



STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Kvantinių kompiuterių įvadas	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: doc. dr. Mindaugas Mačernis	Fizikos fakultetas

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	Pasirenkamas

Igyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	6 semestras	Lietuvių, anglų

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Studentas turi būti išklaušęs kvantinės mechanikos ir struktūrinio programavimo pagrindus.	Gretutiniai reikalavimai (jei yra): nėra

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	140	64	76

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos			
Suvokti pagrindinius kvantinio kompiuterio veikimo ir su juo skaičiavimo principus. Gebėti programuoti algoritmus kvantiniam kompiuteriui ir jo simulatoriui.			
Dalyko (modulio) studijų siekiniai	Studijų metodai	Vertinimo metodai	
Gebės paaiškinti kvantinio kompiuterio ir kvantinės informacijos principus.	Paskaitos, pratybos, savarankiškas darbas.	Savarankiškas darbas, egzaminas.	
Gebės projektuoti ir programuoti nesudėtingus kvantinio kompiuterio programų projektus	Paskaitos, pratybos, savarankiškas darbas.	Savarankiškas darbas, egzaminas.	
Studentas gebės pasirinkti optimaliausią kvantinį algoritmo metodiką.	Paskaitos, pratybos, savarankiškas darbas.	Savarankiškas darbas, egzaminas.	

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminariai	Pratybos	Laboratoriniai darbai	Praktika	Visas kontaktinis darbas	Savarankiškas darbas	Užduotys
1. Kvantiniai skaičiavimai Skaičiavimo modeliai: Tiuringo (Turing) mašina, teorinė kompiuterinė algebra. Kompiuterinių taikymų analizė: kompiuterinis kompleksiskumas, loginiai sprendimų uždaviniai, sudėtingos perteklinės klasės ir pertekliniai skaičiavimai. Kvantinė	20							22	Literatūra, užduotys.

mechanika: Šmidto (Schmidt) dekompozija, EPR (Einstein-Podolsky-Rosen) paradoksas ir Belo (Bell) nelygybė. Kvantinė teorinė kompiuterinė algebra. Kvantiniai algoritmai. Kubitas. Kubito operacija. Universalūs kvantiniai elementai. Kvantinis kompiuterinės algebros modelis. Kvantinių sistemų simuliacija. Kvantinė Furje transformacija. Fazės įvertinimas. Kvantinės Furje transformacijos algoritmai. Kvantinės paieškos algoritmai. Kvantinė paieška kaip kvantinė simuliacija. Kvantinė paieška nestruktūrizuoti duomenų basei. Juodos dėžės algoritmų ribos.								
2. Kvantinių kompiuterių fizinis realizavimas. Kvantinių skaičiavimų sąlygos. Harmoniniais osciliatoriais grįstas kvantinis kompiuteris. Optiniais fotonais grįstas kvantinis kompiuteris. Kvantinė elektrodinamika. Jonų gaudyklės. Branduolinis magnetinis rezonansas. Kitos realizavimo schemos.	8						10	Literatūra, užduotys.
3. Kvantinės informacijos įvadas. Kvantinis triukšmas ir kvantinės operacijos. Kvantinis triukšmo ir kvantinių operacijų pavyzdžiai. Kvantinių operacijų formalizmo ribos. Atstumas ir kvantinė informacija. Klaidoms palankus kvantinis skaičiavimas. Kvantinis informacijos perdavimas per triukšmingus kvantinius kanalus. Kvantinis supainiojimas (entanglement). Kvantinė kriptografija. Kvantinių raktų perdavimas ir saugumas.	4						6	Literatūra, užduotys.
4. Kvantinis kompiuteris, skaičiavimai, kvantinio kompiuterio simulatoriai					16		18	Literatūra, užduotys.
5. Kvantinis kompiuteris ir skaičiavimai					14		16	Literatūra, užduotys.
6. Kvantinės informacijos įvadas					2		4	Literatūra, užduotys.
Iš viso	32				32		76	

Vertinimo strategija	Svoris proc.	Atsiskaitymo laikas	Vertinimo kriterijai
Savarankiškas darbas	70	1–16 semestro savaitės	Pratybų metu atliekamos pavyzdinės užduotys, išsiaiškinamos jų programinio įgyvendinimo galimybės. Studentai privalo atlikti ir atsiskaityti 80% pratybų, laboratorinių ir savarankiškų užduočių. Rašomas vienas kontrolinis darbas (K1) ir vienas referatas (K2).
Egzaminas	30	16-a semestro savaitė	Egzaminas: atsakymai į klausimus raštu ir žodžiu. Egzamino metu pateikiami 2 klausimai (K3). Gautinis įvertinimas: $P = 0,35 K1 + 0,35K2 + 0.3 K3$.

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda
Privaloma literatūra				
Radhika Vathsan	2015	Introduction to Quantum Physics and Information Processing		CRC Press
Michael A. Nielsen, Issac L. Chuang	2011	Quantum Computation and Quantum Information		Cambridge University Press
Ved Prakash Gupta, Prabha Mandayam, V.S. Sunder	2015	The Functional Analysis of Quantum Information Theory: A Collection of Notes Based on Lectures		Springer
Papildoma literatūra				
Hans Delfs, Helmut Knebl.	2015	Introduction to Cryptography: Principles and Applications (Information Security and Cryptography)		Springer
Song Y. Yan	2013	Quantum Attacks on Public-Key Cryptosystems		Springer