Nr.	Dėstytojas	Tema LT	Tema En	Pastabos
1	Adomas Birštunas	Skaičiavimai BDI logikai	Calculi for BDI logic	
2	Agnė Brilingaitė	Elektromobilio pasiekiamos zonos skaičiavimas	Computation of iso-chrone regions for electric vehicles	Daugelio dabar naudojamų elektromobilių, ypač pigesnių, akumuliatorių talpa yra ribota. Svarstant ar pirkti elektromobilį, bei pradėjus jį naudoti, neretai minimas taip vadinamas "range anxeity" -- netikrumas ar pakaks energijos nuvažiuoti ten kur reikia. Egzistuojantys servisai bei informacinės sistemos pačiuose automobiliuose gali pateikti tik gana apytikslę informaciją apie elektromobilio pasiekiamą zoną. Būtų įdomu patyrinėti algoritmus, kurie kaip galima našiau ir tiksliau paskaičiuotų geografinę zoną, kuri yra elektromobilio pasiekiama per duotą laiką. Tokia zona yra vadinama isochrona. Kaip duomenis būtų galima naudoti duomenis apie esamą ir numatomą eismo situaciją (pvz. iš Google Maps), bei elektromobilio energijos vartojimo modelius. Taip pat būtų galima nagrinėti kaip konstruoti ir palaikyti tokius modelius remiantis realiais konkretaus elektromobilio eksploatavimo duomenimis. Problema darosi sudėtingesnė, jei dalį laiko galima skirti baterijų krovimuisi prieš išvykstant. Pasirinkus šią temą, bus galimybė įsidarbinti programuotoju projekte "Duomenų valdymas ir algoritmai sumaniam transportui (Daltra)": (https://tinyurl.com/rdmuhct) Kreiptis į Simoną Šaltenį arba Agnę Brilingaitę. S. Šaltenis bus studentės(-o) konsultantas.
3	Agnė Brilingaitė	Transporto maršrutų planavimas dinaminėje aplinkoje: ar naudoti papildomas duomenų struktūras?	Exploration of pre-computation for routing algorithms on highly dynamic trasportation networks	Kad paspartinti transporto maršrutų planavimo algoritmus ant didelių žemėlapių, naudojamos įvairios papildomos grafų duomenų struktūros, kurios suskaičiuojamos remiantis kelių žemėlapiu prieš pradedant vykdyti maršrutų planavimo užklausas. Tokia taktika puikiai veikia, jei žemėlapis, įskaitant atributus susietus su kelių atkarpomis, nekinta. Visgi moderniuose navigacijos servisuose, pvz. Google Maps, minėti atributai pastoviai kinta. Pavyzdžiui, kintant eismui, kinta ir numatytas laikas, kurio reikia, kad pravažiuoti duotą kelio atkarpą. Kintant atributams, reikia pataisyti arba perskaičiuoti ir papildomas duomenų struktūras. Taigi papildomos duomenų struktūros pagreitina užklausas (reduced query latency), bet deja sumažina kiek žemėlapio duomenų keitimų galima įvykdyti per laiko vienetą (reduced update throughput), kas reiškia mažiau "šviežią" žemėlapį. Pasirinkus modernią grafų duomenų struktūrą, projektas galėtų pastudijuoti balansą tarp šių dviejų prieštaraujančių vienas kitam "quality of servise" reikalavimų. Pasirinkus šią temą, bus galimybė įsidarbinti programuotoju projekte "Duomenų valdymas ir algoritmai sumaniam transportui (Daltra)": (https://tinyurl.com/rdmuhct) Kreiptis į Simoną Šaltenį arba Agnę Brilingaitę. S. Šaltenis bus studentės(-o) konsultantas.
4	Agnė Brilingaitė	Transporto maršrutizavimo algoritmų lygiagretinimo strategijos	Paralellization strategies for advanced routing algorithms	Naujos kartos transporto maršrutizavimo algoritmai ant labai dinamiškų transporto žemėlapio duomenų susiduria su našumo problemomis. Dėl duomenų dinamiškumo, sudėtinga naudoti iš anksto paskaičiuotas grafų duomenų struktūras, kurios įprastai naudojamos pagreitinti maršrutizavimo algoritmus. Kitas būdas pagreitinti tokius algoritmus yra jų lygiagretinimas. Būtų įdomu patyrinėti, kaip geriausiai lygiagretinti tokius algoritmus, išnaudojant šiuolaikinių procesorių ir grafikos procesorių GPU galimybes. Pasirinkus šią temą, bus galimybė įsidarbinti programuotoju projekte "Duomenų valdymas ir algoritmai sumaniam transportui (Daltra)": (https://tinyurl.com/rdmuhct) Kreiptis į Simoną Šaltenį arba Agnę Brilingaitę. S. Šaltenis bus studentės(-o) konsultantas.
5	Gintaras Skersys	McEliece viešojo rakto kriptografinės sistemos saugumo tyrimas	Study of the Security of the McEliece Public-Key Cryptosystem	
6	Gintaras Skersys	Courtois-Finiasz-Sendrier skaitmeninio parašo schemos ir jos variantų tyrimas	Study of the Courtois-Finiasz-Sendrier Digital Signature Scheme and Its Variants	
7	Gintaras Skersys	Turbo kodų tyrimas	Study of Turbo Codes	
8	Gintautas Dzemyda	Geometrinio Daugiamačių skalių metodo, skirto daugiamačiams duomenims vizualizuoti, tyrimas	Investigation of the Geometric multidimensional scaling for multidimensional data visualization	Eksperimentinis metodo tyrimas, siekiant kuo geresnės duomenų vizualizavimo kokybės

9	Gintautas Dzemyda	Kepenų radiologinių vaizdų analizė siekiant nustatyti vėžio pažeistą vietą	Analysis of radiological images of the liver to identify the site of cancer	Vaizdų analizės uždavinys
10	Gintautas Dzemyda	Duomenų klasifikatorių efektyvumo priklausomybės nuo besikeičiančios mokymo imties tyrimas	A study of the dependence of the efficiency of data classifiers on a changing training sample	Reikės patyrinėti kelis klasikinius duomenų klasifikatorius
11	Gintautas Dzemyda	Geometrinio daugiamačių skalių metodo daugiaekstremiškumo tyrimas	A study of multiextremality of the geometric multidimensional scaling	Eksperimentinis metodo tyrimas, siekiant įvertinti optimizuojamos funkcijos daugiaekstremiškumą.
12	Haroldas Giedra	Buridano logikos verifikavimas	Verification of Buridan logic	
13	Haroldas Giedra	Matematinės logikos įrankių taikymas fizikoje	Applications of mathematical logic tools on physics	
14	Haroldas Giedra	Išvedimo paieška laiko logikai	Proof search for temporal logic	
15	Irmantas Radavičius	Studento pasirinkta tema	Student Propoused Topic	Gali būti rengiamas darbas studento pasirinkta/pasiūlyta tema duomenų struktūrų ir algoritmų, grafų teorijos, algoritmų analizės tematikose. Susidomėjus, dėl temos formulavimo ir konkretizavimo KUO ANKSČIAU susisiekti su vadovu.
16	Julius Žilinskas	Pusiau teigiamai apibrėžtas optimizavimas	Semidefinite programming	
17	Julius Žilinskas	Kalnų kelionių technikos trasų įveikimo modeliavimas ir optimizavimas	Imitation and optimization of accomplishment of mountaineering routes	
18	Karolis Petrauskas	TLA+ specifikacijų išskyrimas iš programinio kodo BEAM virtualiai mašinai.	Extracting TLA+ specifications out of a program for a BEAM virtual machine.	Formal languages are widely used to design and verify distributed systems and algorithms. One of such languages is TLA+ (https://lamport.azurewebsites.net/tla/book-02-08-08.pdf). Specifications are designed at a high level using TLA+, thus there is a gap between an implementation and the spec. Erlang/OTP is a programming language designed for building distributed systems and is used to build online game servers, banking applications, systems integrations and other. This language is compiled to several intermediate formats, that can be used to extract program structure. The aim of this topic is to develop a translation from a BEAM based language (Erlang/Elixir/LFE or other) to a TLA+ specification. The extracted specification then could be used to prove a refinement mapping between the abstract specification and the extracted one thus narrowing the gap between the spec and the implementation. One of the attempts to formalize the semantics of the intermediate format can be found here <https://dl.acm.org/doi/10.1145/3406085.3409008>. See also references in the related work section.
19	Karolis Petrauskas	Formalių specifikacijų taikymas projektuojant paskirstytas sistemas.	Applying formal specifications to design distributed systems.	A student should develop a formal specification in the TLA+ language (https://lamport.azurewebsites.net/tla/book-02-08-08.pdf) for a chosen distributed algorithm (e.g. Kademlia) or a system (e.g. Kafka replication, Riak KV, RabbitMQ distribution, LevelDB). Another specification language can be chosen, if it will be more appropriate for the specific task. The specification will be used to investigate properties of the selected system or the algorithm. If any flaws are identified, solutions should be provided and validated formally. In the case of notable results, a student is encouraged to present them in a scientific conference.
20	Linas Laibinis	Paskirstytų, gedimams atsparių, dinamiškai konfiguruojamų programų sistemų formalus modeliavimas ir verifikavimas	Formal modelling and verification of distributed, fault tolerant, dynamically reconfigurable software-based systems	Darbo metu yra sukuriamas pasirinktos paskirstytos programinės sistemos formalus modelis (remiantis jos aprašymu ar reikalavimų sąrašu). Sukurtas modelis yra analizuojamas ir verifikuojamas, naudojantis automatinio įrodymo ar modelių patikrinimo įrankiais. Atsparumas gedimams ir galimybė dinamiškai konfiguruoti tokias sistemas priklausomai nuo besikeičiančios aplinkos yra esminės savybės, į kurias fokusuojamasi verifikavimo metu.
21	Linas Laibinis	Sistemų prototipų kūrimas ir skaitinis įvertinimas naudojant diskretinių įvykių simuliavimo metodus	System prototyping and quantitative assessment by discrete event simulation techniques	Diskretinių įvykių simuliavimo aplinkos leidžia sukurti būsimos paskirstytos sistemos prototipą, aprašyti joje vykstančius įvykius, komunikacijas tarp komponenčių, galimus gedimus ir modeliuoti laiko pauzes. Darbo metu sukurto sistemos prototipo simuliavimas duotų galimybę skaitiškai įvertinti sistemos darbo charakteristikas (efektyvumą, patikimumą ir t.t.) bei tuo pačiu palyginti skirtingas tokių sistemų konfiguracijas.

22	Linas Laibinis	Paskirstytų sistemų modeliavimas ir verifikavimas remiantis statistinio modelių patikrimo metodais	Modelling and verification of distributed systems using statistical model checking methods	Darbo metu sukurtas paskirstytos sistemos modelis (prototipas) yra analizuojamas statistinio modelių patikrinimo metodais (pvz., naudojantis automatizuota aplinka Uppaal). Analizės rezultatas yra statistinis ar tikimybinis suformuluotų sistemos savybių (efektyvumo, patikimumo ir t.t.) ar jos skaitinių apribojimų įvertini as bei grafinis pateikimas.
23	Linas Laibinis	Paskirstytų programinių sistemų kūrimas ir skaitinis įvertinimas naudojantis komunikavimo šablonais	Design and quantitative evaluation of distributed software-based systems using communication patterns	Darbo metu yra skaitiškai įvertinami paskirstytų sistemų kūrime naudojami komunikavimų šablonai ir jų kompozicijos. Identifikuojami sistemos ar šablonų parametrai, tiesiogiai įtakojantys sistemos darbą, ir jų optimalumas yra analizuojamas naudojantis statistinio ar įprasto modelių patikrinimo metodais.
24	Linas Laibinis	Automatizuotos matematinio įrodymo ir sistemų verifikavimo aplinkos	Automated environments for mathematical proof and system verification	Darbe palyginamos plačiai naudojamos automatizuotos matematinio įrodymo ir sistemų verifikavimo aplinkos. Analizės metu yra fokusuojamasi į esamas automatinio įrodymo priemones ir jų plėtimo galimybes bei galimybę integruoti skirtingus verifikavimo įrankius vieno projekto ribose.
25	Linas Litvinas	Dirbtiniai neuroniniai tinklai laiko eilutėms	Artificial neural networks for time series	
26	Linas Litvinas	Biojutiklio daugiakriterinis optimizavimas	Multiobjective optimization of biosensor	
27	Linas Petkevičius	Pamaininio darbo tvarkaraščio sudarymas naudojant giliuosius neuroninius tinklus	Shift sheduling using deep neural networks	
28	Mindaugas Bloznelis	Epidemijos plitimas tinkle	Epidemic spread in networks	Epidemijos plitimo ir kontrolės (įvairių stabdymo priemonių taikymas) modeliavimas dideliuose socialiniuose tinkluose.
29	Mindaugas Bloznelis	Tinklo bendruomenių paieška	Network community detection.	Tinklo bendruomenių atskleidimas. Algoritmų veikimas realiuose tinkluose, algoritmų analizė sintetiniuose tinkluose. (Spektrinis algoritmas, atsitiktinio klaidžiojimo algoritmas)
30	Olga Kurasova	Generatyviniai besivaržantys neuroniniai tinklai vaizdams iš teksto generuoti	Generative Adversarial Networks for Synthesis of Images from Text	
31	Olga Kurasova	Dirbtinių neuroninių tinklų generalizavimo savybių tyrimas	Investigation of Generalization Properties of Artificial Neural Networks	
32	Olga Kurasova	Transformatorių tinklai natūraliai kalbai apdoroti	Transformer Networks for Natural Language Processing	
33	Pijus Kasparaitis	Lietuvių kalbos sintezė naudojant neuroninius tinklus	Text-to-speech synthesis of Lithuanian based on neural networks	Dėstytojui dėl temos rašyti šiuo e-pašto adresu: pkasparaitis@yahoo.com
34	Rimantas Vaicekauskas	Pamaininio darbo tvarkaraščio optimizavimo algoritmų lygiagretus įgyvendinimas	Parallel implementation of shift sheduling optimization algorithms	
35	Rimantas Vaicekauskas	Pamaininio darbo tvarkaraščio optimizavimo algoritmai	Shift sheduling optimization algorithms	
36	Saulius Gražulis	Gardelės parametrų išgavimas iš žmogui skirtų tekstų ir COD apžvalginės DB kūrimas	Extrating Unit cell parameters of crystals from human-readible scientific papers	Deja, kol kas ne visuose straipsniuose paskelbtos kristalų struktūros yra atvirai aprašytos viešai prieinamais duomenimis. Daugeliui tokių „paslėptų“ struktūrų straipsniuose nurodomi pagrindiniai kristalo parametrai – gardelės konstantos, simetrijos grupė, molekulės cheminė formulė ir pavadinimas. Tai, nors ir nepilni, bet vis viena labai vertingi duomenys, nes leidžia preliminariai identifikuoti kristalinę medžiagą. Kursiniame darbe bus pasiūlyta surinkti visų publikuotų kristalų struktūrų bibliografijas ir pagal atvirai prieinamus straipsnių tekstus arba santraukas (abstracts), naudojant paprastas Perl reguliarias išraiškas (o vėliau gal būt ir sudėtingesnę lingvistinę analizę) automatiškai išgauti kiekviename straipsnyje publikuotų medžiagų kristalų parametrus.

37	Saulius Gražulis	Informacijos išgavimas iš mokslinių straipsnių	Extracting scientific facts from research papers	Pastaruoju metu publikuojamų mokslinių straipsnių skaičius auga eksponentiškai [1]. Tikėtina, kad šiuo metu straipsnių paskelbiama tiek daug, jog net ekspertai negali fiziškai perskaityti visų straipsnių savo darbų tematika, jau nekalbant apie gretimų tyrimo krypčių straipsnius. Mokslo žinios tampa išsklaidytos po daugelį žmogui sunkiai aprėpiamų šaltinių, jas vis sunkiau susisteminti, o tarpdisciplininiai tyrimai – vienas svarbių inovacijos šaltinių – dėl šių priežasčių neatskleidžia viso savo potencialo. Turėtų būti įmanoma sukurti apmokytus DNT ir/arba kitas kompiuterines sistemas, gebančias iš žmogui skirto teksto (mokslinio straipsnio, patento, monografijos, disertacijos, preprinto) išgauti faktinę mokslinę informaciją, pvz. medžiagos formulę, kristalo ir molekulės struktūros aprašymą, molekulės chemines ir fizines savybes, tų savybių epistemologinį statusą (matavimo rezultatas, teorinis skaičiavimas), ir pateikti šią informacija formalizuotu, automatiniam apdorojimui tinkamu pavidalu, pavyzdžiui, formaliai specifikuotų CIF, CML a SDF failų pavidalu, reliacinių duomenų lentelių pavidalu, RDF failų pavidalų naudojant kurią nors žiniatinklio ontologiją ar pan. Darbe bus pasiūlyta, pasitelkiant įvairias teksto analizės priemones (teksto segmentatorius, simbolių atpažinimo programas, tokias kaip 'tesseract', dirbtinius neuroninius tinklus, mašinų mokymo programas) išgauti iš mokslinių straipsnių vertingus faktus ir apjungti juos į sistemingą duomenų bazę greitai ir išsamiai paieškai.
38	Saulius Gražulis	Naršyklės įskiepis kristalografinei informacijai rinkti	Browser plugin for collection of scientific information	Šiuolaikiniame mokslo pasaulyje labai didelė informacijos dalis yra išbarstyta po daugybę teksto puslapių (mokslinių straipsnių, disertacijų, monografijų), ir jų sisteminga paieška kompiuterinėmis priemonėmis yra labai apsunkinta. Deja, automatinė tekstų analizė ne visada sugeba teisingai išgauti reikiamus duomenis, ir tenka įdėti daug žmogaus rankų darbo, įvedant informaciją į kompiuterizuotas duomenų bazes. Siūloma sukurti įrankį, kuris palengvintų tyrėjams informacijos surinkimą ir kaupimą vienoje gerai struktūruotoje duomenų bazėje. Siūlomas darbas būtų skirtas įskiepiui, kuris padeda rinkti kristalografinę ir cheminę informaciją, sukurti. Tai leistų šimtams tyrėju vienu metu visame pasaulyje rinkti informaciją, dėti ją į bendrą duomenų bazę ir po to bendrai naudotis surinktais duomenimis. Toks modelis jau neblogai pasiteisino renkant citavimo ir bibliografinius duomenis; naudinga būtų pritaikyti jį kitoms mokslo duomenų rūšims.
39	Saulius Gražulis	Mažų molekulių, randamų COD DB, susiejimas su PDB	Linking the Crystallography Open Database (COD) with the Protein Data Bank (PDB)	COD duomenų bazėje sukaupta virš 450000 įrašų apie mažų molekulių kristalų struktūras. Apie 2/3 jų yra organinės molekulės. Dalis tų molekulių yra ligandai, kofaktoriai ar vaistai, galintys jungtis su baltymų molekulėmis, o šių baltymų struktūros gali būti randamos PDB duomenų bazėje. Darbo metu bus pasiūlyta surasti tas molekules COD duomenų bazėje, kurios yra chemiškai tokios pačios, kaip ir PDB archyve rasti ligandai, ir susieti COD su PDB, naudojant PDB papildomos informacijos pateikimo JSON schemą.
40	Saulius Gražulis	Saugumo auditas COD ir panašiose interneto svetainėse	Security audit in the Crystallography Open Database and related Web sites.	Žiniatinklis (World Wide Web) buvo sukurtas tam, kad įgalintų mokslininkus greitai ir patogiai keistis tyrimų rezultatais bei kita informacija. Naujos žiniatinklio priemonės leidžia ne tik parsisiųsti informaciją iš nutolusios svetainės, bet ir interaktyviai pateikti informaciją šioms svetainėms arba paleisti procesus nutolusiuose serveriuose. Deja, šios galimybės atveria eilę saugumo spragų – serveriai gali būti panaudojami ne taip ir ne tam, kam jie buvo sukurti, ir tai gali atsitikti be svetainės kūrėjo žinios. Šiame darbe, naudojant įvairius svetainių audito įrankius (e.g Kali Linux), bus pasiūlyta patikrinti įvairių mokslo duomenims skurtų interneto svetainių (COD, RestfulDB, Web Scriptlets) saugumą; kitaip tariant, pabandyti „nulaužti“ ;) programinę įrangą, kurios pagrindu veikia šios svetainės, ir pasiūlyti, kaip galima nuo išnagrinėtų grėsmių apsisaugoti.

41	Saulius Gražulis	Teisingumo įrodymų palaikymas daugiaparadigminėje programavimo kalboje Starta	Integrating correctness proofs into multi-paradagim programming language Starta.	Šiuolaikiniai aukšto lygio programavimo kalbų kompiliatoriai stebimai padidino programuotojų darbo efektyvumą, palyginus su autokodais ar asemblerio kalbomis. Deja, nuo to laiko nauja "magiška kulka", leidžianti pasiekti dar didesnių darbo našumų ar aukštesnės programų kokybės, taip ir nėra atrasta. Vienas iš stebėtinų dabartinių kompiliatorių trūkumų -- visiškas atotrūkis tarp teorinių darbų, skirtų programų teisingumo įrodymams, ir praktiniam programavimui naudojamų programavimo kalbų bei kompiliatorių. Darbo eigoje bus siūloma realizuoti automatinę sistemą teiginiams apie programą įrodyti, integruotą į aukšto lygio programavimo kalbos kompiliatorių. Pirmame etape planuojama naudoti specialiai tam tikslui sukurtą programavimo kalbą ir kompiliatorių, kuriuos, reikalui esant, galima keisti, siekiant supaprastinti įrodymų išvedimą; tačiau sistema turėtų būti pakankamai moduliarizuota, kad įrodymų posistemę galima būtų perkelti į kitų kalbų (Java, C, C++, C#, Perl, Python, etc.) kompiliatorius.
42	Saulius Gražulis	Mažų molekulių kristalų kontaktų paviršiai	Contact surfaces in small molecule crystals	Siūloma peržvelgti visas COD organinių kristalų struktūras, visų pirma tas, kuriuose yra vaistinių medžiagų molekulės ar į jas panašios molekulės. Surasti šių molekulių kontaktus su *savo pačių* kristalais, aprašyti šių kontaktų paviršius. Surasti tas molekules, kurių kompleksai su baltymais patalpinti PDB archyve. Palyginti mažos molekulės kristalo ir baltymo kontaktinius paviršius; nustatyti, ar pagal šių paviršių panašumą galima prognozuoti susirišimą su baltymu.
43	Saulius Gražulis	Paskirstytos, patikimos ir atsparios trikdžiams bei padalinimams COD duomenų bazės kūrimas.	Creating reliable and fault-tolerant server system for Crystallography Open Database	Šiuo metu COD duomenų bazė, organizuota kaip centrinis (angl. "master") serveris, kurio duomenis patikimumo dėlei replikuoja visa eilė antrinių (angl. "mirror") kompiuterių. Tokia sistema, deja, neužtikrina nenutrūkstamo sistemos darbo, centriniam serveriui išėjus iš rikiuotės ar nutrūkus ryšiui tarp centrinio serverio ir Interneto. Darbo metu bus siūloma realizuoti paskirstytą, lygių serverių mainais (angl. "peer-to-peer") paremtą sistemą, atsparią sistemos padalinimui, užtikrinančią duomenų neprieštaringumą (consistency) ir minimizuojančią sistemos prastovas. Nors CAP teorema teigia, kad visų trijų tikslų (neprieštaringumo, prieinamumo ir atsparumo padalinimams) vienu metu pasiekti nejmanoma, bus bandoma surasti inžinerinius sprendimus, leidžiančius minimizuoti praradimus (prastovas, duomenų praradimą ir pan.), atsiradusius dėl to, kad COD bus realizuota kaip paskirstyta duomenų bazė. Darbo metu reikės išnagrinėti įvairius galimus sistemos variantus, įvertinant įvairius kompromisus (prieinamumas/neprieštaringumas, prieinamumas/patikimumas ir pan.).
44	Saulius Gražulis	Didelės apimties duomenų archyvavimas paskirstytoje duomenų saugykloje	Archiving high volume scientific data in a distributed peer-to-peer repository	Naujausios IUCr (Tarptautinės kristalografų sąjungos, angl. International Union of Crystallography) rekomendacijos siūlo archyvuoti visus pradinius duomenis, panaudotus struktūros nustatymui, įskaitant difrakcijos (išsklaidytų Rentgeno spindulių) vaizdus, užregistruotus monokristalinių difraktometrų. Šios rekomendacijos įgyvendinimas kelia naujus iššūkius -- bus reikalingas gerokai didesnis pastovios atminties (diskų, juostų) kiekis, negu naudotas iki šiol, ir duomenys turi būti prieinami bent jau ateinančius dešimtmečius, t.y. pergyventi kelias kompiuterinės įrangos kartas. Visa tai susiję su papildomomis sąnaudomis ir duomenų laikymo kaštais. Vienas iš galimų šių problemų sprendimo būdų -- panaudoti paskirstytą, daugelio institucijų ir/arba individų palaikomą duomenų archyvavimo sistemą, turinčią pakankamą duomenų perteklumą, užtikrinantį patikimą sistemos darbą ilgą laiką. Tokios sistemos prototipas buvo išbandytas 2018 m. studentų bakalaurų darbų metu. Darbo metu bus siūloma realizuoti veikiančią, mokslininkams tinkamą sistemą Tahoe-LAFS ir/arba IPFS pagrindu.

45	Saulius Gražulis	Vidutinių trimačių simetrijos grupių apskaičiavimas iš keturmačių moduliuotų struktūrų simetrijos operatorių.	Computing average space groups from 4D and higher-dimensional space group operators	Pastaruoju metu daugėja informacijos apie medžiagos būvį, kuris, nors ir turi daugumą kristalo savybių (pvz., sklaido Rentgeno spindulius siaurais koncertuotais atspindžiais), nėra tikras kristalas, nes negali turėti periodinės gardelės, suderinamos su stebima objekto ar sklaidymo vaizdo simetrija, tokia kaip penkto laipsnio simetrijos ašis. Tai -- kvazikristalai (http://en.wikipedia.org/wiki/Quasicrystals) ir (nebendramatės) moduliuotos struktūros. Šioms struktūroms aprašyti kuriamas matematinis aparatas, panaudojantis simetrijos grupių teoriją. Pasirodo, kad neperiodines trimates struktūras galima aprašyti kaip periodinių struktūrų daugiamatėse erdvėse pjūvius. Pavyzdžiui, kai kurias moduliuotas struktūras galima nagrinėti kaip periodinių 4-mačių gardelių pjūvius. Perėjimas į aukštesnių matavimų erdves leidžia panaudoti jau žinomą erdvinių simetrijos grupių mat. aparatą, ir kompaktiškai aprašyti neperiodines struktūras. Darbo metu bus siūloma sukurti programinę įrangą, kuri tikrintų keturmačių simetrijos grupių aprašymus, pagal šiuos aprašymus sukurtų vidutinius nemoduliuotos trimatės simetrijos grupės aprašus, ir integruoti šiuos algoritmus į duomenų bazę COD, kad būtų galima efektyviai kaupti ir tvarkyti neperiodinių medžiagos pavyzdžių aprašymus.
46	Saulius Gražulis	BOINC serverio ir klientų parengimas statistiniams skaičiavimams ir jų pritraukymas COD duomenų bazės analizei	Creating BOINC clients and setting up BOINC server for large volume data analysis in the COD	Statistiniai skaičiavimai, paremti Bajeso statistikos principais, duoda universalią ir koherentišką skaičiavimo metodiką, bet reikalauja itin daug skaičiavimo resursų. Vienas iš būdų tokius resursus surinkti -- panaudoti masinį paralelizmą „savanorių skaičiuotojų“ (angl. "volunteer computing") pateiktuose kompiuteriuose. Šiuo principu yra paremta Berklio universiteto BOINC sistema. Darbo metu bus siūloma: a) paleisti BOINC sistemos serverį; b) parašyti paprasčiausius BOINC klientus; c) parašyti klientus, skirtus COD atstumų ir jungčių parametrų tikimybių pasiskirstymų pasiskirstymų radimui ir atnaujinimui, naudojant Bajeso statistikos metodus, ir skaičiavimų organizavimas.
47	Saulius Gražulis	C kalba parašytų programų transliavimas į Java JVM baitų kodą.	Translating C into Java bytecode	Mūsų turimas CIF sintaksinis analizatorius parašytas C programavimo kalba. C kodas yra efektyvus, perkeliamas į daugelį OS ir skaičiavimo platformų, leidžia sukurti sąsajas (angl. bindings) daugeliui programavimo kalbų: Perl'ui, Pitonui, C++ ir kitoms. Java kalba parašytose programose būtų galima naudoti šią biblioteką JNI sąsajos pagalba, tačiau toks sprendimas Java „pasaulyje“ turi savų trūkumų: kai kurios platformos, pvz. Android/Dalvik arba HTML5/JS, nepalaiko JNI sąsajų, arba šių sąsajų naudojimas per daug sudėtingas, o Java taikomosioms programoms naudojamas klases tenka perkompiliuoti kiekvienai procesoriaus architektūrai vietoj to, kad panaudoti Java baitų kodą ir, jei reikia, turimus JIT optimizuojančius kompiliatorius. Idėja yra surasti transliatorių, kuris transliuotų C kalbos programas į Java virtualios mašinos kodą. Tyrimo eigoje reikės nustatyti ir aprašyti, kaip suderinti C standartą atitinkančias vykdymo aplinkas ir Java virtualias mašinas. Jei reikės, bus modifikuojamas egzistuojantis C kompiliatorius (tcc, lcc arba gcc), nutaikant jį JVM kodo generavimui. Tikslas yra sukompiliuoti turimą CIF sintaksinio analizatoriaus tekstą į gryną JVM baitų kodą.
48	Saulius Gražulis	Taisyklėmis paremtos ekspertinės sistemos sukūrimas COD esančių atomų cheminiams tipams nustatyti	Rule-based expert system for deriving chemical properties from crystal structures	Siūloma paversti molekulių aprašymus Prolog duomenų baze ir užkoduoti chemines žinias taip, kad būtų galima automatiškai gauti išvadas apie molekulių ir jose sujungtų atomų savybes (hibridizaciją, geometriją, dalinius ir formalius krūvius, reakcingumą).
49	Saulius Gražulis	dRel programavimo kalbos realizavimas	Implementing dRel programming language	Siūloma įgyvendinti dRel programavimo kalbos interpretatorių CIF failuose įterptų funkcijų interpretavimui.
50	Saulius Gražulis	Molekulinių mazgų ir sankabų analizė COD duomenų bazėje	Finding molecular knots in the Crystallography Open Database	Molekulių kovalentiniai ryšiai gali būti traktuojami kaip tvirti strypeliai, jungiantys atomus (briaunos, jungiančios grafo viršūnes). Jei tokiame molekuliniame grafe yra ciklai, jie gali sudaryti mazgus arba sankabas (pavyzdžiui, sukabintus žiedus, Boromėjaus žiedus ar sudėtingesnes topologines struktūras). Kol kas nėra efektyvių programų, kurios leistų aptikti ir suklasifikuoti tokias struktūras, aptiktas molekuliniuose medžiagos kristaluose. Darbo metu bus siūloma sukurti programas, generuojančias 3D grafo aprašymą pagal kristalografinės informacijos CIF failus su kristalų struktūromis, pritaikyti šias programas Crystallography Open Database (COD, https://www.crystallography.net/) duomenų bazei, sugeneruoti iš gauto molekulinio grafo mazgo aprašymą, ir pagal mazgo aprašymą pritaikyti įvairius mazgo invariantus skaičiuojančius algoritmus. Darbo pabaigoje sukursime aptiktų mazgų duomenų bazę.

51	Saulius Gražulis	Kvantinės mechanikos metodų pritaikymas kristalografinių duomenų validavimui	Validating experimental crystallographic data using first-principles quantum mechanics	Darbe bus siūloma pritaikyti kelias atviro kodo kvantinės mechanikos programas (Abinit, Quantum Espresso) atviros kristalografinės duomenų bazės Crystallography Open Database (COD, https://www.crystallography.net/) duomenims patikrinti ir galimoms eksperimento ar duomenų tvarkymo klaidoms aptikti.
52	Saulius Gražulis	DNT ir mašinų mokymo pritaikymas kristalų savybėms prognozuoti	Applying ANN and machine learning for crystal property prediction	Nauji Dirbtinių neuroninių tinklų (DNT) ir mašinų mokymo algoritmai leidžia aptikti dėsningumus ir atpažinti bruožus didelėse duomenų masyvuose, kurie seniau buvo neprieinami išsamiai analizei. Atviroje kristalografinėje duomenų bazėje Crystallography Open Database (COD, https://www.crystallography.net/) yra sukaupta virš 450 tūkst įrašų apie kristalų struktūras, o susieti straipsniai talpina informaciją apie šių kristalų savybes. Darbe bus siūloma panaudoti COD DB duomenų imtį DNT ar mašinų mokymo sistemai apmokyti, siekiant prognozuoti įvairias kristalo savybes (pvz. kristalo elementaraus narvelio tūrį, lydymosi temperatūrą ir pan.). Gauti tinklai gali būti naudojami COD ir kitų publikuotų duomenų validavimui, naujų kristalų savybių nustatymui.
53	Saulius Gražulis	Interaktyvios COD recenzavimo svetainės kūrimas	Interactive collaboration platform for the Crystallography Open Database	Interaktyvios programų archyvų svetainės, tokios kaip GitLab, GitGub ar BitBucket, gerai užsirekomendavo programinės įrangos kūrimo procese. Darbe bus siūloma pritaikyti analogiškus programų kūrimo įrankius mokslo duomenims tvarkyti. Atvira kristalografinė duomenų bazė Crystallography Open Database (COD, https://www.crystallography.net/) sėkmingai naudoja Subversijos versijų kontrolės sistemą duomenims versijuoti ir kaupti. Natūralu panaudoti sistemą, analogišką aukščiau minėtoms priemonėms, pvz. Redmine, kuri leistų kristalografams aptarinėti ir taisyti kristalų struktūrų duomenis, panašiai kaip programuotojai aptarinėja ir taiso programas. Darbo metu reikės sukurti COD ir Redmine svetainių sąsają ir išbandyti kristalografinių duomenų valdymo srautą realaus gyvenimo sąlygomis.
54	Saulius Gražulis	COD P1 narvelių skaičiavimas	Computing chemical structures in P1 cell for the Crystallography Open Database	Kristalografiniai duomenų failai pateikia minimalų parametrų rinkinį, būtiną kristalo struktūrai atstatyti naudojant kristalo simetrijos grupės operatorius. Toks aprašymas dažnai nepateikia visos chemikų tikslams reikalingos informacijos; pavyzdžiui, kristale molekulė gali būti aprašyta, nurodant tik jos dalį, o likusi dalis turi būti suskaičiuota, pritaikant informaciją apie simetriją. Toks atvaizdavimo būdas chemikams yra nepatogus ir sukelia sunkumų tolimesnėje duomenų analizėje. Darbe bus siūloma pagaminti iš COD duomenų bazę su pilna informacija apie kristalų elementarius narvelius, t.y. sugeneruojant visus atomus, kurių reikia, norint aprašyti kristalo struktūrą tik elementarių transliacijų pagalba (taip vadinamus P1 narvelius). Šioje duomenų bazėje galima atlikti tolimesnę analizę, pavyzdžiui optinių izomerų paiešką.
55	Saulius Gražulis	Srautinio CIF parserio (sintaksinio analizatoriaus) sukūrimas	Creating a streaming CIF parser	Dabar paplitę Crystallography Interchange File (CIF) failų formato sintaksiniai analizatoriai veika, naudodami DOM modelį, t.y. visas failas perskaitomas į atmintį ir tada apdorojamas. Toks metodas visiškai netinka dideliems konkatenuotiems CIF srautams skaityti, pvz. visiems PDB arba COD duomenų bazių įrašams Unix konvejeryje apdoroti. Siūloma sukurti jau esamo cod-tools sintaksinio analizatoriaus pagrindu (C/Bison) srautinį analizatorių, t.y. tokį analizatorių, kuris perskaitytų ir grąžintų failo informaciją po vieną įrašą, ir leistų kreiptis į save daug kartų, pratęsiant sintaksinę analizę nuo tos failo vietos, kurioje buvo sustojęs.
56	Saulius Gražulis	Kokybiško CIF parserio (sintaksinio analizatoriaus) sukūrimas Java ir C# (.NET) platformoms	High quality CIF parser for Java and .NET platforms	CIF (Crystallography Interchange Format) yra paplitęs struktūruotas duomenų formatas kristalografinių duomenų archyvavimui ir mainams. Yra parašyti kokybiški sintaksiniai šio formato analizatoriai C, Perl ir Python kalbomis. Deja, Java ir .NET aplinkoms šie analizatoriai nėra labai tinkami, nes minėtos platformos sukelia daug keblumų, paleidžiant joms svetimomis kalbomis parašytas bibliotekas. Pvz. Java JNI sąsaja sunkiai perkeliame į mobilias platformas ir dėl to programuotojai labiau vertina „gryna Java“ ("pure Java") parašytus modulius. Darbe bus siūloma perkelti CIF (CIF 1.1 ir CIF 2.0) standarto sintaksinius analizatorius į grynos Java ir C# terpes.
57	Saulius Grigaitis	Blokų grandinių technologijų "įrodymo turtu" protokolai	Blockchain Proof-of-Stake Protocols	Ištirti "įrodymo turtu" (angl. Proof of Stake) protokolus, fokusuojantis į naujausius pasiekimus Ethereum 2.0 "įrodymo turtu" protokole. Pasiūlyti patobulinimus ir juos eksperimentiškai ištirti. (Research Proof-of-Stake protocols focusing on the latest achievements in Ethereum 2.0 Proof-of-Stake protocol. Propose protocol improvements and conduct experiments.)

58	Saulius Grigaitis	Privatumą saugančios išmaniosios sutartys blokų grandinių technologijose	Blockchain Privacy Preserving Smart Contracts	Ištirti privatumą saugančius algoritmus, tinkančius apsaugoti išmaniųjų sutarčių privatumą blokų grandinių technologijose. Tyrimas fokusuosis į naujausius pasiekimus homomorfiniame šifravime ir jų pritaikymą saugoti išmaniųjų sutarčių privatumą vykdant naujos kartos vykdymo aplikose, tokiose kaip EWASM. (Research privacy preserving algorithms suitable for blockchain smart contracts. This research should focus on latest achievements in homomorphic encryption and applying it to preserve privacy of smart contracts on the latest generation execution environments such as EWASM).
59	Saulius Ragaišis	DevOps proceso modeliavimas	DevOps Process Modelling	
60	Viačeslav Pozdniakov	Funkcinės programavimo kalbos su priklausomais tipais kompiliavimas į Go programavimo kalbą	Golang as a compilation target for functional programming languages with dependent types	
61	Vytautas Čyras	Ištirti loginio išvedimo „forward chaining“ ir „backward chaining“ panaudojimą informacinėse sistemose su web-servisais.	Forward chaining and backward chaining logical inference in information systems with web services	
62	Vytautas Čyras	Faktų, pareigų ir teisių modeliavimas Jason sistemoje AgentSpeak kalba agentiniu Belief-Desire-Intention stiliumi	Modeling facts, obligations and rights in Jason using AgentSpeak language in Belief-Desire-Intention” agent-based style	Remtis knyga Bordini, Hübner & Wooldridge „Programming multi-agent systems in AgentSpeak using Jason“ ir atlikti tyrimą. Pavyzdžiuose ištirti agentų „įsitikinimų-norų-ketinimų“ atitikimą faktams, pareigoms ir teisėms.
63	Vytautas Čyras	Faktų, pareigų ir teisių bei jų nesuklastojamumo modeliavimas išmaniųjų sutarčių kontekste. Pasirinkti dominančią tematiką, pvz., „smart contracts“ ir technologiją, pvz., Solidity kalbą; atlikti tyrimą; aprašyti demonstracinius pavyzdžius.	Modeling facts, obligations and rights in smart contracts. Choose the research subject and technology, e.g. Solidity.	Komentaras temai: Pareigų ir teisių modeliavimas yra prieš dešimtmečius įvardinta kryptis teisės informatikoje (legal informatics). Pareigos ir teisės yra iš taip vadinamos privalomybės srities (the Ought realm), o programos ir faktai yra iš esamybės (the Is realm). Is ir Ought nesusijusios sritys ta prasme, kad iš Ought neišplaukia Is. Deontinės logikos terminais iš Obligatory p neišplaukia p. Jeigu privaloma p, pvz., grąžinti knygą į biblioteką, tai dar nereiškia, kad agentas ją grąžins. Yra įvairių sampratų ir realizacijos pareigų įgyvendinimui, pvz., prievartos aktas bauda iš kito agento pusės ir pan.; žr. Jones & Sergot 1993, On the characterisation of law and computer systems: The normative systems perspective.