Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2022/2023

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka Stosowana — Profil: Praktyczny

Forma sudiów: stacjonarne — Kod kierunku: MS

Stopień studiów: I

Specjalności: Analityka Danych,Matematyka z Informatyką

1 Informacje o przedmiocie

Nazwa przedmiotu	Wstęp do matematyki kwantowo-obliczeniowej
Nazwa przedmiotu w języku angielskim	Introduction to quantum-computational mathematics
Kod przedmiotu	WIiT MS pIS D14 22/23
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	3.00
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
6	30	30	0	0	0	0

3 Cele przedmiotu

Cel 1 Cel przedmiotu W XX wieku fizyka kwantowa dokonała rewolucji w zrozumieniu fundamentalnej natury świata, aw 21 - może dokonać rewolucji w teorii obliczeń komputerowych. Do 2020 roku, biorąc pod uwagę współczesne tempo miniaturyzacji podstawowych technologii komputerowych, staniemy w obliczu faktu, że podstawowe bloki średnich urządzeń i procesorów klasycznego komputera (Turinga) osiągnęły rozmiary porównywalne z atomowym i nie mogą być poprawnie opisane w ramach klasycznej teorii ocen. Dalszy roz-

wój technologii komputerowych jest niemożliwy bez zmiany środków klasycznej teorii ewaluacji opartej na fizyce klasycznej, z aparatem kwantowym, opartym na mechanice kwantowej. Zasadnicza różnica między charakterami praw kwantowych i klasycznymi wymaga, ogólnie rzecz biorąc, rewizji teorii ewaluacji w celu uświadomienia sobie różnic w zasadach funkcjonowania komputera kwantowego, jego zalet i wad w porównaniu z konwencjonalnym komputerem. I już dziś widać, że przezwyciężając problem miniaturyzacji urządzeń komputerowych i wyposażając je w kwantowy model operacji na danych otrzymujemy coś znacznie więcej niż możliwość dalszej kompaktacji podzespołów sprzętowych komputera. Uzyskamy dostęp do potencjalnie ogromnego zasobu obliczeniowego, istniejącego wyłącznie dzięki kwantowym właściwościom mechanicznym układów kwantowych (superpozycji stanów kwantowych i ich splątania) oraz mechanizmom kwantowym, które pozwolą nam operować informacją kwantową. Obecnie wiadomo już o kilku problemach, w których rozwiązaniu komputer kwantowy mógłby się znacznie udać w porównaniu z klasycznym komputerem. Przede wszystkim jest to problem faktoryzacji dużej liczby na czynniki pierwsze. Na konwencjonalnych komputerach najbardziej znane algorytmy faktoryzacji są realizowane za pomocą kroków, gdzie N - numer wejścia, a - długość wejścia jako logarytm do podstawy, określony przez skalę notacji. Tak więc takie algorytmy rosną wykładniczo wraz z rozmiarem danych wejściowych N, co jest barierą nie do pokonania dla dzisiejszego sprzętu komputerowego i raczej długoterminowej przyszłości, nawet dla liczby 250 jednostek. Jednak w 1994 roku opracowano algorytm faktoryzacji liczb na komputerze kwantowym, który jest wykonywany krokami, w których jest niewielką liczbą. Należy zaznaczyć, że stanowi bezpośrednie zagrożenie dla większości współczesnych kryptosystemów (RSA, EIGamal, DiffieHellman), opartych na faktoryzacji. Komputer kwantowy nie będzie miał wielomianu, ale mimo to znaczną przewagę, ponad klasyczną, w problemie wyszukiwania w niesortowanych bazach danych. W rezultacie niezbędny element można znaleźć tylko dla O (exp [(64/9) 1/3 (lnN) 1/3 (lnlnN) 2/3]) kroków, gdzie N - numer wejścia, a lnN - długość wejście jako logarytm podstawy, określony przez skalę notacji. Tak więc takie algorytmy rosną wykładniczo wraz z rozmiarem danych wejściowych N, co jest barierą nie do pokonania dla dzisiejszego sprzętu komputerowego i raczej długoterminowej przyszłości, nawet dla liczby 250 jednostek. Oto wyliczenie niektórych problemów, które komputer kwantowy obiecuje rozwiązać do tej pory w najbardziej imponujący sposób. W ramach PROGRAMU przedmiotu są zaplanowane takie tematy: Wprowadzenie. Podstawy matematyki kwantowej. 1. Krótka historia obliczeń kwantowych 2. Klasyczne podstawy obliczeń 3. Informacje kwantowe, bity kwantowe. 4. Obwody boolowskie 5. Obwody odwracalne 6. Obwody kwantowe Algorytmy dekrypcji obliczeń kwantowych 1. Szybka faktoryzacja 2. Kwantowa transformata Fouriera 3. Transformacja Hadamarda-Walsha 4. Kwantowa transformata Fouriera w Zn 5. Algorytm Shora dla faktoryzacji liczb 6. Od okresów do faktoringu. 7. Znajdowanie ukrytej podgrupy 8. Uogólniony algorytm Simona 9. Znalezienie zamówienia 10. Logarytm dyskretny 11. Oryginalny problem Simona Problem kwantowych poszukiwań obliczeniowych 1. Algorytm wyszukiwania Grovera 2. Problem wyszukiwania 3. Problem satysfakcji 4. Poszukiwanie probabilistyczne 5. Wyszukiwanie kwantowe za pomocą jednego zapytania 6. Metoda amplifikacji Grovera 7. Operatory kwantowe dla algorytmu wyszukiwania Grovera 8. Wykorzystanie metody wyszukiwania Grovera 9. Wyszukiwanie z nieznaną liczbą rozwiązań 10. Granice złożoności dla obwodów kwantowych 11. Uwagi, komentarze, perspektywy

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Wymaganie 1 Podstawy fizyki kwantowej: a) stany kwantowe; b) ewolucja stanów ; c) pomiary jednstek fizycznych d) efekt splatania qubitów; e) stany splątane; f) teleportacja informatyczna

2 Wymaganie 2 Podstawy matematyki: a)algebra linuiowa; b) definicja jednostki informacji-bit c) definicja jednostki informacji- kwantowej - qubit; d) iloczyn tensorowy wektorów przestzreni Hilberta; e) przestrzeni tensorowe; f) odwzorowania liniowe; g) bramki kwantowe; h) kodowanie informacji i) obliczenia kwantowe

5 Efekty kształcenia

EK1 Kompetencje społeczne a) Posiadanie nowoczesnej wiedzy w dziedzinie obliczeń kwantowo-komputerowych; b) Zdolność do działalności naukowej w kierunku "bezpieczeństwo informacji:

EK2 Umiejętności a) Umiejętność dokonywania oprogramowania nowoczesnych systemów informatycznych; b) Zdolność konstruowania nowoczesnych algorytmów wyszukiwania obiektów w bazach danych; c) Posiadanie umiejętności kodowania probabilistycznego informacji

EK3 Wiedza a) podstawy kwantowo-matematyczne oraz algebraiczne algorytmów obliczeniowych; c) algorytm faktoryzacju Shor'a liczb całkowitych;

EK4 Wiedza d) algorytm wyszukiwania obiektu w chmurze danych; e) podstawy kodowania informacji kwantowo-komputerowego;

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Treści programowe 1 Wprowadzenie. Podstawy matematyki kwantowej. 1. Krótka historia obliczeń kwantowych 2. Klasyczne podstawy obliczeń 3. Informacje kwantowe, bity kwantowe. 4. Obwody boolowskie 5. Obwody odwracalne 6. Obwody kwantowe	6
W2	Treści programowe 2 Algorytmy dekrypcji obliczeń kwantowych 1. Szybka faktoryzacja 2. Kwantowa transformata Fouriera 3. Transformacja Hadamarda-Walsha 4. Kwantowa transformata Fouriera w Zn 5. Algorytm Shora dla faktoryzacji liczb 6. Od okresów do faktoringu. 7. Znajdowanie ukrytej podgrupy 8. Uogólniony algorytm Simona 9. Znalezienie zamówienia 10. Logarytm dyskretny 11. Oryginalny problem Simona	12
W3	Treści programowe 3 Problem kwantowych poszukiwań obliczeniowych 1. Algorytm wyszukiwania Grovera 2. Problem wyszukiwania 3. Problem satysfakcji 4. Poszukiwanie probabilistyczne 5. Wyszukiwanie kwantowe za pomocą jednego zapytania 6. Metoda amplifikacji Grovera 7. Operatory kwantowe dla algorytmu wyszukiwania Grovera 8. Wykorzystanie metody wyszukiwania Grovera 9. Wyszukiwanie z nieznaną liczbą rozwiązań 10. Niższe granice złożoności dla obwodów kwantowych 11. Uwagi, komentarze, perspektywy	12

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
C1	Treści programowe 1 Ćwiczenia. 1.Algebra Liniowa (krótki przegląd) - zostaną przypomniane podstawowe terminy algebry liniowej.	2
C2	Treści programowe 2 2.Postulat 1 obliczeń kwantowych: Definicja bitu kwantowego lub kubitu. Pryzkłady kubitów, ich własności: norma, rozkład na elementy bazowe.	4
C3	Treści programowe 3 3. Postulat 2 obliczeń kwantowych: : Jak kubit (y) ewolują w przestzreni Euklidesowej-Hilberta, przykładu operatorów unitarnych. Odwzorowanie fazowe, przykłady.	4
C4	Treści programowe 4 4.Postulat 3 obliczeń kwantowych: Efekty pomiarów kwantowych: oczekiwanie matematyczne.	4
C5	Treści programowe 5 5.Postulat 4 obliczeń kwantowych: Analiza sposobów łączenia kubitów w systemy kubitów, wielokubitowe stany.	4

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
C6	Treści programowe 6 6.Przykłady splątania stanów kwantowych.	4
C7	Treści programowe 7 7.Przykłady teleportacji stanów.	4
C8	Treści programowe 8 8.Konstruowanie bramek algorytmów obliczeniowych. Rotacja bramek, superpozycja bramek. 9.Algorytm Deutscha, przykłady. Analiza algorytmu Deutscha z punktu widzenia algorytmów klasycznych: jak wszystkie znane algorytmy kwantowe, które zapewniają wykładniczą złożoność w stosunku do klasycznych systemów, odpowiada na pytanie o globalną właściwość zbioru wszystkich możliwych rozwiązań. Są one często nazywane problemami obietnicowymi, w których struktura przestrzeni rozwiązań ma być w pewnej zadanej postaci przy czym trzeba ostrożnie używać superpozycji i splątania, więc mozliwe wtedy zakłócenia nie pozwolą wyodrębnić potrzebnej informacji. Powodem, dla którego te problemy uzyskują wykładniczą złożoność w stosunku do wszystkich znanych klasycznych	4

7 Narzędzia dydaktyczne

N1 Narzędzie 1 A. Kitayev, Quantum Computing, AMS, 2012

N2 Narzędzie 2 P. Shor. Polynomial-time algorithms for prime factorization and discrete logs on a quantum computer //SIAM J. Sci. Statist. Comput. 1997, v. 26, 1484 p.

N3 Narzędzie 3 R. Feynman. Simulating physics with computers //Int. J. Theoret. Phys. 1982, v. 21, p. 467-488.

N4 Narzędzie 4 L.K. Grover. A fast quantum mechanical algorithm for database search //Proc. 28th Annual ACM Problems Of Atomic Science And Technology (PAST).-2007.-No.3(1).-p.230-235 Symposium on the Theory of Computing. 1996, p. 212-219.

N5 Narzędzie 5 C. Monroe et. al. Demonstration of a Fundamental Quantum Logic Gate //Physical Review Letters. 1995, v. 75, p. 4714-4717

N6 Narzędzie 6 . D. Deutsch. Quantum theory, the Church-Turing principle, and the universal quantum computer //Proc. R. Soc. London A., 1985, v. 400, p. 97-117.

N7 Narzędzie 7 D. Deutsch, A. Barenco, A. Ekert. Universality in quantum computation //Proc. Roy. Soc. London A 1995, v. 449, p. 669-677.

N8 Narzędzie 8 R. Rivest et al. On digital signatures and public-key cryptosystems: Preprint MIT/LCS/TR-212,MIT Laboratory for Computer Science, 1979.

N9 Narzędzie 9 M.A. Nielsen, I.L. Chuang. Quantum Computation and Quantum Information. Cambridge: "Cambridge University Press", 2000, 665 p. 10) A. Barenco et al. Elementary gates for quantum computation. //Phys.Rev. A. 1995, v. 52, p. 3457-3488. 11) D.P. Di Vincenzo. Quantum computation //Science. 1995, v. 270, N 5234, p. 255-261. 12) G.P. Collins. Computing with Quantum Knots //Scientific American. April 2006, p. 57-63. 13) P.W. Shor. Scheme for reducing decoherence in quantum computer memory //Phys. Rev. A. 1995, v. 52, p. 2493–2496.

N10 Narzędzie 10 D.P. Di Vincenzo. Quantum computation //Science. 1995, v. 270, N 5234, p. 255-261..

N11 Narzędzie 11 G.P. Collins. Computing with Quantum Knots //Scientific American. April 2006, p. 57-63

N12 Narzędzie 12 Mathematics of Quantum Computation and Quantum Technology: Edited by Goong Chen Louis Kauffman Samuel J. LomonacoAPPLIED MATHEMATICS AND NONLINEAR SCIENCE SERIES Boca Raton London New York Chapman & Hall/CRC

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	5
Egzaminy i zaliczenia w sesji	0
kolokwium	5
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	7
Opracowanie wyników	6
Przygotowanie raportu, projektu, prezentacji, dyskusji	7
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**90**
Sumaryczna liczba punktów ECTS dla przedmiotu	3.00

9 Sposoby oceny

1) kolokium (2)

Ocena formująca

F1 Ocena 1 kolokwium

F2 Ocena 2 kolokwium

Ocena podsumowująca

P1 Ocena 1 Średnia ocena na podstawie kolokwiów

Warunki zaliczenia przedmiotu

W1 Ocena 1 pozytywne oceny na podstawie kolokwiów

Ocena aktywności bez udziału nauczyciela

B1 Ocena 1 aktywny udział na ćwiczeniach

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie spełnia kryteriów na ocenę 3.0.
Na ocenę 3.0	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, potrafi objaśnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania
Na ocenę 3.5	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, potrafi objaśnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne,
Na ocenę 4.0	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, potrafi objaśnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych
Na ocenę 4.5	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, potrafi objaśnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasadydziałania bramek kwantowych, umie skonstruować algorytm obliczenia zadanej funkcji
Na ocenę 5.0	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, potrafi objaśnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych, umie skonstruować algorytm obliczenia zadanej funkcji, korzysta z metody dyskretnej transformacji Fourier'a
Efekt kształcenia 2	
Na ocenę 2.0	Student nie spełnia kryteriów na ocenę 3.0.
Na ocenę 3.0	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania,
Na ocenę 3.5	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne,
Na ocenę 4.0	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej,może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych,
Na ocenę 4.5	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych, umie skonstruować algorytm obliczenia zadanej funkcji, korzysta z metody dyskretnej transformacji Fourier'a
Na ocenę 5.0	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, podrafi objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych, umie skonstruować algorytm obliczenia zadanej funkcji, korzysta z metody dyskretnej transformacji Fourier'a
Efekt kształcenia 3	

Na ocenę 2.0	Student nie spełnia kryteriów na ocenę 3.0.
Na ocenę 3.0	posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania,
Na ocenę 3.5	posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne,
Na ocenę 4.0	posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych,
Na ocenę 4.5	posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych, umie skonstruować algorytm obliczenia zadanej funkcji,
Na ocenę 5.0	posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objasnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania, rozwiązuje zadania praktyczne, objaśnia zasady działania bramek kwantowych, umie skonstruować algorytm obliczenia zadanej funkcji, korzysta z metody dyskretnej transformacji Fourier'a
Efekt kształcenia 4	
Na ocenę 2.0	Student nie spełnia warunków na ocenę 3.0.
Na ocenę 3.0	Student posiada podstawową wiedzę z matematyki kwantowo-komputerowej, może objaśnić algorytmy Shore'a, Growera oraz teoretyczne zasady kodowania.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	K_W01 K_W20	Cel 1	W1 W2 W3 C1 C2 C3 C4 C5 C6 C7 C8	N1 N2 N3 N4 N5 N6 N7 N8 N9 N10 N11 N12	F1 F2 P1
EK2	K_W02 K_U25	Cel 1	W1 W2 W3 C1 C2 C3 C4 C5 C6 C7 C8	N1 N3 N4 N5 N6 N7 N8 N9 N10 N11 N12	F1 F2 P1
EK3	K_W01 K_U13	Cel 1	W1 W2 W3 C1 C2 C3 C4 C5 C6 C7 C8	N1 N2 N3 N4 N5 N6 N7 N8 N9 N10 N11 N12	F1 F2 P1

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK4	K_W02 K_K06	Cel 1	W1 W2 W3	N1	F1 F2 P1

11 Wykaz literatury

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr Mariusz Jużyniec (kontakt: juzyniec@pk.edu.pl)

Osoby prowadzące przedmiot

1 prof. dr hab Anatolij Prykarpatski (kontakt: anatolij.prykarpastki@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .