Federal State Autonomous Educational Institution of Higher Education "Moscow Institute of Physics and Technology (National Research University)"

APPROVED
Head of the Phystech School of Applied Mathematics and Informatics
A.M. Raygorodskiy

Work program of the course (training module)

course:	Computability and Complexity/Вычислимость и вычислительная сложность
major:	Applied Mathematics and Informatics
specialization:	Contemporary Combinatorics/Современная комбинаторика
	“Pusk” Online and Supplementary Education Centre
	Chair of Discrete Mathematics
term:	1
qualification:	Master

Semester, form of interim assessment: 2 (spring) - Grading test

Academic hours: 45 AH in total, including:
lectures: 15 AH.
seminars: 30 AH.
laboratory practical: 0 AH.

Independent work: 45 AH.

In total: 90 AH, credits in total: 2

Author of the program: D.V. Musatov, candidate of physics and mathematical sciences, associate professor

The program was discussed at the Chair of Discrete Mathematics 08.08.2022

Annotation

This course is intended to provide a theoretical base of computer science. It can be also called “Philosophy of computing” or “Main concepts of computer science”. Unlike the courses on mathematical programs, it is focused on notions and ideas rather than on detailed proofs. The main goal is to provide intuition about what is an algorithmic problem, which problems can be solved in principle and which problems can be solved efficiently.

1. Study objective

Purpose of the course

mastering additional chapters of complex calculations.

Tasks of the course

- students mastering basic knowledge (concepts, concepts, methods and models) in the field of complex computing;
- acquisition of theoretical knowledge and practical skills in the field of complex computing;
- providing advice and assistance to students in conducting their own theoretical research in the field of complex computing.

2. List of the planned results of the course (training module), correlated with the planned results of the mastering the educational program

Mastering the discipline is aimed at the formation of the following competencies:

Code and the name of the competence	Competency indicators
UC-1 Use a systematic approach to critically analyze a problem, and develop an action plan	UC-1.1 Systematically analyze the problem situation, identify its components and the relations between them
	UC-1.3 Develop a step-by-step strategy for achieving a goal, foresee the result of each step, evaluate the overall impact on the planned activity and its participants
UC-2 Able to manage a project through all stages of its life cycle	UC-2.1 Set an objective within a defined scientific problem; formulate the agenda, relevance, significance (scientific, practical, methodological or other depending on the project type), forecast the expected results and possible areas of their application
	UC-2.2 Forecast the project outcomes, plan necessary steps to achieve the outcomes, chart the project schedule and monitoring plan
	UC-2.3 Organize and coordinate the work of project stakeholders, provide the team with necessary resources
UC-6 Determine priorities and ways to improve performance through self-assessment	UC-6.1 Achieve personal growth and professional development, determine priorities and ways to improve performance
Gen.Pro.C-1 Address current challenges in fundamental and applied mathematics	Gen.Pro.C-1.1 Apply fundamental scientific knowledge, new scientific principles, and research methods in applied mathematics and computer science
	Gen.Pro.C-1.2 Consolidate and critically assess professional experience and research findings
	Gen.Pro.C-1.3 Understand interdisciplinary relations in applied mathematics and computer science and apply them in professional tasks
Gen.Pro.C-2 Iimprove upon and implement new mathematical methods in applied problem solving	Gen.Pro.C-2.2 Assess the relevance and practical importance of applied mathematical research in professional settings
Gen.Pro.C-4 Combine and adapt current information and communications technologies (ICTs) to meet professional challenges	Gen.Pro.C-4.1 Use ICTs to search and analyze professional information, highlight, structure, format, and present it in the form of analytical reviews with sound conclusions and recommendations

3. List of the planned results of the course (training module)

As a result of studying the course the student should:

know:

- fundamental concepts, laws, theories of complex calculations;
- modern problems of the relevant sections of complex calculations;
- concepts, axioms, methods of proof and proof of the main theorems in the sections included in the basic part of the cycle;
- basic properties of the corresponding mathematical objects;
- analytical and numerical approaches and methods for solving typical applied problems of complex calculations.

be able to:

- understand the task;
- use your knowledge to solve fundamental and applied problems of EC;
- evaluate the correctness of task statements;
- strictly prove or disprove the statement;
- independently find algorithms for solving problems, including non-standard ones, and conduct their analysis;
- independently see the consequences of the results;
- accurately represent mathematical knowledge in the field of complex computing in oral and written form.

master:

- skills of mastering a large amount of information and solving problems (including complex ones);
- skills of independent work and mastering new disciplines;
- the culture of the formulation, analysis and solution of mathematical and applied problems requiring the use of mathematical approaches and EC methods for their solution;
- the subject language of complex calculations and the skills of competent description of problem solving and presentation of the results.

4. Content of the course (training module), structured by topics (sections), indicating the number of allocated academic hours and types of training sessions

4.1. The sections of the course (training module) and the complexity of the types of training sessions

№	Topic (section) of the course	Types of training sessions, including independent work			
		Lectures	Seminars	Laboratory practical	Independent work
1	What is an algorithm? Computation models. Computable functions. General purpose computable functions. Computing resources.	2	4		4
2	Algorithmically unsolvable problems: self-applicability problem, halting problem, “busy beavers”, etc.	2	4		6
3	Links between computability and formal arithmetic. Gödel's Incompleteness Theorem.	2	4		6
4	The concept of polynomial reducibility (according to Karp). NP-hardness and NP-completeness. Cook-Levin theorem and examples of NP complete problems from combinatorics, logic, graph theory, etc.	2	4		6

5	Probabilistic computing. Complexity classes BPP, RP and coRP. Reducing the error. Probabilistic tests of simplicity and equality of polynomials.	2	4		6
6	Average Difficulty and Foundations of Cryptography. One-way functions and pseudo-random number generators. Cryptographic protocols, their correctness and reliability.	2	4		7
7	Вероятностно проверяемые доказательства и их связь с приближённым решением NP-трудных задач.	3	6		10
AH in total		15	30		45
Exam preparation		0 AH.			
Total complexity		90 AH., credits in total 2			

4.2. Content of the course (training module), structured by topics (sections)

Semester: 2 (Spring)

1. What is an algorithm? Computation models. Computable functions. General purpose computable functions. Computing resources.

Decidable and enumerable sets. Several equivalent properties and basic properties. Post's theorem.

2. Algorithmically unsolvable problems: self-applicability problem, halting problem, “busy beavers”, etc.

The concept of m-reducibility. Construction of a non-enumerable set whose complement is also non-enumerable (the totality problem).

3. Links between computability and formal arithmetic. Gödel's Incompleteness Theorem.

Computing with an oracle: the concept and its properties. Relativization of computability. Non-deterministic computing. Complexity classes P, NP, coNP. The problem of equality between P and NP.

4. The concept of polynomial reducibility (according to Karp). NP-hardness and NP-completeness. Cook-Levin theorem and examples of NP complete problems from combinatorics, logic, graph theory, etc.

Spatial complexity. Complexity classes PSPACE, L and NL. Game-theoretic interpretation of PSPACE.

5. Probabilistic computing. Complexity classes BPP, RP and coRP. Reducing the error. Probabilistic tests of simplicity and equality of polynomials.

Interactive communication protocols and evidence systems. Complex IP class: examples and applications.

6. Average Difficulty and Foundations of Cryptography. One-way functions and pseudo-random number generators. Cryptographic protocols, their correctness and reliability.

Zero knowledge proofs. Perfectly, statistically and computationally zero knowledge properties.

7. Вероятностно проверяемые доказательства и их связь с приближённым решением NP-трудных задач.

Derandomization techniques and pseudo-random designs. Why are we confident that probabilistic algorithms do not expand computational power (i.e. P = BPP).

5. Description of the material and technical facilities that are necessary for the implementation of the educational process of the course (training module)

A standard classroom.

6. List of the main and additional literature, that is necessary for the course (training module) mastering

Main literature

1. Введение в сложность вычислений [Текст] / В. Н. Крупский - М.Факториал Пресс,2006

2. Коммуникационная сложность [Текст] / А. А. Разборов ; пер. с англ. Ю. Л. Притыкина ; под ред. В. А. Клепцына, С. М. Львовского - М.МЦНМО,2012

Additional literature

1. Вычислительная математика и структура алгоритмов [Текст] : 10 лекций о том, почему трудно решать задачи на вычислительных системах параллельной архитектуры и что надо знать дополнительно, чтобы успешно преодолевать эти трудности : учебник для вузов / В. В. Воеводин ; Моск. гос. ун-т им. М. В. Ломоносова .— 2-е изд., стереотип. — М. : Изд-во Моск. ун-та, 2010 .— 168 с.

7. List of web resources that are necessary for the course (training module) mastering

http://dm.fizteh.ru

8. List of information technologies used for implementation of the educational process, including a list of software and information reference systems (if necessary)

Multimedia technologies can be employed during lectures and practical lessons, including presentations.

9. Guidelines for students to master the course

1. It is recommended to successfully pass the test papers, as this simplifies the final certification in the subject.
2. To prepare for the final certification in the subject, it is best to use the lecture materials.

SUPPLEMENT

Assessment funds for course (training module)

major:	Applied Mathematics and Informatics
specialization:	Contemporary Combinatorics/Современная комбинаторика
	“Pusk” Online and Supplementary Education Centre
	Chair of Discrete Mathematics
term:	1
qualification:	Master

Semester, form of interim assessment: 2 (spring) - Grading test

Author: D.V. Musatov, candidate of physics and mathematical sciences, associate professor

1. Competencies formed during the process of studying the course

Code and the name of the competence	Competency indicators
UC-1 Use a systematic approach to critically analyze a problem, and develop an action plan	UC-1.1 Systematically analyze the problem situation, identify its components and the relations between them
	UC-1.3 Develop a step-by-step strategy for achieving a goal, foresee the result of each step, evaluate the overall impact on the planned activity and its participants
UC-2 Able to manage a project through all stages of its life cycle	UC-2.1 Set an objective within a defined scientific problem; formulate the agenda, relevance, significance (scientific, practical, methodological or other depending on the project type), forecast the expected results and possible areas of their application
	UC-2.2 Forecast the project outcomes, plan necessary steps to achieve the outcomes, chart the project schedule and monitoring plan
	UC-2.3 Organize and coordinate the work of project stakeholders, provide the team with necessary resources
UC-6 Determine priorities and ways to improve performance through self-assessment	UC-6.1 Achieve personal growth and professional development, determine priorities and ways to improve performance
Gen.Pro.C-1 Address current challenges in fundamental and applied mathematics	Gen.Pro.C-1.1 Apply fundamental scientific knowledge, new scientific principles, and research methods in applied mathematics and computer science
	Gen.Pro.C-1.2 Consolidate and critically assess professional experience and research findings
	Gen.Pro.C-1.3 Understand interdisciplinary relations in applied mathematics and computer science and apply them in professional tasks
Gen.Pro.C-2 Iimprove upon and implement new mathematical methods in applied problem solving	Gen.Pro.C-2.2 Assess the relevance and practical importance of applied mathematical research in professional settings
Gen.Pro.C-4 Combine and adapt current information and communications technologies (ICTs) to meet professional challenges	Gen.Pro.C-4.1 Use ICTs to search and analyze professional information, highlight, structure, format, and present it in the form of analytical reviews with sound conclusions and recommendations

2. Competency assessment indicators

As a result of studying the course the student should:

know:

- fundamental concepts, laws, theories of complex calculations;
- modern problems of the relevant sections of complex calculations;
- concepts, axioms, methods of proof and proof of the main theorems in the sections included in the basic part of the cycle;
- basic properties of the corresponding mathematical objects;
- analytical and numerical approaches and methods for solving typical applied problems of complex calculations.

be able to:

 understand the task;
 use your knowledge to solve fundamental and applied problems of EC;
 evaluate the correctness of task statements;
 strictly prove or disprove the statement;
 independently find algorithms for solving problems, including non-standard ones, and conduct their analysis;
 independently see the consequences of the results;
 accurately represent mathematical knowledge in the field of complex computing in oral and written form.

master:

 skills of mastering a large amount of information and solving problems (including complex ones);
 skills of independent work and mastering new disciplines;
 the culture of the formulation, analysis and solution of mathematical and applied problems requiring the use of mathematical approaches and EC methods for their solution;
 the subject language of complex calculations and the skills of competent description of problem solving and presentation of the results.

3. List of typical control tasks used to evaluate knowledge and skills

The grade for the course consists of 3 home assignments (each gives 10% of the final grade), the midterm (30%) and the final test (40%). Home assignments contain several problems and represent the three main blocks: computability, basics of complexity, and interactive protocols. The midterm contains computability and theory of NP-completeness, the final test contains all topics, but with greater emphasis on the second half of the course. The midterm and the final test may contain not only problems, but also multiple-choice questions and some theoretical questions: for instance, on definitions.

Example home assignment problems

1. Let f: N→N be a nondecreasing function approaching infinity. Prove that there exists an undecidable set A such that for all k the set A∩{0,1,…,k} consists of at most f(k) elements.
2. Prove that a given set is neither enumerable, nor co-enumerable.
3. Prove that a given language is PSPACE-complete.
4. Provide an interactive proof system for a given language.
5. For a given puzzle construct a computationally zero-knowledge protocol proving that an equilibrium exists. This protocol should not use a reducibility for some other problem.
6. Prove that for some ρ approximate solution of a given optimization problem with factor ρ is NP-hard.

Examples of multiple-choice problems from the midterm and the final

1. Which of the following properties imply that the set is enumerable?
   a. Decidability of the set
   b. Infinity of the set
   c. Co-finiteness of the set
   d. Enumerability of the complement
   e. Enumerability of some subset
2. For various complexity assumptions draw a Euler's diagram for the following classes: coNP,BPP,PSPACE,L,IP.
3. Which variations of the definition do not change the class IP?

Examples or ordinary problems from the midterm and the final

1. Provide NP-complete languages A and B such that A∩B∈P.
2. Prove NP-completeness of a given language.
3. Let f:{0,1}^n→{0,1}^n be a one-way function and g:{0,1}^n→{0,1}^n be a polynomially computable function. Prove that the function h:{0,1}^2n→{0,1}^2n defined by h(xy)=f(g(x))y is also one-way.
4. Derandomize the given approximation algorithm by using the method of conditional expectations.

4. Evaluation criteria

1. Computation models: single-tape and multi-tape Turing machines. Turing's thesis in strong form.

2. Measurement of the running time of the algorithm. Class P and examples of tasks from it.

3. NP class: two definitions and their equivalence. Class coNP. Polynomial Karp reducibility and its properties. NP-hard and NP-complete problems. Hierarchy Theorems.

4. Ludner's theorem on the existence of NP-intermediate problems. Measurement of the zone of operation of the algorithm. PSPACE class. Savich's theorem. PSPACE-complete tasks.

5. Classes L, NL and coNL. NL-completeness. NL = coNL.

6. Probabilistic algorithms. Classes of BPP and RP. Probabilistic simplicity verification algorithms. Interactive evidence and IP class.

7. Interactive proofs with common random bits and class AM.

8. IP = PSPACE.

9. Basic concepts of cryptography: one-way functions and pseudo-random generators.

10. Zero-disclosure evidence.

11. Approximate determination of the optimum: polynomial algorithms for individual problems and the PCP theorem.

12. Introduction to the theory of Kolmogorov complexity.

13. Introduction to the theory of quantum computing.

Assessment “excellent (10)” is given to a student who has displayed comprehensive, systematic and deep knowledge of the educational program material, has independently performed all the tasks stipulated by the program, has deeply studied the basic and additional literature recommended by the program, has been actively working in the classroom, and understands the basic scientific concepts on studied discipline, who showed creativity and scientific approach in understanding and presenting educational program material, whose answer is characterized by using rich and adequate terms, and by the consistent and logical presentation of the material;

Assessment “excellent (9)” is given to a student who has displayed comprehensive, systematic knowledge of the educational program material, has independently performed all the tasks provided by the program, has deeply mastered the basic literature and is familiar with the additional literature recommended by the program, has been actively working in the classroom, has shown the systematic nature of knowledge on discipline sufficient for further study, as well as the ability to amplify it on one’s own, whose answer is distinguished by the accuracy of the terms used, and the presentation of the material in it is consistent and logical;

Assessment “excellent (8)” is given to a student who has displayed complete knowledge of the educational program material, does not allow significant inaccuracies in his answer, has independently performed all the tasks stipulated by the program, studied the basic literature recommended by the program, worked actively in the classroom, showed systematic character of his knowledge of the discipline, which is sufficient for further study, as well as the ability to amplify it on his own;

Assessment “good (7)” is given to a student who has displayed a sufficiently complete knowledge of the educational program material, does not allow significant inaccuracies in the answer, has independently performed all the tasks provided by the program, studied the basic literature recommended by the program, worked actively in the classroom, showed systematic character of his knowledge of the discipline, which is sufficient for further study, as well as the ability to amplify it on his own;

Assessment “good (6)” is given to a student who has displayed a sufficiently complete knowledge of the educational program material, does not allow significant inaccuracies in his answer, has independently carried out the main tasks stipulated by the program, studied the basic literature recommended by the program, showed systematic character of his knowledge of the discipline, which is sufficient for further study;

Assessment “good (5)” is given to a student who has displayed knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, who while not being sufficiently active in the classroom, has nevertheless independently carried out the main tasks stipulated by the program, mastered the basic literature recommended by the program, made some errors in their implementation and in his answer during the test, but has the necessary knowledge for correcting these errors by himself;

Assessment “satisfactory (4)” is given to a student who has discovered knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, who while not being sufficiently active in the classroom, has nevertheless independently carried out the main tasks stipulated by the program, learned the main literature but allowed some errors in their implementation and in his answer during the test, but has the necessary knowledge for correcting these errors under the guidance of a teacher;

Assessment “satisfactory (3)” is given to a student who has displayed knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, not showed activity in the classroom, independently fulfilled the main tasks envisaged by the program, but allowed errors in their implementation and in the answer during the test, but possessing necessary knowledge for elimination under the guidance of the teacher of the most essential errors;

Assessment “unsatisfactory (2)” is given to a student who showed gaps in knowledge or lack of knowledge on a significant part of the basic educational program material, who has not performed independently the main tasks demanded by the program, made fundamental errors in the fulfillment of the tasks stipulated by the program, who is not able to continue his studies or start professional activities without additional training in the discipline in question;

Assessment “unsatisfactory (1)” is given to a student when there is no answer (refusal to answer), or when the submitted answer does not correspond at all to the essence of the questions contained in the task.

5. Methodological materials defining the procedures for the assessment of knowledge, skills, abilities and/or experience

During examination the student are allowed to use the program of the discipline.