Toruń, 28.10.2019

Prof. dr hab. Dariusz Chruściński
Instytut Fizyki
Uniwersytet Mikołaja Kopernika

Recenzja dorobku naukowego dra Karola Horodeckiego w postępowaniu habilitacyjnym

Pan dr Karol Horodecki uzyskał stopień doktora nauk matematycznych w zakresie informatyki na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego w roku 2009 przedstawiając rozprawę doktorską pt. „*General paradigm for distilling classical key from quantum states – on quantum entanglement and security*". W roku 2008 został zatrudniony w Instytucie Informatyki Uniwersytetu Gdańskiego na stanowisku asystenta, a od maja 2009 na stanowisku adiunkta.

Na rozprawę habilitacyjną dra Horodeckiego składa się cykl 7 prac oryginalnych [H1-H7] opublikowanych w prestiżowych czasopismach naukowych w latach 2012-2017 pt. „**Wybrane, wzajemne relacje między nielokalnością Bella, kluczem kryptograficznym bezpiecznym względem adwersarza i kwantowym splątaniem**". Prace [H2-H7]wchodzące w skład rozprawy są wieloautorskie. Dołączona dokumentacja zawiera oświadczenia wszystkich współautorów określające ich rolę w procesie tworzenia artykułów:

- praca [H2]: 5 autorów; wkład habilitanta 50%
- praca [H3]: 2 autorów; wkład habilitanta 55%
- praca [H4]: 4 autorów; wkład habilitanta 25%
- praca [H6]: 6 autorów; wkład habilitanta 25%
- praca [H7]: 3 autorów; wkład habilitanta 25%

Lista współautorów obejmuje:

- Paweł Horodecki, Andrzej Grudka (3 prace)
- Michał Horodecki, Ryszard Horodecki, Pankaj Joshi (2 prace)
- Waldemar Kłobus, Justyna Łodyga, Stefan Baeuml, Glaucia Murta, Andreas Winter, Matthias Christandl, Konrad Banaszek (1 praca)

Habilitant dołączył również do dokumentacji zgrabnie napisany autoreferat (w języku polskim i angielskim). Pisanie w języku polskim nie jest proste, ponieważ duża część używanych terminów istnieje jedynie w języku angielskim i tłumaczenie często jest problematyczne. Autoreferat jest profesjonalnie przygotowany, chociaż habilitant nie ustrzegł się kilku drobnych usterek (np. druga suma w równaniu (13) powinna przebiegać po „a" nie po „b"). Rysunek na str. 8 znakomicie ilustruje powiązania między różnymi elementami rozprawy i pokazuje na rozległość badań habilitanta.

Ocena osiągnięcia naukowego

Przedstawione prace dotyczą fundamentalnych aspektów teorii kwantowej takich jak nielokalność Bella, kwantowe splątanie czy też kontekstualność, oraz analizie ich praktycznych zastosowań w teorii kwantowej informacji. Tym samym rozprawa dra Horodeckiego wpisuje się w bardzo ważny i aktualny nurt badań. Co więcej, uzyskane wyniki oprócz fundamentalnego aspektu poznawczego posiadają nietrywialny potencjał aplikacyjny. Motywem przewodnim rozprawy jest tzw. teoria zasobów (resource theory). W kontekście teorii kwantowej zasobem jest pewna klasa stanów kwantowych, które mogą być użyteczne w pewnych protokołach kwantowo-informatycznych. Stany, które nie zawierają danego zasobu (np. stany separowalne w teorii splątania) są w takim protokole bezużyteczne i w teorii zasobu są tzw. stanami „darmowymi". Kluczowym elementem teorii jest zdefiniowanie klasy operacji (przekształceń), które nie generują zasobu. W teorii splątania to znana klasa operacji lokalnych (na podukładach) + klasyczna komunikacja między laboratoriami. Następny krok to próba ilościowej charakteryzacji zasobu (np. miary splątania w teorii splątania). Praca habilitacyjna dra Horodeckiego poświęcona jest analizie porównawczej różnych zasobów (kwantowe splątanie, klucz kryptograficzny, nielokalność Bella oraz kontekstualność) oraz ich ilościowej charakteryzacji. Co ciekawe w swoich badaniach habilitant wychodzi również poza teorię kwantową rozważając bardziej ogólny schemat warunkowych rozkładów prawdopodobieństwa spełniających warunek braku sygnalizacji, ale niekoniecznie konsystentnych z kwantowym paradygmatem. Warto dodać, że teoria zasobów stała się bardzo owocnym podejściem do wielu problemów kwantowej teorii informacji. W ostatnich kilku latach była rozwijana teoria, w której zasobem jest kwantowa koherencja.

Do najważniejszych wyników rozprawy zaliczam:

1. wprowadzenie ważnych miar kontekstualności w pracy [H5]. Te miary to:
- wzajemna informacja kontekstualności (Mutual Information of Contextuality),
- względna entropia kontekstualności (Relative Entropy of Contextuality), oraz
- koszt kontekstualności (Cost of Contextuality).

Pierwsza z miar posiada interesującą interpretację optymalizacji strategii w pewnej grze. Autorzy[H5] pokazują, że dwie pierwsze miary dają tę samą wartość kontekstualności. Z kolei względna entropia kontekstualności jest ograniczona z góry przez koszt kontekstualności. Praca [H2] analizuje aksjomatyczne podejście do kwantowej kontekstualności i nielokalności. Centralnym wynikiem tej pracy jest wykazanie, że dwie pierwsze miary posiadają własność asymptotycznej ciągłości. Własność ta jest kluczowa dla wszystkich eksperymentów wykrywających kontekstualność, ponieważ każda miara asymptotycznie ciągła nie jest wrażliwa na możliwe błędy przygotowania eksperymentu. Na podkreślenie zasługuje fakt, że jest to pierwsza propozycja ilościowej charakteryzacji kontekstualności w literaturze.

2. Wprowadzenie świadka prywatności w pracy [H7]. (Pewnie omyłkowo habilitant załączył w dokumentacji wersję [H7] z Physical Review A z ciekawymi prywatnymi komentarzami/pytaniami do współautorów). Świadek splątania był powszechnie znany w teorii splątania – operator hermitowski (kwantowa obserwabla), którego wartość średnia jest nieujemna na wszystkich stanach separowalnych i staje się ujemna na pewnych stanach splątanych. Habilitant i współautorzy pracy zaproponowali analogiczny obiekt jako świadka prywatności (privacy witness). Jest to obserwabla, która wykrywa obecność klucza kryptograficznego. Co ciekawe dotyczy to także stanów ze splataniem związanym. Dodatkowo świadek prywatności

pozwala oszacować ilość klucza na podstawie stosunkowo niewielkiej liczby pomiarów co ma istotne znaczenie w praktycznych zastosowaniach pozwalając na ekonomiczne wykrywanie zasobu.

3. Ograniczenia powtarzaczy klucza kryptograficznego (quantum key repeaters) wyprowadzone w pracy [H4]. Jednym z istotnych zastosowań kwantowej komunikacji jest dystrybucja stanów splątanych do generacji klucza kryptograficznego. Aby osiągnąć realistyczne odległości dystrybucji konieczne jest stosowanie linii przesyłowych wyposażonych w kwantowe powtarzacze (quantum repeaters). Kluczowa jest zatem analiza fundamentalnych ograniczeń na powtarzacze dla ekstrakcji klucza kryptograficznego. Habilitant stawia dwa fundamentalne pytania:

a) czy klucz jest przekazywalny za pomocą stanów mieszanych,

b) czy klucz zawarty w stanie mieszanym jest powtarzalny za pomocą kwantowego powtarzacza.

Praca [H4] pokazuje, że w obu przypadkach odpowiedź jest negatywna. Habilitant podał przykłady stanów zawierających klucz kryptograficzny, które posiadają klucz powtarzalny, który zbiega do zera wraz z wymiarem stanu. Wynik ten pokazuje na związek bezpieczeństwa klucza kryptograficznego i nielokalności Bella, gdzie również nie ma możliwości przekazywania i powtarzania nielokalności. Habilitant uważa, że jedynie stany czyste pozwalają na powtarzanie klucza. Fakt ten wymaga jednak dowodu.

4. W samodzielnej pracy [H1] habilitant analizował problem rozróżnialności warunkowych niesygnalizujących rozkładów prawdopodobieństwa w schemacie dwa laboratoria, dwa urządzenia pomiarowe + dwa możliwe wyniki pomiaru. Rozkłady te tworzą wielościan oznaczany w literaturze przez NS(2,2,2,2). Stosując techniki wykorzystywane wcześniej w teorii splątania habilitant oszacował prawdopodobieństwo sukcesu rozróżnienia zbioru rozkładów warunkowych. Ponadto, pokazano, że każda para rozkładów ekstremalnych odpowiadających wierzchołkom wielościanu NS(2,2,2,2) jest rozróżniana konkluzywnie z niezerowym prawdopodobieństwem.
5. Nierozgłaszalność nielokalności Bella wykazane w pracy [H6]. Jak wiadomo teoria kwantowa zabrania klonować nieznane stany kwantowe. Istnieje również silniejsze ograniczenie, które zabrania rozgłaszać nieznane stany, tzn. tworzyć stan układu złożonego, którego ślady częściowe odtwarzają początkowy (nieznany) stan kwantowy. Istnieje również wersja 2-cząstkowa (bipartite) zasady nierozgłaszania, w której stan jest znany, ale możemy używać jedynie lokalnych operacji (wynik uzyskany przez M. Piani i P. Horodecki). W pracy [H6] habilitant analizował analogiczny problem dla zasobu jakim jest nielokalność Bella. Analizując ponownie wielościan NS(2,2,2,2) dr Horodecki wykazał, że rozgłaszanie nielokalności Bella jest zabronione przy użyciu operacji zachowujących lokalność (są one analogiem znanych w teorii splątania operacji lokalnych i klasycznej komunikacji).

Ocena pozostałego dorobku naukowego

Pozostały dorobek naukowy dra Horodeckiego jest również bardzo wartościowy i dowodzi bardzo wysokiej aktywności naukowej. Składa się na niego 27 publikacji z listy filadelfijskiej. Prace dra Horodeckiego były cytowane ponad 4300 (wg. Web of Science) a index h=14. Prace te dotyczą podstaw teorii kwantowej, kwantowej teorii informacji oraz generacji i amplifikacji losowości (randomness). Ostatni numer Physical Review Letters zawiera kolejną pracę habilitanta:

D. Yang, K. Horodecki, and A. Winter, *Distributed Private Randomness Distillation*. Phys. Rev. Lett. **123**, 170501(2019).

Dr Horodecki jest współautorem przeglądowej pracy
R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 966 (2009), która była już cytowana prawie 4000 razy i weszła do kanonu literatury na temat kwantowego splątania.

Dr Horodecki wygłaszał referaty na wielu konferencjach międzynarodowych (w dokumentacji wymienia 18 wystąpień). Sam miałem okazję kilka razy słuchać wystąpień habilitanta, które oceniam jako bardzo profesjonalne.

Ocena działalności dydaktycznej i popularyzatorskiej

Dr Karol Horodecki opracował i prowadził wykład „Podstawy informatyki kwantowej". W latach 2008-218 prowadził szereg zajęć dydaktycznych:

- projektowanie i przetwarzanie języków XML
- wstęp do programowania
- języki programowania
- środowisko programisty
- matematyka dyskretna

Jest współautorem opracowania

- H. Furmańczyk i K. Horodecki, P. Żyliński, *Matematyka dyskretna dla studentów kierunku informatyka*, Uniwersytet Gdański (2010).

Brał udział jako promotor pomocniczy w dwóch przewodach doktorskich:

- Waldemar Kłobus, „Wybrane własności korelacji w mechanice kwantowej i ogólnych teoriach probabilistycznych" UAM
- Pankajkumar Rajeshkumar Joshi, „Quantitive approach to some aspects of Bell nonlocality and contextuality", UG

Pozyskiwanie środków na badania naukowe

Dr Horodecki kilka razy kierował projektami naukowymi Uniwersytetu Gdańskiego. Aktualnie jest kierownikiem grantu Sonata Bis 5 NCN „Bezpieczeństwo komunikacji w sytuacji podsłuchu i włamania, oparte o prawa fizyki". Brał również aktywny udział w wielu projektach europejskich:

- 5 Program Ramowy EU „Quantum properties of distributed systems" (2003-2006)
- 5 Program Ramowy EU „Resources for quantum computing" (2003-2006)
- 6 Program Ramowy EU „Scalable quantum computing with light and atoms" (2005-2009)
- 7 Program Ramowy EU Q-ESSENCE
- Grant European Research Council Advance Grant: Quantum resOurces: conceptuaLs and AplicationS (QOLAPS) (2012-2016)

Nagrody i wyróżnienia

Habilitant był kilkakrotnie nagradzany

- Stypendium Miasta Gdyni (2002/2003)
- Stypendium Ministra Edukacji Narodowej i Sportu (2003/2004)
- Zespołowa nagroda Ministra za cykl prac dotyczących teorii splątania i kryptografii kwantowej (2006)
- Stypendium Fundacji na rzecz Nauki Polskiej (2206/2007 i 2007/2008)

Podsumowanie: uważam, że dorobek naukowy dra Karola Horodeckiego jest wybitny, a przedstawiony cykl 7 prac, składający się na rozprawę habilitacyjną, stanowi znaczący wkład w rozwój dyscypliny naukowej zgodnie z wymogami ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki. Dlatego wniosek o nadanie panu dr. Karolowi Horodeckiemu stopnia doktora habilitowanego uważam za całkowicie uzasadniony i z pełnym przekonaniem wnoszę o jego przyjęcie przez Radę Wydziału Matematyki, Fizyki i Informatyki Uniwersytetu Gdańskiego.

D. Chruściński

prof. dr hab. Dariusz Chruściński