Warszawa, 21.07.2023

dr hab. inż. Remigiusz Augusiak
Centrum Fizyki Teoretycznej
Polska Akademia Nauk
al. Lotników 32/46, 02-668 Warszawa

Recenzja rozprawy doktorskiej mgr. inż. Ryszarda Kukulskiego
pt. ,,*Probabilistyczne kwantowe kody korekcyjne w zastosowaniu do ogólnych kanałów szumu*"

Uwagi ogólne. Rozprawa pt. ,,*Probabilistyczne kwantowe kody korekcyjne w zastosowaniu do ogólnych kanałów szumu*" została przygotowana w Instytucie Informatyki Teoretycznej i Stosowanej PAN pod kierunkiem dr hab. Zbigniewa Puchały oraz dr hab. inż. Łukasza Paweli. Uwzględniając spis literaturowy rozprawa liczy 123 strony i jest napisana w języku angielskim na bardzo dobrym poziomie. Choć nie udało się Autorowi uniknąć pewnych wpadek językowych, to warto tutaj pochwalić Autora za trud związany z pisaniem rozprawy w języku obcym, ponieważ dzięki temu rozprawa, a także wyniki w niej zawarte stają się dostępne dla szerszego grona odbiorców.

Praca rozpięta jest na oryginalnych wynikach opublikowanych w dwóch artykułach naukowych a także na nieopublikowanych wynikach Autora. Warto tutaj dodać, że jeden z tych dwóch artykułów ukazał się w prestiżowym czasopiśmie *IEEE Transactions on Information Theory* publikującym artykuły z teorii informacji (także kwantowej), a także to, że wyniki zawarte w tej pracy, a w szczególności algorytm 17 (w rozprawie algorytm 28) pozwalający generować probabilistyczne kody dla kubitów stanowią podstawę wniosku patentowego, którego jak rozumiem współautorem jest mgr Kukulski.

Rozprawa składa się z sześciu rozdziałów. W pierwszym rozdziale Autor w zgrabny sposób nakreślił kontekst badań i przypomniał znane wyniki literaturowe, a także sformułował problem badawczy, z którym zmaga się w dalszych rozdziałach. Rozdział drugi pracy to w zasadzie wstęp matematyczny, którego celem jest wprowadzenie najważniejszych pojęć i narzędzi matematycznych potrzebnych do sformułowania oraz zrozumienia wyników naukowych zaprezentowanych w rozprawie. Ten rozdział czytałem z przyjemnością, ale uważam, że mógłby być nieco obszerniejszy i obejmować także przynajmniej niektóre pojęcia, które są potem ,,ad-hoc" formułowane w ,,rozdziałach badawczych" takie jak np. instrumenty kwantowe (strona 32), czy też superkanały (zdefiniowane na stronie 35). Dodam jeszcze, że wydaje mi się, że w równaniu (2.54) brakuje maksimum. Z kolei rozdział 6 to podsumowanie pracy, w którym Autor streszcza najważniejsze wyniki, a także nakreśla kilka problemów badawczych, które stanowią materiał dla dalszych badań. Poniżej opiszę pokrótce najważniejsze wyniki zawarte w pozostałych rozdziałach.

Tematyka rozprawy. Rozprawa dotyczy kwantowych kodów korekcji błędów, które maja kluczowe znaczenie w procesach przetwarzania informacji kwantowej. Jest to obszar fizyki kwantowej, który w ostatnich latach jest intensywnie eksplorowany ze względu na możliwości jakie drzemią w układach kwantowych z punktu widzenia ich zastosowań w nowych technologiach takich jak np. wspomniane w rozprawie komputery kwantowe. Niestety układy kwantowe, a także oparte na nich technologie kwantowe są bardzo wrażliwe na szumy i błędy o różnorakiej naturze jak np. dekoherencja, czy niedoskonałości w implementacji bramek kwantowych. Kwantowe kody korekcji błędów to narzędzie, którego głównym celem jest ochrona informacji kwantowej przed owymi błędami. Kodem nazywamy parę kanałów lub podkanałów kwantowych, przy czym jeden służy do kodowania informacji kwantowej w inny, z reguły większy układ kwantowy, a drugi służy od dekodowania. Owa para jest dobrana tak, aby pozwalała chronić informację kwantową przed błędami reprezentowanymi przez pewien inny kanał kwantowy. Większość wyników literaturowych dotyczy sytuacji, w której dla zadanego szumu dekodowanie zwraca dokładnie ten sam stan kwantowy, który został zakodowany. To mocno ogranicza scenariusze, dla których można taki perfekcyjny kod korekcji błędów

skonstruować. Głównym celem pracy było przebadanie obszerniejszej klasy probabilistycznych kodów korekcji błędów, czyli takich, dla których zakodowany stan kwantowy jest dekodowany tylko z pewnym prawdopodobieństwem, a także udowodnienie, że tego typu kody mogą chronić informację kwantową w przypadkach, w których kody deterministyczne nie istnieją. Uważam, że mgr Kukulski postawiony sobie cel osiągnął i to z nawiązką. W istocie w swojej rozprawie zawarł szereg nietrywialnych i ważnych wyników dotyczących charakteryzacji oraz konstrukcji probabilistycznych kodów korekcji błędów, które w dalszej części rozprawy są omówione w bardziej szczegółowy sposób. Dodam jeszcze, że rozprawa podejmuje jeszcze jeden problem badawczy jakim jest porównanie i przebadanie własności różnych technik losowania kanałów kwantowych oraz ich uogólnień takich jak np. superkanały kwantowe, czyli odwzorowań liniowych działających na kanały kwantowe. O ile wyniki te zostały zamieszczone w rozprawie ze względu na ich późniejsze zastosowania w badaniu kodów korekcji, to tworzą one jednak nieco odrębną całość.

Wyniki. Rozdział 3 dotyczy losowania kanałów kwantowych, superkanałów, czy instrumentów kwantowych. Dokonano tutaj dogłębnego porównania znanych z wcześniejszych prac różnych technik losowego generowania kanałów kwantowych, które to techniki są pochodną różnych sposobów reprezentowania kanałów kwantowych, np. w oparciu o postać Krausa, czy też o izomorfizm Choia-Jamiołkowskiego. Z jednej strony udowodniono ich równoważność w tym sensie, że odpowiadające im miary probabilistyczne są sobie równe. Z drugiej strony, pokazano, że z punktu widzenia złożoności obliczeniowej optymalnym sposobem generowania losowych kanałów jest ten oparty na postaci Krausa. Następnie, Autor pokazuje jak metody losowego wytwarzania kanałów kwantowych można uogólnić na instrumenty kwantowe, czyli zbiory podkanałów kwantowych, które sumują się do kanału kwantowego, a które można uznać za uogólnienia pomiarów kwantowych, oraz superkanałów kwantowych, czyli odwzorowań działających na kanałach kwantowych. Autor pokazuje także, że pod pewnymi warunkami wygenerowane przy pomocy tych uogólnień obiekty kwantowe mają jednostajne rozkłady. Wreszcie w podrozdziale 3.2 przebadane są pewne własności losowych kanałów kwantowych takie jak np. ekstremalność, koherencja kanałów czy też rozkłady stanów kwantowych otrzymanych po zadziałaniu na zadany stan kwantowy.

W tej części pracy Autor sformułował szereg bardzo cennych obserwacji dotyczących losowych kanałów kwantowych (oraz ich uogólnień wymienionych wyżej), które mają duże znaczenie np. z punktu widzenia ich zastosowań do badania efektywności protokołów kwantowych. W istocie, niektóre z wyników zaprezentowanych w tym rozdziale są wykorzystywane do badania kodów korekcji błędów w rozdziałach 4 i 5. Mam jednak małą uwagę krytyczną dotyczącą sposobu prezentacji wyników, którą w zasadzie stosuje się do wszystkich rozdziałów ,,badawczych" rozprawy. Otóż niektóre wyniki podane są w zasadzie beż żadnej interpretacji tak jak np. wzory (3.42). Sprawia to, że nie jest do końca jasne co Autor chciał powiedzieć podając ten czy inny wynik.

Rozdziały 4 i 5 to zasadnicza część pracy, w której podano wyniki dotyczące probabilistycznych kodów korekcji błędów. Głównym celem rozdziału 4 jest pokazanie, że w sytuacji, w której takie perfekcyjne kody nie istnieją, wciąż można korygować błędy używając kodów probabilistycznych. Ilość wyników zaprezentowana w tym rozdziale jest ogromna i nie ma sensu ich tutaj streszczać. Ograniczę się do wymienienia kilku najważniejszych:

1. Sformułowanie warunków koniecznych i dostatecznych na to, aby dla danego modelu szumu reprezentowanego przez kanał kwantowy istniała probabilistyczna wersja korekcji błędów (Twierdzenie 4.4). Otrzymane warunki są odpowiednikami twierdzenia Knill-Laflamme dla deterministycznych kodów korekcji błędów.

2. Dowód, że zbiór kanałów kwantowych reprezentujących szum, dla których istnieją probabilistyczne kody nadzbiorem dla zbioru kanałów, dla których istnieją standardowe kody. W istocie, pokazano mocniejszy wynik mówiący, że w przypadku gdy wymiar przestrzeni, w której kodowana jest informacja kwantowa jest większy niż wymiar wyjściowej przestrzeni, drugi z owych zbiorów jest nigdziegęsty w pierwszym zbiorze.

3. Ograniczenia górne na maksymalne rzędy kanałów Shura (czyli kanałów, których operatory Krausa są diagonalne w bazie obliczeniowej), które mogą są korygowalne przy pomocy kodów probabilistycznych i

deterministycznych (Lemat 4.22). Następnie udowodniono, że ograniczenia te dla dostatecznie dużego wymiaru przestrzeni, w której kodowana jest informacja są osiągalne, co implikuje, że istnieją kanały Shura, dla których istnieją kody probabilistyczne, ale nie deterministyczne.

4. Wreszcie w oparciu o rozdział 3 pokazano w Twierdzeniu 4.29, że dla kanałów losowych istnieje separacja pomiędzy kanałami dla których istnieją kody korekcji w wersji probabilistycznej i deterministycznej.

5. Dowód, że dla pewnych kanałów kwantowych w celu zwiększenia prawdopodobieństwa prawidłowego dekodowania informacji kwantowej należy informację kwantową kodować w stan mieszany.

6. Sformułowanie metod konstrukcji probabilistycznych kodów korekcji błędów oraz wyznaczania lub estymacji prawdopodobieństwa sukcesu w oparciu o programowanie półokreślone (Lematy 4.8 i 4.11).

7. Dowód, że w przypadku czterowymiarowym wszystkie kanały o rzędzie nie większym niż dwa należą do klasy kanałów korygowalnych probabilistycznie, w przypadku gdy wymiar układu wejściowego to dwa. Oznacza to, że w przypadku kubitowym wystarczy kodować kwantową informację w dwóch kubitach tak, aby istniała procedura probabilistycznej korekcji błędu dla dowolnego kanału kwantowego reprezentującego szum o rzędzie 2. Fakt ten leży u podstaw algorytmu 28 (strona 80), który jest obiektem wniosku patentowego.

O ile jestem pod wrażeniem wyników zawartych w rozdziale 4, to mam jednak dwie uwagi krytyczne odnośnie sposobu ich prezentacji. Autor w rozprawie przyjął styl typowy dla prac matematycznych, w których po definicjach następuje seria twierdzeń i faktów. O ile to sprawia, że praca jest uporządkowana i łatwo się można po niej poruszać, to podobnie jak w przypadku rozdziału 3, w niektórych miejscach zabrakło kilku zdań interpretacji. Przykładowo, zabrakło mi dyskusji jak można odtworzyć oryginalne warunki z twierdzenia Knill-Laflamme (4.25) z warunków (4.24) sformułowanych dla kodów probabilistycznych w przypadku, gdy p=1.

Ponadto, dowody są podane w dość skrótowy sposób. Przykładowo, w Proposition 3.12 nie jest dla mnie jasne dlaczego po prawej stronie pierwszej równości operatory Q i G pojawiają się tylko ,,w kecie". Ponadto, nie jest jasne jak bezpośrednio z ostatniego zdania dowodu wynika, że rząd macierzy, która pojawia się w ostatniej równości w (3.28), jest równy min(r^2,dim(X)^2). Owa macierz jest bowiem sumą macierzy, a rząd nie jest funkcją addytywną. Weźmy przykładowo macierze K_0=I oraz K_1=S_z, gdzie I to po prostu macierz jednostkowa 2x2, a S_z to macierz Pauliego diagonalna w bazie obliczeniowej. Rząd obu macierzy to oczywiście dwa, ale rząd sumy iloczynów tensorowych tych macierzy nie jest równy 4, ale też dwa. Zapewne został tam użyty jakiś dodatkowy fakt, o którym Autor już nie wspomniał.

Rozdział piąty dotyczy badania kodów probabilistycznych, a także porównania ich z kodami deterministycznymi od strony jakościowej, przy czym wyznacznikiem „jakości" są tutaj: średnia wierność i średnia wierność warunkowa, w zależności od tego, czy dekodowanie jest kanałem czy podkanałem oraz średnie prawdopodobieństwo sukcesu w przypadku kodów probabilistycznych. Najważniejszym wynikiem tej części pracy jest podanie konstrukcji, dla pewnej klasy kanałów reprezentujących szum zadanych w równaniu (5.7), aproksymacyjnych kodów korekcji błędów (w obu wersjach deterministycznej i probabilistycznej), która jest tak dobrana, aby dawała jak największe wartości średnich wierności. Autor przekuwa również swoją konstrukcję w algorytm i analizuje jego złożoność obliczeniową. Jako że otrzymana konstrukcja nie jest w ogólności optymalna, Autor podaje też sposoby zwiększenia średniej wierności, np. przy użyciu metody ,,huśtawkowej" (ang. *see-saw*) w oparciu o programowanie półokreślone. Jakość tego algorytmu jest wreszcie przebadana na kanałach losowych, a otrzymane wyniki są zobrazowane na serii wykresów (Fig. 5.2-5.11). Wynika z nich, że w przeważającej większości przypadków aproksymacyjne kody probabilistyczne przewyższają kody deterministyczne jeśli chodzi o średnią wierność, co stanowi kolejne potwierdzenie, że kody probabilistyczne stanowią bardzo interesująca alternatywę dla kodów deterministycznych.

Mam jednak, podobnie jak wcześniej, krytyczną uwagę dotyczącą prezentacji wyników. Mianowicie zabrakło mi kilku zdań wyjaśnienia dlaczego Autor bierze pod uwagę wielkości podane w równaniach (5.1), (5.2) i (5.3), a nie inne, oraz skąd się te wzory wzięły; jak rozumiem są one wynikiem jakiejś procedury uśredniania. Przyczepię się jeszcze do numeracji algorytmów: algorytm na stronie 80 nosi numer 28, a ten podany później na stronie 95 ma numer 3.

Konkluzja. Wysoko oceniam rozprawę mgr Kukulskiego. Przedstawił on w niej sporą ilość wysoce nietrywialnych wyników dotyczących kodów korekcji błędów czy metod generowania losowych kanałów kwantowych, które z całą pewnością będą miały duży wpływ na rozwój dziedziny. W szczególności, Autor z powodzeniem wywiązał się z postawionego sobie celu, którym było udowodnienie, że "zastosowanie probabilistycznych kodów korekcji błędów może poprawić jakość ,,zaszumionych" układów kwantowych". Dodam również, że rozprawa bardzo pozytywnie świadczy o warsztacie matematycznym mgr. Kukulskiego. Sprawnie się on posługuje pojęciami, a także technikami dowodzenia z zakresu teorii macierzy losowych, algebry liniowej, czy analizy funkcjonalnej. Ponadto, Autor opanował metody optymalizacji wypukłej oraz potrafi zaimplementować zaprojektowane przez siebie algorytmy na komputerze kwantowym. Z drugiej strony, moje negatywne uwagi dotyczą jedynie sposobu prezentacji wyników i nie mają wpływu na moją ogólną pozytywną ocenę rozprawy. **Podsumowując, jednoznacznie stwierdzam, że rozprawa mgr Kukulskiego spełnia ustawowe wymogi stawiane rozprawom doktorskim i wnoszę o dopuszczenie jej do publicznej obrony.**

Poniżej odpowiem jeszcze pokrótce na pytania zamieszczone w umowie o sporządzenie recenzji.

1. Czy tematyka rozprawy jest aktualna i jak jest związana z rozwojem dyscypliny?

Jak już wspomniałem na początku recenzji tematyka rozprawy jest jak najbardziej aktualna. Metody korekcji błędów są nieodzowną częścią protokołów przetwarzania informacji i mają ogromne znaczenie dla rozwoju nowych technologii kwantowych takich jak wspomniane w rozprawie komputery kwantowe.

2. Jaki jest problem naukowy podejmowany przez Autorkę i czy został on trafnie sformułowany?

Problem naukowy podejmowany w rozprawie to rozwijanie metod korekcji błędów w wersji probabilistycznej oraz wykazanie, że metody te są użyteczne w ochronie informacji kwantowej. Problem jest bardzo trafnie sformułowany ze względu na użyteczność tego typu metod w przetwarzaniu informacji kwantowej. Autor dowodzi w rozprawie, że w przypadku generycznych kanałów kwantowych opisujących błędy nie istnieją kody deterministyczne, które mogłyby chronić informację kwantową i de facto kody w wersji probabilistycznej stają się jedyną opcją jeśli chodzi o ochronę informacji kwantowej przed błędami. Ponadto, wykazuje on również, że aproksymacyjne kody probabilistyczne ,,na średnio" lepiej sobą radzą niż kody deterministyczne.

3. Czy Autor rozwiązała postawiony problem i czy wykorzystała w tym celu właściwe metody?

W serii wyników teoretycznych mgr Kukulski udowodnił, że probabilistyczne kody korekcji błędów są użyteczne w ochronie informacji kwantowej, w przypadku gdy odpowiednie kody deterministyczne nie istnieją. Ponadto, w oparciu o programowanie półkreślone, bardzo popularne i przydatne narzędzie w ramach kwantowej teorii informacji, Autor sformułował metody znajdowania kodów korekcji dla zadanego kanału reprezentującego szumy, a także metody optymalizacji prawdopodobieństwa sukcesu. Stwierdzam, że postawiony problem został przez Autora rozwiązany i że użyte metody były dobrane bardzo trafnie.

4. Na czym polega oryginalny wkład Autora w dyscyplinę?

Mgr Kukulski podał szereg wyników naukowych, które w zasadzie zostały już przez mnie opisane powyżej. Powtórzę więc w skrócie, że pomijając już cześć dotycząca kanałów kwantowych (rozdział 3) oryginalny

wkład Autora w dyscyplinę to: (i) dogłębna charakteryzacja probabilistycznych kodów korekcji błędów, dowód, że owe kody są użyteczne w ochronie informacji kwantowej w przypadku, gdy odpowiednie kody deterministyczne nie istnieją; (ii) zaproponowanie metod konstrukcji tego typu kodów; (iii) konstrukcja kodów aproksymacyjnych dla pewnej klasy kanałów oraz wykazanie, że owe kody w wersji probabilistycznej mogą zwiększać średnią wierność w stosunku do kodów deterministycznych.

5. Jakie jest znaczenie poznawcze oraz znaczenie praktyczne wkładu Autora?

Znaczenie poznawcze to dogłębna charakteryzacja metod losowania kanałów kwantowych oraz kodów korekcji błędów (w tym przypadku zarówno od strony jakościowej jak i ilościowej), a znaczenie praktyczne to algorytmy, które pozwalają kody korekcji konstruować. W istocie, przedstawiony w rozprawie algorytm 28 jest podstawą wniosku patentowego, którego mgr Kukulski jest współautorem.

6. Czy rozprawa świadczy o dostatecznej wiedzy Autora w zakresie nauk technicznych i w szczegółowej wiedzy w odpowiadającej zakresowi badań?

Jednoznacznie mogę stwierdzić, że rozprawa świadczy o rozległej wiedzy autora w dziedzinie informatyki kwantowej, w szczególności w obszarze metod korekcji błędów. Rozwój komputerów kwantowych, którego nieodzowną częścią są kody korekcji błędów, wpisuje się w obszar zainteresowania dyscypliny informatyka techniczna. Ponadto, rozprawa dowodzi, że mgr Kukulski dysponuje świetnym warsztatem matematycznym. Bez problemu posługuje się pojęciami oraz technikami dowodzenia z teorii macierzy losowych, analizy funkcjonalnej czy algebry liniowej.

7. Jakie są słabe strony rozprawy?

Słabe strony rozprawy jakie udało mi się zidentyfikować dotyczą w gruncie rzeczy sposobu prezentacji wyników. W moim odczuciu, niektóre dowody są zaprezentowane zbyt skrótowo, a ponadto w przypadku niektórych wyników brakuje kilku zdań interpretacji. Rozprawa doktorska jest miejscem, gdzie doktorant może rozwinąć rozważania zawarte w publikacjach, które bardzo często są zaprezentowane w okrojony sposób.

Remigiusz Michał Augusiak

Elektronicznie podpisany przez Remigiusz Michał Augusiak
Data: 2023.07.21 13:37:57 +02'00'