Remigiusz Augusiak Załącznik nr 2 (autoreferat po polsku)

AUTOREFERAT

I. IMIONA I NAZWISKO

Remigiusz Michał Augusiak

II. POSIADANE DYPLOMY I STOPNIE NAUKOWE

- **Czerwiec 2008, Doktor nauk fizycznych w zakresie fizyki,**
  Wydział Fizyki Technicznej i Matematyki Stosowanej, Politechnika Gdańska,
  rozprawa: *On the distillation of cryptographic key from multipartite entangled quantum states,*
  promotor: prof. dr hab. P. Horodecki

- **Wrzesień 2012, Magister inżynier matematyki,**
  Wydział Fizyki Technicznej i Matematyki Stosowanej, Politechnika Gdańska,
  praca magisterska: *Wielokopiowe kryteria separowalności dla dwupodukładowych stanów kwantowych*
  promotor: dr M. Kuna

- **Czerwiec 2003, Magister inżynier fizyki technicznej,**
  Wydział Fizyki Technicznej i Matematyki Stosowanej, Politechnika Gdańska,
  praca magisterska: *Rozpraszanie elektronów na nielokalnych potencjałach separowalnych*
  promotor: prof. dr hab. R. Szmytkowski

III. INFORMACJE O DOTYCHCZASOWYM ZATRUDNIENIU W JEDNOSTKACH NAUKOWYCH

- **Od stycznia 2016, Adiunkt**
  Centrum Fizyki Teoretycznej Polskiej Akademii Nauk, Warszawa, Polska

- **Czerwiec 2008–Grudzień 2015, Staż podoktorski**
  Institut de Ciències Fotòniques (ICFO), Barcelona, Hiszpania

- **Luty 2005–Czerwiec 2005, Październik 2005–Lipiec 2006, Październik 2007–Luty 2008, Asystent naukowo-dydaktyczny**
  Politechnika Gdańska, Gdańsk, Polska

- **Październik 2003–Czerwiec 2008, Doktorant**
  Politechnika Gdańska, Gdańsk, Polska

RA

IV. WSKAZANIE OSIĄGNIĘCIA* WYNIKAJĄCEGO Z ART. 16 UST. 2 USTAWY Z DNIA 14 MARCA 2003 R. O STOPNIACH NAUKOWYCH I TYTULE NAUKOWYM ORAZ O STOPNIACH I TYTULE W ZAKRESIE SZTUKI (Dz. U. 2016 r. poz. 882 ze zm. w Dz. U. z 2016 r. poz. 1311.):

A. TYTUŁ OSIĄGNIĘCIA NAUKOWEGO

Cykl publikacji pt. *Nielokalność w złożonych układach fizycznych: wybrane zagadnienia*

B. LISTA PUBLIKACJI WCHODZĄCYCH W SKŁAD OSIĄGNIĘCIA (kolejność chronologiczna)

[H1] A. Acín, R. Augusiak, D. Cavalcanti, C. Hadley, J. K. Korbicz, M. Lewenstein, Ll. Masanes, M. Piani, *Unified framework for correlations in terms of local quantum observables*, Physical Review Letters **104**, 140404 (2010).

[H2] R. Augusiak, D. Cavalcanti, G. Prettico, and A. Acín, *Perfect Quantum Privacy Implies Nonlocality*, Physical Review Letters **104**, 230401 (2010).

[H3] R. Augusiak, J. Stasińska, C. Hadley, J. K. Korbicz, M. Lewenstein, A. Acín *Bell inequalities with no quantum violation and unextendible product bases*, Physical Review Letters **107**, 070401 (2011).

[H4] R. Augusiak, T. Fritz, Ma. Kotowski, Mi. Kotowski, M. Pawłowski, M. Lewenstein, A. Acín, *Tight Bell inequalities with no quantum violation from qubit unextendible product bases*, Physical Review A **85**, 042113 (2012).

[H5] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, and A. Acín, *Detecting nonlocality in many-body quantum states*, Science **344**, 1256–1258 (2014).

[H6] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, A. Acín, *Elemental and tight monogamy relations in nonsignalling theories*, Physical Review A **90**, 052323 (2014).

[H7] R. Augusiak, M. Demianowicz, A. Acín, *Local hidden–variable models for entangled quantum states*, Journal of Physics A: Mathematical and Theoretical **42**, 424002 (2014).

[H8] J. Tura, A. B. Sainz, T. Vértesi, A. Acín, M. Lewenstein, R. Augusiak, *Translationally invariant multipartite Bell inequalities involving only two-body correlators*, Journal of Physics A: Mathematical and Theoretical **42**, 424024 (2014).

[H9] R. Augusiak, M. Demianowicz, J. Tura, A. Acín, *Entanglement and Nonlocality are Inequivalent for Any Number of Parties*, Physical Review Letters **115**, 030404 (2015).

[H10] R. Augusiak, *Simple and tight monogamy relations for a class of Bell inequalities*, Physical Review A **95**, 012223 (2017) (wraz z erratą Phys. Rev. A **96**, 049901(E) (2017)).

RA

C. OMÓWENIE CELU NAUKOWEGO WW. PRAC I OSIĄGNIĘTYCH WYNIKÓW WRAZ Z OMÓWIENIEM ICH EWENTUALNEGO WYKORZYSTANIA.

Struktura tej części autoreferatu jest następująca. W części IV.1 znajduje się krótkie wprowadzenie w tematykę, następnie w częściach IV.2-IV.6 omówione są wyniki prac [H1-H10]. Ostatnia część IV.7 zawiera przykładowe problemy, którymi mam zamiar zajmować się w najbliższej przyszłości.

IV.1 Wstęp i preliminaria

W teorii kwantowej lokalne pomiary na złożonych układach fizycznych mogą prowadzić do ciekawych korelacji, które nie mogą być wytłumaczone w ramach fizyki klasycznej. Takie korelacje są zazwyczaj nazywane nielokalnymi, podczas gdy ich istnienie w złożonych układach fizycznych nielokalnością (zob. [1]). W ostatnich latach stało się jasne, że nielokalność jest interesująca nie tylko z poznawczego punktu widzenia, ale też dlatego, że jest ona kluczowym zasobem dla pewnych zastosowań. W istocie leży ona u podstaw poddziedziny kwantowej informatyki jaką jest przetwarzanie informacji niezależne od urządzeń (*device-independent quantum information processing*). Jej celem jest opracowywanie protokołów wykorzystujących korelacje nielokalne i nie wymagających czynienia żadnych założeń o urządzeniach użytych do ich wykonania. Przykładami takich protokołów są kwantowa dystrybucja klucza [2, 3], wykrywanie splątania niezależne od urządzeń (*device-independent entanglement detection*) [4] lub wytwarzanie i wzmacnianie prawdziwej losowości [5, 6].

W tym kontekście nie ulega wątpliwości, że charakteryzacja i detekcja nielokalności w złożonych układach fizycznych należy do głównych problemów kwantowej teorii informacji. Przedstawiony poniżej cykl prac [H1–H10] jest owocem moich wieloletnich badań, których celem była charakteryzacja nielokalności, a przynajmniej przestudiowanie pewnych zagadnień dotyczących tego pojęcia. W skrócie, w [H1] udowodniliśmy, że wszystkie korelacje spełniające zasadę niesygnalizowania mogą być w ujednolicony sposób reprezentowane poprzez tzw. regułę Borna oraz udowodniliśmy, że wyniki pracy [7] nie uogólniają się na przypadek wielu obserwatorów. W pracach [H2,H7,H9] badaliśmy relacje między nielokalnością a innymi zasobami informatyki kwantowej: bezpiecznymi korelacjami i splątaniem. W pracach [H3,H4] wprowadziliśmy, korzystając z wyników pracy [H1], ogólną konstrukcję gier dla wielu obserwatorów, w wygraniu których mechanika kwantowa nie daje żadnej przewagi nad korelacjami klasycznymi, w przeciwieństwie do pozakwantowych korelacji niesygnalizujących, które taką przewagę dają. Prace [H6,H10] wprowadzają pewne relacje monogamii nowego typu dla ogólnych korelacji spełniających zasadę niesygnalizowania. Wreszcie w pracach [H5,H8] pokazaliśmy, że możliwa jest detekcja nielokalności w układach wielu ciał jedynie przez pomiar dwuciałowych korelacji.

Przed przejściem do bardziej szczegółowego opisu powyższych prac, postaram się przybliżyć pewne pojęcia, a także wprowadzić notację, które będą stosowane w późniejszych rozważaniach.

RA

Scenariusz Bella. Rozważmy scenariusz, w którym pewien N-cząstkowy stan kwantowy ρ_N działający na iloczynowej przestrzeni Hilberta

$$\mathcal{H}_N = \mathbb{C}^{d_1} \otimes \ldots \otimes \mathbb{C}^{d_N}, \tag{1}$$

przy czym $d_i < \infty$ dla każdego i, jest rozdystrybuowany pomiędzy N odseparowanych obserwatorów $A_1, \ldots, A_N$. Przykładem takiego układu może być stan opisujący N cząstek o spinie 1/2 (kubitów), przy czym i-ta cząstka znajduje się w laboratorium obserwatora A_i. Załóżmy, że każdy obserwator na swoim podukładzie ρ_N wykonuje jeden z m pomiarów $M_{x_i}^{(i)}$, gdzie $x_i = 1, \ldots, m$ dla każdego i. Załóżmy ponadto, że każdy pomiar ma d wyników, zwyczajowo oznaczanych przez $0, \ldots, d-1$. Przypomnijmy, że pomiar $M_{x_i}^{(i)}$ jest rozumiany jako zbiór $M_{x_i}^{(i)} = \{M_{x_i}^{a_i}\}$ operatorów dodatnich $M_{x_i}^{a_i} \geq 0$, takich że $\sum_{a_i} M_{x_i}^{a_i} = \mathbb{1}_i$ dla każdego x_i i i, gdzie $\mathbb{1}_i$ oznacza macierz identycznościową działającą na przestrzeni Hilberta $\mathbb{C}^{d_i}$. Przypomnijmy także, że jeżeli dodatkowo operatory pomiaru $M_{x_i}^{a_i}$ spełniają $M_{x_i}^{a_i} M_{x_i}^{a_i'} = M_{x_i}^{a_i} \delta_{a_i a_i'}$, gdzie $\delta_{i,j}$ to delta Kroneckera, to pomiar taki nazywamy rzutowym.

Takie pomiary lokalne na stanie ρ_N, po wielu powtórzeniach, prowadzą do korelacji, które są opisywane przez zbiór rozkładów prawdopodobieństw

$$\{p(a_1, \ldots, a_N | x_1, \ldots, x_N)\}_{a_1, \ldots, a_N; x_1, \ldots, x_N}, \tag{2}$$

gdzie $p(\boldsymbol{a}|\boldsymbol{x}) := p(a_1, \ldots, a_N | x_1, \ldots, x_N)$ to prawdopodobieństwo, że obserwatorzy otrzymują wyniki $\boldsymbol{a} := a_1, \ldots, a_N$ po wykonaniu pomiarów $\boldsymbol{x} := x_1, \ldots, x_N$ i wyraża się ono przez regułę Borna:

$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) = \operatorname{Tr}\left[\rho_N \left(M_{x_1}^{a_1} \otimes \ldots \otimes M_{x_N}^{a_N}\right)\right]. \tag{3}$$

Dla prostoty, świadomie nadużywając terminologii, zbiór (2) będziemy także nazywać korelacjami, natomiast powyższy scenariusz jest zazwyczaj nazywany scenariuszem Bella lub po prostu scenariuszem (N, m, d). Zauważmy także, że dla ustalonych N, m i d korelacje otrzymane przez lokalne pomiary na stanach kwantowych tworzą zbiór wypukły $\mathbb{Q}_{N,m,d}$ w rzeczywistej przestrzeni liniowej $\mathbb{R}^D$ o wymiarze $D = [m(d-1)+1]^N - 1$[1].

W przypadku dwu lub trzypodukładowym obserwatorów będziemy oznaczać także literkami A, B i C oraz, analogicznie, wykonywane przez nich pomiary i otrzymane wyniki będziemy indeksować za pomocą, odpowiednio, x, y, z oraz a, b i c. Ponadto w przypadku, gdy $d = 2$, korelacje powstające w eksperymencie Bella można równoważnie opisywać przez zbiór wszystkich wartości średnich postaci

$$\langle M_{x_{i_1}}^{(i_1)} \ldots M_{x_{i_k}}^{(i_k)} \rangle = \operatorname{Tr}\left[\rho_{i_1 \ldots i_k} \left(M_{x_{i_1}}^{(i_1)} \otimes \ldots \otimes M_{x_{i_k}}^{(i_k)}\right)\right], \tag{4}$$

dla $k = 1, \ldots, N$ oraz $i_1 < i_2 < \ldots < i_k = 1, \ldots, N$ (wszystkie możliwe wartości oczekiwane, od jednociałowych do N-ciałowych, są brane pod uwagę). Tutaj $M_{x_i}^{(i)}$ są obserwablami o wartościach własnych ± 1, natomiast $\rho_{i_1 \ldots i_k}$ to stan kwantowy współdzielony przez obserwatorów $A_{i_1}, \ldots, A_{i_k}$, to znaczy powstający z ρ_N przez wyśladowanie wszystkich podukładów poza $A_{i_1}, \ldots, A_{i_k}$. Ten opis będzie używany w części IV.6.

[1] Prawdopodobieństw w zbiorze (2) jest $(dm)^N$, ale ze względu na warunki niesygnalizowania oraz normalizację, są one liniowo zależne. Pominięcie zbędnych prawdopodobieństw daje wymiar $[m(d-1)+1]^N - 1$.

RA

Modele ukrytych zmiennych i nierówności Bella. Rozważmy teraz korelacje $\{p(a|x)\}$ otrzymane w scenariuszu (N, m, d), które przyjmują następującą postać

$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) = \sum_{\lambda \in \Omega} p(\lambda) p_{A_1}(a_1 | x_1, \lambda) \cdot \ldots \cdot p_{A_N}(a_N | x_N, \lambda), \tag{5}$$

gdzie $\lambda \in \Omega$ to pewne parametry, zwyczajowo zwane zmiennymi ukrytymi, $p(\lambda)$ to rozkład prawdopodobieństwa na zbiorze Ω, a $p_{A_i}(a_i|x_i, \lambda)$ są funkcjami deterministycznymi, które zależą jedynie od lokalnego wyboru pomiaru x_i, jego wyniku a_i oraz zmiennej λ i przyjmują wartości ze zbioru $\{0, 1\}$. Takie korelacje są zwane lokalnie realistycznymi (*local realistic*) lub, nadużywając nieco terminologii, po prostu lokalnymi. Zbiór Ω wraz z lokalnymi prawdopodobieństwami $p(a_i|x_i, \lambda)$ tworzą tzw. model zmiennych ukrytych (*local-hidden variable (LHV) model*) zwany, po prostu, modelem lokalnym. Zauważmy, że w danym scenariuszu (N, m, d) korelacje postaci (5) tworzą wielościan[2] zwany wielościanem lokalnym lub wielościanem Bella, którego wierzchołkami są deterministyczne korelacje lokalne, dla których $p(a|x) = p_{A_1}(a_1|x_1) \cdot \ldots \cdot p_{A_N}(a_N|x_N)$, przy czym $p_{A_i}(a_i|x_i) \in \{0, 1\}$ dla każdego x_i oraz i. Obiekt ten będziemy oznaczać przez $\mathbb{P}_{N,m,d}$. Ponadto jeżeli wszystkie korelacje otrzymane ze stanu kwantowego ρ_N w dowolnym scenariuszu (N, m, d) można dają się zapisać w postaci (5), wtedy stan ρ_N także nazywamy lokalnym.

Postać (5) została wprowadzona przez Bella [8][3], aby sformalizować możliwość opisu korelacji kwantowych za pomocą ukrytych zmiennych. Te ostatnie zostały z kolei zaproponowane przez Einsteina, Podolsky'ego i Rosena [9] w celu uczynienia mechaniki kwantowej teorią kompletną. Ponadto, w pracy [8] Bell udowodnił, że w teorii kwantów istnieją korelacje, które nie mogą być wytłumaczone za pomocą modeli LHV (5). Skonstruował w tym celu liniową nierówność ograniczającą zbiór korelacji lokalnych i pokazał, że pewne korelacje kwantowe ją łamią. Nierówności tego typu, o ogólnej postaci

$$I := \sum_{a,x} T_{a,x} p(a|x) \leq \beta_C, \tag{6}$$

gdzie $T_{a,x}$ to macierz współczynników, nazywamy nierównościami Bella. W powyższym wzorze β_C to tak zwane ograniczenie klasyczne, czyli maksymalna wartość lewej strony nierówności dla wszystkich korelacji przyjmujących postać (5); w istocie aby wyznaczyć β_C wystarczy znaleźć wartość maksymalną I po wszystkich wierzchołkach wielościanu Bella. Wyrażenie I w (6) będziemy nazywać wyrażeniem Bella. Korelacje, które łamią nierówności Bella (oraz stan kwantowy, z którego je otrzymano), a więc nie mogą być zapisane w postaci (5), nazywamy nielokalnymi, natomiast fakt ich istnienia w złożonych układach kwantowych nielokalnością. Z drugiej strony, dla dowolnych korelacji nielokalnych można stworzyć nierówność Bella, która będzie przez nie złamana; zatem korelacje $\{p(a|x)\}$ są nielokalne wtedy i tylko wtedy, gdy nie spełniają jakiejś nierówności Bella.

Z operacyjnego punktu widzenia równanie (5) opisuje korelacje, które mogą być wytworzone przez obserwatorów w pełni klasyczny sposób, to znaczy bez użycia kwan-

---

[2]Właściwszym byłoby użycie pojęcia wielokomórki, czyli uogólnienia pojęcia wielościanu na przypadek przestrzeni liniowych o wymiarze większym niż trzy. Jednak w literaturze polskiej dotyczącej zbiorów wypukłych [10] używa się także nazwy wielościan, więc, dla prostoty, pozostajemy przy tym określeniu.

[3]Mówiąc dokładniej, postać (5) jest bezpośrednim uogólnienem formuły wprowadzonej w [8] dla $N = 2$ na przypadek dowolnej liczby obserwatorów.

RA

towych zasobów. Jedynym zasobem jaki obserwatorzy współdzielą, jest klasyczna informacja reprezentowana przez zmienną λ, która może być rozumiana jako lista instrukcji uzgodniona przez obserwatorów $A_1, \ldots, A_N$ przed rozpoczęciem eksperymentu. Ponadto $p(a_i|x_i, \lambda)$ to deterministyczne strategie, numerowane przez λ, jakich obserwatorzy używają, aby wygenerować zadane korelacje: po otrzymaniu x_i obserwator A_i sprawdza na liście, której strategii ma użyć i zgodnie z jej specyfikacją zwraca wynik a_i. Z tego powodu korelacje (5) zwane są także klasycznymi.

Zauważmy wreszcie, że skoro w danym scenariuszu (N, m, d) zbiór $\mathbb{P}_{N,m,d}$ jest wielościanem, to aby go w pełni scharakteryzować potrzebna jest skończona liczba nierówności Bella odpowiadających ścianom tego wielościanu; takie nierówności Bella nazywamy optymalnymi (*tight*). Zatem, znając wszystkie ściany $\mathbb{P}_{N,m,d}$ bylibyśmy w stanie jednoznacznie stwierdzić, czy dane korelacje $\{p(\boldsymbol{a}|\boldsymbol{x})\}$ są nielokalne, czy nie. Do wyznaczenia wszystkich optymalnych nierówności Bella używa się algorytmów komputerowych takich jak CDD [11], które mając dane wierzchołki wielościanu $\mathbb{P}_{N,m,d}$ (deterministyczne korelacje klasyczne), znajdują jego ściany. Niestety, problem ten może być rozwiązany tylko w najprostszych scenariuszach Bella; wraz ze wzrostem jednego z parametrów N, m lub d wyznaczenie ścian $\mathbb{P}_{N,m,d}$ staje się zbyt trudne z obliczeniowego punktu widzenia.

Korelacje niesygnalizujące. Przypomnijmy jeszcze definicje korelacji niesygnalizujących, to znaczy korelacji, które spełniają zasadę niesygnalizowania. Mówi ona, że informacja nie może się rozchodzić szybciej niż prędkość światła, co na poziomie eksperymentu Bella opisanego powyżej oznacza, że pomiary wykonane przez dowolny podzbiór obserwatorów nie mogą wpływać na statystyki wyników widziane przez pozostałych obserwatorów. Równoważnie, prawdopodobieństwa warunkowe $p(\boldsymbol{a}|\boldsymbol{x})$ spełniają następujące warunki liniowe:

$$\sum_{a_i} p(a_1, \ldots, a_i, \ldots, a_N | x_1, \ldots, x_i, \ldots, x_N) = \sum_{a_i} p(a_1, \ldots, a_i, \ldots, a_N | x_1, \ldots, x_i', \ldots, x_N) \quad (7)$$

dla dowolnych $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_N$, $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_N$, $x_i \neq x_i'$ oraz i. Zauważmy, że zbiór korelacji niesygnalizujących, podobnie jak zbiór korelacji klasycznych, jest wielościanem, który będziemy oznaczać przez $\mathbb{N}_{N,m,d}$. Co ciekawe, jak pokazano w [12], jest on jednak ściśle większy niż zbiór korelacji kwantowych lub, inaczej mówiąc, istnieją niesygnalizujące korelacje, które nie mają kwantowego opisu w ramach reprezentacji (3). Zatem, w ogólności, $\mathbb{P}_{N,m,d} \subsetneq \mathbb{Q}_{N,m,d} \subsetneq \mathbb{N}_{N,m,d}$ [8, 12].

Możemy teraz przejść do bardziej szczegółowego opisu prac [H1-H10].

IV.2 Zasady teorio-informacyjne dla korelacji kwantowych

Jak już wspomniano, zasada niesygnalizowania, która mówi, że informacja nie może być przesłana z dowolną prędkością, definiuje zbiór korelacji, który jest ściśle większy od zbioru korelacji kwantowych. Co więcej, istnienie takich korelacji, które nie mają kwantowej realizacji, miałoby istotne znaczenie dla przetwarzania informacji. Przykładowo pozakwantowe korelacje niesygnalizujące trywializowałyby pewne problemy w dziedzinie złożoności komunikacyjnej [13]: każdy taki problem mógłby zostać rozwiązany przy użyciu jednego bitu komunikacji klasycznej, niezależnie od jego złożoności. Zatem zrozumienie dlaczego Natura

RA

nie może być bardziej nielokalna niż pozwala na to mechanika kwantowa stało się jednym z kluczowych problemów kwantowej teorii informacji, motywując poszukiwanie zasad o informacyjnej naturze, które pozwoliłyby wyróżnić zbiór korelacji kwantowych ze wszystkich korelacji niesygnalizujących. To doprowadziło do sformułowania kilku zasad takich jak przyczynowość informacyjna [14], rzeczywistość makroskopowa [15], brak kwantowej przewagi w nielokalnych obliczeniach [16] oraz lokalna ortogonalność [C11,C12].

Alternatywne podejście do badania zbioru korelacji kwantowych zostało zaprezentowane w pracy [7], w której pokazano, że przy założeniu, że lokalnie mechanika kwantowa jest spełniona (poniżej będziemy je nazywać założeniem LQT od angielskiego *local quantum theory*), w przypadku dwóch obserwatorów zasada niesygnalizowania jest wystarczająca, aby w pełni opisać zbiór korelacji kwantowych. Założenie LQT oznacza, że każdy obserwator ma przypisaną przestrzeń Hilberta o ustalonym wymiarze oraz, że może on wykonać na swoim podukładzie dowolny pomiar kwantowy, przy czym, przypomnijmy, pomiary reprezentowane są przez zbiory operatorów dodatnich, których suma to operator identycznościowy działający na danej przestrzeni Hilberta. W pracy [H1] pokazujemy, że ten prosty opis zbioru kwantowego nie przenosi się na przypadek wielocząstkowy. Aby zaprezentować ten wynik zacznijmy od ujednoliconego opisu korelacji niesygnalizujących.

Zunifikowany opis korelacji. W [H1] dowodzimy, że dowolne korelacje niesygnalizujące (nie tylko kwantowe) można reprezentować za pomocą reguły Borna (3). Mając dane korelacje $\{p(a_1,\ldots,a_N|x_1,\ldots,x_N)\}$, które spełniają warunki (7), pokazujemy, że

$$p(a_1,\ldots,a_N|x_1,\ldots,x_N) = \mathrm{Tr}\left[O\left(M_{x_1}^{a_1}\otimes\ldots\otimes M_{x_N}^{a_N}\right)\right], \tag{8}$$

gdzie $M_{x_i}^{a_i}$ to operatory pomiaru dla obserwatora A_i, a O to pewien operator hermitowski o śladzie jednostkowym, $\mathrm{Tr}(O) = 1$. Należy zauważyć, że w ogólności dany operator hermitowski, ale nie dodatni O, odpowiadający pewnym korelacjom niesygnalizującym, nie będzie prowadził, poprzez formułę (8), do poprawnych rozkładów prawdopodobieństwa dla wszystkich operatorów pomiaru.

Aby zilustrować powyższą reprezentację rozważmy najprostszy scenariusz $(2,2,2)$ i dwuciałowe korelacje niesygnalizujące, zwyczajowo nazywane pudłem Popescu-Rohrlicha (*PR-box*) [12], zdefiniowane jako

$$p_{\mathrm{PR}}(a,b|x,y) = \begin{cases} \frac{1}{2}, & a+b = x\cdot y \bmod 2 \\ 0, & \text{w przeciwnym przypadku} \end{cases}. \tag{9}$$

W tym przypadku operator O w (8) jest postaci $O = \alpha_+\Phi_+ + \alpha_-\Phi_-$, gdzie $\alpha_\pm = (1\pm\sqrt{2})/2$ oraz $\Phi_\pm$ to projektory na $|\Phi_\pm\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$, podczas gdy lokalne obserwable mają postać σ_x, σ_y dla pierwszego obserwatora oraz $(\sigma_x \mp \sigma_y)/\sqrt{2}$ dla drugiego obserwatora. Nie trudno zauważyć, że O jest hermitowski, ale niedodatni.

Wszystkie trzy zbiory korelacji omówione w części IV.1: lokalne, kwantowe oraz niesygnalizujące mogą być zunifikowane w ramach jednego opisu przy użyciu lokalnych obserwabli kwantowych. Zmieniając własności operatora O otrzymujemy różne zbiory korelacji: (i) wszystkie korelacje niesygnalizujące (w tym te, które nie mają kwantowej realizacji) są reprezentowane przez operatory hermitowskie, (ii) dodatnie operatory O generują korelacje

RA

kwantowe, podczas gdy (iii) dodatnie i separowalne operatory O generują korelacje opisywane przez modele LHV.

Wielocząstkowe korelacje Gleasona. Mając powyższy formalizm możemy teraz rozważyć teorię spełniająca założenie LQT oraz zasadę niesygnalizowania. Korelacje w ramach takiej teorii mogą *a priori* tworzyć większy zbiór niż korelacje kwantowe, jako że nie czynimy żadnego założenia o globalnym stanie opisującym układ. W istocie, w tym przypadku operator O w (8) musi generować poprawne rozkłady prawdopodobieństwa dla wszystkich wyborów lokalnych pomiarów. Mówiąc równoważnie, wartości średnie operatora O na wszystkich iloczynach tensorowych operatorów dodatnich muszą być nieujemne, co oznacza, że operator O musi być wielocząstkowym świadkiem splątania [17]. Co interesujące, takie korelacje pojawiły się już w kilku pracach badających rozszerzenie znanego twierdzenia Gleasona [18] na lokalne obserwable w N-cząstkowych przestrzeniach Hilberta (zob. [19]); w [H1] nazwaliśmy je korelacjami Gleasona.

Zauważmy teraz, że w [7] udowodniono (w [H1] podajemy alternatywny dowód), że w przypadku dwucząstkowym zbiór korelacji Gleasona jest tożsamy ze zbiorem kwantowym, co oznacza, że w tym przypadku założenie LQT i zasada niesygnalizowania są wystarczające do pełnego opisu zbioru korelacji kwantowych. Głównym narzędziem wykorzystanym w dowodzie w pracy [7] jest izomorfizm Jamiołkowskiego pomiędzy świadkami splątania i odwzorowaniami dodatnimi sformułowany w przypadku dwuobserwatorowym w [20]. Ponieważ analogiczny izomorfizm dla świadków wielocząstkowych nie istnieje, można oczekiwać, że wynik pracy [7] nie uogólnia się na przypadek większej liczby cząstek. W [H1] pokazujemy, że w istocie tak się dzieje, to znaczy już w przypadku trzech obserwatorów równoważność pomiędzy korelacjami Gleasona i kwantowymi przestaje być prawdziwa, jako że istnieją korelacje Gleasona generowane przez wielocząstkowe świadki splątania, które nie mają kwantowej realizacji.

Dowód powyższego faktu wykorzystuje trzycząstkową nierówność Bella w scenariuszu $(3,2,2)$ znalezioną w [21]. Przedstawiamy ją tutaj w postaci zaproponowanej w [22]:

$$p(000|000) + p(101|011) + p(011|110) + p(110|101) \leq 1. \tag{10}$$

W [22] pokazano, że nierówność ta nie jest łamana przez mechanikę kwantową, to znaczy nie istnieje stan kwantowy ani lokalne pomiary, dla których wartość lewej strony nierówności (10) byłaby większa niż jeden; innymi słowy, jej maksymalna wartość kwantowa jest równa jej ograniczeniu klasycznemu $\beta_C = 1$. Rozważmy ponadto następujący zbiór wektorów iloczynowych z $(\mathbb{C}^2)^{\otimes 3}$,

$$|000\rangle, \quad |1e^{\perp}e\rangle, \quad |e1e^{\perp}\rangle, \quad |e^{\perp}e1\rangle \tag{11}$$

gdzie $\{|0\rangle, |1\rangle\}$ and $\{|e\rangle, |e^{\perp}\rangle\}$ to dwie różne bazy ortonormalne w $\mathbb{C}^2$. Zbiór ten tworzy obiekt zwany nierozszerzalną bazą iloczynową (*unextendible product basis (UPB)*), ponieważ nie istnieje żaden inny wektor iloczynowy w $(\mathbb{C}^2)^{\otimes 3}$, który byłby ortogonalny do każdego z nich (zob. [23]). Rozważmy następnie świadka splątania skonstruowanego z tego zbioru: $W = (\Pi_{\mathrm{UPB}} - \epsilon\mathbb{1})/(4 - 8\epsilon)$, gdzie $\mathbb{1}$ i Π_{UPB} to, odpowiednio, macierz identycznościowa działająca na $(\mathbb{C}^2)^{\otimes 3}$ i projektor na podprzestrzeń rozpiętą przez (11) oraz

$$\epsilon = \min_{|\psi_{\mathrm{prod}}\rangle} \langle\psi_{\mathrm{prod}}|\Pi_{\mathrm{UPB}}|\psi_{\mathrm{prod}}\rangle > 0, \tag{12}$$

RA

gdzie minimum jest brane po wszystkich wektorach iloczynowych z $(\mathbb{C}^2)^{\otimes 3}$. Powyższy świadek splątania wraz z lokalnymi pomiarami zdefiniowanymi w bazach $\{|0\rangle, |1\rangle\}$ i $\{|e\rangle, |e^{\perp}\rangle\}$, generuje korelacje niesygnalizujące, które łamią (10), co oznacza, że korelacje te nie mają kwantowej realizacji. Zatem korelacje Gleasona, czyli korelacje otrzymane ze świadków splątania tworzą zbiór, który jako podzbiór właściwy zawiera zbiór korelacji kwantowych. A więc w przeciwieństwie do przypadku dwucząstkowego, w przypadku wielocząstkowym założenie LQT i zasada niesygnalizowania są w ogólności niewystarczające do jednoznacznego wyróżnienia zbioru kwantowych korelacji ze zbioru wszystkich korelacji niesygnalizujących. Oczywiście ciekawym kierunkiem badań byłoby zrozumienie dlaczego tak się dzieje w przypadku wielu obserwatorów i o jaki dodatkowy warunek należałoby uzupełnić założenie LQT i zasadę niesygnalizowania, aby wyrugować pozakwantowe korelacje Gleasona.

IV.3 Zadania informacyjne bez kwantowej przewagi

Powyżej wspomniano (zob. część IV.1), że nielokalne korelacje kwantowe pozwalają uzyskać przewagę nad korelacjami klasycznymi w realizacji wielu zadań informacyjnych. Można by więc przypuszczać, że dają one przewagę w każdym nietrywialnym zadaniu. Okazuje się jednak, że intuicja ta jest nieprawdziwa, bowiem w pewnych intrygujących sytuacjach korelacje klasyczne działają równie dobrze jak korelacje kwantowe. Taką równoważność można w szczególności utożsamić z nierównościami Bella, których nie łamią żadne korelacje kwantowe; w skrócie będziemy je nazywać nierównościami Bella bez kwantowego łamania. Pierwsze przykłady takich nierówności, odpowiadających zadaniu obliczeń nielokalnych, zostały podane w przypadku dwucząstkowym w [16]. Natomiast w przypadku wielocząstkowym, nierówności Bella bez kwantowego łamania dla dowolnej liczby obserwatorów zostały skonstruowane w [22] i definiują zadanie zwane „zgadnij wejście twojego sąsiada" *(guess your neighbour's input (GYNI))*. Nierówność GYNI dla trzech obserwatorów jest podana w (10).

Okazuje się, że powyższe nierówności Bella są łamane przez pewne pozakwantowe korelacje niesygnalizujące. Gdyby więc w obrębie modeli niesygnalizujących istniała bardziej ogólna teoria niż mechanika kwantowa i pozwalała na generowanie takich korelacji, możliwe byłoby uzyskanie przewagi nad korelacjami kwantowymi w realizacji powyższych zadań. Ten zaskakujący fakt został użyty do sformułowania zasad informacyjnych mających na celu charakteryzację zbioru korelacji kwantowych: zasady braku kwantowej przewagi w obliczeniach nielokalnych w [16] oraz zasady lokalnej ortogonalności w [C11,C12], obu wspomnianych w części IV.2.

Poza powyższymi przykładami niewiele wiadomo o zadaniach informacyjnych (równoważnie, nierównościach Bella), w realizacji których korelacje kwantowe nie dają żadnej przewagi nad korelacjami klasycznymi. W [H3,H4], opierając się na wynikach pracy [H1], podaliśmy ogólną konstrukcję wielocząstkowych nierówności Bella bez kwantowego łamania, czym uogólniliśmy wyniki pracy [22].

Nierówności Bella bez kwantowego łamania z nierozszerzalnych baz iloczynowych. Punktem wyjścia naszych rozważań jest *a priori* nieoczekiwana relacja pomiędzy trzycząstkową nierozszerzalną bazą iloczynową i nierównością Bella (10) znaleziona w [H1] i nakreślona

RA

w części IV.2. W [H3] pokazujemy, że związek ten jest silniejszy i bardziej ogólny: dowolna wielocząstkowa nierozszerzalna baza iloczynowa spełniająca pewien warunek generuje nierówność Bella bez kwantowego łamania, która jednocześnie jest łamana przez pewne pozakwantowe korelacje niesygnalizujące.

Zacznijmy od przypomnienia definicji UPB. Rozważmy wielocząstkową przestrzeń Hilberta $\mathcal{H}_N$ zdefiniowaną w (1). Następnie niech S będzie k-elementowym zbiorem wektorów iloczynowych z $\mathcal{H}_N$, to znaczy

$$S = \left\{ |\psi_j\rangle = |\psi_j^{(1)}\rangle \otimes \ldots \otimes |\psi_j^{(N)}\rangle \right\}_{j=1}^{k}, \tag{13}$$

gdzie $|\psi_j^{(i)}\rangle \in \mathbb{C}^{d_i}$ dla każdego i i j. Zbiór S nazywamy nierozszerzalną bazą iloczynową jeśli następujące warunki są spełnione: (i) $k < \dim \mathcal{H}_N$, co oznacza, że S nie rozpina całej przestrzeni Hilberta $\mathcal{H}_N$ oraz (ii) nie istnieje żaden wektor iloczynowy w podprzestrzeni ortogonalnej do $\mathrm{span}(S)$.

Opiszmy teraz jak nierozszerzalne bazy iloczynowe mogą być użyte do konstrukcji nierówności Bella bez kwantowego łamania. Najpierw, mając dane UPB S, konstruujemy zbiory lokalne $S^{(i)}$ jako te, które zawierają wszystkie wektory lokalne występujące na pozycji i w $|\psi_j\rangle$. Następnie, w każdym $S^{(i)}$ wyróżniamy lokalne podzbiory $S_m^{(i)}$ wzajemnie ortogonalnych wektorów. Każdy zbiór $S_m^{(i)}$ definiuje pomiar lokalny, podczas gdy wektory w tym zbiorze wyniki tego pomiaru. Aby wykluczyć możliwość podziału danego zbioru $S^{(i)}$ na kilka sposobów, rozważamy tylko takie UPB S, które mają następującą własność: dowolne dwa wektory należące do różnych podzbiorów $S_m^{(i)}$ nie mogą być ortogonalne. W dalszej części rozdziału będziemy własność tę będziemy oznaczać przez (P). Zauważmy, że wszystkie UPB w wielokubitowych przestrzeniach Hilberta trywialnie spełniają ten warunek.

Po zdefiniowaniu zbiorów lokalnych każdemu wektorowi z S można przypisać prawdopodobieństwo warunkowe $p(a_1, \ldots, a_N | x_1, \ldots, x_N)$ w następujący sposób: pomiar obserwatora A_i jest zadany przez indeks m określający zbiór $S_m^{(i)}$, do którego należy $|\psi_j^{(i)}\rangle$, podczas gdy wynik tego pomiaru odpowiada pozycji tego wektora w zbiorze. Biorąc następnie kombinację otrzymanych w ten sposób prawdopodobieństw warunkowych z dodatnimi wagami q_j, konstruujemy wielocząstkową nierówność Bella

$$\sum_j q_j p(\boldsymbol{a}_j | \boldsymbol{x}_j) \leq \max\{q_j\}, \tag{14}$$

przy czym jej klasyczne ograniczenie można łatwo wyznaczyć korzystając z faktu, że dowolna para prawdopodobieństw warunkowych ma ten sam wybór pomiaru na pewnej pozycji, ale różne wyniki. Zatem dla wszystkich deterministycznych modeli LHV tylko jedno prawdopodobieństwo $p(\boldsymbol{a}_j | \boldsymbol{x}_j)$ przyjmuje niezerową wartość, podczas gdy pozostałe muszą znikać. Ta sama własność implikuje także, że nierówności Bella (14) nie mogą być złamane przez teorię kwantową (zob. [H3]).

Z drugiej strony nie jest trudno udowodnić, że dla dowolnego UPB S, które ma własność (P), odpowiadająca mu nierówność Bella z $q_j = 1$ dla wszystkich j jest łamana przez pewne pozakwantowe korelacje spełniające zasadę niesygnalizowania. Aby to pokazać rozważmy świadka splątania

$$W = \frac{1}{|S| - \epsilon D} \left(\Pi_{\mathrm{UPB}} - \epsilon \mathbb{1} \right), \tag{15}$$

RA

gdzie $|S|$ to liczba elementów w S, $D = \dim \mathcal{H}_N$, Π_{UPB} jest projektorem na podprzestrzeń rozpinaną przez S oraz

$$\epsilon = \min_{|\psi_{\mathrm{prod}}\rangle} \langle \psi_{\mathrm{prod}} | \Pi_{\mathrm{UPB}} | \psi_{\mathrm{prod}} \rangle > 0, \tag{16}$$

gdzie minimum jest brane po wszystkich wektorach iloczynowych z $\mathcal{H}_N$.

Jeśli lokalne pomiary odpowiadają zbiorom $S_k^{(i)}$, to korelacje wytworzone ze świadka W łamią nierówność Bella (14) skonstruowaną ze zbioru S. Ponadto, zgodnie z tym co powiedzieliśmy w części (IV.2), korelacje te spełniają zasadę niesygnalizowania.

Co ciekawe, głównym powodem, dla którego ta nierówność jest łamana przez korelacje niesygnalizujące, jest fakt, że S jest UPB. Pokazujemy w [H3], że dla dowolnego zbioru wektorów iloczynowych spełniających własność (P), który jest uzupełnialny do pełnej bazy w odpowiedniej przestrzeni Hilberta, odpowiadająca jej nierówność Bella jest trywialna w tym sensie, że żadne korelacje nie mogą jej złamać.

Oczywiście nasza konstrukcja może być zastosowana w drugą stronę: mając daną nierówność Bella typu (14), można skonstruować, stosując powyższy przepis, zbiór wektorów produktowych. W szczególności pokazujemy, że wielocząstkowa nierówność Bella GYNI generuje N-kubitową nierozszerzalną bazę iloczynową, nieznaną wcześniej w literaturze.

Warto również zauważyć, że skoro, jak pokazano w [22], nierówność Bella GYNI jest optymalna (*tight*) dla $3 \leq N \leq 7$, nasza konstrukcja pozwala wyprowadzać także optymalne nierówności Bella z UPB. W pracy [H3] pokazujemy jednak, że nie dzieje się tak dla każdego UPB. Ciekawym problemem otwartym pozostaje więc zrozumienie, z jakich UPB nasza konstrukcja pozwala otrzymać optymalne nierówności Bella bez kwantowego łamania.

Nierówności Bella bez kwantowego łamania i N-kubitowe UPB. W [H4], kontynuując powyższy kierunek badań, przebadaliśmy związek pomiędzy UPB i nierównościami Bella sformułowany w [H3], kładąc szczególny nacisk na N-kubitowe przestrzenie Hilberta. Otrzymaliśmy następujące wyniki:

- Podaliśmy dwa alternatywne dowody faktu, że nierówności Bella wygenerowane przez zbiory wektorów iloczynowych, które można uzupełnić do baz iloczynowych rozpinających $\mathcal{H}_N$, są trywialne w tym sensie, że żadne korelacje niesygnalizujące ich nie łamią. W konsekwencji nierówność Bella skonstruowana ze zbioru N-kubitowych wektorów iloczynowych jest nietrywialna wtedy i tylko wtedy, gdy ten zbiór jest UPB lub może być uzupełniony do UPB.
- W bardziej szczegółowy sposób zaprezentowaliśmy dowód faktu, że nierówności Bella GYNI generują N-kubitowe nierozszerzalne bazy iloczynowe.
- Pokazaliśmy, że nierówności Bella GYNI są optymalne (innymi słowy, definiują ściany odpowiednich wielościanów Bella) dla dowolnego nieparzystego N. Fakt ten został udowodniony w [22] tylko dla $3 \leq N \leq 7$ przy użyciu algorytmu komputerowego.
- Używając prostej metody numerycznej skonstruowaliśmy nowe przykłady nierozszerzalnych baz iloczynowych w czterokubitowej przestrzeni Hilberta, które generują, w ramach naszej metody, optymalne nierówności Bella bez kwantowego łamania. Rozważaliśmy bazy z różną liczbą baz lokalnych.

RA

- Podaliśmy także metody rozszerzania N-kubitowych baz iloczynowych (równoważnie nierówności Bella) do $(N+1)$-kubitowych baz iloczynowych. Zilustrowaliśmy jedną z tych metod przez zastosowanie jej do wybranych czterocząstkowych optymalnych nierówności Bella, otrzymując w ten sposób pięciocząstkowe optymalne nierówności Bella.

IV.4 Nielokalność a inne zasoby kwantowej informacji

Kwantowa teoria informacji może być rozumiana jako teoria, której celem jest wykorzystywanie zjawisk fizycznych przewidywanych przez teorię kwantów jako zasobów do wykonania pewnych zadań informacyjnych. Takimi zasobami w teorii kwantowej są splątanie, bezpieczne korelacje lub nielokalność. Podczas gdy bezpieczne korelacje mogą być zdefiniowane już w klasycznym formalizmie, splątanie i nielokalność nie mają klasycznych odpowiedników. Jednym z celów informatyki kwantowej jest więc charakteryzacja tych pojęć oraz zrozumienie związków między nimi, a w szczególności, czy możliwość wytworzenia jednego zasobu ze stanu kwantowego implikuje możliwość wytworzenia innego zasobu z tego samego stanu. Innymi słowy chcemy zrozumieć, czy dany stan kwantowy może mieć wiele zastosowań w zależności od tego, który zasób można przy jego użyciu otrzymać. W serii trzech prac zajmowaliśmy się tym ostatnim problemem, a dokładniej mówiąc, przestudiowaliśmy związek pomiędzy splątaniem oraz bezpiecznymi korelacjami i nielokalnością.

IV.4.1 Wszystkie stany prywatne są nielokalne

Oczywiście, pierwszym krokiem w zbadaniu powyższych zasobów jest identyfikacja ich podstawowych jednostek; przykładowo jednostką splątania jest maksymalnie splątany stan dwóch kubitów, zwyczajowo nazywany *e-bitem*. Całkiem niedawno udowodniono, że jednostką bezpiecznych korelacji w przypadku kwantowym są stany prywatne, z których odseparowani obserwatorzy mogą wygenerować idealnie bezpieczny klucz kryptograficzny [24, 25]. Okazuje się, że takie stany muszą być splątane, bowiem nie można wytworzyć bezpiecznego klucza kryptograficznego bez użycia splątania [26], jednakże pytanie czy są też nielokalne pozostawało otwarte (zauważmy, że jak to opisano poniżej, splątanie i nielokalność są w ogólności pojęciami nierównoważnymi, a więc fakt, że dany stan kwantowy jest splątany nie oznacza, że łamie on nierówności Bella).

Naszym celem w [H2] było odpowiedzieć na to pytanie. Pokazaliśmy, że każdy stan prywatny łamie pewną nierówność Bella, co oznacza, że bezpieczne korelacje implikują nie tylko splątanie, ale też nielokalność.

Aby przedstawić nasz dowód w bardziej szczegółowy sposób, zacznijmy od definicji stanów prywatnych. W ogólnym N-cząstkowym przypadku przyjmują one następującą postać [24, 25], [B7]:

$$\Gamma^{(d)}_{\mathsf{AA}'} = \frac{1}{d}\sum_{i,j=0}^{d-1} (|i\rangle\langle j|)^{\otimes N}_{\mathsf{A}} \otimes U_i \rho_{\mathsf{A}'} U_j^{\dagger}, \tag{17}$$

gdzie $\rho_{\mathsf{A}'}$ jest pewną macierzą gęstości, U_i to dowolne operacje unitarne, a indeksy $\mathsf{A} = A_1 \ldots A_N$ i $\mathsf{A}' = A'_1 \ldots A'_N$ oznaczają, odpowiednio, część klucza i tarczy stanu prywatnego (część klucza to ta, z której generuje się klucz kryptograficzny, natomiast część tarczy to ta,

RA

która zabezpiecza klucz przed podsłuchiwaczem). Podukłady A_i oraz A_i' są w posiadaniu obserwatora i. W ramach podejścia zaproponowanego w [24, 25], a następnie uogólnionego na dowolną liczbę obserwatorów w [B7], z każdego takiego stanu prywatnego można uzyskać $\log_2 d$ bitów idealnie bezpiecznego wielocząstkowego klucza kryptograficznego.

Pierwszym krokiem naszego dowodu jest pokazanie, że przez zastosowanie odpowiednio dobranych lokalnych operacji kwantowych (bez użycia komunikacji klasycznej) postaci

$$\Lambda_i = V_i(\cdot)V_i^\dagger + W_i(\cdot)W_i^\dagger, \tag{18}$$

do podukładów stanu prywatnego (17), a następnie wyśladowanie części tarczy tego stanu, można sprowadzić go do następującego N-cząstkowego stanu

$$\rho_N' = \sum_{i,j=0}^{d-1} \alpha_{ij} |i\rangle\langle j|^{\otimes N}, \tag{19}$$

w którym przynajmniej jeden pozadiagonalny element macierzowy α_{ij} nie znika oraz wszystkie diagonalne elementy wynoszą $\alpha_{ii} = 1/d$. W równaniu (18) V_i i W_i to tak zwane operatory Krausa, których jawne postaci nie są istotne dla dalszych rozważań. Należy tutaj zauważyć, że powyższe operacje lokalne bez udziału komunikacji klasycznej nie mogą wytworzyć stanu nielokalnego ze stanu, dla którego istnieje model LHV.

Teraz chcemy udowodnić, że stan (19) jest nielokalny. W pierwszej kolejności rozważmy najprostszy przypadek $N = 2$ i wprowadźmy nierówność Bella CHSH [27] dla scenariusza $(2, 2, 2)$ w jej sformułowaniu zaproponowanym przez Clausera i Horne'a [28]:

$$p(00|11) + p(00|21) + p(00|12) - p(00|22) - p_A(0|1) - p_B(0|1) \leq 0, \tag{20}$$

gdzie $p_{A(B)}(0|1)$ to prawdopodobieństwo, że obserwator A (B) otrzymał wynik $a = 0$ $(b = 0)$ po pomiarze obserwabli A_1 (B_1). Załóżmy następnie, że α_{kl} jest niezerowym elementem pozadiagonalnym macierzy ρ_2' oraz przepiszmy ten stan jako

$$\rho_2' = \begin{pmatrix} \ddots & \vdots & & \vdots & \\ \cdots & 1/d & \cdots & \alpha_{kl} & \cdots \\ & \vdots & \ddots & \vdots & \\ \cdots & \alpha_{kl}^* & \cdots & 1/d & \cdots \\ & \vdots & & \vdots & \ddots \end{pmatrix}. \tag{21}$$

Aby złamać nierówność Bella (20) za pomocą powyższego stanu, możemy wykorzystać fakt, że, z dokładnością do czynnika normalizacyjnego $2/d$, czteroelementowy blok pokazany w równaniu (21) można postrzegać jako stan dwukubitowy. Zatem konstruujemy obserwable A_x i B_y $(x, y = 1, 2)$ tak, aby ich wyniki $a = b = 0$ odpowiadały jednokubitowym projektorom $P_A^{(x)}$ oraz $P_B^{(y)}$, które prowadzą do łamania (20) przez ten stan dwukubitowy. Pozostałe wyniki będą odpowiadały operatorom $\mathbb{1} - P_{A/B}^{(i)}$. Można teraz bezpośrednio sprawdzić, że tak zdefiniowane pomiary prowadzą do łamania nierówności (20) przez stan ρ_2'.

Aby pokazać, że stan (19) jest nielokalny dla dowolnego N, można wykorzystać następujący, bardzo pomocny fakt udowodniony w [29]: jeżeli dla danego N-cząstkowego stanu kwantowego ρ_N istnieją lokalne rzuty $N - k$ cząstek na stan produktowy, po których stan kwantowy ρ_k odpowiadający pozostałym k cząstkom jest nielokalny, to stan ρ_N też jest nielokalny.

RA

Nietrudno zauważyć, że po zrzutowaniu dowolnych $N-2$ podukładów stanu ρ'_N na $|\phi\rangle = (1/\sqrt{d})(|0\rangle + \ldots + |d-1\rangle)$, pozostałe dwa podukłady będą dokładnie w stanie ρ'_2. Jak już pokazaliśmy jest on nielokalny, a więc, na mocy powyższego faktu, stan ρ_N też jest nielokalny. W konsekwencji dowolny stan prywatny jest nielokalny. Jako otwarte pozostawiamy pytanie jak bardzo nielokalne są stany prywatne i jakie inne nierówności Bella mogą one łamać.

IV.4.2 Nierównoważność splątania i nielokalności

Przejdźmy teraz do związku splątania z nielokalnością. Wiadomo już, że każdy nielokalny stan kwantowy musi być splątany, bowiem stany separowalne nie łamią nierówności Bella. Jednak pytanie czy przeciwna implikacja jest też prawdziwa, to znaczy czy wszystkie splątane stany kwantowe są nielokalne jest znaczniej bardziej skomplikowane. Pomimo tego, że jak udowodniono w [30, 31, 29], wszystkie czyste splątane stany czyste są nielokalne, splątanie nie musi implikować nielokalności w ogólnym przypadku stanów mieszanych. W istocie istnieją splątane stany kwantowe, które mają modele LHV, a więc nie łamią nierówności Bella.

Pierwszy przykład splątanych stanów mieszanych, dla których istnieje model LHV dla pomiarów rzutowych został podany przez Wernera [32]. Model Wernera został później uogólniony na dowolne pomiary kwantowe przez Barretta [33]. Od tego czasu pojawiła się w literaturze seria prac przedstawiających modele LHV dla różnych splątanych stanów kwantowych. Głównie jednak zajmowano się przypadkiem dwucząstkowym, pozostawiając przypadek wielocząstkowy prawie niezbadany (poza pracą [34], która dotyczy stanów trzycząstkowych).

Wraz ze współpracownikami w [H9] przebadałem problem nierównoważności splątania i nielokalności w przypadku dowolnej liczby obserwatorów. Uprzednio, niejako „na rozgrzewkę", w pracy przeglądowej [H7] zebraliśmy znane wyniki dotyczące tego problemu, w większości otrzymane w przypadku $N=2$.

Przegląd modeli LHV dla splątanych stanów kwantowych. W pracy [H7] opisaliśmy wszystkie znane dotychczas modele LHV dla splątanych stanów kwantowych. Poza wprowadzeniem do tematyki, koniecznymi definicjami i pojęciami, nasza praca zawiera w szczególności następujące wyniki literaturowe:

- Model Wernera dla pomiarów rzutowych wraz ze szczegółowym wyprowadzeniem granicznej wartości parametru mieszania, dla której stosuje się ten model; zauważmy, że w oryginalnej pracy Wernera [32] tak szczegółowego wyprowadzenia nie ma.
- Model LHV Barreta [33] uogólniający model Wernera na wszystkie możliwe pomiary kwantowe wraz ze wszystkimi szczegółowymi obliczeniami.
- Związek pomiędzy modelami LHV dla dwuwynikowych pomiarów i pojęciem stałej Grothendiecka wraz z wynikającym z niego ogólniejszym modelem LHV dla pomiarów rzutowych dla dwukubitowych stanów Wernera [35]; model ten działa w większym zakresie parametru mieszania niż oryginalny model Wernera.
- Model LHV dla stanów izotropowych [36], które są mieszaninami stanu maksymalnie splątanego o dowolnym wymiarze lokalnym i stanu maksymalnie mieszanego, wraz z

RA

uogólnieniami tego modelu na inne mieszane stany splątane oraz analizę odporności nielokalności na szum podane w [37].

- Metodę konstrukcji dwupodukładowych mieszanych stanów kwantowych wraz z modelami LHV dla dowolnych pomiarów kwantowych ze stanów, dla których istnieją modele LHV dla pomiarów rzutowych [38]. Metoda ta została użyta w [38], aby udowodnić, że ukryta nielokalność (*hidden nonlocality*) istnieje w przypadku, gdy obserwatorzy używają dowolnych pomiarów kwantowych. W naszej pracy podajemy także uogólnienie tej metody na przypadek dowolnej ilości obserwatorów.

- Model LHV dla dwuwynikowych pomiarów rzutowych dla pewnej klasy trzykubitowych stanów prawdziwie splątanych zaproponowany w pracy [34]. Podajemy także alternatywny dowód, że model ten odtwarza prawdopodobieństwa warunkowe otrzymane z tych stanów.

Poza powyższymi rezultatami otrzymanymi w standardowym scenariuszu Bella, w pracy [H7] podajemy listę alternatywnych scenariuszy, w których również można badać związek nielokalności i splątania. Listę tę uzupełniamy znanymi wynikami literaturowymi otrzymanymi w tych scenariuszach. Wreszcie w podsumowaniu pracy stawiamy kilka ciekawych pytań, które mogą stanowić dobry punkt wyjścia do dalszych badań nad związkiem splątania i nielokalności.

Nierównoważność splątania i nielokalności w przypadku wielocząstkowym. Problem nierównoważności splątania i nielokalności w przypadku wielocząstkowym znacznie się komplikuje z dwóch powodów. Po pierwsze, scenariusz wielocząstkowy oferuje całą gamę różnych rodzajów splątania i nielokalności, a więc o wiele trudniej jest porównywać oba pojęcia. Jak twierdzimy w [H9] właściwe pytanie, na które należy odpowiedzieć w tym przypadku to czy dla dowolnej liczby cząstek N zawsze istnieją N-cząstkowe prawdziwie splątane[4] stany kwantowe, które nie są prawdziwie nielokalne. Kolejny problem, który się pojawia w scenariuszu wielocząstkowym to fakt, że dopiero niedawno definicje wielocząstkowej nielokalności zostały prawidłowo sformułowane [39, 40]. Okazało się bowiem, że poprzednia definicja podana przez Svetlichny'ego [41] była niezgodna z operacyjną interpretacją nielokalności. Te nowe definicje nakładają pewne warunki na rozkłady prawdopodobieństw, które należy brać pod uwagę konstruując modele LHV dla stanów wielocząstkowych.

W [H9] pokazaliśmy, że rzeczywiście splątanie i nielokalność są nierównoważnymi zasobami dla dowolnej liczby obserwatorów. W tym celu wprowadziliśmy ogólną konstrukcję prawdziwie splątanych stanów wielocząstkowych, które nie są prawdziwie nielokalne, jako że można dla nich skonstruować pewne dwulokalne modele LHV.

Aby zilustrować naszą metodę rozważmy pewien dwucząstkowy stan splątany ρ_{AB} działający na przestrzeni Hilberta $\mathbb{C}^d \otimes \mathbb{C}^d$ i załóżmy, że ma on model LHV dla dowolnych pomi-

[4] Wielocząstkowy stan kwantowy ρ jest prawdziwie splątany jeśli nie może być zapisany jako kombinacja wypukła stanów kwantowych, które są separowalne ze względu na dowolne podziały wszystkich osób na dwie grupy. Analogicznie, zgodnie z definicją podaną w [41], ρ jest prawdziwie nielokalny jeżeli można z niego wytworzyć korelacje $\{p(a|x)\}$, które nie są kombinacją wypukłą korelacji lokalnych ze względu na dowolny podział wszystkich obserwatorów na dwie grupy. Jak pokazano w [39, 40] należy dodatkowo założyć, że wszystkie korelacje występujące w tej kombinacji wypukłej są niesygnalizujące.

RA

arów kwantowych taki jak na przykład model wprowadzony przez Barretta [33]. Rozważmy następnie parę kanałów kwantowych

$$\Lambda_{A\to S}:\mathcal{B}(\mathbb{C}^d)\to\mathcal{B}((\mathbb{C}^{d'})^{\otimes L}),\qquad \Lambda_{B\to\bar{S}}:\mathcal{B}(\mathbb{C}^d)\to\mathcal{B}((\mathbb{C}^{d'})^{\otimes N-L}), \tag{22}$$

odwzorowujących operatory działające na jednocząstkowej przestrzeni Hilberta na operatory działające odpowiednio na L-cząstkowej i $(N-L)$-cząstkowej przestrzeni Hilberta o wymiarze lokalnym d', który w ogólności może się różnić od d. Działając tymi kanałami na podukłady stanu ρ_{AB} można skonstruować następujący N-cząstkowy stan kwantowy

$$\sigma_{\mathbf{A}}=(\Lambda_{A\to S}\otimes\Lambda_{B\to\bar{S}})(\rho_{AB}). \tag{23}$$

Jak dowodzimy w [H9], ten stan nie jest prawdziwie N-cząstkowo nielokalny w ramach definicji podanej w [41], ponieważ zawsze można dla niego skonstruować model LHV ze względu na podział $\mathcal{S}|\bar{\mathcal{S}}$, gdzie zbiory $\mathcal{S}$ i $\bar{\mathcal{S}}$ składają się odpowiednio z L i $N-L$ cząstek. Ponadto w szczególnym przypadku, gdy $L=1$ stan ten będzie dwulokalny także w ramach definicji podanych w [39, 40].

Teraz musimy zagwarantować, by stan $\sigma_{\mathbf{A}}$ był prawdziwie N-cząstkowo splątany dla odpowiednio dobranych kanałów (22). W tym celu rozważamy kanały o rzędach jeden $\Lambda_{A\to S}(\cdot)=V_L(\cdot)V_L^{\dagger}$ i $\Lambda_{A\to\bar{S}}(\cdot)=V_{N-L}(\cdot)V_{N-L}^{\dagger}$, gdzie V_M jest macierzą zdefiniowaną poprzez $V_M|i\rangle=|i\rangle^{\otimes M}$ dla dowolnego elementu $|i\rangle$ bazy standardowej w $\mathbb{C}^d$. Wykorzystując fakty, że V_M jest izometrią, a więc oba kanały są odwracalne oraz, że stan początkowy ρ_{AB} jest splątany, pokazujemy w [H9], że stan $\sigma_{\mathbf{A}}$ jest prawdziwie wielocząstkowo splątany. Zatem startując z dwucząstkowego stanu splątanego, który ma model LHV, jesteśmy w stanie skonstruować stan kwantowy o dowolnej liczbie cząstek, który jest prawdziwie wielocząstkowo splątany, ale nie prawdziwie wielocząstkowo nielokalny. Co ważne, nasza konstrukcja działa także jeśli rozważyć niedawno sformułowane definicje wielocząstkowej nielokalności [39, 40]. Co więcej, pozwala ona udowodnić, że prawdziwe splątanie wielocząstkowe nie jest równoważne sterowalności (*steering*)—kolejnej formie korelacji kwantowych (zob. [42]). To znaczy, stosując naszą metodę do dwucząstkowego stanu kwantowego można wytworzyć prawdziwie splątany stan, który jest niesterowalny (w przynajmniej jednym kierunku) ze względu na ten sam podział, w którym ten stan jest dwulokalny.

Podsumowując wyniki pracy [H9] stawiamy także pytanie o to, czy istnieją prawdziwie splątane stany wielocząstkowe z w pełni lokalnymi modelami LHV (por. (5)). Warto więc dodać, że przykłady takich stanów zostały znalezione [43] niedługo po opublikowaniu naszej pracy.

IV.5 Relacje monogamii dla korelacji niesygnalizujących

Nielokalne korelacje są zasobem w dziedzinie informacji kwantowej. Okazuje się jednak, że korelacje te nie mogą być rozdystrybuowane pomiędzy obserwatorami w dowolny sposób. Zasady fizyczne narzucają bowiem pewne ograniczenia na to jak mogą być one współdzielone; zazwyczaj te ograniczenia są sformułowane w postaci relacji monogamii. Aby zilustrować ideę relacji monogamii rozważmy najprostszy scenariusz $(3,2,2)$, w którym trzech obserwatorów A,B,C wykonuje lokalnie jeden z dwóch dwuwynikowych pomiarów na swoim podukładzie,

RA

wytwarzając pewne korelacje $\{p(a,b,c|x,y,z)\}$. Toner pokazał [44], że zasada niesygnalizowania „nakazuje" tym korelacjom spełniać następującą nierówność

$$I_{AB} + I_{AC} \leq 4, \tag{24}$$

gdzie I_{AB} oraz I_{AC} to wyrażenia Bella CHSH pomiędzy, odpowiednio, A i B oraz A i C. Ponieważ maksymalne kwantowe łamanie nierówności Bella CHSH to $2\sqrt{2}$, powyższa nierówność oznacza, że tylko jedna z par AB lub AC może złamać nierówność CHSH, więc tylko jedna para może dzielić korelacje nielokalne. Ta interesująca obserwacja została później uogólniona na inne, bardziej złożone scenariusze (zob. przykładowo [45, 46]). Zilustrujmy te konstrukcje dla następującej klasy nierówności Bella [47]:

$$I_{AB}^{m,d} := \sum_{x=1}^{m} \left(\langle [A_x - B_x] \rangle + \langle [B_{x+1} - A_x] \rangle\right) \geq d-1, \tag{25}$$

która uogólnia nierówność Bella CHSH na większą liczbę pomiarów i wyników. Zauważmy, że używamy tutaj przeciwnej konwencji dotyczącej znaku nierówności, to znaczy zamiast zwyczajowego $\leq$ używamy $\geq$. Ponadto A_x i B_y $(x, y = 1, \ldots, m)$ oznaczają d-wynikowe obserwable mierzone przez obserwatorów A i B o wynikach ze zbioru $\{0, \ldots, d-1\}$, $\langle X \rangle$ jest standardową wartością oczekiwaną zmiennej losowej X, to znaczy $\langle X \rangle = \sum_{k=0}^{d-1} kP(X = k)$, $[X]$ oznacza X modulo d, natomiast $P(X = k)$ to prawdopodobieństwo tego, że zmienna losowa X przyjmuje wartość k. Przypomnijmy jeszcze, że nierówność Bella (25) została uogólniona na dowolną liczbę obserwatorów w [48]:

$$\begin{aligned} I_{A_1 \ldots A_N}^{N,m,d} \;&:=\; \sum_{x_1, \ldots, x_{N-1}=1}^{m} \Big(\langle [A_{x_1}^{(1)} - A_{x_1+x_2-1}^{(2)} + \ldots + (-1)^N A_{x_{N-2}+x_{N-1}-1}^{(N-1)} + (-1)^{N-1} A_{x_{N-1}}^{(N)}] \rangle \\ &\qquad + \langle [A_{x_1+x_2-1}^{(2)} - A_{x_1+1}^{(1)} + \ldots + (-1)^{N-1} A_{x_{N-2}+x_{N-1}-1}^{(N-1)} + (-1)^N A_{x_{N-1}}^{(N)}] \rangle \Big) \\ &\geq\; m^{N-2}(d-1), \end{aligned} \tag{26}$$

gdzie $A_{x_i}^{(i)}$ to d-wynikowe obserwable mierzone przez obserwatora A_i. Powyższa nierówność jest typu Svetlichny'ego [41], to znaczy korelacje, które ją łamią są prawdziwie wielocząstkowo nielokalne.

Pierwsza relacja monogamii dla nierówności (25) została wyprowadzona w [45] i można ją zapisać w następującej postaci

$$I_{AB_1}^{m,d} + \ldots + I_{AB_m}^{m,d} \geq m(d-1). \tag{27}$$

Implikuje ona, że suma wartości wyrażenia Bella $I^{m,d}$ pomiędzy obserwatorem A i m innymi osobami B_i nie może przekroczyć m-krotności klasycznego ograniczenia tej nierówności Bella. O wiele prostszą relację monogamii dla (25) wyprowadzono w pracy [46] i jest ona postaci

$$I_{AB}^{m,d} + I_{AC}^{m,d} \geq 2(d-1). \tag{28}$$

Wynika z niej, że podobnie jak w przypadku nierówności Bella CHSH, tylko jedna para osób może łamać nierówność Bella (25). Zauważmy jednak, że choć ta relacja monogamii jest o wiele prostsza niż (27), to poza przypadkiem $m = 2$ nie jest optymalna w tym sensie, że nie

RA

dla każdej pary wartości $I_{AB}^{m,d}$ i $I_{AC}^{m,d}$, które ją wysycają istnieją korelacje niesygnalizujące, które realizowałyby te wartości.

Podczas mojego pobytu w ICFO włączyłem się w badania nad relacjami monogamii, które kontynuowałem po przeniesieniu się do Polski. Po pierwsze, w [H6] zaproponowaliśmy alternatywne podejście do relacji monogamii dla korelacji niesygnalizujących, a następnie w [H10] pokazałem jak zmodyfikować relację (28) tak, aby była ona optymalna.

Elementarne relacje monogamii. W [H6] pokazaliśmy, że zasada niesygnalizowania ogranicza korelacje w silniejszy sposób niż wynika to z omówionych powyżej standardowych relacji monogamii. Zamiast porównywać łamanie nierówności Bella pomiędzy różnymi podzbiorami obserwatorów, jak ma to miejsce w powyższych relacjach monogamii, pokazujemy, że nielokalność współdzielona przez grupę obserwatorów znacząco ogranicza wiedzę jaką zewnętrzny obserwator może uzyskać o wynikach dowolnego pomiaru wykonanego przez obserwatorów.

Aby omówić nasze wyniki w bardziej szczegółowy sposób, rozważmy dla prostoty przypadek trzech obserwatorów i załóżmy, że współdzielą oni pewne korelacje $\{p(a,b,c|x,y,z)\}$, które powstają w eksperymencie z m d-wynikowymi pomiarami na osobę i spełniają zasadę niesygnalizowania (korelacje te nie muszą być kwantowe). Wówczas, następujące nierówności są spełnione [H6]:

$$I_{AB}^{m,d} + \langle [A_x - C_z] \rangle + \langle [C_z - A_x] \rangle \geq d-1 \qquad (x,z=1,\ldots,m) \tag{29}$$

gdzie $I_{AB}^{m,d}$ to wyrażenie Bella (25), a pozostałe symbole zostały zdefiniowane powyżej. Ponieważ relacje te wiążą wartość nierówności Bella pomiędzy obserwatorami A i B z pojedynczymi korelatorami pomiędzy A i C, w pracy [H6] nazywamy je elementarnymi.

Aby zinterpretować otrzymane nierówności, przepiszmy je w następującej postaci

$$p(A_x = C_z) \leq \frac{1}{d}\left[1 + I_{AB}^{m,d}\right] \tag{30}$$

i dodajmy, że zachodzą one także dla dowolnej zmiennej losowej C, a w szczególności jeżeli dodamy do niej dowolna liczbę ze zbioru $\{1,\ldots,d-1\}$. Zauważmy teraz, że $p(A_x = C_z)$ może być rozumiane jako miara tego, jak wyniki pomiarów A_x i C_z są (klasycznie) skorelowane. Zatem nierówności (30) wiążą nielokalność mierzoną łamaniem nierówności Bella (25) pomiędzy dwiema dowolnymi osobami oraz klasyczne korelacje, które trzeci obserwator może wytworzyć z wynikami dowolnego pomiaru wykonanego przez jednego z tych dwóch obserwatorów. W szczególnym przypadku maksymalnego łamania nierówności (25) dla korelacji niesygnalizujących, to znaczy, gdy $I_{AB}^{m,d} = 0$, otrzymujemy $p(A_x = C_z + k) = 1/d$ dla dowolnego $k = 0,\ldots,d-1$, co oznacza, że wyniki A_x i C_z są nieskorelowane. Co więcej nasze relacje są optymalne: dla dowolnych wartości $I_{AB}^{m,d}$ i $\langle [A_x - C_z] \rangle + \langle [C_z - A_x] \rangle$, dla których nierówności (29) są wysycane, istnieją korelacje niesygnalizujące realizujące te wartości.

Następnie uogólniamy relacje monogamii (29) na przypadek większej liczby obserwatorów niż trzy. Używamy w tym celu nierówności Bella (26). Ściślej mówiąc, dowodzimy, że dowolne korelacje niesygnalizujące współdzielone między $N+1$ osobami spełniają

$$I_{A_1\ldots A_N}^{N,m,d} + \langle [A_{x_i}^{(i)} - A_{x_{N+1}}^{(N+1)}] \rangle + \langle [A_{x_{N+1}}^{(N+1)} - A_{x_i}^{(i)}] \rangle \geq d-1 \tag{31}$$

RA

dla dowolnego $x_k = 1, \ldots, m$ i dowolnego $i = 1, \ldots, N+1$. Jak wyżej $A_{x_i}^{(i)}$ $(x_i = 1, \ldots, m)$ to zmienne losowe odpowiadające d-wynikowym obserwablom o wynikach ze zbioru $\{0, \ldots, d-1\}$ mierzonym przez obserwatora A_i.

Używając prawdopodobieństw powyższe nierówności można przepisać jako

$$p(A_{x_k}^{(k)} = A_{x_{N+1}}^{(N+1)}) \le \frac{1}{d}\left[1 + I_{A_1 \ldots A_N}^{N,m,d}\right]. \tag{32}$$

Jak wyżej, można opuścić indeks x_{N+1}, jako że nierówność (31), a więc także (32) pozostają spełnione dla dowolnej zmiennej losowej zewnętrznego obserwatora A_{N+1}. Zatem łamanie $I_{A_1 \ldots A_N}^{N,m,d}$ w optymalny sposób ogranicza korelacje jakie zewnętrzny obserwator może ustanowić pomiędzy wynikami swoich pomiarów i pomiarów wykonanych przez dowolnego obserwatora.

Wspomnijmy jeszcze, że podobną relacje monogamii wyprowadziliśmy także dla korelacji kwantowych w najprostszym scenariuszu $(3, 2, 2)$. Rozważmy następującą klasę nierówności Bella dla dwóch obserwatorów

$$\widetilde{I}_{AB}^{\alpha} := \alpha(\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle) + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \le 2\alpha \qquad (\alpha \ge 1), \tag{33}$$

która odtwarza standardową nierówność CHSH dla $\alpha = 1$. Wówczas dowolne trzyciałowe korelacje kwantowe $\{p(a, b, c|x, y, z)\}$ w scenariuszu $(3, 2, 2)$ spełniają nierówność

$$\left(\widetilde{I}_{AB}^{\alpha}\right)^2 + 4\langle A_x C_z \rangle^2 \le 4(1 + \alpha^2). \tag{34}$$

Zauważmy, że w przeciwieństwie do relacji (29), powyższe nierówności są nieliniowe.

Zastosowania w zadaniach informacyjnych. Co ciekawe, nasze relacje monogamii (29), (31) znajdują zastosowania w takich protokołach jak kwantowa dystrybucja klucza lub wzmacnianie losowości. Wynika to z faktu, że jak dowodzimy w [H6], pozwalają one na wyprowadzanie optymalnych ograniczeń na prawdopodobieństwo zgadnięcia (*guessing probability*)–powszechnie używaną miarą losowości–wyrażonych przez wartość $I^{N,m,d}$. Nasze ograniczenia są znacząco silniejsze niż te udowodnione wcześniej dla tej samej nierówności Bella [47].

Oznaczając przez $P_g(x_k)$ prawdopodobieństwo prawidłowego odgadnięcia wyniku pomiaru x_k wykonanego przez obserwatora A_k, dowodzimy w [H6], że nasze relacje monogamii implikują następujące nierówności

$$P_g(x_k) \le \frac{1}{d}\left[1 + I_{A_1 \ldots A_N}^{N,m,d}\right], \tag{35}$$

gdzie $I_{A_1 \ldots A_N}^{N,m,d}$ jest wyrażeniem Bella wprowadzonym powyżej. A więc łamanie nierówności $I_{A_1 \ldots A_N}^{N,m,d}$ ogranicza możliwość poprawnego odgadnięcia wyników dowolnego pomiaru wykonanego przez każdego z N obserwatorów. W szczególnym przypadku jej maksymalnego łamania przez korelacje niesygnalizujące, to znaczy, gdy $I_{A_1 \ldots A_N}^{N,m,d} = 0$, (35) implikuje $P_g(x_k) = 1/d$, czyli wyniki pomiaru x_k są niemożliwe do przewidzenia dla zewnętrznego obserwatora.

Co ważne, powyższe ograniczenia można zastosować w zadaniach informacyjnych takich jak kwantowa dystrybucja klucza lub wzmacnianie losowości. Po pierwsze pokazujemy,

RA

że (35) można przetłumaczyć na lepsze ograniczenia na ilość bezpiecznego klucza w protokole kwantowej dystrybucji klucza w modelu z ograniczoną pamięcią kwantową (*bounded-quantum-storage model*) rozważanym w [49]. Dowodzimy następnie, że nierówności (35) pozwalają uogólnić wyniki pracy [6] o wzmacnianiu losowości na dowolną liczbę obserwatorów i wyników, pokazując w szczególności, że dowolna ilość losowości może być otrzymana w przypadku dwóch obserwatorów. Pokazujemy także jak zmodyfikować scenariusz rozważany w Ref. [6] tak, aby pozwalał on wzmacniać losowość dla dowolnego

$$\varepsilon < \varepsilon_N'' = \frac{1}{2}\frac{2^{1/(N-1)} - 1}{2^{1/(N-1)} + 1}, \tag{36}$$

gdzie, nie wchodząc w szczegóły, ε jest parametrem określającym jak losowy jest wybór pomiarów w eksperymencie Bella ($\varepsilon = 0$ oznacza pełna losowość, natomiast $\varepsilon = 1/2$ to brak losowości). Dla $N = 2$ powyższa formuła daje wartość $\varepsilon_2'' = 1/6$, która jest większa niż $\varepsilon_2 \simeq 0.086$ otrzymana w [6] oraz wartość $\varepsilon' \simeq 0.0961$ wyznaczona później w [50].

Optymalne relacje monogamii. Innym pytaniem dotyczącym zjawiska monogamii w korelacjach niesygnalizujących, na które próbowałem odpowiedzieć, to czy przez zmodyfikowanie nierówności (28) do postaci

$$a(m,d)I_{AB}^{m,d} + b(m,d)I_{AC}^{m,d} \geq c(m,d), \tag{37}$$

można otrzymać optymalną relację monogamii dla nierówności Bella (25). Tutaj $a(m,d)$, $b(m,d)$ i $c(m,d)$ oznaczają dowolne parametry, które w ogólności mogą zależeć od m oraz d. W [H10], wykorzystując metody użyte w pracy [H6], pokazałem, ze tak rzeczywiście jest. Dokładniej mówiąc, dla dowolnych korelacji trzycząstkowych $\{p(a,b,c|x,y,z)\}$ z m pomiarami i d wynikami na stronę, następująca nierówność jest spełniona

$$(m-1)\min\{I_{AB}^{m,d}, I_{AC}^{m,d}\} + \max\{I_{AB}^{m,d}, I_{AC}^{m,d}\} \geq m(d-1). \tag{38}$$

Omówmy tę nierówność pokrótce. Po pierwsze zauważmy, że tylko jedna para osób AB lub AC może łamać nierówność Bella (25); jeśli, powiedzmy, nierówność ta jest złamana przez parę AB, to znaczy $I_{AB}^{m,d} < d-1$, wówczas para AC nie może jej złamać. Po drugie w przeciwieństwie do relacji (28), powyższa monogamia jest optymalna dla dowolnego m i d; dla dowolnych wartości $I_{AB}^{m,d}$ i $I_{AC}^{m,d}$, dla których (38) jest wysycana, można znaleźć korelacje niesygnalizujące, które realizują te wartości.

Używając wyrażenia Bella $I_{A_1\ldots A_N}^{N,m,d}$ powyższą relację monogamii (38) można następnie uogólnić na przypadek dowolnej liczby obserwatorów. Mówiąc ściśle, dowolne $(N+1)$-cząstkowe korelacje niesygnalizujące $\{p(\mathbf{a}|\mathbf{x})\}$ muszą spełniać

$$(m-1)\min\{\bar{I}_{A_1\ldots A_N}^{N,m,d}, \bar{I}_{A_1\ldots A_{N-1},A_{N+1}}^{N,m,d}\} + \max\{\bar{I}_{A_1\ldots A_N}^{N,m,d}, \bar{I}_{A_1\ldots A_{N-1}A_{N+1}}^{N,m,d}\} \geq m(d-1), \tag{39}$$

gdzie $\bar{I}_{A_1\ldots A_N}^{N,m,d} = I_{A_1\ldots A_N}^{N,m,d}/m^{N-2}$. Wynika z tego, że łamanie $I_{A_1\ldots A_N}^{N,m,d}$ przez N-elementowy podzbiór obserwatorów powoduje, że żaden inny podzbiór N osób nie może złamać tej nierówności Bella. Co więcej, nierówność (26) może być złamana tylko przez prawdziwie wielocząstkowo nielokalne korelacje, więc powyższa nierówność jest monogamią dla prawdziwie nielokalnych korelacji; przykładowo, jeżeli korelacje współdzielone przez $A_1, \ldots, A_N$ są

RA

prawdziwie nielokalne i łamią (39), to korelacje widziane przez $A_1, \ldots, A_{N-1}, A_{N+1}$ nie mogą złamać (39).

Zauważmy jeszcze, że relacje monogamii (39) są optymalne, co oznacza, że nie da się znaleźć silniejszej relacji ograniczającej korelacje niesygnalizujące przy użyciu dwóch wartości $\bar{I}^{N,m,d}_{A_1\ldots A_N}$ oraz $\bar{I}^{N,m,d}_{A_1\ldots A_{N-1}A_{N+1}}$.

W [H10] omawiamy także jak monogamie (38) mogą być przekute, używając wyników pracy [H6], w optymalne ograniczenia na prawdopodobieństwo zgadnięcia.

Muszę tutaj dodać, że w pracy [H10] błędnie zostały podane korelacje wysycające (39). Poprawne korelacje zostały podane w erracie dołączonej do pracy.

IV.6 Detekcja wielocząstkowej nielokalności przy użyciu korelacji dwuciałowych

W ostatniej części tej prezentacji podejmiemy zagadnienie eksperymentalnej weryfikacji nielokalności w złożonych stanach kwantowych. Badania nad tym problemem w przypadku wielocząstkowym są mniej zaawansowane niż w przypadku dwucząstkowym, w którym całkiem niedawno udało się dokonać eksperymentalnej weryfikacji łamania nierówności Bella zamykając pewne eksperymentalne luki [51, 52]. Są dwa tego powody: matematyczna złożoność problemu znalezienia wszystkich optymalnych nierówności Bella w danym scenariuszu oraz fakt, że większość znanych klas wielociałowych nierówności Bella (przykładowo [53, 54]) jest skonstruowana z funkcji korelacji zawierających pomiary wykonywane przez wszystkich obserwatorów. Niestety, pomiary takich wielkości są niedostępne w układach wielu ciał, w których możliwy jest pomiar kilkuciałowych, a często tylko dwuciałowych korelacji.

Aby przezwyciężyć te trudności można rozważyć detekcję nielokalności jedynie przy użyciu dwuciałowych korelacji. Z jednej strony redukuje to wymiar odpowiedniego wielościanu Bella; dla porównania, w ogólnym przypadku wymiar wielościanu Bella skaluje się eksponencjalnie z liczbą obserwatorów N, podczas gdy w przypadku dwuciałowych korelacji wymiar ten skaluje się kwadratowo z N. Z drugiej strony, korelacje takie są rutynowo mierzone w pewnych układach wielu ciał.

W długofalowym projekcie naszym celem było skonstruowanie wielocząstkowych nierówności Bella składających się tylko z dwuciałowych korelatorów (dodatkowo używamy jednociałowych wartości oczekiwanych), które nazwaliśmy *dwuciałowymi nierównościami Bella*. Ogólna ich postać dla N obserwatorów w najprostszym scenariuszu $(N,2,2)$, w którym każdy obserwator ma do wyboru dwa dwuwynikowe pomiary $M^{(i)}_{x_i}$ $(x_i = 1,2)$ to

$$\sum_{i=1}^{N}\left(\alpha_i\langle M_1^{(i)}\rangle + \beta_i\langle M_2^{(i)}\rangle\right) + \sum_{i<j}\gamma_{ij}\langle M_1^{(i)}M_1^{(j)}\rangle + \sum_{i\neq j}\delta_{ij}\langle M_1^{(i)}M_2^{(j)}\rangle + \sum_{i<j}\varepsilon_{ij}\langle M_2^{(i)}M_2^{(j)}\rangle + \beta_C \geq 0, \tag{40}$$

gdzie α_i, β_i, γ_{ij}, δ_{ij} i ε_{ij} to parametry, które chcemy wyznaczyć oraz β_C oznacza klasyczne ograniczenie tej nierówności.

Niezmienniczość permutacyjna. Pomimo zredukowania liczby parametrów, a zatem także i wymiaru wielościanu Bella, problem znalezienia nierównosci Bella postaci (40), które wykry-

RA

wałyby nielokalne korelacje dla dowolnej liczby obserwatorów jest wciąż trudny. Można go uprościć poprzez narzucenie pewnych symetrii na rozważane wyrażenia Bella. W [H5] rozważaliśmy podklasę dwuciałowych nierówności Bella, zwanych dalej symetrycznymi, które są niezmiennicze ze względu na zamianę dowolnej pary obserwatorów. W tym przypadku (40) upraszcza się do postaci

$$\alpha\mathcal{S}_1 + \beta\mathcal{S}_2 + \frac{\gamma}{2}\mathcal{S}_{11} + \delta\mathcal{S}_{12} + \frac{\varepsilon}{2}\mathcal{S}_{22} + \beta_C \geq 0, \tag{41}$$

gdzie α, β, γ, δ, and ε to pewne rzeczywiste parametry oraz $\mathcal{S}_k$ i $\mathcal{S}_{kl}$ oznaczają zsymetryzowane dwuciałowe wartości oczekiwane dane wzorami

$$\mathcal{S}_k = \sum_{i=1}^{N} \langle M_k^{(i)} \rangle, \qquad \mathcal{S}_{kl} = \sum_{i \neq j}^{N} \langle M_k^{(i)} M_l^{(j)} \rangle \qquad (k, l = 1, 2). \tag{42}$$

Znaleźliśmy następnie prostą charakteryzację wierzchołków wielościanu Bella odpowiadającego tej symetrii, co pozwoliło nam analitycznie znaleźć ogólną klasę dwuciałowych symetrycznych nierówności Bella, odpowiadających znacznej części ścian tego wielościanu. Ciekawym przykładem nierówności Bella należącej do tej klasy jest

$$-2\mathcal{S}_1 + \frac{1}{2}\mathcal{S}_{11} - \mathcal{S}_{12} + \frac{1}{2}\mathcal{S}_{22} + 2N \geq 0. \tag{43}$$

Zbadaliśmy czy jest ona łamana przez teorię kwantową. W tym celu rozważaliśmy następujące obserwable (takie same dla każdego obserwatora)

$$M_1^{(i)} = M_1 = \sigma_z, \qquad M_2^{(i)} = M_2 = \cos(\theta)\sigma_z + \sin(\theta)\sigma_x \tag{44}$$

i numerycznie wyznaczyliśmy najmniejszą wartość własną części operatora Bella działającej na podprzestrzeni symmetrycznej $(\mathbb{C}^2)^{\otimes N}$ dla $N \leq 10^4$. W ten sposób pokazaliśmy, że nierówność (43) jest łamana przez wielocząstkowe stany kwantowe dla każdego $N \geq 5$. Co ważne stany te są prawdziwie splątane, bowiem należą do podprzestrzeni symetrycznej N-kubitowej przestrzeni Hilberta, a także ich dwuciałowe podukłady są lokalne w tym scenariuszu, więc nie mogłyby złamać na przykład nierówności CHSH. Wartość łamania względnego Q_V^N/β_C^N, gdzie maksymalna wartość klasyczna nierówności (43) to $\beta_C^N = -2N$, rośnie z N i dąży do $-1/4$ dla dużych N, co oznacza, że maksymalna wartość kwantowa nierówności (43) rośnie przynajmniej liniowo z N. Warto również wspomnieć, że otrzymane łamania są odporne na błędy w doborze optymalnego ustawienia kąta θ w (44) oraz na straty cząstek.

Następnie w [H5] zadaliśmy pytanie, czy nasze dwucialowe nierówności Bella pozwalają wykrywać nielokalność w „ciekawych" wielocząstkowych stanach kwantowych, które albo są użyteczne w pewnych protokołach kwantowo-informacyjnych albo można je stosunkowo łatwo generować eksperymentalnie. Aby odpowiedzieć na to pytanie skonstruowaliśmy klasę symetrycznych dwuciałowych nierówności Bella, które wykrywają nielokalność w N-kubitowych stanach Dicke'go $|D_N^{\lfloor N/2 \rfloor}\rangle$ z $\lfloor N/2 \rfloor$ wzbudzeniami dla dowolnej liczby obserwatorów N. Przypomnijmy, że ogólna postać stanów Dicke'go z k wzbudzeniami to

$$|D_N^k\rangle = \mathcal{S}(|\{0, N-k\}, \{1, k\}\rangle) \qquad (k = 0, \ldots, N), \tag{45}$$

RA

gdzie $|\{0, N-k\}, \{1,k\}\rangle$ to dowolny czysty stan iloczynowy z $N-k$ kubitami w stanie $|0\rangle$ i k kubitami w stanie $|1\rangle$, a $\mathcal{S}$ to operacja symetryzacji. Warto wspomnieć, że taki stan Dicke'go dla $N=6$ i $k=3$ został eksperymentalnie wytworzony w [55, 56].

Nierówności wprowadzone w [H5] zadane są następującymi parametrami $\alpha_N = N(N-1)(\lceil N/2 \rceil - N/2)$, $\beta_N = \alpha_N/N$, $\gamma_N = N(N-1)/2$, $\delta_N = N/2$ oraz $\varepsilon_N = -1$, dla których można analitycznie znaleźć klasyczne ograniczenie wynoszące

$$\widetilde{\beta}_C^N = \frac{1}{2}N(N-1)\left\lceil \frac{N+2}{2} \right\rceil. \tag{46}$$

Ponadto są one niezależne od nierówności Bella (43) i dla $N=2$ odtwarzają nierówność Bella CHSH [27].

Aby przetestować je na stanie $|D_N^{\lfloor N/2 \rfloor}\rangle$ rozważamy ponownie obserwable (44), dla których można analitycznie wyznaczyć maksymalną[5] wartość kwantową

$$\widetilde{Q}_V^N = -\frac{\lfloor N/2 \rfloor}{\lceil N/2 \rceil + 1}, \tag{47}$$

co oznacza, że stan Dicke'go łamie nasze nierówności dla dowolnego N. Zauważmy jednak, że względna wartość tego łamania $\widetilde{Q}_V^N/\widetilde{\beta}_C^N$ skaluje się z N jak $1/N^3$, a więc szybko zanika dla dużych N. Okazuje się, że obserwable (44) nie są optymalne w tym przypadku; numerycznie potwierdziliśmy, że biorąc ogólniejsze obserwable (wciąż takie same dla każdego obserwatora) skalowanie $\widetilde{Q}_V^N/\widetilde{\beta}_C^N$ może być znacząco poprawione na $1/N$.

Zauważmy wreszcie, że w przypadku kiedy wszyscy obserwatorzy mierzą te same obserwable, jedno i dwuciałowe symetryczne wartości oczekiwane (42), a także wartość średnia operatora Bella, mogą być wyznaczone poprzez kolektywne pomiary operatorów całkowitego momentu pędu $S_\alpha = (1/2)\sum_{i=1}^N \sigma_\alpha^{(i)}$, gdzie $\alpha = x, y, z$, a $\sigma_\alpha^{(i)}$ to macierze Pauliego działające na i-tej pozycji, a także ich kombinacje $\boldsymbol{n}\cdot\boldsymbol{S}$ w dowolnym kierunku $\boldsymbol{n} \in \mathbb{R}^3$, gdzie $\boldsymbol{S} = [S_x, S_y, S_z]$. Ściślej mówiąc, dla dowolnej pary obserwabli $M_j^{(i)} = \boldsymbol{m}_j \cdot \boldsymbol{\sigma}$ $(j=1,2)$, zsymetryzowane wartości średnie (42) dadzą się przepisać jako

$$\begin{aligned} \mathcal{S}_k &= 2\langle \boldsymbol{m}_k \cdot \boldsymbol{S}\rangle, \quad \mathcal{S}_{kk} = 4\langle (\boldsymbol{m}_k \cdot \boldsymbol{S})^2\rangle - N, \quad (k=1,2) \\ \mathcal{S}_{12} &= \langle ((\boldsymbol{m}_1 + \boldsymbol{m}_2)\cdot \boldsymbol{S})^2\rangle - \langle ((\boldsymbol{m}_1 - \boldsymbol{m}_2)\cdot \boldsymbol{S})^2\rangle - N(\boldsymbol{m}_1 \cdot \boldsymbol{m}_2). \end{aligned} \tag{48}$$

Takie wielkości można mierzyć na przykład w sieciach optycznych za pomocą polaryzacyjnej spektroskopii spinowej [57, 58].

Należy jednak podkreślić, że w ogólności eksperyment wykorzystujący wielkości (48) nie jest poprawnym testem Bella, jako że, przykładowo, w układzie, w którym poszczególne cząstki nie są przestrzennie odseparowane, nie można zweryfikować, czy założenie o lokalności jest spełnione. Niemniej jednak, pomiar wartości oczekiwanej operatora Bella odpowiadającego naszym nierównościom Bella przez powyższe wielkości kolektywne może być postrzegany jako wskaźnik lub świadek, który pozwala stwierdzić, czy dany stan byłby

[5] Podobnie jak poprzednio wyrażenie „maksymalna wartość" jest tutaj używana w potocznym sensie i oznacza wartość najbardziej nieklasyczną. Dokładniej mówiąc ze względu na konwencję przyjętą w (40) należałoby raczej używać wyrażenia minimalna wartość kwantowa.

RA

nielokalny gdyby poprawnie wykonać na nim eksperyment Bella. Warto również wspomnieć, że w pracy [59] eksperymentalnie zmierzono takiego świadka korelacji Bella odpowiadającego naszej nierówności (43) w kondensacie Bosego-Einsteina składającym się z 480 atomów i pokazano, że otrzymany stan ją łamie.

Niezmienniczość translacyjna. Oczywiście niezmienniczość permutacyjna rozważana powyżej nie jest jedyną symetrią, która może być użyta do wyprowadzenia nierówności Bella. W pracy [H8], która jest bezpośrednią kontynuacją [H5], naszym celem było skonstruowanie dwuciałowych nierówności Bella spełniających mniej wymagającą symetrię: niezmienniczość translacyjną. Ich ogólna postać to

$$\alpha\mathcal{S}_1 + \beta\mathcal{S}_2 + \sum_{k=1}^{\lfloor N/2 \rfloor}\left(\gamma_k\mathcal{T}_{11}^{(k)} + \epsilon_k\mathcal{T}_{22}^{(k)}\right) + \sum_{k=1}^{N-1}\omega_k\mathcal{T}_{12}^{(k)} + \beta_C \geq 0, \tag{49}$$

gdzie α, β, γ_k, ϵ_k i ω_k to pewne parametry, $\mathcal{S}_1$ i $\mathcal{S}_2$ są zdefiniowane jak wyżej oraz $\mathcal{T}_{ij}^{(k)}$ oznaczają wszystkie translacyjnie niezmiennicze korelatory dane wzorem

$$\mathcal{T}_{ij}^{(k)} = \sum_{m=1}^{N}\langle M_i^{(m)}M_j^{(m+k)}\rangle \qquad (i \leq j = 1,2), \tag{50}$$

gdzie $k = 1,\ldots,\lfloor N/2 \rfloor$ dla $i = j$ oraz $k = 1,\ldots,N-1$ dla $i < j$. Zauważmy, że teraz liczba parametrów w (49) to $N + 1 + 2\lfloor N/2 \rfloor$, a więc w przeciwieństwie do poprzedniego przypadku, rośnie ona wraz z N. Oznacza to w szczególności, że analityczne metody rozwinięte przez nas w [H5] do badania symetrycznych, dwuciałowych nierówności Bella nie stosują się tutaj.

Użyliśmy więc programu komputerowego CDD [11], który pozwala znaleźć wszystkie ściany wielościanu Bella mając dane jego wierzchołki. Z jego pomocą znaleźliśmy wszystkie optymalne translacyjnie niezmiennicze, nierówności Bella dla trzech i czterech obserwatorów, a następnie pogrupowaliśmy je w klasy równoważności ze względu na pewne symetrie specyficzne dla nierówności Bella (przenumerowanie obserwatorów oraz pomiarów i ich wyników). Następnie wyznaczyliśmy ich klasyczne ograniczenia oraz maksymalne wartości dla korelacji kwantowych i niesygnalizujących. W przypadku wartości kwantowej numerycznie wyznaczaliśmy najmniejszą wartość własną operatora Bella biorąc następujące pomiary rzeczywiste[6]

$$M_{x_i}^{(i)} = \cos\phi_{x_i}^{(i)}\sigma_z + \sin\phi_{x_i}^{(i)}\sigma_x, \tag{51}$$

gdzie $\phi_{x_i}^{(i)}$ to dowolne kąty. Otrzymane wyniki zostały skatalogowane w tabelach w [H8].

Następnie rozważyliśmy przypadki $N = 5$ i $N = 6$. Podczas gdy przypadek $N = 6$ jest zbyt trudny do rozwiązania ze względu na złożoność problemu, w przypadku $N = 5$ znaleźliśmy, używając algorytmu CDD, 4198 różnych klas nierówności Bella. Ponieważ tych nierówności jest zbyt dużo, aby je w pełni zanalizować, skupiliśmy się na nierównościach, które zawierają tylko korelatory pomiędzy najbliższymi sąsiadami. Co ciekawe, jak pokazujemy w [H8], takie nierówności Bella pozwalają na detekcję nielokalności w układach wielociałowych pomimo

[6]Zauważmy, że jak pokazano w [60], maksymalne kwantowe łamanie każdej nierówności Bella z dwoma dwuwynikowymi pomiarami dla każdego obserwatora jest zawsze osiągana na wielokubitowym stanie kwantowym i rzeczywistych jednokubitowych pomiarach lokalnych postaci (51).

RA

tego, że w rzeczywistości wykorzystują one bardzo małą ilość informacji o badanym układzie kwantowym (tylko dwuciałowe korelacje pomiędzy najbliższymi sąsiadami).

Badając translacyjnie niezmiennicze nierówności Bella zadawaliśmy sobie pytanie, czy każda taka nierówność z m pomiarami na obserwatora jest zawsze łamana maksymalnie przez translacyjnie niezmiennicze stany i ten sam zbiór obserwabli dla każdego obserwatora. W [H8] pokazujemy, że mając dany N-cząstkowy stan kwantowy o wymiarze lokalnym d, który lamie maksymalnie pewną translacyjnie niezmienniczą nierówność Bella i realizujące to łamanie optymalne pomiary (w ogólności inne dla każdego obserwatora), pokazujemy jak skonstruować translacyjnie niezmienniczy stan o wyższym wymiarze lokalnym Nd i identyczne pomiary dla wszystkich obserwatorów, które osiągają to maksymalne łamanie. Wreszcie podajemy metodę numeryczną typu *see-saw* pozwalającą wyznaczyć maksymalne łamanie kwantowe translacyjnie niezmienniczych nierówności Bella przez translacyjnie niezmiennicze stany kwantowe o określonym wymiarze lokalnym i tych samych pomiarach dla wszystkich obserwatorów.

IV.7 Plany na przyszłość

Nielokalność w złożonych układach fizycznych jest interesującym zjawiskiem zarówno z fundamentalnego jak i aplikacyjnego punktu widzenia. Powyżej dokonaliśmy krótkiego przeglądu pewnych zagadnień dotyczących nielokalności, które zostały zbadane i przynajmniej częściowo rozwiązane w pracach [H1–H10]. Wciąż jednak pełne zrozumienie tego pojęcia oraz potencjału jaki w nim drzemie jest przed nami.

Poniżej wymieniam jeszcze kilka problemów, które mogą stanowić punkt wyjścia do dalszych badań nad nielokalnością.

- Okazuje się, że dwuciałowe nierówności Bella badane w pracach [H5,H8] mogą być powiązane z układami spinowymi wielu ciał, co zostało niedawno pokazane w [C25]. Jednak, praca ta dotyczy tylko łańcuchów spinowych, czyli układów o najniższym wymiarze przestrzennym. Warto więc rozważyć dwu lub trójwymiarowe układy spinowe w tym kontekście.

- Nielokalność znalazła interesujące zastosowanie w samotestowaniu, które pozwala uwierzytelnić obecność pewnego stanu kwantowego w urządzeniu kwantowym przy użyciu tylko statystycznych danych wytwarzanych przez to urządzenie [61]. Niedawno pokazano, że wszystkie dwucząstkowe czyste stany splatane mogą być samotestowane [62]. Jednak poza kilkoma wynikami dotyczącymi konkretnych stanów, niewiele wiadomo o przypadku wielocząstkowym. Ciekawym problemem było by więc poszukiwanie wydajnych metod samotestowania wszystkich splątanych stanów wielocząstkowych.

- Ciekawym z fundamentalnego punktu widzenia zagadnieniem pozostaje szukanie zasad informacyjnych, które pozwoliłyby wyróżnić zbiór korelacji kwantowych spośród wszystkich korelacji niesygnalizujących. Możliwym kierunkiem byłoby zbadanie jak mocno założenie LQT (opisane powyżej) oraz zasada lokalnej ortogonalności sformułowana w [C16,C17] ograniczają zbiór korelacji kwantowych.

RA

V. OMÓWIENIE POZOSTAŁYCH OSIĄGNIĘĆ NAUKOWO–BADAWCZYCH

A. DANE BIBLIOMETRYCZNE

- liczba publikacji: **50**
- łączna liczba cytowań bez autocytowań (wg. bazy Web of Science): **539**
- indeks Hirscha (wg. bazy Web of Science): **14**
- całkowity współczynnik wpływu: **205,3**

B. OSIĄGNIĘCIA PRZED UZYSKANIEM STOPNIA NAUKOWEGO DOKTORA

Poniżej opisane zostały badania, które prowadziłem przed uzyskaniem stopnia naukowego doktora wraz z otrzymanymi rezultatami. Artykuły są pogrupowane tematycznie i opatrzone krótkim wstępem zawierającym kontekst, który objaśnia motywację do podjęcia badań.

Rozpraszanie elektronów na nielokalnych potencjałach separowalnych. Badania te zostały wykonane w ramach mojej pracy magisterskiej z fizyki. Dotyczyły one zastosowania metody kanałów własnych sformułowanej przez Szmytkowskiego [63] do przypadku elastycznego rozpraszania elektronów na nielokalnych potencjałach separowalnych, dla których równanie Lippmana-Schwingera może być rozwiązane przy użyciu metod algebraicznych. W serii dwóch prac [B1,B2], w których rozważałem przypadki nierelatywistyczny i relatywistyczny, wyprowadziłem wzory na amplitudy rozpraszania oraz całkowite przekroje czynne wyrażone przez tak zwane wektory kanałów własnych (*eigenchannel vectors*) oraz własne przesunięcia fazowe (*eigenphaseshifts*). Oba obiekty są rozwiązaniami pewnego uogólnionego zagadnienia własnego. Jako przykład przedyskutowałem rozpraszanie elektronów na pewnym potencjale separowalnym typu δ o rzędzie jeden.

[B1] R. Augusiak, *Non–relativistic quantum scattering from non–local separable potentials: The eigenchannel approach*, Annalen der Physik **14**, 398 (2005).

[B2] R. Augusiak, *Scattering of Dirac particles from nonlocal separable potentials: The eigenchannel approach*, Physical Review C **75**, 064002 (2007).

Nielokalność w wielocząstkowych stanach kwantowych o splątaniu związanym. To jeden z głównych kierunków badawczych, którym podążałem podczas moich studiów doktoranckich na Politechnice Gdańskiej. Dotyczył on bardzo ciekawego, z fundamentalnego punktu widzenia, pytania, czy stany kwantowe o splątaniu związanym—czyli stany, z których nie można wydestylować czystych stanów splątanych—mogą łamać nierówności Bella (lub, równoważnie, czy mogą być nielokalne) [64]. W serii trzech artykułów inni autorzy podali przykłady wielocząstkowych stanów kwantowych o splątaniu związanym, które łamią nierówności Bella [65, 66, 67]. Stan o najmniejszej liczbie podukładów, znaleziony w [67], składa się z sześciu kubitów, ale do udowodnienia, że jest on nielokalny użyto tzw. funkcjonalnej nierówności Bella, która wymaga ciągłych klas pomiarów. Pytanie jaki jest minimalny

RA

rozmiar stanu kwantowego (w terminach liczby podukładów) o splątaniu związanym, który łamałby nierówności Bella pozostawało wciąż otwarte.

Wraz z promotorem mojej pracy doktorskiej prof. P. Horodeckim włączyliśmy się w ten nurt badań. W [B3] pokazaliśmy, że czterokubitowy stan kwantowy o splątaniu związanym wprowadzony przez Smolina [68], łamie maksymalnie pewną nierówność Bella, która jest uogólnieniem znanej nierówności CHSH [27]. Zatem nie tylko zmniejszyliśmy liczbę cząstek w stanie o splątaniu związanym, który przejawia nielokalność do czterech, ale także wykazaliśmy, że stany niedestylowalne mogą łamać nierówności Bella maksymalnie. Co więcej rozważany przez nas scenariusz jest bardzo prosty z ekperymentalnego punktu widzenia, ponieważ wymaga on tylko dwóch pomiarów na obserwatora oraz otrzymane łamanie jest odporne na biały szum. W istocie, nasze teoretyczne przewidywania zostały później potwierdzone eksperymentalnie [69, 70].

W [B4] uogólniliśmy wyniki z [B3] na dowolną parzystą liczbę cząstek większą niż trzy. Po pierwsze, zaproponowaliśmy metodę konstrukcji wielocząstkowych stanów kwantowych zachowującą pewne kluczowe własności czterokubitowego stanu Smolina. Następnie podaliśmy prostą konstrukcję wielocząstkowych nierówności Bella łamanych maksymalnie przez te stany, a także przesudiowaliśmy ich odporność na biały szum. Wreszcie pokazaliśmy, że pomimo tego, że nasze stany są niedestylowalne, to mogą one być użyteczne w różnych protokołach kwantowo-informacyjnych takich jak na przykład koncentracja odległej informacji (*remote information concentration*), uogólniając tym samym wyniki pracy [71].

[B3] R. Augusiak, P. Horodecki, *Bound entanglement maximally violating Bell inequalities: Quantum entanglement is not fully equivalent to cryptographic security*, Physical Review A **74**, 010305(R) (2006).

[B4] R. Augusiak, P. Horodecki, *Generalized Smolin states and their properties*, Physical Review A **73**, 012318 (2006).

Destylacja klucza kryptograficznego z wielocząstkowych stanów o splątaniu związanym. Drugim głównym kierunkiem badań, który podjąłem podczas studiów doktoranckich, komplementarnym do wyżej opisanych badań, było pytanie czy można destylować klucz kryptograficzny ze stanów o splątaniu związanym. To pytanie pozostawało otwarte przez długi czas do momentu aż w 2005 roku Horodeccy wraz ze współpracownikami sformułowali ogólną teorii destylacji klucza kryptograficznego z dwupodukładowych stanów kwantowych [24, 25], w ramach której udowodnili, że z pewnych stanów kwantowych o splątaniu związanym można otrzymać bezpieczny klucz kryptograficzny.

Wraz z moim promotorem zajęliśmy się tą tematyką. Po pierwsze, w ramach rozgrzewki, udowodniliśmy w [B5], że każdy tak zwany stan prywatny—stan, z którego można wydestylować $\log_2 d$ bitów idealnie bezpiecznego klucza kryptograficznego (tutaj d oznacza wymiar lokalny tak zwanej części klucza stanu)—jest destylowalny przez lokalne operacje i klasyczną komunikację. Podaliśmy także alternatywny dowód tego, że koszt splątania, który jest jedną z miar splątania, jest ograniczeniem górnym na destylowalny klucz kryptograficzny, co zostało wcześniej udowodnione w pracach [24, 25]. Po drugie, w pracy [B6] podaliśmy nową konstrukcję dwucząstkowych stanów kwantowych o splątaniu związanym, które mają niezerowy destylowalny klucz kryptograficzny. Po trzecie, w [B7] uogólniliśmy wyniki prac [24, 25] na

RA

przypadek wielu cząstek i podaliśmy konstrukcję wielocząstkowych stanów kwantowych o splątaniu związanym, z których można destylować klucz kryptograficzny. Wreszcie w [B8] podaliśmy alternatywną konstrukcję takich stanów, tym razem wykorzystując strukturę stanów *W* (jeden z symetrycznych stanów Dicke'go z jednym wzbudzeniem) i udowodniliśmy, że mają one niezerowy destylowalny klucz przez zaadaptowanie idei losowej destylacji splątania zaproponowanej w [72].

Pomimo tego, że artykuły [B7,B8] zostały opublikowane po otrzymaniu przeze mnie stopnia naukowego doktora, wyniki w nich zamieszczone tworzą znaczną część mojej pracy doktorskiej.

[B5] P. Horodecki, R. Augusiak, *Quantum states representing perfectly secure bits are always distillable*, Physical Review A **74**, 010302(R) (2006).

[B6] P. Horodecki, R. Augusiak, *On quantum cryptography with bipartite bound entangled states*, in *Quantum Information Processing: From Theory to Experiment*, NATO Science Series III, Vol. 199 (edited by D. G. Angelakis *et al.*), IOS Press, Amsterdam, 2006, pp. 19–29.

[B7] R. Augusiak, P. Horodecki, *Multipartite secret key distillation and bound entanglement*, Physical Review A **80**, 042307 (2009).

[B8] R. Augusiak, P. Horodecki, *W-like bound entangled states and secure key distillation*, Europhysics Letters **85**, 50001 (2009).

Wielokopiowe świadki splątania. Splątanie, oprócz swojego fundamentalnego znaczenia, jest także kluczowym zasobem w pewnych informacyjnych zadaniach, których realizacja w ramach fizyki klasycznej jest niemożliwa (zob. [73]). Zatem jego detekcja w złożonych układach kwantowych (dwucząstkowych i wielocząstkowych) była i wciąż jest jednym z głównych nierozwiązanych problemów informatyki kwantowej (zob. [74]).

Niezależnie od tematyki badawczej opisanej powyżej, zajmowałem się także rozwijaniem kryteriów pozwalających wykrywać splątanie w układach kwantowych, kładąc szczególny nacisk na ich stosowalność w eksperymencie. W szczególności interesowały mnie tak zwane wielokopiowe świadki splątania [75], czyli obserwable kwantowe, których wartości średnie mierzone na wielu kopiach tego samego stanu kwantowego pozwalają wykryć jego splątanie.

Najpierw w pracy [B9] pokazaliśmy, że każde odwzorowanie dodatnie, ale nie kompletnie dodatnie, może być pośrednio użyte w eksperymentalnej detekcji splątania przez pomiary wartości oczekiwanych pewnych wielokopiowych obserwabli, uogólniając wyniki Carteret [76] otrzymane jedynie dla transpozycji. Należy podkreślić w tym momencie, że odwzorowania dodatnie, ale nie kompletnie dodatnie nie reprezentują żadnych procesów fizycznych, jako że ich działanie na jeden z podukładów splątanego stanu kwantowego może prowadzić do macierzy, która nie jest dodatnia, a więc nie opisuje żadnego stanu kwantowego. Zatem odwzorowania takie nie mogą być bezpośrednio wykorzystane w eksperymencie, którego celem jest weryfikacja czy dany stan kwantowy jest splątany czy nie. Zaletą naszego podejścia jest to, że nie wykorzystuje ono tak zwanego strukturalnego przybliżenia fizycznego (*structural physical approximation (SPA)*) [75, 77, 78], to znaczy nie wymaga stucznego dodawania szumu do układu.

RA

W pracy [B10] udowodniliśmy, że splątanie wszystkich dwukubitowych stanów kwantowych może być wykryte przez jednego świadka nieliniowego, którego wartość średnia jest mierzona na czterech kopiach danego stanu kwantowego (ten sam świadek dla wszystkich stanów). Nasz rezultat implikuje możliwość stworzenia układu kwantowego, który po włożeniu do niego czterech kopii nieznanej macierzy gęstości, rozstrzygałby czy jest ona splątana czy nie.

Następnie, we współpracy z P. Horodeckim i J. Stasińską, rozwijałem różne nowe konstrukcje silnych kryteriów splątania, które mogłyby być eskperymentalnie zaimplementowane przez pomiar pewnych świadków splątania na wielu kopiach stanu [B11,B12]. Kryteria te mogą być postrzegane jako uogólnienie entropijnych kryteriów splątania, początkowo sformułowanych dla entropii von Neumanna w [79], później uogólnionych dla entropii Rényi'ego i Tsallisa w [80, 81]. Co ciekawe, w przeciwieństwie do kryteriów entropijnych, nasze kryteria wykrywają splątanie związane.

Wreszcie w pracy [B13] podaliśmy alternatywne sformułowanie problemu separowalności. Mianowicie pokazaliśmy, że separowalność dwucząstkowych stanów kwantowych działających na przestrzeni o dowolnym wymiarze lokalnym jest równoważna pytaniu czy pewien świadek splątania działający na dwóch kopiach danej przestrzeni Hilberta jest słabo optymalny (*weakly optimal*), to znaczy hiperpłaszczyzna, którą on generuje ma nietrywialną część wspólną ze zbiorem stanów separowalnych. Dzięki temu problem separowalności można przeformułować jako pewien problem optymalizacyjny, który w pewnych przypadkach powinien być rozwiązywalny. Artykuł [B13] został całkowicie stworzony w czasie moich studiów doktoranckich, ale opublikowany w czasopiśmie dużo później.

[B9] P. Horodecki, R. Augusiak, M. Demianowicz, *General construction of noiseless networks detecting entanglement with the help of linear maps*, Physical Review A **74**, 052323 (2006).

[B10] R. Augusiak, M. Demianowicz, P. Horodecki, *Universal observable detecting all two-qubit entanglement and determinant-based separability tests*, Physical Review A **77**, 030301(R) (2008).

[B11] R. Augusiak, J. Stasińska, *General scheme for construction of scalar separability criteria from positive maps*, Physical Review A **77**, 010303(R) (2008).

[B12] R. Augusiak, J. Stasińska, P. Horodecki, *Beyond the standard entropic inequalities: Stronger scalar separability criteria and their applications*, Physical Review A **77**, 012333 (2008).

[B13] P. Badziąg, P. Horodecki, R. Horodecki, R. Augusiak, *Separability in terms of a single entanglement witness*, Physical Review A **88**, 010301(R) (2013).

Splątanie związane w dwucząstkowych stanach kwantowych niezmienniczych ze względu na obroty. W kolejnym projekcie, odrębnym od tematyki mojej pracy doktorskiej, badałem, wraz z J. Stasińską, splątanie związane w dwucząstkowych stanach kwantowych, które są niezmiennicze ze względu na obustronne działanie grupy $SO(3)$ (dla prostoty nazywane również stanami niezmienniczymi ze względu na obroty). Głównym wynikiem otrzymanym przez nas jest fakt, że pośród takich stanów, których jeden z lokalnych wymiarów jest parzysty, zawsze istnieją stany o splątaniu związanym [B14]. Nasz rezultat uzupełnia wcześniejszą prace Breuera, której celem była charakteryzacja stanów niezmienniczych ze względu na obroty w

RA

przypadku, gdy jeden z podukładów ma wymiar trzy [82]. Pokazał on w szczególności, że jeśli wymiar drugiego podukładu jest nieparzysty, to nie istnieją splątane stany PPT niezmiennicze na działanie obrotów, co oznacza, że transpozycja częściowa jest warunkiem koniecznym i dostatecznym splatątania dla tych stanów.

[B14] R. Augusiak, J. Stasińska, *Rotationally invariant states and bound entanglement*, Physics Letters A **363**, 182 (2007).

C. BADANIA PO UZYSKANIU STOPNIA NAUKOWEGO DOKTORA NIE WCHODZĄCE W SKŁAD HABILITACJI

Poniżej zamieszczam opis rezultatów uzyskanych po otrzymaniu stopnia doktora. Opis ten podzieliłem na dwie części: pierwsza dotyczy splątania, a druga nielokalności. Podobnie jak wyżej, artykuły są pogrupowane tematycznie i opatrzone krótkim wstępem zawierającym kontekst, który objaśnia motywację do podjęcia badań.

C.1. SPLĄTANIE

Wielokopiowe świadki splątania–ciąg dalszy. W czasie mojego pobytu na stażu podoktorskim w ICFO kontynuowałem badania nad świadkami wielokopiowymi. Owocem tego jest praca [C1], w której wprowadziliśmy ogólną konstrukcję koniecznych kryteriów separowalności z odwzorowań dodatnich, sformułowanych przy użyciu pojęcia słabej majoryzacji. Kryteria te mogą być postrzegane jako uogólnienia kryterium majoryzacyjnego wprowadzonego przez Nielsena i Kempe [83]. Wykorzystując związek słabej majoryzacji z funkcjami wklęsłymi w sensie Schura, nasze kryteria implikują skalarne warunki separowalności, które mogą być testowane przez pomiary pewnych wielokopiowych świadków splątania.

Powyższy kierunek badań zwieńczyłem pracą przeglądową [C2], napisaną wspólnie z M. Lewensteinem, w której opisałem znane metody ograniczania miar splątania przez pewne wielkości mierzalne, między innymi obserwable wielokopiowe.

[C1] R. Augusiak, J. Stasińska, *Positive maps, majorization, entropic inequalities and detection of entanglement*, New Journal of Physics **11**, 053018 (2009).

[C2] R. Augusiak, M. Lewenstein, *Towards measurable bounds on entanglement measures*, Quantum Information Processing **8**, 493–521 (2009).

Ekstremalne splątane stany PPT. Charakteryzacja splątania w złożonych stanach kwantowych z dodatnimi transpozycjami częściowymi (zwane dalej stanami PPT od angielskiego *positive partial transposition*) jest niewątpliwie trudnym problemem (zob. [73, 74]). Jedną z przyczyn jest brak uniwersalnego kryterium separowalności, które umożliwiłoby jednoznaczne rozróżnienie stanów separowalnych od pozostałych stanów PPT, które są splątane (warto wspomnieć, że znanych jest wiele koniecznych warunków separowalności; zob. [74]). Istnieją jednak metody pozwalające uzyskać pewien wgląd w strukturę splątanych stanów PPT. Jedna z nich wykorzystuje fakt, że wszystkie macierze gęstości, kóre pozostają dodatnie po zadziałaniu na nie

RA

transpozycji częściowej tworzą zbiór wypukły, który jako podzbiór właściwy zawiera splątane stany PPT. Zatem aby scharakteryzować ten zbiór wypukły wystarczy wyznaczyć wszystkie jego elementy ekstremalne.

W pracy [C3] sformułowaliśmy kryterium, które pozwala sprawdzić czy dany stan PPT jest ekstremalny w zbiorze wszystkich stanów PPT przez rozwiązanie pewnego układu równań liniowych. Następnie pokazaliśmy, że kryterium to można łatwo przekuć w efektywny algorytm pozwalający wyznaczać stany ekstremalne zbioru stanów PPT. Przestudiowaliśmy także własności ekstremalnych splątanych stanów PPT w konkretnych przetrzeniach Hilberta takich jak $\mathbb{C}^2 \otimes \mathbb{C}^4$, $(\mathbb{C}^2)^{\otimes 3}$ oraz $(\mathbb{C}^2)^{\otimes 4}$. Należy zauważyć, że to samo kryterium zostało niezależnie sformułowane w pracy [84].

[C3] R. Augusiak, J. Grabowski, M. Kuś, M. Lewenstein, *Searching for extremal PPT entangled states*, Optics Communications **283**, 805 (2010).

Kwantowe kinetyczne modele Isinga. Zajmowałem się także zastosowaniami teorii splątania w fizyce układów wielu ciał. We współpracy z F. Haakem z Duisburga (Niemcy) zaproponowaliśmy w [C4] kwantowe uogólnienia klasycznych kinetycznych modeli Isinga, opisywane przez pewną klasę wielociałowych kwantowych równań master. Podobnie jak w przypadku klasycznych modeli spełniających warunek równowagi szczegółowej, które są równoważne układom hamiltonowskim, nasze modele można traktować jako zbiór takich układów hamiltonowskich wyznaczających dynamikę elementów macierzowych wielociałowej macierzy gęstości. Stany podstawowe odpowiadających im hamiltonianów da się dobrze opisać przez pewne czyste stany kwantowe o ograniczonym splątaniu (*matrix product states* lub *pair entangled projected states*). Przedyskutowaliśmy własności krytyczne tych hamiltonianów, a także splątanie w ich niskoenergetycznych stanach własnych.

Projekt ten kontynuowaliśmy w pracy przeglądowej [C5], w której z jednej strony badaliśmy inne modele kinetyczne, a z drugiej strony opisaliśmy najnowsze dokonania w fizyce wielu ciał z perspektywy informatyki kwantowej, takie jak na przykład prawa powierzchni (*area laws*).

[C4] R. Augusiak, F. M. Cucchietti, F. Haake, and M. Lewenstein, *Quantum kinetic Ising models*, New Journal of Physics **12**, 025021 (2010).

[C5] R. Augusiak, F. M. Cucchietti, M. Lewenstein, *Many body physics from a quantum information perspective*, in: *Modern Theories of Many-Particle Systems in Condensed Matter Physics* (eds. D. C. Cabra, A. Honecker, and P. Pujol), Lecture Notes in Physics **843**, pp. 245–294 (2012).

Optymalność świadków splątania. Świadki splątania stanowią jedną z najważniejszych metod detekcji splątania w układach kwantowych [17]. Wynika to z faktu, że są one kwantowymi obserwablami i jako takie mogą być wykorzystane w eksperymentalnej weryfikacji splątania. Co więcej, ich wartości oczekiwane mogą wiele powiedzieć o tym, jak bardzo splątany jest dany stan kwantowy (zob. [85]). Konstrukcja świadków splątania wykorzystuje geometrię zbioru stanów separowalnych: dla każdego stanu splątanego istnieje hiperpłaszczyzna, reprezentowana przez operator hermitowski, bedący właśnie świadkiem splątania, który „oddziela" ten stan od zbioru stanów separowalnych. Szczególnie ważne są tak

RA

zwane optymalne świadki splątania [86], czyli te, które wykrywają „największe" zbiory stanów splątanych. W serii prac opublikowanych w latach 2011-2014 badałem pewne zagadnienia dotyczące optymalności świadków splątania.

W [C6,C7] naszym celem była charakteryzacja optymalnych świadków splątania, które są rozkładalne, to znaczy dają się zapisać jako suma operatora dodatniego i transpozycji częściowej operatora dodatniego. Po pierwsze, w [C6] podaliśmy pełną charakteryzację takich świadków działających na przestrzeni Hilberta $\mathbb{C}^2 \otimes \mathbb{C}^d$. W szczególności pokazaliśmy, są one optymalne wtedy i tylko wtedy, gdy mają tak zwaną własność rozpinania: zbiór wektorów produktowych leżących w płaszczyźnie wyznaczanej przez takiego świadka rozpina całą przestrzeń Hilberta. Następnie we współpracy z G. Sarbickim z Torunia udowodniliśmy, że w przeciwieństwie do przypadku $\mathbb{C}^2 \otimes \mathbb{C}^d$, w wyżej wymiarowych przestrzeniach Hilberta istnieją optymalne świadki rozkładalne, które nie mają własności rozpinania [C7], co wcześniej udowodnione zostało tylko dla świadków nierozkładalnych.

Z drugiej strony w [C8,C9] badaliśmy hipotezę sformułowaną w [87], która mówi, że strukturalne przybliżenia fizyczne (SPA) optymalnych świadków splątania są separowalnymi stanami kwantowymi lub, równoważnie, że strukturalne przybliżenia fizyczne optymalnych map dodatnich są kanałami niszczącymi splątanie. Przypomnijmy, że SPA to metoda pozwalająca na eksperymentalną implementację odwzorowań dodatnich, ale nie kompletnie dodatnich, która została wprowadzona i zbadana w serii prac [77, 78, 75]. W [C8] podaliśmy kolejne przykłady optymalnych świadków splątania, które spełniają powyższa hipotezę; w szczególności pokazaliśmy, że optymalny świadek splątania powstający przez zastosowanie transpozycji częściowej do dowolnego czystego stanu splątanego spełnia tę hipotezę. Z drugiej strony sformułowaliśmy i udowodniliśmy jej słabszą wersję: dla dowolnego świadka splątania W (równoważnie, mapy dodatniej Λ) istnieje stan separowalny ρ (kanał niszczący splątanie Φ) taki, że SPA świadka W (Λ) skonstruowane za pomocą ρ (Φ) jest znowu stanem separowalnym (kanałem niszczącym splątanie). Wreszcie w [C9] dowodzimy, że świadek splątania skonstruowany przez Ha i Kye [88] w celu obalenia powyższej hipotezy w istocie nie jest świadkiem optymalnym. Warto wspomnieć, że hipoteza ta została ostatecznie obalona w [89, 90].

[C6] R. Augusiak, J. Tura, and M. Lewenstein, *A note on the optimality of decomposable entanglement witnesses and completely entangled subspaces*, Journal of Physics A: Mathematical and Theoretical **44**, 212001 (2011). **(Editorial highlight in 2011)**

[C7] R. Augusiak, G. Sarbicki, and M. Lewenstein, *Optimal decomposable witnesses revisited*, Physical Review A **84**, 052323 (2011).

[C8] R. Augusiak, J. Bae, Ł. Czekaj, and M. Lewenstein, *On structural physical approximations and entanglement breaking maps*, Journal of Physics A: Mathematical and Theoretical **44**, 185308 (2011).

[C9] R. Augusiak, J. Bae, J. Tura, and M. Lewenstein, *Checking the optimality of entanglement witnesses: an application to structural physical approximations*, Journal of Physics A: Mathematical and Theoretical **47**, 065301 (2014). **(Editorial highlight in 2014)**

Splątanie PPT w wielocząstkowych stanach symetrycznych. Ze względu na ostatnie postępy w eksperymentalnym wytwarzaniu różnych ciekawych stanów kwantowych wielu ciał ([55,

RA

56, 91]), wzrosło znaczenie problemu separowalności w przypadku wielocząstkowym. W porównaniu z przypadkiem dwucząstkowym, tutaj problem ten jest jeszcze bardziej skomplikowany, bowiem nie tylko chcemy odpowiedzieć na pytanie, czy dany stan jest splątany, ale także chcemy stwierdzić jaki ma rodzaj splątania; przypomnijmy, że dany wielocząstkowy stan kwantowy może być splątany na wiele sposobów (zob. [73]). Szczególnie trudnym problemem jest charakteryzacja tych stanów wielocząstkowych, które maja wszystkie częściowe transpozycje dodatnie (stany PPT). W serii dwóch prac [C10,C11] zajęliśmy się tym problemem, ale aby go znacząco uprościć, rozważaliśmy wielokubitowe stany symetryczne, to znaczy te stany, które są zdefiniowane na podprzestrzeni symetrycznej wielokubitowej przestrzeni Hilberta.

W [C10] pokazaliśmy, że istnieją czterokubitowe symetryczne splątane stany PPT, odpowiadając na pytanie czy częściowa transpozycja jest koniecznym i dostatecznym warunkiem separowalności w takich układach (przypomnijmy, że tak jest w przypadku trzykubitowych symetrycznych stanów PPT). W tym celu użyliśmy dwóch metod: pierwsza półanalityczna, która pozwala na konstrukcję wielokubitowych splątanych stanów PPT z pewnej klasy kubitowo-kuditowych splątanych stanów PPT, a druga, oparta na algorytmie z pracy [C3], polegała na szukaniu ekstremalnych splątanych stanów PPT. Następnie przestudiowaliśmy separowalność czterokubitowych symetrycznych stanów PPT biorąc pod uwagę ich rzędy i rzędy macierzy otrzymanych po zaaplikowaniu różnych transpozycji częściowych.

W [C11] kontynuowaliśmy charakteryzację wielocząstkowych symetrycznych stanów PPT, mając na celu uogólnienie wyników i metod zawartych w [C10] na układy składające się z dowolnej liczby cząstek. Wyprowadziliśmy kryteria separowalności dla takich stanów sformułowane w kategoriach ich rzędów i rzędów ich częściowych transpozycji. Co ciekawe, w większości przypadków, symetryczne stany PPT są albo separowalne, albo typowo separowalne. Następnie przestudiowaliśmy tak zwane stany brzegowe (*edge states*) w tych układach, pokazując w szczególności, że aby scharakteryzować generyczne stany PPT splątane o czterech lub pięciu kubitach, wystarczy przestudiować tylko takie, które mają kilka specyficznych konfiguracji ranków. Wreszcie, używając algorytmu z pracy [C3] wyznaczaliśmy numerycznie ekstremalne stany PPT splątane w stanach symetrycznych składających się $N \leq 23$ kubitów. Warto wspomnieć, że dla układów składających się z nieparzystej liczby kubitów znaleźliśmy tylko jeden układ rzędów, w którym mogą istnieć ekstremalne, splątane stany PPT.

[C10] J. Tura, R. Augusiak, P. Hyllus, M. Kuś, J. Samsonowicz, M. Lewenstein, *Four-qubit PPT entangled symmetric states*, Physical Review A **85**, 060302(R) (2012).

[C11] R. Augusiak, J. Tura, J. Samsonowicz, M. Lewenstein, *Entangled symmetric states of N qubits with positive partial transpositions*, Physical Review A **86**, 042316 (2012).

Dystrybucja splątania. W [C12] gruntownie przebadaliśmy problem dystrybucji splątania pomiędzy dwoma odległymi obserwatorami. Naszym celem było zrozumienie jak dużo splątania można otrzymać poprzez przesłanie cząstki kwantowej od jednego obserwatora do drugiego w scenariuszach z szumem i bez szumu, a także w przypadku, w którym obserwatorzy współdzielą pewnie korelacje przed wykonaniem protokołu.

[C12] A. Streltsov, R. Augusiak, M. Demianowicz, M. Lewenstein, *Progress towards a unified approach to entanglement distribution*, Physical Review A **92**, 012335 (2015).

RA

Dostateczne kryteria separowalności z odwzorowań dodatnich. W pracy [C13] przestudiowaliśmy globalne (na oba podukłady) działanie klas odwzorowań dodatnich i kompletnie dodatnich na dwuciałowe stany kwantowe. Zaobserwowaliśmy, że dla pewnych odwzorowań takich jak odwzorowanie redukcyjne [36] lub odwzorowanie wprowadzone przez Breuera i Halla [92, 93], otrzymane macierze są zawsze separowalne (w ogólności nieunormowane). To pozwoliło wyprowadzić rodziny dostatecznych kryteriów separowalności, które są mniej powszechne w literaturze i trudniejsze w wyprowadzeniu niż konieczne kryteria separowalności. Podaliśmy także konkretne przykłady dla stanów kwantowych działających na przestrzeniach Hilberta o dowolnym wymiarze lokalnym, ze szczególnym uwzględnieniem przypadku, w którym jeden z podukładów jest kubitem. Część z tych kryteriów można uogólnić tak, aby wykrywały także tak zwaną liczbę Schmidta (*Schmidt number*). Nasze wyniki uogólniają znany rezultat, który mówi, że w dostatecznie bliskim sąsiedztwie stanu kompletnie zdepolaryzowanego (unormowana macierz identycznościowa), wszystkie stany kwantowe są separowalne [94].

[C13] M. Lewenstein, R. Augusiak, D. Chruściński, S. Rana, J. Samsonowicz, *Sufficient separability criteria and positive maps*, Physical Review A **93**, 042335 (2016).

Użyteczność wielocząstkowego splątania w metrologii kwantowej. Kolejną tematyką badań, którą się zajmowałem w czasie mojego pobytu w ICFO w Hiszpanii, a którą potem kontynuowałem w CFT w Warszawie, było badanie związku pomiędzy splątaniem w wielocząstkowych stanach kwantowych i ich użytecznością w metrologii kwantowej (zob. [95]).

W [C14] wyprowadziliśmy relację ciągłości dla kwantowej informacji Fishera w przypadku estymacji fazy, która pozwoliła nam powiązać ją z geometrią stanów kwantowych, a w szczególności z geometryczną miarą splątania [96]. Pokazaliśmy także, że skalowanie precyzji w estymacji fazy wraz z ilością cząstek dowolnie bliskie tzw. granicy Heisenberga, która wyznacza maksymalną możliwą dokładność w ramach metrologii kwantowej, jest osiągalne pomimo asymptotycznie znikającego splątania.

Następnie, w [C15] przebadaliśmy użyteczność losowych stanów kwantowych w paradygmatycznych scenariuszach interferencyjnych. Pokazujemy, że typowe czyste stany wielu rozróżnialnych cząstek, pomimo tego, że są mocno splątane, nie oferują asymptotycznej przewagi w estymacji parametrycznej nad strategiami klasycznymi. Z drugiej strony pokazujemy, że symetryczne (bozonowe) stany kwantowe, nawet jeśli wybierane w losowy sposób, taką przewagę pozwalają osiągnąć; w istocie, kwantowa informacja Fishera dla typowych stanów z przestrzeni symetrycznej skaluje się kwadratowo z liczbą cząstek. Co więcej, dowodzimy, że to polepszenie może być uzyskane w obecności szumu i strat skończonej liczby cząstek, oraz przy użyciu ustalonego pomiaru kwantowego (tego samego dla różnych stanów).

[C14] R. Augusiak, J. Kołodyński, A. Streltsov, M. N. Bera, A. Acín, M. Lewenstein, *Asymptotic irrelevance of entanglement in quantum metrology*, Physical Review A **94**, 012339 (2016).

[C15] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acín, M. Lewenstein, *Random symmetric states for robust quantum metrology*, Physical Review X **6**, 041044 (2016).

RA

C.2. NIELOKALNOŚĆ

Zasady informacyjne dla korelacji kwantowych. Jak już wspomniano, zrozumienie struktury korelacji kwantowych pozostaje fundamentalnym problemem otwartym. W szczególności nie znamy żadnego intuicyjnego, a jednocześnie operacyjnego kryterium pozwalającego odpowiedzieć na pytanie, które korelacje nielokalne są kwantowe, czyli będące wynikiem pomiarów lokalnych na złożonych stanach kwantowych. Pierwszy rezultat uzyskany w celu odpowiedzenia na powyższe pytanie, podany przez Popescu i Rohrlicha [12], to dowód, że zasada o dobrze ugruntowanej pozycji w fizyce jaką jest zasada niesygnalizowania, mówiąca, że informacja nie może się rozchodzić z prędkością większą od prędkości światła, jest niewystarczająca, aby opisać zbiór korelacji kwantowych; istnieją korelacje nielokalne spełniające zasadę niesygnalizowania, które nie mają kwantowej realizacji. Ten zaskakujący wynik sprowokował poszukiwanie innych zasad o informacyjnej naturze, które mogłyby wyróżnić zbiór korelacji kwantowych spośród wszystkich korelacji nielokalnych. Zaowocowało to sformułowaniem kilku takich zasad w przypadku dwuciałowym: nietrywialna złożoność komunikacyjna *(nontrivial communication complexity)* [13], zasada braku kwantowej przewagi w obliczeniach nielokalnych *(no quantum advantage in nonlocal computation (no-NLC))* [16], przyczynowość informacyjna *(information causality)* [14], bądź rzeczywistość makrospokowa *(macroscopic reality)* [97].

W czasie stażu podoktorskiego włączyłem się w tę linię badań, uzyskując, we współpracy z wieloma naukowcami, kilka ciekawych wyników.

Po pierwsze, żadna z powyższych zasad dwuciałowych nie pozwala na dokładny opis korelacji kwantowych w przypadku wielocząstkowym [98], a z drugiej strony żadna prawdziwie wielociałowa zasada nie została sformułowana. W [C16,C17], opierając się na wynikach pracy [H9], sformułowaliśmy i drobiazgowo przestudiowaliśmy prawdziwie wielocząstkową zasadę, którą nazwaliśmy zasadą lokalnej ortogonalności *(local orthogonality)*. Aby ją przebadać wykorzystaliśmy związek nierówności Bella bez kwantowego łamania z pewnymi pojęciami teorii grafów takimi jak kliki. Jednak jak pokazano w [99], jest ona „zbyt słaba", aby w pełni scharakteryzować zbiór korelacji kwantowych.

Z drugiej strony, w [C18] rozważaliśmy uogólnienie zasady no-NLC na przypadek dowolnej liczby wyników, pokazując, że kwantowa teoria nie daje przewagi nad korelacjami klasycznymi w zadaniu nielokalnych obliczeń dla pewnej klasy funkcji z d wynikami, przy d będącym liczbą pierwszą, podczas gdy ogólne korelacje niesygnalizujące taką przewagę pozwalają uzyskać. W tym celu wyprowadziliśmy ograniczenie górne na maksymalna kwantową wartość gier liniowych (równoważnie, liniowych nierówności Bella), które potem użyliśmy do sformułowania kilku ciekawych własności tak zwanych gier XOR-d (podklasa gier liniowych) dla d będącego liczbą pierwszą. Ograniczenie to zilustrowaliśmy na przykładzie tak zwanej nierówności Bella CHSH-d, gdzie d jest liczbą pierwszą bądź potęgą liczby pierwszej [100], otrzymując to samo ograniczenie górne, które zostało wyprowadzone alternatywnymi, bardziej technicznymi metodami. Następnie w [C19] uogólniliśmy to ograniczenie i użyliśmy go do przebadania optymalności (*tightness*) pewnych korelacyjnych nierówności Bella, które nie mają kwantowego łamania.

[C16] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, A. Acín, *Local Or-*

RA

thogonality: a multipartite principle for correlations, Nature Communications **4**, 2263 (2013).

[C17] A. B. Sainz, T. Fritz, R. Augusiak, J. Bohr Brask, R. Chaves, A. Leverrier, A. Acín, *Exploring the Local Orthogonality Principle*, Physical Review A **89**, 032117 (2014).

[C18] R. Ramanathan, R. Augusiak, G. Murta, *XOR games with d outcomes and the task of non-local computation*, Physical Review A **93**, 022333 (2016).

[C19] R. Ramanathan, M. T. Quintino, A. B. Sainz, G. Murta, R. Augusiak, *On the tightness of correlation inequalities with no quantum violation*, Physical Review A **95**, 012139 (2017).

Aksjomatyzacja mechaniki kwantowej. Teoria kwantów jest pierwszą teorią, która poprawnie opisuje świat na poziomie pojedynczych cząstek. To kontrastuje z naszym ograniczonym zrozumieniem samej mechaniki kwantowej. W szczególności jej standardowe postulaty sformułowane są za pomocą abstrakcyjnych pojęć matematycznych takich jak przestrzenie Hilberta i operatory na nich działające, a przez to trudno im nadać jasną fizyczną interpretację. W ostatnich latach pojawiła się fala alternatywnych aksjomatyzacji teorii kwantowej z zastosowaniem bardziej fizycznego i mniej matematycznego podejścia (zob. [101]).

W [C20] zaproponowaliśmy kolejny zbiór aksjomatów i pokazaliśmy, że abstrakcyjny formalizm mechaniki kwantowej może być z nich całkowicie wyprowadzony. W przeciwieństwie do poprzednich prac, nasza aksjomatyzacja ma jasną i bezpośrednią fizyczną interpretację. Aby ją skonstruować, w [C21] przebadaliśmy wszystkie teorie fizycznych układów dwuciałowych spełniające dwa z naszych aksjomatów, przy założeniu, że przestrzeń stanów każdego z podukładów ma geometrię kuli euklidesowej o dowolnym wymiarze (przypomnijmy, że w standardowej mechanice kwantowej kubit jest opisywany przez kulę o wymiarze trzy, zwaną także kulą Blocha). Okazuje się, że we wszystkich takich teoriach, poza mechaniką kwantową właśnie, układy z dwoma rozróżnialnymi stopniami swobody nie oddziałują ze sobą, a więc nie mogą być splątane i łamać nierówności Bella.

[C20] Ll. Masanes, M. P. Müller, R. Augusiak, D. Pérez-García, *Existence of an information unit as a postulate of quantum theory*, Proceedings of the National Academy of Sciences **110**, 16373 (2013).

[C21] Ll. Masanes, M. P. Müller, D. Perez-García, R. Augusiak, *Entangling dynamics beyond quantum theory*, Journal of Mathematical Physics **55**, 122203 (2014).

Nierównoważność splątania kwantowego, sterowalności i nielokalności w przypadku dwucząstkowym. Zjawisko sterowalności (ang. *steering*) Einsteina, Podolsky'ego i Rosena (EPR), zauważone już przez Schrödingera, jest jedną z form korelacji w teorii kwantowej. (zob. [42]). Pomimo dużego zainteresowania tym zjawiskiem, pytanie czy ta forma korelacji kwantowych jest nierównoważna splątaniu i nielokalności Bella pozostało otwarte. Mówiąc dokładniej nie było jasne, czy istnieją splątane stany kwantowe, które są bezużyteczne w sterowalności, a z drugiej strony, czy istnieją stany użyteczne w sterowalności, które nie mogą prowadzić do łamania nierówności Bella. Choć taka nierównoważność została już udowodniona dla szczególnego przypadku pomiarów rzutowych [42, 37, 102, 103], pytanie czy pozostałaby ona prawdziwa gdyby wziąć pod uwagę wszystkie możliwe pomiary kwantowe

RA

pozostało otwarte. Głównym celem pracy [C22] było znalezienie odpowiedzi na to pytanie. Udowodniliśmy, że sterowalność kwantowa jest rzeczywiście pojęciem nierównoważnym splątaniu i nielokalności Bella dla wszystkich możliwych pomiarów kwantowych; skonstruowaliśmy przykłady stanów splątanych, które nie prowadzą do zjawiska sterowalności, a także przykłady sterowalnych stanów kwantowych, które nie łamią żadnej nierówności Bella. Wykazujemy także, że istnieją stany, które są sterowalne w jedną stronę, ale nie w obie strony. Ponadto pokazujemy istnienie zjawiska ukrytego sterowalności (*hidden steering*)–przez analogię do ukrytej nielokalności [104, 105]–gdzie sterowalność może być aktywowana przez użycie lokalnych filtrów.

[C22] M. T. Quintino, T. Vértesi, D. Cavalcanti, R. Augusiak, M. Demianowicz, A. Acín, N. Brunner, *Entanglement, steering, and Bell nonlocality are inequivalent for general measurements*, Physical Review A **92**, 032107 (2015).

Moc komunikacyjna korelacji łamiących relacje monogamii. Jak już wspomniano, w dowolnej teorii spełniającej zasadę niesygnalizowania, korelacje wytworzone pomiędzy przestrzennie odseparowanymi obserwatorami w eksperymencie Bella, podlegają pewnym ograniczeniom znanym jako relacje monogamii. Jednakże ostatnie badania dotyczące problemu strat informacji w czarnych dziurach sugerują, że w pewnych sytuacjach takie relacje monogamii mogą być łamane [106]. Wówczas korelacje łamiące relacje monogamii mogą być użyte do transmisji informacji pomiędzy obserwatorami. W [C23] szczegółowo przebadaliśmy to zagadnienie, a w szczególności ilość informacji, która może być przesłana w ten sposób. W tym celu pokazaliśmy jak dowolnym korelacjom uzyskanym w eksperymencie Bella można przyporządkować pewne kanały klasyczne, których pojemności są następnie używane do ilościowego określenia użyteczności tych korelacji w przesyłaniu informacji. Nasze podejście zostało zilustrowane na przykładzie relacji monogamii dla łańcuchowej nierówności Bella [107].

[C23] W. Kłobus, M. Oszmaniec, R. Augusiak, A. Grudka, *Communication strength of boxes violating monogamy relations*, Foundations of Physics **46**, 620 (2016).

Dwuciałowe nierówności Bella i wielociałowe układy spinowe. W [C24] kontynuowaliśmy nasze badania nad dwuciałowymi nierównościami Bella zapoczątkowane w [H5,H8]. W szczególności sformułowaliśmy kryterium, które pozwala stwierdzić czy dana dwucząstkowa, permutacyjnie niezmiennicza nierówność Bella należąca do klasy nierówności znalezionej w [H5] jest optymalna (*tight*). Ponadto znaleźliśmy nierówności Bella, które są łamane przez wszystkie symetryczne stany Dicke'go. Badaliśmy także czy możliwa jest eksperymentalna weryfikacja nielokalności przy użyciu naszych nierówności Bella w wielocząstkowych stanach kwantowych wytworzonych w eksperymencie zaprezentowanym w pracy [108].

Następnie w [C25] podaliśmy związek pomiędzy detekcją nielokalności przy użyciu kilkuciałowych korelacji oraz wielociałowymi układami spinowymi. Z jednej strony pokazujemy, że pewne narzędzia zwyczajowo używane w fizyce układów spinowych, takie jak transformacja Jordana-Wignera lub programowanie dynamiczne mogą być z powodzeniem używane w badaniach nierówności Bella. Pozwalają one, na przykład, znacznie uprościć obliczanie ograniczeń klasycznych, a także znajdywanie łamania kwantowego, dla

RA

pewnej klasy nierówności. Z drugiej strony, zaproponowaliśmy metodę pozwalającą badać nielokalność w niskoenergetycznych stanach własnych pewnych Hamiltonianów spinowych.

[C24] J. Tura, R. Augusiak, A. B. Sainz, B. Lücke, C. Klempt, M. Lewenstein, A. Acín, *Nonlocality in many-body quantum systems detected with two-body correlators*, Annals of Physics **362**, 370 (2015).

[C25] J. Tura, G. de las Cuevas, R. Augusiak, M. Lewenstein, A. Acín, I. Cirac, *Energy as a detector of nonlocality of many-body spin systems*, Physical Review X **7**, 021005 (2017).

Samotestowanie maksymalnie splątanych stanów kwantowych. Ostatnie zdobycze na polu technologii kwantowych—technologii wykorzystujących zjawiska kwantowe—powodują, że niezbędne jest stworzenie wiarygodnych narzędzi uwierzytelniających, które pozwalałyby potwierdzić, że dane urządzenie kwantowe działa zgodnie z jego specyfikacją. Jednym z podejść do tego problemu jest tak zwane samotestowanie (ang. *self-testing*) [61]. Pozwala ono na uwierzytelnianie stanu kwantowego oraz pomiarów na nim wykonywanych opierając się tylko na statystyce, którą dane urządzenie kwantowe generuje, bądź, w ekstremalnym przypadku, tylko z łamania nierówności Bella.

W [C26] skonstruowaliśmy protokół samotestowania oparty na łańcuchowych nierównościach Bella [107], zdefiniowanych dla dwóch obserwatorów wykonujących dowolną liczbę pomiarów dwuwynikowych. Protokół ten pozwala samotestować dwukubitowy stan maksymalnie splątany oraz dowolną liczbę pomiarów dwuwynikowych z płaszczyzny rozpiętej przez macierze Pauliego σ_x i σ_z. Nasz rezultat oznacza, że zbiór rozkładów prawdopodobieństwa łamiących maksymalnie łańcuchowe nierówności Bella jest unikatowy dla dowolnej liczby pomiarów. Dowodzimy wreszcie, że łańcuchowe nierówności Bella mogą być użyte do uwierzytelnienia dwóch bitów idealnej losowości.

W [C27] podjęliśmy się próby znalezienia metody samotestowania maksymalnie splątanych stanów o wymiarze lokalnym większym niż dwa. W tym celu skonstruowaliśmy nierówności Bella dla dowolnej liczby pomiarów z dowolną liczba wyników, które są łamane maksymalnie przez stany maksymalnie splątane o dowolnym wymiarze lokalnym. Następnie gruntowanie je przebadaliśmy, znajdując analitycznie ich maksymalne klasyczne, kwantowe i niesygnalizujące wartości. Pokazaliśmy wreszcie, przy użyciu metod numerycznych, że nasze nierówności Bella pozwalają samotestować dwukutritowy stan maksymalnie splątany.

[C26] I. Šupić, R. Augusiak, A. Salavrakos, A. Acín, *Self-testing protocols based on the chained Bell inequalities*, New Journal of Physics **18**, 035013 (2016).

[C27] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, S. Pironio, *Bell inequalities tailored for the maximally entangled states*, Physical Review Letters **119**, 040402 (2017).

Nieograniczona ilość losowości z dwukubitowych stanów o dowolnie małym splątaniu. Znany faktem jest to, że wyniki pomiarów użytych do wytworzenia korelacji, które łamią nierówności Bella są losowe. Co ważne taka losowość kwantowa może być użyta w wielu zastosowaniach takich jak bezpieczna komunikacja oraz wierne obliczenia numeryczne. Ciekawe jest więc pytanie jak dużo losowości można wytwarzać z danego splątanego stanu kwantowego. Wiadomo, że w standardowym scenariuszu Bella, w którym każda z osób wykonuje

RA

pojedynczy pomiar na swojej części stanu kwantowego, co najwyżej $4 \log_2 d$ bitów losowości może być wytworzone ze splątanego stanu kwantowego o wymiarze lokalnym d. W [C28] pokazujemy, że rozważając ogólniejszy scenariusz Bella, w którym obserwator może wykonać serię pomiarów na tej samej cząstce, można to ograniczenie pokonać. Dokładnie mówiąc, pokazujemy, że w takim sekwencyjnym scenariuszu możliwe jest wytworzenie nieograniczonej liczby bitów losowości z jednego stanu kwantowego, o dowolnie małym splątaniu.

[C28] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, A. Acín, *Unbounded randomness certification using sequences of measurements*, Phys. Rev. A **95**, 020102(R) (2017). **(Editors' suggestion in PRA)**

Literatura

[1] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Bell nonlocality*, Rev. Mod. Phys. **86**, 419 (2014).

[2] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[3] A. Acín *et al.*, *Device-Independent Security of Quantum Cryptography against Collective Attacks*, Phys. Rev. Lett. **98**, 230501 (2007).

[4] J.-D. Bancal, N. Gisin, Y.-C. Liang, S. Pironio, *Device-Independent Witnesses of Genuine Multipartite Entanglement*, Phys. Rev. Lett. **106**, 250404 (2011).

[5] S. Pironio *et al.*, *Random numbers certified by Bell's theorem*, Nature **464**, 1021 (2010).

[6] R. Colbeck, R. Renner, *Free randomness can be amplified*, Nat. Phys. **8**, 450 (2012).

[7] H. Barnum, S. Beigi, S. Boixo, M. B. Elliott, S. Wehner, *Local Quantum Measurement and No-Signaling Imply Quantum Correlations*, Phys. Rev. Lett. **104**, 140401 (2010).

[8] J. S. Bell, *On the Einstein Podolsky Rosen Paradox*, Physics **1**, 195 (1964).

[9] A. Einstein, N. Rosen, and B. Podolsky, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777 (1935).

[10] M. Moszyńska, *Geometria zbiorów wypukłych*, Wydawnictwa Naukowo-Techniczne (Warszawa, 2001).

[11] K. Fukuda, https://www.inf.ethz.ch/personal/fukudak/cdd_ home/.

[12] S. Popescu and N. Rohrlich, *Quantum nonlocality as an axiom*, Found. Phys. **24**, 379 (1994).

[13] W. van Dam, *Non-locality and communication complexity*, PhD thesis (University of Oxford, 2000); G. Brassard *et al.*, Phys. Rev. Lett. **96** , 250401 (2006).

[14] M. Pawłowski *et al.*, *Information causality as a physical principle*, Nature **461**, 1101 (2009).

[15] M. Navascués, H. Wunderlich, *A glance beyond the quantum model*, Proc. R. Soc. A **466**, 881 (2010).

RA

[16] N. Linden, S. Popescu, A. J. Short and A. Winter, *Quantum Nonlocality and Beyond: Limits from Nonlocal Computation*, Phys. Rev. Lett. **99**, 180502 (2007).

[17] M. Horodecki, P. Horodecki, R. Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Phys. Lett. A **223**, 1 (1996).

[18] A. Gleason, *Measures on the closed subspaces of a Hilbert space*, J. Math. Mech. **6**, 885 (1957).

[19] N. R. Wallach, *An Unentangled Gleason's Theorem*, arXiv:quant-ph/0002058.

[20] A. Jamiołkowski, *Linear transformations which preserve trace and positive semidefinitness of operators*, Rep. Math. Phys. **3**, 275 (1972).

[21] C. Śliwa, *Symmetries of the Bell correlation inequalities*, Phys. Lett. A **317**, 165 (2003).

[22] M. L. Almeida *et al.*, *Guess Your Neighbor's Input: A Multipartite Nonlocal Game with No Quantum Advantage*, Phys. Rev. Lett. **104**, 230404 (2010).

[23] C. H. Bennett *et al.*, *Unextendible Product Bases and Bound Entanglement*, Phys. Rev. Lett. **82**, 5385 (1999).

[24] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *Secure Key from Bound Entanglement*, Phys. Rev. Lett. **94**, 160502 (2005).

[25] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *General paradigm for distilling classical key from quantum states*, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[26] M. Curty, M. Lewenstein, and N. Lütkenhaus, *Entanglement as a Precondition for Secure Quantum Key Distribution*, Phys. Rev. Lett. **92**, 217903 (2004).

[27] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, *Proposed experiment to test local hidden variable theories*, Phys. Rev. Lett. **23**, 880 (1969).

[28] J. F. Clauser, M. A. Horne, *Experimental consequences of objective local theories*, Phys. Rev. D **10**, 526 (1974).

[29] S. Popescu, D. Rohrlich, *Generic quantum nonlocality*, Phys. Lett. A **166**, 293 (1992).

[30] N. Gisin, *Bell's inequality holds for all non-product states*, Phys. Lett. A **154**, 201 (1991).

[31] N. Gisin and A. Peres, *Maximal violation of Bell's inequality for arbitrarily large spin*, Phys. Lett. A **162**, 15 (1992).

[32] R. F. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Rev. A **40**, 4277 (1989).

[33] J. Barrett, *Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality*, Phys. Rev. A **65**, 042302 (2002).

[34] G. Tóth, A. Acín, *Genuine tripartite entangled states with a local hidden-variable model*, Phys. Rev. A **74**, 030306(R) (2006).

RA

[35] A. Acín, N. Gisin, and B. Toner, *Grothendieck's constant and local models for noisy entangled quantum states*, Phys. Rev. A **73**, 062105 (2006).

[36] M. Horodecki, P. Horodecki, *Reduction criterion of separability and limits for a class of distillation protocols*, Phys. Rev. A **59**, 4206 (1999).

[37] M. L. Almeida, S. Pironio, J. Barrett, G. Tóth, and A. Acín, *Noise Robustness of the Nonlocality of Entangled Quantum States*, Phys. Rev. Lett. **99**, 040403 (2007).

[38] F. Hirsch, M. T. Quintino, J. Bowles, N. Brunner, *Genuine Hidden Quantum Nonlocality*, Phys. Rev. Lett. **111**, 160402 (2013).

[39] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, *Operational Framework for Nonlocality*, Phys. Rev. Lett. **109**, 070401 (2012).

[40] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio, *Definitions of multipartite nonlocality*, Phys. Rev. A **88**, 014102 (2013).

[41] G. Svetlichny, *Distinguishing three-body from two-body nonseparability by a Bell-type inequality*, Phys. Rev. D **35**, 3066 (1987).

[42] H. M. Wiseman, S. J. Jones, and A. C. Doherty, *Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox*, Phys. Rev. Lett. **98**, 140402 (2007).

[43] J. Bowles, J. Francfort, M. Fillettaz, F. Hirsch, and N. Brunner, *Genuinely Multipartite Entangled Quantum States with Fully Local Hidden Variable Models and Hidden Multipartite Nonlocality*, Phys. Rev. Lett. **116**, 130401 (2016).

[44] B. Toner, *Monogamy of non-local quantum correlations*, Proc. R. Soc. A **465**, 59 (2009).

[45] M. Pawłowski, Č. Brukner, *Monogamy of Bell's Inequality Violations in Nonsignaling Theories*, Phys. Rev. Lett. **102**, 030403 (2009).

[46] R. Ramanathan, P. Horodecki, *Strong Monogamies of No-Signaling Violations for Bipartite Correlation Bell Inequalities*, Phys. Rev. Lett. **113**, 210403 (2014).

[47] J. Barrett, A. Kent, and S. Pironio, *Maximally Nonlocal and Monogamous Quantum Correlations*, Phys. Rev. Lett. **97**, 170409 (2006).

[48] L. Aolita, R. Gallego, A. Cabello, and A. Acín, *Fully Nonlocal, Monogamous, and Random Genuinely Multipartite Quantum Correlations*, Phys. Rev. Lett. **108**, 100401 (2012).

[49] S. Pironio, Ll. Masanes, A. Leverrier, and A. Acín, *Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model*, Phys. Rev. X **3**, 031007 (2013).

[50] A. Grudka *et al.*, *Free randomness amplification using bipartite chain correlations*, Phys. Rev. A **90**, 032322 (2014).

[51] B. Hensen *et al.*, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, Nature **526**, 682 (2015).

RA

[52] L. K. Shalm *et al.*, *Strong Loophole-Free Test of Local Realism*, Phys. Rev. Lett. **115**, 250402 (2015).

[53] N. D. Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states*, Phys. Rev. Lett. **65**, 1838 (1990).

[54] R. F. Werner and M. M. Wolf, *All-multipartite Bell-correlation inequalities for two dichotomic observables per site*, Phys. Rev. A **64**, 032112 (2001); H. Weinfurter and M. Żukowski, *Four-photon entanglement from down-conversion*, Phys. Rev. A **64**, 010102(R) (2001); M. Żukowski and Č. Brukner, *Bell's Theorem for General N-Qubit States*, Phys. Rev. Lett. **88**, 210401 (2001).

[55] R. Prevedel *et al.*, *Experimental Realization of Dicke States of up to Six Qubits for Multiparty Quantum Networking*, Phys. Rev. Lett. **103**, 020503 (2009).

[56] W. Wieczorek *et al.*, *Experimental Entanglement of a Six-Photon Symmetric Dicke State*, Phys. Rev. Lett. **103**, 020504 (2009).

[57] K. Hammerer, A. S. Srensen, E. S. Polzik, *Quantum interface between light and atomic ensembles*, Rev. Mod. Phys. **82**, 1041 (2010).

[58] K. Eckert *et al.*, *Quantum non-demolition detection of strongly correlated systems*, Nat. Phys. **4**, 50 (2008).

[59] R. Schmied *et al.*, *Bell correlations in a Bose-Einstein condensate*, Science **352**, 441 (2016).

[60] L. Masanes, *Extremal quantum correlations for N parties with two dichotomic observables per site*, arXiv:quant-ph/0512100.

[61] D. Mayers, A. Yao, *Self testing quantum apparatus*, Quantum Inf. Comput. **4**, 273 (2004).

[62] A. Coladangelo, K. T. Goh, V. Scarani, *All Pure Bipartite Entangled States Can Be Self-Tested*, Nat. Comm. **8**, 15485 (2017).

[63] R. Szmytkowski, *Eigenchannel method in quantum potential scattering*, Ann. Phys. **311**, 503 (2004).

[64] A. Peres, *All the Bell Inequalities*, Foundations of Physics **29**, 589 (1999).

[65] W. Dür, *Multipartite Bound Entangled States that Violate Bell's Inequality*, Phys. Rev. Lett. **87**, 230402 (2001).

[66] D. Kaszlikowski *et al.*, *Multipartite bound entanglement and three-setting Bell inequalities*, Phys. Rev. A **66**, 052309 (2002).

[67] A. Sen(De), U. Sen, M. Żukowski, *Functional Bell inequalities can serve as a stronger entanglement witness than conventional Bell inequalities*, Phys. Rev. A **66**, 062318 (2002).

[68] J. A. Smolin, *Four-party unlockable bound entangled state*, Phys. Rev. A **63**, 032306 (2001).

[69] E. Amselem and M. Bourennane, *Experimental four-qubit bound entanglement*, Nat. Phys. **5**, 748 (2009).

RA

[70] J. Lavoie, R. Kaltenbaek, M. Piani, and K. J. Resch, *Experimental Bound Entanglement in a Four-Photon State*, Phys. Rev. Lett. **105**, 130501 (2010).

[71] M. Murao and V. Vedral, *Remote Information Concentration Using a Bound Entangled State*, Phys. Rev. Lett. **86**, 352 (2001).

[72] H.-K. Lo and B. Fortescue, *Random Bipartite Entanglement from W and W-Like States*, Phys. Rev. Lett. **98**, 260501 (2007).

[73] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Quantum entanglement*, Rev. Mod. Phys. **81**, 865 (2009).

[74] O. Gühne, G. Tóth, *Entanglement detection*, Phys. Rep. **474**, 1 (2009).

[75] P. Horodecki, *From limits of quantum operations to multicopy entanglement witnesses and state-spectrum estimation*, Phys. Rev. A **68**, 052101 (2003).

[76] H. A. Carteret, *Noiseless Quantum Circuits for the Peres Separability Criterion*, Phys. Rev. Lett. **94**, 040502 (2005).

[77] P. Horodecki, A. K. Ekert, *Method for Direct Detection of Quantum Entanglement*, Phys. Rev. Lett. **89**, 127902 (2002).

[78] C. Moura Alves, P. Horodecki, D. K. L. Oi, L. C. Kwek, A. K. Ekert, *Direct estimation of functionals of density operators by local operations and classical communication*, Phys. Rev. A **68**, 032306 (2003).

[79] R. Horodecki and P. Horodecki, *Quantum redundancies and local realism*, Phys. Lett. A **194**, 147 (1994).

[80] M. Terhal, *Detecting quantum entanglement*, Theor. Comput. Sci. **287**, 313 (2002).

[81] K. G. H. Vollbrecht and M. M. Wolf, *Conditional entropies and their relation to entanglement criteria*, J. Math. Phys. **43**, 4299 (2002).

[82] H.-P. Breuer, *State space structure and entanglement of rotationally invariant spin systems*, J. Phys. A: Math. Gen. **38**, 9019 (2005).

[83] M. A. Nielsen, J. Kempe, *Separable States Are More Disordered Globally than Locally*, Phys. Rev. Lett. **86**, 5184 (2001).

[84] J. M. Leinaas, J. Myrheim, E. Ovrum, *Extreme points of the set of density matrices with positive partial transpose*, Phys. Rev. A **76**, 034304 (2007).

[85] F. G. S. L. Brandão, *Quantifying entanglement with witness operators*, Phys. Rev. A **72**, 022310 (2005).

[86] M. Lewenstein, B. Kraus, J. I. Cirac, P. Horodecki, *Optimization of entanglement witnesses*, Phys. Rev. A **62**, 052310 (2000).

RA

[87] J. Korbicz, M. L. Almeida, J. Bae, M. Lewenstein, and A. Acín, *Structural approximations to positive maps and entanglement-breaking channels*, Phys. Rev. A **78**, 062105 (2008).

[88] K.-C. Ha and S.-H. Kye, *Separable states with unique decompositions*, arXiv:1210.1088v3.

[89] K.-C. Ha and S.-H. Kye, *The structural physical approximations and optimal entanglement witnesses*, J. Math. Phys. **53**, 102204 (2012).

[90] G. Sarbicki and D. Chruściński, *Disproving the conjecture on structural physical approximation to optimal decomposable entanglement witnesses*, J. Phys. A: Math. Theor. **47**, 195301 (2014).

[91] Y.-F. Huang *et al.*, *Experimental generation of an eight-photon Greenberger-Horne-Zeilinger state*, Nat. Comm. **2**, 546 (2011).

[92] H.-P. Breuer, *Optimal Entanglement Criterion for Mixed Quantum States*, Phys. Rev. Lett. **97**, 080501 (2006).

[93] W. Hall, *A new criterion for indecomposability of positive maps*, J. Phys. A: Math. Gen. **39**, 14119 (2006).

[94] L. Gurvits, H. Barnum, *Largest separable balls around the maximally mixed bipartite quantum state*, Phys. Rev. A **66**, 062311 (2002).

[95] G. Tóth, I. Apellaniz, *Quantum metrology from a quantum information science perspective*, J. Phys. A: Math. Theor. **47**, 424006 (2014).

[96] A. Shimony, *Degree of Entanglement*, Ann. NY Acad. Sci. **755**, 675 (1995); T.-C. Wei, P. M. Goldbart, *Geometric measure of entanglement and applications to bipartite and multipartite quantum states*, Phys. Rev. A **68**, 042307 (2003).

[97] M. Navascués and H. Wunderlich, *A glance beyond the quantum model*, Proc. R. Soc. A **466**, 881 (2010).

[98] R. Gallego, L. E. Würflinger, A. Acín, M. Navascúes, *Quantum Correlations Require Multipartite Information Principles*, Phys. Rev. Lett. **107**, 210403 (2011).

[99] M. Navascués, Y. Guryanova, M. J. Hoban, A. Acín, *Almost quantum correlations*, Nat. Comm. **6**, 6288 (2015).

[100] H. Buhrman, S. Massar, *Causality and Tsirelson's bounds*, Phys. Rev. A **72**, 052103 (2005).

[101] M. P. Müller, Ll. Masanes, *Information-Theoretic Postulates for Quantum Theory*, w *Quantum Theory: Informational Foundations and Foils*, edytorzy: G. Chiribella, R. W. Spekkens, strony: 139-170 (Springer, 20016).

[102] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, *Experimental EPR-steering using Bell-local states*, Nature Phys. **6**, 845 (2010).

[103] S. Jevtic, M. J. W. Hall, M. R. Anderson, M. Zwierz, and H. M. Wiseman, *Einstein-Podolsky-Rosen steering and the steering ellipsoid*, J. Opt. Soc. Am. B **32**, A40 (2015).

RA

[104] S. Popescu, *Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality*, Phys. Rev. Lett. **74**, 2619 (1995).

[105] J. Bowles, T. Vértesi,M. T. Quintino, and N. Brunner, *One-way Einstein-Podolsky-Rosen Steering*, Phys. Rev. Lett. **112**, 200402 (2014).

[106] A. Almheiri, D. Marolf, J. Polchinski, J. Sully, *Black holes: complementarity or firewalls?* JHEP **02**, 062 (2013); J. Oppenheim, B. Unruh, *Firewalls and flat mirrors: an alternative to the AMPS experiment which evades the Harlow-Hayden obstacle*, JHEP **03**, 120 (2014).

[107] P. A. Pearle, *Hidden-Variable Example Based upon Data Rejection*, Phys. Rev. D **2**, 1418 (1970); S. L. Braunstein, C. Caves, *Wringing out better Bell inequalities*, Ann. Phys. **202**, 22 (1990).

[108] B. Lücke *et al.*, *Quantum metrology from a quantum information science perspective*, Phys. Rev. Lett. **112**, 155304 (2014).

Warszawa, 11.10.2017
Anguriel