyprowadzenia (na przykład wprowadzenie kanałów defazujących nad wzorem (4.62), uzasadnione jedną stronę dalej). Odnośniki do Appendiksów i "the next section

of this Supplementary Material" (nie istniejącego w rozprawie) pokazują, że te fragmenty były kopiowane z innych publikacji bez odpowiedniego przeredagowania.

- Podrozdział 4.2.5. Byłoby lepiej zastąpić: "figure of merit can be rewritten" na: "figure of merit originates in".

- Dlaczego podrozdział 4.2.6 zaczyna się słowami "In this paper" ?

- *the third family of constraints in (4.55) ensures that all inner products between the states* $\{\rho_{\vec{x}}\}_{\vec{x}}$ *are the same for both choices of Bob's operations* - nie widzą żadnego uzasadnienia tego stwierdzenia. Podobne stwierdzenie jest użyte nad wzorem (4.69), również bez uzasadnienia.

- Nad wzorem (4.57): wartości własne mogą być efektów, nie POVMów.

- Druga formuła w (4.58) jest tylko prostą konsekwencją formuły (4.57), nie są potrzebne żadne przewidywania numeryczne.

- Parametr γ w (4.73) nie ma podanego żadnego uzasadnienia ani interpretacji.

- Jeżeli protokół EAMRAC jest łączony za pomocą stanów GHZ, obie zaprezentowane architektury są przypadkami szczególnymi - można zbudować dowolne drzewo binarne. Można się zastanawiać nad optymalnymi drzewami ze względu na wagi nadane prawdopodobieństwom sukcesu stron protokołu. Należy oczekiwać konstrukcji podobnej do drzew/kodu Huffmana.

Czasami referencje do równań są bez nawiasów, co sugeruje szukanie w podrozdziałach o podanych numerach. Znalazłem jeszcze pewną liczbę błędów typograficznych i mniejszych błędów, których nie będę wypisywał.

Rozprawa jest oparta na trzech artykułach. W żadnym z nich autor rozprawy nie jest pierwszym autorem. W takiej sytuacji byłoby pożądane, gdyby autor opisał swój wkład w każdy z artykułów. Jeden z wymienionych artykułów jest jeszcze nie opublikowany (od roku), ale na arxivie można przeczytać, że artykuł jest "revised after referees' comments". Chciałbym poznać postęp procesu publikacji artykułu.

Rozpraw i bibliografia ukazują szeroką i głęboką wiedzę w dziedzinie Informatyki Kwantowej i doświadczenie w używaniu, implementowaniu i modyfikowaniu metod optymalizacji wypukłej. Artykuły autora, opublikowane w prestiżowych czasopismach, mają w wilu punktach wkład w dziedzinę. Szczególne wrażenie robi propozycja ataku na problem 4 baz w $\mathbb{C}^6$. Otwarte problemy i przyszłe kierunki badań są również prawidłowo nakreślone. Mimo to, w pewnych fragmentach sposób prezentacji treści mógłby zostać poprawiony. W mojej opinii rozprawa spełnia wszystkie formalne i zwyczajowe wymogi stawiane rozprawom doktorskim i wnoszę o dopuszczenie pana Jakuba Borkały do dalszych etapów procedury obrony.

Gniewomir Sarbicki