Podsumowanie osiągnięć zawodowych

Michał Grzegorz Studziński

Wydział Matematyki, Fizyki i Informatyki
Uniwersytet Gdański
Gdańsk
2023

Spis treści

1 Imię i nazwisko

Michał Grzegorz Studziński

2 Posiadane dyplomy, stopnie naukowe lub artystyczne - z podaniem podmiotu nadającego stopień, roku ich uzyskania oraz tytułu rozprawy doktorskiej

1. Stopień doktora nauk fizycznych – 11.06.2015
   Instytucja: Wydział Matematyki, Fizyki i Informatyki, Uniwersytet Gdański, Gdańsk, Polska
   Rozprawa doktorska: Zastosowanie teorii reprezentacji grup i algebr do niektórych problemów informatyki kwantowej
   Promotor: prof. dr hab. Michał Horodecki
   Promotor pomocniczy: dr Jarosław Korbicz
   Recenzenci: prof. dr hab. Marek Kuś, prof. dr hab. Andrzej Jamiołkowski
   Źródło finansowania: Międzynarodowy Projekt Doktorancki: Physics of future quantum-based information technologies, grant MPD/2009-3/4 Fundacji na rzecz Nauki Polskiej.

2. Stopień magistra astronomii – 01.07.2010
   Instytucja: Wydział Fizyki, Astronomii i Informatyki, Uniwersytet Mikołaja Kopernika w Toruniu, Toruń, Polska
   Rozprawa magisterska: Badanie całkowalności wymiernych jednorodnych potencjałów
   Promotor: dr hab. Maria Przybylska
   Ocena: bardzo dobry

3. Stopień licencjata astronomii – 11.05.2009
   Instytucja: Fizyki, Astronomii i Informatyki, Uniwersytet Mikołaja Kopernika w Toruniu, Toruń, Polska
   Praca licencjacka: Badanie całkowalności wybranych klas wymiernych jednorodnych potencjałów
   Promotor: dr hab. Maria Przybylska
   Ocena: bardzo dobry

3 Informacja o dotychczasowym zatrudnieniu w jednostkach naukowych lub artystycznych

- 02.01.2022-obecnie, adiunkt (pełny etat naukowo-dydaktyczny)
  Instytucja: Wydział Matematyki, Fizyki i Informatyki, Uniwersytet Gdański, Gdańsk, Polska
  Bezpośredni przełożony: dr hab. Marek Krośnicki, prof. UG

- 01.01.2019-01.01.2022, adiunkt naukowy (staż podoktorski)
  Instytucja: Uniwersytet Gdański, Gdańsk, Polska
  Źródło finansowania: Narodowe Centrum Nauki (Polska), grant: Sonatina 2 (2018/28/C/ST2/00004), kierownik
  Bezpośredni przełożony: dr hab. Marcin Marciniak, prof. UG/dr hab. Marek Krośnicki, prof. UG

- 01.01.2016-31.12.2018, staż podoktorski
  Instytucja: Department of Applied Mathematics and Theoretical Physics, The University of Cambridge, Cambridge, Wielka Brytania

Opiekun naukowy: prof. Richard Jozsa
Źródło finansowania: Ministerstwo Nauki i Szkolnictwa Wyższego, grant: Mobilność Plus IV (1271/MOB/IV/ 2015/0)

- 06.2015-31.01.2106, adiunkt naukowy (staż podoktorski)
Instytucja: Wydział Matematyki, Fizyki i Informatyki/Krajowe Centrum Informatyki Kwantowej (KCIK), Uniwersytet Gdański, Gdańsk, Polska
Bezpośredni przełożony: prof. dr hab. Michał Horodecki
Źródło finansowania: Seventh framework programme EU, grant: RAndomness and QUantum EntangLement (RAQUEL), nr id: 323970

4 Omówienie osiągnięć, o których mowa w art. 219 ust. 1 pkt. 2 Ustawy

4.1 Tytuł osiągnięcia naukowego

Jednotematyczny cykl publikacji pt.: *Teoria reprezentacji grup i algebr jako narzędzie do opisu i konstrukcji nowych kwantowych protokołów przetwarzania informacji.*

4.2 Publikacje (autor/autorzy, tytuł/tytuły publikacji, rok wydania, nazwa wydawnictwa, recenzenci wydawniczy)

1. *Square-root measurements and degradation of the resource state in port-based teleportation scheme*
M. Studziński, M. Mozrzymas, P. Kopszak
Journal of Physics A: Mathematical and Theoretical **55** 375302 (2022)
IF: 1.996 / punkty MNiSW: 100
`https://arxiv.org/abs/2105.14886`

2. *Efficient multi-port teleportation schemes*
M. Studziński, M. Mozrzymas, P. Kopszak, M. Horodecki
IEEE Transactions on Information Theory **68(12)** 7892-7912 (2022)
IF: 2.978 / punkty MNiSW: 200
`https://arxiv.org/abs/2008.00984`

3. *Optimal Multi-port-based Teleportation Schemes*,
M. Mozrzymas, M. Studziński, P. Kopszak
Quantum **5**, 477 (2021)
IF: 2.921 / punkty MNiSW: 140
`https://arxiv.org/abs/2105.14886`

4. *Efficient Classical Simulation and Benchmarking of Quantum Processes in the Weyl Basis*,
D. S. França, S. Strelchuk, M. Studziński
Physical Review Letters **126** 210502 (2021)
IF: 9.185 / punkty MNiSW: 200
`https://arxiv.org/abs/2008.12250`

5. *Multiport based teleportation – protocol and its performance*
P. Kopszak, M. Mozrzymas, M. Studziński, M. Horodecki
Quantum **5**, 576 (2021)
IF: 2.921 / punkty MNiSW: 140
`https://arxiv.org/abs/2008.00856`

6. *Positive Maps From Irreducibly Covariant Operators*
   P. Kopszak, M. Mozrzymas, M. Studziński
   Journal of Physics A: Mathematical and Theoretical **53** 395306 (2020)
   IF: 1.996 / punkty MNiSW: 100
   https://arxiv.org/abs/1911.13137

7. *Simplified formalism of the algebra of partially transposed permutation operators with applications*
   M. Mozrzymas, M. Studziński, M. Horodecki
   Journal of Physics A: Mathematical and Theoretical **51** 125202 (2018)
   IF: 1.996 / punkty MNiSW: 100
   https://arxiv.org/abs/1708.02434

8. *Optimal Port-based Teleportation*
   M. Mozrzymas, M. Studziński, S. Strelchuk, M. Horodecki
   New Journal of Physics **20.5** (2018): 053006
   IF: 3.539 / punkty MNiSW: 140
   https://arxiv.org/abs/1707.08456

9. *Port-based teleportation in arbitrary dimension*
   M. Studziński, S. Strelchuk, M. Mozrzymas, M. Horodecki
   Scientific Reports **7**: 10871 (2017)
   IF: 3.998 / punkty MNiSW: 140
   https://arxiv.org/abs/1612.09260

10. *Structure of irreducibly covariant quantum channels for finite groups*
    M. Mozrzymas, M. Studziński, N. Datta
    Journal of Mathematical Physics **58**, 052204 (2017)
    IF: 1.488 punkty MNiSW: 70
    https://arxiv.org/abs/1610.05657

5 Omówienie celu naukowego/artystycznego ww. pracy/prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania

Moje osiągnięcia naukowe są częścią prac zbiorowych. Mój wkład do każdej z prac opisany jest w rozdziale I.2 osobno załączonego dokumentu *Wykaz osiągnięć naukowych albo artystycznych, stanowiących znaczny wkład w rozwój określonej dyscypliny.* Wkład pozostałych współautorów prac w formie ich oświadczeń jest załączony jako osobny dokument. Dodatkowo, w niniejszej prezentacji, posługuję się następującą konwencją dotyczącą referencji:

- publikacje należące do cyklu habilitacyjnego cytowane są jako [H1]-[H10],
- inne publikacje, których jestem współautorem, nienależące do cyklu habilitacyjnego, są cytowane jako [P1]-[P15],
- pozostałe publikacje są cytowane jako [E1]-[E107].

5.1 Wstęp

Zjawisko splątania kwantowego uważa się za najbardziej zdumiewające i wymykające się schematom klasycznego myślenia. Fakt ten został zauważony bezpośrednio po sformułowaniu matematycznych zasad nierelatywistycznej mechaniki kwantowej [E1]. Naukowcy badający

wspomniane efekty mechaniki kwantowej zdali sobie sprawę, że gdybyśmy mogli je kontrolować i stosować, otworzyłoby to zupełnie nowe, niedostępne dla klasycznych implementacji obszary [E2]. Dziś wykorzystujemy te odkrycia i rozwijamy teorię bezpiecznych algorytmów kwantowych [E3, E4], kryptografii kwantowej [E5] lub obliczeń kwantowych [E6, E7] - przytoczyliśmy tutaj tylko kilka klasycznych wyników. Tak obiecujące perspektywy praktycznej implementacji właściwości kwantowych jako zasobu, dobitnie pokazują wagę podejmowanych wysiłków na rzecz poprawy teoretycznego zrozumienia tego zjawiska, a także jego eksperymentalnej implementacji, w końcu komercjalizacji, którą można zaobserwować we współczesnym rozkwicie rozwoju technologii kwantowych. Oprócz ogromnego postępu w tej dziedzinie w ostatnich dziesięcioleciach, informacja kwantowa jest nadal bogatym obszarem nowych i ważnych wyników, pochodzących z obu kierunków - wdrożeń teoretycznych i praktycznych. Jednym ze sposobów osiągnięcia postępu w tej dziedzinie może być wykorzystanie i rozwijanie podejścia matematycznego. W naszym przypadku zostało to osiągnięte poprzez wykorzystanie wewnętrznych symetrii rozważanego układu. Powszechnie wiadomo, że ilekroć układ posiada jakieś symetrie, jego opis staje się znacznie prostszy i można otrzymać często zamknięte formuły opisujące jego pewne własności. Aby zidentyfikować i wykorzystać ukryte symetrie, możemy użyć potężnego narzędzia, jakim jest teoria reprezentacji grup i algebr, która w większości przypadków pozwala nam zredukować złożoność problemu. To jest powód, dla którego tak ważne jest dogłębne zrozumienie abstrakcyjnych narzędzi wraz z ich praktycznym tłumaczeniem.

Celem niniejszej serii habilitacyjnej jest dostarczenie *nowych zaawansowanych narzędzi matematycznych* bazujących na teorii reprezentacji, dostarczenie nowych wyników dotyczących zbioru *kowariantnych kanałów kwantowych* i ich zastosowań w problemach związanych z *zaszumionymi obwodami kwantowymi i ich klasyczną symulowalnością* oraz z jednym z najważniejszych efektów w informacji kwantowej wykorzystujący kwantowe splątanie - *kwantowej teleportacji*. Bardziej szczegółowa motywacja do podjęcia takiego programu badawczego zawarta jest w każdym dziale poświęconym danemu zadaniu badawczemu.

Wszelkie wyniki naukowe powstały w ścisłej współpracy naukowej z polskimi oraz zagranicznymi ośrodkami naukowymi – *Uniwersytet Wrocławski, Uniwersytet w Cambridge (Wielka Brytania)* oraz *Uniwersytet w Kopenhadze*. Część rezultatów aplikanta została także wypracowana w trakcie jego stażu podoktorskiego na Uniwersytecie w Cambridge (prace [H1],[H2],[H3],[H4]) oraz na Uniwersytecie Gdańskim (prace [H5],[H6],[H7],[H8]). Ostatnie dwa artykuły [H9],[H10] zostały opublikowane po zatrudnieniu apliknata na stanowisku naukowo-badawczym na Uniwersytecie Gdańskim.

Szczegółowy dorobek podjętej problematyki badawczej w serii habilitacyjnej można podsumować w poniższym zestawieniu:

1. Klasyfikacja i konstrukcja liniowych odwzorowań nieredukowalnie kowariantnych względem grup skończonych i wybranych grup zwartych. Jest to omówione w dwóch artykułach [H1] i [H5].

2. Rozwój protokołów losowego testowania porównawczego (ang. *randomized benchmarking protocol, RB protocols*) i klasycznej symulacji obwodów kwantowych poprzez wykorzystanie nowych klas nieredukowalnie kowariantnych kanałów kwantowych. Jest to omówione w artykule [H6].

3. Opracowanie nowatorskiego zestawu narzędzi matematycznych inspirowanych dualnością Schur-Weyla wraz z zastosowaniami do opracowania i opisu nowych kowariantnych protokołów teleportacji kwantowej typu port-based. Wszystkie opracowane narzędzia matematyczne są opisane w artykułach na temat teleportacji kwantowej w serii artykułów [H2], [H10], [H3] i [H9].

4. Grupowo-teoretyczny opis istniejących protokołów teleportacji kwantowej port-based dla każdego wariantu i dla dowolnego wymiaru przestrzeni Hilberta wraz ze szczegółową

analizą ich wydajności. Opis i analiza protokołu recyklingu dla deterministycznego protokołu teleportacji kwantowej port-based. Jest to omówione w serii trzech artykułów [H3], [H4] i [H9].

5. Konstrukcja i opis nowych kowariantnych protokołów teleportacji kwantowej typu port-based do transmisji dużej ilości informacji kwantowych. Badanie fundamentalnych ograniczeń nałożonych na protokoły port-based przez mechanikę kwantową. Jest to omówione w serii trzech artykułów [H7], [H10] i [H8].

Rezultaty dotyczące narzędzi matematycznych oraz protokołów teleportacji (multi) port-based były prezentowane jako referaty na najbardziej prestiżowej, corocznej konferencji w dziedzinie - Quantum Information Processing (2018: `https://qipconference.org/2018/qutech.nl/qip2018/qip-2018-program-details/index.html`, 2021: `https://www.mcqst.de/qip2021/program/friday.html`).

5.2 Niezbędne pojęcia wstępne z teorii reprezentacji

W celu uczynienia materiału prezentowanego w cyklu habilitacyjnym bardziej przystępnym dla czytelników, przedstawiamy tutaj krótkie wprowadzenie w niektóre aspekty teorii reprezentacji grup. Skupiamy się tutaj tylko na głównych definicjach, notacji i twierdzeniach użytych w dalszej części tego autoreferatu. Po więcej szczegółów zachęcamy czytelników do zapoznania się z literaturą umieszczoną w niniejszym tekście lub pracami habilitacyjnymi. Informacje zawarte w tym podrozdziale nie są oryginalnymi wynikami aplikanta, z wyjątkiem samej prezentacji i użytej notacji.

Niech S_n będzie grupą symetryczną skończonego, n elementowego zbioru (liczba układów). Reprezentacją permutacyjną nazywamy odwzorowanie $V : S_n \to \mathrm{Hom}((\mathbb{C}^d)^{\otimes n})$ grupy symetrycznej S_n w przestrzeń $\mathcal{H} \equiv (\mathbb{C}^d)^{\otimes n}$ zdefiniowanego poprzez działanie na wektory bazowe $\{|e_k\rangle\}_{k=1}^d$ $d-$wymiarowej przestrzeni $\mathbb{C}^d$:

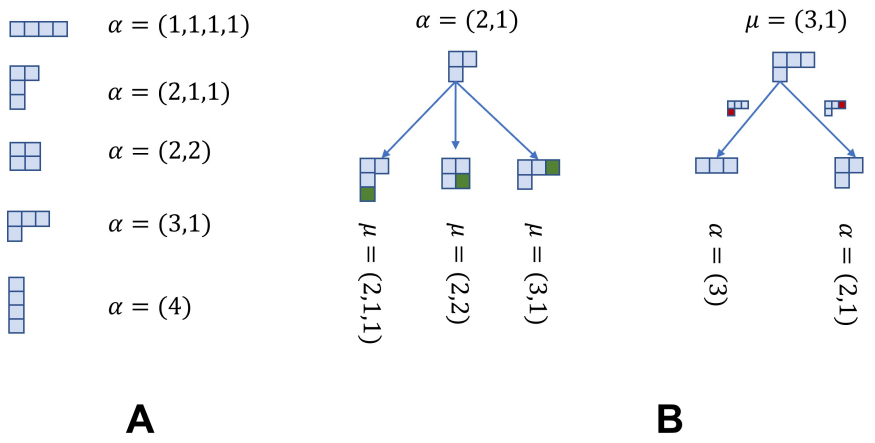
$$\forall \pi \in S_n \qquad V_\pi.|e_{i_1}\rangle \otimes |e_{i_2}\rangle \otimes \cdots \otimes |e_{i_n}\rangle := |e_{i_{\pi^{-1}(1)}}\rangle \otimes |e_{i_{\pi^{-1}(2)}}\rangle \otimes \cdots \otimes |e_{i_{\pi^{-1}(n)}}\rangle. \tag{1}$$

Ponieważ reprezentacja V jest zdefiniowana względem wybranej bazy w przestrzeni $\mathbb{C}^d$ jest reprezentacją macierzowa, a operatory V_π permutują wektory bazowe zgodnie z zadaną permutacją $\pi \in S_n$. Reprezentacja V w naturalny sposób rozszerza się do algebry grupowej $\mathbb{C}[S_n]$ zdefiniowanej jako:

$$\mathbb{C}[S_n] \equiv \mathcal{A}_n(d) := \mathrm{span}_{\mathbb{C}}\{V_\pi : \pi \in S_n\} \subset \mathrm{Hom}((\mathbb{C}^d)^{\otimes n}). \tag{2}$$

W dalszej części przez $V_{(a,n)}$ rozumiemy następujący operator $\mathbf{1}_{1\ldots\bar{a}\ldots n-1} \otimes V_{(a,n)}$ permutujący układy zgodnie z permutacją $\pi = (a, n)$ przy pominiętej części identycznościowej. Operator identycznościowy $\mathbf{1}_{1\ldots\bar{a}\ldots n-1}$ działa na $n-1$ pierwszych układach, oprócz układu $a-$tego. Będziemy używali konwencji, w której pomijamy operator identycznościowy, gdy będzie to jasno wynikało z kontekstu prezentowanego materiału.

Do pracy z nieredukowalnymi reprezentacjami (dalej: irrep) grupy symetrycznej S_n konieczne jest wprowadzenie pojęcia *podziału (partycji)*. Podziałem α liczby naturalnej n, oznaczanego jako $\alpha \vdash n$, nazywamy ciąg liczb dodatnich $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r)$, takich że $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r$ oraz $\sum_{i=1}^r \alpha_i = n$. Każdy podział α można zobrazować graficznie jako *diagram Younga*, który jest zbiorem komórek ułożonych w rzędy wyrównane do lewej - zilustrowaliśmy to w części A Rysunku 1. Dla ustalonej liczby n, ilość diagramów Younga determinuje ilość nierównoważnych nieredukowalnych reprezentacji grupy S_n w rozkładzie abstrakcyjnym. Zbiór wszystkich diagramów Younga o n komórkach jest oznaczany jako $\mathbb{Y}_n$. Jednakże wybierając jako przestrzeń reprezentacji $\mathcal{H} \equiv (\mathbb{C}^d)^{\otimes n}$, w rozkładzie grupy S_n na nieredukowalne reprezentacje pojawiają się tylko takie diagramy Younga α, dla których wysokość $h(\alpha)$ jest równa



Rysunek 1: **Panel A** przedstawia pięć możliwych diagramów Younga dla $n = 4$, które odpowiadają wszystkim abstrakcyjnym nieredukowalnym reprezentacjom grupy S_4. Rozważając przestrzeń reprezentacji jako $(\mathbb{C}^d)^{\otimes 4}$ widzimy, że występują tylko takie nieredukowalne reprezentacje grupy S_4, dla których wysokość $h(\cdot)$ (długość pierwszej kolumny) odpowiedniego diagramu Younga jest nie większa niż d. W szczególności, jeśli rozważymy przypadek kubitowy $(d = 2)$ mamy jedynie trzy dozwolone diagramy dla $n = 4$: $(4), (3,1), (2,2)$. **Panel B** przedstawia wszystkie możliwe diagramy Younga $\mu \vdash 4$ spełniające relację $\mu \in \alpha$ dla $\alpha = (2,1)$. Zielonym kolorem oznaczone są komórki dodane do początkowego diagramu $\alpha = (2,1)$. Następnie, najbardziej po prawej stronie prezentujemy wszystkie możliwe diagramy Younga $\alpha \vdash 3$ spełniające relację $\alpha \in \mu$ dla $\mu = (3,1)$. Czerwonym kolorem oznaczyliśmy komórki, które zostały odjęte od początkowego diagramu $\mu = (3,1)$.

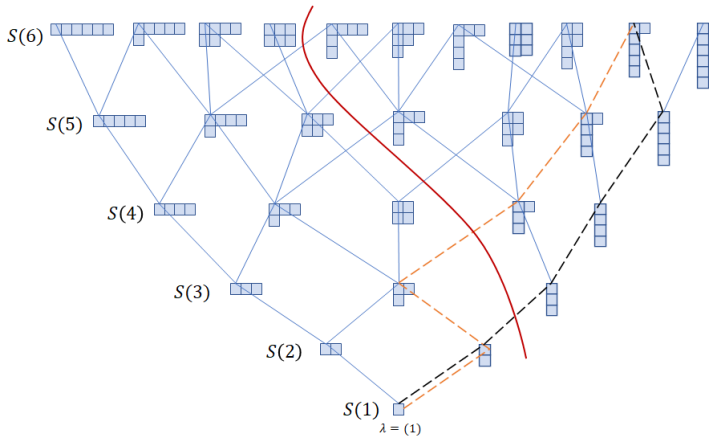
co najwyżej d. Redukuje to zbiór diagramów Younga do zbioru diagramów z nie więcej niż d wierszami, zbiór taki oznaczamy jako $\mathbb{Y}_{n,d}$. W obu zbiorach $\mathbb{Y}_n, \mathbb{Y}_{n,d}$ możemy wprowadzić strukturę porządku częściowego jako

$$\alpha \preceq \mu, \tag{3}$$

jeżeli $\mu_i \geq \alpha_i$ dla wszystkich $i = 1, 2, \ldots, l$. Jeżeli $\alpha \preceq \mu$ poprzez μ/α rozumiemy skośny kształt Younga powstały poprzez usunięcie z diagramu Younga μ komórek diagramu Younga α. Rozważmy teraz następujące dwa podziały $\alpha \vdash n-1$ oraz $\mu \vdash n$. Pisząc $\mu \in \alpha$ rozumiemy diagramy Younga μ, które powstały z α poprzez dodanie jednej komórki. Podobnie, pisząc $\alpha \in \mu$ oznaczymy diagramy Younga α, które powstały z μ poprzez odjęcie jednej komórki. Rysunek 1 w części B ilustruje te zagadnienia. Oczywiście zagadnienie to można uogólnić na dodawanie/odejmowanie większej ilości komórek. Będziemy tutaj używać tych samych symboli $\mu \in \alpha$, $\alpha \in \mu$ niezależenie od ilości k dodanych/odjętych komórek ponieważ wartość k zawsze będzie jasno wynikała z kontekstu. Dla dowolnych $\alpha, \mu \in \mathbb{Y}_n$ mówimy, że μ pokrywa α, albo α jest pokrywane przez μ jeżeli $\alpha \preceq \mu$ oraz

$$\alpha \preceq \nu \preceq \mu, \quad \nu \in \mathbb{Y}_n \Rightarrow \nu = \alpha \text{ lub } \nu = \mu. \tag{4}$$

Innymi słowy, μ pokrywa α wtedy i tylko wtedy, gdy $\alpha \preceq \mu$ i μ/α składa się przynajmniej z jednej komórki. Mając wprowadzone pojęcie diagramu Younga oraz zbiorów $\mathbb{Y}_n, \mathbb{Y}_{n,d}$ definiujemy kratownice Younga oraz jej zredukowaną wersję. Kratownica Younga dla $\mathbb{Y}_n$ jest grafem niezorientowanym (nieskierowanym) z wierzchołkami, które są elementami zbioru $\mathbb{Y}_n$ oraz krawędziami z λ do μ wtedy i tylko wtedy, gdy λ pokrywa μ. Taka sama definicja stosuje się do zredukowanej kratownicy Younga $\mathbb{Y}_{n,d}$, gdzie usuwamy wszystkie diagramy Younga zawierające więcej niż d wierszy. Idea ta została zilustrowana na Rysunku 2. Możemy również wprowadzić w zbiorze wszystkich diagramów Younga dla ustalonego n porządek leksykograficzny. Niech $\lambda = (\lambda_1, \ldots, \lambda_k)$ oraz $\mu = (\mu_1, \ldots, \mu_l)$ będą podziałami n. Porządek leksykograficzny jest zdefiniowany w następujący sposób: dla pierwszego indeksu i, dla którego istnieje $\mu_i \neq \lambda_i$, takie że $\mu_i \leq \lambda_i$ piszemy $\mu \leq \lambda$. W szczególności wykorzystujemy porządek leksykograficzny do



Rysunek 2: Kratownica Younga $\mathbb{Y}_6$ zbudowana z sześciu kolejnych warstw numerowanych grupami permutacji od S_1 do S_6. Pomarańczowe oraz czarne przerywane linie oznaczają ścieżki z irrepu $\lambda = (1)$ grupy S_1 do irrepu $\lambda' = (2,1,1,1,1)$ grupy S_6. Zredukowana kratownica Younga $Y_{6,2}$, tj. dla $d = 2$ jest zdefiniowana jako diagram na lewo od czerwonej linii.

porządkowania diagramów Younga w każdym z wierszy (zredukowanej) kratownicy Younga na Rysunku 2 oraz później do numerowania wierszy i kolumn macierzy teleportacji opisanej w Rozdziale 5.6.1.

Przypomnijmy teraz słynną dualność Schura-Weyla [E8, E9], która stwierdza, że diagonalne działanie grupy unitarnej $\mathcal{U}(d)$ macierzy zespolonych oraz działanie grupy symetrycznej S_n na przestrzeni $(\mathbb{C}^d)^{\otimes n}$ komutują ze sobą:

$$[V_\sigma, U \otimes \cdots \otimes U] = 0, \tag{5}$$

gdzie $\sigma \in S_n$ oraz $U \in \mathcal{U}(d)$, a przestrzeń $(\mathbb{C}^d)^{\otimes n}$ może być rozłożona w następujący sposób:

$$(\mathbb{C}^d)^{\otimes n} = \bigoplus_{\substack{\alpha \vdash n \\ h(\alpha) \leq d}} \mathcal{H}^\alpha_\mathcal{U} \otimes \mathcal{H}^\alpha_\mathcal{S}. \tag{6}$$

Grupa symetryczna S_n działa nietrywialnie na przestrzeni $\mathcal{H}^\alpha_\mathcal{S}$, a grupa $\mathcal{U}(d)$ działa nietrywialnie na przestrzeni $\mathcal{H}^\alpha_\mathcal{U}$, numerowanej tym samym podziałem α. Z rozładu przestrzeni opisanej równaniem (6) widzimy, że dla danego irrepu α grupy S_n, przestrzeń $\mathcal{H}^\alpha_\mathcal{U}$ jest przestrzenią krotności o wymiarze m_α (krotność irrepu α), podczas gdy przestrzeń $\mathcal{H}^\alpha_\mathcal{S}$ jest przestrzenią reprezentacji o wymiarze d_α (wymiar irrepu α). Każdy operator komutujący z diagonalnym działaniem $U^{\otimes n}$, zgodnie z lematem Schura, musi być proporcjonalny do identyczności na przestrzeniach $\mathcal{H}^\alpha_\mathcal{U}$ i posiadać swoją nietrywialną część na przestrzeniach $\mathcal{H}^\alpha_\mathcal{S}$. Odwrotnie, każdy operator komutujący z działaniem grupy permutacji S_n jest nietrywialnie reprezentowany na przestrzeniach $\mathcal{H}^\alpha_\mathcal{U}$. W każdej nieredukowalnej przestrzeni $\mathcal{H}^\alpha_\mathcal{S}$ można zbudować bazę ortonormalną $\{|\alpha, i\rangle\}$, gdzie $i = 1, \ldots, d_\alpha$, wykorzystując na przykład konstrukcję Younga-Yamanouchiego [E9, E10]. Ze skonstruowanymi wektorami bazy możemy stowarzyszyć nieredukowalne operatory bazowe E^α_{ij}, dla $i, j = 1, \ldots, d_\alpha$ postaci:

$$E^\alpha_{ij} := \mathbb{1}_{\mathcal{H}^\alpha_\mathcal{U}} \otimes |\alpha, i\rangle\langle\alpha, j|_{\mathcal{H}^\alpha_\mathcal{S}}. \tag{7}$$

Ponieważ baza $\{|\alpha, i\rangle\}_{i=1}^{d_\alpha}$ jest ortonormalna powyższe operatory spełniają następujące relacje:

$$E^\alpha_{ij} E^{\alpha'}_{kl} = \delta^{\alpha\alpha'} \delta_{jk} E^\alpha_{il}, \qquad \operatorname{Tr} E^\alpha_{ij} = \delta_{ij} m_\alpha. \tag{8}$$

Z operatorów E^{α}_{ij}, używając relacji zupełności $\sum_i |\alpha, i\rangle\langle\alpha, i|_{\mathcal{H}^{\alpha}_{\mathcal{S}}} = \mathbb{1}_{\mathcal{H}^{\alpha}_{\mathcal{S}}}$ możemy zbudować tak zwane projektory Younga P^{α} na nieredukowalne podprzestrzenie numerowane przez α:

$$P^{\alpha} := \sum_{i=1}^{d_{\alpha}} E^{\alpha}_{ii} = \mathbb{1}_{\mathcal{H}^{\alpha}_{\mathcal{U}}} \otimes \mathbb{1}_{\mathcal{H}^{\alpha}_{\mathcal{S}}}, \qquad P^{\alpha} P^{\alpha'} = \delta^{\alpha\alpha'} P^{\alpha}, \qquad \mathrm{Tr}\, P^{\alpha} = m_{\alpha} d_{\alpha}. \tag{9}$$

Dla ustalonego irrepu α grupy S_n operatory E^{α}_{ij} z (7) oraz P^{α} z (9) mogą być także zapisane za pomocą operatorów permutacji V_{π} zdefiniowanych w (1) permutujących układy przestrzeni $(\mathbb{C}^d)^{\otimes n}$:

$$E^{\alpha}_{ij} = \frac{d_{\alpha}}{n!} \sum_{\pi \in S_n} \phi^{\alpha}_{ji}(\pi^{-1}) V_{\pi}, \qquad P^{\alpha} = \frac{d_{\alpha}}{n!} \sum_{\pi \in S_n} \chi^{\alpha}(\pi^{-1}) V_{\pi}, \tag{10}$$

gdzie liczby $\phi^{\alpha}_{ji}(\pi^{-1})$ są elementami macierzowymi nieredukowalnych reprezentacji $\pi \in S_n$, a $\chi^{\lambda}(\pi^{-1}) = \sum_i \phi^{\alpha}_{ii}(\pi^{-1})$ są odpowiednimi nieredukowalnymi charakterami. Oczywiście, operatory dane poprzez powyższe równania spełniają te same relacje składania (8). Rzeczywiście, operatory E^{α}_{ij} rozpinają nieredukowalne przestrzenie $\mathcal{H}^{\alpha}_{\mathcal{S}}$ w $(\mathbb{C}^d)^{\otimes n}$, ponieważ dla każdego elementu $V_{\pi} \in \mathcal{A}_n(d)$ mamy:

$$V_{\pi} = \sum_{\alpha} \sum_{i,j=1}^{d_{\alpha}} \phi^{\alpha}_{ij}(\pi) E^{\alpha}_{ij}. \tag{11}$$

Ostatecznie, używając relacji (10) oraz (11) możemy podać lewe działanie (odpowiednio prawe) dowolnego operatora V_{π} na operatory bazowe:

$$V_{\pi} E^{\alpha}_{ij} = \sum_{k=1}^{d_{\alpha}} \phi^{\alpha}_{ki}(\pi) E^{\alpha}_{kj}, \qquad E^{\alpha}_{ij} V_{\pi} = \sum_{l=1}^{d_{\alpha}} \phi^{\alpha}_{jl}(\pi) E^{\alpha}_{il}. \tag{12}$$

Ostatnie wyrażenia również dowodzą, że operatory E^{α}_{ij} rozpinają nieredukowalną bazę w każdym z irrepów, ponieważ ich działanie jest zamknięte ze względu na α.

5.3 Nieredukowalnie kowariantne odwzorowania liniowe

W dwóch pracach [H1], [H5] scharakteryzowaliśmy kompletną dodatniość oraz dodatniość odwzorowań liniowych, które są kowariantne względem działania nieredukowalnej reprezentacji grupy skończonej. Odwzorowanie takie nazywamy *nieredukowalnie kowariantnymi odwzorowaniami liniowymi* (ang. *ICLM - irreducibly covariant linear map*). Mówimy, że odwzorowanie liniowe $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ jest ICLM względem nieredukowalnych reprezentacji $U(g), V(g)$ grupy skończonej G, jeżeli dla każdego operatora $X \in \mathcal{B}(\mathcal{H})$ oraz dla każdego elementu $g \in G$ zachodzi:

$$\Phi\left(U(g) X U(g)^{\dagger}\right) = V(g) \Phi(X) V(g)^{\dagger}. \tag{13}$$

Przełomowe wyniki w charakteryzowaniu takiej klasy odwzorowań pochodzą od Scutaru [E11]. Udowodnił on twierdzenie typu Stinespringa w języku C^*-algebr dla dowolnego całkowicie dodatniego odwzorowania liniowego, które jest kowariantne względem unitarnej reprezentacji grupy lokalnie zwartej. Jego wynik nie daje jednak jednoznacznego sposobu konstruowania takich odwzorowań, ani bardziej szczegółowego wglądu w ich wewnętrzną strukturę. Niemniej jednak odwzorowania ICLM tworzące nieredukowalnie kowariantne kanały kwantowe (ang. *ICQC - irreducibly covariant quantum channels*) mają szeroki zakres zastosowań, od fizyki ciała stałego po informatykę kwantową. Na przykład $SU(2)$-kowariantne kanały zostały użyte do opisu splątania w układach spinowych [E12] i pozwalają udowodnić rozszerzoną wersję twierdzenia Lieba-Mattisa-Schultza przy użyciu tzw. Matrix Product States [E13]. Zwiększając wymiar i biorąc pod uwagę grupę $SU(d)$ można badać aspekty dimeryzacji kwantowych łańcuchów spinowych [E14]. W informacji kwantowej kanały kowariantne pomagają

analizować właściwość addytywności pojemności Holevo [E15] i minimalnej entropii wyjściowej [E16, E17, E18, E19, E20]. Własność kowariancji pozwala również udowodnić strong converse property dla pojemności klasycznej [E21] i klasycznej pojemności wspomaganej splątaniem [E22] (ang. *entanglement-assisted classical capacity*). Omawiana tutaj klasa kanałów pozwala także na sformułowanie ciekawych rezultatów w kontekście twierdzenia Birkhoffa [E23, E24] oraz na konstrukcje nowych nierówności macierzowych ze stożka dodatniego [E25]. Powyższa dyskusja wraz przykładami ilustruje znaczenie (nieredukowalnie) kowariantnych kanałów i podkreśla potrzebę bardziej szczegółowego zrozumienia ich struktury wraz z ich własnościami na bardziej ogólnym poziomie - bez wybierania konkretnej grupy, a więc przedstawienie bardziej systematycznego podejścia do zagadnienia.

W artykule [H1] podajemy szczegółowy opis matematyczny kanałów kwantowych – kompletnie dodatnich, zachowujących ślad odwzorowań liniowych (ang. *CPTP– completely positive trace preserving*) nieredukowalnie kowariantnych względem grupy skończonej G, w przypadku gdy:

1. wejściowa oraz wyjściowa przestrzeń Hilberta są takie same, tzn. $\mathcal{H} = \mathcal{K}$,
2. rozważana jest wyróżniona nieredukowalna reprezentacja U,
3. iloczyn tensorowy $U \otimes U^c$ jest prosto-redukowalny (ang. multiplicity free), gdzie U^c oznacza reprezentację kontragradientną, tzn. dla każdego $g \in G$, $U^c(g) = U(g^{-1})^T \equiv \overline{U}(g)$.

Jak to zostało zaobserwowane w Corollary 15 w [H1], odwzorowanie Φ, które jest ICLM musi być następującej postaci:

$$\Phi = l_{\mathrm{id}}\Pi^{\mathrm{id}} + \sum_{\alpha \neq \mathrm{id}} l_\alpha \Pi^\alpha : \quad l_{\mathrm{id}}, l_\alpha \in \mathbb{C}, \tag{14}$$

gdzie Π^α są ortogonalnymi projektorami rzutującymi na nieredukowalne podprzestrzenie numerowane indeksem α w rozkładzie $U \otimes U^c$, indeks id oznacza reprezentację identycznośiową (trywialną). Na przykład, jeżeli za grupę G wybierzemy grupę permutacji S_n to operatory Π^α są projektorami Younga z równania (9). Z powyższego rozkładu jasno wynika, że aby odwzorowanie ICLM było ICQC na współczynniki $l_{\mathrm{id}}, \{l_\alpha\}_{\alpha \neq \mathrm{id}}$ muszą zostać narzucone pewne dodatkowe warunki.

W celu ustalenia takich warunków, w pierwszym kroku, wyliczamy warunki spektralne obrazu Choi-Jamiołkowskiego $J(\Phi)$ dla dowolnego odwzorowania Φ, które jest ICLM. Wartości własne i projektory ortogonalne, pojawiające się w rozkładzie spektralnym, są wyrażone całkowicie przez nieredukowalne reprezentacje rozważanej grupy G. Zapewniając, że $J(\Phi) \geq 0$ otrzymujemy warunki konieczne i dostateczne na to, aby rozważane odwzorowanie liniowe Φ było ICLM (Twierdzenie 40 w [H1]). W szczególności, pokazaliśmy że odwzorowanie Φ jest ICLM zachowującym ślad wtedy i tylko wtedy, gdy $l_{\mathrm{id}} = 1$ (Proposition 25 w [H1]). Dodatkowo, podaliśmy jawne wyrażenia na operatory Krausa dla rozważanej klasy kanałów (Twierdzenie 41 w [H1]). Otrzymane rezultaty są warunkami operacyjnymi, gdy ustalimy grupę G oraz reprezentację U. Dokładniej, aby zapewnić, że rozważane odwzorowanie jest ICQC, musimy rozwiązać układ liniowych nierówności względem współczynników z równania (14) – to z kolei można zrobić efektywnie, przynajmniej numerycznie. Ten rezultat daje również geometryczną interpretację rozwiązań wspomnianego zbioru nierówności, dla którego odwzorowanie jest ICLM jest kanałem ICQC. Mówiąc bardziej formalnie, pokazaliśmy że wszystkie wartości własne obrazu Choi-Jamiołkowskiego odwzorowania, które jest ICQC muszą znajdować się w przecięciu zredukowanego sympleksu oraz pewnej przestrzeni generowanej przez macierz otrzymanej ze spektralnej analizy projektorów pojawiających się w rozkładzie odwzorowania ICLM (Proposition 43, Proposition 47 in [H1]).

Rozwinięte narzędzia i charakteryzacja, która jest spełniona dla każdej skończonej, prosto-redukowalnej grupy G pozwoliła na podanie szerokiej klasy kanałów kwantowych, które są

nieredukowalnie kowariantne bezpośrednio z konstrukcji. Rezultaty te są zawarte w Twierdzeniu 50 w Rozdziale 8.1 omawianego artykułu. Konstrukcja taka polega na szczególnym wyborze współczynników $\{l_\alpha\}_{\alpha\neq \mathrm{id}}$ in (14):

$$l_\alpha = \frac{1}{|G|}\frac{1}{|\varphi^\alpha|}\sum_{g\in G}\chi^\alpha(g)f(g), \tag{15}$$

gdzie na $f : G \to \mathbb{C}$ narzucone są pewne dodatkowe warunki, $\chi^\alpha(g)$ jest nieredukowalnym charakterem, a $|\varphi^\alpha|$ oznacza wymiar irrepu α. Dodatkowo, podajemy przykłady odwzorowań ICQC dla wybranych grup prosto-redukowalnych: grupy symetrycznej S_3 i S_4 oraz grupy kwaternionów Q. W każdym z przypadków konstruujemy odpowiednie reprezentacje macierzowe oraz reprezentacje Krausa rozważanych ICQC. Dodatkowo, oprócz rozwiązań analitycznych, ilustrujemy graficznie przestrzenie dozwolonych parametrów z (14) dla których rozważane odwzorowania są ICQC. Następnie, dla przypadku grup S_3 oraz Q, przy użyciu kryterium Peresa-Horodeckiego lub inaczej kryterium PPT (ang. *positive partial transpose*) [E26, E27], podajemy warunki po spełnieniu których rozważane odwzorowania ICQC są kanałami łamiącymi splątanie [E28].

W artykule [H5] badaliśmy odwzorowania liniowe Φ z (13), spełniające warunki 1,2 oraz 3, ale zamiast żądania spełniania warunku CPTP, chcemy aby odwzorowanie było jedynie dodatnie (ang. *P – positive*). Zagadnienie klasyfikacji konstrukcji nowych przykładów dodatnich odwzorowań liniowych, nawet z dodatkowymi własnościami, jest nadal zagadnieniem otwartym oraz bardzo złożonym pomimo wielu fundamentalnych rezultatów i podjętych prób w tej dziedzinie [E29, E30, E31, E32, E33, E34, E35, E36, E37]. Jedną z głównych przeszkód w postępie na tym polu jest brak uniwersalnego operacyjnego kryterium dodatniości. Dokładniej, aby udowodnić, że dane odwzorowanie jest dodatnie musimy pokazać, że obraz Choi-Jamiołkowskiego jest blokowo dodatni, gdy do pokazania kompletnej dodatniości wystarcza wyliczenie wartości własnych ów obrazu, co może być zrobione efektywnie. Dlatego też ważne jest dostarczanie nowych przykładów odwzorowań dodatnich i metod ich konstrukcji, dających wgląd w wewnętrzną strukturę rozważanego zbioru odwzorowań.

Nasze rozważania rozpoczęliśmy od bezpośredniej (z definicji) konstrukcji odwzorowań dodatnich ICLM dla grup skończonych. Jednakże, metoda ta może efektywnie działać jedynie dla niskich wymiarów – w naszej pracy dla przypadku kubitowego. Zbudowaliśmy odwzorowania dodatnie dla dwu-wymiarowych nieredukowalnych reprezentacji grupy S_3 oraz grupy kwaternionów Q. Dodatkowo, pokazaliśmy, że każde dodatnie kubitowe odwzorowanie ICLM może być przedstawiona jako suma odwzorowań CP oraz CoP (ang. co-positive), które także są ICLM.

Aby pozbyć się konieczności sprawdzania warunku blokowej dodatniości obrazu Choi-Jamiołkowskiego zaproponowaliśmy nową metodę konstrukcji. Metoda ta bazuje na rezultatach zawartych w pracy [P1] i wykorzystuje odwzorowanie odwrotnej redukcji
$R^{-1} \in \mathrm{End}[\mathrm{M}(d,\mathbb{C})]$ [E38, E39]:

$$\forall X \in \mathrm{M}(d,\mathbb{C}) \quad R^{-1}(X) = \frac{\mathrm{Tr}(X)}{d-1}\mathbf{1} - X. \tag{16}$$

W celu konstrukcji nowych rodzin odwzorowań dodatnich ICLM używaliśmy Twierdzenia 15 z pracy [H5], które jest adaptacją Twierdzenia 1 z pracy [P1]. W pierwszym kroku definiujemy operator $W := (\mathbf{1}\otimes\Phi)P_d^+$ dla rozważanego odwzorowania liniowego ICLM Φ, przy czym żądamy, aby operator W był niedodatni. To zapewnia nam, że badane odwzorowanie na pewno nie jest odwzorowaniem CPTP. Widzimy, że tak naprawdę operator W jest obrazem Choi-Jamiołkowskiego odwzorowania Φ (dla wygody utrzymujemy tutaj oryginalną notację). Następnie żądamy, aby operator $\widetilde{W} = (\mathbf{1}\otimes R^{-1})W$ był dodatnio określony - to z kolei zapewnia, że rozważane odwzorowanie Φ jest dodanie (na mocy Twierdzenia 15). Ponieważ dodatkowo,

rozważane odwzorowanie jest ICLM, to musi być ono w postaci (14). Zatem zgodnie z rezultatami pracy [H1], warunki na dodatniość (niedodatniość) obrazu Choi-Jamiołkowskiego tego odwzorowania można zapisać jako zbiór nierówności liniowych względem nieznanych współczynników $l_{\mathrm{id}}, \{l_\alpha\}_{\alpha\neq\mathrm{id}}$ z (14) – Corollary 17 z pracy [H5]. Używając przedstawionego tutaj podejścia skonstruowaliśmy odwzorowania dodatnie indukowane przez trójwymiarową nieredukowalną reprezentację grupy permutacji S_4 oraz reprezentacje grupy $MU(d,n)$, która jest podgrupą grupy monomialnych macierzy unitarnych $MU(d)$, gdzie n jest pewnym naturalnym parametrem. W szczególności, pokazaliśmy, że obszar parametrów dla odwzorowania ICLM generowanego przez grupę $MU(3,n)$, dla którego odwzorowanie jest dodatnie, zawiera w sobie obszar dodatniości dla uogólnionego odwzorowania Choi [E40]. Przy czym, obszar dodatniości odwzorowania generowanego przez grupę $MU(3,n)$ jest wyraźnie większy. Rezultat ten pozwala nam rozważać uogólnione odwzorowanie Choi jako dodatnie odwzorowanie ICLM generowane przez grupę $MU(3,n)$. Dla grupy $M(d,n)$ byliśmy także w stanie określić obszar dodatniości, bezpośrednio sprawdzając blokową dodatniość obrazu Choi-Jamiołkowskiego. Obszar ten jest oczywiście większy niż wyznaczony za pomocą odwzorowania odwrotnej redukcji. Rezultaty odnoszące się do grupy $M(d,n)$ mogą być interesujące także z innych względów. Mianowicie, odwzorowanie generowane przez tą grupę znalazło zastosowanie w protokole losowego testowania porównawczego (ang. *randomized benchmarking protocol, RB protocols*) [E41], w szczególnym przypadku gdy rozważany zbiór bramek kwantowych składa się z elementów grupy skończonej, ale nie tworzy tzw. 2-design. Ponadto, grupa $M(d,n)$ zawiera kwantową bramkę T [E42], która wraz z bramkami Clifforda tworzy zbiór uniwersalny do obliczeń kwantowych. Dodatkowo wspomniana grupa została użyta w pewnych zagadnieniach teorii układów wielocząstkowych [E43]. Związek pomiędzy protokołami RB oraz odwzorowaniami ICLM motywował nas do dalszych studiów w tym zakresie, które są opisane w następnej sekcji autoreferatu.

Ostatnim rezultatem jest związek pomiędzy słynnymi warunkami Fujiwara-Algolet [E44] a unitalnymi nieredukowalnie kowariantnymi kanałami kwantowymi generowanymi przez grupę kwaternionów Q. Pokazaliśmy, że każdy unitalny kubitowy kanał kwantowy może być przedstawiony jako nieredukowalnie kowariantny kanał indukowany przez dwu-wymiarową nieredukowalną reprezentację grupy Q. Ten końcowy rezultat zawarty jest w Proposition 35 pracy [H5]. Wynik ten obowiązuje także dla unitalnych odwzorowań dodatnich, dając nam niejako klasyfikację odwzorowań zachowujących identyczność w formie warunków czysto geometrycznych.

5.4 Efektywny protokół losowego testowania porównawczego i klasyczna symulacja procesów kwantowych w bazie Weyla

Szum w warunkach eksperymentalnych oraz praktycznych wdrożeniach technologii kwantowych jest nieunikniony ze względu na oddziaływanie z otoczeniem. Identyfikacja jego źródeł i sprawna diagnostyka błędów powstałych w procesie ewolucji kwantowej jest jednym z kluczowych kroków w budowie skalowalnego komputera kwantowego. Różne implementacje mają wiele zależnych od specyfikacji (architektury) sprzętu źródeł szumu, co sprawia, że problem ich sprawnej detekcji jest bardzo złożony. Jak dotąd opracowano wiele różnych metod detekcji: protokół losowego testowania porównawczego (protokół RB) [E45, E46, E47, E48], tomografia stanu i kanału [E49, E50], tomografia zbioru bramek [E51] oraz bezpośrednia estymacja wierności [E52]. W ogólności różne metody detekcji szumu w obwodach kwantowych, czyli także potencjalnie w komputerach kwantowych, mają różne zakresy zastosowań oraz różnią się kosztami.

W artykule [H6] wprowadziliśmy nowe podejście do protokołu RB oraz klasycznej symulacji obwodów kwantowych wykorzystując operatory unitarne Weyla. Po raz pierwszy nasz model pozwala na identyfikację wielu modeli szumu (w tym także ich mieszanki), który działa zarówno dla kubitów jak i wyżej wymiarowych układów. W szczególności, skupiliśmy się na

umotywowanych eksperymentalnie modelach szumu: depolarycujący, defazujący oraz modele over-rotations bazujące na wpływających na realizację danej bramki. Zaproponowany protokół jest odporny na tzw. błędy w przygotowaniu stanu i pomiaru (ang. state preparation and measurement error - SPAM) oraz skaluje się wraz z rozmiarem układu, przy naturalnym założeniu lokalności szumu, ale bez zakładania żadnej dodatkowej struktury obwodu. Wyniki te w sposób znaczący rozszerzają prace [E53, E54].

W tym samym artykule stosujemy rozwinięty przez nas protokół RB do symulacji na klasycznym komputerze wyników dostarczanych przez obwody kwantowe. Mając do dyspozycji obwód kwantowy o znanym profilu szumu, podajemy analityczne ograniczenie na liczbę próbek wymaganych do klasycznej estymacji wyników obwodu z założoną precyzją. Innymi słowy, możemy podać nietrywialne obliczalne ograniczenie na zaszumienie bramki, które trzeba dodać do każdej bramki kwantowej w badanym obwodzie, aby zapewnić jego efektywną klasyczną symulację. Rozwinięte przez nas w pracy [H6] narzędzia nie zależą od geometrii obwodu, ani struktury wybranego zbioru bramek. Te cechy odróżniają nasze od wcześniej istniejących metod [E55] i mogą być użyte do badania złożoności klasycznej symulowalności dla szerokiej klasy urządzeń kwantowych używanych na przykład w reżimie VQE (ang. *Variational Quantum Eigensolver*) oraz urządzeń kwantowych bliskiej przyszłości [E56, E57, E58].

Matematycznie, gdy implementujemy znaną operację unitarną U działającą na n kuditach, otrzymana transformacja, z powodu występującego szumu (błędu) opisanego kanałem $\mathcal{N}$, jest modelowana za pomocą kanału kwantowego postaci $\mathcal{N} \circ \mathcal{U}$, gdzie $\mathcal{U}$ oznacza kanał odpowiadający unitarnemu sprzężeniu unitarnością U. Jednym z głównych celów jest poznanie (oszacowanie) parametrów opisujących dany kanał reprezentujący szum $\mathcal{N}$ i można to osiągnąć studiując właśnie protokoły randomised benchmarking. Nasz protokół używa unitarności Weyla-Heisenberga $\{W_{(a,b)}\}_{a,b=0}^{d-1}$, które są uogólnieniami macierzy Pauliego na wyższe wymiary. Są one zdefiniowane jako $W_{(a,b)} = Z^a X^b$, gdzie $X \in U(d)$ jest unitarnym operatorem translacji, a $Z \in U(d)$ jest unitarnym operatorem mnożącym przez fazę. Jeżeli pracujemy z układem n kuditów, wtedy $W_{(\mathbf{a},\mathbf{b})} := W_{(a_1,b_1)} \otimes W_{(a_2,b_2)} \otimes \cdots \otimes W_{(a_n,b_n)}$ jest bazą w przestrzeni macierzy $M(d^n, \mathbb{C})$, gdzie $(\mathbf{a}, \mathbf{b}) \in (\mathbb{Z}_d)^{2n}$.

Jak wspomnieliśmy wcześniej, wiele ważnych z praktycznego punktu widzenia modeli szumu, takich jak (lokalny) szum defazujący czy (lokalny) szum depolaryzujący, są diagonalne w bazie operatorów Weyla. Są one elementami szerszej klasy diagonalnych kanałów Weyla i oznaczane są przez $\mathcal{T}$. Dla każdego $d \geq 2$ mogą być one zapisane jako wypukła kombinacja sprzężeń operatorami Weyla [E59], [E60, Chapter 4]:

$$\mathcal{T}(A) = \sum_{(\mathbf{a},\mathbf{b}) \in (\mathbb{Z}_d)^{2n}} p(\mathbf{a},\mathbf{b}) W_{(\mathbf{a},\mathbf{b})} A W_{(\mathbf{a},\mathbf{b})}^{\dagger}, \tag{17}$$

gdzie $p(\mathbf{a},\mathbf{b})$ jest rozkładem prawdopodobieństwa na $(\mathbb{Z}_d \times \mathbb{Z}_d)^n$, a A jest dowolnym operatorem. Jasne jest, że klasa kanałów z (17) należy do rodziny kanałów nieredukowalnie kowariantnych omawianych w Rozdziale 5.3 niniejszego autoreferatu, a my prezentujemy tutaj ich nowe zastosowanie. Ponieważ dyskutowane modele szumu są diagonalne w bazie Weyla, to do ich pełnego opisu wystarczy poznać ich diagonalne elementy $\langle \mathcal{T} \rangle_{(\mathbf{a},\mathbf{b})}^{(\mathbf{a},\mathbf{b})}$ obliczone w tejże bazie. Uzyskujemy to formułując i wykorzystując protokół złożony z następujących kroków:

Protokół losowego testowania porównawczego w bazie Weyla (protokół WRB)

Wejście: $(\mathbf{a},\mathbf{b}) \in (\mathbb{Z}_d)^{2n}$ odpowiadający elementowi diagonalnemu, który chcemy poznać oraz sekwencja długości m. Stan początkowy ρ oraz pomiar POVM[a] E działający na n kuditach.
Wyjście: liczba y.

1. Wybieramy losowo $(\mathbf{a}_0,\mathbf{b}_0) \in (\mathbb{Z}_d)^{2n}$, stosujemy $W_{(\mathbf{a}_0,\mathbf{b}_0)}$, a następnie sekwencję $\bar{W} = (W_{(\mathbf{a}_1,\mathbf{b}_1)},\ldots,W_{(\mathbf{a}_m,\mathbf{b}_m)})$ jednakowo prawdopodobnych, loklanych unitarności Weyla działających na n kuditów na przemian z zaszumioną operacją unitarną U.
2. Stosujemy $\bar{W}^\dagger$.
3. Wykonujemy pomiar na stanie wykorzystując POVM $\{E, \mathbf{1}-E\}$.
4. Jeżeli zmierzymy E wynikiem jest $y = \chi_{(\mathbf{a},\mathbf{b})}(\mathbf{a}_0,\mathbf{b}_0) = \exp(i\frac{2\pi}{d}\langle(\mathbf{b},-\mathbf{a}),(\mathbf{a}_0,\mathbf{b}_0)\rangle)$. W przeciwnym przypadku, wynikiem jest $y = 0$.

[a] ang. *positive-operator valued measure* - POVM

Wybierając sekwencje różnej długości oraz przeprowadzając eksponencjalne dopasowanie otrzymujemy estymację diagonali $\mu(\mathbf{a},\mathbf{b}) = \langle \mathcal{T}\circ\mathcal{U}\rangle_{(\mathbf{a},\mathbf{b})}^{(\mathbf{a},\mathbf{b})}$ w bazie Weyla. Znajomość $\mu(\mathbf{a},\mathbf{b})$ oraz fakt, że $\mathcal{T}$ jest diagonalny w bazie Weyla jest wystarczające do estymacji parametrów opisujących szum, ponieważ w tym przypadku: $\mu(\mathbf{a},\mathbf{b}) = \langle \mathcal{U}\rangle_{(\mathbf{a},\mathbf{b})}^{(\mathbf{a},\mathbf{b})}\langle \mathcal{T}\rangle_{(\mathbf{a},\mathbf{b})}^{(\mathbf{a},\mathbf{b})}$. To już kompletnie charakteryzuje kanał $\mathcal{T}$, jeżeli elementy diagonalne operacji unitarnej nie są równe zeru. Maksymalna długość sekwencji jest określona przez przerwę spektralną λ rozważanego kanału kwantowego. W rzeczywistości parametr λ^{-1} jest miarą głębokości obwodu, na której szum będzie już widoczny. Twierdzenie 2 w artykule [H6] mówi, że dla dowolnego $\epsilon > 0$ parametry opisujące szum, $\mu(\mathbf{a},\mathbf{b})$ mogą zostać oszacowane z prawdopodobieństwem δ, przez przeprowadzenie $M = \mathcal{O}(\epsilon^{-2}\log(\delta^{-1}\log(1-\lambda)^{-1}))$ eksperymentów RB w bazie Weyla, każdy zawierający co najwyżej $M_{\max} = \mathcal{O}(\lambda^{-1})$ bramek w pojedynczej sekwencji. Parametr λ^{-1} może zostać określony przy użyciu danych na temat zakresu parametrów szumu dostarczonych przez producenta danego urządzenia. Jednakże nasz protokół nie jest ograniczony jedynie do kanałów diagonalnych w bazie Weyla. Dokładniej, mając dostęp do bramki Clifforda o odpowiednio niskim zaszumieniu, możemy estymować także pozadiagonalne elementy $\langle \mathcal{N}\rangle_{(\mathbf{a}_2,\mathbf{b}_2)}^{(\mathbf{a}_1,\mathbf{b}_1)}$ dla dowolnego kanału $\mathcal{N}$ zapisanego w bazie Weyla. W tym przypadku również udowodniliśmy analog przywołanego tutaj Twierdzenia 1 (Twierdzenie 2 w materiałach dodatkowych pracy [H6]). W szczególności to rozszerzenie pozwala na identyfikację parametrów innych modeli szumu zawierających błędy typu przekręcenia (ang. *over-rotations*).

W tym samym artykule [H6] używamy informacji na temat szumu w obwodzie kwantowym do badania ograniczeń na złożoność ich klasycznej symulacji. Mówiąc bardziej formalnie, pracujemy w reżimie tzw. słabej symulacji. Oznacza to, że dla danej obserwabli E możemy klasycznie symulować zaszumiony obwód $\mathcal{C}_\mathcal{B} = \mathcal{N}^{(N)}\circ\cdots\circ\mathcal{N}^{(1)}$ działający na produktowy stan wejściowy ρ, jeżeli potrafimy klasycznie estymować $\mathrm{Tr}(\sigma E)$ z dokładnością do addytywnego błędu $\epsilon > 0$, gdzie $\sigma = \mathcal{C}_B(\rho)$. W naszej pracy zaproponowaliśmy algorytm próbkujący, bazujący na próbkowaniu względem normy ℓ_1 dla macierzy oraz wektorów, który wykorzystuje wyniki testu WRB i może być stosowany do zaszumionych obwodów dla czasu dyskretnego jak i ciągłego:

Algorytm próbkowania obwodu

Wejście: zaszumiony obwód kwantowy określony za pomocą kwantowych kanałów $\mathcal{N}^{(1)}, \ldots, \mathcal{N}^{(N)}$, kwantowy stan początkowy ρ oraz obserwabla E.
Wyjście: liczba x taka, że $\mathbb{E}(x) = \mathrm{Tr}(E\sigma)$, gdzie $\sigma = \mathcal{C}_B(\rho)$.

1. Próba $(\mathbf{a}_0, \mathbf{b}_0)$ z rozkładu p_0.
2. Dla $k = 1, \ldots, n$: Próba $(\mathbf{a}_k, \mathbf{b}_k)$ z $p_k(\mathbf{a}_{k+1}, \mathbf{b}_{k+1} | \mathbf{a}_k, \mathbf{b}_k)$
3. Wynik x jest dany jako

$$x = \mathrm{sign}(\rho(\mathbf{a}_0, \mathbf{b}_0)) \|\rho\|_{\ell_1} E(\mathbf{a}_n, \mathbf{b}_n) \times \prod_{k=1}^{N} \|\mathcal{N}^{(k)}(\mathbf{a}_k, \mathbf{b}_k)\|_{\ell_1} \mathrm{sign}(\langle \mathcal{N}^{(k)} \rangle_{(\mathbf{a}_{k+1}, \mathbf{b}_{k+1})}^{(\mathbf{a}_k, \mathbf{b}_k)})$$

W Twierdzeniu 1 zawartym w pracy [H6] udowodniliśmy, że rzeczywiście zaproponowany algorytm próbkuje z rzeczywistego rozkładu oraz podajemy liczbę próbek wymaganych aby być $\epsilon-$blisko empirycznej wartości oczekiwanej. Następnie ilustrujemy jak zastosować nasze wyniki do symulacji obwodów kwantowych, także w reżimie VQE. W przypadku, gdy kanały kwantowe opisujące szum w obwodzie są lokalne, stan początkowy oraz obserwable są produktowe pokazujemy, że złożoność naszego algorytmu próbkującego skaluje się wielomianowo. Ilekroć stosujemy w obwodzie bramki Clifforda, to nie zwiększają one złożoności algorytmu, ponieważ działają one jak permutacje w bazie Weyla. Dodatkowo rozszerzamy zaproponowany algorytm próbkujący do kanałów kwantowych postaci $e^{t\mathcal{L}}$, gdzie $\mathcal{L}$ jest operatorem Lindblada (rozdział VII materiałów dodatkowych pracy [H6]).

Podsumowując, nasze rezultaty oferują narzędzia zarówno dla praktyków – poprzez dostarczenie metod porównywania oraz wykrywania szerokiego wachlarza złożonych modeli szumów, oraz dla teoretyków – dzięki dostarczeniu obliczalnych ograniczeń górnych, z jasną operacyjną interpretacją, na faktyczną moc obliczeniową zaszumionych urządzeń kwantowych.

5.5 Wkład w rozwój teorii reprezentacji

Kolejnym ważnym elementem cyklu habilitacyjnego jest wkład w rozwój teorii reprezentacji algebry grupowej $\mathbb{C}[S_n] \equiv \mathcal{A}_n(d)$ oraz *algebry częściowo transponowanych operatorów permutacji* $\mathcal{A}_n^{(k)}(d)$ względem k ostatnich układów:

$$\mathcal{A}_n^{(k)}(d) := \mathrm{span}_{\mathbb{C}}\{V_\pi^{(k)} : \pi \in S_n\} \subset \mathrm{Hom}((\mathbb{C}^d)^{\otimes n}), \tag{18}$$

gdzie (k) jest skrótowym zapisem złożenia operacji częściowej transpozycji $t_n \circ t_{n-1} \circ \cdots \circ t_{n-k+1}$ względem układów $n, n-1, \ldots, n-k+1$. Czasami w literaturze algebrę $\mathcal{A}_n^{(k)}(d)$ nazywa się także *algebrą częściowej transpozycji permutacji* [E61]. Okazuje się, że elementy algebry $\mathcal{A}_n^{(k)}(d)$ są reprezentacjami macierzowymi na przestrzeni $(\mathbb{C}^d)^{\otimes n}$, zdefiniowanej w [E62, E63, E64] abstrakcyjnej Walled Brauer Algebra (WBA). Każdy element algebry $\mathcal{A}_n^{(k)}(d)$ spełnia relację podobną do (5), mianowicie mamy:

$$[X, U^{\otimes(n-k)} \otimes \cdots \otimes \overline{U}^{\otimes k}] = 0, \quad \forall X \in \mathcal{A}_n^{(k)}(d), \tag{19}$$

gdzie kreska oznacza sprzężenie zespolone. Mówimy, że operator, który spełnia relację (19) posiada *symetrię częściową*, w przeciwieństwie do operatorów komutujących z diagonalnym działaniem produktu tensorowego n operacji unitarnych (5). Widzimy, że każdy operator posiadający symetrię częściową może zostać zapisany jako kombinacja liniowa częściowo transponowanych operatorów permutacji. Odwrotnie, każdy operator zapisany przy użyciu operatorów $V_\pi^{(k)}$ spełnia relację (19). Oznacza to, że mamy sytuację podobną do dualizmu Schura-Weyla i

oczekujemy analogicznego rozkładu przestrzeni $(\mathbb{C}^d)^{\otimes n}$ jak w (6):

$$(\mathbb{C}^d)^{\otimes n} = \bigoplus_{\xi} \mathcal{H}^{\xi}_{\mathcal{U}} \otimes \mathcal{H}^{\xi}_{\mathcal{WBA}}, \tag{20}$$

gdzie suma prosta przebiega wszystkie nierównoważne nieredukowalne reprezentacje rozważanej algebry. Numerowanie nieredukowalnych jest znane dzięki wcześniejszym pracom, na przykład [E65, E64] wraz z referencjami wewnątrz tych prac. Dokładniej mówiąc pokazano, że każdy indeks ξ jest dwójką $\xi = (\alpha, \mu)$, gdzie $\alpha \vdash n - k$ i $\mu \in \alpha$ jest otrzymane przez dodanie k komórek do α. Naszym celem jest konstrukcja nieredukowalnej bazy operatorowej, pozwalającej na reprezentowanie operatorów działających na części $\mathcal{H}^{\xi}_{\mathcal{WBA}}$, co w rezultacie pozwoli na efektywne obliczenia dla dowolnej ilości układów n, liczby częściowych transpozycji k oraz dowolnego wymiaru d.

W przypadku $d = 2$ mamy dysponujemy relacją $\overline{U} = \sigma_y U \sigma_y$, gdzie $\sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$ jest macierzą Pauliego. Relacja ta definiuje izomorfizm pomiędzy dwiema omawianymi algebrami $\mathcal{A}^{(k)}_n(2)$ oraz $\mathcal{A}_n(2)$. Dla każdego innego $d > 2$ nie dysponujemy już wspomnianym izomorfizmem i nowa algebra $\mathcal{A}^{(k)}_n(d)$ nie jest już algebrą grupową, jak to miało miejsce w przypadku $\mathcal{A}_n(d)$. Jest to bardzo łatwe do zauważenia w najprostszym przypadku, gdy $k = 1$, tzn. kiedy częściowa transpozycja działa na ostatnim $n-$tym układzie. Dokładniej, rozważmy operator permutacji $V_\pi \in \mathcal{A}_n(d)$ dla $\pi = (a, n)$, jasne jest, że wtedy mamy $V_\pi V_\pi^\dagger = \mathbf{1}$. Jednakże, wybierając $V^{t_n}_\pi \in \mathcal{A}^{(1)}_n(d) \equiv \mathcal{A}'_n(d)$, mamy $V^{t_n}_\pi (V^{t_n}_\pi)^\dagger = d V^{t_n}_\pi = d^2 P^+_{an}$, gdzie operator P^+_{an} jest dwu-układowym stanem maksymalnie splątanym. Własność ta powoduje, że rozważana algebra różni się strukturalnie od algebry $\mathcal{A}_n(d)$, co czyni naszą dalszą analizę bardziej skomplikowaną. Okazuje się, że bezpośrednie zastosowanie teorii reprezentacji dla algebry grupowej grupy symetrycznej S_n jest tutaj niewystarczające i jest niezbędne rozwinięcie nowych narzędzi. Jednakże z ogólnej teorii wiemy, że każda skończeniewymiarowa C^*-algebra jest sumą prostą algebr macierzowych i w konsekwencji jest algebrą półprostą. Oczywiście algebra $\mathcal{A}^{(k)}_n(d)$ wraz ze sprzężeniem hermitowskim † tworzy C^*-algebrę i jest zatem półprosta dla każdej wartości n oraz d. Oznacza to, że możemy ją rozłożyć na sumę prostą ideałów minimalnych (nieredukowalnych) M_ξ:

$$\mathcal{A}^{(k)}_n(d) \cong \bigoplus_{\xi} M_\xi \qquad \text{with} \qquad M_\xi = \mathrm{span}_{\mathbb{C}}\{F^{\xi}_{ij} :\ F^{\xi}_{ij} F^{\theta}_{kl} = \delta^{\xi\theta}\delta_{jk} F^{\xi}_{il}\}. \tag{21}$$

Widzimy zatem, że naszym głównym celem jest identyfikacja nieredukowalnych ideałów M_ξ i konstrukcja nieredukowalnej bazy operatorowej F^{ξ}_{ij}.

Chronologicznie nasz praktyczny zestaw narzędzi dla nieredukowalnych reprezentacji algebry $\mathcal{A}^{(k)}_n(d)$ został najpierw rozwinięty dla $k = 1$, a dopiero później został uogólniony na przypadek dowolnego k. Co więcej, wszystkie rezultaty w tej materii zostały uzyskane na przestrzeni wielu lat w cyklu artykułów [H3, H9, H2, H10], które nie zawsze są całkowicie poświęcone czysto matematycznym rozważaniom – większość prac jest dedykowana kwantowej teleportacji. Tutaj jednak, aby uczynić niniejszy autoreferat bardziej przejrzystym zrezygnujemy z chronologicznego prezentowania rezultatów. W zamian prezentujemy dyskusję dla dowolnego $k \geq 1$, dodając odpowiednie komentarze w przypadku $k = 1$. W tym miejscu bardzo ważne jest aby dodać, że część rezultatów odnośnie przypadku $k = 1$ została wypracowana przez habilitanta podczas jego studiów doktoranckich [P3, P4]. Jednakże, podejście przedstawione tam jest nieco innej natury i o ograniczonej praktycznej stosowalności – jest to dobrze opisane w Rozdziale 2.3 oraz Rozdziale 3 artykułu [H2].

Dla przejrzystości dalszej prezentacji zaczniemy od krótkiego podsumowania głównych wyników zawartych w artykułach z cyklu habilitacyjnego:

1. W artykule [H10] podajemy efektywne narzędzia do obliczania śladów częściowych względem dowolnej liczby układów z nieredukowalnych operatorów bazowych rozpinających nieredukowalne reprezentacje grupy S_n sugerowanych dualizmem Schura-Weyla. Dodatkowo dowodzimy nowych relacji ortogonalności dla grupy S_n motywowanych sławnymi relacjami ortogonalności Schura [E66]. W szczególności mówimy tutaj o Proposition 6, Lemacie 9 oraz Corollary 10 ze wspomnianego artykułu. Rezultaty te, w tym stopniu ogólności rozszerzają wyniki z prac [E10, E67] dla operatorów P_μ i są całkowicie nowe dla operatorów bazowych E^μ_{kl}. Z powodu prezentacji w dalszej części autoreferatu przytoczymy tutaj rezultaty dotyczące wspomnianych śladów częściowych:

$$\mathrm{Tr}_{(k)}\, E^{r_{\mu/\beta}\ \widetilde{r}_{\mu/\beta'}}_{i_\beta\quad j_{\beta'}} = \frac{m_\mu}{m_\beta} E^\beta_{i_\beta j_\beta}\delta_{r_{\mu/\beta}\widetilde{r}_{\mu/\beta'}}, \qquad \mathrm{Tr}_{(k)}\, P_\mu = \sum_{\beta\in\mu} m_{\mu/\beta}\frac{m_\mu}{m_\beta}P_\beta, \tag{22}$$

gdzie użyliśmy uproszczonej notacji na ślad częściowy względem ostatnich k układów $\mathrm{Tr}_{(k)} = \mathrm{Tr}_{n-2k+1,\ldots,n-k}$.

2. W artykułach [H3, H10, H2] używamy faktu, że algebra $\mathcal{A}^{(k)}_n(d)$ częściowo transponowanych operatorów permutacji jest reprezentacją macierzową Walled Brauer Albegra na przestrzeni $(\mathbb{C}^d)^{\otimes n}$. Zależność ta, zgodnie z pracą [E65], daje nam wszystkie abstrakcyjne ideały rozważanej algebry (nie minimalne), pokazuje ich wzajemne zagnieżdżenie oraz ich związek z nieredukowalnymi reprezentacjami grup permutacji S_{n-k} oraz S_{n-2k}. Rezultaty te dają nam narzędzie do konstrukcji nieredukowalnej bazy operatorowej macierzowych reprezentacji Walled Brauer Algebra na przestrzeni $(\mathbb{C}^d)^{\otimes n}$, co jest pierwszym w historii rezultatem tego typu. W szczególności, identyfikujemy ideał, który jest głównym obiektem naszych badań w kierunku zrozumienia protokołów teleportacji kwantowej multi oraz port-based. Ta identyfikacja jest możliwa dzięki analizie symetrii wykazywanych przez rozważane protokoły teleportacji w Rozdziale 5.6.

3. Wykorzystując zbudowaną bazę, w tych samych pracach, obliczamy *nieredukowalne elementy macierzowe* podstawowych obiektów naszych studiów – operatorów permutacji częściowo transponowanych względem k ostatnich układów, jak również operatorów permutacji należących do podgrupy S_{n-k}, gdzie operacja częściowej transpozycji nie zmienia rozważanych operatorów. Ta część jest krótko podsumowana z technicznego punktu widzenia w Rozdziale 5.5.1.

Otrzymane rezultaty są nietrywialnym rozszerzeniem narzędzi wykorzystywanych w dualizmie Schura-Weyla do przypadku, gdy mamy do czynienia z symetrią innego typu (symetria częściowa) – $U^{\otimes(n-k)} \otimes \overline{U}^{\otimes k}$, gdzie istniejące wcześniej narzędzia nie mogły być zastosowane bezpośrednio. Dostarczyliśmy narzędzi do badania i lepszego zrozumienia Walled Brauer Algebra na najbardziej przyjaznym poziomie z punktu widzenia praktycznych zastosowań – nieredukowalnych reprezentacji macierzowych. Narzędzia te pozwalają na efektywne obliczenia składania oraz śladów częściowych operatorów z częściowymi symetriami, które wykorzystujemy później w opisie protokołów teleportacji kwantowej, ale nie tylko.

Okazuje się, że rozważany komutant i ogólna teoria Walled Brauer Algebra odgrywa istotną rolę w wielu aspektach fizyki. W układach antyferromagnetycznych, podejście reprezentacyjne bazujące na algebrze WBA, pozwala na redukcję złożoności obliczeniowej przy numerycznej diagonalizacji hamiltonianów opisujących badany układ [E68]. Nasze narzędzia mogą przyczynić się do bardziej analitycznego podejścia do problemu, potencjalnie prowadząc do dalszych uproszczeń. Elementy teorii WBA mogą być także stosowane z sukcesem to wybranych zagadnień fizyki cząstek [E69] oraz teorii grawitacji [E70, E71], gdzie ponownie podejście reprezentacyjne prowadzi do uproszczeń w obliczeniach analitycznych. Narzędzia tutaj omówione mogą być także stosowane w kwantowej teorii informacji – poza wspomnianymi tutaj protokołami

teleportacji kwantowej. Macierzy reprezentacji WBA można użyć do badania i charakteryzacji własności PPT wielocząstkowych stanów kwantowych w duchu pracy Eggelinga i Wernera [E72]. Następnie można analizować odwzorowania ICLM generowane przez rozważaną algebrę wraz z ich $k-$dodatniością [E73, E74, E25]. W szczególności, można się ograniczyć do ICQC i próbować budować nowe przykłady kanałów kwantowych, dla których minimalna entropia Rényi'ego na wyjściu kanału nie jest addytywna [E75]. Pierwszy krok w tym kierunku został zrobiony w pracy [E76], gdzie autorzy konstruują kanały kwantowe rozważając algebrę Temperley-Lieba. Mając solidne narzędzia matematyczne jesteśmy także w stanie podać pełny algebraiczny opis uniwersalnych maszyn klonujących $M \to N$. Dla przypadku $1 \to N$ zostało to częściowo pokazane w pracy [P2], a następnie rozwinięte w [E77]. W ogólności, moglibyśmy również spróbować zastosować nasze narzędzia do podania bardziej ciasnych ograniczeń na wierność splątania dla przybliżonych kowariantnych kodów błędów [E78, E79, E80], co z kolei mogłoby mieć implikacje dla obliczeń kwantowych odpornych na błędy (ang. fault-tolerant quantum computing) oraz pewnych aspektów dualności AdS-CFT [E81]. Wreszcie, korzystając z opracowanych metod, mogliśmy analizować operacje kwantowe wyższego rzędu. W szczególności motywowani pracami [E82, E83] możemy próbować budować grzebienie kwantowe produkujące transpozycję nieznanej unitarnej operacji mając do dyspozycji jej k użyć. Tak szeroki zakres wybranych zagadnień pokazuje ogromny potencjał opracowanych przez nas narzędzi matematycznych do zastosowań w innych problemach współczesnej fizyki i matematyki, co dowodzi, że nie były one wypracowane tylko do jednego konkretnego zastosowania.

5.5.1 Algebra częściowo transponowanych operatorów permutacji - podsumowanie techniczne

Sekcja ta zawiera skrócone podsumowanie techniczne głównych rezultatów dotyczących teorii reprezentacji algebry częściowo transponowanych operatorów permutacji $\mathcal{A}_n^{(k)}(d)$, które są zawarte w cyklu artykułów [H3, H2, H10]. Zaczniemy od wprowadzenia pojęcia *częściowo nieredukowalnych reprezentacji* (ang. *partially irreducible representations (PRIR)*) wprowadzonym dla łatwiejszego obliczania złożeń i śladów częściowych operatorów z symetriami częściowymi, będącym macierzową wersją na konstrukcji Gelfand-Tsetlin'a [E9] dla grupy symetrycznej. W pierwszej kolejności musimy jednak opisać używaną przez nas tutaj notację. Rozważmy $\mu \vdash n$ oraz $\alpha \vdash n-k$ dla $k < n$. Przez indeks $r_{\mu/\alpha}$ oznaczamy ścieżkę na kratownicy Younga prowadzącą od diagramu μ do α. Ścieżka ta jest jednoznacznie wyznaczona poprzez wybór łańcucha nakrywających się diagramów Younga z μ do α, różniących się między sobą o jedną komórkę w każdym kroku:

$$r_{\mu/\alpha} = (\mu, \mu_{n-1}, \ldots, \mu_{n-k+1}, \alpha), \quad \text{i} \quad \mu \ni \mu_{n-1} \ni \cdots \ni \mu_{n-k+1} \ni \alpha. \tag{23}$$

W szczególności oznacza to, że indeks i_μ numerujący elementy macierzowe ϕ^μ może być przedstawiony jednoznacznie jako ścieżka na kratownicy Younga w postaci

$$i_\mu \equiv (r_{\mu/\alpha}, l_\alpha), \qquad \alpha \in \mu, \tag{24}$$

gdzie l_α oznacza teraz indeks przebiegający tylko w zakresie wyznaczonym przez irrep α. Dodatkowo poprzez zapis $\delta_{i_\mu j_\nu}$, gdzie $\mu \vdash n$ oraz $\alpha \vdash n-k$, rozumiemy:

$$\delta_{i_\mu j_\nu} = \delta^{r_{\mu/\alpha}\widetilde{r}_{\nu/\beta}} \delta_{l_\alpha l'_\beta} = \delta_{\mu\nu}\delta_{\mu_{n-1}\nu_{n-1}} \cdots \delta_{\mu_{n-k+1}\nu_{n-k+1}} \delta_{\alpha\beta}\delta_{l_\alpha l'_\beta}. \tag{25}$$

Używając tak wprowadzonej notacji możemy zilustrować nasze macierzowe podejście (PRIR) do konstrukcji Gelfanda-Tsetlin'a. Dowolna nieredukowalna reprezentacja ϕ^μ grupy S_n może zawsze zostać unitarnie przekształcona do PRIRów względem podgrupy $S_{n-k} \subset S_n$ w następujący sposób

$$\forall \sigma \in S_{n-k} \quad \phi_R^\mu(\sigma) = \left(\delta^{r_{\mu/\alpha}\widetilde{r}_{\mu/\beta}} \varphi^\alpha_{i_\alpha j_\alpha}(\sigma)\right) = \bigoplus_{\alpha \in \mu} \varphi^\alpha(\sigma), \tag{26}$$

gdzie indeksy i_α, j_α przebiegają od 1 do wymiaru irrepu α. Bloki pozadiagonalne są macierzami zerowymi i w ogólności nie muszą być kwadratowe. Dla dowolnego elementu $\sigma \in S_n$ forma rozkładu (26) względem podgrupy S_{n-k} jest już bardziej skomplikowana, ponieważ pojawiają się już niezerowe bloki pozadiagonalne:

$$\forall \sigma \in S_n \quad \phi_R^\mu(\sigma) = \left((\phi_R^\mu)_{i_\alpha \; j_\beta}^{r_{\mu/\alpha}, \widetilde{r}_{\mu/\beta}}(\sigma) \right), \tag{27}$$

gdzie znów macierze na diagonali są wymiaru odpowiedniego irrepu φ^α grupy S_{n-k}. Mając wprowadzone pojęcie PRIRów dowodzimy pierwszy techniczny rezultat zawarty w Lemacie 9 oraz Corollary 10 artykułu [H10] dotyczący śladów częściowych z operatorów E_{ij}^μ i P^μ z równania (10):

$$\mathrm{Tr}_{(k)} E_{i_\beta \; j_{\beta'}}^{r_{\mu/\beta} \; \widetilde{r}_{\mu/\beta'}} = \frac{m_\mu}{m_\beta} E_{i_\beta j_\beta}^\beta \delta_{r_{\mu/\beta} \widetilde{r}_{\mu/\beta'}}, \qquad \mathrm{Tr}_{(k)} P_\mu = \sum_{\beta \in \mu} m_{\mu/\beta} \frac{m_\mu}{m_\beta} P_\beta, \tag{28}$$

gdzie wprowadzamy uproszczoną notację na ślad częściowy względem ostatnich k układów $\mathrm{Tr}_{(k)} = \mathrm{Tr}_{n-2k+1,\ldots,n-k}$. Rezultaty te są użyte przez nas później do konstrukcji nieredukowalnej bazy operatorowej rozważanej algebry $\mathcal{A}_n^{(k)}(d)$. W algebrze tej, z przyczyn technicznych wynikających z badania przez nas protokołów teleportacji (multi) port-based opisanych w dalszych rozdziałach, wyróżniamy szczególny częściowo transponowany operator permutacji

$$V^{(k)} := V_{(n-2k+1,n)}^{t_n} V_{(n-2k+2,n-1)}^{t_{n-1}} \cdots V_{(n-k,n-k+1)}^{t_{n-k+1}}, \tag{29}$$

który jest złożeniem rozłącznych częściowo transponowanych operatorów transpozycji działających na przestrzeni $(\mathbb{C}^d)^{\otimes n}$. Naszym głównym celem była konstrukcja nieredukowalnej bazy operatorowej dla ideału dwustronnego $\mathcal{M}$ generowanego przez element $V^{(k)}$ wprowadzony w (29) oraz elementy algebry $\mathcal{A}_n^{(k)}(d)$:

$$\mathcal{M} := \{ V_\tau V^{(k)} V_{\tau'}^\dagger \mid \tau, \tau' \in S_{n-k} \} \subset \mathcal{A}_n^{(k)}(d). \tag{30}$$

Mając wyprowadzone wzory na ślady częściowe po dowolnej ilości układów z nieredukowalnych operatorów bazowych dla grupy symetrycznej (28), możemy zbudować nieredukowalną bazę macierzową dla ideału $\mathcal{M}$. Jest to jeden z głównych rezultatów dotyczących narzędzi matematycznych i jest zawarty w Twierdzeniu 11 pracy [H10]:

$$F_{i_\mu \; j_\nu}^{r_{\mu/\alpha} r_{\nu/\alpha}} = \frac{m_\alpha}{\sqrt{m_\mu m_\nu}} E_{i_\mu \; 1_\alpha}^{r_{\mu/\alpha}} V^{(k)} E_{1_\alpha \; j_\nu}^{r_{\nu/\alpha}}, \tag{31}$$

gdzie m_μ, m_ν oraz m_α są krotnościami irrepów odpowiednio grupy S_{n-k} i S_{n-2k} w dualizmie Schura-Weyla. Dodatkowo, powyższe operatory spełniają następujące prawa składania:

$$F_{i_\mu \; j_\nu}^{r_{\mu/\alpha} r_{\nu/\alpha}} F_{k_{\mu'} \; l_{\nu'}}^{r_{\mu'/\beta} r_{\nu'/\beta}} = \delta^{r_{\nu/\alpha} r_{\mu'/\beta}} \delta_{j_\nu k_{\mu'}} F_{i_\mu \; l_{\nu'}}^{r_{\mu/\alpha} r_{\nu'/\alpha}}. \tag{32}$$

Rezultaty zawarte w (31) oraz (32) są analogami nieredukowalnej bazy macierzowej E_{ij}^α danej poprzez (10) z relacjami ortogonalności (8) dla algebry grupowej $\mathcal{A}_n(d)$ na przestrzeni $(\mathbb{C}^d)^{\otimes n}$. Pierwsze podejście do konstrukcji macierzowych nieredukowalnych operatorów bazowych zostało zaprezentowane dla $k = 1$ w pracy [H2] w Twierdzeniu 38. W artykule tym poczyniliśmy kluczowy krok w kierunku zrozumienia ogólnej teorii $\mathcal{A}_n'(d)$ przedstawionej przez autora na jego wcześniejszym etapie kariery naukowej w pracach [P3, P4]. Mówiąc dokładniej, pozbyliśmy się wielu technicznych problemów, które powodowały realne trudności ze stosowaniem wprowadzonych wcześniej narzędzi matematycznych nawet dla przypadku $k = 1$. W szczególności, możemy wspomnieć tutaj o konieczności wyboru niezerowego elementu operatorów rozpinających algebrę $\mathcal{A}_n(d)$, co może być zrobione dla ustalonego n oraz d, ale nie jest możliwe w ogólnym przypadku – zostało to zilustrowane w Twierdzeniu 12 oraz Remark 13 w

pracy [H2]. Dodatkowo, wszystkie bardzo złożone wyrażenia opisujące algebrę $\mathcal{A}'_n(d)$ dzięki użyciu pojęcia częściowo nieredukowalnych reprezentacji mogą zostać znacznie uproszczone – zostało to omówione z Rozdziale 4 pracy [H2]. Pomimo poczynionego postępu w tym temacie nadal istniała potrzeba analizy dla większych wartości k, co jest prezentowane w pracy [H10].

Idąc dalej, w tym samym Twierdzeniu 11 z pracy [H10] udowadniamy, że element $V^{(k)}$ generujący ideał $\mathcal{M}$, może zostać zapisany poprzez operatory z (31), co jest relacją podobną do wzoru (11):

$$V^{(k)} = \sum_{\mu,\nu} \sum_{r_{\mu/\alpha}, \widetilde{r}_{\nu/\alpha}} \sum_{l_\alpha} \frac{\sqrt{m_\mu m_\nu}}{m_\alpha} F_{l_\alpha \; r_{\mu/\alpha} \; \widetilde{r}_{\nu/\alpha} \; l_\alpha}^{\quad r_{\mu/\alpha} \; \widetilde{r}_{\nu/\alpha}}. \tag{33}$$

Ten szczególny rezultat jest uogólnieniem wyniku zawartego w Twierdzeniu 38 w [H2] dla dowolnej liczby częściowych transpozycji k. Relacja ta, razem z własnościami nieredukowalnej bazy operatorowej dla $\mathcal{A}_n(d)$ pozwala nam na udowodnienie Lematu 12 z omawianego artykułu, w którym obliczamy odpowiednie lewe działania operatorów bazowych:

$$F_{k_\beta \; r_{\mu/\beta} \; r_{\nu/\gamma} \; l_\gamma}^{\quad r_{\mu/\alpha} \; r_{\nu/\alpha}} V^{(k)} = \sum_{\mu'} \sum_{r_{\mu'/\gamma}} \frac{\sqrt{m_\nu m_{\mu'}}}{m_\gamma} F_{k_\beta \; r_{\mu/\beta} \; r_{\mu'/\gamma} \; l_\gamma}^{\quad r_{\mu/\gamma} \; r_{\mu'/\gamma}} \delta^{r_{\nu/\alpha} r_{\nu/\gamma}} \tag{34}$$

oraz

$$F_{k_\beta \; r_{\mu/\beta} \; r_{\nu/\gamma} \; l_\gamma}^{\quad r_{\mu/\alpha} \; r_{\nu/\alpha}} V_\tau = \sum_{k_\nu} \phi^\nu_{j_\nu k_\nu}(\tau) F_{i_\mu \quad k_\nu}^{r_{\mu/\alpha} r_{\nu/\alpha}} \tag{35}$$

gdzie $\phi^\nu_{j_\nu k_\nu}(\tau)$ są elementami macierzowymi V_τ dla $\tau \in S_{n-k}$, które mogą zostać obliczone z relacji (11). Rezultaty te pozwalają na wyprowadzenie wyrażeń na elementy macierzowe nieredukowalnych reprezentacji interesujących nas obiektów (Lemat 13 [H10]):

$$\left(V^{(k)}\right)_{k_\beta \; r_{\mu/\beta} \; r_{\nu/\gamma} \; l_\gamma}^{\quad r_{\mu/\alpha} \; r_{\nu/\alpha}} = \delta_{k_\beta l_\gamma} \delta^{r_{\mu/\alpha} r_{\mu/\beta}} \delta^{r_{\nu/\alpha} r_{\nu/\gamma}} \frac{\sqrt{m_\mu m_\nu}}{m_\alpha}, \tag{36}$$

oraz

$$(V_\tau)_{i_\mu \quad j_\nu}^{r_{\mu/\alpha} r_{\nu/\alpha}} = \delta^{r_{\mu/\alpha} r_{\nu/\alpha}} \delta_{i_\mu j_\nu} \sqrt{\frac{m_\mu}{m_\nu}} \sum_{k_\mu} \phi^\mu_{k_\mu i_\mu}(\tau), \tag{37}$$

Jak widzimy elementy z równań (36) i (37) są powiązane z parametrami opisującymi irrepy grupy symetrycznej S_n oraz S_{n-2k}. Skonstruowaliśmy również projektory, które są analogami projektorów Younga z (10). Każdy taki projektor w swoim działaniu powoduje organicznie do nieredukowalnych bloków algebry $\mathcal{A}_n^{(k)}(d)$ w ideale $\mathcal{M}$ (Definicja 15 w pracy [H10]):

$$\forall \alpha \; \forall \mu \in \alpha \quad F_\mu(\alpha) := \sum_{r_{\mu/\alpha}} \sum_{k_\mu} F_{k_\mu \quad k_\mu}^{r_{\mu/\alpha} r_{\mu/\alpha}}. \tag{38}$$

Operatory tego typu zostały po raz pierwszy podane dla $k = 1$ w Twierdzeniu 1 w artykule [H3] w kontekście protokołów teleportacji port-based. Ponadto, operatory te spełniają reguły ortogonalności podobne do tych z (9) w indeksach α, μ (Lemat 15 w [H10]. Pisząc dokładniej mamy:

$$F_\mu(\alpha) F_\nu(\beta) = \delta^{\mu\nu} \delta^{\alpha\beta} F_\mu(\alpha). \tag{39}$$

Zobaczymy później, że projektory te odgrywają centralną rolę w opisie pomiarów w protokołach teleportacji (multi) port-based. Motywowani tym zastosowaniem dowodzimy bardziej technicznych lematów i faktów w duchu relacji (28). W szczególności, główne rezultaty są zawarte w Lemacie 18, Lemacie 19 oraz Lemacie 21 artykułu [H10]. Ponieważ nie opisujemy tutaj szczegółowo wszystkich dowodów dotyczących schematów teleportacji, zdecydowaliśmy się więc nie wypisywać tutaj tych wyrażeń wprost.

5.6 Warianty protokołu teleportacji kwantowej port-based

Protokół port-based teleportation (PBT) został wprowadzony w roku 2008 przez Hiroshimę i Ishizakę w cyklu dwóch prac [E84, E85]. Jego przełomowość polega na tym, że odbiorca teleportowanego stanu nie musi stosować już unitarnej korekcji, tak jak to ma miejsce oryginalnym protokole teleportacji wprowadzonym w 1993 roku w pracy [E86]. To właśnie brak wspomnianej korekcji pozwolił na całkowicie nowe zastosowania protokołu PBT, gdzie zwykły protokół teleportacji nie może być stosowany.

Pierwszym ważnym zastosowaniem PBT jest podanie nowej architektury dla uniwersalnych programowalnych procesorów kwantowych, przeprowadzających obliczenia z wykorzystaniem teleportacji [E7, E87, E84, E85]. Schemat PBT został także z powodzeniem użyty w kwantowej kryptografii (ang. port-based cryptography), gdzie posłużył do budowy protokołów do natychmiastowej implementacji pomiarów i obliczeń. To zastosowanie pozwoliło na podanie nowych ataków kryptograficznych, dla których ilość zasobu mierzona poprzez ilość zużytego splątania, została zredukowana z podwójnie eksponencjalnej do eksponencjalnej [E88]. Wersja kubitowa protokołu PBT pozwoliła na podanie związku pomiędzy teorią złożoności komunikacyjnej, a łamaniem nierówności Bella [E89]. To całkowicie nowe zastosowanie pozwoliło wykazać, że każda dla kwantowej przewagi w złożoności komunikacyjnej zawsze jest możliwość otrzymania takiej statystyki pomiarów, która łamie jakąś nierówność Bella. Istnieje zatem głęboka zależność pomiędzy nielokalnością, a przewagą kwantową w złożoności komunikacyjnej. Kubitowe PBT może być również interpretowane jako uniwersalny symulator dla kanałów kubitowych [E90], poprawiając symulację kanału tłumiącego amplitudę (ang. *amplitude damping channel*). Rozszerzając protokół PBT do tzw. protokołu *PBT streching* możemy podać fundamentalne ograniczenia na możliwość rozróżniania kanałów kwantowych [E91]. Ostatnio, niektóre aspekty protokołu PBT odegrały rolę w analizie i konstrukcji uniwersalnych obwodów kwantowych produkujących odwrotność dowolnej nieznanej operacji unitarnej [E92, E82], w teorii przechowywania i odzyskiwania unitarnych kanałów kwantowych [E93], a także w kontekście dualności AdS/CFT [E94]. Ta szeroka gama zastosowań i możliwość dalszego rozwoju w wielu problemach współczesnej teorii informacji kwantowej motywuje nas do bardziej szczegółowego badania protokołu PBT we wszystkich jego wariantach, zwłaszcza w przypadku wyższego wymiaru.

W każdej z wersji protokołu PBT nadawca (Alicja) oraz odbiorca (Bob) współdzielą N par maksymalnie splątanych, każdą z nich zwaną *portem*, jest to zilustrowane na Rysunku 3. Zbiór wszystkich stanów splątanych (portów) jest z kolei nazywany *stanem zasobu*, który jest postaci

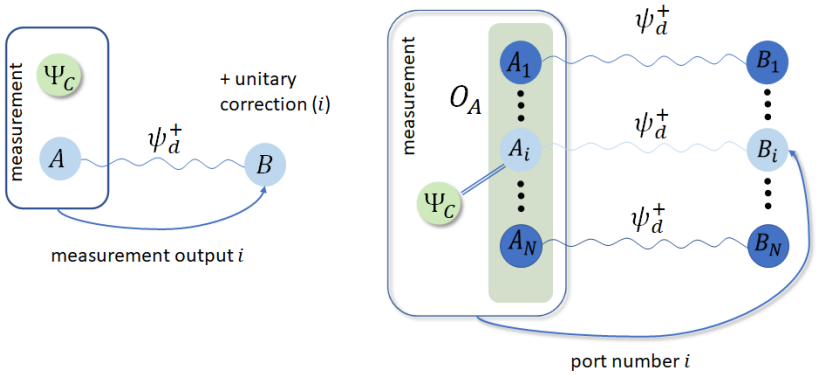
$$|\Psi\rangle_{AB} = (O_A \otimes \mathbf{1}_B)|\Psi^+\rangle_{AB} = (O_A \otimes \mathbf{1}_B)|\psi^+\rangle_{A_1B_1} \otimes |\psi^+\rangle_{A_2B_2} \otimes \cdots \otimes |\psi^+\rangle_{A_NB_N}, \qquad (40)$$

gdzie $A = A_1A_2\cdots A_N$, $B = B_1B_2\cdots B_N$ oraz O_A, wraz z warunkiem normalizacyjnym $\mathrm{Tr}(O_A^\dagger O_A) = d^N$, jest pewną globalną operacją zwiększającą wydajność protokołu [E85, E95], [H3, H4]. W nieoptymalnym protokole PBT mamy $O_A = \mathbf{1}_A$, podczas gdy dla optymalnego schematu jej jawna postać jest znana i dyskutowana w [E85] i [H4]. Alicja, aby przesłać do Boba nieznany stan Ψ_C cząsteczki, dokonuje globalnego pomiaru Π_i^{AC} na stanie Ψ_C oraz swojej części stanu zasobu A, otrzymując klasyczny wynik $1 \leq i \leq N$. Następnie za pośrednictwem klasycznego kanału Alicja komunikuje indeks i Bobowi, wskazując port na którym dokonała się teleportacja i żadna dalsza korekcja przesłanego stanu nie jest już wymagana.

Rozróżniamy dwa warianty PBT:

1. *Deterministyczny PBT (dPBT):* Nieznany stan kwantowy Ψ_C jest zawsze przesyłany do odbiorcy, ale transmisja nie jest doskonała. Kanał teleportacyjny $\mathcal{N}$ może być zapisany jako:

$$\mathcal{N}(\Psi_C) = \sum_{i=1}^{N} \mathrm{Tr}_{AC}\left[\Pi_i^{AC}\left(\left(O_A \otimes \mathbf{1}_{\widetilde{B}}\right)\sigma_{A_i\widetilde{B}}\left(O_A^\dagger \otimes \mathbf{1}_{\widetilde{B}}\right) \otimes \psi_C\right)\right], \qquad (41)$$



Rysunek 3: Lewy rysunek przedstawia konfiguracje protokołu teleportacji kwantowej wprowadzonej w [E86]. W tym protokole odbiorca aby odzyskać teleportowany stan musi zastosować operację unitarnej korekcji, która zależy od klasycznej informacji przesłanej przez nadawcę. Prawy rysunek przedstawia konfigurację protokołu PBT [E84, E85]. W tym przypadku, przeciwnie do standardowej teleportacji, nadawca i odbiorca współdzielą N maksymalnie splątanych par (portów). Odbiorca, aby odzyskać teleportowany stan musi jedynie wybrać jeden z portów wskazanych przez klasyczną informację od nadawcy. Żadna dalsza procedura korekcji nie jest już potrzebna. Jednakże z powodu twierdzenia o zakazie programowania [E96], przesył nie jest idealny i wierność teleportacji jest mniejsza niż 1. Doskonały przesył jest możliwy jedynie w asymptotycznym scenariuszu, gdy $N \to \infty$.

gdzie przez Tr_{AC} oznaczamy ślad częściowy po układach AC z wyłączeniem układu $\widetilde{B}$. Stany $\sigma_{A_a\widetilde{B}}$ są nazywane *stanami sygnałowymi* i mają następującą postać:

$$\sigma_{A_i\widetilde{B}} := \sigma_i := \frac{1}{d^{N-1}} \mathbf{1}_{\overline{A}_i} \otimes P^+_{A_i\widetilde{B}}, \tag{42}$$

gdzie $P^+_{A_i\widetilde{B}}$ jest projektorem na stan maksymalnie splątany pomiędzy układem A_i oraz$\widetilde{B}$. Aby poznać efektywność kanału teleportacji możemy zapytać jak dobrze przesyła on nieklasyczne korelacje. Oznacza to, że interesuje nas obliczenie wierności splątania $F(\mathcal{N})$ pomiędzy stanem na wyjściu kanału teleportującego $\mathcal{N}$, gdy dokonujemy przesyłu podukładu C ze stanu maksymalnie splątanego P^+_{CD}, a stanem po idealnym przesyle $P^+_{\widetilde{B}D}$:

$$F(\mathcal{N}) = \mathrm{Tr}\left[P^+_{\widetilde{B}D}(\mathcal{N}_C \otimes \mathbf{1}_D)(P^+_{CD})\right] = \frac{1}{d^2}\sum_{i=1}^{N} \mathrm{Tr}\left[\left(O_A^\dagger \otimes \mathbf{1}_{\widetilde{B}}\right) \Pi_i^{A\widetilde{B}} \left(O_A \otimes \mathbf{1}_{\widetilde{B}}\right) \sigma_{A_i\widetilde{B}}\right]. \tag{43}$$

W szczególności, w artykule [E85] pokazano, że kanał teleportacji $\mathcal{N}$ jest kanałem depolaryzującym i jako rezultat jego działania otrzymujemy stan izotropowy z parametrem mieszania $p = p(N, d)$ związanym z wiernością splątania $F(\mathcal{N})$ w następujący sposób [E91]:

$$F(\mathcal{N}) = 1 - p + \frac{p}{d^2}. \tag{44}$$

Zgodnie z ostatnimi wynikami zawartymi w artykule [E97], wiemy że pomiary postaci *square-root measurements* (SRM) są optymalne w każdej wersji protokołu PBT (w nie- i optymalnym PBT). Przy czym pomiary optymalne (POVM) w wersji nieoptymalnej protokołu PBT mają postać:

$$\forall 1 \le i \le N \qquad \Pi_i^{AC} = \frac{1}{\sqrt{\rho}} \sigma_{A_iC} \frac{1}{\sqrt{\rho}}, \quad \text{where} \quad \rho = \sum_{i=1}^{N} \sigma_{A_iC}. \tag{45}$$

Operator ρ^{-1} jest określony na nośniku operatora ρ, zatem aby zapewnić sumowanie się wszystkich POVMów do identyczności $\mathbf{1}_{AC}$ na całej przestrzeni $(\mathbb{C}^d)^{\otimes N+1}$, musimy

do każdego z Π_i^{AC} dodać dodatkowy wyraz $\Delta = \frac{1}{N}\left(\mathbf{1}_{AC} - \sum_{i=1}^{N}\Pi_i^{AC}\right)$. Okazuje się, że ten zabieg nie zmienia wierności splątania $F(\mathcal{N})$ kanału $\mathcal{N}$, ponieważ dodatkowy wyraz Δ jest ortogonalny do przestrzeni, na kórej określone są operatory opisujące PBT [E85, E84], [H3].

2. *Probabilistyczny PBT (pPBT):* W tym wariancie teleportacji nieznany stan jest transmitowany do Boba z wiernością $F = 1$, jednak nadawca i odbiorca muszą zaakceptować niezerowe prawdopodobieństwo, że protokół zakończy się niepowodzeniem (brakiem teleportacji). W tym protokole Alicja ma dostęp do $N+1$ POVMów $\{\Pi_0^{AC}, \Pi_1^{AC}, \ldots, \Pi_N^{AC}\}$, przy czym za niepowodzenie teleportacji odpowiada pomiar Π_0^{AC}. Efektywność protokołu jest opisana poprzez średnie prawdopodobieństwo sukcesu teleportacji p_{succ}, które jest równe [E85], [H3]:

$$p_{succ} = \frac{1}{d^{N+1}} \sum_{i=1}^{N} \mathrm{Tr}\left[O_A^\dagger \Pi_i^{AC} O_A\right]. \tag{46}$$

Wymóg idealnego przesyłu stanu teleportowanego nakłada dodatkowe warunki na pomiary dostępne dla Alicji, a dokładniej mówiąc mogą one być tylko następującej postaci [E85], [H3]:

$$\forall 1 \leq i \leq N \qquad \Pi_i^{AC} = P_{A_iC}^{+} \otimes \Theta_{\overline{A}_i}, \tag{47}$$

gdzie forma dodatnich operatorów $\Theta_{\overline{A}_i}$ musi zostać znaleziona i zostanie to przedyskutowane później. W tym przypadku $\overline{A}_i$ oznacza, że operator działa na wszystkich układach $A_1 \cdots A_N$, oprócz układu A_i. Optymalna forma operatorów $\Theta_{\overline{A}_i}$ w obu wersjach protokołu probabilistycznego (nieoptymalnej i optymalnej) została podana dla kubitów w [E85] i dla większych wymiarów przestrzeni w [H3].

Zwróćmy tutaj uwagę na pewną konwencję notacyjną. Zarówno w przypadku deterministycznych oraz probabilistycznym operację optymalizującą oznaczamy jako O_A. Należy przy tym pamiętać, że jest ona różna dla różnych wersji protokołu, to samo dotyczy pomiarów wykorzystywanych przez Alicję. To o jakiej operacji O_A, czy pomiarach mówimy, zawsze będzie jasno wynikało z kontekstu.

W każdym z przypadków idealna transmisja z jednostkową wiernością lub z jednostkowym prawdopodobieństwem jest możliwa tylko w przypadku asymptotycznym, gdy $N \to \infty$. Własność ta jest konsekwencją twierdzenia no-go dla uniwersalnych procesorów o skończonych rozmiarach (ang. *no-programming theorem*) [E96]. To ograniczenie na PBT rodzi fundamentalne pytanie, zwłaszcza w świetle wymienionych na początku zastosowań, jak dobrze strony mogą przesyłać stany kwantowe poprzez protokoły PBT o skończonej liczbie N portów oraz jego dowolnym wymiarze d.

Jasne jest, że bezpośrednie zastosowanie obliczeń numerycznych nie daje dobrych rezultatów, ponieważ wymiary macierzy wszystkich obiektów opisujących PBT rosą jak d^{N+1}, co powoduje realne komplikacje obliczeniowe. Do tej pory analiza wydajności protokołów PBT znana była tylko w przypadku kubitowym, gdy $d = 2$ [E84, E85]. Wiążącą analizę uzyskano używając formalizmu teorii momentu pędu $SU(2)^{\otimes N}$, w tym teorii współczynników Clebscha-Gordana wraz z metodami programowania wypukłego. Narzędzia te działają jednak efektywnie tylko w przypadku kubitowym i nie dają się zastosować do analizy w wyższych wymiarach. W przypadku $d > 2$ znane były jedynie cząstkowe rezultaty pokazujące dolne/górne ograniczenia na wierność F, na prawdopodobieństwo sukcesu p_{succ} w funkcji wymiaru oraz liczby portów [E88, E85, E98] dla protokołów nieoptymalnych. Dla przypadku deterministycznego, ograniczenia polegały na analizie spektralnej operatora ρ [E85], oraz związku z protokołem rozróżniania stanów kwantowych [E88]. W przypadku probabilistycznym z kolei, ograniczenie bazowało na zakazie kwantowego klonowania i zasadzie niesygnalizowania [E98]. Jednak we wszystkich przypadkach nie wiadomo było do końca jak bliskie są one rzeczywistych wartości dla skończonej liczby portów N i w dowolnego wymiaru d. Pierwsze bezpośrednie ana-

lityczne podejście do opisu wydajności PBT w wyższych wymiarach zostało zaproponowane w [E99] dzięki wykorzystaniu graficznych metod dla algebry Temperley-Lieb. Autorzy podali wyrażenia na wierność splątania oraz prawdopodobieństwo sukcesu dla dowolnego wymiaru d oraz $N \in \{2, 3, 4\}$. Metody graficzne również nie są zadowalające ze względu na bardzo dużą liczbę przypadków niezbędnych do rozważenia, która rośnie eksponencjalnie z liczbą portów. Dlatego istniała konieczność wypracowania nowych, bardziej efektywnych metod do analizy protokołów PBT. W tym celu zdecydowaliśmy się zidentyfikować, a następnie wykorzystać istniejące w problemie symetrie, co pozwala na zastosowanie elementów teorii reprezentacji grup i algebr skończonych. Poniżej podam i omówię najważniejsze uzyskane wyniki dotyczące badania efektywności PBT w wyższych wymiarach.

5.6.1 Protokół teleportacji kwantowej port-based dla dowolnego wymiaru przestrzeni

Jak to opisaliśmy w poprzednim rozdziale, wielkim otwartym problemem było znalezienie opisu PBT w wyższych wymiarach oraz ich optymalnej wersji w najbardziej ogólnej konfiguracji – z optymalnym pomiarem, który działa dla dowolnego wymiaru i liczby portów, a także ustalenie ich wydajności wraz z dostarczeniem możliwie łatwych do analizy wyrażeń na wierność splątania i prawdopodobieństwo sukcesu. W pracach [H3, H4, H2], wraz z współautorami, podałem pełną charakteryzację wydajności wszystkich istniejących wariantów PBT dla dowolnego wymiaru d oraz dowolnej liczby portów N. Możliwość pełnego opisu wszystkich protokołów PBT wynikała z dwóch kluczowych innowacji opisanych w rozdziale 5.5:

1) Nowatorskie połączenie protokołów PBT z algebrą częściowo transponowanych operatorów permutacji $\mathcal{A}'_d(n)$.

2) Nowe i efektywne narzędzia (analityczne i numeryczne) do obliczania złożeń operatorów z symetriami częściowymi wraz z ich śladami częściowymi i częściowymi transpozycjami.

W pierwszej kolejności zidentyfikowaliśmy symetrie występujące w protokołach PBT oraz pokazaliśmy ich związek z nieredukowalnymi reprezentacjami algebry częściowo transponowanych operatorów permutacji $\mathcal{A}'_d(n)$. Przypomnijmy, że każdy stan maksymalnie splątany jest $U \otimes \overline{U}$ niezmienniczy [E100], gdzie kreska oznacza sprzężenie zespolone elementu U z grupy unitarnej $\mathcal{U}(d)$. Implikuje to następujące symetrie dla wszystkich stanów sygnałowych $\sigma_i^{A\widetilde{B}}$ z (42):

$$[U^{\otimes N} \otimes \overline{U}, \sigma_i^{A\widetilde{B}}] = 0, \quad \forall\, U \in \mathcal{U}(d), \tag{48}$$

gdzie $\overline{U}$ działa na $\widetilde{B}$, a $U^{\otimes N}$ działa na układach $A = A_1 \cdots A_N$. Konstrukcja $\sigma_i^{A\widetilde{B}}$ pozwala na zidentyfikowanie dodatkowej symetrii – kowariancji względem elementów grupy symetrycznej S_N, działających na pierwszych N układach:

$$V_\pi \sigma_i^{A\widetilde{B}} V_\pi^\dagger = \sigma_{\pi(i)}^{A\widetilde{B}}, \quad \forall\, \pi \in S_N. \tag{49}$$

W szczególności, wybierając dowolny stan sygnałowy z całego zbioru, na przykład $\sigma_N^{A\widetilde{B}}$, to każdy inny może być z niego wygenerowany poprzez zadziałanie elementem z warstwy S_N/S_{N-1}, gdzie elementy te w reprezentacji V są postaci $V_{(i,N-1)}$, dla $i = 1, \ldots, N-1$. Takie same relacje kowariancji jak w (49) zachodzą również dla pomiarów $\{\Pi_i^{AC}\}_{i=1}^N$ we wszystkich wariantach PBT:

$$V_\pi \Pi_i^{AC} V_\pi^\dagger = \Pi_{\pi(i)}^{AC}, \quad \forall\, \pi \in S_N. \tag{50}$$

Przypomnijmy teraz, że operator ρ (45) jest sumą wszystkich możliwych stanów $\sigma_N^{A\widetilde{B}}$:

$$\rho = \frac{1}{d^N} \sum_{i=1}^N V_{(A_i,C)}^{t_C} \equiv \frac{1}{d^N} \sum_{i=1}^N V'_{(i,n)}. \tag{51}$$

Przy czym w drugim wyrażeniu przenumerowaliśmy układy zgodnie z regułą $A_1 \mapsto 1, A_2 \mapsto 2, \ldots, A_N \mapsto N, C \mapsto n = N+1$. Dla notacyjnej przejrzystości przez $'$ oznaczamy częściową transpozycję względem $n-$tego układu. Relacja (51) implikuje to, że operator ρ również posiada symetrie opisane równaniem (48) oraz dodatkowo jest on niezmienniczy względem działania grupy symetrycznej S_N. W dalszej części tego podrozdziału będziemy w dużym stopniu korzystać z tej właściwości. Widzimy zatem, że główne elementy niezbędne do efektywnego opisu PBT mogą być zapisane przy pomocy częściowo transponowanych operatorów permutacji z algebry $\mathcal{A}'_d(n)$.

Wykorzystując opisane wyżej symetrie wraz z narzędziami matematycznymi opisanymi w Rozdziale 5.5.1, dowodzimy Twierdzenia 1 oraz Proposition 2 w artykule [H3], mówiące że operator ρ z równania (51) posiada następujący rozkład spektralny:

$$\rho = \sum_{\alpha \vdash n-2} \sum_{\mu \in \alpha} \lambda_\mu(\alpha) F_\mu(\alpha), \tag{52}$$

gdzie $F_\mu(\alpha)$ są projektorami na nieredukowalne komponenty algebry $\mathcal{A}'_n(d)$ z równania (38) dla $k = 1$, którym odpowiadają następujące wartości własne

$$\lambda_\mu(\alpha) = \frac{N}{d^N} \frac{m_\mu d_\alpha}{m_\alpha d_\mu}. \tag{53}$$

Wynik ten pozwala na rozwiązanie pierwszej technicznej przeszkody, mianowicie pozwala na obliczenie ρ^{-1} oraz $1/\sqrt{\rho}$ z równiania (45). Dzięki temu z kolei możemy obliczyć wierność splątania kanału teleportującego $F(\mathcal{N})$ z (43), gdy $O_A = \mathbf{1}_A$ (nieoptymalne deterministyczne PBT), w terminach czysto teoriogrupowych parametrów opisujących irrepy S_N w dualizmie Shura-Weyla (Twierdzenie 12 w [H3]):

$$F = \frac{1}{d^{N+2}} \sum_{\alpha \vdash n-2} \left(\sum_{\mu \in \alpha} \sqrt{d_\mu m_\mu} \right)^2. \tag{54}$$

Wielkości z ostatniego wyrażenia są już efektywnie obliczalne. W tym celu stworzyliśmy dedykowane oprogramowanie napisane w języku Python z wykorzystaniem pakietu Sage [E101]. Wyniki numerycznych obliczeń przedstawione są na rysunku 4. Widzimy z niego, że wierność splątania maleje wraz ze wzrostem wymiaru portu d, ale zmierza do 1 dla ustalonego d i rosnącej ilości portów N. Dodatkowo w artykule [H2] dowodzimy, że faktycznie wyrażenie (54) osiąga 1 dla $N \to \infty$ (Twierdzenie 52) dla dowolnego wymiaru d.

W artykule [H4] dostarczamy analizy wydajności optymalnego deterministycznego PBT, tzn. gdy Alicja optymalizuje pomiary oraz stan zasobu przy pomocy operacji O_A z (40). W tym przypadku sytuacja jest bardziej skomplikowana w porównaniu do nieoptymalnego deterministycznego PBT, ponieważ musimy także podać wyrażenia na optymalne pomiary oraz operację optymalizującą O_A, zapewniającą maksymalizację wierności splątania F. Może to zostać zrealizowane poprzez sformułowanie, a następnie rozwiązanie odpowiedniego problemu prymalnego i dualnego SDP (Rozdział 5.1 z Twierdzeniem 30 oraz Rozdział 5.2 z Twierdzeniem 31 w [H4]). W tym przypadku wykorzystując wewnętrzne symetrie występujące w problemie możemy rozwiązać odpowiednie problemy optymalizacyjne SDP analitycznie. Co więcej, rozwiązanie problemu prymalnego i dualnego pokrywają się, dając nam wyrażenie na optymalną wierność splątania F_{opt} oraz optymalne postaci rozważanych operatorów (Proposition 32 w [H4]), jest to tzw. własność *strong duality*. Optymalna wierność splątania F_{opt} jest opisana za pomocą statycznego obiektu – minorów głównych tzw. *macierzy teleportacji* M_F^d wprowadzonej w Rozdziale 4 pracy [H4]):

$$F_{opt} = \frac{1}{d^2} ||M_F^d||_\infty. \tag{55}$$

Na rysunku 4 przedstawione są wartości numeryczne optymalnej wierności plątania F_{opt} z (55) w porównaniu z wiernością splątania F daną wzorem (54) dla protokołu nieoptymalnego –

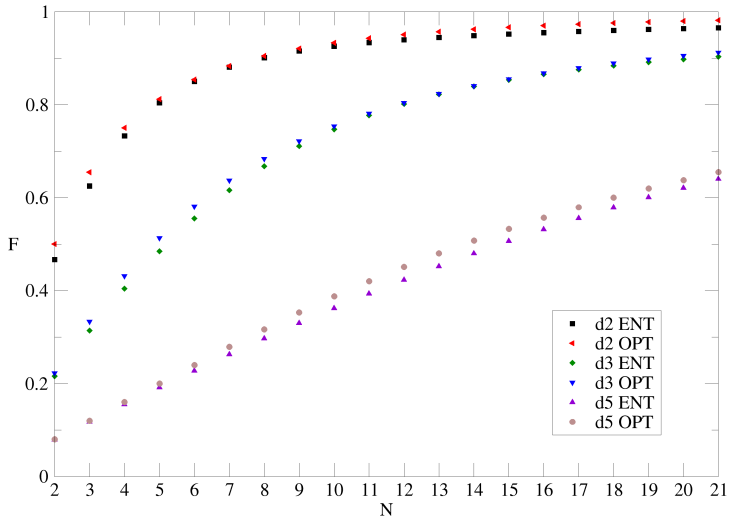
widzimy większą wydajność protokołu optymalnego. Jak zatem widzimy, aby obliczyć wierność F_{opt} musimy poznać maksymalną wartość własną $\lambda_{\max}(M_F^d)$ minorów głównych macierzy teleportacji M_F^d, musimy zatem poznać jej strukturę wewnętrzną. Okazuje się, że wiersze i kolumny macierzy teleportacji są numerowane diagramami Younga o N komórkach, uszeregowanych w malejącym porządku leksykograficznym. Następnie każdy element macierzowy koduje wzajemną relację pomiędzy diagramami Younga o N oraz $N-1$ komórkach. Dokładniej, każdy element macierzy M_F^d jest następującej postaci (Definicja 4 w [H4]):

$$M_F := (n_\mu \delta_{\mu,\nu} + \Delta_{\mu,\nu}), \tag{56}$$

gdzie n_μ jest liczbą diagramów Younga $\alpha \vdash N-1$, dla których $\alpha \in \mu$, oraz

$$\Delta_{\mu,\nu} = \begin{cases} 1 \text{ jeżeli } \mu/\nu = \square, \\ 0 \text{ w przeciwnym razie.} \end{cases} \tag{57}$$

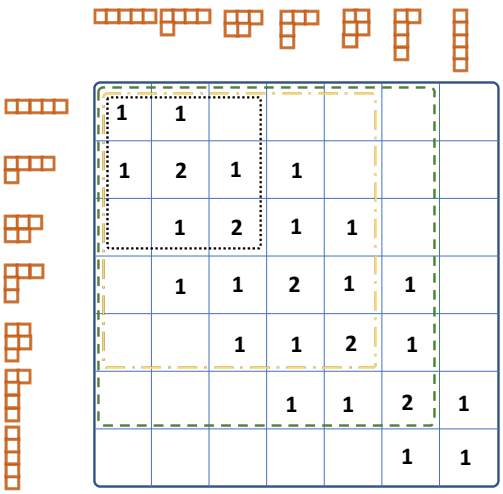
Symbol $\mu/\nu = \square$ oznacza diagramy Younga μ, ν, które mogą zostać otrzymane jeden z dru-



Rysunek 4: Wykres przedstawia porównanie nieoptymalnego oraz optymalnego deterministycznego protokołu PBT. Symbolem dX ENT oznaczamy wierność protokołu deterministycznego, gdy stan zasobu składa się z par maksymalnie splątanych, a pomiary są w postaci *square-root measuremnts*; X odpowiada wymiarowi portu. Symbol dX OPT odpowiada najlepszą możliwą wartość wierności osiągniętą poprzez optymalizację stanu zasobu oraz pomiarów równocześnie, tzn. gdy rozważamy optymalny wariant protokołu teleportacji.

giego poprzez przemieszczenie jednej komórki. Na rysunku 5 przedstawiamy jawną postać macierzy teleportacji dla różnych wartości wymiaru portu d oraz ilości portów N. Okazuje się, że jawna analityczna postać $\lambda_{\max}(M_F^d)$ jest znana tylko w dwóch przypadkach, gdy $d \geq N$ (Corollary 8 w [H4]) oraz $d = 2$ w Rozdziale 5.3 w [H4]). W pierwszym przypadku maksymalna wartość własna jest równa N dając w rezultacie wierność splątania $F_{opt} = N/d^2$. W drugim przypadku, macierz teleportacji jest macierzą trójdiagonalną, dla której zagadnienie własne zostało rozwiązane w artykule Losonczi'ego [E102]. Wykorzystując te rezultaty odtwarzamy wynik na optymalną wierność w przypadku kubitowym [E85], który jest następujący:

$$F_{opt} = \cos^2\left(\frac{\pi}{N+2}\right). \tag{58}$$



Rysunek 5: Grafika przedstawia macierze teleportacji dla optymalnego deterministycznego PBT przy ustalonej liczbie portów $N = 5$ i różnych wymiarów portów $d = 2, 3, 4$ oraz $d \geq 5$. Na rysunku zaznaczyliśmy kolejne minory główne, które są zdefiniowane przez diagramy Younga o wysokości nie większej niż d. Cała macierz odpowiada przypadkowi, gdy wymiar portu jest nie mniejszy niż 5. Zielona przerywana linia odpowiada przypadkowi $d = 4$. Następnie, mamy odpowiednio $d = 3$ (żółty) oraz $d = 2$ (czarny). Puste komórki wypełniamy zerami.

W pozostałych przypadkach musimy używać efektywnych metod numerycznych opisanych w Rozdziale 5.4 w pracy [H4]. Ostatecznie, jak już wspomnieliśmy, rozwiązanie problemów optymalizacyjnych, pozwala nie tylko na wyliczenie optymalnej wierności splątania ale także na podanie wyrażeń na optymalne pomiary Alicji, które są elementami algebry $\mathcal{A}'_n(d)$:

$$\forall 1 \leq i \leq N \quad \Pi_i = \Pi \sigma_i \Pi, \quad \text{gdzie} \quad \Pi = \frac{d^N}{\sqrt{N}} \sum_{\alpha} \sum_{\mu \in \alpha} \sqrt{\frac{m_\alpha}{d_\alpha}} \frac{v_\mu}{m_\mu} F_\mu(\alpha), \tag{59}$$

gdzie $F_\mu(\alpha)$ są projektorami z wyrażenia 38 dla $k = 1$. Optymalna operacja O_A z (40) należy do algebry grupowej $\mathcal{A}_n(d)$:

$$O_A = \sqrt{d^N} \sum_{\mu} \frac{v_\mu}{\sqrt{d_\mu m_\mu}} P_\mu. \tag{60}$$

W dwóch powyższych wyrażeniach liczby v_μ są elementami wektora własnego macierzy teleportacji odpowiadającego jej maksymalnej wartości własnej. Na liczby te można podać odpowiednie wyrażenia analityczne dla $d \geq N$ oraz $d = 2$, w innych przypadkach musimy posiłkować się metodami numerycznymi.

W przypadku obu protokołów probabilistycznych kluczową rolę także odgrywają narzędzia wywodzące się z teorii reprezentacji grupy symetrycznej S_N, algebry częściowo transponowanych operatorów permutacji $\mathcal{A}'_n(d)$ oraz metod SDP (ang. *semidefinite programming*). Jednak w przeciwieństwie do deterministycznego protokołu PBT, tutaj w obu przypadkach optymalna forma pomiarów musi być znaleziona – pomiary nie są w postaci *square-root measurements (SRM)*, tak jak w (45), oraz dodatkowo muszą one spełniać zależność (47) aby zapewnić jednostkową wierność w procesie teleportacji. Formułując i rozwiązując analitycznie odpowiednie problemy pierwotne i dualne pokazaliśmy, że ich rozwiązania są takie same dając nam optymalne wartości średniego prawdopodobieństwa sukcesu oraz optymalne postaci pomiarów.

W nieoptymalnym przypadku, gdy obserwatorzy współdzielą N kopii stanu maksymalnie splątanego, optymalna wartość średniego prawdopodobieństwa sukcesu dana jest wyrażeniem

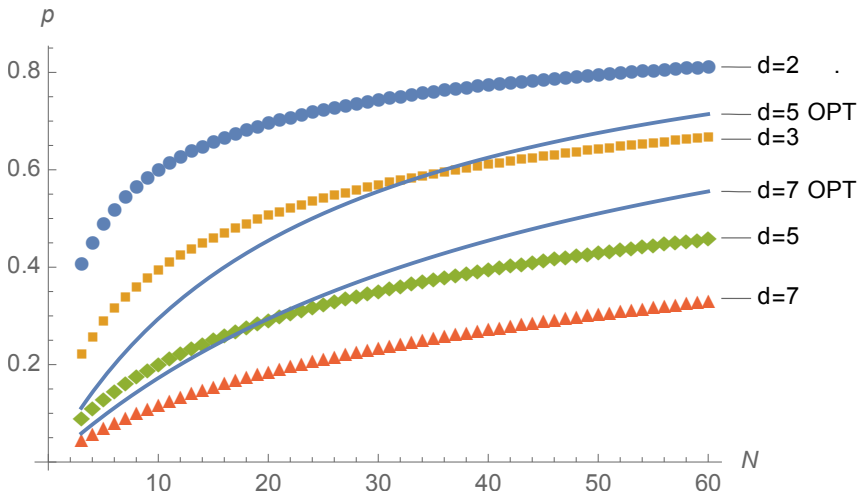
(Twierdzenie 3 w [H3]):

$$p_{succ} = \frac{1}{d^N} \sum_{\alpha} m_\alpha^2 \min_{\mu \in \alpha} \frac{d_\mu}{m_\mu}, \tag{61}$$

gdzie minimalizacja jest przeprowadzana po wszystkich $\mu \vdash N$, które mogą być otrzymane z danego $\alpha \vdash N-1$ poprzez dodanie jednej komórki. Wartości numeryczne średniego prawdopodobieństwa sukcesu p_{succ} z wyrażenia (61) są przedstawione na rysunku 6. Optymalna forma operatorów $\{\Theta_i\}_{i=1}^N$, a co za tym idzie optymalnych pomiarów $\{\Pi_i\}_{i=1}^N$ z (47), jest następująca (Proposition 7 w [H3]):

$$\Pi_i^{AC} = P_{i,n}^{+} \otimes \sum_{\alpha \vdash N-1} \frac{d}{\gamma_{\mu^*}(\alpha)} P_\alpha, \tag{62}$$

gdzie wielkość $\gamma_{\mu^*}(\alpha)$ jest maksymalną wartością własną operatora $d^N\rho$ przy ustalonym α a P_α jest projektorem Younga z (9) działającym na wszystkich układach z wyjątkiem $i-$tego oraz $n-$tego. Pomiar Π_0^{AC} odpowiadający porażce w protokole może zostać otrzymany z warunku normalizacyjnego $\sum_{i=0}^N \Pi_i^{AC} = \mathbf{1}_{AC}$.



Rysunek 6: Linie kropkowane przedstawiają prawdopodobieństwo sukcesu, gdzie Alicja optymalizuje jedynie po pomiarach, a stan zasobu dany jest jako N par maksymalnie splatanych. Linie ciągłe prezentują prawdopodobieństwo sukcesu dla protokołu optymalnego, gdzie Alicja optymalizuje po stanie zasobu i pomiarach. Widzimy, że protokół optymalny daje wyraźnie wyższe prawdopodobieństwo sukcesu dla ustalonego wymiaru d.

W przypadku protokołu optymalnego, gdzie Alicja optymalizuje jednocześnie stan zasobu oraz pomiary, ogólna strategia postępowania jest podobna – jednakże bardziej wymagająca z technicznego punktu widzenia. Aby to sobie unaocznić zachęcam do porównania odpowiednich programów SDP danymi równaniami (24), (25) w [H3]) oraz równaniami (19), (20) w tym samym artykule. Pomimo to, nadal możemy rozwiązać problemy optymalizacyjne analitycznie, nadal mają własność *strong duality* (rozwiązania problemu pierwotnego i dualnego porywają się), przez co nasze rozwiązania na średnie prawdopodobieństwo sukcesu p_{succ} oraz odpowiednie pomiary $\{\Pi_i\}_{i=1}^N$ są optymalne (Twierdzenie 8 w [H3]):

$$p_{succ} = 1 - \frac{d^2-1}{N+d^2-1}, \qquad \Pi_i^{AC} = P_{i,n}^{+} \otimes \frac{d^{N+1}}{N \sum_{\nu \vdash N} m_\nu^2} \sum_{\alpha \vdash N-1} \frac{m_\alpha}{d_\alpha} P_\alpha. \tag{63}$$

Numeryczne wartości dla średniego prawdopodobieństwa sukcesu p_{succ} w tym przypadku są przedstawione na rysunku 6 – widzimy wyraźną przewagę schematu optymalnego nad nieoptymalnym. Tym razem wyrażenie na optymalne średnie prawdopodobieństwo sukcesu

p_{succ} zależy tylko od parametrów globalnych opisujących protokół, takich jak liczba portów N czy ich wymiar d. Z powyższego wyrażania bezpośrednio odczytujemy asymptotyczne zachowanie się rozważanego protokołu. Na przykład dla $d = 2$ widzimy, że $p_{succ} = 1 - \mathcal{O}(1/N)$, co reprodukuje rezultat z [E85], natomiast dla $d > 2$ otrzymujemy całkowicie nowe wyniki i analizę. Ważne jest, aby podkreślić tutaj, że tak zwarte wyrażenie na p_{succ} z (63) było możliwe do uzyskania dzięki udowodnieniu czysto teoriogrupowych technicznych lematów znajdujących się w dodatku E artykułu [H3].

5.6.2 Struktura pomiarów i stanów sygnałowych w protokole teleportacji kwantowej port-based

Jak wspomnieliśmy wcześniej, stany sygnałowe oraz pomiary należą do algebry $\mathcal{A}'_n(d)$. Oznacza to, że możemy stosować rozwinięty przez nas zestaw narzędzi matematycznych do ich szczegółowego opisu. Na osobną uwagę zasługują rezultaty zawarte w artykułach [H2] and [H9], które pozwoliły na analizę protokołu recyklingu dla PBT omówionego w następnej sekcji. Omówimy tutaj rezultaty ściśle związane z tytułem rozdziału, rozważania czysto teoretyczno-reprezentacyjne zostały podsumowane w Rozdziale 5.5.1.

Zacznijmy od podsumowania rezultatów zawartych w pracy [H2]. Głównym osiągnięciem było podanie analitycznych wyrażeń na wektory własne operatorów $V'_{(a,n)}$, gdzie $1 \leq a \leq n-1$ – zostało to pokazane w Proposition 54. Operatory te to nieunormowane stany sygnałowe σ_a z równania (42). Używając tych wyników byliśmy z kolei wstanie pokazać, że wierność splątania F z równania (54) zmierza do 1, gdy $N \to \infty$ dla każdego $d \geq 2$. Rezultat ten jest zawarty w twierdzeniu 52, w którym także jako wynik dodatkowy otrzymaliśmy ograniczenie dolne na F, które zależy jedynie od parametrów globalnych, którymi są liczba portów N oraz wymiar portu d:

$$F \geq \frac{N}{d^2 + N - 1}. \tag{64}$$

Odzyskaliśmy w ten sposób wynik z pracy Köning'a oraz Beigi [E88], ale uzyskaliśmy go poprzez zastosowanie całkowicie innych, czysto teoriogrupowych narzędzi, bez żadnego odwoływania się do problemu dyskryminacji stanów kwantowych.

W artykule [H9] zajeliśmy się dalszą analizą pomiarów $\{\Pi_i\}_{i=1}^N$ z równania (45). W pierwszej kolejności, w Proposition 4, przy użyciu Lematu 35 z pracy [H2], wyliczyliśmy nieredukowalne elementy macierzowe operatorów $V'_{(a,n)}$. Rezultat ten pozwolił nam na wyprowadzenie reguł składania dla dwóch dowolnych pomiarów, co zostało sformułowane w Proposition 5 i pozwoliło na bardzo ciekawe wnioski. Mianowicie, jeżeli tylko lokalny wymiar przestrzeni jest odpowiednio duży, tzn. gdy $h(\alpha) < d$, gdzie α numeruje irrepy grupy symetrycznej S_{N-1}, to rozważane POVMy są pomiarami projektywnymi – spełniają następującą regułę składania $\Pi_i \Pi_j = \delta_{ij} \Pi_i$. We wszystkich innych przypadkach rozważane POVMy są są pseudoprojektorami na każdym z irrepów algebry $\mathcal{A}'_n(d)$ z różną stałą. Posiadając te rezultaty mogliśmy rozwiązać jeden z naszych głównych problemów, którym było wyliczenie nieredukowalnych elementów macierzowych pierwiastka kwadratowego dowolnego POVMa (Proposition 6), wraz z jego śladem z operatorem $V'_{(a,n)}$ (Twierdzenie 8). Rezultaty te są bardzo techniczne, dlatego też nie będziemy ich bezpośrednio przywoływać w tym podsumowaniu. Czytelnika odsyłamy do rozdziału IV w pracy [H9] w celu zapoznania się ze szczegółami technicznymi. Tutaj, ze względu na koherentność prezentacji przywołamy jedynie ostateczny rezultat dotyczący obliczenia wyżej wspomnianego śladu (Twierdzenie 8 w [H9]):

$$\begin{aligned} \mathrm{Tr}\left(\sqrt{\Pi_a} V'_{(a,n)}\right) = &\sum_{\alpha: h(\alpha) < d} \frac{1}{n-1} \left(\sum_{\nu \in \alpha} \sqrt{m_\nu d_\nu} \right)^2 + \\ &+ \sum_{\alpha: h(\alpha) = d} \frac{1}{\sqrt{(n-1)d_\alpha - d_\theta}} \frac{\sqrt{d_\alpha}}{\sqrt{(n-1)}} \left(\sum_{\nu \neq \theta} \sqrt{m_\nu d_\nu} \right)^2, \end{aligned} \tag{65}$$

gdzie $n = N + 1$. Widzimy, że ostateczny wynik zależy jedynie od parametrów teoriogrupowych, takich jak krotności oraz wymiary irrepów grupy symetrycznej S_N oraz S_{N-1} w dualizmie Schura-Weyla oraz nie zależy od wyboru indeksu $1 \leq a \leq N$. Symbolem d_θ oznaczamy wymiary irrepów grupy S_N, które nie pojawiają się w rozkładzie, gdy wymiar portu jest zbyt mały. Pisząc bardziej formalnie, nieredukowalne reprezentacje θ należą do następującego zbioru:

$$\Theta := \{\theta \vdash N \mid \theta \in \alpha \vdash N-1 \text{ with } h(\alpha) = d \text{ and } h(\theta) = d+1\}. \tag{66}$$

Gdy rozważymy nieredukowalne reprezentacje grupy S_{N-1}, dla których $h(\alpha) < d$ to zbiór Θ jest pusty. Dodatkowo podaliśmy zwarte wyrażenia na wszystkie opisane tutaj wielkości w przypadku kubitowym, które zależą jedynie od ilości portów N (Lemat 9). Było to możliwe, ponieważ w tym przypadku wszystkie diagramy Younga numerujące odpowiednie irrepy mogą mieć co najwyżej dwa wiersze.

5.6.3 Recykling stanu zasobu w deterministycznym protokole teleportacji kwantowej port-based

Z rozdziału 5.6.1 wiemy, że niezależnie od wybranej wersji protokołu PBT, nadawca i odbiorca, aby uzyskać zadowalającą efektywność protokołu, mierzoną wiernością splątania (dPBT) czy prawdopodobieństwem sukcesu (pPBT), muszą użyć znacznej ilości portów N. To z kolei rodzi pytanie jak bardzo protokoły typu PBT, w każdym możliwym wariancie, są kosztowne w terminach ilości maksymalnie splątanych par, które muszą zostać przygotowane przed wykonaniem protokołu. Jeżeli stan zasobu po jednej turze teleportacji jest bardzo mocno zaburzony, to może okazać się, że nie jest już przydatnym zasobem dla PBT. To z kolei prowadzi do wniosku, że nawet po jednej turze teleportacji należy przygotować i rozpropagować nowy stan zasobu – jest to oczywiście poważne praktyczne ograniczenie. Okazuje się, że sytuacja nie jest aż tak niekorzystna – w artykule [E103] autorzy pokazują, że istnieje wariant protokołu PBT nazywany protokołem recyklingu dla PBT, w którym strony mogą ponownie użyć stanu zasobu pozostałym po wcześniejszej turze teleportacji, cały czas uzyskując asymptotycznie idealną teleportację. Protokół recyklingu w każdym wariancie PBT może być podsumowany następująco:

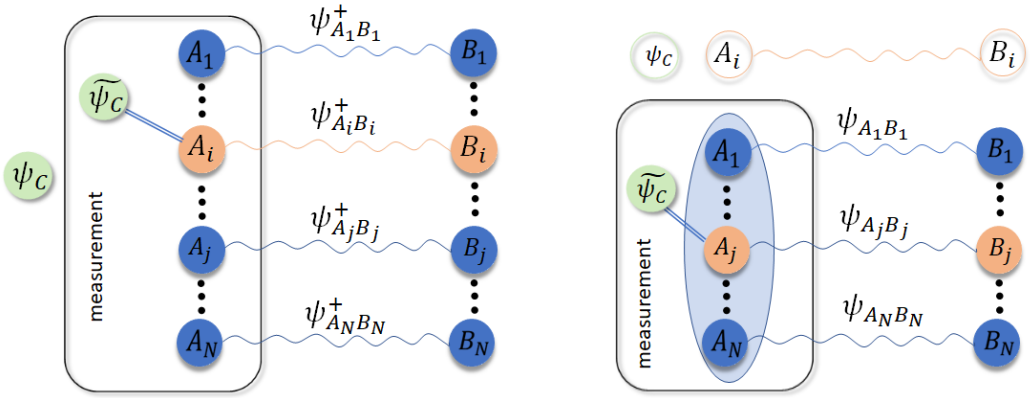
1. Alicja przeprowadza pomiar $\{\Pi_i^{AC}\}_{i=1}^N$, otrzymując wynik $1 \leq i \leq N$.
2. Alicja wysyła kanałem klasycznym wynik i do Boba.
3. Strony stosują permutację (SWAP) pomiędzy $i-$tym, a pierwszym portem.
4. Strony nie używają pierwszego portu w następnej turze protokołu teleportacji – używają tylko pozostałych $N-1$ portów.
5. Strony powtarzają kroki 1-4 używając pozostałych portów, aż dokonają teleportacji k stanów.

Jak to zostało wyjaśnione w pracy [E103], protokół recyklingu $\mathcal{P}_{rec}(N,2,k)$ jest rzeczywiście wydajny jeśli wierność $F(\mathcal{P}_{rec}(N,2,1))$ pomiędzy stanami zasobu w przypadku sytuacji wyidealizowanej, gdy stan zostaje teleportowany, a pozostałe porty nie doznały uszczerbku, oraz pomiędzy prawdziwym stanem zasobu po teleportacji, jest odpowiednio duża. W przypadku kubitowym dla dPBT autorzy pracy [E103] udowodnili następujące ograniczenie dolne:

$$F(\mathcal{P}_{rec}(N,2,1)) \geq 1 - \frac{11}{4N} + \mathcal{O}\left(\frac{1}{N^2}\right). \tag{67}$$

Następnie mając już ograniczenie dolne na $F(\mathcal{P}_{rec}(N,2,1))$ po jednej turze teleportacji, byliśmy w stanie wyprowadzić analogiczne ograniczenie po k rundach protokołu (Lemma 2 w [E103]):

$$F(\mathcal{P}_{rec}(N,2,k)) \geq 1 - \frac{11k}{2N}. \tag{68}$$



Rysunek 7: Schematyczne przedstawienie protokołu recyklingu dla teleportacji dwóch nieznanych stanów kwantowych $\psi_C, \widetilde{\psi}_C$. Po lewej widzimy zwykły protokół PBT, gdzie transmisja odbyła się z wykorzystaniem $i-$tego portu. Po przesyle, strony pozostają z $N-1$ portami, ponieważ port $\psi^+_{A_iB_i}$ został zużyty do teleportacji stanu ψ_C – rysunek prawy. Po pomiarze w pierwszej turze, każdy z portów nie jest już w postaci stanu maksymalnie splątanego i pomiędzy portami występują już pewne korelacje (jasnoniebieska elipsa). W drugiej rundzie strony chcą przesyłać stan $\widetilde{\psi}_C$, do czego muszą wykorzystać zaburzony stan zasobu.

Widzimy, że błąd w każdej turze teleportacji jest co najwyżej addytywny w ilości rund k. Wyniki te mówią, że po każdej turze teleportacji Alicja może używać optymalnych pomiarów square-root otrzymując wysoką wydajność przy ponownym użyciu pozostałych portów.

W artykule [H9] skupiliśmy się na rozszerzeniu rezultatów dotyczących protokołu recyklingu dla deterministycznego PBT (dPBT) poza przypadek kubitowy oraz jako pierwsi analizujemy recykling dla optymalnego protokołu dPBT. Co więcej podajemy jawne wyrażenia na $F(\mathcal{P}_{rec}(N,d,1))$ w każdym z dwóch dyskutowanych wariantów dPBT. Omówmy teraz pokrótce nasze rezultaty.

Pierwszym i zasadniczym krokiem w kierunku uzyskania wyników końcowych była analiza wewnętrznej struktury obiektów opisujących protokół recyklingu z punktu widzenia teorii reprezentacji. Jak to napisaliśmy w Rozdziale 5.6.1, rozważane pomiary należą do algebry $\mathcal{A}'_d(n)$ i narzędzia wypracowane w artykułach [H3, H2] mogą być tutaj użyte w sposób efektywny. W pracy tej, udowodniliśmy szereg lematów, wśród nich najważniejszymi są: prawo składania pomiarów, wyliczenie elementów macierzowych pomiarów na nieprzywiedlnych reprezentacjach i finalnie obliczenie pierwiastka kwadratowego z rozważanych pomiarów w dPBT wraz z odpowiednimi śladami. Wyniki te zostały omówione w poprzednim rozdziale niniejszego autoreferatu.

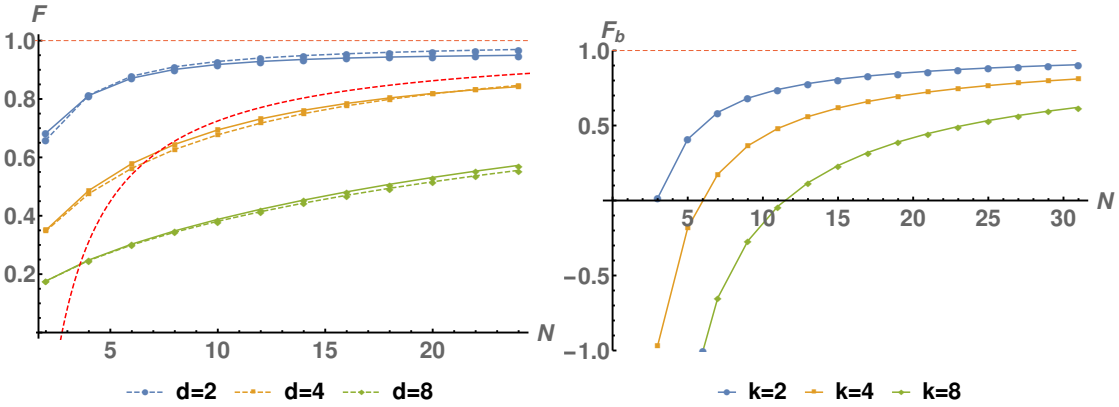
Wykorzystując wspomniane rezultaty techniczne wyliczyliśmy jawne wyrażenie na wielkość $F(\mathcal{P}_{rec}(N,d,1))$, w przypadku nieoptymalnego oraz optymalnego dPBT dla dowolnego wymiaru $d \geq 2$. W przypadku nieoptymalnego protokołu dPBT mamy (Twierdzenie 12 [H9]):

$$F(\mathcal{P}_{rec}(N,d,1)) = \frac{\sqrt{N}}{d^{N+1}} \left[\sum_{\alpha: h(\alpha)<d} \frac{1}{N} \left(\sum_{\nu\in\alpha} \sqrt{m_\nu d_\nu} \right)^2 + \sum_{\alpha: h(\alpha)=d} \frac{1}{\sqrt{N d_\alpha - d_\theta}} \frac{\sqrt{d_\alpha}}{\sqrt{N}} \left(\sum_{\nu\neq\theta} \sqrt{m_\nu d_\nu} \right)^2 \right], \tag{69}$$

gdy dla przypadku optymalnego dPBT zachodzi (twierdzenie 14 [H9]):

$$F(\mathcal{P}_{rec}(N,d,1)) = \frac{1}{d^{1/2}} \sum_{\alpha\vdash N-1} \sum_{\mu\in\alpha} \frac{v_\alpha v_\mu}{m_\alpha^{1/2}} \frac{\sum_{\substack{\nu\neq\theta \\ \nu\in\alpha}} \sqrt{m_\nu d_\nu}}{\sqrt{N d_\alpha - d_\theta}}. \tag{70}$$

Liczby v_μ, v_{nu} są elementami wektora własnego odpowiadającego maksymalnej wartości własnej macierzy teleportacji omówionej pokrótce w Rozdziale 5.6.1 oraz szczegółowo w pracy [H4].



Rysunek 8: Lewy rysunek przedstawia wartości wierności $F(P_{rec}(N,d,1))$ obliczone dla nieoptymalnego (linie przerywane) oraz optymalnego (linie ciągłe) dPBT. Z wykresu wnioskujemy, że stan zasobu dla optymalnego dPBT nie jest koniecznie lepszy dla protokołu recyklingu niż stan zasobu dla odpowiednika nieoptymalnego. W szczególności dla $d = 2$ wartości $F(P_{rec}(N,2,1))$ dla optymalnej wersji są nawet niższe niż dla przypadku nieoptymalnego. Przerywana linia czerwona przedstawia ograniczenie dolne dane równaniem (67) z dokładnością do wyrazów rzędu $\mathcal{O}(1/N^2)$. Prawy rysunek przedstawia ograniczenie dolne na $F(P_{rec}(N,2,k))$ (przypadek kubitowy) dla różnej liczby tur teleportacji k. Z rysunku widzimy, że $F(P_{rec}(N,2,k))$ przyjmuje relatywnie wysokie wartości nawet dla niezbyt dużej liczby portów.

Parametry teoriogrupowe były obliczane numerycznie z wykorzystaniem pakietu SAGE [E101]. W szczególności dla $d = 2$ podaliśmy łatwo obliczalne wyrażenia, które zależą jedynie od liczby portów N i nie ma potrzeby do odwoływania się do specjalistycznego oprogramowania – Lemat 13 oraz Lemat 14 w pracy [H9]. Mając wyrażenia na $F(\mathcal{P}_{rec}(N,d,1))$ w obu wariantach dPBT, mogliśmy podać ograniczenie dolne na wielkość $F(\mathcal{P}_{rec}(N,d,k))$ po k turach teleportacji:

$$F(P_{rec}(N,d,k)) \geq 1 - 2k(1 - F(P_{rec}(N,d,1))), \tag{71}$$

które oczywiście zbiega do 1, gdy $F(P_{rec}(N,d,1)) \to 1$. Nasze wyniki analityczne podsumowuję na Rysunku 8 zaczerpniętym z pracy [H9]. Ostatecznie z naszych rezultatów wnioskujemy, że nie ma zależności pomiędzy typem protokołu dPBT (tym samym stanem zasobu), a wartością $F(P_{rec}(N,d,1))$. Mówiąc dokładniej, widzimy że wierność splątania $F(|\Psi^+\rangle_{AB}, |\Psi\rangle_{AB})$ pomiędzy stanem zasobu dla protokołu nieoptymalnego i optymalnego maleje gdy zwiększamy ilość portów N (Lemat 16 w [H9]), a wartości $F(P_{rec}(N,d,1))$ nie różnią się mocno od siebie.

5.7 Teleportacja dużej ilości kwantowej informacji: protokoły teleportacji kwantowej multiport-based

W dyskutowanych powyżej rozdziałach dotyczących protokołu port-based teleportation, rozważaliśmy transmisje pojedynczego stanu kwantowego przy użyciu N portów, każdy o wymiarze d. Naturalne staje się zatem pytanie w jaki sposób efektywnie przesyłać stan układu złożonego lub wiele oddzielnych stanów kwantowych za pomocą różnych wariantów protokołów PBT - a więc dużej ilości kwantowej informacji. Możemy wyobrazić sobie następujące scenariusze:

1. Zastosowanie PBT do każdego układu z osobna. Wadą tego podejścia jest angażowanie znacznej ilości oddzielnych stanów zasobów oraz pomiarów – każdy stan zasobu i zbiór pomiarów dla pojedynczego układu. Jednak naszym celem jest praca z zasobem o ustalonej liczbie portów N, bez możliwości posiadania nowego, oddzielnego stanu zasobu dla obydwu stron. Z tego powodu ten wariant nie będzie dla nas interesujący.

2. Zastosowanie protokołu recyklingu dla deterministycznego PBT [E103] [H9]. Zgodnie z tym jak to zostało opisane w Rozdziale 5.6.3, w protokole tym strony ponownie używają stanu zasobu do następnych tur teleportacji, w każdej kolejnej mając do dyspozycji zaburzony stan zasobu z jednym portem mniej. Rezultaty dla tego protokołu zostały wypracowane dość niedawno, dla deterministycznego przypadku (nie-)optymalnego, bez jawnych wyrażeń na wierność kanału teleportującego. W szczególności, obecnie nie jest znana analiza protokołu recyklingu dla wariantu probabilistycznego. Dodatkowo, w każdym kroku konieczne jest zastosowanie nowego zestawu pomiarów, zatem również nie jest to przypadek interesujący.

3. Zastosowanie PBT z odpowiednio dużym wymiarem portu, równym $d = D^k$, gdzie k to liczba teleportowanych układów, a D ich lokalny wymiar. Scenariusz taki nie jest efektywny, ponieważ wierność oraz średnie prawdopodobieństwo sukcesu drastycznie spadają, gdy wymiar portu rośnie. Powoduje to, że musimy użyć znacznej ilości współdzielonych par splątanych w stanie zasobu, co zilustrowaliśmy w Tabeli 1.

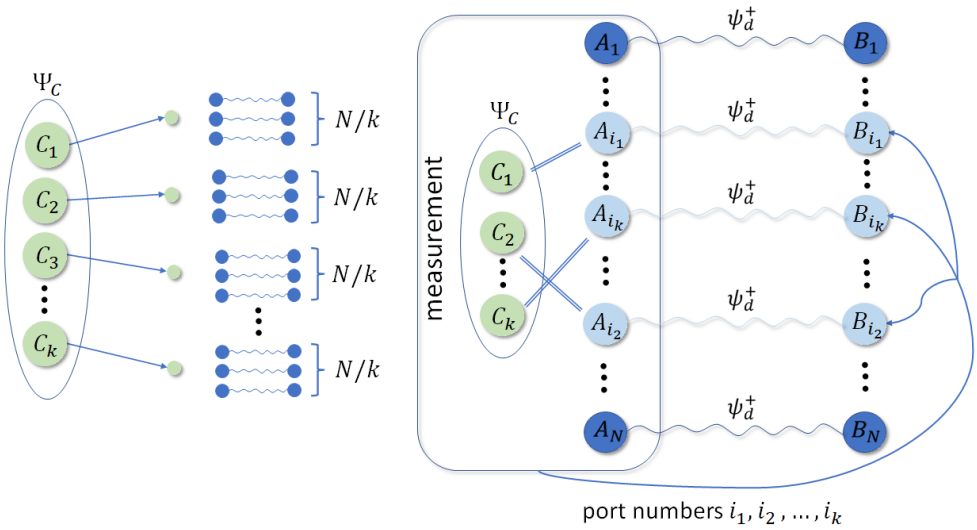
Protokół teleportacji	**Wierność splątania** F
Nieoptymalny dPBT	$F = 1 - \frac{d^2-1}{4N} + O\left(N^{-3/2+\delta}\right)$
Optymalny dPBT	$F \geq 1 - \frac{d^5+O\left(d^{9/2}\right)}{4\sqrt{2}N^2} + O\left(N^{-3}\right)$
Protokół teleportacji	**Średnie prawdopodobieństwo sukcesu** p_{succ}
Nieoptymalny pPBT	$p_{succ} = 1 - \sqrt{\frac{d}{N-1}}\mathbb{E}[\lambda_{\max}(\mathbf{G})] + o\left(N^{-1/2}\right)$
Optymalny pPBT	$p_{succ} = 1 - \frac{d^2-1}{d^2-1+N}$

Tablica 1: Asymptotyczne zachowanie protokołu dPBT oraz pPBT dla dowolnego wymiaru portu d i liczby portów N. Wszystkie rezultaty zostały zaczerpnięte z [E95] oraz [H3].

4. Zastosowanie upakowanego PBT (*ang. packaged PBT*), gdzie N portów dzielimy na k grup, po czym na każdej z tych grup (każdy z pakietów składa się z N/k portów) przeprowadzamy protokół teleportacji PBT, tak jak ma to miejsce na rysunku 9. Całkowita wierność splątania $F_{pack}(N,k)$ jest równa iloczynowi wierności splątania $F(N/k,1)$ dla każdego z pakietów z osobna, zatem $F_{pack}(N,k) := F(N/k,1)^k$. Protokół ten został po raz pierwszy zaproponowany w pracy [E103], a następnie rozwinięty w artykule [H7].

5. Zastosowanie wieloportowego protokołu PBT (*ang. multi port-based teleportation (MPBT)*). Istnienie takiego protokołu zostało zasugerowane dla nieoptymalnego protokołu deterministycznego w pracy [E103], jednakże jego rygorystyczny opis wraz z analizą wydajności nie był znany, aż do pojawienia się prac [H10, H8, H7]. W podstawowej wersji protokołu nadawca wraz z odbiorcą współdzielą N par maksymalnie splątanych, ale tym razem ich zadaniem jest transmisja złożonego stanu $k-$cząstkowego $\Psi_C = \Psi_{C_1C_2\cdots C_k}$, bądź po prostu k niezależnych stanów $\Psi_C = \psi_{C_1} \otimes \psi_{C_2} \otimes \cdots \otimes \psi_{C_k}$ (rysunek 9). Aby tego dokonać nadawca wykonuje łączny pomiar na stanie Ψ_C oraz części swojego stanu zasobu otrzymując wynik w formie multi-indeksu $\mathbf{i} = \{i_1, i_2, \ldots, i_k\}$, który jest przesyłany kanałem klasycznym do odbiorcy. Bob chcąc odzyskać teleportowany stan musi jedynie wybrać k portów w porządku wskazanym przez $\mathbf{i}$. Warto zauważyć, że w tym przypadku Alicja musi dysponować $k!\binom{N}{k}$ pomiarami, zatem tyle też mamy możliwych indeksów $\mathbf{i}$. Jedynie w przypadku probabilistycznym dochodzi jeden dodatkowy indeks odpowiadający pomiarowi związanemu z porażką procesu teleportacji. Oznaczamy zbiór wszystkich możliwych wartości indeksu $\mathbf{i}$ jako $\mathcal{I}$.

Jak podkreśliliśmy powyżej, ze względu na brak narzędzi technicznych, brakowało analizy wydajności protokołu MPBT, jego uogólnienia na optymalny przypadek deterministyczny, jak



Rysunek 9: Lewy rysunek przedstawia konfigurację dla protokołu upakowanego PBT składającego się z k pakietów, każdy zawierający N/k portów. Prawy rysunek przedstawia schematyczny opis protokołu teleportacji multi-port based (MPBT) składającego się z N portów. W obu przypadkach strony chcą teleportować nieznany $k-$cząstkowy stan kwantowy Ψ_C z jak największą możliwą wydajnością.

również sformułowania jego probabilistycznego odpowiednika. W pełni odnieśliśmy się do tych kwestii w serii artykułów [H7, H10, H8], które podsumuję w kolejnych dwóch rozdziałach.

Opis protokołów MPBT w ujęciu teorio-reprezentacyjnym Tak jak to miało miejsce w przypadku protokołu PBT opisanego w rozdziale 5.6.1, naszym celem było opisanie deterministycznego i probabilistycznego protokołu MPBT w (nie-)optymalnej wersji poprzez podanie ich wydajności oraz optymalnych pomiarów i stanów zasobu. Zostało to zrobione w dwóch artykułach [H10, H8]. Ogólna idea opisu stojąca za protokołami MPBT jest podobna do tej wykorzystanej do opisu zwykłego PBT, gdy $k = 1$. Jednakże z technicznego punktu widzenia problem ich opisu jest dużo bardziej złożony, ponieważ wymaga narzędzi wywodzących się z teorii reprezentacji algebry częściowo transponowanych operatorów permutacji dla więcej niż jednej częściowej transpozycji $\mathcal{A}_n^{(k)}(d)$ – zostało to podsumowane w Rozdziale 5.5.1. Dlaczego potrzebujemy reprezentacji tego typu, bardzo łatwo zauważyć rozważając symetrie wykazywane przez obiekty opisujące protokoły MPBT. Mianowicie, wszystkie stany sygnałowe $\{\sigma_{\mathbf{i}}^{AB}\}_{\mathbf{i}\in\mathcal{I}}$ spełniają następujące relacje komutacyjne:

$$\begin{aligned} \left[U^{\otimes(n-k)} \otimes \overline{U}^{\otimes k}, \sigma_{\mathbf{i}}^{AB}\right] &= 0, \qquad \forall\, U \in \mathcal{U}(d), \\ \left[V(\pi), \sigma_{\mathbf{i}}^{AB}\right] &= 0, \qquad \forall\, \pi \in S_{n-2k}, \end{aligned} \tag{72}$$

oraz są one kowariantne względem działania grupy symetrycznej S_{n-k}:

$$V(\pi)\sigma_{\mathbf{i}}^{AB}V^\dagger(\pi) = \sigma_{\pi(\mathbf{i})}^{AB}, \qquad \forall\, \pi \in S_{n-k}. \tag{73}$$

Takie same typy symetrii wykazują także odpowiednie pomiary $\{\Pi_{\mathbf{i}}^{AB}\}_{\mathbf{i}\in\mathcal{I}}$ stosowane przez Alicję. Z definicji zbioru $\mathcal{I}$ widzimy, że dla $k = 1$, powyższe relacje redukują się do tych opisanych w rozdziale 5.6.1. Mając rozwinięte niezbędne narzędzia reprezentacyjno-teoretyczne, głownie w artykule [H10], mogliśmy napisać odpowiednie problemy optymalizacyjne SDP w algebrze $\mathcal{A}_n^{(k)}(d)$ i rozwiązać je analitycznie. Rozwiązania problemów pierwotnego i dualnego pokrywają się, dając nam optymalne wartości wierności splątania, średniego prawdopodobieństwa sukcesu, a także optymalną formę pomiarów.

W nieoptymalnym deterministycznym przypadku Alicja wybiera tzw. square-root measurements postaci

$$\forall\ \mathbf{i} \in \mathcal{I} \qquad \Pi_{\mathbf{i}}^{AC} = \frac{1}{\sqrt{\rho}} \sigma_{\mathbf{i}}^{AC} \frac{1}{\sqrt{\rho}} + \Delta, \qquad \rho = \sum_{\mathbf{i}\in\mathcal{I}} \sigma_{\mathbf{i}}^{AC}, \tag{74}$$

gdzie Δ jest dodatkowym członem zapewniającym sumowanie się pomiarów do identyczności na całej przestrzeni $(\mathbb{C}^d)^{\otimes n}$. Widzimy, że główną techniczną przeszkodą jest obliczenie odwrotności operatora $\rho = \sum_{\mathbf{i}} \sigma_{\mathbf{i}}$. Jednakże wykorzystując omówione symetrie możemy udowodnić następujący rozkład spektralny ρ (twierdzenie 17 w [H10]):

$$\rho = \sum_{\alpha\vdash N-k} \sum_{\substack{\mu\vdash N \\ \mu\in\alpha}} \lambda_\mu(\alpha) F_\mu(\alpha), \qquad \lambda_\mu(\alpha) = \frac{k!\binom{N}{k}}{d^N} \frac{m_\mu}{m_\alpha} \frac{d_\alpha}{d_\mu}, \tag{75}$$

gdzie $F_\mu(\alpha)$ są projektorami własnymi z wyrażenia (38). Tym razem diagramy Younga μ zbudowane z N komórek są otrzymane z diagramów Younga α, zbudowane z $N-k$ komórek poprzez dodanie kolejno k komórek. Mając powyższe, dowodzimy Twierdzenie 22 z pracy [H10] dając w tym przypadku teorio-grupowe wyrażenie na wierność splątania

$$F = \frac{1}{d^{N+2k}} \sum_{\alpha\vdash N-k} \left(\sum_{\mu\in\alpha} m_{\mu/\alpha} \sqrt{m_\mu d_\mu} \right)^2, \tag{76}$$

gdzie $m_{\mu/\alpha}$ oznacza ilość możliwych sposobów otrzymania μ z α poprzez dodanie k komórek. W szczególnym przypadku $k = 1$ zawsze mamy $m_{\mu/\alpha} = 1$, co powoduje, że powyższe wyrażenie redukuje się do wierności splątania z nieoptymalnego dPBT danej wzorem (53). Wielkość ta może zostać obliczona numerycznie z użyciem naszego oprogramowania, a w przypadku kubitowym znane są zwarte wyrażenia analityczne [E104, E105]. Na rysunku 10 przedstawiamy numeryczne wartości wierności splątania dla dyskutowanego protokołu porównane ze zwykłym protokołem PBT dyskutowanym w rozdziale 5.6.1, ale z odpowiednio większym wymiarem portu. Widzimy, że protokół MPBT jest wyraźnie lepszy, nawet od optymalnego PBT. Dla nieoptymalnego probabilistycznego protokołu badanego w [H10], do zapewnienia jednostkowej wierności splątania musimy zażądać, aby pomiary spełniały relację analogiczną do tej z równania (47) dla standardowego PBT:

$$\forall \mathbf{i} \in \mathcal{I} \qquad \Pi_{\mathbf{i}}^{AC} = P^+_{A_{\mathbf{i}}C} \otimes \Theta_{\overline{A}_{\mathbf{i}}}, \tag{77}$$

gdzie postać $\{\Theta_{\overline{A}_{\mathbf{i}}}\}_{\mathbf{i}\in\mathcal{I}}$ jest wyliczona z odpowiednich SDP (szara ramka na stronie 7 w [H10]). Rozwiązanie dla tych problemów SDP razem z wyrażeniami na średnie prawdopodobieństwo sukcesu jest zawarte w Twierdzeniu 23 w [H10]. Pomiary są elementami algebry $\mathcal{A}_n^{(k)}(d)$ z (18):

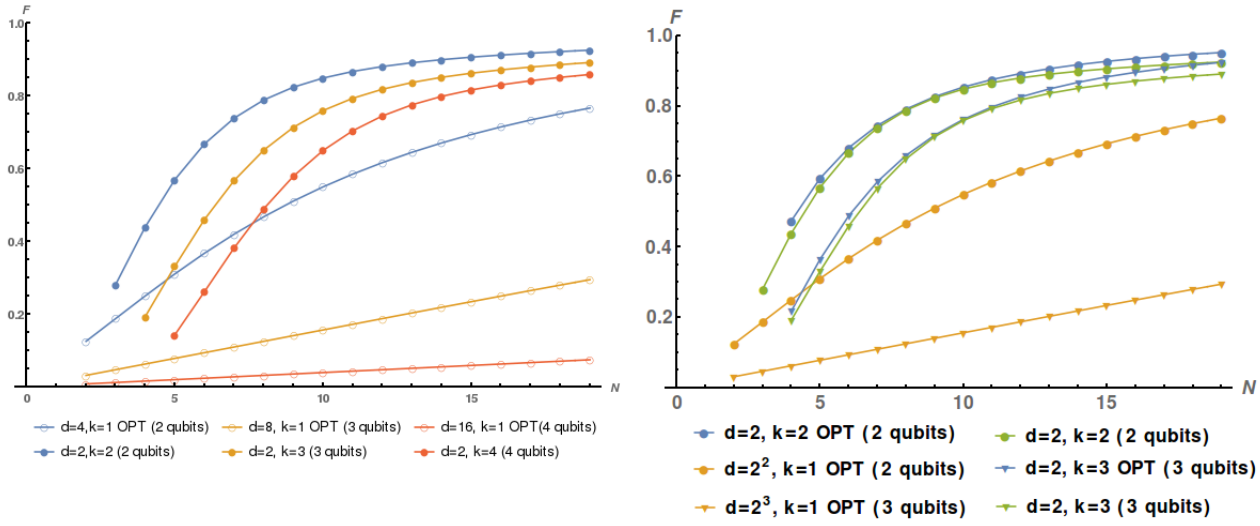
$$\forall\ \mathbf{i} \in \mathcal{I} \qquad \Pi_{\mathbf{i}}^{AC} = \frac{k!\binom{N}{k}}{d^{2N}} P^+_{A_{\mathbf{i}}C} \otimes \sum_{\alpha\vdash N-k} P_\alpha \min_{\mu\in\alpha} \frac{1}{\lambda_\mu(\alpha)}, \tag{78}$$

a średnie prawdopodobieństwo sukcesu jest postaci:

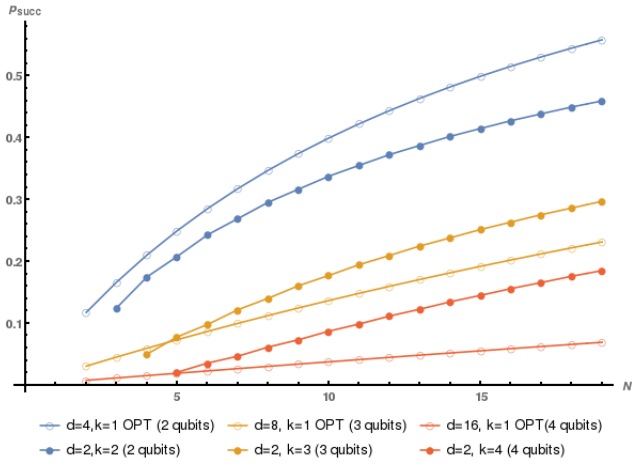
$$p_{succ} = \frac{k!\binom{N}{k}}{d^{2N}} \sum_{\alpha\vdash N-k} \min_{\mu\in\alpha} \frac{m_\alpha d_\alpha}{\lambda_\mu(\alpha)}, \tag{79}$$

gdzie minimalizacja jest przeprowadzona względem wszystkich diagramów Younga μ, które mogą zostać otrzymane z danego diagramu Younga α o $N-k$ komórkach, poprzez dodanie k kolejnych komórek. Numeryczne wartości p_{succ} porównane ze standardowym optymalnym probabilistycznym PBT są przedstawione na Rysunku 11.

Optymalny deterministyczny i probabilistyczny przypadek był badany głownie w artykule [H8]. Rozwiązując analitycznie problem pierwotny i dualny doszliśmy do wniosku, że



Rysunek 10: Lewy wykres przedstawia wydajność nieoptymalnego deterministycznego protokołu MPBT mierzoną wiernością splątania F dla różnych wyborów początkowych parametrów, takich jak lokalny wymiar d, liczba portów N oraz ilość teleportowanych stanów k. Osiągamy wyższą wydajność niż standardowe optymalne PBT (OPT) z odpowiednio dużym wymiarem portu już przy teleportacji stanu dwóch kubitów ($d = 2, k = 2$). Na prawym wykresie przedstawiamy porównanie optymalnego deterministycznego protokołu MPBT ($k > 1$, OPT) z jego nieoptymalną wersją. W każdym przypadku protokół optymalny wykazuje wyższą wydajność. Dodatkowo do zilustrowania skoku efektywności na wykres nanieśliśmy wierność splątania dla standardowego optymalnego PBT ($k = 1$).



Rysunek 11: Wykres przedstawia wydajność probabilistycznej wersji nieoptymalnego protokołu MPBT, mierzoną za pomocą średniego prawdopodobieństwa sukcesu p_{succ}, dla różnych wartości parametrów początkowych, takich jak lokalny wymiar d, liczba portów N oraz ilość teleportowanych stanów k. Widzimy, że zaczynamy uzyskiwać wyższe wartości od odpowiedniego optymalnego protokołu PBT z odpowiednio dużym wymiarem portu dla stanu trzech kubitów ($d = 2, k = 3$).

optymalna wierność splątania jest opisana *uogólnioną macierzą teleportacji* $M_F^{d,k}$. Macierz ta została wprowadzona w Definicji 6 w [H8] i dyskutowana w Rozdziale 6.2 tego samego artykułu. Zgodnie z Twierdzeniem 7 z pracy [H8] mamy następujące wyrażenie na wierność splątania.

$$F = \frac{1}{d^{2k}} \lambda_{\max}(M_F^{d,k}), \tag{80}$$

gdzie k to ilość teleportowanych układów, a $\lambda_{\max}(M_F^{d,k})$ jest maksymalną wartością własną uogólnionej macierzy teleportacji $M_F^{d,k}$. Ostatecznie, w Twierdzeniu 8 podajemy formę opty-

malnych pomiarów wykonywanych przez Alicję

$$\Pi_{\mathbf{i}} = \Pi\sigma_{\mathbf{i}}\Pi \quad \text{with} \quad \Pi = \sum_{\alpha\vdash N-k}\sum_{\mu\in\alpha}\frac{d_\mu}{\sqrt{k!\binom{N}{k}}}\sqrt{\frac{m_\alpha}{d_\alpha}}\frac{v_\mu}{m_\mu}F_\mu(\alpha), \tag{81}$$

gdzie $F_\mu(\alpha)$ jest projektorem własnym danym równaniem (38). Widzimy zatem, że pomiary należą do algebry $\mathcal{A}_n^{(k)}(d)$ z równania (18), podczas gdy operacja optymalizująca O_A jest elementem algebry grupowej $\mathcal{A}_n(d)$ z (2):

$$O_A = \sqrt{d^N}\sum_\mu \frac{v_\mu}{d_\mu m_\mu}P_\mu, \tag{82}$$

gdzie P_μ oznacza projektor Younga na nieprzywiedlne reprezentacje grupy S_N numerowane poprzez $\mu \vdash N$. W dwóch powyższych wyrażeniach liczby v_μ są elementami wektora własnego odpowiadającego maksymalnej wartości własnej uogólnionej macierzy teleportacji, które można wyznaczyć numerycznie. W przypadku optymalnego protokołu probabilistycznego, dzięki udowodnieniu czysto teorio-grupowego Twierdzenia 9 w artykule [H8], wyliczyliśmy zwięzłą formułę na średnie prawdopodobieństwo sukcesu p_{succ} (Twierdzenie 3 [H8]):

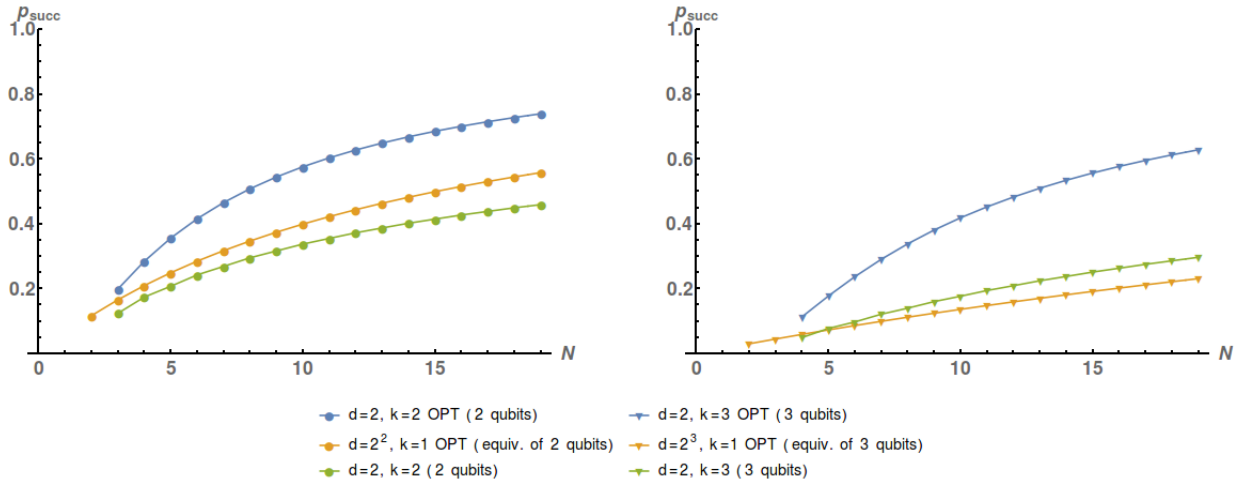
$$p_{succ} = \frac{N!}{(N-k)!}\frac{(d^2+N-k-1)!}{(d^2+N-1)!}. \tag{83}$$

Wykorzystując powyższe rezultaty, w twierdzeniu 4 w pracy [H8] pokazujemy że jeżeli liczba teleportowanych stanów $k = k(N)$ zmienia się jak $o(N)$, to średnie prawdopodobieństwo sukcesu dąży do 1, gdy $N \to \infty$ dla dowolnego wymiaru portu. Ponadto, w szczególnym przypadku kubitowym, pokazujemy że średnie prawdopodobieństwo sukcesu dla optymalnego MPBT dąży do 1 wraz z $N \to \infty$, gdy $k = o(N)$. Wynik ten polepsza rezultat uzyskany dla nieoptymalnego protokołu MPBT, dla którego mamy takie same zachowanie przy $k = o(\sqrt{N})$. Rysunek 12 pokazuje porównanie wartości średniego prawdopodobieństwa sukcesu p_{succ} dla optymalnego MPBT z jego standardowym odpowiednikiem, probabilistycznym PBT z odpowiednio dużym wymiarem portu. Ostatecznie w Twierdzeniu 5 w pracy [H8] wyliczyliśmy optymalną formę pomiarów oraz operacji O_A jako odpowiednio elementy algebry $\mathcal{A}_n(d)$ oraz $\mathcal{A}_n(d)$:

$$\Pi_{\mathbf{i}} = P^+_{A_{\mathbf{i}}B}\otimes\sum_{\alpha\vdash N-k}\frac{d^{N+k}\frac{m_\alpha}{\sum_{\nu\vdash N}m_\nu^2}}{k!\binom{N}{k}d_\alpha}P_\alpha, \quad O_A = \sqrt{d^N}\sum_\mu\sqrt{\frac{m_\mu}{d_\mu\sum_{\nu\vdash N}m_\nu^2}}P_\mu. \tag{84}$$

Przez P_α, P_μ oznaczamy projektory Younga odpowiednio na nieprzywiedlne reprezentacje S_{N-k} oraz S_k.

Protokoły MPBT - analiza asymptotyczna W tej sekcji podsumuję główne rezultaty zawarte w artykule [H7]. Głównym zadaniem podjętym w tej pracy było obliczenie i porównanie zdolności transmisji wariantów protokołów MPBT i porównanie ich z innymi efektywnymi metodami transmisji dużej ilości kwantowej informacji, opisanych na początku Rozdziału 5.7. Byliśmy zainteresowani odpowiedzią na pytanie jak zmienia się efektywność transmisji, gdy liczba teleportowanych stanów wynosi $k \sim N^\alpha$, gdzie $\alpha \in (0,1)$ oraz liczba portów N dąży do nieskończoności. Jest to niejako najbardziej naturalne podejście do badania asymptotycznego zachowania się protokołów MPBT, ponieważ tylko w takim scenariuszu liczba teleportowanych stanów k zmienia się wraz z liczbą portów, pokazując nam prawdziwą zdolność danego schematu. W tradycyjnym podejściu do badania pojemności kanału główną rozważaną wielkością jest asymptotyczne zachowanie ilorazu k/N– liczby wysłanych kubitów (kuditów) w przeliczeniu na liczbę użyć kanału (lub pary splątanej). Tutaj głównym celem staje się zidentyfikowanie wykładników asymptotycznych α, dla których transmisja jest możliwa, ponieważ wspomniany



Rysunek 12: Prawy wykres przedstawia porównanie optymalnego probabilistycznego protokołu MPBT ($k > 1$, OPT) z jego nieoptymalną wersją oraz ze standardowym optymalnym PBT z odpowiednio dużym wymiarem portu. Widzimy wyraźnie, że optymalne MPBT wykazuje lepszą wydajność w stosunku do każdego z wariantów. Dodatkowo, na lewym wykresie, wykreśliliśmy prawdopodobieństwa sukcesu dla optymalnego PBT dla wymiarów portów $d = 4$ oraz $d = 8$. Widzimy, że optymalny protokół MPBT dla $k = 2$, $d = 2$ wykazuje wyższe wartości prawdopodobieństw, w przeciwieństwie do nieoptymalnego MPBT w porównaniu ze standardowym PBT dla tych samych parametrów. Jest to jedyny taki przypadek.

wcześniej iloraz znika dla PBT. Takie rozważania, w których pytamy, ile informacji kwantowych możemy wiarygodnie przesłać za pomocą protokołów teleportacji, zostały rozważone po raz pierwszy i doprowadziły nas do nowych wyników jakościowych i ilościowych.

Pokazaliśmy, że ogólnie liczba układów do teleportacji może być dynamicznie zmieniana przez nadawcę wraz z rosnącą liczbą portów, przy jednoczesnym zapewnieniu wysokiej wydajności w protokole deterministycznym i probabilistycznym. W każdym wariancie PBT i MPBT uzyskujemy krytyczne zachowanie jakości transmisji. Identyfikujemy wartości krytyczne α_{cr} wykładników α dla kilku wariantów, zarówno dla dokładnych asymptotycznych wartości parametrów opisujących wydajność protokołów, jak i ich dolnych granic. Ilekroć wartość α jest poniżej wartości krytycznej α_{cr}, wartości wierności (lub prawdopodobieństwa sukcesu, w zależności od schematu) opisujące transmisję wynoszą 1, a w przeciwnym razie 0.

Teraz podsumujmy pokrótce główne wyniki, skupiając się niezależnie na deterministycznym i probabilistycznym protokole MPBT:

1. **Protokół deterministyczny:** We wszystkich deterministycznych protokołach (M)PBT wynikową wierność splątania F przesyłu możemy połączyć z prawdopodobieństwem sukcesu p_{dist} rozróżniania stanów sygnałowych $\{\sigma_{\mathbf{i}}\}_{\mathbf{i}\in\mathcal{I}}$, gdy każdy z nich występuje z równym prawdopodobieństwem $1/|\mathcal{I}| = 1/k!\binom{N}{k}$. Idea ta została po raz pierwszy zasugerowana przez Köning'a i Beigi w pracy [E88] dla $k = 1$, a następnie rozwinięta przez nas w artykule [H7]. Dla protokołów MPBT i jakiegokolwiek możliwego zbioru pomiarów $\{\Pi_{\mathbf{i}}\}_{\mathbf{i}\in\mathcal{I}}$ wspomniana relacja jest następująca:

$$F = \frac{k!\binom{N}{k}}{d^{2k}} p_{dist}, \qquad p_{dist} = \frac{1}{k!\binom{N}{k}} \sum_{\mathbf{i}\in\mathcal{I}} \text{Tr}(\Pi_{\mathbf{i}}\sigma_{\mathbf{i}}). \tag{85}$$

Aby znaleźć ograniczenie dolne na F jako pomiary $\{\Pi_{\mathbf{i}}\}_{\mathbf{i}\in\mathcal{I}}$ wybraliśmy *square-root measurements* dane wyrażeniem (74). Dla takiego wyboru udowodniliśmy uogólnienie Lematu A.3 z pracy [E88], gdzie dostarczamy ograniczenie dolne na p_{dist} w terminach śladu ze

	$F=0$	F_{cr}	$F=1$
Pack.PBT	$\alpha > 1/2$	$\alpha_{\text{cr}} = 1/2\,,\ F_{\text{cr}} = e^{-3a^2/4}$	$\alpha < 1/2$
Pack.OPBT	$\alpha > 2/3$	$\alpha_{\text{cr}} = 2/3\,,\ F_{\text{cr}} = e^{-\pi a^3}$	$\alpha < 2/3$
MPBT	$-$	$\alpha_{\text{cr}} = 1, \quad F_{\text{cr}} \geq e^{-\frac{3a}{1-a}}$	$\alpha < 1$

Tablica 2: Porównanie zachowania asymptotycznego dwóch wariantów upakowanego PBT z MPBT w deterministycznym przypadku, gdzie $k = aN^{\alpha}$. Przez 'cr' oznaczamy krytyczną wartość parametru α, dla którego asymptotyczna wartość F wykazuje przeskok.

znormalizowanego operatora $\overline{\rho} = \rho / \operatorname{Tr}(\rho)$, gdzie ρ dany jest przez (75):

$$p_{dist} \geq \frac{1}{d^{N-k} \operatorname{Tr} \overline{\rho}^2}. \tag{86}$$

Następnie dowodzimy główny techniczny rezultat dany poprzez Lemat 1 z [H7], gdzie używając czysto kombinatorycznej analizy obliczyliśmy wielkość $\operatorname{Tr}\overline{\rho}^2$, która dana jest poprzez:

$$\operatorname{Tr}(\overline{\rho}^2) = d^{-N-k} \binom{N}{k}^{-1} \binom{d^2+N-1}{k}. \tag{87}$$

To z kolei prowadzi nas do dolnego ograniczenia na F, zawartego w Twierdzeniu 2 w pracy [H7], które zależy tylko od parametrów globalnych – liczby portów N, wymiaru portu d, liczby teleportowanych układów k:

$$F \geq \binom{N}{k} \binom{d^2+N-1}{k}^{-1} \geq \left(1 - \frac{d^2-1}{d^2+N-k}\right)^k. \tag{88}$$

Dysponując powyższym wynikiem możemy już zbadać zachowanie się protokołu MPBT dla $N \to \infty$, gdy k zmienia się wraz z N, czyli w interesującym nas reżimie. Okazuje się, że w deterministycznym przypadku, nawet optymalne upakowane PBT wykazuje niższą wydajność niż dolne ograniczenie wyliczone dla nieoptymalnego MPBT. W szczególności pokazaliśmy, że asymptotycznie dla nieoptymalnego deterministycznego MPBT można przesłać znacznie większą ilość kwantowej informacji, tzn. z $\alpha_{\text{cr}} = 1$, w przeciwieństwie do optymalnego upakowanego PBT, gdzie $\alpha_{\text{cr}} = 2/3$, w związku z czym możemy przesłać asymptotycznie tylko nie więcej niż $o(N^{2/3})$ kubitów w sposób wierny. Wyniki te podsumowaliśmy w Tabeli 2 oraz na lewym wykresie na Rysunku 13.

2. **Protokół probabilistyczny:** Rezultaty dotyczące asymptotycznego zachowania się nieoptymalnego probabilistycznego protokołu zostały uzyskane poprzez wykorzystanie teoriogrupowych wyrażeń na prawdopodobieństwo sukcesu wyliczonych w pracy [H10], wzór (79) w niniejszym autoreferacie. W tym przypadku ograniczyliśmy się do zbadania przypadku kubitowego, gdzie rozważane równanie przyjmuje bardzo elegancką postać, zadaną poprzez parametry opisujące kwantowy moment pędu, gdzie możemy wykonać analitycznie minimalizację z równania (79):

$$p_{succ} = \frac{1}{2^N} \frac{1}{N+1} \sum_{s=0(\frac{1}{2})}^{\frac{N-k}{2}} (2s+1)^2 \binom{N+1}{\frac{N-k}{2}-s}. \tag{89}$$

W przeciwieństwie do przypadku deterministycznego, w wariancie probabilistycznego MPBT, skalowanie jest takie samo jak dla probabilistycznego optymalnego upakowanego PBT, pozwalając nam na asymptotyczną transmisję $o(N^{\alpha})$ z parametrem $\alpha_{\text{cr}} = 1/2$. Pokazuje to jakościową różnicę pomiędzy przypadkiem deterministycznym a probabilistycznym. Dodatkowo dla skończonej liczby portów N wyliczyliśmy dolne oraz górne

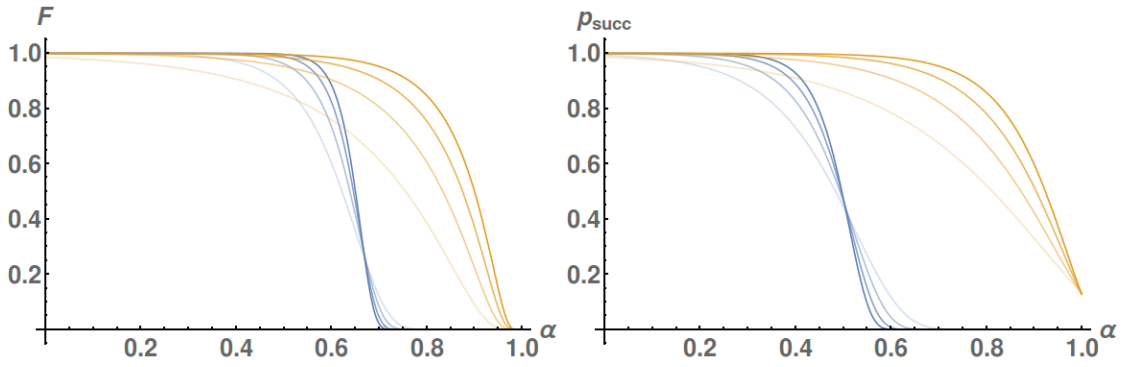
	$p_{succ} = 0$	$p_{succ,\mathrm{cr}}$	$p_{succ} = 1$
Pack.PBT	$\alpha > 1/3$	$\alpha_{\mathrm{cr}} = 1/3$, $p_{succ,\mathrm{cr}} = e^{-ca^{3/2}}$	$\alpha < 1/3$
Pack.OPBT	$\alpha > 1/2$	$\alpha_{\mathrm{cr}} = 1/2$, $p_{succ,\mathrm{cr}} = e^{-3a^2}$	$\alpha < 1/2$
MPBT	$\alpha > 1/2$	$\alpha_{\mathrm{cr}} = 1/2$, eq. (15) in [H7]	$\alpha < 1/2$
OMPBT	–	$\alpha_{\mathrm{cr}} = 1$, $p_{succ,\mathrm{cr}} = (1+a)^3$	$\alpha < 1$

Tablica 3: Porównanie asymptotycznego zachowania się p_{succ} dla wszystkich wariantów upakowanego PBT z MPBT w wersji probabilistycznej, gdy $k = aN^{\alpha}$. Przy czym mamy $c = \sqrt{8/\pi}$ oraz przez 'cr' oznaczamy krytyczną wartość parametru α, dla którego asymptotyczna wartość p_{succ} wykazuje przeskok.

ograniczenie na p_{succ} naszego protokołu (Proposition 18 z [H7]). Cel ten osiągnęliśmy dzięki kombinacji zaawansowanych narzędzi z analizy statystycznej, w szczególności słynnemu twierdzeniu Berry-Essen [E106, E107] z bezpośrednim oszacowaniem wyrażeń dwumianowych poprzez gaussowskie przybliżenia. W optymalnej wersji probabilistycznego MPBT możemy pracować z wyrażeniem na dokładną wartość prawdopodobieństwa sukcesu dla dowolnego wymiaru portu d. Było to możliwe dzięki temu, że wyrażenie takie zostało wyprowadzone w pracy [H8] (równanie (83) w niniejszym autoreferacie) i przekształcone do formy bardziej dla nas dogodnej:

$$p_{succ} = \prod_{m=2}^{d^2} \left(1 - \frac{k}{N-1+m}\right). \tag{90}$$

Badając powyższe równanie pokazaliśmy, że asymptotycznie możemy przesłać $o(N^{\alpha})$ kubitów z parametrem krytycznym równym 1, co wyraźnie przewyższa możliwości różnych wariantów PBT. Zostało to zilustrowane w Tabeli 3 oraz na prawym wykresie Rysunku 13.



Rysunek 13: Lewy wykres: Asymptotyczne wartości dla dolnego ograniczenia na wierność splątania dla MPBT (linie pomarańczowe) porównane z wiernością upakowanego optymalnego PBT (niebieskie linie), gdzie $k = aN^{\alpha}, a = 1$, $\alpha \in (0,1)$. N rośnie wraz z pogrubianiem się linii, mamy odpowiednio $10^2, 10^3, 10^4$ oraz 10^5. Prawy wykres: Prawdopodobieństwo sukcesu porównane z upakowanym optymalnym PBT (linie niebieski) wraz z optymalnym protokołem MPBT (linie pomarańczowe), gdzie $k = aN^{\alpha}, a = \frac{1}{2}$. Tutaj również N rośnie wraz ze wzrostem intensywności koloru linii, mamy odpowiednio $10^2, 10^3, 10^4$ oraz 10^5.

6 Prezentacja osiągnięć dydaktycznych, organizacyjnych oraz popularyzujących naukę

6.1 Osiągnięcia dydaktyczne

Nauczanie akademickie:

1. Wykład *Mechanika klasyczna* (45 godzin, rok akademicki 2022/2023, semestr zimowy, dla studentów drugiego roku fizyki)
2. Ćwiczenia rachunkowe *Mechanika klasyczna* (45 godzin, rok akademicki 2022/2023, semestr zimowy, dla studentów drugiego roku fizyki)
3. Wykład *Klasyczna teoria informacji* (w języku angielskim, 30 godzin, rok akademicki 2021/2022, semestr letni, dla studentów pierwszego roku studiów uzupełniających kierunku Quantum Information Technology)
4. Laboratorium *Python z podstawami algorytmiki* (45 godzin, rok akademicki 2021/2022, semestr letni, dla studentów pierwszego roku bioinformatyki)
5. Wykład *Mechanika klasyczna - elementy Szczególnej Teorii Względności* (15 godzin, rok akademicki 2021/2022, semestr letni, dla studentów drugiego roku fizyki)
6. Ćwiczenia rachunkowe *Mechanika klasyczna* (30 godzin, rok akademicki 2021/2022, semestr letni, dla studentów drugiego roku fizyki)
7. Ćwiczenia rachunkowe *Procesy stochastyczne: podstawy i zastosowania* (30 godzin, rok akademicki 2021/2022, semestr letni, dla studentów drugiego roku modelowania matematycznego i analizy danych)
8. Ćwiczenia rachunkowe *Algebra liniowa z geometrią* (30 godzin, rok akademicki 2013/2014, semestr zimowy, dla studentów pierwszego roku fizyki)
9. Ćwiczenia rachunkowe *Wstęp do matematyki* (30 godzin, rok akademicki 2012/2013, semestr zimowy, dla studentów pierwszego roku bioinformatyki)

Opieka nad doktorantami:

1. Promotor pomocniczy dla Piotra Adama Kopszaka, 2019-obecnie, Wydział Fizyki i Matematyki, Uniwersytet Wrocławski,
2. Przełożony dla Tomasza Patryka Młynika jako doktoranta zatrudnionego w ramach grantu Sonata 16 (UMO-2020/39/D/ST2/01234), 2022-obecnie, Wydział Matematyki, Fizyki i Informatyki, Uniwersytet Gdański.

Nauczanie pozaakademickie:

1. Prowadzenie wykładów podczas szkoły letniej: *Next generation of quantum information scientists. Gdańsk series of international school for students*, 11.07.2022-22.07.2022, Wydział Matematyki, Fizyki i Informatyki, Uniwersytet Gdański. Przeprowadziłem 8 godzin wykładów zatytułowanych: *Introduction to quantum computing*.

6.2 Osiągnięcia organizacyjne

1. Współudział w organizacji szkoły letniej *Next generation of quantum information scientists. Gdańsk series of international school for students*, 11.07.2022-22.07.2022, Wydział Matematyki, Fizyki i Informatyki, Uniwersytet Gdański. Wraz z Dr. Sergii Strelchuk'iem (The University of Cambridge, Wielka Brytania) przygotowałem cały program nauczania, notatki do wykładów, listy problemów z rozwiązaniami na 40 godzin wykładu + 20 godzin ćwiczeń rachunkowych `https://gqi.ug.edu.pl/`

2. Członek komitetu naukowego planowanej konferencji *Mathematical Structures in Quantum Mechanics*, 19-22.06.2023, Wydział Matematyki, Fizyki i Informatyki, Uniwersytet Gdański. `https://gwmp.ug.edu.pl/`

6.3 Osiągnięcia w popularyzowaniu nauki

1. 16.03.2023, Wykład z okazji dni otawrtych Uniwersytetu Gdańskiego, tytuł wystąpienia: *Ńa problemy jutra FIZYKA!"*

2. 09-11.09.2019, Zdolni z Pomorza, Matematyka gier planszowych.

3. 19.11.2017, Polish Science Cafe, Trinity Hall, Cambridge, tytuł wystąpienia: *Ą few steps towards everyday quantum cryptography"* (zaproszone)

7 Inne osiagniecia naukowe

7.1 Dane bibliometryczne

Źródło: Google Scholar (14.03.2023)

- Liczba recenzowanych publikacji: 25 (9 przed doktoratem)
- Liczba nieopublikowanych manuskryptów w bazie arXiv: 7 (5 znajduje się na etapie recenzji w czasopismach naukowych `https://arxiv.org/search/?searchtype=author&query=Studzi%C5%84ski%2C+M&order=-announced_date_first&size=50&abstracts=hide`)
- Całkowita liczba cytowań: 560
- H-indeks: 11
- I10-indeks: 12

Źródło: Web of Science (14.03.2023)

- Liczba recenzowanych publikacji: 23 (9 przed doktoratem)
- Całkowita liczba cytowań: 345 (całkowita), 309 (bez autocytowań)
- H-indeks: 9

7.2 Nagrody

1. 08.2021-07.2024, Stypendium Ministra dla wybitnych młodych naukowców, Ministerstwo Edukacji i Nauki, UMO-SMN/16/0938/2020

2. 05.10.2021, Nagroda Rektora Uniwersytetu Gdańskiego 3-go stopnia

7.3 Publikacje przed uzyskaniem stopnia doktora

7.3.1 Badania uwzględnione w rozprawie doktorskiej:

1. **Wkład w rozwój teorii reprezentacji i teorii separowalności** Słynne kryterium separowalności Peresa-Horodeckiego jest jednym z głównych rezultatów kwantowej teorii informacji. Stwierdza ono, że każdy stan kwantowy $2 \otimes 2$ oraz $2 \otimes 3$ pozostający po częściowej transpozycji dodatni jest spearowalny. W wyższych wymiarach własność dodatniej częściowej transpozycji (ang. positive partial transposition, PPT) jest tylko warunkiem koniecznym spearowalności. W ogólności zdecydowanie czy dany stan kwantowy jest separowalny/splątany jest bardzo złożonym problemem, do którego rozwiązania możemy stosować metody numeryczne, jak na przykład algorytm Doherty'iego (który nie zawsze jest konkluzywny) lub teorię świadków splątania. Problem staje się jeszcze bardziej złożony, gdy rozważymy stany wielocząstkowe. Inną metodą może być ograniczenie zbioru rozważanych stanów kwantowych do stanów posiadających określone symetrie, ale wciąż stanowiących szeroką klasę obiektów. W artykułach [P3] i [P4] rozwijamy idee po raz pierwszy wprowadzone przez Wernera i Eggeling'a dla stanów, które są $U \otimes U \otimes U$ niezmiennicze i pozostają dodatnie po operacji częściowej transpozycji względem któregoś z podukładów. Zadaniem było rozwinięcie narzędzi matematycznych pozwalających w ogólności na konstrukcję stanów PPT w reżimie wielocząstkowym, gdzie częściowa transpozycja działa pierwotnie na ostatnim układzie. Kluczową obserwacją w naszej konstrukcji był fakt, że obiekty początkowo $U^{\otimes n}$ niezmiennicze, po operacji częściowej transpozycji stają się $U^{\otimes(n-1)} \otimes \overline{U}$ niezmiennicze, gdzie kreska oznacza sprzężenie zespolone. W rezultacie obiekty te należą do algebry częściowo transponowanych operatorów permutacji, gdzie transpozycja działa na ostatnim układzie. W naszej pracy zidentyfikowaliśmy nieredukowalne (minimalne) ideały rozważanej algebry oraz przedstawiliśmy algorytm na konstrukcję nieredukowalnej bazy operatorowej w każdym z nich. Zrobiliśmy to dwojako, w artykule [P4] poprzez konstrukcję nieortonormalnej bazy wektorowej, do której z kolei musieliśmy zastosować procedurę ortogonalizacji używając odwrotności macierzy Grama. W pracy [P3], zastosowaliśmy z kolei metody wywodzące się czysto z teorii reprezentacji algebr, uzyskując ortonormalny zbiór niereduowalnych operatorów bazowych. Jednakże w obu tych przypadkach metody działały efektywnie dla relatywnie małej ilości cząstek n w układzie, ale sam formalizm pozostawał w mocy dla dowolnego n oraz wymiaru przestrzeni Hilberta. Dzięki temu byliśmy w stanie podać, jak rozkłada się każdy częściowo transponowany operator permutacji w języku zaproponowanej bazy. Dodatkowo, byliśmy w stanie prowadzić efektywne obliczenia dla układów o małej ilości cząstek posiadających dyskutowane tutaj symetrie. W szczególności, rozwinięte metody pozwoliły nam na szczegółowy opis maszyn klonujących (omówione poniżej) oraz konstrukcję kwantowych stanów PPT dla małej ilości cząstek n. Wykorzystując nasze narzędzia byliśmy również w stanie odzyskać wcześniej znane rezultaty dotyczących stanów $U^{\otimes 3}$ niezmienniczych.

2. **Opis uniwersalnych kwantowych maszyn klonujących** Niemożliwość idealnego klonowania nieznanych stanów kwantowych jest jedną z głównych cech różniących mechanikę kwantową od świata klasycznego. Własność ta wynika bezpośrednio z liniowości rozważanej teorii kwantowej. Jednakże mechanika kwantowa nadal pozwala na produkcję klonów, które nie są idealne lub mówiąc bardziej formalnie wierność obliczona pomiędzy klonami a stanem, który chcemy z klonować jest mniejsza niż 1. Mając taką własność możemy zapytać: jak dobrze możemy klonować stany kwantowe i jakie jest ograniczenie na wynikową wierność narzucone przez teorię kwantową? W pracach [P2] i [P5] rozważamy ogólny przypadek uniwersalnych kwantowych maszyn klonujących (ang. universal quantum cloning machines, UQCM), produkujących N klonów z jednego stanu wejściowego. Nasze rozważania rozpoczęliśmy od przypadku kubitowego [P5], gdzie byliśmy

w stanie pokazać, że stan łączny (stany kolnów + stan klonowany) posiada symetrie pozwalające stosować dualizm Schura-Weyla. Dokładniej, zagadnienie znalezienia dozwolonego zakresu wierności klonów zostało zredukowane do problemu określenia zakresu dozwolonej wierności na każdej z nieredukowalnych podprzestrzeni osobno. Następnie do otrzymania całkowitego dozwolonego obszaru należało znaleźć otoczkę wypukłą otrzymanych obszarów. W szczególności przeanalizowaliśmy przypadek maszyny klonującej $1 \to 3$ wraz z prezentacją dozwolonego obszaru wierności dającego się zilustrować w przestrzeni trójwymiarowej. Dodatkowo, pokazaliśmy jak rekonstruować stany opisujące klony, gdy zażądamy konkretnych wartości ich wierności. Dla wyższych wymiarów dualizm Schura-Weyla nie jest już wystarczający przez co należało wypracować i zastosować nowe metody. W pracy [P2] pokazaliśmy, że rozważany stan łączny jest elementem badanej w [P3] oraz w [P4] algebry częściowo transponowanych operatorów permutacji. Stosując wypracowane w tych pracach narzędzia byliśmy w stanie przeprowadzić podobną analizę jak to było zrobione dla kubitów.

3. **Wkład w teorię destylacji splątania** Jednym z najważniejszych i najbardziej fundamentalnych zasobów w kwantowo-informatycznych protokołach jest czyste splątanie. Niestety, w praktyce jeżeli chcemy użyć wybranego protokołu, to mamy dostęp jedynie do mieszanki, co jest pewnym ograniczeniem. Jednym ze sposobów obejścia tego problemu jest wydestylowanie przez zastosowanie naszego docelowego protokołu, czystego splatania w postaci par maksymalnie splątanych. W tym celu stosujemy tak zwane protokoły destylacji kwantowego splątania. W pracy [P6] prezentujemy procedurę destylacji z mieszanki stanów dwukubitowych wraz z trzema wzajemnie ortogonalnymi innymi stanami. Wykorzystując istniejące w układzie symetrie mogliśmy zastosować narzędzia wynikające z dualizmu Schura-Weyla oraz symetryzatorów Younga. Mówiąc bardziej ściśle, destylujemy splątanie poprzez projekcję n kopii naszego stanu na podprzestrzenie permutacyjnie niezmiennicze, a następnie stosujemy jednokierunkowy protokół haszujący. Przepisanie problemu w języku czysto teorio-grupowym pozwoliło na znalezienie analitycznych wyrażeń na wydajność protokołu (rate protokołu). Dodatkowo, postawiony problem rozwiązaliśmy wykorzystując alternatywne podejście bazujące na algebraicznych schematach asocjacji zwanych schematami Johnsona. Nasze podejście uogólniliśmy także na przypadek wyższych wymiarów.

7.3.2 Badania nieuwzględnione w rozprawie doktorskiej:

1. **Geometryczne własności zbioru stanów prywatnych** Głównym zadaniem kwantowej kryptografii jest otrzymanie klasycznego sekretnego klucza do szyfrowania danych ze stanów kwantowych. Może to zostać osiągnięte poprzez wykorzystanie stanów maksymalnie splątanych lub szerszej klasy stanów splątanych zwanych stanami prywatnymi. Stany te zbudowane są z dwóch części – dwuukładowej części klucza, z której otrzymujemy sekretny klucz oraz dwuukładowej części chroniącej klucz przed podsłuchem, nazywanej tarczą. W pracy [P7] analizujemy geometryczne własności zbioru stanów prywatnych z punktu widzenia ich odległości od zbioru stanów separowalnych. Byliśmy zainteresowani stanami prywatnymi posiadającymi własność PPT (pozostają dodatnie po operacji częściowej transpozycji) oraz są możliwie daleko od stanów separowalnych. Oznacza to, że ze stanów takich nie możemy wydestylować czystego splątania, ale cały czas możemy otrzymać klucz kryptograficzny. Pokazaliśmy, że dla ustalonego wymiaru tarczy, odległość od zbioru stanów separowalnych rośnie wraz ze wzrostem wymiaru tarczy. Nową cechą naszej konstrukcji jest fakt, że nie musi stosować metody zwanej *boosting*, polegającej na tensorowaniu wielu kopii stanu prywatnego, aby uzyskać stan prywatny dowolnie odległy od seprawowalnych. Zabieg ten pozwolił na uzyskanie lepszego skalowania odległości w stosunku do wcześniejszych prac. Dodatkowo, przedstawiliśmy

konstrukcję stanów prywatnych posiadających żądane cechy, co uczyniło nasze wyniki konstuktywnymi.

2. **Badania nad lokalnymi kwantowymi obwodami** Losowe macierze unitarne są ważnym zasobem w teorii obliczeń kwantowych i kwantowej teorii informacji. Ich możliwe zastosowania sięgają od kwantowej kryptografii, kwantowego ukrywania danych, podstaw mechaniki statystycznej do problemów kwantowej termodynamiki jak na przykład ekwilibracja układów kwantowych. Niestety, aby zaimplementować losową macierz unitarną Haara potrzebujemy eksponencjalnie wiele kubitowych bramek kwantowych i bitów – ta własność czyni niemożliwą ich praktyczną implementację. Jedną z metod radzenia sobie z tym problemem jest rozważane tzw. przybliżonych unitarnych $t-$modeli (ang. $t-$design), które imitują własności miary Haara dla wielomianów stopnia nie większego niż t. Obecnie wiemy, że obwód kwantowy, którego rozmiar skaluje się wielomianowo z liczbą kubitów n, tworzy przybliżony unitarny design (poly$(n)-$ design). Idea dowodu polegała na wykorzystaniu narzędzi z fizyki układów wielocząsteczkowych i przetłumaczeniu zagadnienia na problem określenia przerwy spektralnej konkretnego hamiltonianu. W artykule [P8] numerycznie zbadaliśmy tę odpowiedniość, skupiając się przede wszystkim na wyliczonych uprzednio ograniczeniach na przerwę spektralną. Dla szerokiego spektrum wartości parametrów, $n \leq 20$ and $t \leq 5$, udowodniliśmy, że znane uprzednio ograniczenia dolne, w ogólności niewiele mówią o faktycznej sytuacji układu, a jedynie stwierdzają istnienie bądź nie przerwy spektralnej. Oznacza to, że w rzeczywistości faktyczna wartość przerwy spektralnej znacznie różni się od odpowiedniego ograniczenia dolnego. Dodatkowo porównaliśmy nasze rezultaty numeryczne z innymi technikami dającymi możliwości dolnego ograniczenia przerwy spektralnej i pokazaliśmy, że one także nie są wysycane, a nawet, że są one niekonkluzywne. Postęp w numerycznych symulacjach mógł zostać dokonany dzięki zastosowaniu dualizmu Schura-Weyla oraz teorii reprezentacji algebry grupowej grupy permutacji S_n. Nasze metody, będące połączeniem numeryki oraz podejścia analitycznego, użyte do konstrukcji odpowiednich nieredukowalnych baz, mogą być użyte do badania także innych układów wielu cząstek wykazujących podobne symetrie.

3. **Transformacje pomiędzy równoważnymi nieredukowalnymi reprezentacjami** Powszechnie wiadomo, że teoria reprezentacji grup jest potężnym narzędziem w fizyce, pozwalającym na wykorzystanie symetrii leżących u podstaw rozważanego systemu w celu uproszczenia jego opisu, znalezienia odpowiednich praw zachowania i uczynienia opisu bardziej eleganckim. Z punktu widzenia obliczania konkretnych parametrów opisujących układ, ograniczenie się do nieredukowalnych bloków zmniejsza złożoność obliczeniową, a także często pozwala na analityczny opis zagadnienia. Jednakże, aby przeprowadzić konkretne rachunki (np. numeryczne) musimy znać reprezentacje macierzowe elementów grupy na każdym z nierównoważnych bloków. Może się oczywiście zdarzyć, że konkretna reprezentacja jest bardziej przydatna do konkretnego zadania niż inna. Istnieje zatem potrzeba przetłumaczenia rozważanego zagadnienia do postaci bardziej dla nas przyjaznej. W artykule [P9] zaproponowaliśmy algorytm konstrukcji transformacji unitarnej pomiędzy równoważnymi reprezentacjami dla grupy skończonej G. Pokazaliśmy, że możliwe jest zbudowanie takiej transformacji wykorzystując własności nieredukowalnych reprezentacji. W naszej konstrukcji używamy relacji ortogonalności dla nieredukowalnych reprezentacji, co jest podejściem innym niż stosowane uprzednio, polegające na rozwiązywaniu układów równań liniowych. Podajemy przykłady obrazujące działanie naszego algorytmu dla grupy permutacji S_n. W szczególności analizujemy transformację podobieństwa dla klasy par równoważnych nieredukowalnych reprezentacji grupy symetrycznej, pokazując że otrzymana macierz unitarna jest antydiagonalna w bazie Youngа-Yamanouchiego. Dodatkowo rozważamy także pewne uogólnienia słynnych relacji ortogonalności dla nieredukowalnych reprezentacji grup skończonych.

4. **Całkowalność klasycznych układów hamiltonowskich** Wiele problemów mechaniki klasycznej jest opisywanych za pomocą układu równań różniczkowych. Na przykład w podejściu Hamiltona, dla układu o n stopniach swobody, jego ewolucja jest opisana za pomocą $2n$ równań różniczkowych rzędu pierwszego. Naturalne jest pytanie pod jakimi warunkami możemy uzyskać analityczne rozwiązanie takiego układu. Czyli pytamy się tak na prawdę o własność całkowalności układu, który rozważamy. W artykule [P10] badamy całkowalność w sensie Liouville'a naturalnego układu hamiltonowskiego z jednorodnym potencjałem wymiernym. Potencjały takie znajdują szerokie zastosowanie w modelach kosmologicznych z konforemnym polem skalarnym, w teorii uogólnionych potencjałów Hélion-Heiles'a opisujących płaski ruch gwiazd w galaktykach, układach Yang-Millis'a z polem cechowana $SU(2)$, a także w wielu innych – co stanowi mocną motywację, z punktu widzenia fizyki, do ich badania. W przypadku układów o dwóch stopniach swobody pokazaliśmy uniwersalną relację dla wartości własnych hesjanu potencjału obliczonymi w tzw. punktach Darboux. Istnienie takiej relacji pozwoliło nam z kolei pokazać, że rozważane potencjały spełniają skończoną liczbę warunków koniecznych na ich całkowalność wynikających z różniczkowej grupy Galois dla równań wariacyjnych wyliczonych wzdłuż wybranego rozwiązania szczególnego. To dało nam narzędzie do klasyfikacji i charakteryzacji badanych potencjałów. W szczególności zbudowaliśmy liczne przykłady potencjałów spełniających podane warunki konieczne całkowalności i udowodniliśmy ich całkowalność budując funkcjonalnie niezależne całki pierwsze.

7.4 Dodatkowe osiągnięcia po doktoracie

Badania, które przeprowadziłem po uzyskaniu stopnia naukowego doktora, a które nie stanowią części osiągnięcia habilitacyjnego, można podzielić na następujące podpunkty:

1. **Ograniczenia na repeatery (wzmacniacze) prywatnej losowości** Większość protokołów kryptograficznych wykorzystuje dwa główne składniki – prywatną losowość oraz klucz prywatny. Rozdystrybuowany bezpieczny klucz, czyli skorelowany ciąg bitów, pomiędzy odległymi i uczciwymi stronami zapewnia bezpieczeństwo komunikacji, która jest kluczowa dla bezpieczeństwa kwantowego internetu. Jedną z bezpiecznych metod dystrybucji klucza jest paradygmat wymiany kluczy sieciowych. Formalizm ten został rozwinięty do najbardziej ogólnego scenariusza stanów prywatnych. W pracy [P11] skupiliśmy się na własnościach sieci w kontekście prywatnej losowości – zasobu komplementarnego do prywatnego klucza. Naszym pierwszym krokiem było pokazanie, że każdy stan prywatny jest szczególnym przypadkiem tzw. stanów niezależnych, czyli stanów zawierających doskonałą, bezpośrednio dostępną prywatną losowość. Używając tego związku byliśmy w stanie pokazać ograniczenie górne na tzw. rate wzmocnionej losowości, podobnie jak to miało miejsce dla stanów prywatnych. Okazuje się, że ograniczenie to jest równe podwojonej entropii względnej obliczonej względem stanu maksymalnie zmieszanego i jest spełnione dla stanów z własnością dodatniej częściowej transpozycji (PPT). Ograniczenie to jest natury fundamentalnej na transfer prywatności w rozważanej sieci. Pokazaliśmy użyteczność wyliczonego ograniczenia poprzez zastosowania go do separowalnych stanów Wernera i pokazaniu przerwy pomiędzy lokalizowalnością oraz prywatną losowością dla dostatecznie dużych wymiarów. Dodatkowo, w ograniczonym scenariuszu, byliśmy w stanie pokazać analogiczne ograniczenie dla dowolnych stanów, nie tylko tych z własnością PPT.

2. **Wyciek prywatnych danych i związek z markowskością** Wszystkie dowody na bezpieczeństwo dystrybucji kluczy kwantowych nie uwzględniają środowiska (warunków) w jakim komunikujące się strony funkcjonują. Oznacza to, że ich użyteczność jest tylko teoretyczna, ponieważ pomijają niedoskonałości w produkcji urządzeń do dystrybucji

klucza kwantowego, czy aktywne ataki podsłuchującego znane jako Trojan Horse Attacks (THAs). Ostatnimi czasy ataki THA, które mogą doprowadzić do tzw. wycieku klucza prywatnego są przedmiotem licznych badań. W artykule [P12] rozważamy scenariusz ataku THA, gdzie podsłuchiwacz ma dostęp do surowego klucza pochodzącego z urządzenia zaufanych stron. Głównym rezultatem tych badań jest podanie dolnego ograniczenia na ilość wycieku prywatnej losowości oraz prywatnego klucza. W szczególności pokazaliśmy, że prywatna losowość nie może spaść bardziej niż $S(a) + \log_2 |a|$, gdzie S jest entropią von Neumanna, a jest układem, który wyciekł do podsłuchiwacza. W rozważanym scenariuszu skupiamy się również na badaniu nieredukowalnych stanów prywatnych i dowodzimy, że ich dwukierunkowy klucz destylowalny jest niezamykalny (ang. non-lockable). Jest to pierwszy znany rezultat tego rodzaju dla nietrywialnej klasy stanów mieszanych. Dodatkowo zaobserwowaliśmy, że dla rozważanej klasy stanów prywatnych ubytek klucza jest niezależny od wymiaru tarczy. Oznacza to w szczególności, że większa tarcza wcale nie ochrania klucza efektywniej. Ostatecznie udowadniamy związek pomiędzy (nie)markowskością dynamiki kwantowej a hakowaniem. Dokładniej pokazujemy, że nieodwracalne odwzorowanie nie jest CP-podzielne wtedy i tylko wtedy, gdy istnieje stan, którego klucz wykrywany przez szczególnego świadka prywatnej losowości zwiększa się w czasie.

3. **Destylacja bezpiecznego klucza z redukowalnych stanów prywatnych** Jak napisaliśmy wcześniej otrzymywanie sekretnego klucza dla bezpiecznej komunikacji/szyfrowania danych ze stanów kwantowych jest jednym z fundamentalnych osiągnięć kwantowej teorii informacji. Zostało to zademonstrowane poprzez wykorzystanie par maksymalnie splątanych. Jednakże otrzymywanie klucza może zostać rozszerzone na stany prywatne, które zawierają w sobie stany maksymalnie splątane. Współcześnie mamy bogatą teorię, która jest intensywnie rozwijana, opisującą ilościowo relacje pomiędzy sekretnością, a zbiorem stanów prywatnych. W artykule [P13] podajemy protokół, który destyluje sekretny klucz poprzez pomiar tarczy redukowalnego stanu prywatnego – nie jesteśmy ograniczeni tylko do części klucza (ang. key part) stanu prywatnego jak to miało miejsce we wszystkich dotychczas znanych protokołach. Dostarczyliśmy ograniczenie górne na wydajność zaproponowanego protokołu w terminach zregularyzowanej względnej entropii splątania. Ograniczenie to jest znacznie lepsze niż stosowane dotychczas w literaturze ograniczenie bazujące na samej względnej entropii splątania. Stosując otrzymane ograniczenie pokazujemy związek pomiędzy zbiorem nieredukowalnych oraz ściśle nieredukowalnych stanów prywatnych oraz istnieniem stanów splątanych z niedestylowalnym kluczem (ang. bound key states). Dokładniej pokazujemy, że jeśli istnieją stany splątane z niedestylowalnym kluczem to zbiory nieredukowalnych oraz ściśle nieredukowalnych stanów prywatnych są sobie równe. Implikacja w przeciwną stronę również zachodzi, dając nam w rezultacie twierdzenie typu 'wtedy i tylko wtedy'. Zakładając, że stany ze związanym kluczem istnieją pokazaliśmy kilka własności nieredukowalnych stanów prywatnych. W szczególności dostarczyliśmy ograniczenie dolne na odległość w normie śladowej pomiędzy stanami ze związanym kluczem, a stanami prywatnymi, które obowiązuje dla odpowiednio dużych wymiarów przestrzeni.

4. **Teoria odwzorowań dodatnich i świadków splątania** Jak napisaliśmy wcześniej jednym ze sposobów zadecydowania czy dany $d \otimes d$ stan kwantowy ρ jest splątany/separowalny jest wykorzystanie pojęcia świadka splątania. Niedodatni operator W jest świadkiem splątania, między innymi, jeśli jego wartość oczekiwana obliczona dla wszystkich stanów separowalnych jest nieujemna. Własność ta czyni pojęcie świadka splątania bardzo ogólnym, ale technicznie jest ją trudno zrealizować. Równoważnie, aby sprawdzić czy dany operator W jest świadkiem splątania można podać odwzorowanie dodatnie, ale nie kompletnie dodatnie Λ, dla którego operator W jest jego obrazem Choi-Jamiołkowskiego. Jednakże z powodu braku charakteryzacji stożka dodatniego, wskazanie takiego odwzo-

rowania jest w ogólności także skomplikowanym zadaniem i jest konieczne dostarczanie innych metod konstrukcji świadków. W pracy [P1] dostarczamy dodatkowej metody konstrukcji świadków splątania. Udowadniamy twierdzenie, że do konstrukcji świadka można użyć odwzorowanie, które nie jest dodatnie i wykorzystać jedynie obszar dziedziny, dla której odwzorowanie to jest dodatnie. Dokładniej, odwzorowanie musi być surjektywne pomiędzy zbiorem projektorów rzędu $k \leq d$, a zbiorem projektorów rzędu jeden. Wskazaliśmy, że odwzorowaniem spełniającym takie warunki jest odwzorowanie odwrotnej redukcji R^{-1}, dla którego podaliśmy konstrukcję nowej klasy świadków splątania, która może być uważana jako uogólnienie świadków splątania Choi.

5. **Badania nad kwantowymi kodami korekcji błędów** W ostatnich latach możemy zaobserwować wzmożone zainteresowanie badaniem nad zaleznością pomiędzy kodami kwantowej korekcji błędów, a teoriami grawitacji znanymi jako odpowiedniość AdS/CFT. Owe teorie grawitacji łączą wnętrze (ang. bulk) przestrzeni anti-de Sittera (AdS) z konforemnymi teoriami pola (CFT) zdefiniowanymi na brzegu tej przestrzeni. Relatywnie niedawno pokazano bezpośredni związek pomiędzy kwantową teorią informacji, a jednym z prostych modeli odpowiedniości AdS/CFT. W artykule [P14] badamy ten związek i eksplorujemy związek pomiędzy stanami absolutnie maksymalnie splątanymi (ang. *maximally entangled states, AME*) oraz kodami kwantowej korekcji błędów, pozwalając na lepsze zrozumienie odpowiedniości AdS/CFT. Dokładniej rozważamy idealny tensor jako stan AME i badamy sposób w jaki zakodowana informacja kwantowa rozchodzi się po sieci. Ponieważ rozważany tensor może być traktowany jako kod kwantowy możemy używać do jego opisu wywodzących się z teorii kodów kwantowych narzędzi (teoria stabilizatorów, łańcuchy kodów). W pierwszym kroku podajemy postać operatorów logicznych i stabilizatorów dla każdego kodu wywodzącego się z $n + m$ kuditowych stabilizujących stanów AME, kodujących n w m kuditów dla $n \leq m$. Nasze wyniki są słuszne dla każdego lokalnego wymiaru, który jest potęgą liczby pierwszej, co wynika ze znanych wcześniej własności pewnych stanów grafowych. Pokazujemy także ograniczenie górne na entropię splątania na brzegu przestrzeni anti-de Sittera, które jest wysycane właśnie dla rozważanych stanów AME, o ile rozważane obszary mają elementy styczne. W szczególności pokazaliśmy, że dla stanów AME nasze ograniczenie odpowiada sławnemu wyrażeniu Ryu-Takayanagi, które łączy entropię splątania pola konforemnego ze stowarzyszoną przestrzenią AdS.

6. **Badania nad kwantowymi drugimi prawami termodynamiki** W erze miniaturyzacji i rozwoju nowych oraz coraz bardziej precyzyjnych eksperymentalnych metod konstrukcji nono-urządzeń musimy odpowiedzieć sobie na pytanie jakie są fundamentalne ograniczenia w ich funkcjonowaniu. W szczególności możemy ograniczyć się do maszyn termodynamicznych, taki jak nano- lub nawet kwantowych silników czy chłodnic, zapytać się o ich funkcjonowanie i być może odkryć nowe własności różniące je od klasycznych odpowiedników. Jest to niezwykle ważny problem teoretyczny, który dotyka fundamentalnych ograniczeń nałożonych prze naturę – zbioru praw termodynamiki, które obowiązują w skali kwantowej. W artykule [P15] wykonaliśmy fundamentalny krok w kierunku ich zrozumienia. Po raz pierwszy rozważyliśmy całkowicie kwantowy przypadek – badamy ewolucję stanów kwantowych posiadających koherencje w paradygmacie, gdy eksperymentator ma dostęp do kąpieli cieplnej o temperaturze T i przeprowadza ewolucję unitarną, która komutuje z całkowitym Hamiltonianem (operacja termiczna). Zapytaliśmy jakie są ograniczenia na ewolucję elementów pozadiagonalnych operatora gęstości przy przejściu pomiędzy różnymi stanami energetycznymi pod działaniem operacji termicznych. Są to de facto realnie drugie prawa termodynamiki dla elementów pozadiagonalnych. Pokazaliśmy, że istnieją dwa rodzaje ograniczeń, jedne dla elementów diagonalnych (termomajoryzacja) oraz drugie dla koherencji. Rozważając macierz prawdopodobieństw przejścia pomiędzy poziomami energetycznymi wyprowadziliśmy ograniczenie

górne na wartość modułu koherencji po transformacji w języku wartości modułu koherencji przed transformacją oraz prawdopodobieństwa przejścia pomiędzy poziomami energetycznymi. W szczególności wykazaliśmy, że owo ograniczenie nie miesza koherencji pomiędzy sobą oraz nie miesza koherencji z elementami diagonalnymi operatora stanu. W przypadku kubitowycm udowodniliśmy, że nasze ograniczenie jest wysycane poprzez bezpośrednią konstrukcję odpowiedniej unitarnej operacji termalnej. Jednakże dla wymiarów wyższych wskazaliśmy konkretny trójpoziomowy kwazi-cykl, dla którego otrzymane przez nas ograniczenie nie może zostać wysycone. To umotywowało nas do wprowadzenia szerszej klasy operacji termicznych zwanych wzmocnionymi operacjami termicznymi.

Referencje: artykuły aplikanta zawarte w serii habilitacyjnej

[H1] Marek Mozrzymas, Michał Studziński, and Nilanjana Datta. Structure of irreducibly covariant quantum channels for finite groups. *Journal of Mathematical Physics*, 58(5):052204, 2017.

[H2] Marek Mozrzymas, Michał Studziński, and Michał Horodecki. A simplified formalism of the algebra of partially transposed permutation operators with applications. *Journal of Physics A: Mathematical and Theoretical*, 51(12):125202, 2018.

[H3] Michał Studziński, Sergii Strelchuk, Marek Mozrzymas, and Michał Horodecki. Port-based teleportation in arbitrary dimension. *Scientific Reports*, 7(1):10871, 2017.

[H4] Marek Mozrzymas, Michał Studziński, Sergii Strelchuk, and Michał Horodecki. Optimal port-based teleportation. *New Journal of Physics*, 20(5):053006, 2018.

[H5] Piotr Kopszak, Marek Mozrzymas, and Michał Studziński. Positive maps from irreducibly covariant operators. *Journal of Physics A: Mathematical and Theoretical*, 53(39):395306, 2020.

[H6] Daniel Stilck França, Sergii Strelchuk, and Michał Studziński. Efficient classical simulation and benchmarking of quantum processes in the weyl basis. *Phys. Rev. Lett.*, 126:210502, 2021.

[H7] Piotr Kopszak, Marek Mozrzymas, Michał Studziński, and Michał Horodecki. Multiport based teleportation – transmission of a large amount of quantum information. *Quantum*, 5:576, 2021.

[H8] Marek Mozrzymas, Michał Studziński, and Piotr Kopszak. Optimal Multi-port-based Teleportation Schemes. *Quantum*, 5:477, June 2021.

[H9] Michał Studziński, Marek Mozrzymas, and Piotr Kopszak. Square-root measurements and degradation of the resource state in port-based teleportation scheme. *Journal of Physics A: Mathematical and Theoretical*, 55(37):375302, 2022.

[H10] Michał Studziński, Marek Mozrzymas, Piotr Kopszak, and Michał Horodecki. Efficient multi port-based teleportation schemes. *IEEE Transactions on Information Theory*, 68(12):7892–7912, 2022.

Referencje: artykuły aplikanta spoza serii habilitacyjnej

[P1] Marek Mozrzymas, Adam Rutkowski, and Michał Studziński. Using non-positive maps to characterize entanglement witnesses. *Journal of Physics A: Mathematical and Theoretical*, 48(39):395302, 2015.

[P2] Michał Studziński, Piotr Ćwikliński, Michał Horodecki, and Marek Mozrzymas. Group-representation approach to $1 \to n$ universal quantum cloning machines. *Phys. Rev. A*, 89:052322, May 2014.

[P3] Marek Mozrzymas, Michał Horodecki, and Michał Studziński. Structure and properties of the algebra of partially transposed permutation operators. *Journal of Mathematical Physics*, 55(3):032202, 2014.

[P4] Michał Studziński, Michał Horodecki, and Marek Mozrzymas. Commutant structure of $u \otimes \cdots \otimes u \otimes u^*$ transformations. *Journal of Physics A: Mathematical and Theoretical*, 46(39):395303.

[P5] Piotr Ćwikliński, Michał Horodecki, and Michał Studziński. Region of fidelities for a $1 \to n$ universal qubit quantum cloner. *Physics Letters A*, 376(32):2178–2187, 2012.

[P6] Mikołaj Czechlewski, Andrzej Grudka, Michał Horodecki, Marek Mozrzymas, and Michał Studziński. Distillation of entanglement by projection on permutationally invariant subspaces. *Journal of Physics A: Mathematical and Theoretical*, 45(12):125303, mar 2012.

[P7] Adam Rutkowski, Michał Studziński, Piotr Ćwikliński, and Michał Horodecki. Construction and properties of a class of private states in arbitrary dimensions. *Phys. Rev. A*, 91:012335, Jan 2015.

[P8] Piotr Ćwikliński, Michał Horodecki, Marek Mozrzymas, Łukasz Pankowski, and Michał Studziński. Local random quantum circuits are approximate polynomial-designs: numerical results. *Journal of Physics A: Mathematical and Theoretical*, 46(30):305301, jul 2013.

[P9] Marek Mozrzymas, Michał Studziński, and Michał Horodecki. Explicit constructions of unitary transformations between equivalent irreducible representations. *Journal of Physics A: Mathematical and Theoretical*, 47(50):505203, nov 2014.

[P10] Michał Studziński and Maria Przybylska. Darboux points and integrability analysis of hamiltonian systems with homogeneous rational potentials. *Physica D: Nonlinear Phenomena*, 249:1–15, 2013.

[P11] Karol Horodecki, Ryszard P. Kostecki, Roberto Salazar, and Michał Studziński. Limitations for private randomness repeaters. *Phys. Rev. A*, 102:012615, Jul 2020.

[P12] Karol Horodecki, Michał Studziński, Ryszard P. Kostecki, Omer Sakarya, and Dong Yang. Upper bounds on the leakage of private data and an operational approach to markovianity. *Phys. Rev. A*, 104:052422, Nov 2021.

[P13] Karol Horodecki, Piotr Ćwikliński, Adam Rutkowski, and Michał Studziński. On distilling secure key from reducible private states and (non)existence of entangled key-undistillable states. *New Journal of Physics*, 20(8):083021, aug 2018.

[P14] Paweł Mazurek, Máté Farkas, Andrzej Grudka, Michał Horodecki, and Michał Studziński. Quantum error-correction codes and absolutely maximally entangled states. *Phys. Rev. A*, 101:042305, Apr 2020.

[P15] Piotr Ćwikliński, Michał Studziński, Michał Horodecki, and Jonathan Oppenheim. Limitations on the evolution of quantum coherences: Towards fully quantum second laws of thermodynamics. *Phys. Rev. Lett.*, 115:210403, Nov 2015.

Referencje: pozostałe artykuły

[E1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[E2] R. Feynman. Simulating Physics with Computers. *Int. J. Th. Phys.*, 21:467–488, 1982.

[E3] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26:1484–1509, 1997.

[E4] Lov K. Grover. Quantum computers can search arbitrarily large databases by a single query. *Phys. Rev. Lett.*, 79:4709–4712, Dec 1997.

[E5] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[E6] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, January 2001.

[E7] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390–393, November 1999.

[E8] Roe Goodman and Nolan R. Wallach. *Symmetry, Representations, and Invariants*. Springer-Verlag, New York, 2009.

[E9] F.Scarabotti T. Ceccherini-Silberstein and F. Tolli. *Representation Theory of the Symmetric Group. The Okounkov-Vershik Approach, Character Formulas, and Partition Algebras*. Cambridge University Press, New York, 2010.

[E10] K. M. Audenaert. A digest on representation theory of the symmetric group. `http://personal.rhul.ac.uk/usah/080/QITNotes_files/Irreps_v06.pdf`. Accessed: 2010-09-30.

[E11] H. Scutaru. Some remarks on covariant completely positive linear maps on c*-algebras. *Rep. Math. Phys.*, 16(1):79–87, 1979.

[E12] J. Schliemann. Entanglement in SU(2)-invariant quantum spin systems. *Physical Review A*, 68(1):012309, 2003.

[E13] M. Sanz, M. M. Wolf, D. Pérez-García, and J. I. Cirac. Matrix product states: Symmetries and two-body Hamiltonians. *Physical Review A*, 79(4):042308, April 2009.

[E14] Bruno Nachtergaele and Daniel Ueltschi. A direct proof of dimerization in a family of su(n)-invariant quantum spin chains. *Letters in Mathematical Physics*, 107(9):1629–1647, Sep 2017.

[E15] A.S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1):269–273, 1998.

[E16] N. Datta, M. Fukuda, and A.S. Holevo. Complementarity and additivity for covariant channels. *Quantum Information Processing*, 5(2):179–207, 2006.

[E17] N. Datta, A.S. Holevo, and Y.M. Suhov. Additivity for transpose. *International Journal of Quantum*, 4(1):85–98, 2006.

[E18] M. Fannes, B. Haegeman, M. Mosonyi, and D. Vanpeteghem. Additivity of minimal entropy output for a class of covariant channels. *arXiv:quant-ph/0410195*, October 2004.

[E19] N. Datta, A.S. Holevo, and Y.M. Suhov. On a sufficient condition for additivity in quantum information theory. *Problems in Information Transmission*, 41:76–90, 2005.

[E20] Motohisa Fukuda and Gilad Gour. Additive bounds of minimum output entropies for unital channels and an exact qubit formula. *IEEE Transactions on Information Theory*, 63(3):1818–1828, 2017.

[E21] Robert König and Stephanie Wehner. A strong converse for classical channel coding using entangled inputs. *Phys. Rev. Lett.*, 103:070504, Aug 2009.

[E22] Nilanjana Datta, Marco Tomamichel, and Mark M. Wilde. On the second-order asymptotics for entanglement-assisted communication. *Quantum Information Processing*, 15(6):2569–2591, Jun 2016.

[E23] M. M. Wolf Ch. B. Mendl. Unital quantum channels - convex structure and revivals of birkhoff's theorem. *Communication in Mathematical Physics*, 289:1057–1096, 2009.

[E24] Laleh Memarzadeh and Barry C. Sanders. Group-covariant extreme and quasiextreme channels. *Phys. Rev. Research*, 4:033206, Sep 2022.

[E25] Maria Balanzó-Juandó, Michał Studziński, and Felix Huber. Positive maps from the walled brauer algebra, arxiv: 2112.12738.

[E26] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed staes: necessary and sufficient conditions. *Physics Letters A*, 223(1):1–8, 1996.

[E27] A. Peres. Separability criterion for density matrices. *Physics Review Letters*, 77(8):1413–1415, 1996.

[E28] P. W. Shor, M. Horodecki, and M.B. Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15(6):629641, 2003.

[E29] S.L. Woronowicz. Positive maps of low dimensional matrix algebras. *Reports on Mathematical Physics*, 10(2):165 – 183, 1976.

[E30] Dariusz Chruściński and Gniewomir Sarbicki. Entanglement witnesses: construction, analysis and classification. *Journal of Physics A: Mathematical and Theoretical*, 47(48):483001, 2014.

[E31] Toshiyuki Takasaki and Jun Tomiyama. On the geometry of positive maps in matrix algebras. *Mathematische Zeitschrift*, 184(1):101–108, 1983.

[E32] Jun Tomiyama. On the geometry of positive maps in matrix algebras. ii. *Linear Algebra and its Applications*, 69:169 – 177, 1985.

[E33] Dariusz Chruściński and Andrzej Kossakowski. Spectral conditions for positive maps. *Communications in Mathematical Physics*, 290(3):1051–1064, 2009.

[E34] A. Kossakowski. A class of linear positive maps in matrix algebras. *Open Systems & Information Dynamics*, 10(3):213–220, 2003.

[E35] Dariusz Chruściński. On kossakowski construction of positive maps on matrix algebras. *Open Systems & Information Dynamics*, 21(03):1450001, 2014.

[E36] Dariusz Chruściński and Andrzej Kossakowski. Geometry of quantum states: New construction of positive maps. *Physics Letters A*, 373(27-28):2301–2305, 2009.

[E37] Wai-Shing Tang. On positive linear maps between matrix algebras. *Linear Algebra and its Applications*, 79:33 – 44, 1986.

[E38] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *PRA*, 59:4206–4216, June 1999.

[E39] Gniewomir Sarbicki, Dariusz Chruściński, and Marek Mozrzymas. Generalising wigner's theorem. *Journal of Physics A: Mathematical and Theoretical*, 49(30):305302, jun 2016.

[E40] S.J. Cho S.H. Kye and S.G. Lee. Generalized choi maps in three-dimensional matrix algebra. *Lin. Alg. Appl.*, 171, 1992.

[E41] James Daniel Whitfield. Communication: Spin-free quantum computational simulations and symmetry adapted states. *The Journal of Chemical Physics*, 139(2):021105, 2013.

[E42] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[E43] Maarten Van den Nest. A monomial matrix formalism to describe quantum many-body states. *New Journal of Physics*, 13(12):123004, dec 2011.

[E44] Akio Fujiwara and Paul Algoet. One-to-one parametrization of quantum channels. *Phys. Rev. A*, 59:3290–3294, May 1999.

[E45] Joseph Emerson, Robert Alicki, and Karol Życzkowski. Scalable noise estimation with random unitary operators. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(10):S347, 2005.

[E46] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. Randomized benchmarking of quantum gates. *Phys. Rev. A*, 77:012307, Jan 2008.

[E47] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman. Real Randomized Benchmarking. *Quantum*, 2:85, August 2018.

[E48] Jonas Helsen, Joel J. Wallman, Steven T. Flammia, and Stephanie Wehner. Multiqubit randomized benchmarking using few samples. *Phys. Rev. A*, 100:032304, Sep 2019.

[E49] J. F. Poyatos, J. I. Cirac, and P. Zoller. Complete characterization of a quantum process: The two-bit quantum gate. *Phys. Rev. Lett.*, 78:390–393, Jan 1997.

[E50] Isaac L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11-12):2455–2467, 1997.

[E51] Seth T. Merkel, Jay M. Gambetta, John A. Smolin, Stefano Poletto, Antonio D. Córcoles, Blake R. Johnson, Colm A. Ryan, and Matthias Steffen. Self-consistent quantum process tomography. *Phys. Rev. A*, 87:062119, Jun 2013.

[E52] Steven T. Flammia and Yi-Kai Liu. Direct fidelity estimation from few pauli measurements. *Phys. Rev. Lett.*, 106:230501, Jun 2011.

[E53] Steven T. Flammia and Joel J. Wallman. Efficient estimation of pauli channels. *ACM Transactions on Quantum Computing*, 1(1), dec 2020.

[E54] Robin Harper, Steven T. Flammia, and Joel J. Wallman. Efficient learning of quantum noise. *Nature Physics*, 16(12):1184–1188, Dec 2020.

[E55] Igor L. Markov and Yaoyun Shi. Simulating quantum computation by contracting tensor networks. *SIAM Journal on Computing*, 38(3):963–981, jan 2008.

[E56] Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M Chow, and Jay M Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature*, 549(7671):242–246, 2017.

[E57] Daochen Wang, Oscar Higgott, and Stephen Brierley. Accelerated variational quantum eigensolver. *Physical review letters*, 122(14):140504, 2019.

[E58] Serwan Asaad, Christian Dickel, Nathan K Langford, Stefano Poletto, Alessandro Bruno, Michiel Adriaan Rol, Duije Deurloo, and Leonardo DiCarlo. Independent, extensible control of same-frequency superconducting qubits by selective broadcasting. *npj Quantum Information*, 2(1):1–7, 2016.

[E59] Katarzyna Siudzińska and Dariusz Chruściński. Quantum channels irreducibly covariant with respect to the finite group generated by the Weyl operators. *Journal of Mathematical Physics*, 59:033508, 2018.

[E60] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[E61] Yong Zhang, Louis H. Kauffman, and Reinhard F. Werner. Permutation and its partial transpose. *International Journal of Quantum Information*, 05(04):469–507, 2007.

[E62] Kazuhiko Koike. On the decomposition of tensor products of the representations of the classical groups: By means of the universal characters. *Advances in Mathematics*, 74(1):57–86, 1989.

[E63] V G Turaev. Operator invariants Of tangles, and *r*-matrices. *Mathematics of the USSR-Izvestiya*, 35(2):411–444, apr 1990.

[E64] G. Benkart, M. Chakrabarti, T. Halverson, R. Leduc, C.Y. Lee, and J. Stroomer. Tensor product representations of general linear groups and their connections with brauer algebras. *Journal of Algebra*, 166(3):529 – 567, 1994.

[E65] Anton Cox, Maud De Visscher, Stephen Doty, and Paul Martin. On the blocks of the walled brauer algebra. *Journal of Algebra*, 320(1):169 – 212, 2008.

[E66] Charles W. Curtis and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras*. John Wiley and Sons, New York, 1988.

[E67] Matthias Christandl, Robert König, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, Mar 2007.

[E68] Constantin Candu. The continuum limit of gl(m|n) spin chains. *Journal of High Energy Physics*, 2011(7):69, Jul 2011.

[E69] Yusuke Kimura, Sanjaye Ramgoolam, and David Turton. Free particles from brauer algebras in complex matrix models. *Journal of High Energy Physics*, 2010(5):52, May 2010.

[E70] Yusuke Kimura and Sanjaye Ramgoolam. Branes, anti-branes and brauer algebras in gauge-gravity duality. *Journal of High Energy Physics*, 2007(11):078, 2007.

[E71] Y. Kimura and S. Ramgoolam. Enhanced symmetries of gauge theory and resolving the spectrum of local operators. *Phys. Rev. D*, 78:126003, Dec 2008.

[E72] T. Eggeling and R. F. Werner. Separability properties of tripartite states with $u \otimes u \otimes u$ symmetry. *Phys. Rev. A*, 63:042111, Mar 2001.

[E73] Benoit Collins, Hiroyuki Osaka, and Gunjan Sapra. On a family of linear maps from $m_n(\mathbb{C})$ to $m_{n^2}(\mathbb{C})$. *Linear Algebra and its Applications*, 555:398–411, Oct 2018.

[E74] Ivan Bardet, Benoit Collins, and Gunjan Sapra. Characterization of equivariant maps and application to entanglement detection. *Annales Henri Poincaré*, 21(10):3385–3406, Aug 2020.

[E75] Andrzej Grudka, Michał Horodecki, and Łukasz Pankowski. Constructive counterexamples to the additivity of the minimum output rényi entropy of quantum channels for allip/i&gt 2. *Journal of Physics A: Mathematical and Theoretical*, 43(42):425304, oct 2010.

[E76] Michael Brannan, Benoit Collins, Hun Hee Lee, and Sang-Gyun Youn. Temperley–lieb quantum channels. *Communications in Mathematical Physics*, 376(2):795–839, May 2020.

[E77] Ion Nechita, Clément Pellegrini, and Denis Rochette. The asymmetric quantum cloning region, arxiv: 2209.11999.

[E78] Sisi Zhou, Zi-Wen Liu, and Liang Jiang. New perspectives on covariant quantum error correction. *Quantum*, 5:521, August 2021.

[E79] Philippe Faist, Sepehr Nezami, Victor V. Albert, Grant Salton, Fernando Pastawski, Patrick Hayden, and John Preskill. Continuous symmetries and approximate quantum error correction. *Phys. Rev. X*, 10:041018, Oct 2020.

[E80] Yuxiang Yang, Yin Mo, Joseph M. Renes, Giulio Chiribella, and Mischa P. Woods. Optimal universal quantum error correction via bounded reference frames. *Phys. Rev. Res.*, 4:023107, May 2022.

[E81] Ahmed Almheiri, Xi Dong, and Daniel Harlow. Bulk locality and quantum error correction in ads/cft. *Journal of High Energy Physics*, 2015(4):163, Apr 2015.

[E82] Marco Túlio Quintino and Daniel Ebler. Deterministic transformations between unitary operations: Exponential advantage with adaptive quantum circuits and the power of indefinite causality. *Quantum*, 6:679, March 2022.

[E83] Satoshi Yoshida, Akihito Soeda, and Mio Murao. Reversing unknown qubit-unitary operation, deterministically and exactly, arxiv: 2209.02907.

[E84] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic Teleportation Scheme as a Universal Programmable Quantum Processor. *Physical Review Letters*, 101(24):240501, December 2008.

[E85] Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Physical Review A*, 79(4):042306, April 2009.

[E86] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[E87] M. A. Nielsen and Isaac L. Chuang. Programmable quantum gate arrays. *Phys. Rev. Lett.*, 79:321–324, Jul 1997.

[E88] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[E89] Harry Buhrman, Łukasz Czekaj, Andrzej Grudka, Michał Horodecki, Paweł Horodecki, Marcin Markiewicz, Florian Speelman, and Sergii Strelchuk. Quantum communication complexity advantage implies violation of a Bell inequality. *Proceedings of the National Academy of Sciences*, 113(12):3191–3196, March 2016.

[E90] Jason Pereira, Leonardo Banchi, and Stefano Pirandola. Characterising port-based teleportation as universal simulator of qubit channels. *Journal of Physics A: Mathematical and Theoretical*, 54(20):205301, apr 2021.

[E91] Stefano Pirandola, Riccardo Laurenza, Cosmo Lupo, and Jason L. Pereira. Fundamental limits to quantum channel discrimination. *npj Quantum Information*, 5:50, Jun 2019.

[E92] Marco Túlio Quintino, Qingxiuxiong Dong, Atsushi Shimbo, Akihito Soeda, and Mio Murao. Reversing unknown quantum transformations: Universal quantum circuit for inverting general unitary operations. *Phys. Rev. Lett.*, 123:210502, Nov 2019.

[E93] Michal Sedlák, Alessandro Bisio, and Mário Ziman. Optimal probabilistic storage and retrieval of unitary channels. *Phys. Rev. Lett.*, 122:170502, May 2019.

[E94] Alex May. Complexity and entanglement in non-local computation and holography. *Quantum*, 6:864, November 2022.

[E95] Matthias Christandl, Felix Leditzky, Christian Majenz, Graeme Smith, Florian Speelman, and Michael Walter. Asymptotic performance of port-based teleportation. *Communications in Mathematical Physics*, Nov 2020.

[E96] M. A. Nielsen and I. L. Chuang. Programmable Quantum Gate Arrays. *Physical Review Letters*, 79:321–324, July 1997.

[E97] Felix Leditzky. Optimality of the pretty good measurement for port-based teleportation. *Letters in Mathematical Physics*, 112(5):98, 2022.

[E98] Damián Pitalúa-García. Deduction of an upper bound on the success probability of port-based teleportation from the no-cloning theorem and the no-signaling principle. *Phys. Rev. A*, 87:040303, Apr 2013.

[E99] Zhi-Wei Wang and Samuel L. Braunstein. Higher-dimensional performance of port-based teleportation. *Scientific Reports*, 6:33004, September 2016.

[E100] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60:1888–1898, Sep 1999.

[E101] Sage. Sage documentation, version 9.2. `https://doc.sagemath.org/`, 2020.

[E102] L. Losonczi. Eigenvalues and eigenvectors of some tridiagonal matrices. *Acta Mathematica Hungarica*, 60(3):309–322, Sep 1992.

[E103] Sergii Strelchuk, Michał Horodecki, and Jonathan Oppenheim. Generalized Teleportation and Entanglement Recycling. *Physical Review Letters*, 110(1):010505, Jan 2013.

[E104] A. C. Aitken. Xxvi.– the monomial expansion of determinantal symmetric functions. *Proceedings of the Royal Society of Edinburgh. Section A. Mathematical and Physical Sciences*, 61(3):300–310, 1943.

[E105] Ron M. Adin and Yuval Roichman. Enumeration of standard young tableaux, 2014.

[E106] Andrew C. Berry. The accuracy of the gaussian approximation to the sum of independent variates. *Transactions of the American Mathematical Society*, 49(1):122–136, 1941.

[E107] Carl-Gustav Esseen. On the liapunoff limit of error in the theory of probability. *Arkiv för Matematik, Astronomi och Fysik A28*, pages 1–19, 1942.

Signed by /
Podpisano przez:

dr Michał Grzegorz
Studziński
Uniwersytet
Gdański

Date / Data:
2023-03-18 14:13