Gdańsk, 10.03.2014

Mgr Marcin Markiewicz
Instytut Fizyki Teoretycznej i Astrofizyki
Uniwersytetu Gdańskiego
Wita Stwosza 57, 80-952 Gdańsk

Streszczenie rozprawy doktorskiej:

Charakteryzacja i detekcja wielocząstkowego splątania

1 Podsumowanie

Celem rozprawy jest badanie struktury wielocząstkowego splątania, poszukiwanie kryteriów jego efektywnej detekcji oraz jego roli w praktycznych zastosowaniach.

Jeśli rozważamy układ złożony z wielu podukładów, to kwantowe korelacje mogą być w nim rozłożone na wiele różnych sposobów. Okazuje się, że n-cząstkowe splątanie nie jest równoważne istnieniu n-cząstkowych korelacji, co komplikuje analizę. W tej rozprawie przyjmujemy podejście geometryczne do analizy splątania. Przestrzeń stanów wielocząstkowego układu kwantowego jest odwzorowana w wielowymiarową euklidesową przestrzeń korelacji. Podejście to ma dwie zasadnicze korzyści. Z jednej strony, dostajemy do dyspozycji proste narzędzia geometryczne, takie jak iloczyny skalarne i metryki, co czyni analizę znacznie łatwiejszą niż w przypadku posługiwania się wprost metodami zepolonej przestrzeni Hilberta. Po drugie, podstawowe obiekty geometryczne – tensory korelacji – są obiektami bezpośrednio mierzalnymi w eksperymencie. W oparciu o formalizm tensorów korelacji konstruujemy warunki na istnienie wielocząstkowego splątania. W przeciwieństwie do warunków znanych dotychczas, wymagają one stosunkowo małej liczby pomiarów.

Następnie badamy znaczenie wielocząstkowego splątania jako podstawowego zasobu w kwantowej metrologii i w kwantowych obliczeniach rozproszonych. Pokazujemy, że wielocząstkowe stany GHZ pozwalają na dokładniejsze niż klasyczne skalowanie precyzji estymacji nieznanych parametrów fizycznych w obecności dekoherencji, jak również na redukcję złożoności obliczeniowej w obliczeniach rozproszonych.

2 Kwantowe splątanie i kwantowe korelacje – wprowadzenie

Po prawie 80 latach od pierwszych dyskusji nad tym zagadnieniem [1, 2], kwantowe splątanie może być traktowane jako znak rozpoznawczy fizyki kwantowej. W licznych publikacjach nazywane jest ono *istotą mechaniki kwantowej*. W nowoczesnym języku splątanie najprościej opisać w języku teorii informacji: dwie cząstki są splątane, jeśli ich stan zawiera więcej informacji o całym układzie, niż o pojedynczych cząstkach [3].

W mechanice kwantowej stan układu złożonego może być jednocześnie *czysty* – czyli zawierać maksymalną możliwą wiedzę o tym układzie – i zawierać korelacje. Jest to niemożliwe w ramach fizyki klasycznej, gdzie stan jest albo czysty, albo zawiera korelacje [4]. Stąd korelacje klasyczne, w przeciwieństwie do korelacji stanów splątanych, zawsze wiążą się z pewną niewiedzą o stanie całości układu. Pokazuje to, że natura korelacji kwantowych jest całkowicie odmienna od ich klasycznych odpowiedników. Ta *nieklasyczność* kwantowych korelacji może być opisana z dwóch punktów widzenia: w ramach formalizmu mechaniki kwantowej, jak i niezależnie od niego.

Odrębne własności stanów i obserwabli w formaliźmie kwantowym wyrażają się w dwóch własnościach. Po pierwsze, przestrzeń stanów układu złożonego opisywana jest iloczynem tensorowym przestrzeni podukładów, a nie ich iloczynem kartezjańskim. Po drugie, obserwable kwantowe, w przeciwieństwie do klasycznych, mogą być nieprzemienne. Obie te cechy są konieczne dla istnienia splątania, gdyż stany splątane mogą istnieć tylko w takiej teorii, w której obserwable w lokalnych podukładach są nieprzemienne [5, 6].

Nieklasyczność kwantowych korelacji może być również scharakteryzowana bez jakiegokolwiek odniesienia do formalizmu kwantowego za pomocą łamania tzw. *nierówności Bella* [7, 8]. Nierówności te opisują klasyczne ograniczenia na probabilistyczny lub teorioinformacyjny opis wyników pomiarów przeprowadzonych na rozseparowanych podukładach. Na przykład, jedna z najbardziej znanych nierówności Bella – nierówność CHSH [9] – wyrażona jest za pomocą dwucząstkowych funkcji korelacji. Jej łamanie, wskazujące na nieklasyczne właściwości układu, związane jest z nieistnieniem łącznego rozkładu prawdopodobieństwa dla wyników pomiarów. W przypadku łamania nierównośći wyrażonych w języku entropii Shannona [10] albo złożoności Kołmogorowa [11], dochodzi do złamania bardziej subtelnych klasycznych własności teorioinformacyjnych [12].

Wspólną własnością leżącą u podstaw obu powyższych charakteryzacji nieklasyczności jest *kwantowa niekompatybilność* [13, 14, 15]. Dla każdego zbioru obserwabli przemiennych istnieje klasyczny model probabilistyczny opisujący wyniki dowolnych pomiarów tych obserwabli. Jednakże modele odpowiadające różnym zbiorom komutujących obserwabli mogą być wzajemnie niekompatybilne, a ich łączenie nieuchronnie prowadzi do sprzeczności na poziomie logicznym i statystycznym [15, 14]. Sprzeczności te sprowokowały długą debatę w kwestii ich znaczenia dla struktury i filozoficznych implikacji mechaniki kwantowej. Dyskusja ta jest wciąż żywa [16].

Kwantowe splątanie znalazło praktyczne zastosowania w kontekście zadań obliczeniowych i komunikacyjnych. Doprowadziło to do powstania nowej interdyscyplinarnej dziedziny: teorii kwantowej informacji (quantum information

science). Dziedzina ta obejmuje obecnie wiele różnorakich zagadnień, takich jak kwantowa komunikacja [17, 18, 19, 20], kwantowa kryptografia [21], kwantowa metrologia [22], a w niedalekiej przyszłości również być może kwantowe obliczenia [23].

3 Szczegółowe przedstawienie wyników

W tym rozdziale przedstawiam podsumowanie wyników badań opublikowanych w pracach [A],[B],[C],[D],[E],[F].

3.1 Struktura wielocząstkowego splątania i wielocząstkowych korelacji

Wielocząstkowe splątanie jest przejawem *kwantowej nieseparowalności* w układach składających się z wielu podukładów. Intuicyjnie, splątanie pomiędzy n cząstkami wskazuje na istnienie silnych nieklasycznych korelacji pomiędzy nimi. Intuicja ta okazuje się być całkowicie trafna w przypadku stanów czystych, zawodzi jednak w przypadku stanów mieszanych [24], [25], [C]. Okazuje się, że precyzyjna definicja wielocząstkowego splątania wymaga określenia stopnia separowalności badanego stanu kwantowego. W tym rozdziale przedstawiam ogólną charakteryzację częściowej separowalności. W dalszej części przedstawiam wyniki badań na związkiem pomiędzy wielocząstkowym splątaniem, korelacjami niższych rzędów oraz istnieniem klasycznych modeli dla tych korelacji w przypadku pewnych stanów splątanych.

3.1.1 Geometryczna charakteryzacja częściowej separowalności

Najogólniej rzecz ujmując separowalność jest własnością układu złożonego, która polega na tym, że całkowity stan układu jest kombinacją wypukłą stanów czystych, które są produktowe względem pewnego podziału na podukłady [26]. W przypadku układu dwóch cząstek oznacza to, że stan całości jest mieszaniną wypukłą stanów produktowych. Operacyjnie oznacza to, że każda funkcja korelacji dla lokalnych pomiarów kwantowych może być zasymulowana za pomocą lokalnych obliczeń oraz współdzielonej losowości, ale bez komunikacji pomiędzy podukładami. W przypadku układów wielocząstkowych pojęcie separowalności staje się mniej oczywiste, ponieważ cały system może być podzielony na podukłady na wiele różnych sposobów. Najbardziej naturalnym uogólnieniem pojęcia separowalności jest w tym przypadku *separowalność ze względu na podział na podukłady* [27, 4]: n-cząstkowy stan ρ jest k-separowalny ze względu na podział $\mathcal{S}$ n cząstek na k podukładów $\{s_1, \ldots, s_k\}$, jeśli może być przedstawiony jako mieszanina wypukła stanów czystych $|\psi_{(k-\mathrm{pr}|\mathcal{S})}\rangle = \bigotimes_{l=1}^{k} |\psi_{r_l \in s_l}\rangle$, które są k-produktowe ze względu na podział $\mathcal{S}$:

$$\rho_{(k-\mathrm{sep}|\mathcal{S})} = \sum_i p_i |\psi^i_{(k-\mathrm{pr}|\mathcal{S})}\rangle\langle\psi^i_{(k-\mathrm{pr}|\mathcal{S})}|. \tag{1}$$

W powyższej definicji, jak i w dalszej części pracy, indeksy 'k–sep' i 'k–pr' oznaczają odpowiednio: 'k–separowalny' i 'k–produktowy'. Niestety, częściowa separowalność (1) nie definiuje częściowo uporządkowanych klas separowalności. Nie może być ona wykorzystana do określenia stopnia separowalności, ponieważ

różne klasy są nieporównywalne. Aby rozwiązać ten problem wprowadza się definicję bezwarunkowej k-separowalności: n-cząstkowy stan ρ jest k-separowalny, jeśli może być on przedstawiony jako kombinacja wypukła czystych stanów k-produktowych: $|\psi_{k-\mathrm{pr}}\rangle = |\psi_{r_1}\rangle \otimes \ldots \otimes |\psi_{r_k}\rangle$:

$$\rho_{k-\mathrm{sep}} = \sum_i p_i |\psi^i_{k-\mathrm{pr}}\rangle\langle\psi^i_{k-\mathrm{pr}}|. \tag{2}$$

Różnica w stosunku do poprzedniej definicji polega na tym, że teraz stany czyste wchodzące w skład mieszaniny mogą być k-produktowe ze względu na różne podziały na podukłady. Zbiory S_{k-sep} stanów k-separowalnych są wypukłe i częściowo uporządkowane przez zawieranie:

$$S_{n-sep} \subseteq S_{(n-1)-sep} \subseteq \ldots \subseteq S_{3-sep} \subseteq S_{2-sep}. \tag{3}$$

Ustalenie, czy dany stan jest k-separowalny w oparciu wprost o definicję (2) jest analitycznie zadaniem trudnym i w wielu przypadkach praktycznie niewykonalnym. Jak dotąd zaproponowano pewne warunki wystarczające na k-separowalność stanów wielokubitowych [27]. W przypadku układów o dowolnych wymiarach przestrzeni podukładów znana jest jedynie efektywna charakteryzacja pełnej separowalności [28].

W pracy [A] podajemy pierwszą ogólną charakteryzację k-separowalności, która obejmuje układy o dowolnym skończonym wymiarze przestrzeni podukładów. Ma ona postać koniecznego i wystarczającego warunku na odrzucenie k-separowalności danego stanu. Ponieważ stany k-separowalne stanowią zbiór częściowo uporządkowany (3), nasz warunek stanowi pełną charakteryzację częściowej separowalności.

Nasz warunek jest wyrażony w języku *uogólnionego tensora korelacji* stanu kwantowego, który w przypadku kubitów jest zdefiniowany w następujący sposób:

$$T_{\mu_1,\ldots,\mu_n} = \langle \sigma_{\mu_1} \otimes \ldots \otimes \sigma_{\mu_n} \rangle_\rho = \mathrm{Tr}\left(\rho\, \sigma_{\mu_1} \otimes \ldots \otimes \sigma_{\mu_n}\right), \tag{4}$$

gdzie σ_μ dla $\mu = 1, 2, 3$ oznacza macierze Pauliego, a σ_0 oznacza macierz jednostkową. Dla niezerowych indeksów powyższy obiekt transformuje się jak tensor. Do zdefiniowania tensora korelacji w przypadku stanów wyżej wymiarowych można zamiast macierzy Pauliego użyć dowolnej hermitowskiej bazy operatorowej (np. uogólnionych macierzy Gell-Manna). Tensor korelacji stanowi jednoznaczną reprezentację dowolnego stanu kwantowego:

$$\rho = \frac{1}{2^n} \sum_{\mu_1,\ldots,\mu_n=0,1,2,3} T_{\mu_1,\ldots,\mu_n} \sigma_{\mu_1} \otimes \ldots \otimes \sigma_{\mu_n}. \tag{5}$$

Dla uproszczenia notacji będę dalej oznaczał $T_{\mu_1,\ldots,\mu_n}$ jako $T_{\vec{\mu}}$.

Posługiwanie się tensorami korelacji przynosi dwie zasadnicze korzyści. Po pierwsze, ich elementy są bezpośrednio mierzalne w eksperymentach. Po drugie, tensory korelacji należą do rodziny przestrzeni unitarnych (przestrzeni wektorowych wyposażonych w iloczyn skalarny), w których uogólniony iloczyn skalarny zdefiniowany jest jako:

$$(X, Y)_G = \sum_{\vec{\mu},\vec{\nu}} X_{\vec{\mu}} G_{\vec{\mu}\vec{\nu}} Y_{\vec{\nu}}, \tag{6}$$

gdzie G jest półdodatnio określonym operatorem działającym na przestrzeni wektorowej tensorów korelacji. Powyższy iloczyn skalarny definiuje G-półnormę[1]:

$$||T||_G^2 = (T, T)_G. \tag{7}$$

Przestrzeń tensorów korelacji z ustalonym G jest zatem *przestrzenią pseudometryczną*. Dla uproszczenia operatory G będą w dalszej części pracy nazywane *metrykami*. Pamiętać należy, że w rzeczywistości definiują one *pseudometrykę* na tych przestrzeniach.

Formalizm przestrzeni unitarnych pozwala sformułować bardzo prosty geometryczny warunek na stwierdzenie, że dany wektor $\vec{a}$ nie należy do zbioru S [29]:

$$\max_{\vec{b}\in S} \vec{a}\cdot\vec{b} < \vec{a}\cdot\vec{a} \Longrightarrow \vec{a} \notin S. \tag{8}$$

Stosując tę własność do zbioru stanów k-separowalnych otrzymujemy następujący warunek, będący uogólnieniem warunku na pełną separowalność z pracy [29]:

$$\begin{gathered} \textit{Jeśli istenieje metryka } G\textit{, dla której:} \\ \max_{T^{k\text{-}sep}} (T^{k\text{-}sep}, T)_G < ||T||_G^2, \\ \textit{stan opisywany tensorem korelacji } T \textit{ nie jest } k\textit{-separowalny.} \end{gathered} \tag{9}$$

Warunek ten jest w pewnym sensie tautologiczny, gdyż w celu stwierdzenia, że dany stan nie jest k-separowalny, wymaga on optymalizacji po zbiorze wszystkich stanów k-separowalnych. Można go jednak istotnie uprościć korzystając z wypukłości stanów k-separowalnych:

$$\max_{T^{k\text{-}sep}} (T^{k\text{-}sep}, T)_G = \max_{\{\{p_i\}, T^{k\text{-}pr}\}} \left(\sum_i p_i T_{(i)}^{k\text{-}pr}, T \right)_G \leqslant \max_{T^{k\text{-}pr}} (T^{k\text{-}pr}, T)_G, \tag{10}$$

co oznacza, że maksymalizacja w warunku (9) może być przeprowadzona jedynie po czystych stanach k-produktowych. Zbiór stanów k-produktowych może być jednoznacznie przedstawiony w postaci sumy zbiorów stanów, które są k-produktowe względem wszystkich możliwych podziałów na podukłady $\mathcal{S}$. Dzięki temu warunek (9) można przeformułować tak, aby maksymalizacja była przeprowadzana osobno dla każdego takiego podziału:

$$\begin{gathered} \textit{Jeśli dla każdego podziału } \mathcal{S} \textit{ istnieje metryka } G_{\mathcal{S}} \textit{ taka, że:} \\ \max_{T^{(k\text{-}pr|\mathcal{S})}} (T^{(k\text{-}pr|\mathcal{S})}, T)_{G_{\mathcal{S}}} < ||T||_{G_{\mathcal{S}}}^2, \\ \textit{stan opisywany tensorem korelacji } T \textit{ nie jest } k\textit{-separowalny.} \end{gathered} \tag{11}$$

Ponadto, w pracy [A] pokazujemy, że powyższy warunek stanowi warunek konieczny, co oznacza, że dla każdego stanu ρ, który nie jest k-separowalny, dla

[1] Półnorma to funkcja o wartościach nieujemnych określona na danej przestrzeni wektorowej, która jest dodatnio jednorodna i spełnia nierówność trójkąta, ale może być *zdegenerowana*, co oznacza, że $||T||_G = 0$ *nie* musi implikować, że $T = 0$. W szczególności tensor korelacji stanu kwantowego nigdy nie jest wektorem zerowym, jednakże można tak dobrać operator G, aby $||T||_G = 0$.

każdego k-podziału $\mathcal{S}$ istnieje metryka $G_{\mathcal{S}}$, taka, że nierówność (11) jest spełniona. W ten sposób otrzymujemy ogólną charakteryzację k-separowalności [A]:

Dowolny n-cząstkowy stan opisywany tensorem korelacji T nie jest k-separowalny wtedy i tylko wtedy, gdy dla każdego podziału $\mathcal{S}$ na k podukładów, istnieje metryka $G_{\mathcal{S}}$ taka, że:

$$\max_{T^{(k\text{-pr}|\mathcal{S})}} (T^{(k\text{-pr}|\mathcal{S})}, T)_{G_{\mathcal{S}}} < (T, T)_{G_{\mathcal{S}}}. \tag{12}$$

Powyższa charakteryzacja jest bardzo istotna, gdyż daje ona pełen opis stopnia separowalności danego stanu, jak również charakteryzację wielocząstkowego splątania. Istotnie, ponieważ stany k-separowalne stanowią zbiór częściowo uporządkowany (3), otrzymujemy naturalny opis stopnia separowalności: najbardziej separowalne są stany n-separowalne, podczas gdy najmniej separowalne są stany *biseparowalne*. Stany w pełni separowalne nie zawierają splątania w ogóle, stany, które nie są k-separowalne zawierają splątanie pomiędzy co najmniej $\lceil \frac{n}{k-1} \rceil$ podukładami, a stany, które nie są biseparowalne, są prawdziwie n-cząstkowo splątane.

3.1.2 Stwierdzenie wielocząstkowego splątania w oparciu o znajomość korelacji dwucząstkowych

W przypadku układów składających się z wielu podukładów, nie istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy splątaniem a korelacjami, co oznacza, że istnieją stany prawdziwie n-cząstkowo splątane, które nie zawierają n-cząstkowych korelacji w rozumieniu definicji (4) [24, 25]. W pracy [B] zbadaliśmy, do jakiego stopnia wielocząstkowe splątanie stanów czystych może być udowodnione w oparciu o znajomość jedynie dwucząstkowych korelacji. Badania te oparte są na zjawisku *monogamii korelacji*, które oznacza, że rozkład korelacji w układzie wielu cząstek jest silnie ograniczony przez własności fizyczne, jakie spełnia ten układ. W przypadku układu trzech kubitów, jeśli dowolne dwa z nich są silnie kwantowo skorelowane, nie mogą być one silnie skorelowane z trzecim kubitem [30]. Własność ta ma istotne znaczenie dla kwantowej kryptografii [31, 32, 33].

W dalszej części tego rodziału używamy opisu stanów kwantowych w języku tensora korelacji (5). Elementy tensora korelacji (4), które zawierają jedynie k niezerowych indeksów opisują korelacje pomiędzy k podukładami. Ponieważ jednocząstkowe wartości średnie (T_x, T_y, T_z) tworzą wektor w trójwymiarowej przestrzeni euklidesowej, lokalne pomiary obserwabli σ_x, σ_y i σ_z są zwyczajowo nazywane pomiarami w kierunkach odpowiednio $\hat{x}$, $\hat{y}$ i $\hat{z}$.

Nasza charakteryzacja wielocząstkowego splątania stanów czystych wielu kubitów oparta jest na następującej relacji monogamii:

Dla każdego stanu n kubitów spełniona jest następująca relacja:

$$\mathcal{M} = \sum_{1 \leqslant k < l \leqslant n} \mathcal{M}_{kl} \leqslant \begin{cases} 2, & \text{jeśli } n = 2 \\ \binom{n}{2}, & \text{jeśli } n \geqslant 3 \end{cases}, \tag{13}$$

w której $\mathcal{M}_{kl} = \sum_{i,j=1,2} T^2_{0,\ldots,0,i_{(k)},0,\ldots,0,j_{(l)},0,\ldots,0}$, gdzie indeksy (k) i (l) oznaczją k-ty i l-ty podukład, a i, j stanowią dwie pary współrzędnych kartezjańskich. Dla uproszczenia zakładamy, że zawsze oznaczają one pomiary w kierunkach $\hat{x}$ i $\hat{y}$.

Warunek (13) oznacza, że w dowolnym stanie n kubitów, suma kwadratów wszystkich możliwych korelacji dwucząstkowych odpowiadających pomiarom w dwóch ortogonalnych kierunkach i, j jest ograniczona przez liczbę $\binom{n}{2}$. Liczba ta jest 4 razy mniejsza od algebraicznego ograniczenia na tę wielkość. W tej postaci powyższy warunek jest bezużyteczny do detekcji splątania, ponieważ $\mathcal{M}$ zawiera wyrazy związane z korelacjami klasycznymi. Aby rozwiązać ten problem definiujemy *preferowaną bazę* dla k-tego obserwatora, jako taką bazę operatorów, w której lokalny wektor Blocha przyjmuje kierunek $\hat{z}$. Wielkość $\mathcal{M}$ odnoszącą się do pomiarów w preferowanej bazie oznaczamy jako $\mathcal{M}^{(pb)}$. W oparciu o nią wyprowadziliśmy dwa kryteria splątania:

$$\begin{gathered}
\textit{Dla } n \geqslant 5, \ \textit{i dla każdego stanu czystego } n \textit{ kubitów } |\psi\rangle, \ \textit{jeśli:} \\
\mathcal{M}^{(pb)}(|\psi\rangle) > \tbinom{n-1}{2} \\
\textit{to } |\psi\rangle \textit{ jest prawdziwie } n \textit{ cząstkowo splątany. Dla n=3 i n=4 mamy:} \\
\mathcal{M}^{(pb)}(|\psi\rangle) > 2 \Longrightarrow |\psi\rangle \textit{ jest prawdziwie trójcząstkowo splątany.} \\
\mathcal{M}^{(pb)}(|\psi\rangle) > 4 \Longrightarrow |\psi\rangle \textit{ jest prawdziwie 4-cząstkowo splątany.}
\end{gathered} \tag{14}$$

oraz:

$$\begin{gathered}
\textit{Dla każdego stanu czystego } n \textit{ kubitów } |\psi\rangle, \ \textit{gdzie } n \geqslant 5, \\
\textit{i dla dowolnego } m \leqslant \left\lfloor \tfrac{n}{2} \right\rfloor - 1 \textit{ zachodzi:} \\
\textit{jeśli } \mathcal{M}^{(pb)}(|\psi\rangle) > \tbinom{m}{2} + \tbinom{n-m}{2} + \delta_{m,2}, \\
\textit{gdzie } \delta_{m,2} \textit{ oznacza deltę Kroneckera,} \\
\textit{stan } |\psi\rangle \textit{ zawiera prawdziwie } m\textit{–cząstkowe splątanie.}
\end{gathered} \tag{15}$$

Aby pokazać zastosowanie powyższych warunków, rozważmy stany Dicke'go: [34]:

$$|D_n^e\rangle = \frac{1}{\sqrt{\binom{N}{e}}} \sum_{\pi} |\pi(1 \ldots 10 \ldots 0)\rangle \,, \tag{16}$$

gdzie π oznacza permutację podukładów, a e – ilość wzbudzeń, czyli stanów $|1\rangle$. Z warunku (14) wynika, że stany D_3^1 i D_5^2 są prawdziwie wielocząstkowo splątane, podczas gdy warunek (15) pokazuje, że stany $D_n^{(n-1)/2}$ w przypadku nieparzystego n zawierają splątanie pomiędzy co najmniej $(n+3)/2$ cząstkami.

Choć wnioski te nie są optymalne z punktu widzenia detekcji splątania (wiadomo, że stany Dicke'go są prawdziwie n cząstkowo splątane), są one istotne przynajmniej z dwóch powodów. Po pierwsze, stoją one w sprzeczności z powszechną intuicją na temat rozważanych stanów. Istotnie, stany D_n^e są jedynymi stanami n cząstkowymi, które są kompatybilne ze swoimi $2e$-cząstkowymi stanami zredukowanymi [35]. Stąd wydaje się, że im większa jest liczna wzbudzeń e, tym więcej informacji o całym stanie zawarte jest w korelacjach wyższych rzędów. Jednakże warunek (15), który korzysta jedynie z korelacji dwucząstkowych, potwierdza splątanie pomiędzy większą ilością cząstek dla większej ilości wzbudzeń. Fakt ten pokazuje, że detekcja wielocząstkowego splątania jest zadaniem całkowicie odmiennym od tzw. *problemu kwantowych marginałów* [36], w którym ustala się, w jakim stopniu stan całego układu wyznaczony jest przez stany zredukowane. Po drugie, warunek (15) zastosowany do stanów Dicke'go stanowi interesującą ilustrację *kwantowego twierdzenia de Finetti* [37]. Twierdzenie to w swojej najprostszej wersji pokazuje, że k-cząstkowy stan zredukowany dowolnego

permutacyjnie niezmienniczego stanu kwantowego n cząstek jest dowolnie bliski stanu separowalnemu dla odpowiednio dużego n, ale przy ustalonym k. Warunek (15) potwierdza wielocząstkowe splątanie stanu $D_n^{(n-1)/2}$ dla dowolnego n, jednak efektywność tego warunku zbiega do zera dla $n \to \infty$. Jest to zgodne z kwantowym twierdzeniem de Finetti, które wskazuje, że dwucząstkowy stan zredukowany stanu D_n^e jest asymptotycznie separowalny, zatem asymptotycznie nie zawiera on informacji o splątaniu.

3.1.3 Niekompatybilność klasycznych modeli dla wielocząstkowych stanów splątanych

Jak wspomniano we wstępie, wielocząstkowe korelacje kwantowe mogą być scharakteryzowane niezależnie od formalizmu kwantowego. W tym celu bada się, w jakim stopniu korelacje te mogą być opisywane przez klasyczne modele statystyczne [15]. Niemożliwość klasycznego opisu można stwierdzić poprzez łamanie nierówności Bella [8], które wyprowadzone są przy założeniu, że model taki istnieje. Warunkiem koniecznym dla nieistnienia takich modeli dla pomiarów kwantowych jest splątanie pomiędzy mierzonymi podukładami, jak również nieprzemienność algebr lokalnych obserwabli w co najmniej dwóch podukładach. Okazuje się, że warunek ten nie jest wystarczający, co pokazał Werner [26].

Rozważmy układ, zwany *n-cząstkowym eksperymentem typu Bella z m lokalnymi ustawieniami*, w którym n obserwatorów wykonuje lokalne binarne pomiary na swoim podukładzie. Zakładamy, że k-ty obserwator lokalnie wybiera swoją obserwablę ze zbioru $\mathcal{A}_1^{[k]}, \ldots, \mathcal{A}_m^{[k]}$. Mówimy, że dla tego eksperymentu istnieje *klasyczny model dla prawdopodobieństw* wyników pomiarów, wtedy i tylko wtedy, gdy każda obserwabla $\mathcal{A}_{x^{[k]}}^{[k]}$ może być przedstawiona jako zmienna losowa na jednej, wspólnej przestrzeni zdarzeń, i jeśli przypisanie to jest *niekontekstualne*, co oznacza, że nie zależy ono od tego, jakie obserwable są mierzone na innych podukładach. Zakłada się, że zmienne losowe przypisane do wszystkich możliwych pomiarów mają łączny rozkład prawdopodobieństwa. Model ten jest prostym przykładem *Kołmogorowskiego modelu probabilistycznego* [38, 15], i ma co najmniej trzy interpretacje:

- *model lokalnych zmiennych ukrytych* [7, 39, 8]; w tym modelu zakładamy, że łączny rozkład prawdopodobieństwa dla wyników pomiarów $y^{[1]}, \ldots, y^{[n]}$ pod warunkiem wyboru obserwabli $\mathcal{A}_{x^{[1]}}^{[1]}, \ldots, \mathcal{A}_{x^{[n]}}^{[n]}$ ma postać [26, 8]:

$$p(y^{[1]}, \ldots, y^{[n]} | x^{[1]}, \ldots, x^{[n]}) = \int_{\lambda \in \mathcal{O}} \rho(\lambda) \cdot p(y^{[1]} | x^{[1]}, \lambda) \cdot \ldots \cdot p(y^{[n]} | x^{[n]}, \lambda) \, \mathrm{d}\lambda; \tag{17}$$

  model ten reprezentuje rozumienie klasyczności korelacji, jakie zrodziło się z dyskusji EPR [1] i Bella [7], w którym podkreśla się rolę λ jako ukrytego parametru, który nie jest obecny w formaliźmie kwantowym; zakłada się, że w momencie, kiedy układ jest przygotowywany, jest mu przypisana pewna wartość λ, tak, że kiedy następnie układ ten jest podzielony na podukłady i rozdystrybuowany w przestrzeni, każdy z podukładów posiada informację o wartości tego parametru; ponadto λ może przyjmować różne wartości dla każdego powtórzenia eksperymentu; zależność ta jest opisana rozkładem prawdopodobieństwa $\rho(\lambda)$;

- *model lokalnego realizmu* [39]; model ten powstaje z połączenia założeń: realizmu i lokalności; realizm postuluje istnienie wartości wszystkich możliwych obserwabli, natomiast lokalność uzasadnia fakt, że są one przypisane tym obserwablom w sposób niekontekstualny; model ten jest szczególnym przypadkiem modelu zmiennych ukrytych, w którym zmiennymi ukrytymi są wartości obserwabli;

- *algorytm probabilistyczny w modelu obliczeń rozproszonych* [39],[F]; w tej, najbardziej operacyjnej, interpretacji zakłada się, że n jednostek obliczeniowych (procesorów), z nieograniczoną mocą obliczeniową, współdzieli losowy ciąg λ; model ten zakłada, że istnieje algorytm randomizowany, który dla każdego zbioru lokalnych danych wejściowych $x^{[1]}, \ldots, x^{[n]}$ pozwala wszystkim procesorom wyprodukować dane wyjściowe $y^{[1]}, \ldots, y^{[n]}$, których rozkład prawdopodobieństwa ma postać (17); bity wyjściowe są obliczane przez procesory tylko i wyłącznie w oparciu o lokalne dane wejściowe oraz współdzielone liczby losowe λ, niedopuszczalna jest natomiast komunikacja pomiędzy procesorami;

Aby uniknąć niekończącej się dyskusji o to, która z powyższych interpretacji jest najbardziej adekwatna, będziemy model (17) nazywać po prostu *modelem klasycznym*.

Można zdefiniować słabszą wersję modelu klasycznego, zwaną *klasycznym modelem dla korelacji* [26, 40], którego istnienie w wielu przypadkach można udowodnić dużo łatwiej. Mówimy, że dla opisanego wcześniej scenariusza Bellowskiego istnieje model dla korelacji, wtedy i tylko wtedy, gdy funkcja korelacji wyników lokalnych pomiarów ma postać:

$$E(x^{[1]}, \ldots, x^{[n]}) = \langle \mathcal{A}^{[1]}_{x^{[1]}} \ldots \mathcal{A}^{[n]}_{x^{[n]}} \rangle_\rho = \int_{\lambda \in \mathcal{O}} \rho(\lambda) \cdot I^{[1]}_{x^{[1]}}(\lambda) \cdot \ldots \cdot I^{[n]}_{x^{[n]}}(\lambda)\, \mathrm{d}\lambda, \quad (18)$$

gdzie funkcje binarne $I^{[k]}_{x^{[k]}}(\lambda)$, zwane *funkcjami odpowiedzi* [41, 26], odpowiadają wartościom obserwabli $\mathcal{A}^{[k]}_{x^{[k]}}$ zmierzonym przez k-tego obserwatora, dla ustalonej wartości ukrytego parametru λ.

Różnica pomiędzy warunkami (17) a (18) polega na tym, że (17) jest dużo silniejszy. Istnienie modelu dla prawdopodobieństw jednoznacznie wyznacza model dla korelacji, jednak implikacja w drugą stronę nie zachodzi. Mając model dla korelacji można zawsze wyznaczyć (zazwyczaj niejednoznaczny) *ukryty rozkład prawdopodobieństwa* dla wszystkich możliwych wyników pomiarów [42]. Jeśli jednak potraktujemy ten rozkład jako rozkład łączny, możemy otrzymać korelacje niższych rzędów niezgodne z przewidywaniami kwantowymi.

Twierdzenie udowodnione przez Żukowskiego i Bruknera [42] podaje warunek wystarczający na istnienie modelu dla korelacji, jeśli pomiary wykonywane są na kubitach. Rozważmy n-kubitowy eksperyment typu Bella, w którym każdy obserwator ma do wyboru dwie różne obserwable. Jeśli dla każdego zbioru lokalnych układów współrzędnych $\{x_1, \ldots, x_n\}$ zachodzi [42]:

$$\sum_{x_1, \ldots, x_n = 1,2} T^2_{x_1, \ldots, x_n} \leqslant 1, \quad (19)$$

to dla funkcji korelacji odpowiadającej dowolnym wyborom obserwabli w tym scenariuszu istnieje opis klasyczny w sensie modelu (18).

Aby scharakteryzować nieklasyczność korelacji wielocząstkowych, zazwyczaj poszukuje się dowodu nieistnienia modelu dla prawdopodobieństw (17) lub modelu dla pełnych korelacji pomiędzy wszystkimi podukładami (18). W pracy [C] pokazujemy, że podejście to jest niewystarczające, aby opisać całościową strukturę nieklasycznych korelacji.

Rozważmy następującą klasę mieszanych stanów splątanych:

$$\rho_n^e = \frac{1}{2}\,|D_n^e\rangle\,\langle D_n^e| + \frac{1}{2}|D_n^{n-e}\rangle\langle D_n^{n-e}|, \tag{20}$$

gdzie $|D_n^e\rangle$ oznacza n-cząstkowy stan Dicke'go z e wzbudzeniami (16). Stany ρ_n^e są prawdziwie n-cząstkowo splątane. Mimo tego, dla nieparzystego n nie posiadają one korelacji pomiędzy nieparzystymi liczbami podukładów, w tym również — pełnych korelacji n-cząstkowych. Oznacza to, że korelacje pomiędzy nieparzystą ilością podukładów posiadają trywialny model klasyczny (18) – model białego szumu. W pracy [C] pokazujemy, że stan ρ_5^2 posiada również klasyczne modele dla korelacji pomiędzy dowolnymi dwoma, jak również pomiędzy dowolnymi czterema kubitami, co wynika wprost z warunku (19). Zatem stan ρ_5^2 posiada klasyczny model dla korelacji pomiędzy dowolną ustaloną ilością podukładów, jednakże dla tego stanu nie istnieje globalny model dla prawdopodobieństw. Operacyjnie oznacza to, że dla dowolnego podzbioru lokalnych obserwabli $\{a_{i_1}, \ldots, a_{i_k}\}$ odpowiadających podukładom $i_1, \ldots, i_k$, gdzie $k \leqslant 5$, istnieje algorytm randomizowany, który pozwala zasymulować k-cząstkową funkcję korelacji dla tych obserwabli na stanie ρ_5^2, w oparciu o znajomość lokalnych ustawień i współdzielonych ciągów liczb losowych.

Ponieważ globalny model dla prawdopodobieństw w eksperymencie Bella z dwoma ustawieniami pomiarowymi dla obserwatora w tym przypadku nie istnieje, klasyczne modele dla korelacji pomiędzy dowolną ustaloną liczbą podukładów muszą być wzajemnie niekompatybilne. Oznacza to, że *ukryte rozkłady prawdopodobieństwa* jakie wynikają z tych modeli nie mogą być rozszerzone do jednego rozkładu łącznego (17). Niekompatybilność ta może pojawić się zarówno pomiędzy modelami dla korelacji dwucząstkowych i czterocząstkowych, jak również pomiędzy modelami dla tej samej liczby cząstek, ale innego wyboru podukładów. Niekompatybilność ta może być wykazana wprost poprzez łamanie nierówności Bella, która zawiera wszystkie możliwe korelacje dwu- i czterocząstkowe:

$$E_{\pi(11110)} + E_{\pi(22220)} + E_{\pi(12220)} - E_{\pi(21110)} - E_{\pi(11000)} - E_{\pi(22000)} \leqslant 6, \tag{21}$$

gdzie indeksy 1 i 2 oznaczają ustawienia dla danych obserwatorów, indeksy 0 oznaczają "pomiary" σ_0 (czyli korelacje niższych rzędów) a $E_{\pi(ijklm)}$ oznacza sumę wszystkich możliwych funkcji korelacji, otrzymanych z permutacji ustawień pomiarowych i, j, k, l, m. Następujące ustawienia pomiarowe:

$$\vec{s}_1 = (\cos\tfrac{\pi}{5}, -\sin\tfrac{\pi}{5}, 0), \tag{22}$$

$$\vec{s}_2 = (\cos\tfrac{\pi}{20}, \sin\tfrac{\pi}{20}, 0), \tag{23}$$

dają prawie optymalne łamanie nierówności (21). Lewa strona (21) dla stanu ρ_5^2 wynosi 7.7831, co jest bliskie maksymalnej wartości kwantowej równej 7.8217.

Powyższy przykład pokazuje, że kiedy bada się stany splątane pod kątem istnienia klasycznych modeli, ich nieklasyczność jest bardzo subtelna. Pomimo,

że stan ρ_5^2 jest prawdziwie 5-cząstkowo splątany, a zatem silnie nieklasyczny, jego korelacje pomiędzy dowolną ustaloną ilością podukładów w scenariuszu dwóch ustawień dla obserwatora są klasyczne w sensie modelu (18). Pokazuje to, że w scenariuszu z ustaloną ilością ustawień pomiarowych w lokalnych podukładach, korelacje nie dają pełnego opisu kwantowej niekompatybilności, i w niektórych przypadkach trzeba wprost sprawdzić, czy istnieje klasyczny model dla prawdopodobieństw [43].

3.2 Eksperymentalnie efektywna detekcja wielocząstkowego splątania za pomocą warunków nieliniowych

Jedną z głównych trudności w detekcji wielocząstkowego splątania jest fakt, że zbiory stanów k-cząstkowo splątanych nie są wypukłe. W ogólności udowodnienie, że dany wektor należy do zbioru, który nie jest wypukły, jest zadaniem trudnym. Dużo łatwiej znaleść położenie danego stanu kwantowego względem pewnego zbioru wypukłego – np. zbioru stanów k-separowalnych (3). Poprzez wykluczenie przynależności badanego stanu do danych klas separowalności (3), dostajemy informację o splątaniu zawartym w tym stanie: stan n-cząstkowy, który nie jest k-separowalny, zawiera splątanie pomiędzy co najmniej $\lceil \frac{n}{k-1} \rceil$ cząstkami.

Precyzyjna geometryczna charakteryzacja zbioru S_{k-sep} jest trudna. Zbiór ten nie jest wielowymiarowym wielościanem, nie można go zatem opisać za pomocą skończonej ilości równań liniowych. Z drugiej strony zbiór ten może być opisany za pomocą ciągłej rodziny funkcjonałów liniowych, zwanych *świadkami splątania* [44, 4], co wynika z twierdzenia Hahna-Banacha. Każdemu takiemu funkcjonałowi odpowiada pewien operator hermitowski [2], a zatem wielkość bezpośrednio mierzalna. W praktyce metoda ta jest z kilku powodów problematyczna. Po pierwsze, operator reprezentujący danego świadka musi dać się przedstawić jako iloczyn tensorowy obserwabli lokalnych [4], i to w taki sposób, żeby liczba lokalnych pomiarów potrzebnych do detekcji splątania była rozsądnie mała. Po drugie, świadek musi być precyzyjnie dobrany do badanego stanu. Pierwszy z powyższych problemów został rozwiązany jedynie w kilku konkretnych przypadkach [45, 46], a drugi został rozwiązany częściowo w przypadku dwucząstkowym za pomocą nieliniowych poprawek [47].

W pracach [A] i [D] proponujemy znacznie bardziej uniwersalną metodę detekcji splątania, opartą na warunku (12). Nasza metoda jest z definicji dopasowana do scenariusza pomiarów lokalnych. Proponowane warunki na splątanie mają formę nieliniowych funkcjonałów, co czyni je bardziej ogólnymi i mniej zależnymi od wiedzy o badanym stanie. Ponadto nasza metoda często wymaga jedynie kilku pomiarów aby potwierdzić splątanie.

W pracy [A] wyprowadziliśmy kilka nieliniowych warunków na splątanie, wynikających bezpośrednio z warunku (12). W przypadku trzech kubitów, wyprowadziliśmy warunki, które nie faworyzują żadnej rodziny stanów splątanych. Biorąc iloczyn skalarny (6) oparty na metryce $G_{\vec{\mu}\vec{\nu}}$ (7) w postaci delty Kronec-

[2] Wynika to z faktu, że przestrzeń wszystkich liniowych ciągłych funkcjonałów na przestrzeni operatorów klasy śladowej jest izomorficzna z algebrą ograniczonych operatorów na przestrzeni Hilberta danego układu.

kera otrzymujemy:

Jeśli spełniona jest następująca nierówność:

$$\max_{\pi,\pi(\hat{O}\otimes\hat{O}',\mathbb{1})} \sqrt{\sum_{i=1}^{3} \left(\left|T_{\pi(11i)} - T_{\pi(22i)}\right| + \left|T_{\pi(33i)}\right|\right)^2} < ||T||^2, \tag{24}$$

to stan opisywany tensorem korelacji T jest prawdziwie trójcząstkowo splątany.

Maksymalizacja lewej strony nierówności wykonywana jest po wszystkich permutacjach podukładów, oraz po wszystkich lokalnych obrotach na podukładach, po których przy danej permutacji nie wykonuje się sumowania. Warunek ten jest bardzo uniwersalny: pozwala on na detekcję prawdziwie trójcząstkowego splątania zarówno stanów GHZ jak i stanów W, mimo, że należą one do dwóch zupełnie różnych rodzin, a struktura ich splątania jest zupełnie odmienna [48].

W powyższym warunku możemy zmodyfikować metrykę (a zatem również normę (7)), tak aby pozbyć się wyrazów typu $T_{\pi(33i)}$:

$$||T||_{\pi}^2 = \sum_{i,j,k=1}^{3} T_{ijk}^2 - \sum_{l=1}^{3} T_{\pi(33l)}^2. \tag{25}$$

W ten sposób otrzymujemy warunek, wymagający mniejszej ilości pomiarów:

Jeśli spełniona jest następująca nierówność:

$$\forall_{\pi} \max_{\pi(\hat{O}\otimes\hat{O}',\mathbb{1})} \sqrt{\sum_{i=1}^{3} \left(T_{\pi(11i)} - T_{\pi(22i)}\right)^2} < ||T||_{\pi}^2, \tag{26}$$

$$gdzie\ ||T||_{\pi}^2 = \sum_{i,j,k=1}^{3} T_{ijk}^2 - \sum_{l=1}^{3} T_{\pi(33l)}^2,$$

to stan opisywany tensorem korelacji T jest prawdziwie trójcząstkowo splątany.

Ponieważ pierwiastek kwadratowy po lewej stronie w nierówności (26) nie przekracza wartości 2, warunek powyższy można uprościć jeszcze bardziej:

$$\forall_{\pi} ||T||_{\pi}^2 > 2,$$

co jest bardzo efektywne eksperymentalnie. Istotnie, wystarczy mierzyć składowe tensora T występujące w $||T||_{\pi}^2$, dopóki dla wszystkich permutacji π suma (25) nie przekroczy wartości 2. W ten sposób prawdziwie trójcząstkowe splątanie może być potwierdzone za pomocą bardzo małej ilości pomiarów.

Podajemy również przykład warunku, który faworyzuje uogólnione stany GHZ n kubitów:

$$|GHZ_{\alpha}\rangle = \cos\alpha\,|0\ldots0\rangle + \sin\alpha\,|1\ldots1\rangle\,. \tag{27}$$

Nasz warunek z metryką $G_{\vec{\mu}\vec{\nu}} = \delta_{\vec{\mu},\vec{\nu}}|G_{\vec{\mu}}^{\mathrm{GHZ}}|$, gdzie $G_{\vec{\mu}}^{\mathrm{GHZ}}$ oznacza tensor korelacji stanu (27), ale z $G_{0,\ldots,0}^{GHZ} = 0$, prowadzi do optymalnej detekcji prawdziwie n-cząstkowego splątania zaszumionych stanów GHZ. Istotnie, uogólniony stan GHZ zmieszany z białym szumem:

$$\rho = v|GHZ\rangle\langle GHZ| + (1-v)\frac{1}{2^n}\mathbb{1}. \tag{28}$$

jest n-cząstkowo splątany dla $v > \frac{2^n\cos^2\alpha - 1}{2^n - 1}$. Zauważmy, że stan ten jest całkowicie separowalny jedynie dla $\alpha = 0$, co pokazuje bardzo interesującą własność

rodziny zbiorów częściowo separowalnych (3): w dowolnie małym otoczeniu stanu całkowicie separowalnego znajdują się stany zawierające splątanie pomiędzy dowolną ilością podukładów.

Warunki przedstawione w pracy [A] nie wymagają dokładnej wiedzy o stanie, którego splątanie jest testowane, mogą być zatem użyte do testowania splątania beż żadnej wiedzy o procedurze przygotowania tego stanu. Często jednak pojawia się inny problem eksperymentalny: chcemy wyprodukować bardzo konkretny stan, a następnie sprawdzić, czy szum jaki pojawił się podczas tej procedury nie zniszczył splątania. W pracy [D] przedstawiliśmy nowe podejście do świadków splątania, które można zastosować, o ile tylko potrafimy znaleść najbliższy stan separowalny ρ_0 (w ogólności k-separowalny) do badanego stanu ρ.

Nasza konstrukcja oparta jest na fakcie, że warunek (12) jest warunkiem koniecznym: dla każdego stanu ρ, który nie jest k-separowalny, istnieje metryka G, taka, że dla każdego podziału $\mathcal{S}$ na podukłady, spełniona jest nierówność (12). Metryka ta dana jest przez warunek:

$$G_{\vec{\mu}\vec{\nu}} = D_{\vec{\mu}} D_{\vec{\nu}}, \tag{29}$$

gdzie indeksy wektorowe oznaczają współrzędne w pewnej operatorowej bazie hermitowskiej, a $D_{\vec{\mu}}$ jest tensorem korelacji (4) operatora $\rho - \rho_0$. Wstawiając tę metrykę do warunku (12) otrzymujemy następujące kryterium:

$$\max_{T^{k-pr}} \sum_{\vec{\mu}\vec{\nu}} T_{\vec{\mu}} D_{\vec{\mu}} D_{\vec{\nu}} T_{\vec{\nu}}^{k-pr} < \sum_{\vec{\mu}\vec{\nu}} T_{\vec{\mu}} D_{\vec{\mu}} D_{\vec{\nu}} T_{\vec{\nu}}. \tag{30}$$

Wartość lewej strony L_G daje następujący warunek na splątanie:

$$\sum_{\vec{\mu}\vec{\nu}} T_{\vec{\mu}} D_{\vec{\mu}} D_{\vec{\nu}} T_{\vec{\nu}} > L_G \Longrightarrow \rho \textit{ określone przez } T \textit{ nie jest separowalne}, \tag{31}$$

który w przypadku odrzucania pełnej separowalności jest równoważmy standardowemu świadkowi [29].

Wartości po lewej stronie nierówności (31) mogą być ujemne, co powoduje, że trzeba zmierzyć wszystkie korelacje tam występujące. Można tego uniknąć, jeśli odpowiednio przedefiniujemy metrykę G, wymazując z niej wyrazy pozadiagonalne:

$$H_{\vec{\mu}\vec{\nu}} = D_{\vec{\mu}}^2 \delta_{\vec{\mu}\vec{\nu}}, \tag{32}$$

gdzie $\delta_{\vec{\mu}\vec{\nu}} = \delta_{\mu_1\nu_1} \cdot \ldots \cdot \delta_{\mu_n\nu_n}$ oznacza iloczyn delt Kroneckera dla wszystkich możliwych par współrzędnych. Nowa metryka H prowadzi do analogicznego warunku:

$$\max_{T^{k-pr}} \sum_{\vec{\mu}} T_{\vec{\mu}} D_{\vec{\mu}}^2 T_{\vec{\mu}}^{k-pr} < \sum_{\vec{\mu}} T_{\vec{\mu}}^2 D_{\vec{\mu}}^2. \tag{33}$$

Jeśli wyznaczymy wartość L_H lewej strony powyższej nierówności, otrzymamy kwadratowe uogólnienie świadka splątania:

$$\sum_{\vec{\mu}} T_{\vec{\mu}}^2 D_{\vec{\nu}}^2 > L_H \Longrightarrow \rho \textit{ określone przez } T \textit{ nie jest separowalne}. \tag{34}$$

Odporność powyższego warunku detekcji splątania na domieszkę białego szumu jest w ogólności inna niż w przypadku standardowego świadka (31). Jednak w przeciwieństwie do niego, zmodyfikowany kwadratowy świadek (34) zawiera

sumowanie tylko i wyłącznie liczb nieujemnych. Pozwala to na zmniejszenie liczby pomiarów koniecznych do detekcji splątania. Istotnie, jeśli po pewnej ilości pomiarów warunek (34) jest spełniony, dalsze pomiary nie są konieczne, gdyż mogą one jedynie zwiększyć wartość lewej strony w tym warunku. W pracy [D] przedstawiamy zastosowanie obu warunków: (31) i (34) do detekcji splątania kilku różnych stanów interesujących z punktu widzenia informacji kwantowej.

Przedstawione podejście do świadków splątania jest bardzo ogólne. Można je stosować do stanów kwantowych o dowolnym skończonym wymiarze. Ponadto można je używać w celu stwierdzenia, że dany stan nie należy do dowolnej innej klasy stanów wypukłych, np. stanów PPT [4].

3.3 Zastosowania wielocząstkowego splątania w różnych scenariuszach.

W rozdziale tym przedstawiam zastosowania wielocząstkowego splątania w kwantowej metrologii i w teorii kwantowych obliczeń rozproszonych.

3.3.1 Precyzyjna estymacja nieznanych parametrów

Jednym z najważniejszych dotychczasowych zastosowań wielocząstkowego splątania jest *kwantowa metrologia* [22]. Dziedzina ta powstała z badań nad możliwością precyzyjnej estymacji przesunięć fazy w interferometrach [49], a następnie została uogólniona, jako teoria precyzyjnej estymacji różnych parametrów fizycznych w oparciu o pomiary na stanach splątanych. Badania te są niezwykle istotne z punktu widzenia spektroskopii atomowej [50], przy konstruowaniu zegarów atomowych [51] oraz w projekcie detekcji fal grawitacyjnych [52].

W najogólniejszym schemacie metrologicznym wyróżnia się cztery fazy: trzy eksperymentalne i jedną teoretyczną. W części eksperymentalnej, na początku przygotowuje się n-cząstkowy układ próbny. Układ ten następnie ewoluuje unitarnie, przy czym ewolucja ta zależy od pewnego nieznanego parametru ω, którego wartość trzeba wyznaczyć. W końcowej fazie wyewoluowany układ jest mierzony lokalnymi uogólnionymi pomiarami kwantowymi[3] (pomiarami typu POVM). Wyniki tych pomiarów są następnie przetwarzane w procesie estymacji parametru ω.

W ogólności im większy jest układ próbny, tym większa możliwa do osiągnięcia precyzja estymacji ω. Okazuje się, że jeśli dodatkowo układ próbny składa się z n cząstek skorelowanych klasycznie (a zatem znajdujących się w stanie separowalnym), najlepsza możliwa precyzja estymacji skaluje się jak $1/\sqrt{n}$, co jest bezpośrednim wnioskiem z *twierdzenia Cramera-Rao* w teorii estymacji [53, 54]. Jeśli jednak początkowy stan układu próbnego jest wielocząstkowym stanem splątanym, optymalna precyzja estymacji osiąga skalowanie $1/n$, zwane *ograniczeniem Heisenberga*. Intuicyjnym powodem tak istotnego zwiększenia asymptotycznej precyzji estymacji jest fakt, że funkcja korelacji dla pomiarów lokalnych na silnie splątanym stanie wielocząstkowym jest znacznie bardziej wrażliwa na ewolucję unitarną, niż funkcja korelacji stanu separowalnego. Niestety okazuje się, że ten *kwantowy zysk precyzji* jest niezwykle wrażliwy na dekoherencję. Załóżmy, że układ próbny składa się z n kubitów, z których każdy podlega zależnej

[3]Założenie to nie zmniejsza ogólności rozważań, gdyż udowodniono, że dopuszczenie globalnych pomiarów nie zwiększa precyzji estymacji.

od ω ewolucji unitarnej, a równocześnie jest wystawiony na wpływ ogólnego lokalnego szumu. Taki rodzaj ewolucji opisywany jest równaniem Kossakowskiego-Lindblada [55, 56]:

$$\frac{\partial \rho\,(t)}{\partial t} = -i[H, \rho] + \mathcal{L}\,(\rho)\,, \tag{35}$$

gdzie Hamiltonian $H = \frac{1}{2}\omega\sigma_{\vec{r}}$ jest *generatorem unitarnego obrotu* wokół osi $\vec{r}$, podczas gdy operator Liouville'a:

$$\mathcal{L}(\rho) = -\frac{1}{2}\gamma\left[\rho - \alpha_x\sigma_x\rho\sigma_x - \alpha_y\sigma_y\rho\sigma_y - \alpha_z\sigma_z\rho\sigma_z\right], \tag{36}$$

opisuje szum generowany przez $\{\sigma_x, \sigma_y, \sigma_z\}$. Ewolucja takiego układu otwartego może być przedstawiona w języku kanałów kwantowych [57, 58, 59]:

$$\rho(t) = \sum_{i=1}^{4} K_i(t)\rho K_i^{\dagger}(t), \tag{37}$$

gdzie operatory ewolucji K_i zwane są operatorami Krausa. Niedawno pokazano, że dowolny szum opisany przez kanał pełnego rzędu (tj. kanał (37) posiadający niezerowe wszystkie operatory Krausa) redukuje skalowanie precyzji estymacji do skalowania klasycznego $1/\sqrt{n}$ [60]. Pokazuje to, że praktyczne możliwości kwantowej metrologii wydają się być mocno ograniczone.

W pracy [E] proponujemy nieco zmodyfikowany schemat metrologiczny, który pozwala pokonać to ograniczenie w przypadku, gdy generator szumu jest prostopadły do generatora ewolucji. Nasz pomysł oparty jest na następującej obserwacji. Precyzja estymacji parametru ω spełnia kwantowe ograniczenie Cramera-Rao [61]:

$$\delta\omega \geqslant \frac{1}{\sqrt{(\mathcal{F}(\rho_\omega)\cdot T)/t}}, \tag{38}$$

gdzie T jest całkowitym czasem eksperymentu, t jest czasem jednej rundy (czyli czasem ewolucji układu próbnego), a $\mathcal{F}(\rho_\omega)$ jest kwantową informacją Fishera (quantum Fisher information – QFI) [62]. QFI jest funkcją stanu końcowego w procesie metrologicznym i opisuje ilość informacji o parametrze ω, jaką można wyciągnąć z pomiarów na stanie końcowym, przy założeniu, że cała procedura estymacji jest optymalna. Zazwyczaj przyjmuje się, że zarówno T jak i t są ustalone, a kwantowa informacja Fishera maksymalizowana jest po wszystkich możliwych stanach początkowych układu próbnego. Jeśli jako stan początkowy weźmiemy n-kubitowy stan GHZ, możemy otrzymać kwadratowe skalowanie $\mathcal{F}(\rho_\omega) \propto n^2$ kwantowej informacji Fishera, co daje optymalną kwantową precyzję. Niestety, wynik z pracy [60] pokazuje, że powrót do skalowania klasycznego $\mathcal{F}(\rho_\omega) \propto n$ jest asymptotycznie nieunikniony, jeśli tylko kanał kwantowy (37) jest pełnego rzędu. Aby rozwiązać ten problem, stosujemy nieco odmienne podejście do kwantowej metrologii, w którym jedynie całkowity czas eksperymentu T jest ustalony, natomiast czas ewolucji t jest optymalizowany dla każdego n z osobna, tak aby zmaksymalizować wielkość[4] $\mathcal{F}(\rho_\omega)/t$. Podejście to było wcześniej rozważane w bardzo zawężonej wersji, w przypadku gdy generator szumu jest współliniowy z generatorem ewolucji [50, 63].

[4] Zauważmy, że $\mathcal{F}(\rho_\omega)$ jest uwikłaną funkcją t, poprzez zależność od ρ_ω.

W pracy [E] pokazujemy, że jeśli generator szumu jest prostopadły do generatora ewolucji, to początkowy n-cząstkowy stan GHZ prowadzi do asymptotycznego skalowania kwantowej informacji Fishera w postci $\mathcal{F}(\rho_\omega) \propto n^{\frac{5}{3}}$. Oznacza to, że precyzja estymacji skaluje się jak $\delta\omega \propto n^{-\frac{5}{6}}$, co jest skalowaniem silniejszym niż klasyczne, ale nie osiągającym granicy Heisenberga.

W naszych rozważaniach zakładamy, że generator ewolucji ma postać σ_z, podczas, gdy generator szumu we wzorze (36) — σ_x. Jako stan początkowy przyjmujemy n-cząstkowy stan GHZ (27) z $\alpha = \frac{\pi}{4}$. Dla tak zdefiniowanego kanału kwantowego wyznaczyliśmy analityczną postać operatorów Krausa (37). Chociaż otrzymaliśmy również analityczną postać kwantowej informacji Fishera, byliśmy zmuszeni obliczyć wyrażenie $\max_t \mathcal{F}(\rho_\omega)/t$ numerycznie, ze względu na niezwykle skomplikowaną postać $\mathcal{F}(\rho_\omega)$. Przeprowadzając maksymalizację względem czasu t dla $n = 2, \ldots, 5000$, otrzymaliśmy skalowanie precyzji $\delta\omega \propto n^{-\frac{5}{6}}$. Potwierdziliśmy to skalowanie dla n sięgającego 10^8 za pomocą numerycznej metody rozszerzania kanałów zaproponowanej w pracach [60, 64].

Badaliśmy również przypadek, w którym generator szumu jest nieznacznie odchylony od kierunku prostopadłego do generatora ewolucji σ_z: przyjęliśmy $\alpha_x = 1 - \epsilon$ i $\alpha_z = \epsilon$ we wzorze (36). W tym przypadku numeryczna analiza wskazuje, że niepewność estymacji $\delta\omega$ początkowo skaluje się ponadklasycznie, jednak dla większych wartości n skalowanie precyzji powraca do skalowania klasycznego. Oszacowaliśmy, że krytyczna wartość n, dla której skalowanie precyzji zaczyna wracać do klasycznego ma przybliżoną postać: $n_{crit} \approx 3\omega/(8\gamma\epsilon^{3/2})$.

Nasze badania stanowią silny numeryczny dowód na to, że jeśli szum jest prostopadły do ewolucji, to precyzja estymacji nieznanej częstości ω skaluje się ponadklasycznie dla $n \to \infty$. Jednakże dowolnie małe odchylenie od wzajemnej prostopadłości tych generatorów przywraca klasyczne skalowanie asymptotyczne. Chociaż nie znaleźliśmy formalnego analitycznego dowodu naszych wniosków, przedstawione wyniki stanowią motywację do dalszego poszukiwania efektywnych realistycznych protokołów metrologicznych [65].

3.3.2 Kwantowe obliczenia rozproszone

Obliczenia rozproszone stanowią szeroką klasę modeli obliczeniowych, których cechą wspólną jest istnienie autonomicznych jednostek obliczeniowych (procesorów), wyposażonych w lokalną pamięć. Procesory te komunikują się pomiędzy sobą w celu rozwiązania wspólnego problemu. W pracy [F] rozważamy grafowy model rozproszony, zwany $\mathcal{LOCAL}$ [66]. W modelu tym zakłada się, że n procesorów przeprowadza obliczenia w *synchronicznych rundach*, przy czym każda runda składa się z dwóch faz: obliczeń lokalnych oraz komunikacji pomiędzy sąsiednimi procesorami. Lokalna moc obliczeniowa każdego procesora, jak również ilość komunikacji pomiędzy sąsiednimi procesorami nie są ograniczone. Dane wejściowe do problemu mają postać grafu etykietowanego G_x, który pełni dwie funkcje: definiuje lokalne dane wejściowe $x(v)$ dla każdego procesora v, jak również topologię połączeń komunikacyjnych pomiędzy nimi. Dane wyjściowe są zdefiniowane jako wektor, którego składowe $y(v)$ oznaczają wartość liczbową na wyjściu z v-tego procesora. *Problem* jest zdefiniowany jako odwzorowanie pomiędzy zbiorem danych wejściowych G_x a zbiorem akceptowalnych danych wyjściowych. *Złożoność problemu* mierzona jest minimalną ilością rund, potrzebną do rozwiązania problemu z prawdopodobieństwem równym 1.

W ostatnich latach pojawiło się kilka prac, w których starano się wprowadzić

do obliczeń rozproszonych efekty kwantowe, takie jak splątanie czy też kwantową komunikację. Zbiór tych hybrydowych modeli określany jest mianem *kwantowych obliczeń rozproszonych* [67]. Wszystkim tym próbom brakowało spójnego i ścisłego schematu, co doprowadziło do przecenienia roli efektów kwantowych przy rozwiązywaniu pewnych problemów rozproszonych[5][69, 70, 71].

W pracy [F] przedstawiamy konstrukcję kilku kwantowych rozszerzeń modelu $\mathcal{LOCAL}$ oraz hierarchię ich mocy obliczeniowych. Definiujemy również model φ-$\mathcal{LOCAL}$, zawierający wszystkie kwantowe rozszerzenia, który reprezentuje pojęcie *fizycznej lokalności* w modelu obliczeń rozproszonych.

Synchroniczne obliczenia rozproszone są jednym z trzech modeli obliczeniowych, w których dodanie zasobów kwantowych redukuje złożoność obliczeniową. Natura tej redukcji złożoności nie jest dziś w pełni rozumiana, choć znane są pewne intuicje. W modelu drzewa decyzyjnego, który obejmuje najbardziej znane kwantowe algorytmy, takie jak algorytm Deutsch-Jozsa [72] czy algorytm Simon'a [73], kwantowa redukcja złożoności tłumaczona jest faktem, że kwantowe wyrocznie mogą przetwarzać superpozycje dużej ilości stanów z bazy obliczeniowej [74]. W modelu *złożoności komunikacyjnej*, czyli modelu rozproszonym, w którym złożoność mierzona jest przez minimalną liczbę wszystkich komunikowanych bitów pomiędzy procesorami, kwantowa redukcja złożoności pojawia się w dwóch scenariuszach. W pierwszym porównuje się moc obliczeniową komunikacji klasycznej (bitów) i kwantowej (kubitów), przy czym porównywalność tych dwóch sposobów komunikacji uzasadniana jest ograniczeniem Holevo [75]. W drugim scenariuszu porównuje się moc obliczeniową układu rozproszonego, w którym procesory komunikują się klasycznie i mają dostęp do zasobów klasycznych (współdzielone bity losowe) bądź kwantowych (splątanie) [39]. .

W pracy [F] pokazujemy, że w synchronicznym modelu obliczeń rozproszonych kwantowa redukcja złożoności związana jest z oboma powyższymi przypadkami redukcji złożoności komunikacyjnej. Wskazuje to na istotne powiązania pomiędzy złożonością w sensie ilości rund i złożonością w sensie ilości komunikowanych bitów. Pokazujemy również, że moc obliczeniowa wszystkich kwantowych rozszerzeń jest istotnie ograniczona przez zasadę *fizycznej lokalności*.

W pierwszym kroku definiujemy dwa rozszerzenia modelu $\mathcal{LOCAL}$, które polegają na wprowadzeniu dodatkowych zasobów w fazie inicjalizacji algorytmu, czyli *zanim* dane wejściowe w postaci grafu G_x są przesłane do procesorów. W pierwszym rozszerzeniu, nazwanym przez nas $\mathcal{LOCAL}^+\mathcal{S}$, zakłada się, że zbiór stanów początkowych wszystkich procesorów wybierany jest losowo zgodnie z zadanym rozkładem prawdopodobieństwa. W sensie fizycznym odpowiada to wytworzeniu stanu separowalnego, który jest współdzielony przez procesory. W sensie obliczeniowym jest to równoważne stwierdzeniu, że procesory mają dostęp do wspólnego źródła losowości. Ponieważ model $\mathcal{LOCAL}$ nie narzuca żadnych ograniczeń na lokalną pamięć ani na lokalną moc obliczeniową, ilość tej *współdzielonej losowości* jest nieograniczona. W drugim rozszerzeniu, $\mathcal{LOCAL}^+\mathcal{E}$, każdy procesor wyposażony jest w rejestr kwantowy, pozwalający przetrzymywać cząstki kwantowe o dowolnym wymiarze przestrzeni stanów. W modelu tym zakładamy, że w fazie inicjalizacji można wytworzyć dowolny (w ogólności silnie splątany) stan kwantowy współdzielony przez wszystkie procesory.

Definiujemy również drugi rodzaj rozszerzenia, $\mathcal{LOCAL}^+\mathcal{Q}$, które dopuszcza

[5]Zauważmy, że podobny problem pojawił się w przypadku tzw. *statycznych gier kwantowych* [68].

dowolną komunikację kwantową pomiędzy procesorami sąsiadującymi ze sobą zgodnie z grafem G_x.

Definiujemy $\mathcal{LOCAL}[t]$ jako klasę złożoności, zawierającą problemy, które mogą być rozwiązane w modelu $\mathcal{LOCAL}$ w co najwyżej t rundach obliczeń. Przez analogię definiujemy klasy złożoności $\mathcal{LOCAL}^+\mathcal{S}[t]$, $\mathcal{LOCAL}^+\mathcal{E}[t]$ i $\mathcal{LOCAL}^+\mathcal{Q}[t]$. Hierarchię zdefiniowanych tu modeli można ustalić za pomocą następujących argumentów:

- $\mathcal{LOCAL} \subsetneq \mathcal{LOCAL}^+\mathcal{S}$; wszystkie problemy zawierające się w $\mathcal{LOCAL}[t]$ należą do $\mathcal{LOCAL}^+\mathcal{S}[t]$ z trywialną inicjalizacją; z drugiej strony problem nadania jednoznacznych etykiet wszystkim procesorom przy pustych danych wejściowych nie może być rozwiązany w $\mathcal{LOCAL}[t]$ dla żadnego t, ale może być rozwiązany w $\mathcal{LOCAL}^+\mathcal{S}[0]$.

- $\mathcal{LOCAL}^+\mathcal{S} \subsetneq \mathcal{LOCAL}^+\mathcal{E}$; wszystkie problemy należące do $\mathcal{LOCAL}^+\mathcal{S}[t]$ należą również do klasy $\mathcal{LOCAL}^+\mathcal{E}[t]$, jeśli w trakcie inicjalizacji wytworzymy stan separowalny; z drugiej strony trójcząstkowy problem *modulo*-4 [76, 77] z pustym grafem początkowym nie może być rozwiązany w $\mathcal{LOCAL}^+\mathcal{S}[t]$ dla żadnego t, podczas gdy może on być rozwiązany w $\mathcal{LOCAL}^+\mathcal{E}[0]$, jeśli podczas inicjalizacji wytworzy się trójcząstkowy stan GHZ współdzielony pomiędzy procesorami; fakt ten jest równoważny z tzw. paradoksem GHZ [78]; redukcja złożoności w tym przypadku ma charakter redukcji złożoności komunikacyjnej: korelacje stanu GHZ nie mogą być zasymulowane za pomocą lokalnie obliczalnych funkcji przy dostępie do dowolnej ilości współdzielonej losowości, ale bez możliwości komunikacji.

- $\mathcal{LOCAL} \subsetneq \mathcal{LOCAL}^+\mathcal{Q}$; wszystkie problemy należące do $\mathcal{LOCAL}[t]$ należą również do $\mathcal{LOCAL}^+\mathcal{Q}[t]$, jeśli założymy brak kwantowej komunikacji; rozważmy teraz problem zdefiniowany na $n = 3k + 1$ procesorach, gdzie graf wejściowy ma postać gwiazdy o trzech gałęziach; trzy zewnętrzne wierzchołki gwiazdy mają za zadanie rozwiązać problem modulo-4; w ramach modelu $\mathcal{LOCAL}^+\mathcal{Q}$ można to osiągnąć w k rundach, tworząc stan GHZ w centralnym procesorze, a następnie rozsyłając go do zewnętrznych węzłów; proces ten nie może być zasymulowany poprzez przesłanie dowolnej ilości klasycznej informacji pomiędzy węzłem centralnym a węzłami na wierzchołkach, ale wymaga on bezpośredniej komunikacji pomiędzy tymi węzłami, na co potrzeba $2k$ rund; w tym przypadku redukcja złożoności powiązana jest z faktem, że rozesłanie splątanych kubitów nie może być zasymulowane za pomocą przesłania dowolnej ilości klasycznie skorelowanych bitów.

- $\mathcal{LOCAL}^+\mathcal{Q} \subsetneq \mathcal{LOCAL}^+\mathcal{E}$; problem modulo-4 z pustym grafem wejściowym, który należy do $\mathcal{LOCAL}^+\mathcal{E}[0]$ nie może być rozwiązany w ramach $\mathcal{LOCAL}^+\mathcal{Q}[t]$, ponieważ nie ma możliwości komunikacji pomiędzy procesorami; z drugiej strony kwantowa komunikacja w ramach modelu $\mathcal{LOCAL}^+\mathcal{E}$ może być zasymulowana za pomocą kwantowej teleportacji [19], stąd każdy problem rozwiązywalny w $\mathcal{LOCAL}^+\mathcal{Q}[t]$ może być rozwiązany w $\mathcal{LOCAL}^+\mathcal{E}[t]$.

- $\mathcal{LOCAL}^+\mathcal{Q}$ i $\mathcal{LOCAL}^+\mathcal{S}$ są nieporównywalne.

Wszystkie powyższe rozszerzenia są całkowicie zgodne z *fizyczną lokalnością*, która w kontekście modelu $\mathcal{LOCAL}$ oznacza, że zbiór danych wejściowych danego procesora v po t rundach obliczeń może mieć wpływ na prawdopodobieństwa danych wyjściowych w procesorach, które znajdują się w odległości co najwyżej t krawędzi od v, przy czym własność ta musi zachodzić dla dowolnego początkowego grafu G_x. Intuicja ta odpowiada skończonej prędkości propagacji informacji w modelach sieciowych z oddziaływaniem najbliższych sąsiadów [79]. Definiujemy model φ-$\mathcal{LOCAL}$, jako najsłabszy model, który spełnia powyższe rozumienie lokalności. W rozszerzonej wersji pracy [80] dowodzimy, że modele $\mathcal{LOCAL}$, $\mathcal{LOCAL}^+\mathcal{S}$, $\mathcal{LOCAL}^+\mathcal{Q}$ i $\mathcal{LOCAL}^+\mathcal{E}$ należą do φ-$\mathcal{LOCAL}$, przy czym pozostawiamy otwartym pytanie, czy zawieranie to jest ścisłe. Zauważmy, że model φ-$\mathcal{LOCAL}$ zdefiniowany jest bez określenia dokładnych fizycznych własności użytych zasobów. Definicja φ-$\mathcal{LOCAL}$ zawężona do $t = 0$ odpowiada pojęciu *niesygnalizowania* w tzw. uogólnionych teoriach probabilistycznych [81].

Wprowadzenie modelu φ-$\mathcal{LOCAL}$ znacznie upraszcza dowodzenie ograniczeń dolnych na złożoność obliczeniową w ramach kwantowych rozszerzeń modelu $\mathcal{LOCAL}$. Istotnie, dużo łatwiej jest udowodnić, że każde rozwiązanie danego problemu w czasie k rund łamie fizyczną lokalność, niż udowodnić wprost, że dany problem nie ma rozwiązania w k rundach w ramach modeli kwantowych. W ten sposób pokazujemy, że rozproszony problem konsensusu (*distributed consensus*) [82][6] $\notin \varphi$-$\mathcal{LOCAL}$[0], co oznacza, że nie może być on rozwiązany za pomocą jakiegokolwiek rozszerzenia kwantowego bez komunikacji, gdyż istnienie takiego rozwiązania naruszyłoby fizyczną lokalność.

W rozszerzonej wersji pracy [80] przedstawiamy formalne definicje wszystkich kwantowych rozszerzeń w języku lokalnych C^* algebr. Charakteryzacja ta motywowana jest pracami nad tzw. lokalną fizyką kwantową [83, 79, 84]. W ramach tej formalizacji podajemy ogólny dowód faktu, że wszystkie rozważane rozszerzenia modelu $\mathcal{LOCAL}$ zawierają się w modelu φ-$\mathcal{LOCAL}$.

Publikacje stanowiące rozprawę doktorską

[A] W. Laskowski, M. Markiewicz, T. Paterek and M. Żukowski, *Correlation tensor criteria for genuine multiqubit entanglement*, Phys. Rev. A **84**, 062305 (2011).

[B] M. Markiewicz, W. Laskowski, T. Paterek and M. Żukowski, *Detecting genuine multipartite entanglement of pure states with bipartite correlations*, Phys. Rev. A. **87**, 034301 (2013).

[C] W. Laskowski, M. Markiewicz, T. Paterek and M. Wieśniak, *Incompatible local hidden-variable models of quantum correlations*, Phys. Rev. A **86**, 032105 (2012).

[D] W. Laskowski, M. Markiewicz, T. Paterek and R. Weinar, *Entanglement witnesses with variable number of local measurements*, Phys. Rev. A. **88**, 022304 (2013).

[6] W *problemie konsensusu* n procesorów otrzymuje lokalne etykiety $\{x_i\}_{i=1}^n$, a ich zadaniem jest wypisać $y \in \{x_i\}_{i=1}^n$.

[E] R. Chaves, J. B. Brask, M. Markiewicz, J. Kołodyński and A. Acín, *Noisy metrology beyond the standard quantum limit*, Phys. Rev. Lett. **111**, 120401 (2013).

[F] C. Gavoille, A. Kosowski and M. Markiewicz, *What Can Be Observed Locally? Round Based Models for Quantum Distributed Computing*, Springer Lecture Notes in Computer Science **5805**, pp. 243-257 (2009).

Literatura

[1] A. Einstein, B. Podolsky, and N. Rosen. *Phys. Rev.*, 47:777, 1935.

[2] E. Schrödinger. Probability relations between separated systems. *Proc. Camb. Phil. Soc.*, 32:446, 1936.

[3] R. Horodecki and P. Horodecki. *Phys. Lett. A*, 197:147, 1994.

[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. *Rev. Mod. Phys.*, 81:865–942, 2009.

[5] W. A. Majewski. Separable and entangled states of composite quantum systems; rigorous description. *quant-ph/9711051*, 1997.

[6] I. Cuculescu. Some remarks on tensor products of standard forms of von neumann algebras. *Bolletino U.M.I.*, 7:907–919, 1993.

[7] J.S. Bell. *Physics*, 1:195, 1964.

[8] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. *arXiv[quant-ph]:1303.284*, 2013.

[9] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. *Phys. Rev. Lett.*, 23:880–884, 1969.

[10] R. Chaves. *Phys. Rev. A*, 87:022102, 2013.

[11] P. Kurzynski, M. Markiewicz, and D. Kaszlikowski. *arXiv[quant-ph]:1310.5644*, 2013.

[12] P. Kurzynski and D. Kaszlikowski. *Phys. Rev. A*, 89:012103, 2013.

[13] R. Omnès. *Rev. Mod. Phys.*, 64:339, 1992.

[14] R. B. Griffiths. *Consistent Quantum Theory*. Cambridge University Press, 2003.

[15] R. F. Streater. *Lost Causes in and beyond Physics*. Springer-Verlag, 2007.

[16] B.-G. Englert. *Eur. Phys. J. D*, 67:238, 2013.

[17] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[18] M. Żukowski, A. Zeilinger, M. Horne, and A. Ekert. *Phys. Rev. Lett.*, 71:4297, 1993.

[19] L. Accardi and M. Ohya. *arXiv:quant-ph/9912087*, 1999.

[20] G. Brassard. *arXiv:quant-ph/0101005*, 2001.

[21] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev. *Rev. Mod. Phys.*, 81:1301, 2009.

[22] V. Giovannetti, S. Lloyd, and L. Maccone. *Nature Photonics*, 5:222, 2011.

[23] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press.

[24] D. Kaszlikowski, A. Sen(De), U. Sen, V. Vedral, and A. Winter. *Phys. Rev. Lett.*, 101:070502, 2008.

[25] C. H. Bennett, A. Grudka, M. Horodecki, P. Horodecki, and R. Horodecki. *Phys. Rev. A*, 83:012312, 2011.

[26] R. F. Werner. *Phys. Rev. A*, 40:4277–4281, 1989.

[27] M. Seevinck and J. Uffink. *Phys. Rev. A*, 78:032101, 2008.

[28] M. Horodecki, P. Horodecki, and R. Horodecki. *Phys. Lett. A*, 283:1, 2001.

[29] P. Badziąg, Č. Brukner, W. Laskowski, T. Paterek, and M. Żukowski. *Phys. Rev. Lett.*, 100:140403, 2008.

[30] V. Coffman, J. Kundu, and W. K. Wootters. *Phys. Rev. A*, 61:052306, 2000.

[31] N. Gisin A. Acin and L. Masanes. *Phys. Rev. Lett.*, 97:120405, 2006.

[32] M. Pawlowski. *Phys. Rev. A*, 82:032313, 2010.

[33] P. Kurzynski, M. Markiewicz, and D. Kaszlikowski. *arXiv[quant-ph]:1312.5263*, 2013.

[34] R. Dicke. *Phys. Rev.*, 93:99, 1954.

[35] P. Parashar and S. Rana. *Phys. Rev. A*, 80:012319, 2009.

[36] A. Klyachko. *arXiv:quant-ph/0409113*, 2004.

[37] M. Christandl, R. Koenig, G. Mitchison, and R. Renner. *Comm. Math. Phys.*, 273:473–498, 2007.

[38] R. F. Streater. *arXiv:math-ph/0002049*, 2000.

[39] C. Brukner and M. Żukowski. *Bell's Inequalities: Foundations and Quantum Communication in Handbook of Natural Computing*. Springer, 2010.

[40] K. Nagata, W. Laskowski, M. Wiesniak, and M. Żukowski. *Phys. Rev. Lett.*, 93:230403, 2004.

[41] A. Fine. *Phys. Rev. Lett.*, 48:291, 1982.

[42] M. Żukowski and C. Brukner. *Phys. Rev. Lett.*, 88:210401, 1990.

[43] J. Gruca, W. Laskowski, M. Żukowski, N. Kiesel, W. Wieczorek, C. Schmid, and H. Weinfurter. *Phys. Rev. A*, 82:012118, 2010.

[44] M. Horodecki, P. Horodecki, and R. Horodecki. *Phys. Lett. A*, 223:1, 1996.

[45] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. *Phys. Rev. A*, 66:062305, 2002.

[46] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. *J. Mod. Opt.*, 50:1079, 2003.

[47] O. Gühne and N. Lütkenhaus. *Phys. Rev. Lett.*, 96:170502, 2006.

[48] W. Dür, G. Vidal, and J. I. Cirac. *Phys. Rev. A*, 62:062314, 2000.

[49] M. Holland and K. Burnett. *Phys. Rev. Lett.*, 71:1355, 1993.

[50] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac. *Phys. Rev. Lett.*, 79:3865, 1997.

[51] V. Buzek, R. Derka, and S. Massar. *Phys. Rev. Lett.*, 82:2207–2210, 1999.

[52] The LIGO Scientific Collaboration. *Nat. Phys.*, 7:962, 2011.

[53] H. Cramer. *Mathematical Methods of Statistics*. Princeton Univ. Press, 1946.

[54] C.R. Rao. *Bulletin of the Calcutta Mathematical Society*, 37:81–89, 1945.

[55] A. Kossakowski. *Rep. Math. Phys.*, 3:247, 1972.

[56] G. Lindblad. *Commun. Math. Phys.*, 48:119, 1976.

[57] E. C. G. Sudarshan et al. *Phys. Rev.*, 121:920–924, 1961.

[58] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer Verlag, 1983.

[59] E. Andersson, J. D. Cresser, and M. J. W. Hall. *J. Mod. Opt.*, 54:1695, 2007.

[60] J. Kolodyński R. Demkowicz-Dobrzaśki and M. Guta. *Nature Communications*, 3:1063, 2012.

[61] S. L. Braunstein and C. M. Caves. *Phys. Rev. Lett.*, 72:3439, 1994.

[62] A. S. Holevo. *Probabilistic and Statistical Aspect of Quantum Theory*. North-Holland, Amsterdam, 1982.

[63] B. M. Eschera, R. L. de Matos Filho, and L. Davidovich. *Nat. Phys.*, 7:406, 2011.

[64] J. Kolodyński and R. Demkowicz-Dobrzaśki. *New J. Phys.*, 15:073043, 2013.

[65] W. Dür, M. Skotiniotis, F. Fröwis, and B. Kraus. *arXiv:1310.3750 [quant-ph]*, 2013.

[66] N. Linial. *28th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 331–335, 1987.

[67] V. S. Denchev and G. Pandurangan. Distributed quantum computing: A new frontier in distributed systems or science fiction? *ACM SIGACT News - Distributed Computing Column*, 39:77–95, 2008.

[68] M. Markiewicz, A. Kosowski, T. Tylec, J. Pykacz, and C. Gavoille. *arXiv:1001.2257 [quant-ph]*, 2010.

[69] S. P. Pal, S. K. Singh, and S. Kumar. *arXiv:quant-ph/0306195*, 2003.

[70] E. D'Hondt and P. Panangaden. *Quant. Inf. Comp.*, 6:173–183, 2006.

[71] L. Helm. Brief announcement: Quantum distributed consensus. *27th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, page 445, 2008.

[72] D. Deutsch and R. Jozsa. *Proceedings of the Royal Soci- ety of London A*, 439, 1992.

[73] D.R. Simon. *Siam J. Comp.*, 26:1474, 1997.

[74] F. Brandao and M. Horodecki. *Q. Inf. Comp.*, 13:0901, 2013.

[75] A. Holevo. *Problems of Information Transmission*, 9:177–183, 1973.

[76] P. Trojek, Ch. Schmid, M. Bourennane, C. Brukner, M. Żukowski, and H. Weinfurter. *Phys. Rev. A*, 72:050305(R), 2005.

[77] M. Żukowski. On bell's theorem, quantum communication, and entanglement detection. *Foundations of Probability and Physics*, 5, 2008.

[78] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*. Kluwer, 1989.

[79] O. Bratelli and D. W. Robinson. *Operator algebras and quantum statistical mechanics, volume II.* Springer-Verlag, 1981.

[80] C. Gavoille, A. Kosowski, and M. Markiewicz. *arXiv: quant-ph/0903.1133*, 2009.

[81] A.J. Short and J. Barrett. *New J. Phys.*, 12:033034, 2010.

[82] N. Lynch. *Distributed Algorithms*. Morgan Kaufmann Publishers, 1997.

[83] O. Bratelli and D. W. Robinson. *Operator algebras and quantum statistical mechanics, volume I.* Springer-Verlag, 1979.

[84] R. Haag. *Local Quantum Physics: Fields, Particles, Algebras*. Springer, 1992.