Los Angeles, 5.03.2018

dr hab. Marcin Wieśniak, prof. UG.

Instytut Informatyki

Wydział Matematyki, Fizyki i Informatyki

Uniwersytet Gdański

Ul. Wita Stwosza 57

80-308 Gdańsk

Recenzja dorobku naukowego i aktywności akademickiej dr Marcina Pawłowskiego w związku z postępowaniem habilitacyjnym.

Dr Pawłowski w chwili składania wniosku legitymował się 41 publikacjami po doktoracie. 10 spośród z nich stanowi dzieło w formie monotematycznej serii pt. *Kody swobodnego dostępu w informatyce kwantowej*. Wybrane publikacje ukazały się w bardzo dobrych czasopismach (głównie w *Phys. Rev. X, Lett., A*). Kody swobodnego dostępu wiążą się zadaniem komunikacyjnym pomiędzy dwoma użytkownikami. Jeden z nich przyjmuje kilka parametrów wejściowych i koduje je w stan nośnika (wiadomość klasyczną, lub kwantową o określonej pojemności). Następnie nośnik jest przesyłany do drugiego użytkownika, którego dane wejściowe określają wartość którego parametru ma być w miarę możliwości odkodowana. Jeżeli pojemność ta jest mniejsza, niż łączna pojemność wszystkich parametrów wejściowych pierwszego obserwatora, nie może się top udać idealnie, co stanowi podstawę najważniejszego wyniku Habilitanta i chyba w ogóle jednego z najważniejszych wyników środowiska gdańskiego, przyczynowości informacji. Tak ogólne sformułowanie zadania pozwala na bardzo szeroką analizę wielu aspektów teorii informacji, nie tylko kwantowej, na przykład bezpieczeństwa protokołów kryptograficznych. Kody takie występują w kilku wariantach. Możemy przesyłać informację klasyczną, cząstkę kwantową, lub, co było odkryte przy udziale Habilitanta, mogą być wspomagane przez współdzielony stan splątany. Ogólnie, prace zawarte w dziele są tematycznie bardzo spójne, a wkład Habilitanta do rozumienia problemu jest ogromny i doceniany w świecie, wprost fundamentalny. Na tym możnaby zamknąć część naukową recenzji, jednak pozwolę sobie na kilka uwag odnośnie przedstawionych prac.

Praca oznaczona jako [1] (lub literą, do czego wrócę później) wyprowadza warunek na bezpieczeństwo klucza kryptograficznego w schemacie kryptograficznym z użyciem kodu losowego (czyli swobodnego) dostępu (RAC). Oczywiście, kwantowy RAC (QRAC) pozwala na wykroczenie ponad wartość graniczną, dzięki temu mamy gwarancję, że Ewa (podsłuchiwacz) przechwyciła od Alicji (nadawcy) mniej bitów, niż Bob (odbiorca). Dowód jest bardzo elegancki.

Gdyby oprzeć się tylko na opisie pracy [2] z Autoreferatu, kojarzyłaby się ona z bardzo kontrowersyjną praktyką „odkrywania dla poddziedziny" znanych już wyników. W tym przypadku

chodzi o układy kwantowe, których pomiary są opisane przez wektor na wielowymiarowej sferze. Dlatego dla mnie istotą tej pracy są hipotezy na temat wydajności RAC przy użyciu takich układów w kilku protokołach. Bez odpowiedzi pozostaje jednak pytanie, o jakie układy tego typu chodzi. W grę wchodzi mechanika kwantowa z amplitudami będącymi uogólnieniami liczb zespolonych (co zostało wykluczone przez Dakicia i Bruknera, oraz układy związane z fermionami Majorany, co jednak kłuci się z ideą przesyłania pojedynczej cząstki.

Układy takie pojawiają się w pracy [3], w której Autorzy analizują wydajność certyfikacji (a właściwie wzmocnienia) losowości przy pomocy RAC. Jest to naturalne podejście, gdyż jak już wspomniałem ilość przesyłanej informacji jest mniejsza, niż informacji zakodowanej. Okazuje się, że miara wzmocnienia splątania, min-entropia jest najwyższa, jeżeli stosujemy kwantowy kod 3->1 (w którym kodujemy 3 bity w stan układu dwuwymiarowego). Jest to o tyle ciekawy wynik, że jego naturalną realizacją jest przesłanie kubitu.

Praca [4] przedstawia związek pomiędzy protokołami niezależnymi i częściowo niezależnymi od urządzeń. Przez niezależność od urządzeń rozumiemy takie sformułowanie protokołu, w którym nie musimy zakładać wymiaru użytych układów. W protokołach częściowo niezależnych zakładamy określony wymiar, jednak precyzujemy szczegółów przygotowania i pomiaru. Podstawowym związkiem pomiędzy tymi podejściami jest założenie, że korelacje pomiędzy wartościami parametrów wyjściowych powstają w laboratorium Alicji, na przykład posiada ona źródło stanów splątanych i przygotowuje ona stan dla Boba przez pomiar. Autorzy pracy podają jednak związek na ogólniejszym poziomie, przy pomocy wartości min-entropii. Wadą tej pracy jest wprowadzenie chaosu w nomenklaturze. Habilitant i współautorzy używają pojęcia „nierówność Bella" dla określenia operatora Bella (pomińmy tu kwestię odpowiedniej struktury czasoprzestrzennej problemu).

Analogiem dla świadectwa (częściej używa się nieco niezręcznego słowa „świadek") splątania jest pojawiające się w pracy [5] świadectwo wymiaru. Wyraża się ono przez nierówność, w której wartość średnia odpowiednio dobranego operatora porównywana jest do ograniczenia. Złamanie tej nierówności oznacza, że dane statystyki wymagają co najmniej wymiaru d. Praca [5] opisuje doświadczalny pomiar takich operatorów dla $d<5$. Technicznie jest to chyba najprostszy możliwy eksperyment, polegający na przygotowaniu i natychmiastowym pomiarze stanu, bez żadnych efektów interferometrycznych. Trzeba tu zauważyć, że Autorzy pracy (a Habilitant był wśród nich wiodącym teoretykiem) nie wyjaśniają w niej jaki jest związek użytego świadectwa ze nierównością CHSH, a nie jest to również oczywiste z jego postaci. Stanowi to duży brak pracy [5], gdyż nierówność CHSH stanowi bazę wielu ważnych wyprowadzeń.

Świadectwa splątania są również centralnym pojęciem w pracy [6], w której poznajemy metody otrzymywania świadectw wymiaru z nierówności Bella. Omówione jest założenie symetryczności statystyk, które istotnie upraszcza wyniki i podane są przykłady. Praca ta nie powiela bałaganu z pracy [4].

Praca [7] ponownie wskazuje na analogię między protokołami niezależnymi i częściowo niezależnymi od urządzeń. Tym razem odbywa się to na bardziej ogólnym poziomie pudeł. Są to ogólne urządzenia, które zwracają wyniki po otrzymaniu danych wejściowych. Najważniejszym przykładem jest pudło Popescu-Rohlinga, wysycające granicę arytmetyczną nierówności CHSH. Autorzy pracy [7] budują z niego pudło RAC stosując technikę wiringu, czyli wprowadzania wyjścia jednego z użytkowników, jako wejścia drugiego (w ogólności łamie to zasadę niesygnalizowania, na której oparte są pudła PR). Porównując działanie obu pudeł formułują oni „nierówność", w której porównują potencjał różnych kombinacji zasobów do realizacji określonych zadań. W szczególności pokazują oni warunek na

nasycenie tej „nierówności". Wynik ten jest niezwykle istotny, gdyż od tej pory wyniki otrzymane przy pomocy RAC można tłumaczyć na język pudeł PR i odwrotnie. Można jedynie oczekiwać, że „nierówność" byłaby sformalizowana. W publikacji łączy ona ze sobą kilka bardzo różnych zasobów, np. jeden bit komunikacji klasycznej, współdzieloną losowość, kanał komunikacyjny i pudła. Warto by było przypisać im jakąś wspólnie określoną wartość liczbową.

Praca [8] podejmuje bardzo ciekawą próbę zastosowania kwantowego RAC w sytuacji życiowej, to jest w grze w brydża. W fazie licytacji drużyna musi wspólnie określić cel gry, zależny od posiadanych przez nich kart. Ci. Gracze nie mogą sobie wprost przekazywać informacji o posiadanej konfiguracji kart. Wykorzystując możliwość zmiany deklaracji w licytacji, Autorzy pokazują, że gracze mogą wykorzystać kwantowy RAC do ulepszenia strategii licytacji. Informacja o kartach nie jest niesiona przez przesyłaną cząstkę, a gracz sam decyduje, który bit zakodowany przez jego partnera chce poznać z pewnym prawdopodobieństwem. Praca jest bardzo ciekawa, gdyż opisuje konkretne, choć oszacowanie strategii klasycznej opiera się na komunikacji z Tommym Gullbergiem, m.in. dwukrotnym drużynowym mistrzem Europy w brydżu sportowym, którego zadaniem było oszacowanie pewnych prawdopodobieństw. Najczęściej jednak nie można zrobić tego dokładnie, zwłaszcza w tak złożonej grze. Przypomnę tu tylko próbę oszacowania prawdopodobieństwa ułożenia pasjansa podjętą przez Banacha, czy też niemożność podania możliwych rozkładów bierek w szachach. Przy wartościach przyjętych w pracy kwantowa licytacja brydżowa daje prawdopodobieństwo sukcesu o 0.007 wyższe, niż wynika z szacunków. Autorzy pracy nie poświęcili jednak uwagi tak małej różnicy, więc wynik wydaje się być kontrowersyjny.

Praca [9] dotyczy ważnego problemu nieidealnej wydajności detekcji w realizacji schematów kryptograficznych. Jest to problem dotyczący każdej konfiguracji doświadczalnej, gdyż w zjawisku tym mieszczą się również straty wskutek propagacji. Teoretycznie, Ewa (podsłuchiwacz), korzystając niedoskonałości detektorów mogłaby zmanipulować w wygodny dla siebie sposób wyniki protokołu, poprzez ukrywanie niektórych wydarzeń poprzez brak reakcji detektora. Autorzy pokazują, między innymi, warunek, w którym protokół oparty na klasycznym RAC, jest odporny na takie ataki. Stanowi to istotny krok do analogicznej analizy dla kodów opartych na kwantowym RAC.

W podobnej tematyce utrzymana jest praca [10], tym razem dotyczy ona jednak problemu wzmocnienia losowości. Autorzy przyjmują protokoły częściowo niezależne od urządzeń, w których zakładamy wymiar układu i rozważają dwa modele. W modelu symetrycznym, Bob ma jedną wartość wydajności wspólną dla obu pomiarów, w modelu asymetrycznym jeden z pomiarów jest idealny. Otrzymane wartości to 0.707 dla pierwszego scenariusza i dowolna efektywność dla drugiego. O ile drugi schemat nie jest bardzo ciekawy ze względu na nierealistyczne założenia, o tyle drugi daje ogromne nadzieje na realizację samotestującego się generatora liczb losowych, co jest celem grantu FNP FIRST TEAM, którym kieruje Habilitant.

Przejdźmy teraz do pozostałych aspektów wniosku. Niestety, Autoreferat napisany jest bardzo niedbale, zwłaszcza w wersji polskiej, co skutkuje jego bardzo ograniczoną użytecznością. W wersji polskiej roi się od błędów stylistycznych, interpunkcyjnych i typograficznych. Dla przykładu, na samym początku znajdujemy oczywiście listę publikacji wchodzących w skład osiągnięcia, ponumerowanych od [1] do [10]. Mimo, że są to wyłącznie teksty angielskie, tytuły czterech z nich zaczynają się od polskich liter, tworząc nowe słowa. Następnie habilitant informuje, że w dalszej części będzie stosował numerację [A]-[J], a numery [1]-[10] rezerwuje dla pozostałych swoich publikacji. Niestety, robi to nie zachowując kolejności. Autorzy wszystkich innych autoreferatów, których miałem okazję czytać, bez problemu wprowadzili własne, konsekwentne oznaczenia prac stanowiących osiągnięcie. Autoreferat jest na pozór objętości właściwej dla serii 10 prac, jednak po

bliższej lekturze czytelnik w wielu miejscach spodziewałby się pełniejszych opisów, zwłaszcza zważywszy na złożoność omawianej materii. Dla przykładu, należałoby wprowadzić do Autoreferatu opisy używanych symboli. Wersja angielska jest oczywiście lepsza językowo, jednak również nie zawsze napisana zgrabnym językiem i równie skrótowa. Należy tu przypomnieć, że habilitacja to krajowe postępowanie awansowe, więc to wersja polska jest kluczowa. Taki poziom przygotowania Autoreferatu stanowi dla czytelnika duże rozczarowanie i łatwo sobie wyobrazić sytuację, w której negatywnie zaważy na decyzji, np. w sprawie grantu.

Dane bibliograficzne są bardzo imponujące: łącznie 52 publikacje, cytowane ponad 700 razy, oraz indeks Hirscha 14 to wyniki zdecydowanie ponadnormatywne na tym szczeblu kariery i w tej dziedzinie. Habilitant może się też poszczycić wykonawstwem 10 grantów i kierownictwem czterech własnych, z których trzy polskie opiewają na łączną sumę zdecydowanie ponad 4 000 000 PLN. Stanowi to o potężnej pozycji habilitanta w systemie grantowym. Dodatkowo granty te przyniosły opiekę nad kilkoma doktorantami, co również jest bardzo istotnym osiągnięciem (Niestety, nie miałem okazji ich egzaminować).

Habilitant jest bardzo aktywny, jeżeli chodzi o współpracę międzynarodową, prawie każda publikacja napisana jest w innej konfiguracji współautorów. Niestety, nie wykazuje się klasycznie rozumianym stażem post-doktorskim, a jedynie 5 wizytami w trzech ośrodkach o łącznej długości 6 miesięcy. Nie powinno to w tym przypadku ważyć na ocenie. Wizyty kilkudniowe traktuję jako oczywistość

dr Pawłowski legitymuje się też pewnym dorobkiem dydaktycznym i popularyzatorskim. Na cele postępowania jest on w zupełności wystarczającym, jednak pozwolę tu sobie na dwie dygresje. Życie naukowe Habilitanta podzielone jest na okresy, w których uczy on mniej lub bardziej przypadkowych przedmiotów, i takie, w których pełnione funkcje zwalniają go z tego rodzaju obowiązków. Uważam, że najlepszą sytuacją z obopólnymi korzyściami byłoby powierzenie prowadzenia równomiernie rozłożonego w czasie przedmiotu bezpośrednio dotyczącego działalności naukowej Habilitanta. Wchodzimy tu jednak w meandry tej sfery życia akademickiego. Po drugie, do kategorii „działalność popularyzatorska" Habilitant zaliczył bardzo dużo różnych doświadczeń. Znajdziemy tu m. in. nauczanie fizyki w liceum (jest to niezwiązane z działalnością naukową), spotkania z uczniami (według mojej wiedzy, bardziej o charakterze biograficznym), czy prowadzenie wykładów w ramach „szkoły" dla studentów (czyli ludzi już związanych z fizyką). Po odjęciu tych pozycji zostaje wciąż dobry dorobek popularyzatorski, brak jednak jasnej informacji o udziale w sztandarowych programach Wydziału MFI UG, takich, jak „Zdolni z Pomorza", czy „Spotkania z fizyką", ja jeżeli miało to miejsce, to sporadycznie.

W kwestii recenzji dla czasopism zaskakują dwie rzeczy: pozytywnie – tytuły czasopism - i negatywnie – niska ich liczba, oszacowana na 40. Trudno uwierzyć, że wynika to z decyzji edytorów. Z drugiej strony, do tej kategorii zaliczę też gościnną edycję numeru czasopisma „Entropy".

Habilitant był kilka razy ważnym organizatorem różnorakich spotkań, choć za ważne imprezy możemy uznać za duże, a pełnił tam rolę członka komitetu programowego (na QIP w Barcelonie był w komitecie „Rump session", o nieco innym charakterze). Na wyróżnienie zasługuje fakt, że dwukrotnie zorganizował własne warsztaty. Szkoda, że z komitetów organizacyjnych dużych imprez w Gdańsku może się legitymować dotychczas jedynie warsztatami NATO z 2009 roku. Z drugiej strony, Uniwersytet Gdański nie co roku gości liczącą się konferencję. Zauważę też, że Habilitant był ważnym członkiem komitetu ds. wniosku o powołanie Międzynarodowej Agendy Badawczej, która wkrótce ruszy w Gdańsku, jest także członkiem rady naukowej Krajowego Centrum Informacji Kwantowej. Ogólnie, jest to kolejna imponująca pozycja na liście.

Ostatnie kilka punktów recenzji wskazuje miejscami na dosyć luźne relacje dr Pawłowskiego z formalnym światem akademickim. Uważam, że jest to pewna szkoda, Habilitant ma potencjał, by być magnesem dla młodych talentów.

Na zakończenie przeglądu osiągnięć wspomnę, że ma on na koncie bardzo imponujący spis aktywności konferencyjnej, wiele wykładów zaproszonych i zgłoszonych. Może się poszczycić czterema nagrodami, w tym indywidualną nagrodą Rektora UG II st. Recenzował również doktorat bardzo zdolnego naukowca (poza granicami kraju).

Konkludując, z przedstawionych dokumentów dr Pawłowski jest w ścisłej światowej czołówce w swojej dziedzinie. Tak obszerny dorobek spełnia wszystkie ustawowe i zwyczajowe wymagania i byłby w zasadzie gotowy do bardzo pewnego wniosku o tytuł profesora. W przedstawionej dokumentacji starałem się wypunktować jego słabsze strony, w przeciwnym razie recenzja byłaby niezwykle lakoniczna. Największym problemem jest tu jakość przygotowanej dokumentacji. W mojej ocenie jednak, żadna z tych wad nie ma mocy wzruszenia niezwykle pozytywnej opinii. Z przyjemnością rekomenduję nadanie dr. Pawłowskiego stopnia doktora habilitowanego. Uważam za miły obowiązek recenzenta takiej habilitacji wniosek o wyróżnienie.

Dr hab. Marcin Wieśniak, prof. UG.