Streszczenie rozprawy doktorskiej

mgr Jacek Aleksander Gruca

Dwupoziomowa optymalizacja związana z twierdzeniem Bella

Solving two-level optimization problems related to Bell's theorem

Instytut Informatyki Teoretycznej i Stosowanej
Polska Akademia Nauk

Instytut Fizyki Teoretycznej i Astrofizyki
Uniwersytet Gdański

Gliwice 2019

1 Wprowadzenie

Rozprawa doktorska składa się z cyklu czterech publikacji naukowych:

1. Jacek Gruca, Wiesław Laskowski, Marek Żukowski, Nikolai Kiesel, Witlef Wieczorek, Christian Schmid, Harald Weinfurter. Nonclassicality thresholds for multiqubit states: Numerical analysis. *Phys. Rev. A*, 82:012118, lipiec 2010,

2. Jacek Gruca, Wiesław Laskowski, Marek Żukowski. Nonclassicality of pure two-qutrit entangled states. *Phys. Rev. A*, 85:022118, luty 2012,

3. Jacek Gondzio, Jacek A. Gruca, J.A. Julian Hall, Wiesław Laskowski, Marek Żukowski. Solving large-scale optimization problems related to Bell's theorem. *J. Comput. Appl. Math.*, 263(C):392–404, czerwiec 2014,

4. Anna de Rosier, Jacek Gruca, Fernando Parisio, Tamás Vértesi, Wiesław Laskowski. Multipartite nonlocality and random measurements. *Phys. Rev. A*, 96:012101, lipiec 2017.

Powyższe publikacje zawierają omówienie obliczeń i zastosowań dwóch miar nieklasyczności stanów splątanych: minimalnej widzialności krytycznej oraz prawdopodobieństwa łamania nierówności Bella. Celem prac jest zastosowanie nowoczesnych narzędzi informatycznych do rozwiązania problemów optymalizacyjnych w teorii informacji kwantowej.

To streszczenie zawiera ogólne wprowadzenie do struktury i tematyki pracy. Niniejsza sekcja, 1., "Wprowadzenie", nakreśla strukturę dokumentu, podaje główne wyniki zawarte w pracy doktorskiej i podaje tezę doktoratu. Sekcja 2., "Wstęp", wprowadza czytelnika w tematykę pracy i oznajmia sposób dociekania zawartych w niej wyników. Ostatnia sekcja 3., "Podsumowanie", zawiera wnioski i kończy streszczenie.

Po streszczeniach w językach angielskim i polskim, w rozprawie znajduje się część IV, "Publication series", która zawiera publikacje stanowiące pracę doktorską.

Główna teza pracy brzmi: "zastosowanie narzędzi optymalizacyjnych dostarczonych przez współczesną informatykę pomaga badać i oceniać stany splątane oraz nakreślić granicę pomiędzy tym, co klasyczne i tym, co kwantowe".

Główne wyniki tej pracy to:

1. Zbiór wyników numerycznych dotyczących minimalnej widzialności krytycznej jako miary nieklasyczności, dla układów wielu kubitów.

2. Numeryczna analiza stanów dwóch kutritów, parametryzowanych dekompozycją Schmidta, w kontekście nieklasyczności.

3. Prezentacja sformułowania eksperymentu Bella jako eksperymentu myślowego w ogólnej postaci uwzględniającej dowolną liczbę obserwatorów, ustawień pomiarowych, dowolny wymiar przestrzeni

Hilberta i innych parametrów, skierowana do czytelników niezaznajomionych z tematyką kwantowej informacji.

4. Analiza i porównanie dwóch silników obliczeniowych programowania liniowego, metody sympleksowej i metody punktu wewnętrznego HOPDM [5], zastosowanych do obliczeń widzialności krytycznej, wraz ze statystyką czasu wykonania.

5. Wprowadzenie pojęcia prawdopodobieństwa łamania i zbiór wyników numerycznych związanych z nim.

6. Oprogramowanie STEAM-ROLLER2 napisane i użyte w celu uzyskania powyższych wyników poprzez numeryczne badanie stanów splątanych [6].

Słowa kluczowe: *optymalizacja, programowanie liniowe (LP), metoda sympleksowa, metoda Neldera-Meada, algorytmy, Ruby, C++, twierdzenie Bella, paradoks EPR, nierówności Bella, teoria informacji kwantowej, informatyka kwantowa, stan kwantowy, kubit, inżynieria splątania.*

2 Wstęp

Teoria informacji kwantowej, dyscyplina popularnie znana jako informatyka kwantowa, dostarcza liczne protokoły i sposoby przetwarzania informacji kwantowej. Część z nich wskazuje na obiecujące zastosowania, np. w kryptografii kwantowej [7], złożoności komunikacyjnej [8] albo dzieleniu się sekretem [9]. Istotnie, kryptografia kwantowa doczekała się zastosowań komercyjnych [10].

Każdy kto rozpoczyna studiowanie tych zastosowań, szybko odkrywa, że sedno ich użyteczności tkwi w różnicach, które dzielą je od klasycznej informatyki. Teoria informacji kwantowej wprowadza całkowicie odmienne podejście do przetwarzania informacji. Klasyczną informatykę rozumiemy więc jako informatykę implementowaną bez przetwarzania informacji kwantowej. Potrzebna jest zatem analiza nieklasyczności w teorii informacji kwantowej. Każde jej zastosowanie wymaga cząstek w stanie splątanym [11], udostępniającym opis przetwarzania układu fizycznego. Proces przygotowania cząstek tak, by spełnić własności splątania, nazywa się inżynierią stanu lub inżynierią splątania [12].

Biorąc powyższe pod uwagę, możemy zapytać: skąd wiemy, który stan z większym prawdopodobieństwem wykaże interesujące cechy stosowalne w informacji kwantowej? Wspomnieliśmy już, że sedno użyteczności zastosowań informacji kwantowej leży w tym, jak różne są one od informatyki klasycznej. Stwierdzamy dalej, że te cechy mogą dotyczyć tylko stanów silnie splątanych i nieklasycznych. Pozostała część rozprawy skupia się na nieklasyczności, przyjmując trzy punkty widzenia na nią.

Po pierwsze, wprowadzamy miarę nieklasyczności, zwaną minimalną widzialnością krytyczną, która może zostać obliczona numerycznie. Obliczenia tej miary, pierwszy raz opisane w [13], dały grunt każdej z publikacji naukowych stanowiących rozprawę.

Po drugie, stwierdzamy, że minimalna widzialność krytyczna jest nie tylko miarą nieklasyczności. Jest ona również bezpośrednim wskaźnikiem praktyczności zastosowań danego stanu, ponieważ mierzy także odporność na szum. Zobaczymy też, że dla danego stanu, im bardziej jest on nieklasyczny, tym trudniej jest zredukować jego nieklasyczne własności poprzez zaszumienie.

Po trzecie, wprowadzamy jeszcze jedną miarę nieklasyczności, prawdopodobieństwo łamania, która jest oparta na widzialności krytycznej i wprowadza dodatkowy wgląd w nieklasyczną naturę stanów splątanych.

Na koniec stwierdzamy, że powyższe miary nieklasyczności są bezpośrednio związane ze splątaniem kwantowym i, w konsekwencji, dotykają one fundamentów mechaniki kwantowej.

Rozprawa jest pracą interdyscyplinarną obejmującą zagadnienia w dziedzinach informatyki i fizyki. Czytelnik ma okazję się przekonać, że relacja pomiędzy informatyką i fizyką jest silnie zarysowana: informatyka rozwiązuje problemy powstające w fizyce, która z kolei dostarcza zastosowań w informatyce.

3 Podsumowanie

Jak pokazano w publikacjach stanowiących rozprawę [1, 2, 3, 4], wiele osiągnięto w zakresie szacowania stanów splątanych oraz ich stosowalności w teorii informacji kwantowej. Istotnie, ta stosowalność jest ściśle związana z granicą pomiędzy klasycznym i kwantowym opisem układów fizycznych, wyrażoną zdecydowanie przez minimalną widzialność krytyczną z jednej strony, a prawdopodobieństwo łamania z drugiej.

Minimalna widzialność krytyczna i prawdopodobieństwo łamania to miary nieklasyczności. Celem tej pierwszej jest znalezienie optymalnych ustawień pomiarowych — operatorów pomiaru, które odpowiadają najbardziej nieklasycznemu zachowaniu danego stanu. Ta druga, zamiast skupiać się na optymalnych operatorach pomiarowych, losuje te operatory, na podstawie konkretnej parametryzacji, i oblicza statystykę łamania w tym losowym procesie. Oba te kryteria to cechy danego stanu. Oba korzystają ze złożonego procesu obliczeń numerycznych, który wymaga zastosowania tego co najlepsze w nowoczesnej informatyce celem wyznaczenia odpowiednich wartości. Do obliczenia ich stosujemy wyrafinowany algorytm, który obejmuje metodę sympleksową i metodę punktu wewnętrznego na potrzeby programowania liniowego, losowe próbkowanie na potrzeby prawdopodobieństwa łamania oraz nieliniową optymalizację na potrzebny minimalizacji widzialności krytycznej.

Informatyka nie tylko dostarczyła narzędzia optymalizacyjne użyte i opisane w rozprawie: metody programowania liniowego i optymalizator nieliniowy. Umożliwiła ona również zbudowanie wyrafinowanego algorytmu spinającego wszystkie metody razem w sposób, który efektywnie rozwiązuje problemy w fizyce. Dzięki uzyskanej w ten sposób informacji możliwe jest stworzenie zastosowań w innych dziedzinach, w szczególności właśnie w informatyce. Jednym z takich zastosowań jest protokół kryptograficzny Ekerta z 1991 roku [7]. Ten protokół bezpiecznego przesyłu informacji bezpośrednio stosuje stany zbudowane przy użyciu inżynierii stanu w eksperymencie Bella. Jego bezpieczeństwo i odporność są gwarantowane przez prawa fizyki kwantowej i zostały zademonstrowane eksperymentalnie

[14, 15]. A zatem minimalna widzialność krytyczna i prawdopodobieństwo łamania stanów splątanych mierzą bezpieczeństwo tego protokołu kryptograficznego, prawdopodobnie jego najważniejszą cechę.

Wyniki numeryczne wyprodukowane w sposób opisany w rozprawie stają się uznanym podejściem do obliczeń w nieklasyczności, co pokazują cytowania publikacji stanowiących rozprawę. Metody opisane w nich stworzyły nowe możliwości, zarówno w teorii informacji kwantowej, jak w obliczeniach numerycznych, co było tematem moich badań aż do dziś.

Literatura

[1] Jacek Gruca, Wiesław Laskowski, Marek Żukowski, Nikolai Kiesel, Witlef Wieczorek, Christian Schmid, Harald Weinfurter. Nonclassicality thresholds for multiqubit states: Numerical analysis. *Phys. Rev. A*, 82:012118, lipiec 2010.

[2] Jacek Gruca, Wiesław Laskowski, Marek Żukowski. Nonclassicality of pure two-qutrit entangled states. *Phys. Rev. A*, 85:022118, luty 2012.

[3] Jacek Gondzio, Jacek A. Gruca, J.A. Julian Hall, Wiesław Laskowski, Marek Żukowski. Solving large-scale optimization problems related to Bell's theorem. *J. Comput. Appl. Math.*, 263(C):392–404, czerwiec 2014.

[4] Anna de Rosier, Jacek Gruca, Fernando Parisio, Tamás Vértesi, Wiesław Laskowski. Multipartite nonlocality and random measurements. *Phys. Rev. A*, 96:012101, lipiec 2017.

[5] Jacek Gondzio, Anna Altman. HOPDM — a higher order primal-dual method for large scale linear programming. *European Journal of Operational Research*, 66:158–160, kwiecień 1993.

[6] Jacek Aleksander Gruca. STEAM-ROLLER2. http://gruca.org/steam-roller2/steam-roller2.zip, 2019. Otwarto: 2019-03-04.

[7] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, sierpień 1991.

[8] Harry Buhrman, Richard Cleve, Wim van Dam. Quantum entanglement and communication complexity. *Phys. Rev. Lett.*, 67:661–663, sierpień 1991.

[9] Christian Schmid, Pavel Trojek, Mohamed Bourennane, Christian Kurtsiefer, Marek Żukowski, Harald Weinfurter. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.*, 95:230505, grudzień 2005.

[10] Quantum Cryptography and Quantum Encryption Companies. https://www.nanalyze.com/2016/09/5-quantum-cryptography-encryption-companies/, 2016.

[11] A. Einstein, B. Podolsky, N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, maj 1935.

[12] K. M. Gheri, C. Saavedra, P. Törmä, J. I. Cirac, P. Zoller. Entanglement engineering of one-photon wave packets using a single-atom source. *Phys. Rev. A*, 58:R2627–R2630, październik 1998.

[13] Dagomir Kaszlikowski, Piotr Gnaciński, Marek Żukowski, Wieslaw Miklaszewski, Anton Zeilinger. Violations of local realism by two entangled N-dimensional systems are stronger than for two qubits. *Phys. Rev. Lett.*, 85:4418–4421, listopad 2000.

[14] Mikio Fujiwara, Ken ichiro Yoshino, Yoshihiro Nambu, Taro Yamashita, Shigehito Miki, Hirotaka Terai, Zhen Wang, Morio Toyoshima, Akihisa Tomita, Masahide Sasaki. Modified E91 protocol demonstration with hybrid entanglement photon source. *Opt. Express*, 22(11):13616–13624, czerwiec 2014.

[15] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, P. G. Kwiat. Entangled state quantum cryptography: Eavesdropping on the Ekert protocol. *Phys. Rev. Lett.*, 84:4733–4736, maj 2000.