

Dr hab. Marek Czachor, prof. nadzwyczajny PG
Katedra Fizyki Teoretycznej i Informatyki Kwantowej
Wydział Fizyki Technicznej i Matematyki Stosowanej
Politechnika Gdańska

Autoreferat

I. Życiorys

Urodziłem się 30 marca 1960 r. w Słupsku. Studia na „fizyce nienauczycielskiej” rozpocząłem na Uniwersytecie Gdańskim w 1979 r. W stanie wojennym, jako student III roku, zostałem skazany przez Sąd Marynarki Wojennej w Gdyni na trzy lata pozbawienia wolności, co efektywnie przedłużyło moje studia o dwa lata. W październiku 1986 r. obroniłem pracę magisterską na temat hamiltonowskich równań falowych (promotor dr A. Posiewnik). W listopadzie 1987 r. zatrudniłem się na Politechnice Gdańskiej na etacie technicznym (specjalista). W związku z ponownym aresztowaniem, zostałem zwolniony z PG przed wygaśnięciem trzymiesięcznego okresu próbnego. Do pracy na PG przywrócony zostałem dopiero jesienią 1990 r. na mocy wyroku Naczelnego Sądu Administracyjnego, który uznał, iż w 1987 r. zwolniono mnie na skutek represji politycznych i z pogwałceniem prawa.

W lutym 1991 r. rozpocząłem studia doktoranckie w Instytucie Fizyki PAN w Warszawie, pracując pod kierunkiem prof. Kazimierza Rzażewskiego. Doktorat na temat nieliniowej mechaniki kwantowej obroniłem w maju 1994 r. Habilitację pt. „Uogólnione równania von Neumanna” obroniłem z wyróżnieniem w czerwcu 2000 r. na Wydziale Fizyki Uniwersytetu Warszawskiego. Od 2004 r. zatrudniony jestem na Politechnice Gdańskiej na stanowisku profesora nadzwyczajnego PG. Wchodzę w skład zespołu naukowego tworzącego Krajowe Centrum Informatyki Kwantowej. Jestem członkiem-korespondentem Centrum CAIROS (Clifford Algebras International Research Open Studies, <http://www.icca7.upstlse.fr/cairos.htm>) oraz stałym współpracownikiem Centrum Leo Apostel przy Vrije Universiteit Brussel (VUB) w Brukseli (<http://www.vub.ac.be/CLEA/people/index.shtml>). Współpracuję z Instytutem Pamięci Narodowej.

W opublikowanej niedawno w Physical Review (F. Radicci i in., Phys. Rev. E, 80, 056103, 2009) analizie cytowań wymienia się moje nazwisko w kontekście osób nisko notowanych w rankingach CC (citation count) i BCC (balanced citation count), a stosunkowo wysoko w ramach SARA (science author rank algorithm). Traktuję to jako rodzaj wyróżnienia¹, choć zdaję sobie sprawę z pewnej przypadkowości umieszczenia tam mojego nazwiska. Całkowita liczba cytowań, bez mych autocytowań, lecz nie wykluczając autocytowań dokonywanych przez mych współautorów – ponad 370. Indeks Hirscha – 11.

II. Współpraca zagraniczna

Byłem stypendystą Fulbrighta (postdoc, Massachusetts Institute of Technology, 1994 – grupa D. Pritcharda, 10 miesięcy; University of Massachusetts at Lowell, 1994, 1 miesiąc, współpraca z G. Kaiserem), DAAD (Arnold Sommerfeld Institute for Mathematical Physics, Clausthal, 1997, 2 miesiące, współpraca z H.-D. Doebnerem), A. von Humboldta (Arnold Sommerfeld Institute for Mathematical Physics, Clausthal, 1999, 22 miesiące, współpraca z H.-D. Doebnerem) i NATO (UIA, Antwerpia, 2001, 7 miesięcy, współpraca z J. Naudtsem). W 2006 r. przez pół roku blisko współpracowałem z B. De Moorem z Katolickiego

¹ Autorzy piszą: „Authors badly ranked in CC or BCC methods and well classified in SARA are generally very prominent physicists” (podpis pod rys. 6).

Uniwersytetu w Leuven, w Belgii (grant belgijskiego FWO). W latach 2000-2003 gościłem na Politechnice Gdańskiej N. V. Ustinowa z Uniwersytetu w Kaliningradzie (pobył finansowany przez Nokia-Poland). Dzięki wsparciu Nokia-Poland w 1997 r. przebywałem przez tydzień w Georgia Institute of Technology (1 tydzień, współpraca z L. You). Wyjazd połączony był z udziałem w konferencji SPIE „Photonic Quantum Computing” w Orlando, USA.

III. Działalność naukowa

1. Za swoje podstawowe osiągnięcia naukowe uważam następujące wyniki:

- a) Odkrycie istnienia relatywistycznych poprawek do nierówności Bella (1984,1997).
- b) Odkrycie możliwości „uzłośliwienia się” kwantowego splątania w wypadku dynamik nieliniowych (1988) i sformułowanie formalizmu nieliniowej mechaniki kwantowej, w którym ten efekt nie występuje (2002).
- c) Sformułowanie nieliniowych uogólnień mechaniki kwantowej w formalizmie typu Lie-Nambu, opartym o nieliniowe równania von Neumanna (1993,1997).
- d) Sformułowanie twierdzenia analogicznego do twierdzenia Bella, lecz dla jednej cząstki i bez użycia nierówności (1994).
- e) Sformułowanie teorii solitonowych równań von Neumanna (1998) oraz stowarzyszonych z nimi solitonowych równań kinetycznych (2006).
- f) Odkrycie roli rzutów spinu na kierunki leżące na stożkach świetlnych dla zdefiniowania q-bitów relatywistycznych odpornych na dekoherencję typu Peres-Scudo-Terno (2003).
- g) Opisanie związków między analizą semantyczną, sztuczną inteligencją i formalizmem kwantowym, a co za tym idzie – wyznaczenie nowego kierunku badań interdyscyplinarnych na pograniczu kognitywistyki i kwantowej teorii informacji (2004).
- h) Wprowadzenie kodowania kwantowo-podobnego bezpośrednio na strukturach geometrycznych, z potencjalnymi zastosowaniami do niekwantowych implementacji obliczeń kwantowych (2007). Analogiczne sformułowanie geometrycznych odpowiedników holograficznych reprezentacji zredukowanych i binarnych kodów rozbryzgowych, z zastosowaniami do kognitywistyki i dziedzin pokrewnych (2009).
- i) Sformułowanie pierwszego kwantowego protokołu kryptograficznego, który zachowuje bezpieczeństwo nawet przy atakach uwzględniających nielokalne zmienne ukryte (2006).
- j) Zaproponowanie nowego podejścia do kwantowania pól, w którym rolę regularyzacji przejmuje sama procedura kwantowania (2000). Analiza pod tym kątem próżniowych oscylacji Rabiego, pól wytwarzanych przez ładunki punktowe, korelacji EPR oraz opis potencjalnego rozstrzygającego eksperymentu (2009).

Recenzowałem kilkanaście prac magisterskich, cztery doktorskie (A. Halim, PG; R. Augusiak, PG; B. Reichel, PG; T. Paterek, UG), jedną habilitacyjną (P. Caban, UŁ) oraz napisałem recenzję wydawniczą rozprawy habilitacyjnej (A. M. Alhasan, AP Słupsk). Byłem recenzentem podręcznika M. Kamiński, K. Giaro, *Wprowadzenie do algorytmów kwantowych* (Akademicka Oficyna Wydawnicza EXIT, Warszawa, 2003). Recenzuję artykuły wysyłane do American Journal of Physics, European Physical Journal, International Journal of Theoretical Physics, Foundations of Physics Letters, Journal of Geometry and Physics, Journal of Mathematical Psychology, Journal of Physics A i B, Open Systems and

Information Dynamics, Physica Scripta, Physics Essays, Physics Letters A, Physical Review A i E, Physical Review Letters, Quantum Information Processing, Reports on Mathematical Physics, TASK Quarterly. Na prośbę redakcji Classical and Quantum Gravity recenzowałem monografię D. Finkelsteina pt. *Quantum Relativity: A Synthesis of the Ideas of Einstein and Heisenberg* (Springer, 1997).

2. Szczegółowy opis głównych osiągnięć naukowych

Ad 1a. W 1984 r., jeszcze jako student, wysłałem do Physics Letters A artykuł, w którym analizowałem tzw. średnią bellowską dla pary elektronów Diraca. Praca została odrzucona i tematykę zarzuciłem aż do roku 1995, kiedy to przypadkowo znalazłem prostszy i ogólniejszy dowód podstawowego wzoru, co opublikowałem w [1]. Zasadnicza teza pracy [1] głosi, iż użytkownicy kwantowego kanału kryptograficznego mogą wyciągnąć wniosek, iż są podsłuchiwani – a jest to tylko efekt relatywistyczny związany z własnościami relatywistycznych operatorów spinu i położenia środka masy. Mój wynik został zauważony przez środowisko fizyków zajmujących się podstawami mechaniki kwantowej i kryptografii dopiero po roku 2002, gdy zaczęło narastać zainteresowanie efektami relatywistycznymi w kwantowej teorii informacji. Obecnie praca [1] ma ok. 80 cytowań, tzn. jest wzmiankowana przez praktycznie wszystkich autorów analizujących relatywistyczne efekty w kwantowej teorii informacji.

Ad 1b. Na przełomie lat 1988-89 wysłałem do Physics Letters A artykuł pokazujący, w jaki sposób dynamika nieliniowa jednego z dwóch wzajemnie nieoddziałujących (w sensie zerowego hamiltonianu oddziaływania) podukładów, znajdujących się początkowo w stanie splątanym, wpływa na oba układy równocześnie – nawet dla nieliniowości związanej tylko z jednym z nich. Praca nie została opublikowana, lecz przedstawiłem ją na konferencji „Problems in Quantum Physics – Gdańsk’89”. Po moim referacie, Bogdan Mielnik poinformował mnie o pracy N. Gisina (Helv. Phys. Acta 62, 363, 1989) gdzie analogiczną konkluzję osiągnięto przy pomocy innego rozumowania. Mielnik pokazał mi również preprint pracy Stevena Weinberga (Ann. Phys. 194, 336, 1989) o nieliniowej mechanice kwantowej, gdzie zaproponowano opis układów nieoddziałujących dla nieliniowych równań Schroedingera. Zastosowałem formalizm Weinberga do mojego pomysłu i wykazałem, iż teoria Weinberga implikuje nielocalne, niefizyczne oddziaływania pomiędzy układami opisywanymi stanami splątanymi. Skontaktowałem się z Weinbergiem i przesłałem mu preprint kolejnej pracy, uwzględniającej jawny przykład oparty o jego teorię [2]. W 1991 r. J. Polchinski, współpracownik Weinberga, opublikował (Phys. Rev. Lett. 66, 397, 1991) artykuł na ten sam temat, lecz podając jeszcze inne, trzecie wyprowadzenie zjawiska. Polchinski cytuje mój preprint, a porównanie dat pokazuje, że mój artykuł [2] był wysłany do druku wcześniej, choć ukazał się później. Weinberg, w książce „Marzenie o teorii ostatecznej” (Alkazar, Warszawa, 1994), omawia prace Gisina i Polchinskiego, o mojej nie wspominając i twierdząc, iż wynik przez nich uzyskany zniechęcił go do prób konstrukcji nieliniowych uogólnień mechaniki kwantowej. Jego zdaniem sugeruje to, że dynamika kwantowa *musi* być liniowa. W 2002 r., modyfikując pewne idee pracy Polchinskiego, wykazaliśmy z H.-D. Doebnerem [3], iż jednak istnieje procedura pozwalająca na konstruowanie nieliniowych dynamik kwantowych, w których wszystkie trzy zjawiska – Gisina, moje i Polchinskiego – się nie pojawiają.

Ad 1c. Jest to główny wynik mojej rozprawy doktorskiej. Wprowadziłem tam nowy typ dynamiki kwantowej, opartej o nawias analogiczny do nawiasu Nambu, lecz wykorzystujący stałe strukturalne algebry Lie. Pozwoliło to sformułować nieliniową mechanikę kwantową

operatora gęstości bez konieczności wprowadzania nieliniowych wartości średnich obserwabli. Dzięki temu teoria miała dobrze określoną interpretację probabilistyczną, co odróżniało ją od teorii wcześniejszych, gdzie nie było jasne, czym jest wartość kwantowej zmiennej losowej, ani jak definiować prawdopodobieństwa. Ponadto pokazałem, iż w tak skonstruowanej teorii nie pojawiają się trudności opisane przeze mnie i Polchinskiego (choć problem Gisina doczekał się rozwiązania dopiero w [3]). Równanie ruchu pojawiające się w mej pracy okazało się nowym typem układu całkowalnego, którego teorię rozwinąłem w latach późniejszych. Zasadnicze publikacje to [4,5,6]. Jako zastosowanie formalizmu pokazałem w [7], iż nie należy utożsamiać formalnej „lokalności” równań różniczkowych z lokalnością wymaganą przez fizykę. Równania uważane za lokalne, np. nieliniowe równanie Białynickiego-Biruli-Mycielskiego dla n cząstek, okazały się fizycznie nielokalne – i odwrotnie, równania uchodzące za nielokalne, okazały się lokalne w odpowiednio skonstruowanym formalizmie. Innym nieoczekiwanym zastosowaniem konstrukcji było wykazanie [8], iż tzw. nieliniowe odwzorowania kompletnie dodatnie, rozważane w literaturze matematycznej, nie spełniają kryteriów fizycznych wiązanych z kompletną dodatniością. Co ciekawe, zachodzi też zjawisko odwrotne: rozwiązania kwantowych nieliniowych równań ruchu spełniają kryteria fizyczne oczekiwane od odwzorowań kompletnie dodatnich, ale kompletnie dodatnie nie są. Wynik miał implikacje dla innych działów fizyki, np. teorii D-bran i kwantowej grawitacji (por. J. Ellis i in., Phys. Rev. D 63, 024024, 2000).

Ad 1d. W pracy [9] pokazałem istnienie nowego rodzaju zjawiska nielokalnego – zależności rezultatu pomiaru od modyfikacji parametrów interferometru w obszarze, gdzie funkcja falowa fotonu tożsamościowo znika. Wynik nie ma konsekwencji eksperymentalnych, gdyż trudność pojawia się dopiero po założeniu istnienia lokalnych zmiennych ukrytych. W tym sensie jest to kolejne twierdzenie o nieistnieniu lokalnych zmiennych ukrytych, analogiczne do twierdzenia Bella. Wykorzystując to samo rozumowanie pokazałem następnie, iż dwa znane zagadnienia – problem wykrywania podsłuchu w kanale kryptograficznym i test Elizura-Vaidmana – są szczególnymi przypadkami jednego problemu, wynikającego z mojej wersji twierdzenia Bella [10]. Moje sformułowanie twierdzenia, uwzględniające tylko jedną cząstkę i nie wykorzystujące nierówności, wykazywało podobieństwa do często cytowanej pracy Hardy’ego (Phys. Rev. Lett. 73, 2279, 1994), wysłanej do druku już po ukazaniu się mojego artykułu. W przeciwieństwie do Hardy’ego (i większości podobnych prac) nie opierałem rozumowania na „splątaniu z próżnią” – koncepcji, którą uważam za artefakt niefizycznej reprezentacji przestrzeni Foka (por. analiza przedstawiona w [11]).

Ad 1e. Uważam się za twórcę teorii solitonowych równań von Neumanna i solitonowych równań kinetycznych. Wyniki uzyskane w tej dziedzinie do roku 1999 stały się podstawą mej rozprawy habilitacyjnej, obronionej na Wydziale Fizyki Uniwersytetu Warszawskiego w czerwcu 2000 r. Rada Wydziału Fizyki UW uznała moją habilitację za wyróżniającą się.

Podstawowe równanie pojawiające się w mej pracy doktorskiej i opublikowane w [5] wyglądało następująco: $id\rho/dt=[H,f(\rho)]$, gdzie f to dowolna funkcja, H – hamiltonian, a ρ – macierz gęstości. W tak ogólnej postaci równanie to nie redukowało się do żadnego znanego układu dynamicznego i nie była znana metoda jego jawnego rozwiązywania. Problem ten podjęliśmy wraz z Sergiejem Leble, przy czym pierwszym krokiem było wymyślenie metody rozwiązywania dla $f(\rho)=\rho^2$, co następnie udało się uogólnić na funkcje bardzo ogólnej postaci. Znaleźliśmy dla $f(\rho)=\rho^2$ Darboux-kowariantną parę Laxa i używając technik solitonowych podaliśmy przykłady jawnych rozwiązań wykazujących nowy rodzaj zjawiska solitonowego (samorozpraszenie) [12]. Rozwiązania nazwaliśmy samorozproszeniowymi, gdyż posiadały

charakterystyczną cechą: dla $t \rightarrow \pm\infty$ zmierzały asymptotycznie do dwóch różnych rozwiązań liniowego równania $idp/dt=[H,p]$. W pracy [13] podaliśmy przykłady jawnych rozwiązań samorozproszeniowych dla funkcji f nie będących wielomianami, a także dla wielomianów dowolnego stopnia. W [14,15] uogólniliśmy technikę rozwiązywania nieliniowych równań von Neumanna na nieliniowości nieabelowe, spełniające $[\rho, f(\rho)] \neq 0$, a nawet mające strukturę jeszcze ogólniejszą. Okazało się przy tym, iż przy odpowiednich wyborach H , f oraz warunku początkowego, równania von Neumanna stają się znanymi lub nowymi równaniami opisującymi dynamikę na kratkach.

Następnym krokiem było zrozumienie, że równania von Neumanna pełnią rolę tzw. laksowskich postaci układów nieliniowych równań kinetycznych, analogicznych do równań znanych z kinetyki chemicznej i biologicznej. W ten sposób odkryliśmy kolejny nieznaną układ dynamiczny: solitonowe równania kinetyczne ze zmiennymi kinetycznymi opisywanymi nieklasycznym rachunkiem prawdopodobieństwa [16]. Pokazaliśmy, iż efekt samorozpraszania (w tym kontekście nazywany przez nas samoprzełączaniem) powoduje konsekwencje analogiczne do zwijania się i rozwijania struktur spiralnych w DNA. W sposób naturalny pojawiają się tu formalne odpowiedniki struktur dwuniciowych, jeśli dynamikę czasową potraktować jako ciągły odpowiednik maszyny Turinga, a nieliniowe równanie von Neumanna jako równanie typu Schroedingera dla układu złożonego. Proces samoprzełączania staje się wtedy analogiczny do replikacji nici DNA, nawet włączając w to znaną własność polimeraz, czyli głowic genetycznej maszyny Turinga, polegającą na poruszaniu się po obu niciach w przeciwnych kierunkach [17].

Wspomniane aspekty biologiczne badane były w ramach mojej współpracy z interdyscyplinarnym Centrum Leo Apostel przy uniwersytecie VUB w Brukseli oraz, bardziej pod kątem dynamik kwantowych, w ramach dwóch grantów KBN, którymi kierowałem.

W opublikowanym w archiwum arXiv.org „nieformalnym materiale źródłowym na temat opublikowanych w arXiv.org do roku 2004 prac dotyczących nieliniowej mechaniki kwantowej” (G. Svetlichny, arXiv:quant-ph/0410036v7), zawierającym 126 pozycji, wymienia się 25 moich artykułów. W porządku chronologicznym, na pierwsze cztery prace – trzy są mojego autorstwa.

Ad 1f. Standardowe q-bity relatywistyczne definiowane są przy pomocy skrętności. W swym artykule Peres, Scudo i Terno (Phys. Rev. Lett. 88, 230402, 2002) zwrócili uwagę na brak relatywistycznej niezmienniczości entropii spinowych stopni swobody. Praca wywołała duże zainteresowanie środowisk badających kwantową teorię informacji. Jednakże, z ogólniejszego punktu widzenia, skrętność jest rzutem wektora Pauliego-Lubanskiego na arbitralnie wybraną „oś czasu”. Jest to więc tylko jeden z możliwych wyborów obserwabli definiujących q-bity. W pracy [18] zwróciłem uwagę na szczególną rolę rzutów wektora Pauliego-Lubanskiego na kierunki zerowe, czyli leżące na stożkach świetlnych. W artykule [19], odnosząc się m.in. do obserwacji Peresa, Scudo i Terno, pokazaliśmy wraz z moim magistrantem, iż q-bity definiowane poprzez takie właśnie „zerowe” rzuty wektora Pauliego-Lubanskiego pozwalają zdefiniować relatywistycznie niezmienniczą entropię spinową, co eliminuje efekt Peresa-Scudo-Terno, jeżeli odpowiednio dostroi się kierunek zerowy do konkretnej transformacji Lorentza (chodzi o tzw. główny kierunek zerowy transformacji Lorentza). Zjawisko to można wykorzystać do konstrukcji relatywistycznego algorytmu korekcji błędów. Bardziej jawna analiza pracy Peresa, Scudo i Terno, z takiego właśnie punktu widzenia, przedstawiona jest w moim komentarzu [20]. Podsumowaniem mego podejścia do relatywistycznych q-bitów jest przeglądowy artykuł [21], napisany na prośbę redakcji czasopisma Quantum Information Processing do numeru specjalnego, poświęconego podstawowym aspektom kwantowej teorii informacji.

Ad 1g. Jednym z powszechnych błędów, popełnianych przy okazji logiki kwantowej i kwantowego prawdopodobieństwa, jest wiązanie „kwantowości” ze skalą mikro. Struktury „kwantowe” nazywane są kwantowymi zazwyczaj z powodów historycznych, a nie ontologicznych – istnieją przykłady sytuacji opisywanych zwykłą klasyczną mechaniką, prowadzących do pojawiania się nieprzemiennej algebry pytań i nieklasycznego rachunku prawdopodobieństwa [22]. Dlatego wolę mówić o strukturach *formalnie* kwantowych. Nieliniowe równania kinetyczne, o których pisałem wcześniej, bazują na kwantowym rachunku prawdopodobieństwa, gdyż istotnym elementem reakcji chemicznych jest ich nieprzemienność: $A \rightarrow C$ to nie to samo co $A \rightarrow B \rightarrow C$. Innym przykładem analogicznej nieprzemienności są testy psychologiczne. Analizowana w lingwistyce kontekstowa aktualizacja znaczeń przypomina kwantową zasadę superpozycji i problem pomiaru. Można więc oczekiwać, iż struktury formalnie kwantowe pojawią się np. w sztucznej inteligencji, kognitywistyce, psychologii lub lingwistyce. W artykule [23], napisanym wspólnie z D. Aertsem, dyrektorem Interdyscyplinarnego Centrum im. Leo Apostela przy Uniwersytecie VUB w Brukseli, przeanalizowaliśmy z tego punktu widzenia tzw. utajoną analizę semantyczną (LSA) i reprezentacje rozproszone stosowane w sztucznej inteligencji. Zwróciliśmy uwagę na intrygujące podobieństwa formalne, połączone z różnicami interpretacyjnymi, pomiędzy kilkoma dziedzinami wiedzy zapoczątkowanymi w latach 90. ubiegłego stulecia i rozwijanymi przez różne środowiska w zupełnym oderwaniu od siebie. Przykładowo, wprowadzone w kontekście sztucznej inteligencji tensorowe reprezentacje predykatów (P. Smolensky, *Artif. Intelligence* 46, 159, 1990) są matematycznie identyczne ze stanami splątanymi pojawiającymi się w kwantowej informatyce, lecz pełnią inne role. Sygnalizowaliśmy też możliwe kierunki dalszych badań interdyscyplinarnych.

Praca spotkała się ze sporym zainteresowaniem. Po upływie roku należała do górnych 1-2% artykułów najczęściej ściąganych ze stron internetowych brytyjskiego Institute of Physics. Pojawiły się też mniej standardowe symptomy oddziaływania naszej publikacji na środowisko naukowe. Przykładowo, w ramach akcji reklamującej publikację IOP („60 seconds with... Authors Edition”) przeprowadzono ze mną wywiad na jej temat, umieszczony na stronie internetowej IOP.

W chwili obecnej można już rzeczywiście mówić o powstaniu nowej dyscypliny badawczej. W latach 2007-2009 odbyła się seria konferencji pod wspólnym tytułem „Quantum Interaction” (Stanford 2007, Oxford 2008, Saarbrücken 2009), dotyczących wykorzystania struktur kwantowych poza mechaniką kwantową. Zainspirowane były one w dużym stopniu naszą publikacją, co przyznał jeden z organizatorów, P. Bruza z Queensland University of Technology (por. <http://www.onlineopinion.com.au/view.asp?article=5486>). Bezpośrednią konsekwencją naszej pracy stały się też dalsze badania, opisane w punkcie następnym.

Ad 1h. Największą słabością obliczeń kwantowych jest ich bardzo duża wrażliwość na zakłócenia i związaną z nimi dekoherencję. Niewykluczone, iż problem ten stanie się barierą uniemożliwiającą powstanie realistycznego procesora kwantowego. Ponieważ jednak, jak już wspominałem, istnieją niekwantowe układy wykazujące pewne formalne kwantowe własności logiczne lub probabilistyczne, uzasadnione jest pytanie, czy nie mogą istnieć niekwantowe implementacje obliczeń kwantowych. W pracy [24] pokazaliśmy w jaki sposób zastąpienie stanów splątanych multiwektorami, pojawiającymi się w algebrze geometrycznej, pozwala przeformułować algorytm Deutscha-Jozsy jako problem geometryczny niemający związku z mechaniką kwantową. Jest to wynik o tyle istotny, że algorytm Deutscha-Jozsy jest historycznie pierwszym przykładem potencjalnej wyższości algorytmów kwantowych nad klasycznymi. W [25] pokazałem, iż wszystkie elementarne kwantowe bramki logiczne mają geometryczne odpowiedniki działające na multiwektory. W częściowo przeglądowym

artykule [26] pokazaliśmy, iż każdy stan n -q-bitowy ma odpowiednik geometryczny w przestrzeni multiwektorów. Krótko mówiąc, każdy algorytm kwantowy można przy pomocy formalizmu algebry geometrycznej przeformułować jako problem geometryczny, lecz w praktyce trudnością jest wysoki wymiar przestrzeni pojawiających się przy przetwarzaniu liczb o dużej ilości bitów. Niemniej, teoretycznie rzecz biorąc, powinno dać się zaimplementować obliczenia kwantowe poza obszarem opisywanym przez mechanikę kwantową (chodzi oczywiście o implementacje porównywalne, w sensie szybkości i równoległości, z technologiami opartymi bezpośrednio o struktury mikroskopowe). Jako szczególne zastosowanie zaproponowanego formalizmu przeanalizowaliśmy z Aertsem i moim magistrantem geometryczną implementację 3-bitowej teleportacji [27]. Inną pracą magisterską, napisaną pod moim kierunkiem na zbliżony temat, jest geometryczna analiza algorytmu Simona [28]. Otwarta pozostaje kwestia konkretnych geometrycznych implementacji obliczeń kwantopodobnych, pozwalających na równoległe przetwarzanie multiwektorów jako całości. Tak postawiony problem wpisuje się w stosunkowo nowy nurt badań nad procesorami wykorzystującymi algebrę Clifforda na poziomie hardware'u (por. S. Gentile i in., *CliffoSor: A parallel embedded architecture for geometric algebra and computer graphics*, w *Computer Architecture for Machine Perception*, str. 90-95, IEEE Computer Society, 2005).

Kolejnym krokiem, opisanym w przygotowanym na zaproszenie redakcji *Journal of Mathematical Psychology* artykule [29], było uogólnienie powyższych obserwacji na kodowanie rozproszone stosowane w kognitywistyce, informatyce, sztucznej inteligencji i innych dziedzinach pokrewnych. Punktem wyjścia była obserwacja, iż tzw. zredukowane reprezentacje holograficzne (HRR, por. T. A. Plate, *Holographic Reduced Representation – Distributed Representation for Cognitive Structures*, Stanford, 2003) i binarne kody rozbryzgowane (BSC, por. P. Kanerva, Binary spatter codes of ordered k -tuples, *Lecture Notes in Computer Science* 1112, 869, 1996) mają strukturę analogiczną do multiwektorów. Praktyczną konsekwencją owego spostrzeżenia jest możliwość wprowadzenia hierarchii nowego typu operacji na 2^n -kach (zrzutowane iloczyny geometryczne [29]) i zastąpienie nimi splotów oraz alternatyw wykluczających stosowanych w HRR i BSC. Tak przeformułowane HRR i BSC uzyskują interpretację geometryczną, co może mieć pojęciowe konsekwencje np. dla modelowania psychologicznego (algebra geometryczna formalizuje proces *rozumienia* struktur geometrycznych). Z czysto implementacyjnego punktu widzenia, zrzutowane iloczyny geometryczne pozwalają na alternatywną konstrukcję np. rozproszonych baz danych. Zastosowania iloczynów geometrycznych w informatyce stanowią przedmiot przygotowywanej pod moim kierunkiem pracy doktorskiej A. Patyk (por. [30,31]).

Ad 1i. W powszechnym odczuciu bezpieczeństwo kwantowych systemów kryptograficznych opiera się na założeniu o nieistnieniu zmiennych ukrytych. Z drugiej strony wiadomo, iż mechanika kwantowa jest nieodróżnialna od pewnych teorii z nielokalnymi zmiennymi ukrytymi. Pojawia się zatem podstawowy problem: do jakiego stopnia bezpieczeństwo kwantowych protokołów kryptograficznych jest kwestią *wiary* w nieistnienie nielokalnych zmiennych ukrytych? Prosta analiza oparta o klasyczne modele nielokalne wykazujące prawdopodobieństwa charakterystyczne dla q -bitów (np. model Aerts'a [22]) pokazuje, iż 1- q -bitowy protokół BB84 i oparty o stany splątane 2- q -bitowy protokół Ekerta, nie są odporne na ataki wykorzystujące znajomość zmiennych ukrytych. Okazuje się jednak, co opisaliśmy z D. Aertsem oraz moim magistrantem M. Pawłowskim [32], że nielokalność zmiennych ukrytych ma w tym wypadku oblicze pozytywne. Można ją wykorzystać do zwiększenia bezpieczeństwa protokołu typu Ekerta, jeżeli jedna ze stron biorących udział w przekazywaniu klucza losowo wybiera jedną z dwóch alternatywnych realizacji standardowego protokołu. Procedura ta jednak nie poprawia bezpieczeństwa protokołów 1-

bitowych, w rodzaju BB84, co jest przykładem wyższości kryptografii opartej o stany splątane nad jej wersja pierwotną, bazującej na zasadzie nieoznaczoności dla jednej cząstki. Protokół opisany przez nas w [32] jest jak dotąd jedynym, który wykazuje odporność na ataki nie tylko standardowe, lecz również przeprowadzane przy użyciu hipotetycznych nielokalnych zmiennych ukrytych. Proponowaną przez nas modyfikację protokołu łatwo jest uwzględnić w eksperymencie, lecz praca nie spotkała się z oddźwiękiem w literaturze. Natomiast dwukrotnie otrzymałem zapytania o pewne szczegóły techniczne z ośrodków wojskowych w Niemczech i USA. Errata uzupełnia istotne przeoczenia bibliograficzne.

Ad 1j. W artykule [33] zwróciłem uwagę na możliwą fizyczną niespójność pierwszej pracy o kwantowaniu pola (M. Born, W. Heisenberg, P. Jordan, *Z. Phys.* 35 557, 1925). Mianowicie, zakłada się tam, iż wektory falowe indeksujące operatory kreacji i anihilacji są parametrami. W rzeczywistych oscylatorach kwantowych wielkości te są obserwabliami – rozróżnienie, którego w 1925 r. nie znano – a zatem oscylatory istnieją w stanach superpozycji różnych częstości (np. długość „nano-wahadła” jest rozmyta, bo położenia środków mas atomowych paczek falowych są rozmyte). Jeżeli zastąpi się klasyczne parametry obserwabliami, uzyskuje się inną reprezentację algebry oscylatora harmonicznego niż zwyczajowo przyjmowana przy kwantowaniu pola. W szczególności próżnia, rozumiana jako stan anihilowany przez wszystkie operatory anihilacji, nie jest jednoznacznie określonym wektorem, lecz całą nieskończenie wymiarową podprzestrzenią w przestrzeni stanów. Podprzestrzeń ta opisuje wszystkie możliwe stany kondensatu Bosego-Einsteina bozonowego gazu oscylatorowego w zerowej temperaturze. Nie trzeba używać nieskończenie wielu oscylatorów do opisu nieskończonego zbioru modów pola – wystarczy jeden oscylator, będący w stanie superpozycji wszystkich możliwych wektorów falowych. Pole kwantowe można zatem spróbować zdefiniować jako gaz składający się ze skończonej liczby oscylatorowych paczek falowych. Liczba oscylatorów N jest niezależna od liczby modów pola i może być traktowana jako parametr reprezentacji algebry Lie oscylatora harmonicznego. Reprezentacja taka jest redukowalna.

Fakt, iż pole można opisywać przy pomocy skończonego zbioru oscylatorów, rodzi nadzieję na sformułowanie teorii „bez nieskończoności”, co jest chyba najstarszym wciąż otwartym problemem teorii kwantów. Pojawia się zatem pytanie, czy odpowiednio skonstruowana teoria może być zgodna z eksperymentem. Z metodologicznego punktu widzenia wystarczy zrozumieć, czy istnieje zasada korespondencji między nową teorią a standardową zrenormalizowaną kwantową teorią pola i jak to się ma do realistycznych danych eksperymentalnych.

Pierwszym naturalnym krokiem było naszkicowanie zmodyfikowanego formalizmu nierelatywistycznej optyki kwantowej [33], choć analizę promieniowania ciała doskonale czarnego dziś napisałbym zupełnie inaczej (z perspektywy późniejszych wyników rozumiem, że z termodynamicznego punktu widzenia należy rozróżniać pomiędzy hamiltonianem pola, rozumianego jako gaz N -oscylatorowy, a hamiltonianem jednego z oscylatorów tworzących ten gaz). W późniejszych artykułach odszedłem też od idei przestrzeni Foka uwzględniającej superpozycje różnych liczb oscylatorów – nie wносиło to niczego istotnego, gdyż żaden operator nie zmieniał liczby oscylatorów, a komplikowało notację i zaciemniało istotę problemu. Z obecnej perspektywy za najbardziej dojrzałe uważam artykuły [34] i [35]. Praca [36] zawiera analogiczne sformułowanie pól fermionowych. Istotnym elementem jest dodatek w pracy [21], precyzujący postać delty Diraca stosowanej przy kwantowaniu pola (chodzi o ciągową konstrukcję delty przyjmującej skończoną wartość w zerze).

Praca [34], napisana z doktorantką i dopracowująca idee wcześniej sygnalizowane w [37] i [38], poświęcona jest Poincaré niezmienniczemu sformułowaniu czteropotencjału w formalizmie z dodatnio określoną metryką w przestrzeni Hilberta. Czteropotencjał jest tu

hermitowskim polem czterowektorowym (transformacja Lorentza nie zmienia cechowania), co zagwarantowane jest przez specyficzne własności transformacyjne „twistorowych” tetrad Minkowskiego. Na poziomie fourierowskim, czteropotencjał okazuje się składać z pola bezmasowego o spinie 1 i dwóch bezmasowych pól skalarnych. Statystyki fotonowe dotyczą jedynie ilości wzbudzeń składowej o spinie 1. Pierwszym interesującym testem tak sformułowanej teorii jest problem pól wytwarzanych przez punktowe źródła klasyczne. Jest on dokładnie rozwiązalny, przy czym standardowy formalizm prowadziłby do katastrofy w podczerwieni. Punktem wyjścia jest dynamika w obrazie oddziaływania, a nie równania Maxwella. Rozwiązanie odpowiadające ładunkowi punktowemu jest operatorem składającym się z części swobodnej i należącego do centrum algebry członu źródłowego. Wartość średnia tego ostatniego, obliczona w dowolnym stanie koherentnym, nie jest dokładnie polem coulombowskim, lecz automatycznie uwzględnia polaryzację próżni (efektywna gęstość ładunku, generująca pole, okazuje się być *operatorem* a nie deltą Diraca – nawet dla punktowego prądu klasycznego). Statystyka fotonowa nie wykazuje katastrofy w podczerwieni. Dla skończonego N uzyskuje się deformację rozkładu Poissona charakterystyczną dla α -entropii Rényi’ego, gdzie $\alpha=1-1/N$. W granicy $N\rightarrow\infty$ odtwarza się *zregularyzowany* rozkład Poissona (tzw. granica shannonowska, $\alpha\rightarrow 1$, dla entropii Rényi’ego). Powyższe efekty biorą się z faktu, iż źle zdefiniowane całki, typowe dla formalizmu standardowego, zastępowane są dobrze zdefiniowanymi całkami spektralnymi (czyli operatorami). Własność tę nazywam „regularyzacją przez kwantowanie”.

Artykuł [35] jest, de facto, ostatnim rozdziałem rozprawy doktorskiej mojego doktoranta, Marcina Wilczewskiego. Analizujemy tam możliwości eksperymentalnych testów mojego formalizmu w ramach elektrodynamiki wnęk rezonansowych. Niejako produktem ubocznym badań nad zmodyfikowanym kwantowaniem pola było rozstrzygnięcie części podnoszonych w literaturze kontrowersji dotyczących znanego eksperymentu grupy paryskiej (M. Bune i in., Phys. Rev. Lett. 76, 1800, 1996) [39].

Dodam, iż praca [21] wykorzystuje formalizm wprowadzony w [34] do analizy polaryzacyjnych korelacji EPR dla fotonów. Zasadniczy wynik [21] głosi, iż eksperymenty EPR nie rozróżniają pomiędzy formalizmem standardowym i moim, jeżeli w tym ostatnim parametr N jest większy niż 1. Zachodzi to przynajmniej dla stanów EPR, które rozważałem jako przykłady. Próba usystematyzowania problemu dla najbardziej ogólnych postaci stanów splątanych, włączając to ich własności relatywistyczne, jest przedmiotem rozprawy doktorskiej przygotowywanej przez Klaudię Wrzask.

W chwili obecnej koncentruję się na problemie diagramów pętlowych w pełnej elektrodynamice kwantowej, opisywanej moim formalizmem. Policzyłem m.in. poprawki drugiego rzędu do przejścia próżnia-próżnia i wykazałem, iż się automatycznie zerują (wynik niepublikowany). W trakcie wykonywania rachunku nie pojawiają się żadne wielkości rozbieżne, choć w podejściu standardowym natrafiłoby się na „trudne” nieskończoności. Istnieją uzasadnione podejrzenia, iż uda się to wykazać dla dowolnego rzędu rachunku zaburzeń.

Jak widać, powyższy program badawczy jest dobrze zdefiniowany, bardzo obiecujący i długofalowy. Wymaga on przemyślenia od podstaw wszystkich etapów konstrukcji kwantowej teorii pola. Jest to, moim zdaniem, najciekawszy i najważniejszy obszar badań w całym moim dorobku naukowym.

IV. Działalność organizacyjna

W kadencji 2005-2008 byłem członkiem uczelnianej Odwoławczej Komisji Dyscyplinarnej dla studentów PG.

Kierowałem dwoma grantami KBN (Uogólnione transformacje typu Darboux w zastosowaniu do nieabelowych dynamik nieliniowych, 2 P03B 163 1, lata 1998-2000; Techniki solitonowe w zastosowaniu do równań mechaniki kwantowej, 5 P03B 040 20, lata 2001-2003). Byłem kierownikiem ze strony polskiej polsko-flamandzkiego projektu bilateralnego „Soliton techniques applied to equations of quantum field theory” (2004-2005). Kierowałem zadaniami badawczymi „Zjawiska nieliniowe i kwantowo-polowe w kwantowej teorii informacji” w projekcie zamawianym MNiSW „Inżynieria i informatyka kwantowa” (2003-2007) oraz „Informatyka kwantowa a podstawowe problemy mechaniki kwantowej”, w projekcie MNiSW, realizowanym przez sieć LFPPI (2008).

Jestem jednym z inicjatorów powołania ogólnopolskiej sieci naukowej LFPPI (Laboratorium Fizycznych Podstaw Przetwarzania Informacji, <http://lfppi.pl/>), skupiającej krajowe ośrodki badające kwantową teorię informacji. Reprezentowałem Politechnikę Gdańską w Radzie Naukowej LFPPI (pierwsza kadencja, 2003-2007). Aktualnie wchodzi w skład Rady Naukowej Krajowego Centrum Informatyki Kwantowej w Gdańsku (od 2007 r.).

V. Działalność dydaktyczna

Prowadziłem na Politechnice Gdańskiej zajęcia z następujących przedmiotów: Matematyka („Analiza I”), Pierwsza pracownia fizyczna, Elektrodynamika, Mechanika klasyczna, Mechanika kwantowa, Mechanika kwantowa 3/2 (wykład obieralny), Teoria informacji, Analiza sygnału, Kryptografia i komputery kwantowe, Kryptografia klasyczna i kwantowa, Równania różniczkowe i całkowe w fizyce i technice, Fizyka (na kierunku Matematyka Stosowana). Mój wykład „Kryptografia i komputery kwantowe” był prawdopodobnie pierwszym regularnym wykładem kursowym prowadzonym na ten temat na polskiej uczelni (nagroda dydaktyczna III stopnia Rektora PG za rok 1997/98). Uczęszczali na niego studenci IV roku specjalności Fizyka Komputerowa oraz, w ramach indywidualnych programów nauczania, studenci chemii z PG i fizyki z UG, a także doktoranci z Wydziału Elektroniki, Telekomunikacji i Informatyki PG.

Byłem promotorem 14 prac magisterskich i jednej doktorskiej (M. Wilczewski, PG, 2010). Dwie moje doktorantki mają zaawansowane rozprawy doktorskie (K. Wrzask, otwarty przewód doktorski na Wydziale FTiMS PG; A. Patyk, praca niemal zakończona, z otwarciem przewodu doktorskiego na Wydziale ETI PG czekamy do momentu przyjęcia do druku kolejnego artykułu). Kilkunastu studentów studiowało pod moim kierunkiem w ramach indywidualnego toku studiów, z czego dwie osoby ukończyły studia w Włoszech w ramach programu Erasmus Mundus (A. Siwecki, M. Twarogowska), a dwie inne pracowały nad dyplomem pod moim kierunkiem w Niemczech, gdy byłem stypendystą DAAD (K. Wasylka, M. Syty).

Bibliografia

1. M. Czachor, Einstein-Podolsky-Rosen-Bohm experiment with relativistic massive particles, *Phys. Rev. A* 55, 72 (1997).
2. M. Czachor, Mobility and nonseparability, *Found. Phys. Lett.* 4, 351 (1991).
3. M. Czachor, H.-D. Doebner, Correlation experiments in nonlinear quantum mechanics, *Phys. Lett. A* 301, 139-152 (2002).
4. M. Czachor, Nonlinear Schroedinger equation and two-level atoms", *Phys.Rev. A* 53, 1310 (1996).
5. M. Czachor, Nambu-type generalization of the Dirac equation, *Phys. Lett. A* 225, 1 (1997).
6. M. Czachor, Lie-Nambu and beyond, *Int. J. Theor. Phys.* 38, 475-500 (1999).

7. M. Czachor, Nonlocal-looking equations can make nonlinear quantum dynamics local, *Phys. Rev. A* 57, 4122 (1998).
8. M. Czachor, M. Kuna, Complete positivity of nonlinear evolution: A case study, *Phys. Rev. A* 58, 128 (1998).
9. M. Czachor, Bell theorem without inequalities: A single particle formulation, *Phys. Rev. A* 49, 2231 (1994).
10. M. Czachor, Quantum cryptography with polarizing interferometers, *Phys. Lett. A* 257, 107 (1999).
11. M. Pawłowski, M. Czachor, Degree of entanglement as a physically ill-posed problem: The case of entanglement with vacuum, *Phys. Rev. A* 73, 042111 (2006)
12. S.B. Leble, M. Czachor, Darboux-integrable nonlinear Liouville-von Neumann equation, *Phys. Rev. E* 58, 7091 (1998).
13. N.V. Ustinov, M. Czachor, M. Kuna, S.B. Leble, Darboux integration of $i\partial_t \rho = [H, \rho]$, *Phys. Lett. A* 279, 333-340 (2001).
14. N.V. Ustinov, M. Czachor, Darboux-integrable equations with non-Abelian nonlinearities, w *Probing the structure of quantum mechanics: Nonlinearity, nonlocality, computation, axiomatics*, red. D. Aerts, M. Czachor, T. Durt, str. 335-353 (World Scientific, Singapore, 2002).
15. J.L. Cieśliński, M. Czachor, N.V. Ustinov, Darboux covariant equations of von Neumann type and their generalizations, *J. Math. Phys.* 44, 1763 (2003).
16. D. Aerts, M. Czachor, Abstract DNA-type systems, *Nonlinearity* 19, 575-589 (2006)
17. D. Aerts, M. Czachor, Two-state dynamics for replicating two-strand systems, *Open Systems and Information Dynamics* 14, 397-410 (2007).
18. M. Czachor, Bargmann-Wigner spinors, w *Photon and Poincare Group*, red. V. V. Dvoeglazov, str. 32-62 (Nova Science, New York, 1999).
19. M. Czachor, M. Wilczewski, Relativistic Bennett-Brassard cryptographic scheme, relativistic errors, and how to correct them, *Phys. Rev. A* 68, 010302(R) (2003).
20. M. Czachor, Comment on 'Quantum entropy and special relativity', by A. Peres, P.F. Scudo, and D. Terno, *Phys. Rev. Lett.* 94, 078901 (2005).
21. M. Czachor, Two-spinors, oscillator algebras, and qubits: aspects of manifestly covariant approach to relativistic quantum information, *Quantum Information Processing* 9, 171-232 (2010).
22. M. Czachor, On classical models of spin, *Found. Phys. Lett.* 3, 249 (1992)
23. D. Aerts, M. Czachor, Quantum aspects of semantic analysis and symbolic artificial intelligence, *J. Phys. A* 37, L123-L132 (2004).
24. D. Aerts, M. Czachor, Cartoon Computation: Quantum-like computing without quantum mechanics, *J. Phys. A: Math. Theor.* 40, F259-F266 (2007).
25. M. Czachor, Elementary gates for cartoon computation, *J. Phys. A: Math. Theor.* 40, F753-F759 (2007).
26. D. Aerts, M. Czachor, Tensor-product versus geometric-product coding, *Phys. Rev. A* 77, 012316 (2008).
27. D. Aerts, M. Czachor, Ł. Orłowski, Teleportation of geometric structures in 3D, *J. Phys. A: Math. Theor.* 42, 135307 (2009); Ł. Orłowski, praca magisterska, Politechnika Gdańska (2007).
28. T. Magulski, Ł. Orłowski, Geometric-algebra quantum-like algorithms: Simon's algorithm, preprint arXiv:0705.4289v1 [quant-ph] (2007); T. Magulski, praca magisterska, Politechnika Gdańska (2007).
29. D. Aerts, M. Czachor, B. De Moor, Geometric Analogue of Holographic Reduced Representation, *J. Math. Psychology* 53, 389-398 (2009). Jest to numer specjalny pt. *Quantum Cognition*.

30. A. Patyk, Geometric algebra model of distributed representations, w *Geometric Algebra Computing in Engineering and Computer Science*, red. E. Bayro-Corrochano, G. Scheuermann, Springer (2010).
31. A. Patyk, M. Czachor, D. Aerts, Geometric analogues of Holographic Reduced Representations and Binary Spatter Codes: Tests and perspectives, praca wysłana do IEEE Transactions on Knowledge and Data Engineering (kwiecień 2010).
32. D. Aerts, M. Czachor, M. Pawłowski, Entangled-state cryptographic protocol that remains secure even if nonlocal hidden variables exist and can be measured with arbitrary precision, *Phys. Rev. A* 73, 034303 (2006); Errata, *Phys. Rev. A* 73, 059901(E) (2006); M. Pawłowski, praca magisterska, Politechnika Gdańska (2006).
33. M. Czachor, Non-canonical quantum optics, *J. Phys. A: Math. Gen.* 33, 8081-8103 (2000).
34. M. Czachor, K. Wrzask, Automatic regularization by quantization in reducible representations of CCR: Point-form quantum optics with classical sources, *Int. J. Theor. Phys.* 48, 2511 (2009).
35. M. Wilczewski, M. Czachor, Theory versus experiment for vacuum Rabi oscillations in lossy cavities (II): Direct test of uniqueness of vacuum, *Phys. Rev. A* 80, 013802 (2009).
36. M. Czachor, Reducible representations of CAR and CCR with possible applications to field quantization, *J. Nonlin. Math. Phys. Supplement* 11, 78-84 (2004).
37. M. Czachor, States of light via reducible quantization, *Phys. Lett. A* 313, 380-388 (2003).
38. M. Czachor, J. Naudts, Regularization as quantization in reducible representations of CCR, *Int. J. Theor. Phys.* 46, 73-104 (2007).
39. M. Wilczewski, M. Czachor, Theory versus experiment for vacuum Rabi oscillations in lossy cavities, *Phys. Rev. A* 79, 033836 (2009).