Department of Physics, Mathematics and Informatics, University of Gdańsk

PhD Thesis in Physics

Michał Studziński

Application of theory of groups and algebras representations to some quantum information processing problems

Supervisor: **prof. dr hab. Michał Horodecki**
Assistant Supervisor: **dr Jarosław Korbicz**
Institute of Theoretical Physics and Astrophysics, Gdańsk
National Quantum Information Centre in Gdańsk, Sopot

Gdańsk, 2014

Student was supported by International PhD Program: *"Physics of Future, Quantum-based Technologies"* grant MPD/2009- 3/4 sponsored by Foundation for Polish Sciences.

List of publications consist in PhD dissertation in the chronological order

A. M. Studziński, P. Ćwikliński, M. Horodecki, M. Mozrzymas, *Group representation approach to* $1 \rightarrow N$ *universal quantum cloning machines*, Physics Letters A

B. M. Mozrzymas, M. Horodecki, M. Studziński, *Structure and properties of the algebra of partially transposed permutation operators*, Journal of Mathematical Physics, **55** 032202 (2014)
`http://arxiv.org/abs/1308.2653`

C. M. Studziński, M. Horodecki, M. Mozrzymas, *Commutant Structure of* $U \otimes \ldots \otimes U \otimes U^*$ *transformations*, J. Phys. A: Math. Theor. **46** 395303 (2013)
`http://arxiv.org/abs/1305.6183`

D. P. Ćwikliński, M. Horodecki, M. Studziński, *Region of fidelities for a* $1 \rightarrow N$ *universal qubit quantum cloner*, Physics Letters A **376** pp. 2178-2187 (2012)
`http://arxiv.org/abs/1201.6077`

E. M. Czechlewski, A. Grudka, M. Horodecki, M. Mozrzymas, M. Studziński, *Distillation of Entanglement by projection on permutationally invariant subspaces*, J. Phys. A: Math. Teor. **45** 125303 (2012)
`http://arxiv.org/abs/1109.3904`

Other publised papers and e-prints in the chronological order

I. P. Ćwikliński, M. Studziński, M. Horodecki, J. Oppenheim, *Limitations for thermodynamical processing of coherences*
`http://arxiv.org/pdf/1405.5029.pdf`

II. M. Mozrzymas, M. Studziński, M. Horodecki, A. W. Harrow, M. B. Ruskai, *Explicit constructions of unitary transformations between equivalent irreducible representations*
`http://arxiv.org/pdf/1405.2169.pdf`

III. P. Ćwikliński, M. Horodecki, M. Mozrzymas, Ł. Pankowski, M. Studziński, *Local random quantum circuits are approximate polynomial-designs - numerical results*, J. Phys. A: Math. Theor. **46** 305301 (2013)
`http://arxiv.org/pdf/1212.2556.pdf`

IV. M. Studziński, M. Przybylska, *Darboux Points and Integrability Analysis of Hamiltonian Systems with Homogeneous Rational Potentials*, Physica D, **249** 1-15 (2013)
`http://arxiv.org/pdf/1205.4395.pdf`

I. MOTYWACJA ORAZ CEL PRACY

Doskonale wiadomo, że językiem fizyki jest matemtyka, ale także czymś więcej [1]. Struktury matematyczne z wielkim sukcesem używane przez fizyków nie tylko opisują przyrodę, ale także modelują jej wewnętrzną strukturę (tzw. modelowanie matematyczne). To właśnie dzięki temu niezrozumiałemu do dziś połączeniu nie tylko opisujemy otaczający nas świat, tj. mówimy jakie otaczające nas rzeczy są, ale także możemy pokusić się poprzez czyste rozważania logiczne o przewidzenie zjawisk, których nie możemy bezpośrednio zaobserwować i odczuć. To właśnie modelowanie matematyczne często mówi nam co mierzyć, które z własności możemy zaniedbać przy konstrukcji odpowiednich detektorów oraz jak powinniśmy interpretować wyniki przeprowadzanych pomiarów. W niniejszej rozprawie doktorskiej autor wraz z współpracownikami porusza cykl problemów wywodzących się z nowej dziedziny nauki jaką jest informatyka kwantowa. Poruszane są aspekty teorio-grupowego opisu maszyn klonujących, destylacji splątania a także konstrukcji nowych narzędzi matematycznych mających pomóc w wyżej wspomnianym modelowaniu matematycznym, tym razem w skali mikroświata.

Przedstawmy teraz pokrótce motywację do zajmowania się problemami kwantowego klonowania oraz destylacji splątania właśnie od strony matematycznej. Zacznijmy od kopiowania stanów kwantowych.

Z liniowości mechaniki kwantowej wiemy, że niemożliwe jest doskonałe skopiowanie nieznanego stanu kwantowego. Mówi o tym tak zwane twierdzenie o zakazie kwantowego klonowania podane po raz pierwszy przez Żurka i Wootersa [1] oraz niezależnie przez Dieksa [2]. Skoro zatem przygotowanie doskonałych klonów jest niemożliwe niejako z definicji, to postawmy pytanie inaczej. Mianowicie zapytajmy: Czy możliwe jest przygotowanie klonów, które są bliskie stanowi wejściowemu? Jeżeli tak to jak blisko możemy się zbliżyć do stanu klonowanego - jak

[1] Wspomniany problem filozoficzny nosi nazwę: "The Unreasonable Effectiveness of Mathematics in the Natural Sciences."

dobrą kopię możemy otrzymać [2]? Okazuje się, że odpowiedź na pierwsze pytanie jest twierdząca, a traktuje o tym szereg prac, m.in. [3–7]. Także na drugie z pytań potrafimy już satysfakcjonująco odpowiedzieć, zarówno dla symetrycznych, uniwersalnych maszyn klonujących [3] jak i w niedawno opublikowanych rezultatach dla asymetrycznych, uniwersalnych maszyn klonujących [4] [8–10]. Mimo znaczącego postępu teorii w tej dziedzine na przestrzeni ostatnich lat i według naszej najlepszej wiedzy nikt nie podał związków pomiędzy maszynami klonującymi a strukturą grupy symetrycznej $S(n)$. Podanie odpowiednich związków jest jednym z celów tej rozprawy doktorskiej.

Drugim fizycznym aspektem poruszanym w rozprawie doktorskiej jest destylacja splątania. Wiadomo już nie od dziś, że czyste splątanie jest jednym z najważniejszych zasobów w informatyce kwantowej, można tutaj przytoczyć chociażby klasyczne w dziedzinie prace [11–13]. Jednakże w znacznej większości praktycznych przypadków mamy dostęp do splątania mieszanego, które w ogólności nie jest już tak uniwersalne a zarazem przydatne. W celu otrzymania czystego splątania, zazwyczaj w formie maksymalnie splątanych par powinniśmy być w stanie je w jakiś sposób wydestylować z posiadanej mieszanki. Procedury, które pozwalają na takie odfiltrowanie czystego splątania są znane jako protokoły destylacji splątania kwantowego, które realizowane są poprzez operacje typu LOCC [5] [14–17]. Jeżeli dwaj obserwatorzy dzielą n kopii stanu zawierającego mieszane splątanie, a następnie wykonają na nim protokół destylacji, to jako rezultat powinni otrzymać czyste splątanie w postaci stanu bliskiego m ($m < n$) kopiom stanu maksymalnie splątanego, a granica $\lim_{n\to\infty} \frac{m}{n}$ jest nazywana wydajnością protokołu. W niniejszej rozprawie doktorskiej podajemy pewien protokół destylacji splątania, do którego opisu wykorzystujemy bardzo silne narzędzie jakim jest teo-

[2]Używając tutaj słowa "bliski" mamy tutaj na myśli miarę, którą nazywamy kwantową wiernością (ang. quantum fidelity)

[3]Kwantowe wierności wszystkich klonów obliczone względem stanu wejściowego są identyczne.

[4]Kwantowe wierności wszystkich klonów obliczone względem stanu wejściowego są w ogólności różne.

[5]ang. Local Operations and Classical Communication

ria reprezentacji grupy symetrycznej $S(n)$.

Jak widzimy z powyższego opisu głównym łącznikiem wszystkich poruszanych problemów w rozprawie doktorskiej jest teoria reprezentacji grupy symetrycznej $S(n)$ jak i pewne jej modyfikacje, o których czytelnik dowie się z dalszej części tekstu. Dlatego też, że zajmujemy się własnościami dość szczególnej klasy obiektów (grupy) warto zanim przejdziemy do streszczenia poszczególnych rezultatów zawartych w rozprawie omówić pokrótce metodologię wykorzystywaną przez autorów i problemy z jakimi musieli się oni zetknąć. Zaczniemy od zarysu znanego już przeszło pół wieku dualizmu Schura-Weyla [18] a następnie postawimy pewien problem stanowiący próbę rozszerzenia wspomnianego dualizmu na inną klasę obiektów.

Rozważmy przestrzeń Hilberta $\mathcal{H}^{\otimes n}$ opisującą n układów, przy czym zakładamy, że $\mathcal{H} \cong \mathbb{C}^d$, gdzie $d \in \mathbb{N}$ jest wymiarem każdej z kopii $\mathcal{H}$. Wiadomo, że każdy operator $X : \left(\mathbb{C}^d\right)^{\otimes n} \to \left(\mathbb{C}^d\right)^{\otimes n}$, który komutuje z operacjami unitarnymi typu $U^{\otimes n}$, tj. spełnia relację

$$\left[X, U^{\otimes n}\right] = 0, \tag{1}$$

może być przedstawiony jako pewna kombinacja liniowa operatorów permutacji $\mathrm{V}(\sigma)$:

$$X = \sum_{\sigma \in S(n)} a(\sigma)\, \mathrm{V}(\sigma), \tag{2}$$

gdzie $a(\sigma)$ dla $\sigma \in S(n)$ są pewnymi, znanymi współczynnikami kombinacji, a operatory permutacji $\mathrm{V}(\sigma)$ działają na wektory bazowe $|e_{i_1}\rangle \otimes \cdots \otimes |e_{i_n}\rangle$ przestrzeni $\mathcal{H}^{\otimes n}$ następująco:

$$\forall \sigma \in S(n) \quad \mathrm{V}(\sigma)|e_{i_1}\rangle \otimes \cdots \otimes |e_{i_n}\rangle = |e_{i_{\sigma^{-1}(1)}}\rangle \otimes \cdots \otimes |e_{i_{\sigma^{-1}(n)}}\rangle. \tag{3}$$

Zatem, aby poznać nieprzywiedlne komponenty operatora X wystarczy poznać nieprzywiedlne komponenty każdego z operatorów $\mathrm{V}(\sigma)$ oddzielnie. W tym momencie z pomocą przychodzi teoria reprezentacji. Mianowicie już od dawna istnieje dobrze opracowana teoria pozwalająca efektywnie znajdować nieprzywiedlne reprezentacje operatorów $\mathrm{V}(\sigma)$.

Mówiąc dokładniej, za każdym razem gdy mamy do czynienia z zagadnieniem, gdzie operator X posiada własność opisaną równaniem (1) możemy posłużyć się teorią reprezentacji aby sprowadzić zagadnienie do badania operatorów $\mathrm{V}(\sigma)$ w postaci blokowo-diagonalnej, tj.

$$\mathrm{V}(\sigma) = \bigoplus_{\lambda} \mathrm{V}_{\lambda}(\sigma), \tag{4}$$

gdzie suma prosta przebiega po wszystkich nieprzywiedlnych reprezentacjach λ grupy symetrycznej $S(n)$.

Idąc dalej możemy posłużyć się dualizmem Schura-Weyla [18], który to stwierdza dualność pomiędzy nieredukowalnymi reprezentacjami grupy symetrycznej oraz pełnej grupy liniowej [6]. Dzięki wspomnianemu dualizmowi każdy ze składników sumy prostej (4) można zapisać jako

$$\mathrm{V}_{\lambda}(\sigma) = \mathbb{1}_{\lambda}^{\mathcal{U}} \otimes \mathrm{V}_{\lambda}^{\mathcal{S}}(\sigma), \tag{5}$$

gdzie symbol $\mathcal{U}$ oznacza część operatora działającą na przestrzeni unitarnej natomiast $\mathcal{S}$ na przestrzeni symetrycznej. Z równania (5) widzimy, że dodatkowo każdy składnik $\mathrm{V}_{\lambda}(\sigma)$ ma strukturę tensorową, przy czym nietrywialna część działa jedynie na tak zwanej części symetrycznej. Zatem, aby poznać nieprzywiedlne reprezentacje operatora X wystarczy poznać nieprzywiedlne reprezentacje każdej z części $\mathrm{V}_{\lambda}^{\mathcal{S}}(\sigma)$, gdzie krotności określone są jako wymiar operatora $\mathbb{1}_{\lambda}^{\mathcal{U}}$. Sposób budowy części symetrycznej a mówiąc dokładniej reprezentacji macierzowych $\mathrm{V}_{\lambda}^{\mathcal{S}}(\sigma)$ jest dany dzięki konstrukcji Younga-Yamanouchiego [19].

Możemy się teraz zapytać, co się stanie z przedstawioną wyżej konstrukcją jeżeli nasz operator X będzie niezmienniczy ze względu na transformacje typu $U^{\otimes(n-k)} \otimes U^{*\otimes k}$, to znaczy gdy

$$\left[X, U^{\otimes(n-k)} \otimes U^{*\otimes k}\right] = 0, \tag{6}$$

gdzie $*$ oznacza sprzężenie zespolone. Okazuję się wtedy, że ów operator X może być przedstawiony nadal jako kombinacja liniowa operatorów permutacji $\mathrm{V}(\sigma)$ tyle, że częściowo transponowanych po k ostatnich

[6] Czytelnik zauważy, że w niniejszej rozprawie interesujemy się tylko pewną podgrupą grupy $\mathrm{GL}(n, \mathbb{C})$, a mianowicie grupą macierzy unitarnych $\mathrm{U}(n, \mathbb{C})$.

układach [7]

$$X = \sum_{\sigma \in S(n)} b(\sigma)\, \mathrm{V}^{\Gamma_k}(\sigma), \qquad \Gamma_k = T_{n-k+1} \cdots T_n, \tag{7}$$

gdzie T_i dla $n-k+1$ i n oznacza standardową transpozycję na $i-$tym podukładzie.

W niniejszej rozprawie ograniczamy się do najprostszego, ale nietrywialnego przypadku, gdy $k=1$, czyli gdy częściowa transpozycja działa tylko na ostatnim $n-$tym podukładzie. Zatem naszym zadaniem jest znalezienie rozkładu operatorów $\mathrm{V}^{T_n}(\sigma)$ podobnie jak w równaniach (5), (6) a także podanie konstrukcji ich nieredukowalnych reprezentacji macierzowych (podrozdział c).

Posiadając już umiejętność rozkładu operatorów odpowiednio z równania (2) oraz (7) na nieprzywiedlne komponenty wraz z ich reprezentacjami macierzowymi możemy stosować je jak to jest wyjaśnione dokładniej w następnym rozdziale do teoriogrupowego oraz algebraicznego opisu maszyn klonujących (podrozdziały a, b) czy obliczeń wydajności pewnego protokołu destylującego splątanie (podrozdział d).

II. OMÓWIENIE WYNIKÓW PRAC SKŁADAJĄCYCH SIĘ NA ROZPRAWĘ

Prace składające się na rozprawę doktorską, tj. artykuły z pozycji [A-E] można zasadniczo podzielić na trzy grupy. Pierwsza grupa, czyli pozycje [E] oraz [D] wykorzysują klasyczne już elementy wiedzy z teorii reprezentacji grup skończonych ze szczególnym naciskiem na grupę symetryczną (permutacji) $S(n)$ do takich problemów jak destylacja splątania poprzez projekcje na permutacyjnie nizemiennicze podprzestrzenie czy teoriogrupowy opis uniwersalnej, kubitowej [8] maszyny klonującej. Druga grupa artykułów z pozycji [C], [B] zawiera konstrukcję nieredukowalnych reprezentacji częściowo transponowanych operatorów permutacji uogólniające i rozszerzające istniejącą już wiedzę na temat ope-

[7] Warto tutaj dodać komentarz, że założenie sprzężenia k ostatnich operacji U nie zminiejsza ogólności problemu. Zawsze możemy dokonać takiej permutacji aby uzyskać żądaną postać.

[8] ang. qubit od quantum bit, bit kwantowy; kubit jest to kwantowomechaniczny układ opisany dwuwymiarową przestrzenią Hilberta

ratorów permutacji. Wreszcie ostatnia praca z serii składającej się na rozprawę, tj. pozycja [A] stosuje wcześniej wypracowane narzędzia matematyczne z prac [C] oraz [B] do rozszerzenia rezultatów z [D] dla wyżej wymiarowych przypadków. Omówmy teraz pokrótce rezultaty zawarte w wyżej wymienionych pracach zaczynając od problemu kwantowego klonowania, zarówno dla kubitów jak i kuditów (podrozdziały a,b), poprzez omówienie konstrukcji nowych narzędzi matematycznych (podrozdział c) i kończąc na pewnym problemie matematycznym związanym z destylacją splątania (podrozdział d).

a. **Teoriogrupowy opis uniwersalnych, kubitowych maszyn klonujących** W pracy [D] prezentujemy teoriogrupowe podejście do problemu w przypadku gdy stanami klonowanymi są kubitowe stany maksymalnie splątane, na przykład jeden ze stanów Bella postaci [9]:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{8}$$

Głównym celem artykułu [D] jest opisanie w sposób analityczny dopuszczalnego obszaru wierności (ang. fidelity) uniwersalnej, kubitowej maszyny klonującej [10] $1 \to N$ wynikającego z praw mechaniki kwantowej przy zastosowaniu teorii reprezentacji grupy symetrycznej $S(n)$. Mówiąc dokładniej chcemy poznać analityczne ograniczenia na następujące wielkości:

$$F_{1i} \equiv F\left(\Phi^+, \mathrm{Tr}_{\overline{1i}}\,\rho_{1\ldots n}\right) = \mathrm{Tr}\left[\sqrt{\sqrt{\Phi^+}\,\mathrm{Tr}_{\overline{1i}}\,\rho_{1\ldots n}\sqrt{\Phi^+}}\right], \tag{9}$$

gdzie $\Phi^+ = |\psi^+\rangle\langle\psi^+|$, wielkość $\rho_{1\ldots n}$ jest łącznym stanem po zastosowaniu maszyny klonującej a $\mathrm{Tr}_{\overline{1i}}\,\rho_{1\ldots n}$ stanem zredukowanym $i-$tej kopii [11]. Do analizy problemu wykorzystywane są informacje opisane pokrótce w pierwszym rozdziale ninijeszego streszczenia (rozdział I). Okazuje się, że w przypadku dwuwymiarowym (kubitowym) singletowe stany maksymalnie splątane (patrz równanie (8)) są $U \otimes U$ niezmiennicze. Pozwala nam to na zapisanie łącznego stanu po zastosowaniu maszyny

[9] Oczywiście za punkt wyjścia możemy wziąć także inny stan Bella

[10] W całej rozprawie stosujemy następującą konwencję: Liczbę kopii oznaczamy wielką literą N, przy czym $n = N + 1$, gdzie n jest stopniem grupy symetrycznej $S(n)$.

[11] Poprzez $\mathrm{Tr}_{\overline{1i}}\,\rho_{1\ldots n}$ oznaczamy ślad częściowy po wszystkich układach poza pierwszym oraz $i-$tym.

klonującej jako

$$\rho_{1\ldots n} = \bigoplus_{\lambda} \mathbb{1}^{\mathcal{U}}_{r(\lambda)} \otimes \widetilde{\rho}^{\lambda}, \tag{10}$$

który to również jest unitarnie niezemienniczy ze względu na transformacje unitarne typu $U^{\otimes n}$. W równaniu (10) przez $r(\lambda)$ oznaczyliśmy wymiar nieprzywiedlnej reprezentacji odpowiadającej podziałowi λ, natomiast $\widetilde{\rho}^{\lambda}$ jest odpowiednią nieprzywiedlną reprezentacją operatora ρ. Dzięki tej własności dalej pokazujemy, że obliczanie kwantowej wierności F_{1i} pomiędzy kubitowym stanem wejściowym ρ a $i-$ tą kopią może być sprowadzone do obliczania wierności na każdej z niezmienniczych permutacyjnie podprzestrzeni wynikającej z rozkładu operatorów permutacji $\mathrm{V}(\sigma)$ na nieprzywiedlne komponenty (Lemat 1):

$$F_{1i} = \sum_{\lambda} F^{\lambda}_{1i}, \quad \text{gdzie} \quad F^{\lambda}_{1i} = \frac{1}{2} - \frac{1}{2}\,\mathrm{Tr}\left(\rho^{\lambda}\, \mathrm{V}^{S}_{\lambda}(1i)\right), \tag{11}$$

gdzie $\mathrm{V}^{S}_{\lambda}(1i)$ oznacza nieredukowalną reprezentację operatora permutacji $\mathrm{V}(\sigma)$, gdy $\sigma = (1i)$. Kolejnym ważnym wynikiem otrzymanym na drodze dalszych rozważań było zauważenie, że do otrzymania całego dozwolonego zakresu działania maszyny klonującej niezbędne jest wzięcie otoczki wypukłej ze zbioru wierności obliczonych dla wszystkich możliwych kopii $1 < i \ \ n$ oraz reprezentacji λ (Twierdzenie 1)

$$\mathcal{F} = \mathrm{conv}\left(\bigcup_{\lambda}\left\{\left(F^{\lambda}_{12}, \ldots, F^{\lambda}_{1n}\right) \ : |\psi\rangle \in \mathbb{C}^{d_{\lambda}} \ \right\}\right). \tag{12}$$

Główna część pracy kończy się dowodem Lematu 3, który stwierdza, że do wygenerowania otoczki opisanej Twierdzeniem 1 potrzeba i wystarcza rozważać czyste stany rzeczywiste. Mówiąc inaczej pokazaliśmy pewnego rodzaju majoryzację stanów zespolonych poprzez stany rzeczywiste w sensie wierności dla tego przypadku maszyn kolnujących. W artykule dodatkowo zamieszczone są reprezentacje graficzne dozwolonego zakresu wierności w przypadku uniwersalnej maszyny klonującej $1 \to 3$ zarówno dla każdej z nieredukowalnych reprezentacji (Rysunek 2) jak także po wygenerowaniu otoczki wypukłej (Rysunek 3). Pokazano również jak można zastosować opisaną w tym rozdziale metodę do odtwarzania stanów kwantowych o z góry zadanych więzach na wierności, oczywiście w ramach dozwolonych przez teorię (Rozdział VF).

b. **Algebraiczny opis uniwersalnych maszyn klonujących** Praca [A] jest rozszerzeniem wyników z pracy [D] na przypadek gdy stanem wejściowym, przeznaczonym do klonowania jest kuditowy [12] stan maksymalnie splątany

$$|\psi^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|ii\rangle, \tag{13}$$

gdzie d jest wymiarem przestrzeni Hilberta na której opisujemy nasz stan.

Okazuję się, że w tym przypadku, gdy $d > 2$ nie możemy zastosować bezpośrednio znanych narzędzi z teorii reprezentacji grupy symetrycznej $S(n)$ jak to miało miejsce w przypadku kubitowym. Wynika to z faktu, że stany z równania (13) dla $d > 2$ nie są już $U \otimes U$ niezmiennicze tylko $U^* \otimes U$ niezmiennicze [13]. Inna symetria w wyżej wymiarowym przypadku powoduje, że stan łączny $\rho_{1\ldots n}$ po zastosowaniu maszyny klonującej jest niezmienniczy na operacje typu $U^* \otimes U^{\otimes(n-1)}$. Chcąc nadal dysponować reprezentacyjnym wyjaśnieniem zagadnienia niezbędna staje się znajomość nieredukowalnych reprezentacji algebry [14] częściowo transponowanych operatorów permutacji $\mathrm{V}^{T_n}(\sigma)$. Oczywisty staje się teraz fakt, że kluczową rolę odgrywają narzędzie matematyczne o których mowa w podrozdziale c) niniejszego streszczenia. Autorzy w pracy [D] pokazują, że wierności pomiędzy stanem wejściowym a dowolnym z klonów można zapisać poprzez nieprzywiedlne reprezentacje częściowo transponowanych operatorów permutacji $\mathrm{V}^{T_n}_{\alpha}(k-1\ n)$, gdzie $1 < k \ \ n$ otrzymanych w [C], [B] oraz operatora gęstości ρ^{α} działającego na odpowiedniej nieprzywiedlnej podprzestrzeni oznaczonej podziałem α. Mianowicie zachodzi (Lemat 1):

$$F^{\mathcal{M}}_{1k} = \sum_{\alpha} F^{\alpha}_{1k}, \quad \text{gdzie} \quad F^{\alpha}_{1k} = \frac{1}{d}\operatorname{Tr}\left[\rho^{\alpha}\,\mathrm{V}^{T_n}_{\alpha}(k-1\ n)\right], \tag{14}$$

---

[12]ang. qudit, jest to kwantowomechaniczny układ opisywany na d wymiarowej przestrzeni Hilberta

[13]Przez $*$ oznaczmy sprzężenie zespolone.

[14]Czytelnik zwróci uwagę na fakt, że zbiór operatorów permutacji tworzy grupę, czyli w szczególności każdy element posiada swoją odwrotność. Natomiast zbiór częściowo transponowanych operatorów permutacji tworzy już tylko algebrę, tzn. istnieją elementy dla których odwrotność nie istnieje.

gdzie d oznacza wymiar całkowitej przestrzeni Hilberta $\mathcal{H}$. Należy przy tym zwrócić uwagę na fakt, że celowo wprowadzamy tutaj indeks α a nie λ jak w przypadku kubitowym aby odróżnić odpowiednie reprezentacje. Z prac [B] oraz [C] wynika rozbicie algebry $\mathcal{A}_n^{t_n}(d)$ na sumę dwóch przestrzeni $\mathcal{M}$ oraz $\mathcal{A}_{n-1}(d)$, przy czym wzory (14) opisują wierności obliczone dla elementów z ideału $\mathcal{M}$. W przypadku ideału $\mathcal{A}_{n-1}(d)$ formuła na wierności redukuje się do prostego wyrażenia

$$F_{1k}^{\mathcal{N}} = \frac{1}{d}. \tag{15}$$

Dalej podobnie jak dla przypadku kubitowego autorzy pokazują, że do otrzymania dozwolonego zakresu wierności w przypadku $1 \to N$ uniwersalnej kuditowej maszyny klonującej niezbedne jest wzięcie otoczki wypukłej ze zbioru wierności obliczonych dla wszystkich możliwych kopii $1 < i \quad n$ oraz reprezentacji α (Twierdzenie 3) oraz fakt, że nadal zachodzi majoryzacja w sensie wierności stanów zespolonych poprzez stany rzeczywiste (Lemat 4).

c. **Nieredukowalne reprezentacje częściowo transponowanych operatorów permutacji** Na tą część rozprawy doktorskiej składają się dwie prace z pozycji [C] oraz [B]. Przedstawiają one dwa równoważne podejścia do tego samego problemu, a mianowicie do znalezienia nieprzywiedlnych reprezentacji algebry $A_n^{T_n}(d)$ częściowo transponowanych operatorów permutacji $V^{T_n}(\sigma)$ o których mowa we wstępie do niniejszego streszczenia.

Mimo, że obydwa artykuły podejmują te samo zagadnienie to jak się przekonamy później dają całkowicie różny wgląd w strukturę problemu, a także artykuł [B] jest istotnym poszerzeniem rezultatów z pracy [C] m.in. na niskowymiarowe przypadki oraz explicite łączy badaną strukturę algebry z reprezentacją pewnej grupy indukowanej. Przybliżmy teraz w paru zdaniach problemy z jakimi musieli zetknąć się autorzy w wyżej wymienionych pracach. Zacznijmy od pozycji [C].

W artykule tym wychodzimy z poziomu przestrzeni Hilberta i budowy bazy wektorowej rozpinającej każdą z nieredukowalnych podprzestrzeni (Definicja 4). Pozwala nam to na budowę nieortogonalnej bazy operatorowej w iloczynie Hilberta-Schmidta (Definicja 5, Lemat 8). Na tym etapie rozważań kluczowe było spostrzeżenie, że istnieje pewien zbiór funkcji $\mathcal{F}^t_{ab}$, który wiąże nam elementy algebry $\mathbb{C}[S(n-2)]$ z elementami algebry $\mathcal{M}$

$$\mathbb{C}[S(n-2)] \ni \mathrm{V}(\sigma) \xmapsto{\mathcal{F}^t_{ba}} \mathrm{V}'(\sigma_{ab}) \in \mathcal{M}, \tag{16}$$

Z liniowości przekształceń $\mathcal{F}^t_{ab}$ wiemy natomiast, że prawdziwe jest

$$\mathbb{C}[S(n-2)] \ni \mathrm{E}^{\alpha}_{ij} \xmapsto{\mathcal{F}^t_{ba}} v^{ab}_{ij}(\alpha) \in \mathcal{M}, \tag{17}$$

gdzie operatory E^{α}_{ij} są dobrze znanymi operatorami Wignera dla grupy symetrycznej $S(n-2)$. Powyższe równania implikują nam bezpośrednio Twierdzenie 9, które jest jednym z kluczowych w całej pracy. A mianowicie mówi nam ono jak wyrażają się częściowo transponowane operatory permutacji poprzez naszą nieortogonalną bazę operatorową i vice versa oraz pozwala nam udowodnić zasady działanie $\mathrm{V}^{T_n}(\sigma)$ na naszą operatorową bazę.

Niestety jak to wspomnieliśmy wyżej baza nasza jest nieortogonalna co nie pozwala nam wyznaczyć reprezentacji macierzowych operatorów $\mathrm{V}^{T_n}(\sigma)$ w formie takiej do jakiej to przywykliśmy pracować w fizyce. W celu obejścia tego problemu a raczej przedefiniowania naszej bazy używamy macierzy $Q(\alpha)$ (Definicja 11), która to jest macierzą Grama wektorów bazowych z definicji 4. Macierz ta jest macierzą blokowo-diagonalną posiadającą wiele interesujących cech, które determinują naszą dalszą drogę w kierunku bazy ortogonalnej. Mianowicie, bloki macierzy $Q(\alpha)$ są macierzowymi reprezentacjami odpowiednich transpozycji (patrz Definicja 11, Spostrzeżenie 12) a i co najważniejsze, ponieważ jest to macierz Grama zdarzyć się może, że dla pewnych relacji pomiędzy wymiarem d przestrzeni Hilberta a liczbą n podukładów zbiór wektorów stanie się liniowo zależny a co za tym idzie macierz $Q(\alpha)$ nie będzie już dłużej odwracalna. Mówi nam o tym Twierdzenie 13, które stwierdza m.in., że kiedy tylko $d > n-2$ macierz Grama zawsze posiada swoją odwrotność. Z kolei pozwala nam to na wspomniane już wcześniej przedefiniowanie bazy operatorowej na nową bazę, już ortogonalną w iloczynie Hilberta-Schmidta właśnie poprzez odwrotność macierzy $Q(\alpha)$ (dokładne sformułowanie znajduje się w definicji 14). Stąd już tylko krok od znalezienia lewego działania już ortogonalnych operatorów bazowych na operatory $V^{T_n}(\sigma)$ (Wniosek 16) a co za tym idzie wyznaczenia elementów macierzowych szukanych niredukowalnych reprezentacji (Lemat 18).

Praca [C] porusza także problem przypadku gdy $d \quad n-2$ (Rozdział IV.B) jednak nie daje wyczerpującej odpowiedzi w języku bazy wektorowej w przestrzeni Hilberta. Autorzy pokazują tam, że do konstrukcji nieprzywiedlnych reprezentacji potrzeba i wystarcza wybrać ze zbioru wektorów liniowo zależnych podzbiór liniowo niezależny a następnie przeprowadzić rozumowanie jak dla przypadku $d > n-2$. Powoduje to oczywiste zmniejszenie się wymiaru tych operatorów bazowych, które działają na nowej "zredukowanej" podprzestrzeni (Przykład 19). Niestety jednak nie jest tam podany przepis w jaki sposób efektywnie przeprowadzić wybór odpowiednich wektorów i jak połączyć go z globalnymi własnościami algebry $A_n^{T_n}(d)$.

Inne podejście do tego samego problemu budowania nieprzywiedlnych reprezentacji operatorów $V^{T_n}(\sigma)$ a zarazem pokrywające lukę przypadku małych wymiarów d w stosunku do liczby podukładów n daje praca [B]. W pracy tej autorzy traktują algebrę $A_n^{T_n}(d)$ w sposób abstrakcyjny oraz korzystają z zaawansowanych technik algebraicznych. Najważniejszą cechą tej pracy było zauważenie, że algebra $A_n^{T_n}(d)$ zawiera podalgebrę $A_{n-1}(d)$ generowaną poprzez operatory reprezentujące podgrupę $S(n-1) \subset S(n)$, które nie są deformowane poprzez częściową transpozycję T_n. Pozwoliło to na następujące rozbicie algebry $A_n^{T_n}(d)$ na sumę dwóch podprzestrzeni

$$A_n^{t_n}(d) = \mathcal{M} + A_{n-1}(d), \tag{18}$$

gdzie podprzestrzeń $\mathcal{M}$ jest ideałem generowanym poprzez operatory $V^{T_n}(\sigma)$, gdy permutacja σ działa na n w sposób nietrywialny. Dodatkowo elementy generujące ideał $\mathcal{M}$ są nieodwracalne co pokazuje jak dodanie nawet jednej częściowej transpozycji zmienia strukturę problemu. Innym bardzo ważnym rezultatem zawartym tym artykule [B] jest powiązanie struktury badanej algebry ze strukturą reprezentacji indukowanej $\operatorname{ind}_{S(n-2)}^{S(n-1)}(\varphi^{\alpha})$ grupy $S(n-1)$ indukowanej poprzez nieprzywiedlne reprezentacje φ^{α} grupy $S(n-2)$ (Rozdział IV). Dokładniej mówiąc autorzy pokazują, że wszystkie wartości własne macierzy $Q^{ab}_{ij}(\alpha)$ są indeksowane właśnie poprzez nieprzywiedlne komponenty $\mathrm{ind}^{S(n-1)}_{S(n-2)}(\varphi^\alpha)$ a ich krotność jest równa wymiarowi takiej reprezentacji (Twierdzenie 31). W kolejnym, piątym rozdziale przedstawiona jest konstrukcja nieredukowalnych reprezentacji operatorów $\mathrm{V}^{T_n}(\sigma)$. Punktem wyjścia dla dalszych badań jest zdefiniowanie zbioru generatorów $\{u(\alpha)\}$ ideału $\mathcal{M}$ (Definicja 39) wraz z prawem ich składania oraz postacią lewego działania na operatory $\mathrm{V}^{T_n}(\sigma)$ (Wniosek 43). Dalej podobnie jak w [C] autorzy przechodzą do nowego zbioru generatorów, który posiada już wymaganą własność ortogonalności (Definicja 48) a także podają szukane formuły na elementy macierzowe nieredukowalnych reprezentacji operatorów $\mathrm{V}^{T_n}(\sigma)$ (Wniosek 51) korzystając z faktów wyprowadzonych dla generatorów $u(\alpha)$. Istotnym punktem tej pracy, w znacznym stopniu poszerzającym dokonania autorów z [C] jest opisanie przypadku $\det Q(\alpha) = 0$, czyli gdy macierz $Q(\alpha)$ nie posiada macierzy odwrotnej. Oznacza to tyle, że część generatorów $u(\alpha)$ jest liniowo zależna. Autorzy prezentują uniwersalną konstrukcję (Twierdzenie 77), która prowadzi do tak zwanej zredukowanej bazy dającej konstruktywny opis zarówno w przypadku generatorów liniowo zależnych jak i może być wykorzystana do opisu przypadku generycznego, gdy rząd macierzy $Q(\alpha)$ jest maksymalny. Wynik ten opiera się na diagonalizacji rozważanej już wcześniej macierzy $Q(\alpha)$ (Twierdzenie 59) a następnie wykorzystanie macierzy diagonalizującej do budowy nowego, obejmującego już przypadek niegeneryczny zbioru generatorów. Okazuję się, że jeżeli tylko $\det Q(\alpha) = 0$ to dla jednej i tylko jednej (z dokładnością do krotności) nieredukowalnj reprezentacji grupy $S(n-2)$ pojawiającej się w $\mathrm{ind}^{S(n-1)}_{S(n-2)}(\varphi^\alpha)$ odpowiadaja zerowa wartość własna $Q(\alpha)$. Wtedy również generatory odpowiadające tej zerowej wartości własnej są operatorami zerowymi a pozostałe tworzą wyżej wspomnianą bazę zredukowaną. Na zakończenie warto dodać, że w pracy tej pokazano również relatywnie prosty algorytm przy tej klasie złożoności problemu do znajdowania wszystkich wartości własnych macierzy $Q(\alpha)$ i "odrzucania" generatorów liniowo zależnych (Dodatek A) oparty na twierdzeniu Frobeniusa [18]. Dzięki temu otrzymujemy pełny opis algebry $A_n^{t_n}(d)$ z konstrukcją nieredukowlanych komponentów, dyskujsą wszelkich dodatkowych jej własności wraz z jawnym wyeksponowaniem struktury grupy indukowanej.

d. **Destylacja splątania kwantowego poprzez projekcje na permutacyjnie niezmiennicze podprzestrzenie** W artykule [E] przedmiotem rozważań był problem destylacji kwantowego splątania ze stanu dwukubitowego, który był mieszanką dwóch czystych stanów splątanych i jednego stanu produktowego, prostopadłego do wcześniej wspomnianych stanów splątanych:

$$\rho_{AB} = x\rho'_{AB} + (1-x)|01\rangle\langle 01|_{AB}, \quad x \in [0,1], \tag{19}$$

gdzie stan ρ'_{AB} jest w ogólności nierówną mieszanką stanów postaci

$$|\Phi^{\pm}(p)\rangle_{AB} = \sqrt{p}|00\rangle_{AB} \pm \sqrt{1-p}|11\rangle_{AB}, \quad p \in [0,1]. \tag{20}$$

W rozważaniach zakładamy, że n kopii stanu ρ_{AB} jest współdzielone pomiędzy dwie osoby, zwyczajowo nazywane Alicją (dolny indeks A) i Bobem (dolny indeks B). Po zaaplikowaniu odpowiedniego protokołu destylującego splątanie ([E], rozdział II) zadanie polegało na dostarczeniu analitycznych formuł na wartości własne operatora gęstości po odpowiednim pomiarze wynikającym z budowy protokołu. Wspomniany stan po pomiarze ma następującą formę:

$$\rho_{lAB}^{(n)} = \frac{P_{lA} \otimes P_{lB} \rho_{AB}^{\otimes n} P_{lA} \otimes P_{lB}}{\mathrm{Tr}(P_{lA} \otimes P_{lB} \rho_{AB}^{\otimes n} P_{lA} \otimes P_{lB})}, \tag{21}$$

gdzie n oznacza ilość kopii stanu ρ_{AB} współdzielonych przez wykonawców protokołu Alicję i Boba. Projektory P_{lA}, P_{lB} rzutują na podprzestrzenie $\mathcal{H}_l^{(n)}$ przestrzeni $\left(\mathbb{C}^2\right)^{\otimes n}$ rozpiętej przez wektory bazy standardowej o wadze Hamminga równej l, tj. wektory zawierające l jedynek oraz $n-l$ zer. Przykładem kanonicznym takiego wektora jest $|\underbrace{0\ldots0}_{n-l}\underbrace{1\ldots1}_{l}\rangle$. Znajomość spektrum operatora stanu $\rho_{lAB}^{(n)}$ pozwalało na obliczenie wydajności protokołu destylującego R_i, która jest proporcjonalna do informacji koherentnej [15] $I_c\left(\rho_{lAB}^{(n)}\right)$. Dalej okazało się, że macierz gęstości $\rho_{AB}^{(n)}$

[15] ang. coherent information

może być przedstawiona jako kombinacja liniowa operatorów $A_k^{(l)}$ działających na podprzestrzeniach $\mathcal{H}_l^{(n)}$ rozpiętych przez wektory o ustalonej liczbie jedynek l (Lemat 1). Zatem znajomość wartości własnych wszystkich operatorów $A_k^{(l)}$ gwarantuje znajomość spektrum operatora gęstości $\rho_{lAB}^{(n)}$. Drugą ważną obserwacją na drodze do rozwiązania problemu jest spostrzeżenie, że przestrzenie $\mathcal{H}_l^{(n)}$ są niezmiennicze ze względu na działanie grupy permutacji $S(n)$. Fakt ten pozwala zapisać przestrzeń $\mathcal{H}_l^{(n)}$ jako sumę prostą nieredukowalnych podprzestrzeni indeksowanych diagramami Younga o maksymalnie dwóch wierszach (Lemat 4). Fakt ten oraz pewne teorio-grupowe oraz dość skomplikowane kombinatoryczne rozważania zawarte w m.in. propozycji 3, lematach 5 oraz 6 pozwala dowieść formuły (41) z twierdzenia 1 podającej analityczny przepis na obliczanie wartości własnych operatorów $A_k^{(l)}$ a co za tym idzie poznać spektrum operatora $\rho_{lAB}^{(n)}$.

III. DALSZE PERSPEKTYWY

Na zakończenie niniejszego streszczenia rozprawy doktorskiej warto wspomnieć o dalszych możliwych kierunkach badań, które to są kontynuacją niektórych koncepcji tutaj omawianych. Pierwszym, najbardziej oczywistym kierunkiem dalszych prac jest poszukiwanie nieredukowalnych reprezentacji częściowo transponowanych operatorów permutacji $V^{\Gamma_k}(\sigma)$ w przypadku większej liczy transpozycji niż jedna jak to miało miejsce w pracach [C] oraz [D]. Zakładamy zatem, że częściowa transpozycja ma postać $\Gamma_k = T_{n-k+1} \circ \cdots \circ T_n$, przy czym T_i dla $n-k+1 \quad i \quad n$ oznacza standardową transpozycję na $i-$tym podukładzie. Ewentualnie otrzymany wynik poszerzy nie tylko teorię reprezentacji na nową klasę obiektów, ale także może znaleźć ciekawe zastosowania w problemach informatyki kwantowej. Wspomnimy tutaj krótko o dwóch możliwych.

Zacznijmy od możliwości opisu uniwersalnych maszyn klonujących $N \to M$, gdy mamy N stanów wejściowych oraz M klonów (oczywiście mamy $M < N$ oraz $M + N = n$). Tematem badań byłoby podobnie jak w przypadku prac [A,D] podanie analitycznych formuł na dopuszczalny zakres wierności wynikający z mechaniki kwantowej w ujęciu teorii reprezentacji algebr.

Drugim znacznie bardziej złożonym zadaniem byłoby zastosowanie wypracowanych narzędzi matematycznych do problemu addytywności kanałów kwantowych. Znajmość nieredukowalnych reprezentacji operatorów $V^{\Gamma_k}(\sigma)$ pozwoli na otrzymanie analitycznych formuł na entropię Rényiego dla dwóch kopii kanału określonego na permutacyjnie niezmienniczych podprzestrzeniach wynikających z dualizmu Schura-Weyla dla dowolnej liczby podukładów i wymiaru lokalnej przestrzeni Hilberta d. To z kolei pozwoli stwierdzić dla których podprzestrzeni oraz przy jakiej kombinacji parametrów zachodzi wspomniane łamanie addytywności.

data i podpis doktoranta

[1] W.K. Wooters and W. H. Żurek, Nature **299**, 802 (1982).

[2] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[3] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[4] D. Bruß, D. P. DiVincenzo, A. Eckert, C. A. Fuchs, C. Macchiavello and J. A. Smolin Phys. Rev. A **57**, 2368 (1998).

[5] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[6] N. J. Cerf J. Mod. Opt. **47**, 187 (2000).

[7] S. Iblisdir, A. Acin, N.J. Cerf, R. Filip, J. Fiurasek and N. Gisin Phys. Rev. A **72**, 042328 (2005).

[8] R. F. Werner Phys. Rev. A **58**, 1827 (1998).

[9] A. Kay, D. Kaszlikowski and R. Ramanathan Phys. Rev. Lett. **103**, 050501 (2009).

[10] A. Kay, R. Ramanathan and D. Kaszlikowski Quant. Inf. Comp. **13**, 0880 (2013).

[11] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[12] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[13] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[14] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[16] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[17] W. Dür and H. J. Briegel, Rep. Prog. Phys. **70**, 1381 (2007).

[18] W. Fulton and J. Harris, *Representation Theory - A First Course* (Springer-Verlag, New York, 1991).

[19] J. Q. Chen, J. Pingand F. Wang *Group Representation Theory for Physicists* (World Scientific, New York, 2002).